

WAVLINK



see the world

User Manual

**WiFi6 AX3000 Dual Band Gigabit High
Performance Mesh Router**

Model: MIGHTY EX1 Pro

@WavlinkOfficial

@WavlinkTechSupport

Table of contents:

- About This Guide
 - Conventions
 - More Info
 - Speed/Coverage Disclaimer
- Chapter 1 Overview
 - Overview
 - Basic Info
 - LED Indicators
 - Specifications
 - In the Box
- Chapter 2 How to Connect
 - 1.Prepare the Modem
 - 2. Install Your Router
 - 3. Configure the Router via Web Browser
 - Mode Selection
 - Router Mode
 - LAN Bridge (AP Mode)
 - Repeater Mode
- Chapter 3 Network Management
 - Network Setting
 - LAN Setting
 - Setting Static IP Binding
 - Setting IPv6
 - IPTV Setting
 - Configuring IPTV
 - Setting Dynamic DNS
 - SQM QoS
- Chapter 4 Managing Wireless Network
 - Wireless
 - Configuring Wireless Network
 - Advanced Settings
 - Schedule (Wireless Timer Switch)
 - Guest Wi-Fi
 - Parental Wi-Fi
- Chapter 5 Mesh

- Mesh Configuration
 - Adding New Mesh Device
 - Advanced Settings
 - Topology Map
- Chapter 6 Net Guardian
 - Secure DNS
- Chapter 7 NAT Forwarding
 - UPnP Settings
 - Port Forwarding
 - DMZ
 - Hardware NAT
- Chapter 8 Network Security
 - Firewall
 - ALG Configuration
 - MAC Filter
- VPN-Server-Client
 - title: Chapter 9 VPN Server and Client hide_table_of_contents: false
 - VPN Server and Client
 - VPN Server Configuration
 - Open VPN Server Configuration
 - Use WireGuard VPN Server
 - VPN Client Configuration
 - PPTP/L2TP VPN Client Configuration
 - OpenVPN Client Configuration
 - WireGuard VPN Client Configuration
 - ZeroTier Configuration
- Chapter 10 Remote Access
 - Remote Web Access
 - Cloud APP
- Chapter 11 NET Tools
 - Network Check
 - Diagnostics
 - Wake-On-LAN
- Chapter 12 System Setting
 - Firmware Upgrade
 - Local Upgrade
 - Online Upgrade:

- [Change Password](#)
- [System Log](#)
- [Time Zone](#)
- [Led Control](#)
- [Backup & Restore](#)
 - [Backup the current configuration of the router](#)
 - [Restore the router's configuration:](#)
 - [Reset the router to the default factory settings](#)
- [Scheduled Reboot](#)
 - [Set Scheduled Reboot Plan](#)
- [Chapter 13 Logoff](#)
 - [Logoff](#)
- [Chapter 14 FAQ](#)
 - [FAQ](#)
 - [GNU General Public License Notice](#)
 - [After-sale Service](#)
- [Chapter 15 Safety and Emission Statement](#)

About This Guide

This guide is a complement to Quick Installation Guide. The Quick Installation Guide provides instructions for quick internet setup, while this guide contains details of each function and demonstrates how to configure them.

When using this guide, please notice that features of the router may vary slightly depending on the model and software version you have, and on your location, language, and internet service provider. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

Conventions

In this guide the following conventions are used :

Convention	Description
<u>Underlined</u>	Underlined words or phrases are hyperlinks. You can click to redirect to a website or a specific section.
Teal	The content and text that needs to be emphasized on the web page is the theme color #1D428A , including menus, items, buttons, etc.
>	The menu structures to show the path to load the corresponding page. For example, More > Network > Mode Selection means the Mode Selection function page is under the Network menu that is located in the More tab.
Note:	Do not ignore this type of comment, it is to remind you to better use the device, to avoid the operation of the error that will cause the function to be invalid.
Tips:	Indicates important information that helps you make better use of your device.

More Info

The latest software, management app and utility are available from the Download Center at <https://docs.wavlink.xyz/Firmware/> .

A quick installation guide can be found in this guide.

Specifications can be found on the product page at <https://docs.wavlink.xyz/>.

If you encounter any issues, please don't hesitate to email contact@wavlink.com to provide feedbacks or contact online customer service, thank you !

Speed/Coverage Disclaimer

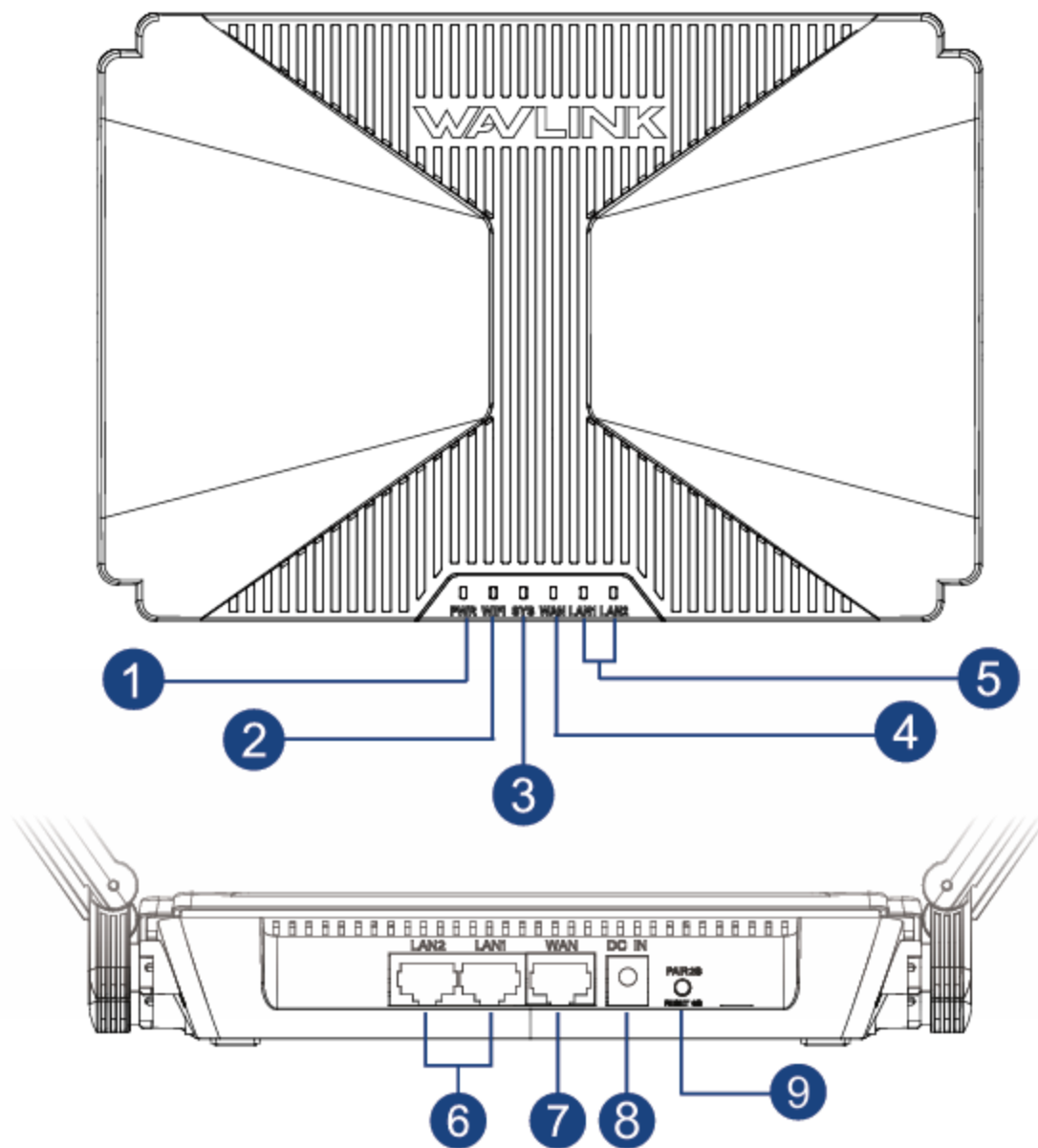
*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of 1) environmental factors, including building materials, physical objects, and obstacles, 2) network conditions, including local interference, volume and density of traffic, product location, network complexity, and network overhead, and 3) client limitations, including rated performance, location, connection, quality, and client condition.

Chapter 1 Overview

This chapter contains the following sections :

- [Overview](#)
- [Basic Info](#)
- [LED Indicators](#)
- [Specifications](#)
- [In the Box](#)

Overview



- ① Power LED
- ② WiFi LED
- ③ SYS LED
- ④ 1 x WAN Port LED
- ⑤ 2 x LAN Port LED
- ⑥ 2 x LAN Port
- ⑦ 1 x WAN Port
- ⑧ Power Port

⑨ PAIR/Reset Button

Pair Button:

Press and hold for **2** seconds to pair with the existing Everything Mesh Wi-Fi system.

Reset Button:

Press and hold for at least **6** seconds to restore the router.

Basic Info

Default IP: 192.168.20.1

Login: <http://wavlogin.link>

Mesh SSID: WAVLINK-Mesh_XXXX

Official Website: www.wavlink.com

Technical Support: support@wavlink.com

LED Indicators

LED	Status	Description
Wi-Fi	Solid on	Wi-Fi enabled
Wi-Fi	Off	Wi-Fi disabled
WAN	Blinking	The WAN port is transmitting or receiving data
WAN	Off	The WAN port is not connected properly
LAN1/2	Blinking	The LAN port is transmitting or receiving data
LAN1/2	Off	The LAN port is not connected properly
Power	Solid on	Powered on
Power	Off	Powered off
SYS	Fast flashing	The device has no Internet connection

LED	Status	Description
SYS	Slow flashing	The device is pairing
SYS	Solid on	The device has Internet connection

Specifications

- WiFi 6 802.11ax, 2.4GHz:573Mbps; 5GHz: 2402Mbps.
- The BSS coloring technology enables better spatial reuse.
- The WiFi 6 MU-MIMO and OFDMA techniques have greatly improved the device efficiency and performance.
- The TWT is a resource managing technique that reduces more power consumption.
- Security: WPA3-SAE/WPA2-PSK MIX, WPA2-PSK, WPA-PSK/WPA2-PSK MIX.
- Support IPV4/IPV6.
- Support 1 x 1000Mbps WAN port, 2 × 1000Mbps LAN ports.
- Antenna: 4 x high-gain & foldable antennas; 1 x built-in antenna.

In the Box

- 1 × WiFi 6 AX3000 Dual Band Gigabit High Performance Mesh Router
- 1 x Power Adapter
- 1 x Ethernet Cable
- 1 x Quick Start Guide

Chapter 2 How to Connect

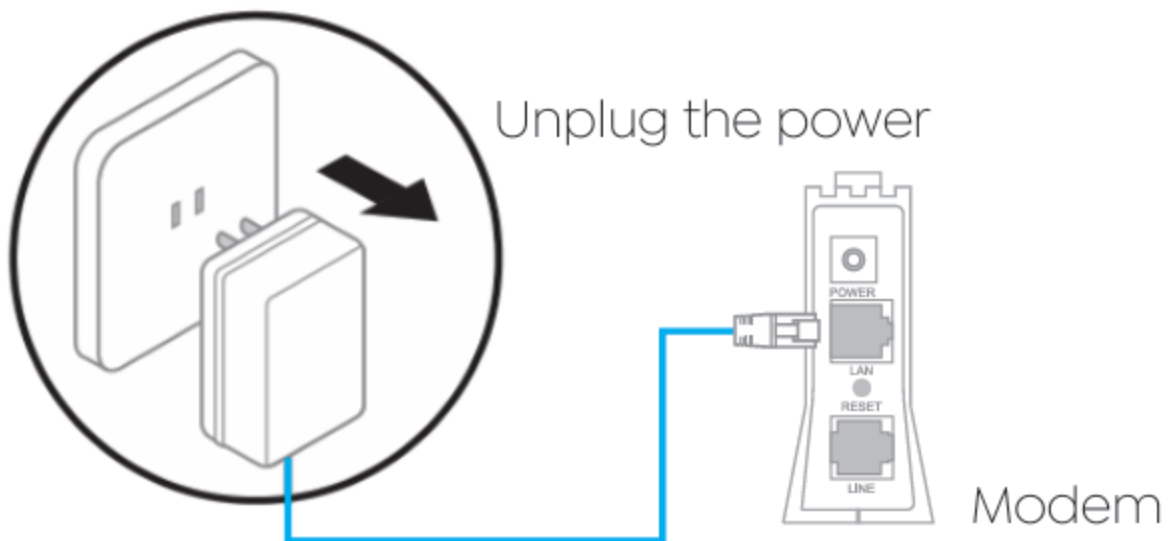
- [Mode Selection](#)

1.Prepare the Modem

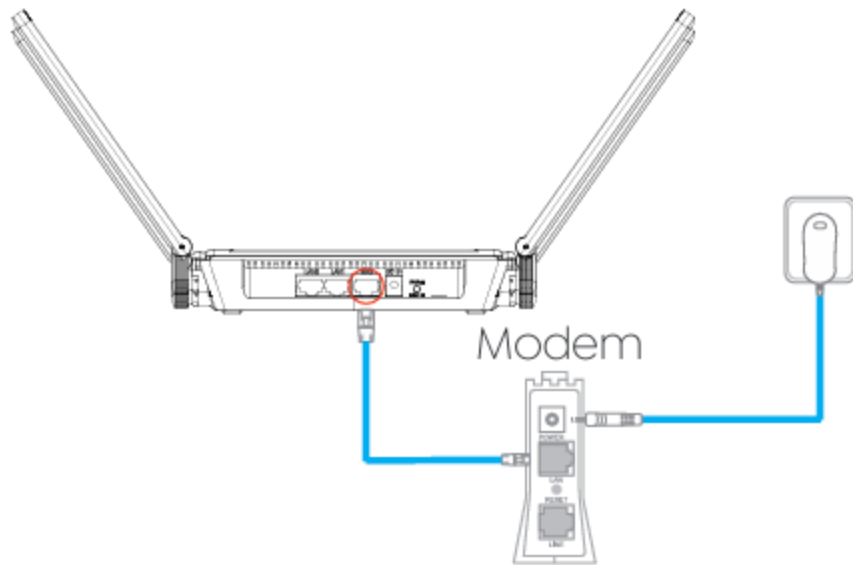
① Unplug the power adapter from your DSL modem. If the modem has backup battery, please remove it.

i NOTE

If using a DSL Internet connection, obtain the login credentials (username/password) from your Internet Service Provider (ISP) to properly configure your wireless router.



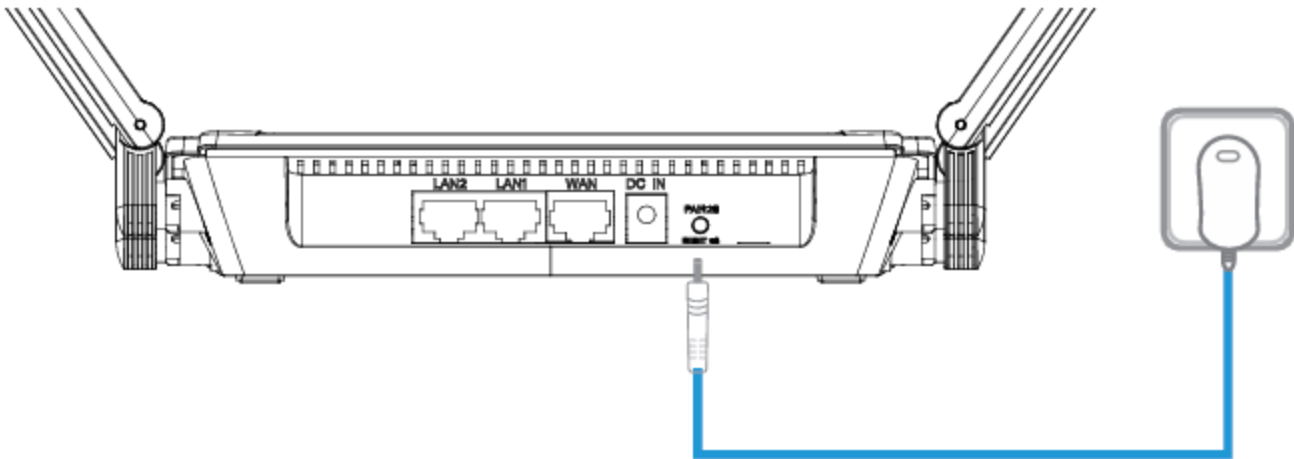
- ② Use the provided Ethernet cable to connect the modem to the WAN port of the router.
- ③ Plug the modem into a power outlet and turn it on.



- ④ Check the indicator lights on the modem to confirm a stable Internet connection.

2. Install Your Router

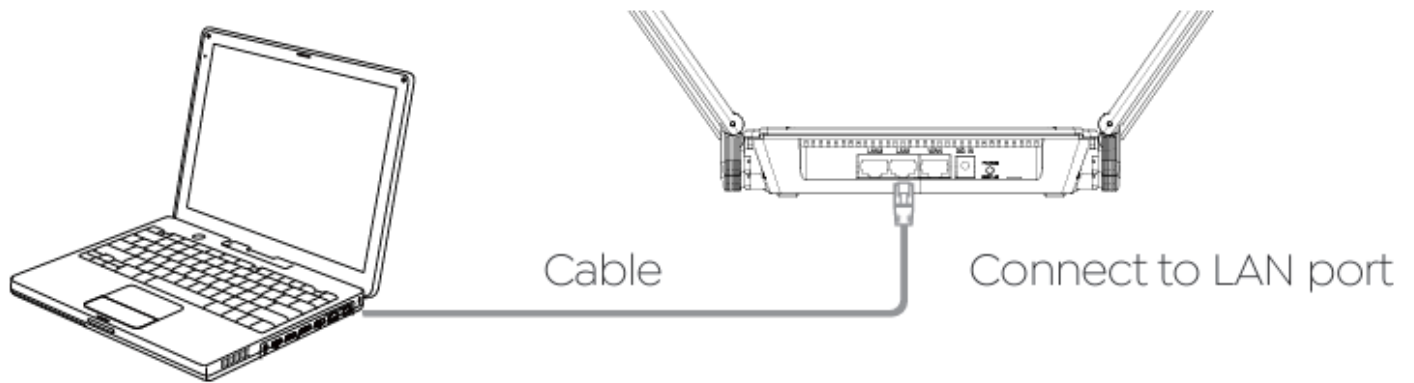
- ① Insert the power adapter into the router's DC IN port and press the power switch (if applicable; some models lack a physical switch).



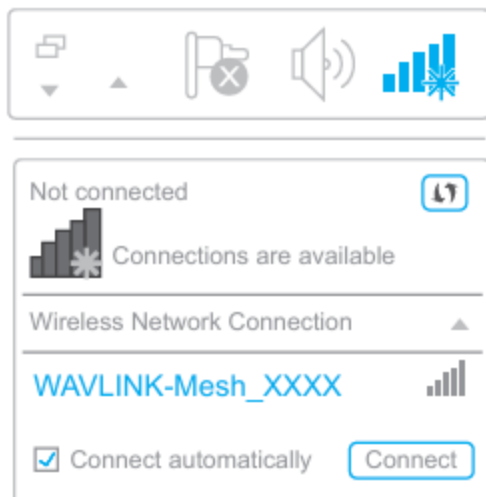
- ② Wait for about 2-3 minutes, then the router is ready.

3. Configure the Router via Web Browser

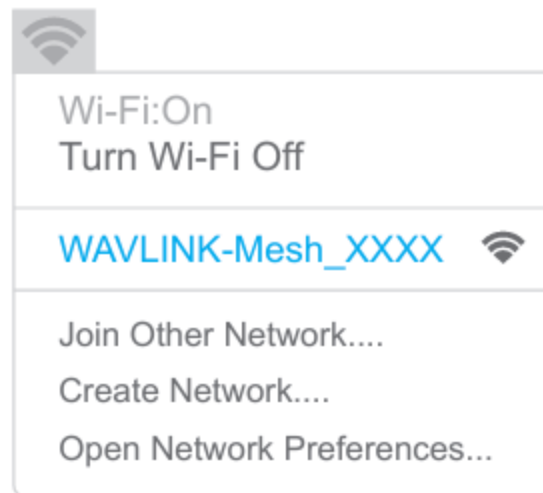
- ① Wired Connection: Use another Ethernet cable to connect your computer to one of the LAN ports on the router.



② Wireless Connection: On your laptop or smartphone, connect to the default SSID printed on the router: WAVLINK-Mesh_XXXX.



For Windows users



For Mac users

③ Open a web browser (via wired or wireless connection) and enter <http://wavlogin.link> in the address bar. You will automatically enter the WAVLINK router initial setup page. If not, manually enter 192.168.20.1 in the browser's address bar and follow the instructions. Please set a new administrator password and then enter the password you set to log in.

Welcome to WAVLINK

[EXPERIENCE NOW](#)[Click here to download the WavRouter APP](#)

④ Please set a new administrator password and then enter the password you set to log in.

Set new administrator password

New password

Confirm new password

[CONFIRM](#)

Welcome to WAVLINK

LOGIN

[Forgot password?](#)[Click here to download the WavRouter APP](#)

⑤ Please choose a WAN Type.

Internet access method

WAN Type

DHCP ▾

DHCP assigned by upstream device.

Internet VLAN ID



Custom MTU



MAC Clone



MAC Clone :

If you select DHCP, you need to choose whether to clone the MAC address. When you first access the Internet through their cable modem, some ISPs register the MAC address of your computer. If you add a router to the network to share an Internet connection, the ISP will not accept it because the MAC address has changed. Therefore, we need to clone the MAC address of your computer to the router.

Auto Mesh



Auto Mesh :

When this function is turned on, the device automatically switches to mesh router or mesh extender mode, depending on the network topology. Otherwise, the device keeps in mesh router mode.

NEXT

① WHICH WAN TYPE AM I SUPPOSED TO CHOOSE?

- If you choose "DHCP", you will need to select whether to clone the MAC address. Some ISPs register the MAC address of your computer when you first access the Internet through their

cable modem, we need to clone the MAC address of your computer to the router.

- If you choose "PPPoE", enter the "Username" and "Password" provided by your ISP. PPPoE is usually designed for such as DSL or fiber optics.
- If you choose "Static IP", enter a specified IP parameters including IP address, Subnet Mask, Gateway, DNS1 and DNS2 provided by your ISP.

⑥ Select your Country/Region and Time Zone. For your network security, please set passwords for 2.4G and 5G Wi-Fi.

The screenshot shows the WAVLINK web interface. At the top is a dark blue header with the WAVLINK logo and the tagline 'see the world'. Below the header is a white form area. The form is divided into two main sections: 'Country code/Time zone' and 'Wi-Fi Settings'. In the 'Country code/Time zone' section, there are two dropdown menus: 'Country/Region' set to 'Global' and 'Time Zone' set to '(UTC+08:00) Beijing, Chongqing, HongKong, Urumqi'. In the 'Wi-Fi Settings' section, there is a 'Dual-band convergence' toggle switch which is currently turned on. Below this, there are input fields for '2.4G SSID' (set to 'WAVLINK-Mesh_0404') and '2.4G Wi-Fi Password' (with a placeholder 'Please enter the 2.4G Wi-Fi password.'). There are also input fields for '5G SSID' (set to 'WAVLINK-Mesh_0404_5G') and '5G Wi-Fi Password' (with a placeholder 'Please enter the 5G Wi-Fi password.'). A 'Dual-band convergence' toggle switch is also present between the 2.4G and 5G settings, which is currently turned on. At the bottom of the form are two buttons: 'BACK' and 'SAVE'.

WAVLINK Official Website | Copyright 2026 WAVLINK Technology Co., Ltd All Rights Reserved.

i NOTE

The Dual-Band convergence switch is on by default. 2.4G WiFi and 5G WiFi use the same SSID and password. Turning off the Dual-Band convergence switch allows you to set the SSID and password for 2.4G WiFi and 5G WiFi separately.

⑦ Setting is successful, wait for the setup to complete.

**Settings have been successfully applied. Please wait for the setup to complete.
Use the new Wi-Fi password to reconnect to the network.**

Wi-Fi Name :

WAVLINK-Mesh_9292

Wi-Fi Password :

***** 



Scan the QR code to download the WavRouter APP for easier router management



100%,Please refresh...

REFRESH

Mode Selection

Configure router's working mode according to your actual requirement.

1 . Enter **More>Network>Mode Selection**.

2 . Select appropriate working mode from the **Mode Selection** list: **Router Mode**, **LAN Bridge (AP Mode)** or **Repeater Mode**.

Router Mode

- In routing mode, the router converts Wi-Fi signals to wireless Internet access for devices by connecting to the network operator's wired network, and provides wired Internet access for devices through a wired port.

Mode Selection

Mode Selection

Router Mode

WAN Type

DHCP

Internet VLAN ID



ID Number

0

Cloud App



Auto Mesh



Auto Mesh :

When this function is turned on, the device automatically switches to mesh router or mesh extender mode, depending on the network topology. Otherwise, the device keeps in mesh router mode.

WAN Status

Connected

SAVE

- **WAN Type: DHCP, PPPoE or Static IP**, inputting the corresponding parameters is required for PPPoE or Static IP.
- **Internet VLAN ID**: After enabling it, input **ID Number**. You should consult the ISP about the detailed configurations.
- **Cloud App**: It allows you to control devices remotely from the cloud using the APP.
- **Auto Mesh**: If it is enabled, the device will automatically switch to Mesh Router Mode or Mesh Extender Mode depending on the network topology; If it is disabled, the device will keep Mesh Router Mode.

LAN Bridge (AP Mode)

- In the AP mode of extending the existing network, you should confirm your device's WAN port has connected to the Internet using the Ethernet cable. One note is that some functions are not available in this mode.

Mode Selection

Mode Selection

LAN Bridge (AP Mode) ▼

Smart DHCP Service



WAN Status

Connected

SAVE

- **Smart DHCP Service:** If it is enabled, the router will configure IP service without connecting to the upper router. Please disable it if it is not required.

Repeater Mode

- In the repeater mode, to extend the Wi-Fi coverage, this router works as a wireless repeater of the upper router. One note is that some functions are not available in this mode.

Mode Selection

Mode Selection

Repeater Mode ▼

NEXT

- 1) Click **NEXT** to rescan the Wi-Fi signal.

Mode Selection

☒ Select Wi-Fi

☐ Manual Input



Scan Time 60s

RESCAN

NEXT

- 2) Select the wireless signal to be relayed, click **NEXT**.
- 3) If the network to be added is not found, click **RESCAN** to rediscover the network. Or select **Manual Input** to set it up.

Mode Selection

☒ Select Wi-Fi

☐ Manual Input

Please select the wireless signal to be relayed

5G/2.4G

	WL531MX3-6E23-5G		☐
	ED55_CSCSCSCS_5G		☐
	winstar_5g		☐
	WAVLINK_Guest		☐
	Parental-Wi-Fi		☐
	ZZH-WIFI_5G		☐
	WAVLINK_Touch_EXT5G		☐
	WAVLINK_Touch		☐
	099-5-1		☐

RESCAN

NEXT

WAVLINK see the world

Home Wireless Network Clients AI Net More

Device Status

Network

Internet

LAN

Static IP

IPv6

IPTV/VLAN

Dynamic DNS

Mode Selection

SQM QoS

Wireless

Mesh

Net Guardian

Parental Control

AI NET

Mode Selection

☐ Select Wi-Fi

☒ Manual Input

Superior wireless network information

Superior Network Name

Frequency Band

Channel

Encryption Method

NEXT

Help

Router Mode

Convert the wired network of the network provider into a Wi-Fi signal to realize the functions of wireless Internet access and wired Internet access.

LAN Bridge (AP Mode)

When extending an existing network in Access Point (AP) mode, it is important to ensure that the WAN port of this device is connected to the network via a cable. Please note that some functions may not be available in this mode, so it is advisable to refer to the on-screen display or user manual for detailed information.

Note:

If you need to set up the device after successfully connecting to the superior in this mode, you need to connect to the Wi-Fi of the device and access the web pages by <http://wavlogin.link/>.

- 4) Enter the password of the superior wireless network and the wireless network information of this device. Click **SAVE** to complete the setup.

Mode Selection

Superior wireless network information

Superior Network Name

WAVLINK-Mesh_C5D7

Password

.....



Wireless network information of this device

Connection Type

Bridge(Recommend)



2.4G Wi-Fi Name

WAVLINK-Mesh_C5D7_EXT2

Encryption Method

OPEN



5G Wi-Fi Name

WAVLINK-Mesh_C5D7_EXT5

Encryption Method

OPEN



SAVE

Chapter 3 Network Management

This chapter contains the following sections :

- [Network Setting](#)
- [LAN Setting](#)
- [Setting Static IP Binding](#)
- [Setting IPv6](#)
- [IPTV Setting](#)
- [Setting Dynamic DNS](#)
- [SQM QoS](#)

Network Setting

The way of network access can be changed as your requirement through configuring the network setting.

- 1 . Access **Network** setting or **More>Network>Network Setting**.
- 2 . Select your network connection way from the **WAN Type** list.

1) DHCP (Dynamic Host Configuration Protocol)

- It assigns network information including IP, Subnet Mask, default Gateway and others for the computer, designed for small network environments such as a home or a small office, managing and assigning IP without manual configuration.
- If the ISP (Internet Service Provider) has provided Auto Assign Feature for you, select DHCP from the WAN Type list.

Advanced

Custom MTU



MAC Clone



Custom DNS



Internet VLAN ID



SAVE

2) PPPoE (Point-to-Point Protocol over Ethernet)

- It functions as a secure connection constructor, including verifying user identity, assigning IP, and others. It is designed for broadband access methods such as ADSL, fiber optics and others to provide a secure network connection.
- If the ISP has provided a **Username** and **Password** for you, enter them after selecting PPPoE from **WAN Type** list.

Username

Password

3) Static IP

- It assigns fixed IP address for the computer automatically. It is designed for network connections, servers, remote access, etc., which require long-term stability to ensure the stability of network connections.
- If the ISP has provided a specified IP parameters including IP address, Subnet Mask, Gateway, DNS1 and DNS2, select Static IP from the list and enter the information provided by the ISP.

Network	WAN Type	Static IP ▼	? Help
	IP		
	Subnet Mask		
	Gateway		
	DNS1		
	DNS2 (Optional)		

4) USB Tethering

- It works to share network connection after connecting the USB devices to the router.

Network	WAN Type	USB Tethering ▼	? Help
----------------	----------	-----------------	------------------------

5) PPPoE Dual Access

- Using dual PPPoE broadband lines, PPPoE Dual Access achieves balanced distribution via the technology of Load Balancing. Designed for improving the network bandwidth and stability, so it is for the occasion that requires large data transmission.
- Enter the account and password provided by the ISP in **Username** and **Password**. Then select **DHCP** or **Static IP** from **Second WAN** list, one note is that **IP** and **Subnet Mask** are required for **Static IP**.

Network	WAN Type	PPPoE Dual Access ▼	? Help
	Username		
	Password		
	Second WAN	DHCP ▼	

6) PPTP Dual Access

- PPTP Dual Access refers to the dual-network accessing method of using two PPTP VPNs. With it, users can configure two PPTP VPN to simultaneously access the Internet, enhancing the reliability of bandwidth and network.
- Enter **Username**, **Password**, **Server URL**, then select **DHCP** or **Static IP**, one note is that **IP** and **Subnet Mask** are required for selecting **Static IP**.

Network

WAN Type

PPTP Dual Access



Help

Username

Password

Server URL

Second WAN

DHCP



7) L2TP Dual Access

- L2TP Dual Access uses two L2TP VPN connections to access the Internet. it allows users to use two VPNs to access the Internet, enhancing the reliability of bandwidth and network.
- Enter **Username**, **Password** and **Server URL**, then select **DHCP** or **Static IP**, one note is that **IP** and **Subnet Mask** are required for **Static IP**.

Network

WAN Type

L2TP Dual Access



Help

Username

Password

Server URL

Second WAN

DHCP



3 . In **Advanced**, open and configure **Custom MTU**, **MAC Clone**, **Internet VLAN ID** and others as your requirements.

Server Name (Optional)	
Access Concentrator Name (Optional)	
Host-Uniq Tag Content	Automatic Leave empty unless your ISP require this
Detect Online Interval (S)	1
Timed Connection	☒
Redial Interval (M)	0
Custom MTU	☒
MAC Clone	☒
Custom DNS	☒
Internet VLAN ID	☒

- **Server Name**

- The Server name, provided by ISP, indicates the name or address of PPPoE server.

- **AC(Access Concentrator) Name**

- The AC name, typically designated by the ISP, identifies the Access Concentrator and distinguishes different access points.

- **Host-Uniq**

- In PPPoE protocol, the Host-Uniq field is optional, used to uniquely identify requests from a host. In the same network, it ensures every request connected is unique while using PPP to connect to multi-users, avoiding confusion and conflicts.

- **Detect Online Interval**

- The detect online interval is used to set the time interval for sending LCP(cLink Control Protocol) Echo request, which is a message from LCP of PPP protocol, used to verify whether the line is still valid or capable of transferring data. The appropriate interval is helpful for timely detecting and addressing link issue.

- **Custom MTU(MaximumTransmission Unit)**

- The Ethernet MTU(MaximumTransmission Unit) is the largest size of a data packet that can be transmitted over the network. If your ISP requires you to adjust the MTU size, enable this option. Otherwise, we recommend you to keep it disabled for optimal network performance.
- **MAC Clone**
 - The MAC clone allows you to copy the MAC address from the computer to the WAN interface of the router. When an ISP restricts internet access to a single MAC address, by cloning the MAC address of the device, the router will appear as the original device, ensuring an uninterrupted internet connection.
- **Custom DNS**
 - The custom DNS allows you to configure optimal DNS server for the network manually, instead of using the default DNS provided by the ISP.
- **Internet VLAN ID**
 - The Internet VLAN ID is set to recognizing the feature of Internet data. For specific settings, please consult your network operator's customer service or technical support staff.

4 . Click **SAVE** to finish configuration.

LAN Setting

DHCP server automatically assigns IP for the devices in the LAN. If it is required, you can change its setting.

1 . Click **More>Network>LAN**.

2 . Click to enable **DHCP**.

LAN

DHCP



IP

192.168.20.1

Subnet Mask

255.255.255.0

Start IP

192.168.20.100

End IP

192.168.20.249

Lease Time

1 day



Custom DNS



DNS1

DNS2(Optional)

SAVE

- **IP Address:** The IP address from which the router connects to the LAN. This can be used to log in to the router's network management page.
- **Subnet Mask:** The subnet mask that the router connects to the LAN.
- **Set IP Address Pool:** When DHCP is enabled, the router automatically assigns IP addresses to devices in the LAN from the address pool. If you need to change the address pool range, modify the Start Address and End Address.
- **Lease Time:** This is the lease time of the IP address that the device obtains when accessing the router. If you need to modify it, please select it again in the Lease Time drop-down list.
- **Custom DNS:** The DNS in LAN Setting is configuration items that the router assigns to internal network devices via DHCP. It is used to designate the default domain name resolution servers for these devices.

3 . Click **SAVE** to finish the configuration.

Setting Static IP Binding

It allows you to link the specific IP to the MAC address of customer devices. Using it, you can assign a fixed IP for the specific device so that the device can automatically obtain the same IP every time it connects to the network.

Static IP

+ ADD

IP	MAC	Operation
192.168.20.187	5A:84:BD:8D:40:8B ▼	BIND CANCEL

- 1 . Click **More>Network>Static IP Binding**.
- 2 . Click **ADD** in the top right corner to add a binding rule.
- 3 . Input the **IP** and **MAC**, then click **BIND**.

Setting IPv6

The IPv6 is the next generation Internet protocol, has more space for address, more advanced functions and enhanced security. It aims to solve more issues on interconnected devices and provide better network performance and security.

IPv6 WAN Settings

Method Of Obtaining Static IPv6 ▼

IPv6 DHCPv6

IPv6 Gateway IPv4+IPv6 PPPoE

Static IPv6

- 1 . Click **More>Network>IPv6**.
- 2 . Click once to enable **IPv6**.
- 3 . **IPv6 WAN Settings**.

IPv6 WAN Settings

Method Of Obtaining IPv4+IPv6 PPPoE ▼

IPv6 WAN Settings

Method Of Obtaining	Static IPv6
IPv6	/
IPv6 Gateway	
Preferred DNS	
Alternative DNS	

- 3.1 Select corresponding **Method Of Obtaining** from the list, then input corresponding information:
 - DHCPv6**: The router automatically obtains the parameters such as IPv6 address. No manual requirements.
 - IPv4+IPv6 PPPoE**: When IPv4 Internet access is also PPPoE, you can select IPv4+IPv6 PPPoE. After enabled, IPv6 will use the IPv4 account and password to dial the number, and you do not need to manually enter the IPv6 account and password. Please note that this requires operator's support.
 - Static IPv6**: Manually input **IPv6(address)**, **IPv6 Gateway**, **Preferred DNS** and **Alternative DNS**.

4 . IPv6 LAN Settings.

IPv6 LAN Settings

IPv6 Address Assignment	Automatic Allocation
IPv6 Prefix	Automatic Allocation
IPv6	SLAAC
	fd00:7c28:acc8::/48

- Selecting appropriate address assignment method from the **IPv6 Address Assignment** list:
 - Automatic Allocation**: It will automatically assign IPv6 addresses to devices on the LAN network.
 - SLAAC**: In the SLAAC, The terminals on the LAN will automatically create IPv6 addresses according to the router.
- 5 . Click **SAVE** to finish the configuration.

IPTV Setting

Setting IPTV allows you to enjoy multimedia service while using the network. You should consult IPTV's service provider about **VLAN ID** and how to select **IPTV Mode**. Then you can select the corresponding VLAN Port, and connect IPTV's cable to the corresponding LAN port on the router.

Configuring IPTV

IPTV/VLAN

IPTV

IPTV Mode

Router Mode

IGMP Proxy

On

SAVE

- 1 . Enter **More>Network>IPTV/VLAN**.
- 2 . Click once to enable **IPTV**.
- 3 . Select appropriate working mode from the **IPTV Mode** list.

3.1 Router Mode

IPTV/VLAN

IPTV

IPTV Mode

Router Mode

IGMP Proxy

On

SAVE

Enable **IGMP Proxy** if you use IPTV service on multiple devices at the same time.

3.2 VLAN Bridge Mode: Enter **VLAN ID** and select **VLAN Port**.

IPTV/VLAN

IPTV

IPTV Mode

VLAN Bridge Mode

VLAN1 ID

0

VLAN1 LAN Port

LAN4

VLAN2 ID

0

VLAN2 LAN Port

LAN4

SAVE

4 . Click **SAVE** to finish the configuration.

- **VLAN1 ID and VLAN1 LAN Port:** The VLAN1 ID indicates the VLAN1, and the VLAN1 LAN Port indicates the LAN port associated with VLAN1.
- **VLAN2 ID and VLAN2 LAN Port:** The VLAN2 ID indicates the VLAN2, and the VLAN2 LAN Port indicates the LAN port associated with VLAN2.

Setting Dynamic DNS

Dynamic DNS(DDNS, Dynamic Domain Name System) is a function of mapping dynamic IP addresses to fixed domain names. After enabling it, the router bind dynamic WAN IP with the fixed domain so that you can connect to the router using the domain remotely. In order to use this service, you need to register for the DDNS service with your service provider.

Dynamic DNS

Dynamic DNS



Connection Status

Disconnected

Service Provider

oray.com



Username

user_ddns

Password



Host Name

www.domain.com

SAVE

- 1 . Enter **More>Network>Dynamic DNS**.
- 2 . Click once to enable **Dynamic DNS**.
- 3 . Select **oray.com** or **NO-IP** from the **Service Provider** list.
- 4 . Input corresponding **Username**, **Password** and **Host Name** from your DNS registration information.
- 5 . Click **SAVE** to finish configuration.

Note: Different dynamic DNS service provider may provide various parameters, and the name or indication may vary. Therefore, you should look up the corresponding explanation so that the correct parameters are input.

SQM QoS

SQM QoS uses smart queue management to classify, schedule, and prioritize network traffic, effectively controlling network congestion, ensuring bandwidth for critical applications, reducing latency, suppressing jitter, and minimizing packet loss, thereby enhancing network service quality.

SQM QoS

SQM QoS



Upload Bandwidth (Mbps)

1000

Download Bandwidth (Mbps)

1000

You Can Click On The Website On The Right
For Speed Measurement To Obtain
Bandwidth.

<https://www.speedtest.net>

(This Website Is A Third-Party Website, Please Pay Attention To Protecting
Personal Privacy)

SAVE

1. Navigate to **More > Network > SQM QoS**.
2. Click to enable **SQM QoS**.
3. Set the maximum **Upload Bandwidth** and the maximum **Download Bandwidth**.
4. Click **SAVE** to complete the configuration.

Chapter 4 Managing Wireless Network

This chapter contains the following sections:

- [Wireless](#)
- [Guest Wi-Fi](#)
- [Parental Wi-Fi](#)

Wireless

Configure the SSID, encryption method, password, and other wireless parameters for both the 2.4G and 5G networks.

1. Navigate to **Wireless** or go to **More > Wireless > Wireless**.

Enable it to make 2.4G and 5G Wi-Fi dual bands in one SSID. The router will automatically select the faster Wi-Fi band for you. If you disable it, you can set up the dual bands separately.



[? Help](#)

Wi-Fi

SSID

WAVLINK-Mesh_ACC8

Encryption Method

WPA2-PSK (Recommended)

Password



Advanced

2.4G Wi-Fi Settings

Channel

Automatic

Bandwidth

20/40MHz

Hide SSID



TWT



MU-OFDMA



5G Wi-Fi Settings

Channel

Automatic

Bandwidth

20/80/160MHz

Hide SSID



DFS



TWT



MU-OFDMA



SAVE

Configuring Wireless Network

1) Dual Frequency Selection

Enabling Dual Frequency Selection combines the 2.4GHz and 5GHz Wi-Fi bands into a single network to provide a better overall network experience. Disabling this feature allows for separate configuration of the 2.4G and 5G networks.

1. Navigate to **Wireless** or go to **More > Wireless > Wireless**.
2. Click to enable/disable **Dual Frequency Selection**.

2) Setting Wi-Fi SSID and Password

1. Navigate to **Wireless** or go to **More > Wireless > Wireless**.
2. Set a new wireless network name in the **SSID**.
3. In the **Encryption Method**, select an encryption method from the dropdown list. (It is recommended to choose **WPA3-SAE** or **WPA2-PSK**)
4. Set a new password for your wireless network in the **Password**.

Note: After setting up the new network, you will need to reconnect to the WiFi network using the new password.

Advanced Settings

1) Setting Channel and Bandwidth

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. From the **Channel** dropdown list, select the operating channel for your wireless network. (If you are unsure about which channel to choose, it is recommended to select **Automatic**, so the device can automatically select the optimal channel based on the surrounding environment for your better network experience.)
3. From the **Bandwidth** dropdown list, select the bandwidth for the router's wireless data transmission.

2) Setting Hide SSID

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **Hide SSID**. After enabling this, the wireless signal for the corresponding network will be hidden.

3) Setting DFS

After enabling this, the device will automatically avoid channels that are restricted in your region.

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **DFS**.

4) Setting TWT

After enabling this feature, the router will automatically optimize resource scheduling between devices, negotiate target wake time to reduce contention, increase device sleep time, and ultimately extend the lifespan of the router.

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **TWT**.

Note: This feature requires terminal devices that support Wi-Fi 6. If the terminal device is inactive for a long time, it may disconnect from the router.

5) Setting MU-OFDMA

After enabling this feature, the router will multiplex multiple users to improve transmission efficiency and reduce network latency in multi-user internet environments.

1. Navigate to **Wireless > Advanced** or go to **More > Wireless > Wireless > Advanced**.
2. Click to enable **MU-OFDMA**.

Schedule (Wireless Timer Switch)

The schedule function allows you to customize event rules to control the wireless network switch, with up to three rules definable. This feature only takes effect after obtaining the network time and only affects the main network. For the guest network, you need to manually enable or disable this feature or define separate rules within the guest network settings.

Schedule

2.4G Wi-Fi Settings

Rule 1



	Blocking Start Time		Blocking End Time				
Internet Blocking Period	00	:	00	~ 00 : 00			
Internet Blocking Day	Sun	Mon	Tues	Wed	Thu	Fri	Sat

Rule 2



Rule 3



5G Wi-Fi Settings

Rule 1



	Blocking Start Time		Blocking End Time				
Internet Blocking Period	00	:	00	~ 00 : 00			
Internet Blocking Day	Sun	Mon	Tues	Wed	Thu	Fri	Sat

Rule 2



Rule 3



1. Navigate to **Wireless > Schedule** or go to **More > Wireless > Wireless > Schedule**.
2. Click on **Rule 1/2/3** under either the **2.4G Wi-Fi Settings** or **5G Wi-Fi Settings** to set the timing rules.
3. Click **SAVE** to complete the settings.

Note:

- The schedule is based on the router's time. You can modify the time by going to **More > System > Time Zone**.
- The wireless network will automatically turn on after the set time period.

Guest Wi-Fi

This feature allows you to provide Wi-Fi to guests without exposing your main network. When you have visitors at your home, apartment, or workplace, you can create a guest Wi-Fi for them. Additionally, you can customize guest Wi-Fi settings to ensure security and privacy.

Guest Wi-Fi

Guest Wi-Fi

SSID

WAVLINK_Guest

Guest Wi-Fi Mode

No Encryption Mode

Device Isolation

On

Schedule

Rule 1

Rule 2

Rule 3

SAVE

1. Navigate to **More > Wireless > Guest Wi-Fi**.
2. Click to enable **Guest Wi-Fi**.
3. Set the **SSID**.
4. In the **Guest Wi-Fi Mode**, set the encryption method: Encryption Mode, No Encryption Mode, and WPA/WPA2. If you select WPA/WPA2, you will need to set the RADIUS server IP, RADIUS port, and RADIUS password.
5. Set the **Device Isolation**. Once on, this feature will isolate devices connected to the same LAN from each other, enhancing network security and privacy protection.
6. Set the guest Wi-Fi open time in the **Schedule**.
7. Click **SAVE** to complete the settings.

Parental Wi-Fi

Parental Wi-Fi allows you to set up a separate wireless network for family members. You can configure its SSID, encryption method, and rules.

Parental Wi-Fi

Enable



SSID

Parental-Wi-Fi

Encryption Method

WPA3-SAE/WPA2-PSK



 Please make sure that the access terminal supports WPA3-SAE/WPA2-PSK mode, and it is recommended to switch to WPA2-PSK mode if you encounter connection problems with the device.

Password



Schedule

Rule 1



	Blocking Start Time		Blocking End Time				
Internet Blocking Period	00	:	00	~ 17 : 00			
Internet Blocking Day	Sun	Mon	Tues	Wed	Thu	Fri	Sat

Rule 2



Rule 3



1. Navigate to **More > Wireless > Parental Wi-Fi**.
2. Click to enable **Parental Control**.
3. Set the **SSID, Encryption Method, and Password**.
4. Set the Internet Blocking Period and Internet Blocking Day in **Rule 1/2/3** to control your child's internet access time.
5. Click **SAVE** to complete the settings.

Chapter 5 Mesh

This chapter contains the following section:

- [Mesh Configuration](#)

Mesh Configuration

If a single router cannot provide adequate wireless coverage for large homes, you can purchase multiple WAVLINK routers that support Mesh networking to achieve full Wi-Fi coverage throughout your home.

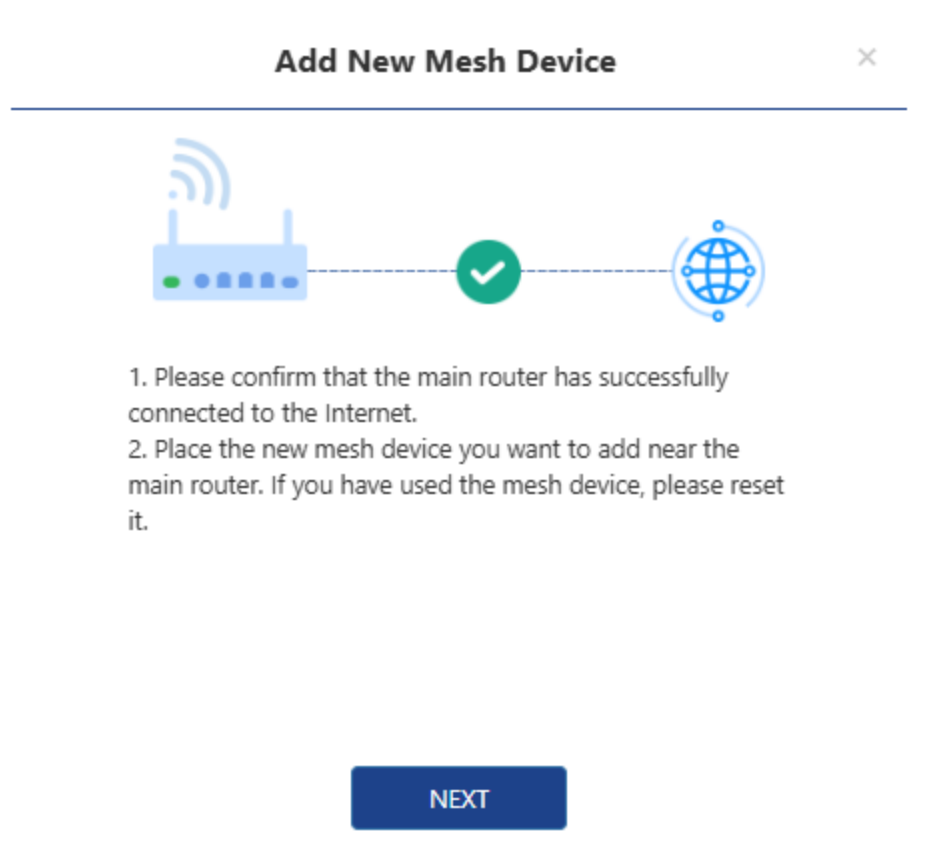
Adding New Mesh Device

Before setting up the Mesh network, ensure that:

The main router is connected to the internet and the setup wizard is completed, with the indicator light showing solid blue.

1. Navigate to **More > Mesh > Mesh Devices**.
2. Click on **+Add**. Follow the on-screen instructions to prepare your mesh device, then click **NEXT**.





3. Follow the on-screen instructions to power on the mesh device and press the pair button when the mesh device starts operating. Click **"SCAN"**. The main router will automatically scan the mesh device that is attempting to pair.



4. Once the scan is completed, select the mesh device you want to add.

Advanced Settings

Advanced ▾

Roaming ☒

Roaming Threshold dBm

Topology Optimization

Threshold Of Topology Optimization dBm

1) Roaming (Wireless Roaming Technology)

Enabling Roaming allows devices to seamlessly switch between two Mesh routers. As you move away from one router and get closer to another, the device will automatically disconnect from the current router and connect to the nearer one to provide a smoother network experience.

1. Navigate to **More > Mesh > Mesh Devices > Advanced**.
2. Click to enable **Roaming**.
3. Set the **Roaming Threshold** to an appropriate parameter.

Note: The wireless roaming trigger threshold should only be set by experienced professionals. If you lack professional experience in setting this, it is recommended to keep the default settings to avoid negatively impacting the network user experience.

2) Topology Optimization

When you have three or more paired devices and all devices have completed pairing, you can enable the topology optimization feature. This function can automatically adjust the optimal path based on the signal strength between devices to ensure that all sub-routers and corresponding upper-level devices have the best signal connection status, achieving optimal network coverage.

1. Navigate to **More > Mesh > Mesh Devices > Advanced**.
2. Click the **OPTIMIZATION** button after **Topology Optimization**.
3. Ensure the **Threshold Of Topology Optimization** is set to an appropriate parameter.

Note: You can adjust the signal threshold that triggers topology optimization to achieve the best mesh network coverage. If you do not have professional setup experience, it is recommended to use the default settings.

Topology Map

In this interface, you can see the network topology map, which shows the device access relationships and network connection status. It will also display the MAC address of each connected device, making it easier to see which terminals the devices are connected to.

1. Navigate to **More > Mesh > Topology Map**.

Topology Map



Chapter 6 Net Guardian

Secure DNS

This feature encrypts your DNS traffic to enhance security and privacy, preventing DNS leaks and DNS hijacking.

1. Navigate to **More > Net Guardian > Secure DNS**
2. Click to enable **Secure DNS**.
3. Set the **DNS Protocol** and **Server Provider**.
4. Click **SAVE** to complete the configuration.

Secure DNS

Secure DNS



DNS Protocol

DNS over HTTPS



Server Provider

AdGuard



SAVE

Chapter 7 NAT Forwarding

This chapter contains the following sections:

- [UPnP Settings](#)
- [Port Forwarding](#)
- [DMZ](#)
- [Hardware NAT](#)

UPnP Settings

UPnP (Universal Plug and Play) is a network protocol designed to make connecting devices simpler and more automated. Using the UPnP protocol, devices can automatically discover each other on the network and establish communication connections without requiring manual configuration or setup.

UPnP allows devices to share resources such as files, printers, and other multimedia content. The UPnP protocol is widely used in home networks and office environments to facilitate communication and interaction between devices.

1. Access **More>NAT Forwarding>UPnP**.
2. Set **ON/OFF UPnP**.
3. Click **SAVE** to finish configuration.

UPnP

UPnP

Connection List ▼

Number of connections: 0

REFRESH

Application Description	Protocol	External Port	Internal Port	IP
No Data				

SAVE

The computer operation system and application program you used need to support the UPnP function.

Port Forwarding

Port forwarding is a network technology. It maps a specific port on a public network to a specified server on the local network, allowing Internet users to access the local network server’s service by accessing the port.

Port Forwarding

⊕ ADD

Server IP	External Port	Internal Port	Protocol	Operation
			TCP ▾	BIND CANCEL

1. Access **More>NAT Forwarding>Port Forwarding**.
2. Click **Add**.
3. Enter the parameters of **Server IP**, **External Port**, and **Internal Port**.
4. Select **Communication Protocol**.
5. Click **Bind** to finish the configuration.

DMZ

Enable DMZ (Demilitarized Zone) management function, only enter one IP address that connects this device, then this device can be DMZ host. So this device can be accessed via external network and open all ports to improve fluency of corresponding communication. Please note security software and firewall on this host need to be closed temporarily when you use this function. So please consider using this function carefully.

DMZ

DMZ Host



DMZ Host IP

192.168.20.215

SAVE

NOTE

DMZ is suitable for use when you are not sure of the ports that need to be opened. Computers will be completely exposed to the WAN after opening DMZ Host, which may bring security risks to computers. So do not enable it unnecessarily. Disable it promptly if you do not need to use DMZ Host.

1. Set the computer to a Static IP such as 192.168.20.215.
2. Access **More>NAT Forwarding>DMZ**.
3. Open **DMZ Host**.
4. Enter the **IP address** of the corresponding computer (192.168.20.215).
5. Click **SAVE** to finish the configuration.

Hardware NAT

Data is forwarded by hardware instead of being processed by the CPU after enabling Hardware NAT, which can improve the device's performance. Disable Hardware NAT if you need to calculate throughput rate, usage statistics of CPU and RAM.

Hardware NAT

Hardware NAT



SAVE

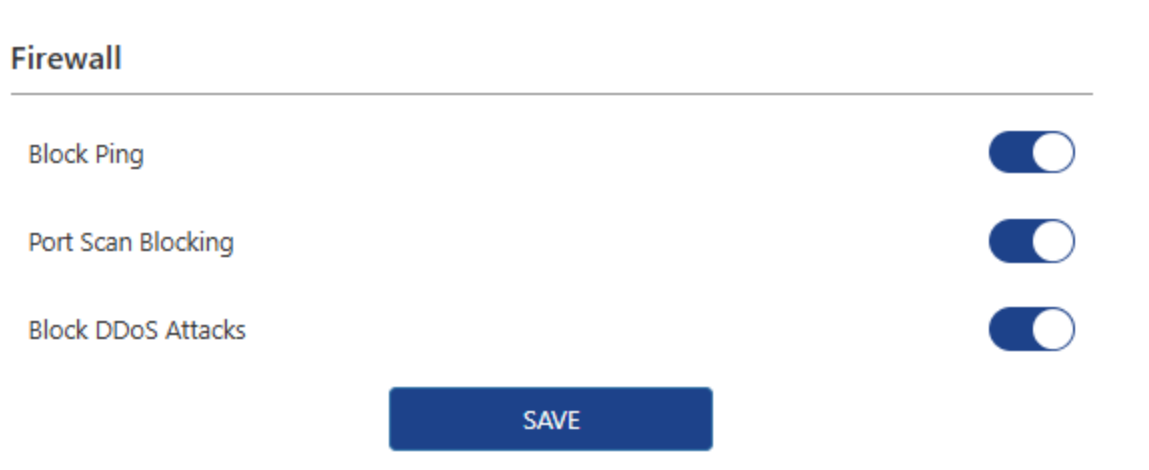
1. Access **More>NAT Forwarding>Hardware NAT**.
2. Open **Hardware NAT**.
3. Click **SAVE** to finish the configuration.

Chapter 8 Network Security

This chapter contains the following sections:

- [Firewall](#)
- [ALG Configuration](#)
- [MAC Filter](#)

Firewall



The screenshot shows a configuration interface for the Firewall. It has a title 'Firewall' at the top. Below the title, there are three settings, each with a label and a toggle switch:

- Block Ping**: The toggle switch is turned on (blue).
- Port Scan Blocking**: The toggle switch is turned on (blue).
- Block DDoS Attacks**: The toggle switch is turned on (blue).

At the bottom of the configuration area, there is a blue button labeled **SAVE**.

- 1 . Access **More>Security>Firewall**.
- 2 . Open **Block Ping**: It can prevent ping attacks and scanning and reduce the risk of network attacks on this device.
- 3 . Open **Port Scan Blocking**: It can protect server ports on devices from attacks.
- 4 . Open **Block DDoS Attacks**: It enables the router to avoid the massive resource consumption caused by DDoS attacks and ensures normal services.
- 5 . Click **SAVE** to finish the configuration.

ALG Configuration

ALG (Application Layer Gateway) allows a custom NAT traversal filter to be inserted into the gateway to support the address and port translation of certain application layer “control/data” protocols. Keeping default settings is recommended. When you use voice and video applications to create or receive calls through the router, you may need to disable SIP ALG because some voice and video applications do not work well with SIP ALG.

ALG

PPTP Passthrough	☒
L2TP Passthrough	☒
IPSec Passthrough	☒
FTP ALG	☐
TFTP ALG	☐
RTSP ALG	☐
H323 ALG	☐
SIP ALG	☐

SAVE

- 1 . Access **More>Security>ALG**.
- 2 . After configuration, please click **SAVE** to finish.

MAC Filter

- 1 . Access **More>Security>MAC Filter**.

MAC Filter

MAC Filter



Guest Network Exception



 ADD

Device Name	MAC	Operation
No Data		

MAC Filter: Enable MAC Filter and all devices added to the MAC Filter list will be blocked from accessing the Internet.

Guest Network Exception: Devices under guest Wi-Fi are not subject to MAC filtering rules.

Add Device

Select from List

☐

Device Name

MAC

☐DESKTOP-336LP6V6C:3C:8C:16:95:1E

CANCEL

APPLY

Add Device

×

Manual Input

▼

Device Name

MAC

: : : : :

CANCEL

APPLY

2 . Click **ADD**, Find the devices that need to be added or manually input them. Click **APPLY** to finish configuration.

VPN-Server-Client

title: Chapter 9 VPN Server and Client **hide_table_of_contents: false**

This chapter contains the following sections:

- [VPN Server Configuration](#)
- [VPN Client](#)

VPN Server and Client

VPN (Virtual Private Network) can encrypt your network connection to ensure the safe transfer of important data and avoid information stealing. Remote users (VPN clients) can safely connect VPN server.

VPN Server Configuration

Open VPN Server Configuration

OpenVPN Server is used for remote devices to establish an OpenVPN connection to access your home network. If you use VPN function, you need to enable the OpenVPN server on a router and then install and run VPN client apps on remote devices.

OpenVPN Server

• OpenVPN Server

Close

Configuration

User

Device IP

192.168.15.82

The current WAN IP is a private network address (10.x.x.x, 172.16.x.x, or 192.168.x.x).

Interface Type

tun

OpenVPN Protocol

tcp

IP

10.8.0.0

Subnet Mask

255.255.255.0

OpenVPN Port

1194

Encryption Method

AES-128-GCM

Identity Verification

SHA256

Login With Username And Password



Allow LAN Access



Restore default settings

Apply configuration

Generate backup file

Export Log File

- 1 . Access **More>VPN>OpenVPN Server**.
- 2 . Open **OpenVPN Server**.
- 3 . Select **Interface Type**.
- 4 . Select **OpenVPN Protocol**.
- 5 . In **IP** and **Subnet Mask**, enter the range of IP addresses the OpenVPN server can lease to devices.

- 6 . Enter **OpenVPN Port**. 1024~65535 is recommended.
- 7 . Select **Encryption Method** and **Identity Verification**.
- 8 . Open **Login With Username And Password** to customize username and password.
If turned off, you can connect without a username and password.
- 9 . Set whether to enable **Allow LAN Access**.

OpenVPN Server

• OpenVPN Server

Close

Configuration

User

Connection List

Virtual Address	Physical Address	Receive Bytes	Send Bytes	Connection Time
-----------------	------------------	---------------	------------	-----------------

- 10 . Click **SAVE**.
- 11 . Click **Generate backup file** to save it. VPN client device will establish VPN connection by using the file.

Use WireGuard VPN Server

WireGuard is a concise, efficient, and secure VPN protocol with advanced encryption algorithms, low latency, high throughput, simple and easy-to-use configuration, and cross-platform support.

WireGuard Server

• WireGuard Server

Close

Configuration

User

IP

10.0.0.1

Local Port

51820

Restore default settings

Apply configuration

- 1 . Access **More>VPN>WireGuard Server**.
- 2 . Open **WireGuard Server**.
- 3 . Enter **IP** and **Local Port**.
- 4 . Click **User** and Click **Add**. Set **Username** and click **APPLY**.

WireGuard Server

• WireGuard Server

Close

Configuration User

Each Client Device Connecting To The WireGuard Server Requires A Different Node Configuration. You Need To Create A Configuration For Each Device, And Each Configuration Must Use A Different Client IP.

Add

User List

Username	IP	Configuration File	QR Code	Operation
				APPLY CANCEL

Connection List

Username	IP	Receive Bytes	Send Bytes	Last Connection
----------	----	---------------	------------	-----------------

- 5 . Click **SAVE** or scan **QR CODE** to export the configuration file. VPN client device will establish VPN connection by using the file.

WireGuard Server

• WireGuard Server

Close

Configuration

User

Each Client Device Connecting To The WireGuard Server Requires A Different Node Configuration. You Need To Create A Configuration For Each Device, And Each Configuration Must Use A Different Client IP.

Add

User List

Username	IP	Configuration File	QR Code	Operation
Wavlink	10.0.0.2/32	 SAVE	 QR CODE	 DELETE

Connection List

Username	IP	Receive Bytes	Send Bytes	Last Connection
No Data				

WireGuard Server

- WireGuard Server

Close

Configuration User

Each Client Device Connecting To The WireGuard Server Requires A Different Node Configuration. You Need To Create A Configuration For Each Device. Each Configuration Must Use A Different Client IP.

User List

Username	IP	Configuration
Wavlink	10.0.0.2/32	Add

Connection List

Username	IP	Receive Bytes	Send Bytes	Last Connection
No Connections				



6 . If the client connects successfully. You can view this client in the **connection list**.

Connection List

Username	IP	Receive Bytes	Send Bytes	Last Connection
Test	10.0.0.2/32	188.62KiB	200.36KiB	1m 34s ago

VPN Client Configuration

A VPN client establishes a VPN connection so that devices in your home network can access a remote VPN server.

PPTP/L2TP VPN Client Configuration

VPN converts public networks (Internet, etc.) into private networks using encryption technology to offer greater security and privacy protection.

VPN Client

Client On/Off



Internet Access Method

PPTP



Server

Server Address



Server Address

172.16.2.216

Username

Password

Connection Status

Disconnected

SAVE

1. Access **More>VPN>VPN Client**.
2. Open **VPN Client**.
3. Select **Internet Access Method**.
4. Select Server Address in **Server** or enter corresponding information in **Server Address**.
5. Enter **Username** and **Password**.
6. Click **SAVE** to finish the configuration.

OpenVPN Client Configuration

1. Access **More>VPN>OpenVPN Client**.

OpenVPN Client

+ Add Group

2. Click **Add Group**.

OpenVPN Client

● New group 2  

+ Add Group

Name

Server Address

Receive

Sent

Operation

+ Add Configuration

3. Click **Add Configuration**.

Please select the OpenVPN file



Click to upload files or drag and drop files here

Supported file types: .ovpn, .conf, .txt, .zip, .tgz, .tar.gz, .tar, .tar.bz2, .tar.xz, .rar, .7z

File Count:0

Cancel

Submit

4. Upload the configuration files and then submit them.

OpenVPN Client

● New group 2  

+ Add Group

Name

Server Address

Receive

Sent

Operation

● master (1)

192.168.15.82 1194

--

--

● master

192.168.15.40 1194

--

--

+ Add Configuration

5. Open the server configuration you want to connect to and you can use the VPN tunnel, if your VPN supplier requires Login With Username and Password, you need to enter VPN Username and Password.

WireGuard VPN Client Configuration

WireGuard Client

 Mullvad VPN

0

 Azire VPN

0

+ Add Group

 **Mullvad VPN**

Account

Enter your 16-digit account number

Login

Sign Up

Forgot Password?

1. Access **More>VPN>WireGuard VPN Client**.
2. Click **Add Group**. If you have a Mullvad or Azire VPN account, you can use it.
3. Click **Add Configuration**.

WireGuard Client

 Mullvad VPN

0

 Azire VPN

0

New group

+ Add Group

Name	Server Address	Receive	Sent	QR Code	Operation
▼ Add Configuration  Upload Configuration File  Manual Configuration					

4. Upload the configuration files and then submit them.

Please select the WireGuard file



Click to upload files or drag and drop files here

Supported file types: .conf, .txt, .zip, .tgz, .tar.gz, .tar, .tar.bz2, .tar.xz, .rar, .7z

File Name:

File Count:

Cancel

Submit

5. Click **Manual Configuration** to manually enter the parameters of WireGuard VPN.

Manual Configuration

Name

Text Mode

Configuration Item Mode

Cancel

Submit

Manual Configuration

Name

Text Mode

Configuration Item Mode

Interface

Address

+

Private Key

MTU(Optional)

Listening Port(Optional)

DNS(Optional)

+

Peer

Endpoint IP

Endpoint Port

Allow IP

+

Public Key

Preshared Key(Optional)

Persistent Keepalive(Optional)

Cancel

Submit

6. Open the server configuration you want to connect to, and you can use the VPN tunnel.

WireGuard Client

•  Mullvad VPN 0

•  Azire VPN 0

• New group 1  

+ Add Group

Name	Server Address	Receive	Sent	QR Code	Operation
• xxxx	192.168.15.40	-	-		☐  

▼ Add Configuration

ZeroTier Configuration

1. Access **More>VPN>ZeroTier**.

ZeroTier

• Zerotier

Close

 Make sure your ZeroTier virtual network is fully configured. If you're using the new ZeroTier Central, note that the "Manage Route" feature may be limited to paid users (server-side restriction, not controllable by this client). When restricted, LAN device access may be affected.

Local Network ID

203624b458

Allow LAN Access



Join New Network

+ Add

Network ID	Network Name	Assigned IP Addresses	Status	Operation
------------	--------------	-----------------------	--------	-----------

No Data

Restore default settings

Apply configuration

2. Open **ZeroTier**. Click **+Add** to join new network.

Join ZeroTier Network

Enter The 16-Character Hexadecimal Network ID To Join:

+

Cancel

Add

3. Successful connection status is as follows:

ZeroTier

• Zerotier

Close

Make sure your ZeroTier virtual network is fully configured. If you're using the new ZeroTier Central, note that the "Manage Route" feature may be limited to paid users (server-side restriction, not controllable by this client). When restricted, LAN device access may be affected.

Local Network ID

203624b458

Allow LAN Access

Join New Network

+ Add

One-click Disconnect

Network ID	Network Name	Assigned IP Addresses	Status	Operation
632ea29085c5a598	zerotier测试	192.168.196.134/24	Connected	View Disconnect

Restore default settings

Apply configuration

4. **Allow LAN Access:** After open it, the device joining ZeroTier can access the LAN devices behind router. The router needs to be configured in the **ZeroTier Center** for the two parties to be able to communicate with each other.

5. Click **View** to check and revise configuration.

View ZeroTier Info

Network ID

632ea29085c5a598

Configuration

☒ **Allow Managed Addresses**

☐ **Allow Assignment of Global IPs**

☐ **Allow Default Route Override**

☐ **Allow DNS Configuration**

Ethernet

9a:85:f3:a1:24:fa

Type

PRIVATE

IP

192.168.196.134/24

Route Info:

Target	Via
192.168.196.0/24	--

Cancel

Application

i NOTE

Allow Managed Addresses: Default Yes. Allow ZeroTier to set IP Addresses and Routes (local/private ranges only).

Allow Assignment of Global IPs: Default No. Allow ZeroTier to set Global/Public/Not-Private range IPs and Routes.

Allow Default Route Override: Default No. Allow ZeroTier to set the Default Route on the system. See Full Tunnel Mode.

Allow DNS Configuration: Default No. Allow ZeroTier to set DNS servers.

Chapter 10 Remote Access

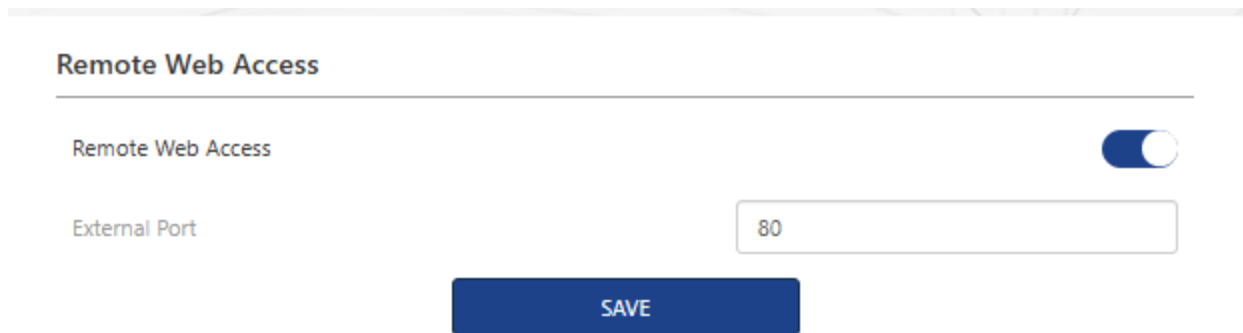
This chapter introduces remote web access and cloud APP.

It contains the following sections:

- [Remote Web Access](#)
- [Cloud APP](#)

Remote Web Access

With this function, you can manage this router remotely via the Internet. Input "http://WAN IP: port number" for remotely accessing this device. We recommend you write this router's WAN port number down before using this function.



Remote Web Access

Remote Web Access ☒

External Port

SAVE

1. Access to **More>Remote Access>Remote Web Access**.
2. Turn on **Remote Web Access**.
3. Set **External Port**.
4. Click on **SAVE** to complete settings.

Cloud APP

With this function, you can control this router remotely from the cloud with the APP.

Cloud App

Cloud App



Connection Status

Connected

SAVE

Don't have the app? [Click to download](#)

1. Access to **More>Remote Access>Cloud APP**.
2. Click on **Cloud APP** to enable the function.
3. Click on "**SAVE**" to complete settings.

NOTE:

If you didn't download APP, please click on **Click to download** to scan the pop-up QR code for downloading. You can also scan the QR code directly to obtain APP.

Scan the QR code using your phone to download the app. 



Chapter 11 NET Tools

This chapter introduces how to check network status, test network connection, and enable Wake-on-LAN function.

It contains the following sections:

- [Network Check](#)
- [Diagnostics](#)
- [Wake-On-LAN](#)

Network Check

You can scan the entire network to analyze and optimize network status via network check.

Network Check



If your device is unable to connect to the Internet or the network is unstable, you are recommended to test

START DETECTION

WAN	Check WAN port status, IP acquisition, and port rate limit	Not detected
Internet	Detect the connectivity status between devices, gateway, and network	Not detected
Wi-Fi	Detect Wi-Fi signal interference	Not detected
Memory	Check memory and CPU usage	Not detected

1. Access to **More>NET Tools>Network Check**.
2. Click on **START DETECTION**.

Network Check



Detection completed. The results are as follows:

ONE-CLICK REPAIR

WAN	Check WAN port status, IP acquisition, and port rate limit	
WAN cable status		✓
WAN IP Status		✓
WAN Port Network Link limit	Link rate: 100M Full duplex	
Internet	Detect the connectivity status between devices, gateway, and network	
Ping Gateway Status		✓
Network		✓
Wi-Fi	Detect Wi-Fi signal interference	
2.4G Wi-Fi Signal Status		✓
5G Wi-Fi Signal Status	Wi-Fi signal interference is strong !	
Memory	Check memory and CPU usage	
CPU Usage		12%
Memory Usage		55%

3. Click on "**ONE-CLICK REPAIR**" or manually optimize your network with prompts.

Diagnostics

Diagnostics

Ping Or Route Tracking

Ping

IP Address Or Domain Name

www.biying.com

PING

```
PING www.biying.com (202.89.233.100): 56 data bytes
64 bytes from 202.89.233.100: seq=0 ttl=117 time=44.165 ms
64 bytes from 202.89.233.100: seq=1 ttl=117 time=43.364 ms
64 bytes from 202.89.233.100: seq=2 ttl=117 time=43.051 ms
64 bytes from 202.89.233.100: seq=3 ttl=117 time=42.965 ms
```

```
--- www.biying.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 42.965/43.386/44.165 ms
```

1. Access to **More>NET Tools>Diagnostics**.
2. In the dropdown list **Ping Or Route Tracking**, choose **Ping** or **Tracert**.
 - **Ping** : used to check whether the connection between the router and the target device is normal.
 - **Tracert** : used for checking the node information between the router and the target device.
3. Input the **IP Address Or Domain Name** that you want to test.
4. Click on **PING** or **TRACEROUTE** button for testing.

Wake-On-LAN

Wake-On-LAN (WOL) is a technology where the network interface card (NIC), along with other software and hardware, sends a specific data frame to the NIC that is in standby mode, enabling the computer to start up from a powered-off state.

1 . Access to **More>NET Tools>Wake-On-LAN**.

Wake on LAN

☐	Describe	MAC	Hour	Minute	Repeat
No Data					

ADD DELETE

2 . Click on **Add** to start Wake-On-LAN setting.

Wake-up Configuration

Describe: Test

MAC: C0 : 25 : A5 : 9F : B5 : 2F

Time setting: 12 Hour 00 Minute

Reboot Time: Su Mo Tu We Th Fr Sa

WAKE UP SAVE

3 . Add the **Describe** of the configuration.

4 . Input the **MAC Address** of the device that you want to remotely wake up.

5 . Set **Time setting** and **Reboot Time**.

6 . Click on **SAVE**, complete the configuration.

Chapter 12 System Setting

This chapter introduces firmware update, password change, system log, system time setting, indicator setting, backup and restore, and how to restart router.

It contains the following sections:

- [Firmware Upgrade](#)
- [Change Password](#)
- [System Log](#)
- [Time Zone](#)
- [Led Control](#)
- [Backup & Restore](#)
- [Scheduled Reboot](#)

Firmware Upgrade

Regular firmware upgrade can obtain the newest functions and security patches, improving the performance and stability of the router, and fixing possible bugs and security risks.

WAVLINK provides two ways to upgrade your firmware: local upgrade and online upgrade. You can choose one of them to update your firmware.

Access to **More>System>Firmware Upgrade**.

Local Upgrade

Manually upgrade the firmware. You can download a new firmware file from the official WAVLINK website. The following devices are the same model as the devices you currently connect to.

☐	Mesh Device	Current Version
☐	Router	M86X3B_V260410_2.0.0

New Firmware

Choose File

UPLOAD FILE

The following devices are different models from the devices you are currently connected to. You can upgrade them by clicking the Upgrade link to access the Manual Upgrade page.

Mesh Device	Current Version	Upgrade Link
No Devices		

Online Upgrade

If the device has Internet access, you can upgrade online. After checking the latest firmware version, click the "ONE-CLICK UPGRADE" button.

☐	Mesh Device	MAC	Current Version	Latest Version	Update Contents
☐	Router	8*:~*:~*:~*:C4:66	M86X3B_V260410_2.0.0	No new version available	--

CHECK FOR NEW VERSION

ONE-CLICK UPGRADE

Local Upgrade

1. Access to WAVLINK official website: www.wavlink.com. Download the corresponding upgraded software of the current hardware version.
2. Select the device that needs to be updated.
3. Click **Choose File** or **File** icon, and select the firmware file that needs to be uploaded. Click on **UPLOAD FILE**.
4. Wait for the completion of updating.

NOTE:

- After updating, the router will automatically reboot to apply new firmware. The process will take few minutes to complete, please wait patiently.
- During updating, the router can't be powered off in case the router's firmware gets damaged.

Online Upgrade:

1. Choose the device that needs to be updated.
2. Click on **CHECK FOR NEW VERSION** to view the upgradable version to update. Or directly use **ONE-CLICK UPGRADE**.
3. Wait for the update completion.

NOTE:

- After updating, the router will automatically reboot to apply new firmware. The process will take few minutes to complete, please wait patiently.
- During updating, the router cannot be powered off in case the firmware gets damaged.
- When CHECK FOR NEW VERSION, if the prompts show that the firmware is the latest version, there is no need to upgrade the router.

Change Password

Change Password

Old Password

New Password

The password should be at least 6 characters 

Confirm New Password

The password should be at least 6 characters 

SAVE

1. Access to **More>System>Change Password**.
2. Input the current one on the **Old Password** text field.
3. Input the new one on the **New Password** text field.
4. Input the new one on the **Confirm New Password** text field, ensuring the input password is the same as the new password.
5. Click on **SAVE** to complete password changing.

System Log

When it comes to malfunction, reserve the system log and send it to technical support for trouble shooting.

System log

System Log

Export log

Tue Nov 19 13:36:38 2024 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Tue Nov 19 13:36:57 2024 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 03 07:28:26 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:28:31 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 03 07:28:34 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:28:36 2025 [USER] login successful, ::ffff:192.168.20.215.
Fri Jan 03 07:29:35 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:29:36 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 3 07:29:42 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.
Fri Jan 03 07:29:47 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:29:52 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 03 07:29:57 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:30:09 2025 [LAN] [DHCPV4] 7a:3a:ee:28:37:08, 192.168.20.135, LAU.
Fri Jan 3 07:31:23 2025 [USER] login successful, ::ffff:192.168.20.215.
Fri Jan 03 07:31:57 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:32:02 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 3 07:32:02 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 03 07:32:09 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:32:14 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 03 07:32:19 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:32:24 2025 [USER] login successful, ::ffff:192.168.20.215.
Fri Jan 3 07:33:03 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.
Fri Jan 3 07:33:47 2025 [LAN] [DHCPV4] 7a:3a:ee:28:37:08, 192.168.20.135, LAU.
Fri Jan 3 07:34:06 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.
Fri Jan 3 07:35:34 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.
Fri Jan 3 07:37:28 2025 [LAN] [DHCPV4] 5a:84:bd:8d:40:8b, 192.168.20.187, *.
Fri Jan 03 07:38:26 2025 [WAN] [DHCPV4] ip: 172.16.2.111, gw: 172.16.2.1.
Fri Jan 3 07:38:31 2025 [LAN] [DHCPV4] c0:25:a5:9f:b5:2f, 192.168.20.215, DESKTOP-BJ3F5MU.
Fri Jan 3 07:38:31 2025 [LAN] [DHCPV4] 7a:3a:ee:28:37:08, 192.168.20.135, LAU.

- 1. Access to **More>System>System Log**.
- 2. Click on **Export log** to save the log to the computer.

Time Zone

The system time is the time displayed when the router is running. The system time you set here is used for other time-based features, like Parental Control.

Time Zone

Current Time

2025/01/03 08:43:37

Time Zone

(UTC-00:00) Dublin, Edinburgh, Lisbon, I ▼

Daylight Saving Time (DST)



SAVE

1. Access to **More>System>Time Zone**.
2. Choose the right time zone in the drop-down list of **Time Zone**.
3. Turn on/off **Daylight Saving Time(DST)**.
4. Click on **SAVE** to complete the configuration.

Led Control

The router's indicators are used for indicating the device's status or running. By setting the indicator, you can know the device's working status more clearly, find and ban machine problems in time.

Led Control

Led Status



SAVE

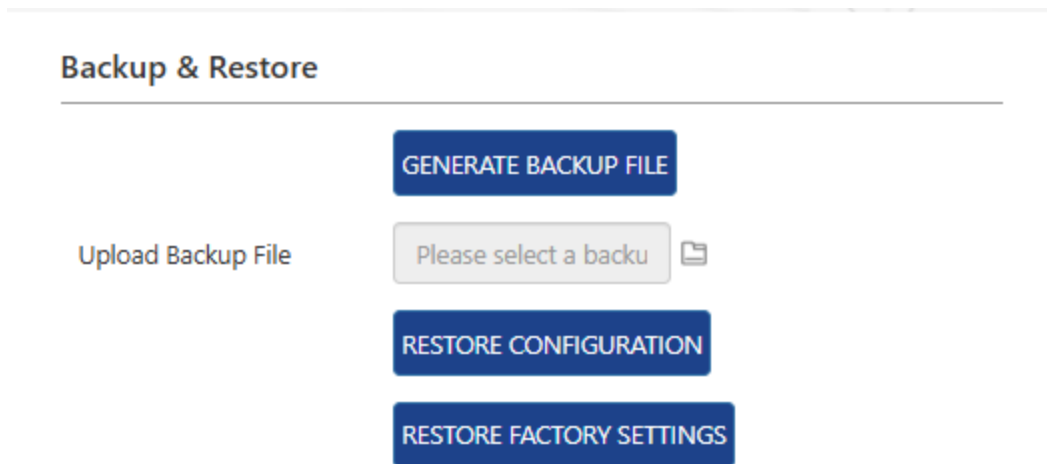
1. Access to **More>System>Led Control**.
2. Turn on/off **LED Status**.
3. Click on **SAVE** to complete the configuration.

Backup & Restore

Please configure settings as a configuration file stored in the router. You can backup this configuration file into your computer for future use, and restore the router to the

previous setting with this backup file. Furthermore, if necessary, you can delete the current system setting and reset the router to the default factory settings.

Access to **More>System>Backup & Restore**.



Backup the current configuration of the router

Click on **GENERATE BACKUP FILE** to store the copy of current setting on the local computer, and name the file **backup settings**.

Restore the router's configuration:

1. Click on **UPLOAD**, and choose the backup configuration file that was stored on the computer.
2. Click on **RESTORE CONFIGURATION**, and wait a few minutes to restore the configuration and restart the router.

Reset the router to the default factory settings

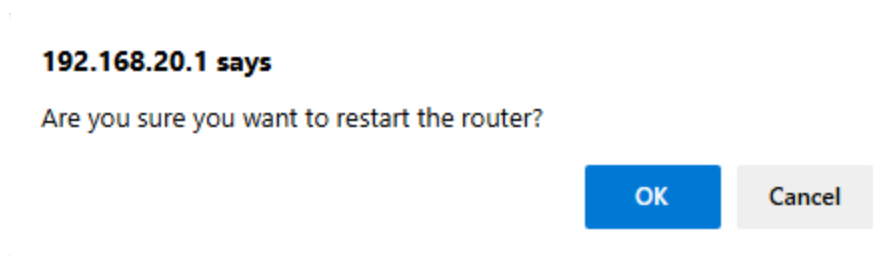
1. Click on **RESTORE FACTORY SETTINGS** to reset the router.
2. Wait a few minutes for the reset and reboot.

Scheduled Reboot

When your router has a network malfunction, you can try to use the reboot function to solve the problem. Sometimes, the router may experience software errors or memory overflow issues, leading to network instability. Under these circumstances, you can reboot the router to solve this problem and get the network back up.

After modifying some settings of this router, you need to reboot the router to make the settings valid. Using the reboot function can quickly update the router's settings and make it valid.

1. Access to **More>System>Scheduled Reboot**.
2. Click on **ROUTER REBOOT**.



3. After clicking, a window will pop up, in which you will be asked whether to restart the router or not. If you want to reboot the router, choose **OK**. If not, choose **Cancel**.

Set Scheduled Reboot Plan

The screenshot shows a configuration page for the 'Reboot Plan'. At the top, there is a toggle switch labeled 'Reboot Plan' which is currently turned on. Below this, the 'Current Time' is displayed as '2025/01/03 09:09:22'. The 'Reboot Time' is set using two dropdown menus showing '03' and '00'. The 'Reboot Date' is selected using a row of buttons for the days of the week: 'Sun', 'Mon', 'Tues', 'Wed', 'Thu', 'Fri', and 'Sat'. The 'Sun' button is highlighted in blue. At the bottom of the form is a large blue button labeled 'SAVE'.

The automatic reboot function can clear unnecessary data in the router and automatically choose the best wireless channel.

Before turning on Reboot Plan, please ensure the system time is right. If the router's designated reboot time is less than 60 minutes, some unnecessary reboots won't be executed.

1. Access to **More>System>Scheduled Reboot**.
2. Turn on **Reboot Plan**.
3. Choose the router's **Reboot Time**, and the **Reboot Date** to decide on reboot frequency.
4. Click on **SAVE** to complete the configuration.

Chapter 13 Logoff

Logoff

If you need to log out, please access to **More** on the management page, then click on **Logout**.

Chapter 14 FAQ

This chapter contains the following sections :

- [FAQ](#)
- [GNU General Public License Notice](#)
- [After-sale Service](#)

FAQ

Q1. Why doesn't the login page appear after entering <http://wavlogin.link>?

1. Make sure you connect the Wi-Fi signal of the WAVLINK device.
2. Make sure you enter the URL in the address bar, not the search bar.
3. Make sure you entered the current URL.
4. Try to use <http://192.168.20.1> to log in to the management page.
5. If you try to log in by phone, please turn off your mobile network and try to log in again.
6. If you try to log in by your PC/laptop, please disconnect other Internet connections.
7. Make sure the VPN should be disabled.

Q2. What should I do if I can't access the Internet after configuration?

1. Restart your modem (wait 5 minutes). Disconnect any extra Ethernet cable connections from the modem.
2. Test by connecting a computer directly to the modem via an Ethernet cable. If you still cannot get Internet, there might be some issues with the modem; please contact the ISP.
3. For cable modems, clone the MAC address of the device which could get Internet from the modem via an Ethernet cable in More >Network >Internet > MAC Clone>Custom MAC, then reboot modem and router.
4.
 - Check the router's web management page:
 - Verify if the Internet icon is blue on the home page.

- If it is blue, set DNS1 to 8.8.8.8 and DNS2 to 8.8.4.4 under More>Network >Internet>Custom DNS.
- If it is gray, check hardware or contact ISP.

Q3. How do I restore the device to factory default settings?

- Press and hold the reset button of the device for 6 seconds.

Q4. What can I do if I forget my login password?

- Try to ensure if you can log in with a Wi-Fi password; if not, restore the factory settings.

Q5. How can I find the best location for my device?

- Please put your device in a relatively open space to avoid obstacles such as metal objects, reinforced concrete walls and so on.

Q6. Why is the traffic data inaccurate?

- Hardware NAT is activated by default to lower CPU loading and improve network performance, which leads to the absence of traffic monitoring; therefore, traffic data is not accurate. If you need it to be accurate, please turn off Hardware NAT.

GNU General Public License Notice

This product includes software codes developed by the third parties. These software codes are subject to either the GNU General Public License (GPL), Version 2, June 1991 or the GNU Lesser General Public License(LGPL), Version 2.1, February 1999. You can copy, distribute, and/or modify in accordance with the terms and conditions of GPL or LGPL. The source code should be complete, if you want us to provide any additional source code files under GNU General Public License (GPL), please contact us in these matters. We are committed to meeting the requirements of the GNU General Public License (GPL). You are welcome to contact our local office to get the corresponding software and licenses. Please inform us your contact details (full address) and the product code. We will send you a software package with the software and license for free. The respective programs are distributed WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY Or FITNESS FOR A PARTICULAR PURPOSE.Please refer to the GNU General Public License Website for further information.

<http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>

<http://www.gnu.org/licenses/gpl.html>

After-sale Service

Need help?

We're here for you!



Online support: wavlink.com

Available Mon-Fri 8:30 am-5:30pm (UTC+8)



support@wavlink.com

Available Mon-Fri 8:30 am-5:30pm (UTC+8)



+1 8889730883

Mon-Fri 9:00 am - 6:00 pm (UTC-5)

www.wavlink.com



**Thank you for purchasing
WAVLINK product!**

Chapter 15

Safety and Emission Statement

CE Mark Warning

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

NOTE:

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

Declaration of Conformity Hereby, Winstars Technology Limited, declares that the radio equipment type AERIAL HD9S is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following Internet address:https://www.wavlink.com/en_us/ce.html

FCC Statement Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

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