

WLD92 Router

User Manual

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

This device is going to be operated in 5.15–5.25GHz frequency range, it is restricted in indoor environment only.

This device is restricted for indoor use.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

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

Table of Contents

1. UNPACKING INFORMATION	3
2. INTRODUCTION	4
2.1 SYSTEM LEDs & LED DEFINITIONS	4
2.2 BACK PANEL	5
3. INSTALLATION	6
4. CONNECT DEVICES TO THE ROUTER	8
5. WEB USER INTERFACE	11
5.1 ACCESSING THE WEB USER INTERFACE.....	11
5.2 WEB USER INTERFACE INTRODUCTION.....	12
6. HOME.....	13
7. WI-FI	14
7.1 WLAN SETTINGS.....	14
7.2 WLAN ADVANCED SETTINGS.....	15
7.3 WLAN MAC FILTER	17
7.4 WPS SETTINGS	18
7.5 CONNECTED DEVICES.....	19
8. SETTINGS.....	20
8.1 QUICK SETUP	20
8.2 DIAL-UP	23
8.3 ETHERNET	26
8.4 OPERATING MODE.....	30
8.5 DHCP	31
8.6 DNS	32
8.7 SECURITY	33
8.8 PARENTAL CONTROL.....	45
8.9 ROUTING	47
8.10 STATISTICS.....	48
8.11 DDNS	49
9. SYSTEM	50
9.1 DEVICE INFORMATION	50
9.2 MODIFY PASSWORD.....	51
9.3 DIAGNOSIS	52
9.4 RESTORE DEFAULTS.....	54
9.5 REBOOT	55
9.6 DATE AND TIME.....	56
10. UPDATE	57
10.1 LOCAL UPDATE.....	57
10.2 ONLINE UPDATE	58
11. SPECIFICATIONS.....	59

1. Unpacking Information

Thank you for purchasing this product. Before installation, please confirm you have all required items on hand:

- WLD92 Router × 1
- Power Adaptor: AC 90 V–264 V (47 Hz–63 Hz) input, DC 12 V output (1 A) × 1
- Ethernet Cable × 1
- Quick Start Guide × 1
- Warranty Card × 1

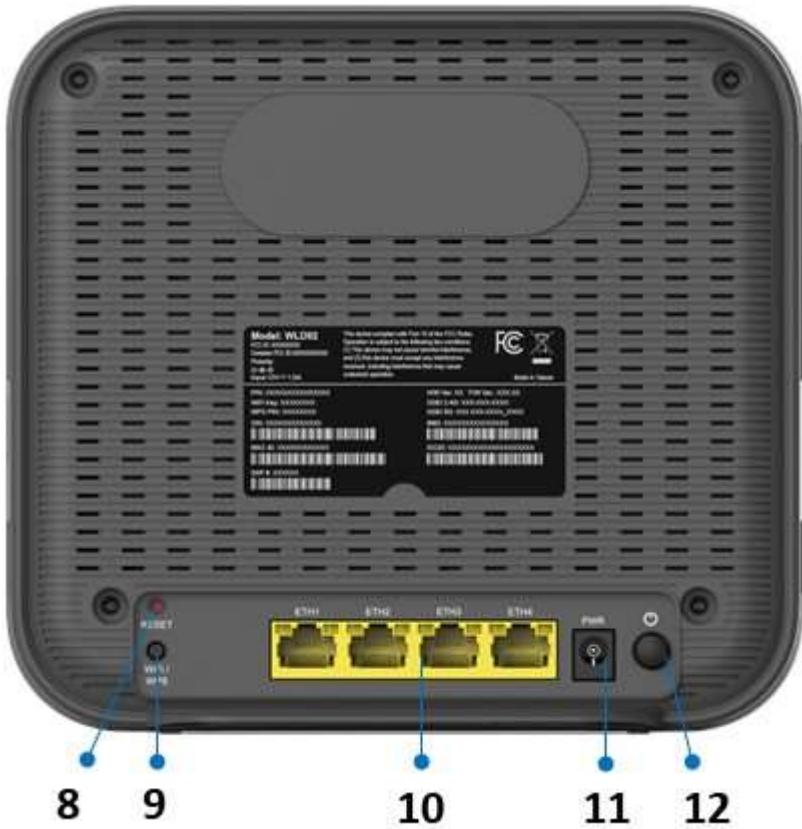
2. Introduction

2.1 System LEDs & LED Definitions



1. 4G Network	Steady cyan: Connected to 4G network Blinking red: No registered network
2. Signal Strength	Steady blue: Good coverage Steady green: Acceptable coverage Blinking red: Poor coverage
3. Ethernet	Steady blue: LAN connected Off: LAN disconnected
4. Wi-Fi 5G/WPS	Steady blue: Wi-Fi on Blinking blue: WPS setup in progress Off: Wi-Fi off
5. Wi-Fi 2.4G/WPS	Steady blue: Wi-Fi on Blinking blue: WPS setup in progress Off: Wi-Fi off
6. Internet	Steady blue: Connected to Internet Off: No Internet connection
7. Power	Activates when the device is powered on

2.2 Back Panel



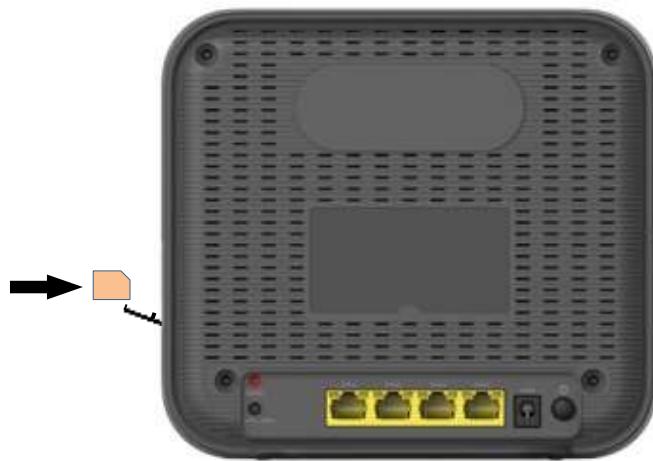
8. Reset button	Reset the Router by pressing this button.
9. Wi-Fi/WPS button	Connect to other WPS-compatible devices by pressing this button. Wi-Fi function is turned on/off by a long press (for 5 seconds). WPS association window is activated by a short press (less than 3 seconds).
10. Ethernet Ports 1–4	Connect to your devices such as a PC and laptop. Note: The Eth1 port also functions as a WAN port for connecting to a DSL or cable modem.
11. 12V DC jack	The power adapter connects to this jack.
12. ON/OFF switch	Press to turn the power on or off.

3. Installation

1. Open the SIM card cap.



2. Insert a Micro SIM card into the SIM card slot, and place the cap back over the SIM card slot.



3. Connect the Router to the power adapter and plug the power adapter into a wall outlet.

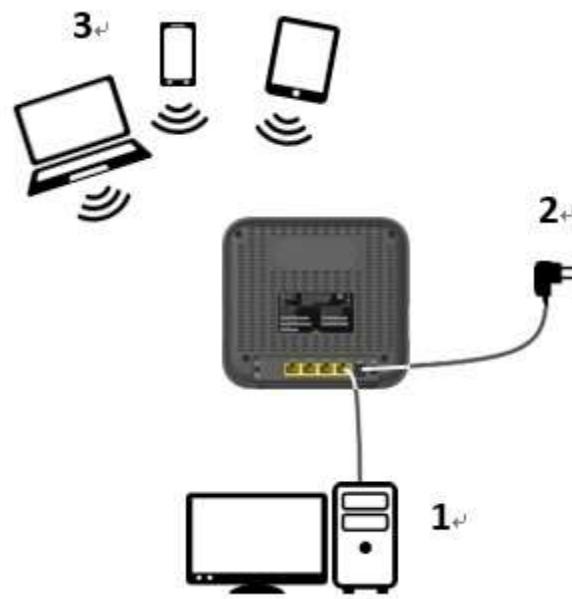
Note: Always use the adapter that comes with the Router for the power supply.

4. Turn on the power switch of the Router.



4. Connect devices to the Router

Scenario 1: Access the Internet through a 4G network



1. Computer

3. Notebook, tablet, or smartphone

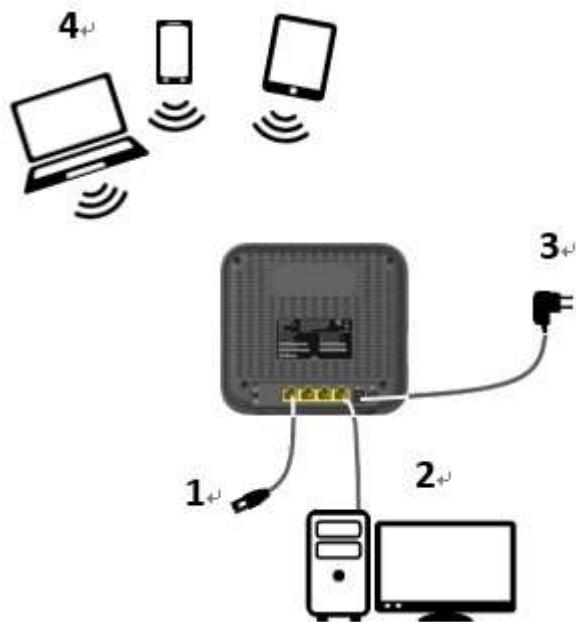
2. Power adapter

1

Note:

The DHCP server in the Router is turned on as a default setting. When connecting a computer to the Router, please ensure that the computer is set up to obtain an IP address automatically.

Scenario 2: Access the Internet via Ethernet



1. Ethernet cable (connect to Ethernet port in wall or other device)	2. Computer
3. Power adapter	4. Notebook, tablet, or smartphone

Scenario 3: Connect devices to the Router wirelessly

1. Enable the Wi-Fi function of devices such as your laptop, tablet PC, or smartphone.
2. If your device supports WPS, press the WPS button on the Router and then press the WPS button on your device to establish a connection. If not, skip this step and complete the steps below.
3. When the device finishes searching for Wi-Fi networks, select the SSID of the Router.

Note: Each Router is configured with a default SSID and its own unique password. Look for the label showing the SSID and password information on the housing of the Router.

4. Enter the password from the label to associate your device with the Router and connect to the Internet.

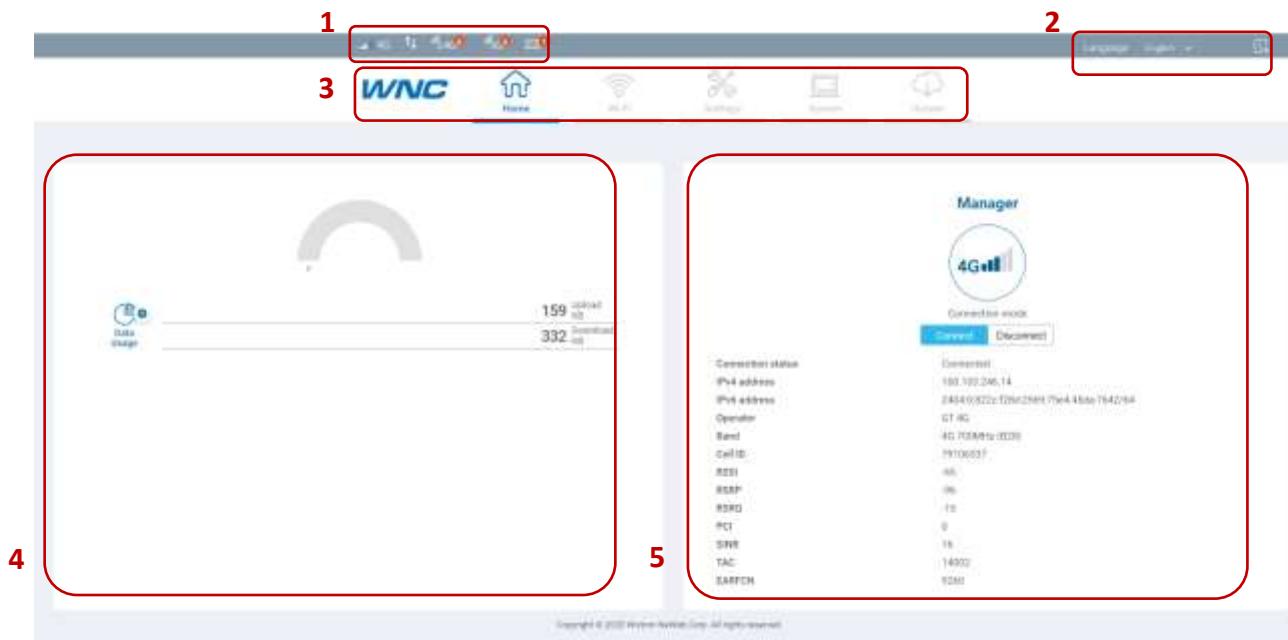
5. Web User Interface

5.1 Accessing the Web User Interface

The **Web User Interface** allows you to configure the Router using your web browser.

1. Ensure that the computer you use is connected to the Router.
2. Open your web browser and type **192.168.1.1** in the address field.
3. An authentication screen will appear. Log into the Web UI page via the username and password below:
Username: admin
Password: admin
4. The Web UI page will appear. Click the items on the banner to access different management functions.
5. We recommend you change the password for greater system security. Please access the Web UI and then go to **System → Modify Password**.

5.2 Web User Interface Introduction



1. Basic Information	Provides information including: Signal strength of the connected mobile network, connection mode, and number of connected devices on each type of connection.
2. Language/Web UI Log-out	Click the drop-down list to select a preferred language.
3. Management Function	Click the icon to access each management function.
4. Internet Usage	Displays data usage
5. Connection Information	Provides information including: Name of the mobile network service provider, connection mode, cell ID, and LTE signal strength indicators

6. Home

This page displays basic system information including a summary of the Internet and Manager.



Internet:

The left side of this page indicates Internet data usage, including total data usage (download/upload).

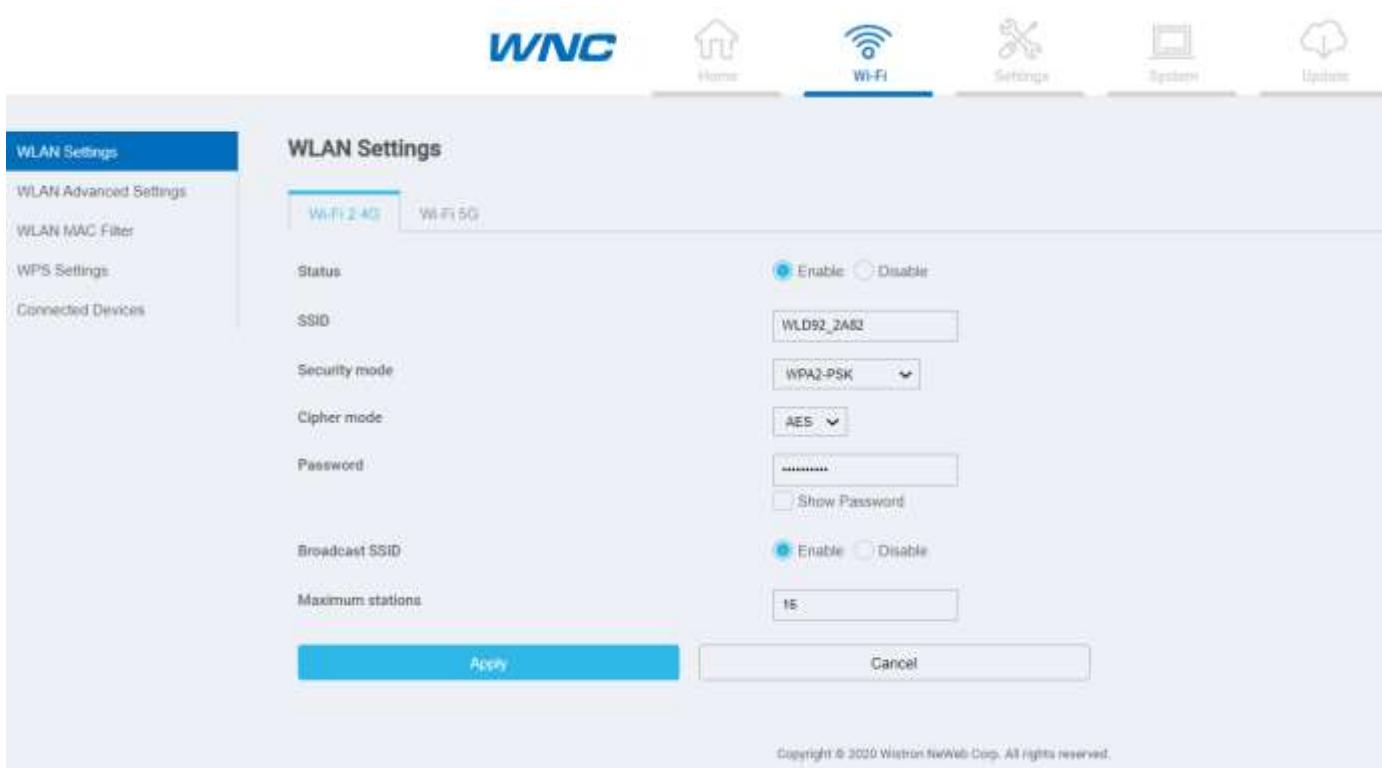
Manager:

Displays the connection mode, connection status, IPv4 address, operator, Band, cell ID, RSSI, TAC, and EARFCN.

7. Wi-Fi

Click the Wi-Fi icon on the top menu, and the following content will appear. The side menu indicates the current displayed menu. When in a Wi-Fi menu page, click the Wi-Fi 2.4G or Wi-Fi 5G tabs located on top to adjust settings for these frequency bands.

7.1 WLAN Settings



Status: Choose **Enable** or **Disable** to enable or disable the SSID function.

SSID: The Service Set Identifier (SSID) is the name of the wireless network broadcasting from this system. In order for computers to connect to the local network over a wireless link, they must select this network name from the list of detected wireless networks in the area.

Security mode: Select one security method from the drop-down menu.

None (Open): This mode allows all Wi-Fi devices to connect to the Router without any security protection.

WPA2-PSK: Use for WPA2-level encryption.

WPA/WPA2-PSK: Enables both WPA- and WPA2-level wireless protected access modes.

Cipher mode: Select one cipher mode from the drop-down menu.

TKIP+AES: This is what the encryption standards are for WPA2 (TKIP) and WPA2/802.11i (AES). It will attempt to use AES if it's available. If not, it will fall back to TKIP. This setting offers the most compatibility but won't guarantee a higher level of encryption if a device falls back to TKIP.

AES: The Advanced Encryption Standard (AES) is a symmetric key encryption standard that has been widely adopted today.

Password: Specify a password for your wireless network.

Show password: Displays the password when the check box is selected.

Broadcast SSID: Select **Enable** if you want to broadcast this SSID. The SSID will be displayed when you search for available networks. Select **Disable** if you do not want to broadcast this SSID.

Maximum stations: The maximum number of guest Wi-Fi clients allowed on the Router.

Click **Apply** to activate your settings, or click **Cancel** to discard any changes you made.

7.2 WLAN Advanced Settings

The screenshot shows the 'WLAN Advanced Settings' configuration page. The 'WiFi 2.4G' tab is active. The configuration fields are as follows:

- Channel:** Auto
- 802.11 Mode:** Auto bgn
- Bandwidth:** 20/40MHz
- Transmission power:** 100%
- Fixed Transmission Rate (MCS):** Auto
- Fragmentation Threshold:** 2347 bytes
- RTS Threshold:** 2346 bytes
- WMM:** Enable (radio button selected)
- DTIM Period:** 3
- Guard Interval:** Auto (radio button selected)
- Preamble type:** Long Preamble (radio button selected)
- Beacon Interval:** 100 ms

At the bottom are 'Apply' and 'Cancel' buttons.

Channel: This specifies the frequency the radio uses to transmit the wireless frames. Select a channel from the list of channels or choose **Auto** to allow the system to determine the best channel to use.

802.11 Mode: Select the 802.11 modulation technique. The available modes are:

For Wi-Fi 2.4G:

Auto b/g/n: Select this mode to allow devices supporting 802.11b, 802.11g, or 802.11n to connect to the Router.

b only: Establishes the Wi-Fi network in 802.11b mode. Only 802.11b-compatible devices can connect to the Router via Wi-Fi.

g only: Establishes the Wi-Fi network in 802.11g mode. Only 802.11g-compatible devices can connect to the Router via Wi-Fi.

n only: Establishes the Wi-Fi network in 802.11n mode. Only 802.11n-compatible devices can connect to the Router via Wi-Fi.

Auto b/g: Select this mode to allow devices supporting 802.11b or 802.11g to connect to the Router.

Auto g/n: Select this mode to allow devices supporting 802.11g or 802.11n to connect to the Router.

For Wi-Fi 5G:

Auto an/ac: Select this mode to allow devices supporting 802.11an or 802.11ac to connect to the Router.

Auto an: Select this mode to allow devices supporting 802.11an to connect to the Router.

a only: Establishes the Wi-Fi network in 802.11a mode. Only 802.11a-compatible devices can connect to the Router via Wi-Fi.

n only: Establishes the Wi-Fi network in 802.11n mode. Only 802.11n-compatible devices can connect to the Router via Wi-Fi.

Bandwidth: You can then specify the bandwidth for each channel.

Transmission power: Select the signal power strength of the Router's Wi-Fi network.

Fixed Transmission Rate (MCS): Modulation and Coding Scheme (MCS) refers to the index values showing the maximum available data rate of the Router. It is based on channel size, number of spatial streams, coding method, modulation technique, and guard interval.

Fragmentation Threshold: This is the maximum length of the frame, in bytes, beyond which packets must be broken up (fragmented) into two or more frames. Collisions occur more often for long frames because while sending them they occupy the channel for a longer time. The default value is 2347, which effectively disables fragmentation.

RTS Threshold: The Request to Send (RTS) threshold is the frame size in bytes above which the Router is required to check the transmitting frames to determine if RTS/Clear to Send (CTS) handshake is required with the receiving client. Using a small value causes RTS packets to be sent more often, thus no available time can be used to transmit data, reducing the apparent throughput of the network packets. The default value is 2346, which effectively disables RTS.

WMM: WMM stands for Wi-Fi Multimedia, a standard that allows routers to rearrange packets based on the contents of those packets. WMM was designed to enhance the streaming of multimedia over wireless devices. Select **Enable** or **Disable** to have the WMM function activated or deactivated.

DTIM Period: A delivery traffic indication map (DTIM) informs client that the broadcast data has been stored in the AP buffer. It is generated within the periodic beacon at a frequency specified by the DTIM Interval. Enter **DTIM Period** between 1 to 10.

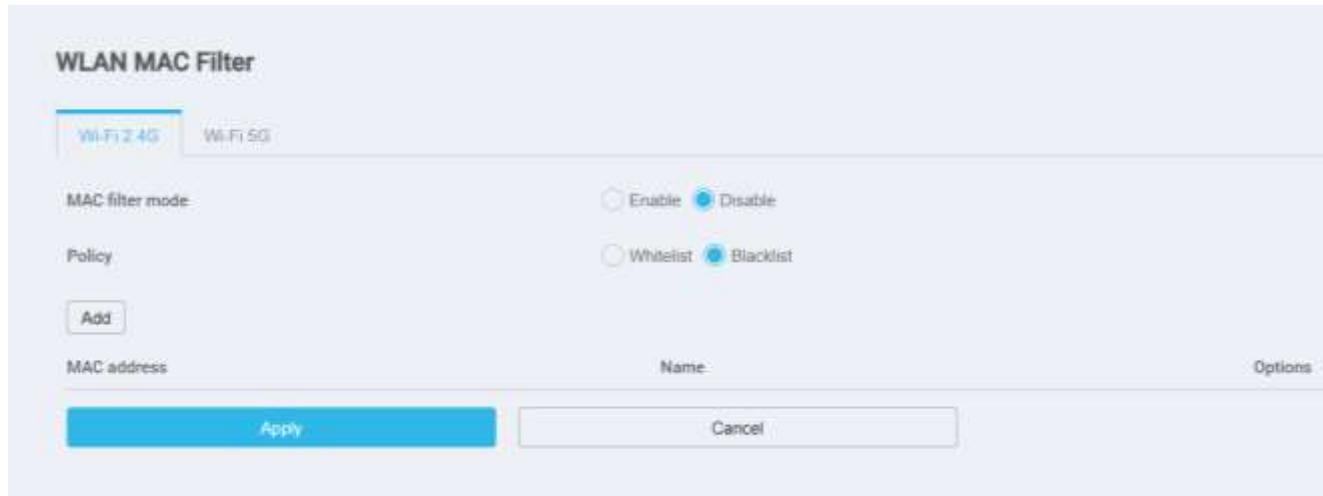
Guard Interval: A guard interval is the space between symbols being transmitted. It is intended to avoid inter-symbol interference from multipath effect. Select **Auto** or **Long** for the guard interval.

Preamble type: Select **Long Preamble** or **Short Preamble** for the Preamble type.

Beacon Interval: Enter the time in milliseconds between beacon transmissions. The default interval is 100 milliseconds.

Click **Apply** to activate your settings, or click **Cancel** to discard any changes you made.

7.3 WLAN MAC Filter



Enabling the WLAN MAC Filter function allows you to block or allow computer devices from establishing a wireless link to the Router. The filtering is based on the wireless computer's unique hardware ID (MAC address). With this feature, you can prevent unauthorized computers from accessing the Router and the services it offers. This feature helps in securing the wireless connectivity of a home network.

1. Choose a corresponding MAC filter mode (**Enable** or **Disable**).

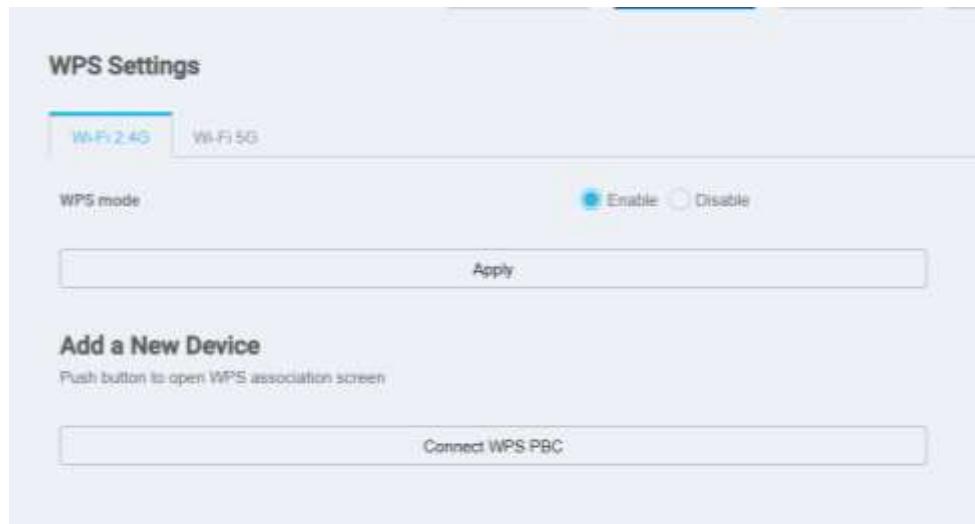
2. Select a **policy** for the **MAC filter mode**:

Whitelist: Only devices with its MAC address listed here are allowed to connect to this Router via Wi-Fi.

Blacklist: Devices with its MAC address listed in the table will be blocked when attempting to connect to this Router via Wi-Fi.

To add a MAC address to the Blacklist or Whitelist, click **Add** and enter the MAC address and the name. Then click **OK** and **Apply**. Click **Cancel** to discard any changes you made.

7.4 WPS Settings



WPS (Wi-Fi Protected Setup) is a computing standard for easy and secure setup of a wireless connection. This function allows rapid wireless connection between the Router and other WPS-compatible devices.

WPS mode:

Select **Enable** or **Disable** to enable or turn off the WPS function, then click **Apply**.

Add a New Device:

Connect WPS PBC (Push-button configuration):

1. Press the WPS button on the WPS-compatible device that supports WPS connectivity.
2. Click **Connect WPS PBC** to establish a wireless connection.

7.5 Connected Devices

The function presents a list of devices that are currently connected to the Router. When a wireless device is connected via Wi-Fi, you can click the **Add to blacklist** button to add this device to the access control list of MAC addresses. Connection to this device will then be blocked.

Connected Devices			
IP address	Host name	MAC address	Options
Copyright © 2020 Wistron Network Corp. All rights reserved.			

8. Settings

Click the **Settings** icon on the top menu, and the following content will appear. The side menu indicates the current menu link.

8.1 Quick Setup

Click **Quick Setup** on the side menu to start configuring the basic settings for using the Router. Detailed instructions can be referenced in other sections of the manual.

1. APN Settings

The screenshot shows the 'APN Settings' page under the 'Quick Setup' menu. The left sidebar lists various configuration options: Dial-up, Ethernet, Operating mode, DHCP, DNS, Security, Parental Control, Bandwidth Management, Routing, Statistics, and DNS. The main content area is titled 'APN Configuration' and is divided into two sections: 'Admin' and 'User'. Both sections contain fields for 'Applied profile' (set to 'Internet'), 'Profile Name' (left empty), 'Authentication' (set to 'None'), 'User name' (left empty), 'Password' (left empty), 'Show Password' (unchecked), 'IP type' (set to 'IPv4&IPv6'), and 'IPv6 prefix delegation' (radio button set to 'Disable'). The 'APN' field is populated with 'usconetel'. At the bottom are 'New Profile' and 'Next >' buttons.

APN Settings	
APN Configuration	
Admin	
Applied profile	Internet
Profile Name	
Authentication	None
User name	
Password	
Show Password	<input type="checkbox"/>
IP type	IPv4&IPv6
IPv6 prefix delegation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APN	usconetel
User	
Applied profile	Internet
Profile Name	
Authentication	None
User name	
Password	
Show Password	<input type="checkbox"/>
IP type	IPv4&IPv6
IPv6 prefix delegation	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APN	usconetel

New Profile Next >

For detailed instructions on the APN Settings, please refer to section 8.2.

2. Ethernet Settings

Select a connection mode and enter its related information to complete the settings. Refer to section 8.3 for detailed descriptions.



3. WLAN Settings



Specify a name and password for your 2.4G or 5G wireless network, then click **Finish**.

Once the statement below appears, you have performed all the necessary settings:

Congratulations! You can now enjoy the Internet!

8.2 Dial-up

Mobile Connection



Mobile connection: Your mobile connection status is displayed here. Click **Disconnect** to disable mobile data connection.

Data roaming: Click **Enable** to activate the data roaming function. Click **Disable** to stop data roaming.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

APN Configuration

The screenshot shows the APN Configuration page with a sidebar on the left containing various network settings. The 'APN Configuration' tab is selected. The main area is divided into two sections: 'Admin' and 'User'. Each section contains fields for Authentication, User name, Password, IP type, IPv6 prefix delegation, and APN. The 'Admin' section has 'None' selected for Authentication, while the 'User' section has 'Internet' selected. The 'User' section also has 'IPv4/IPv6' selected for IP type and 'Enable' selected for IPv6 prefix delegation. Both sections have 'us00inet' entered in the APN field. At the bottom are buttons for 'New Profile', 'Apply', and 'Cancel'.

APN Configuration		
Admin	Authentication	None
	User name	
	>Password	<input type="checkbox"/> Show Password
	IP type	IPv4/IPv6
	IPv6 prefix delegation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	APN	us00inet
	Applied profile	Internet
	Profile Name	Internet
	Authentication	None
User	User name	
	Password	<input type="checkbox"/> Show Password
	IP type	IPv4/IPv6
	IPv6 prefix delegation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	APN	us00inet
	New Profile	Apply
		Cancel

Applied profile: Select a profile from the drop-down list.

Profile Name: Specify a profile name for the selected profile.

Authentication: Select an authentication type for the profile.

User name: The user name that you registered for the service.

Password: The password that you registered for the service.

Show Password: The password that you registered for the service.

IP type:

IPv4: Use Internet Protocol version 4 (IPv4).

IPv6: Use Internet Protocol version 6 (IPv6).

IPv4 & IPv6: Use both IPv4 and IPv6.

IPv6 prefix delegation: Click **Enable** to enable prefix delegation. Click **Disable** to stop the prefix delegation function.

APN: Specify the Access Point Name (APN).

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

Network Settings

You can select a cellular network mode and set the band(s) for it on this page.

The screenshot shows the Network Settings page with a sidebar on the left containing various network configuration options. The 'Network Settings' option is highlighted with a blue bar. The main content area is divided into two sections: 'Band Settings' and 'Network Settings'.

Band Settings: This section allows selecting LTE bands. It shows an 'LTE band setting' field with checkboxes for bands B2, B4, B5, B12, and B66, all of which are checked. Below this are 'Apply' and 'Cancel' buttons.

Network Settings: This section allows selecting the cellular network mode and the search mode. It shows a 'Cellular network mode' dropdown set to '4G' and a 'Network search mode' section with 'Auto' (selected) and 'Manual' radio buttons. Below this are 'Apply' and 'Cancel' buttons.

At the bottom right of the main content area, there is a copyright notice: 'Copyright © 2020 Wistron NeWeb Corp. All rights reserved.'

Band Settings:

Tick the checkboxes to select the LTE bands for your cellular network.

Network Settings:

Cellular network mode: Select your operator's network mode to log in to the network.

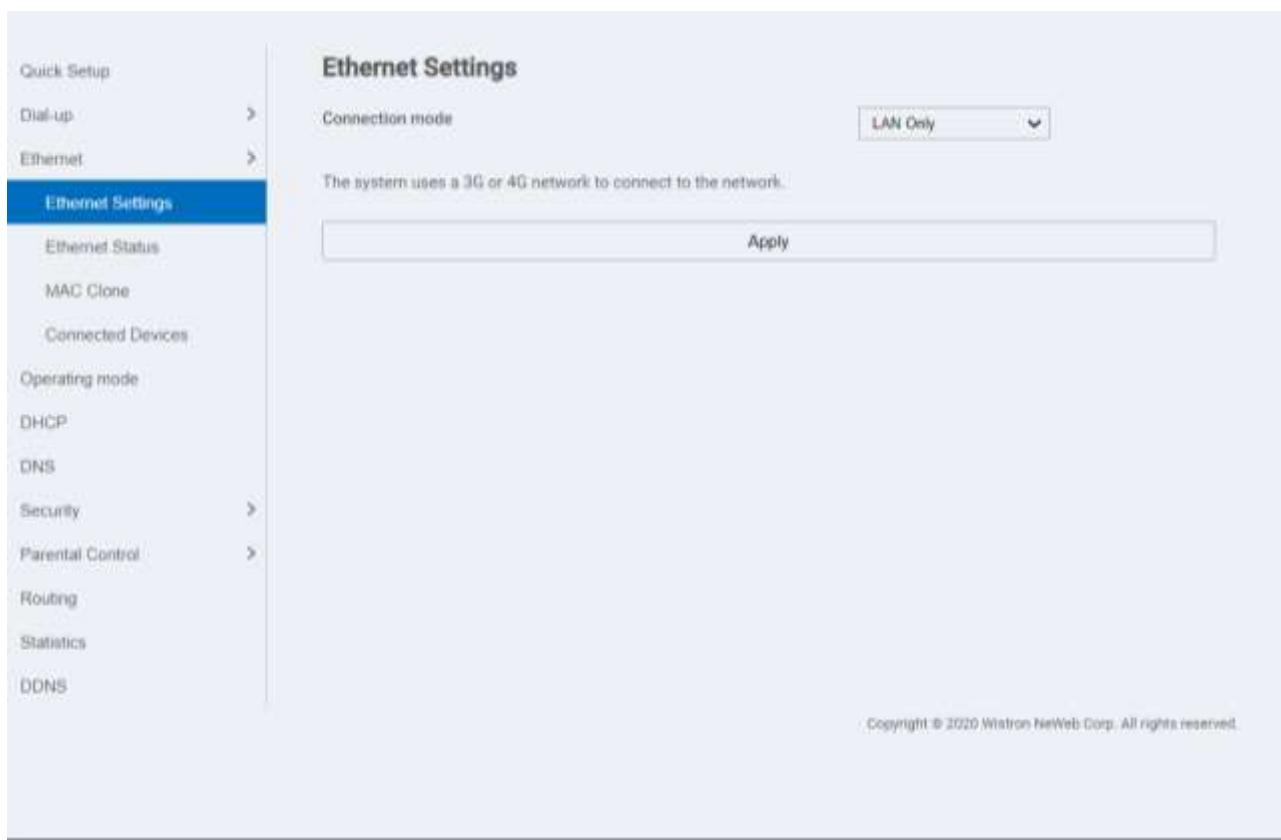
Network search mode: Select **Auto** or **Manual** to search the network.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

8.3 Ethernet

Ethernet Settings

You can select a connection mode for your Internet connection according to your application situation.



<Auto>

In Auto mode, the Router selects the best network access mode based on the network environment.

1. Select **Auto** from the **Connection mode** drop-down list.
2. Click **Apply** to save your changes.

< PPPoE + Dynamic IP >

The **PPPoE + Dynamic IP** mode enables you to access the Internet using a PPPoE dial-up connection or a dynamic IP address.

1. Select **PPPoE + Dynamic IP** from the **Connection mode** drop-down list.
2. Set **Point-to-Point Protocol over Ethernet (PPPoE)** and **Dynamic IP** parameters.
3. Click **Apply** to save your changes.

< PPPoE>

This option is normally used by the DSL modem users to enter authentication information. You will need to have the user name and password provided by your network service provider for the PPPoE dial-up connection.

1. Select **PPPoE** from the **Connection mode** drop-down list.
2. Enter the user name and password provided by your network service provider.
3. Set the **MTU**. The default MTU size is 1492. Please do not edit the number unless absolutely necessary.
4. Choose to **Enable** or **Disable** IPv6.
5. Click **Apply** to save your changes.

<Dynamic IP>

This option is suitable for Internet services that do not require account authentication, for example, in

most cable-modem usage scenarios.

1. Select **Dynamic IP** from the **Connection mode** drop-down list.
2. Select the **Set DNS server manually** check box.
3. Enter **Primary DNS server** and **Secondary DNS server**.
4. Set the **MTU**. The default MTU size is **1500**. Please do not edit the number unless absolutely necessary.
5. Click **Apply** to save your changes.

<Static IP>

This option is suitable for services that use a fixed IP address.

1. Select **Static IP** from the **Connection mode** drop-down list.
2. Enter the **IP address**, **subnet mask**, **gateway address**, **primary DNS address**, and **secondary DNS address** (optional) provided by your network service provider.
3. Set the **MTU**. The default MTU size is **1500**. Please do not edit the number unless absolutely necessary.
4. Click **Apply** to save your changes.

<LAN only>

This option is suitable when the client is connected with a network cable but without Ethernet connection.

1. Select **LAN only** from the **Connection mode** drop-down list.
2. Click **Apply** to save your changes.

Ethernet Status

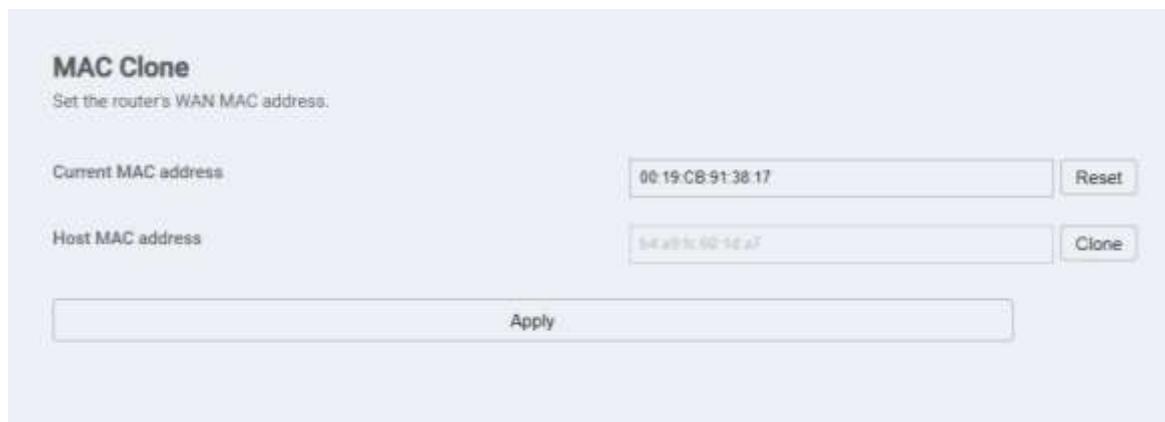
The section displays basic Ethernet status. To change the connection mode, go to **Settings** → **Ethernet** → **Ethernet Settings**.



Ethernet Status	
Duration	00:00:00:00
Connection status	Disconnected
MAC Address	00:19:CB:91:38:17
Connection mode	LAN Only
IP address	0.0.0.0
Subnet mask	0.0.0.0
Default gateway	0.0.0.0
Primary DNS server	0.0.0.0
Secondary DNS server	0.0.0.0

To update the information on this page, click **Refresh**.

MAC Clone



MAC Clone	
Set the router's WAN MAC address.	
Current MAC address	<input type="text" value="00:19:CB:91:38:17"/> <input type="button" value="Reset"/>
Host MAC address	<input type="text" value="00:19:CB:91:38:17"/> <input type="button" value="Clone"/>
<input type="button" value="Apply"/>	

Some ISPs may register the MAC address of your computer when dialing up to the Internet for the first time via modem. If you add a router into your network to share your Internet connection, the ISP will not accept that policy. Therefore, you need to create a MAC clone on the Router.

At the **Host MAC address** field, click **Clone** to clone your PC's MAC address as the WAN MAC address of the Router. The same MAC address will be cloned to the **Current MAC address** field.

Click **Apply** to save the settings.

Connected Devices

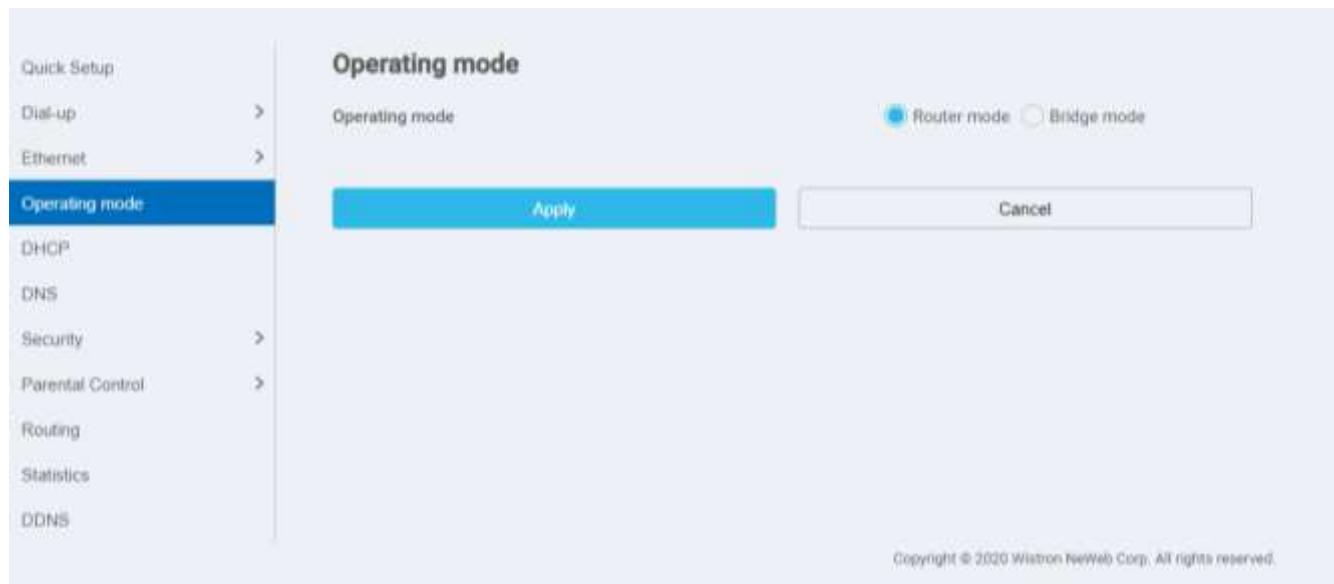
The section displays information of LAN connected devices, including the connection type, IP address, host name, and MAC address.

Connected Devices			
Type	IP address	Host name	MAC address
DHCP	192.168.1.10	T1-1-1-Q-45363	b4:e9:fc:60:1d:a7

8.4 Operating Mode

You can use the Router in Router mode or Bridge mode. When in Bridge mode, the Router supports one device and Wi-Fi will be disabled.

Operating mode: Select the desired mode to set up the device as a router or as a bridge.

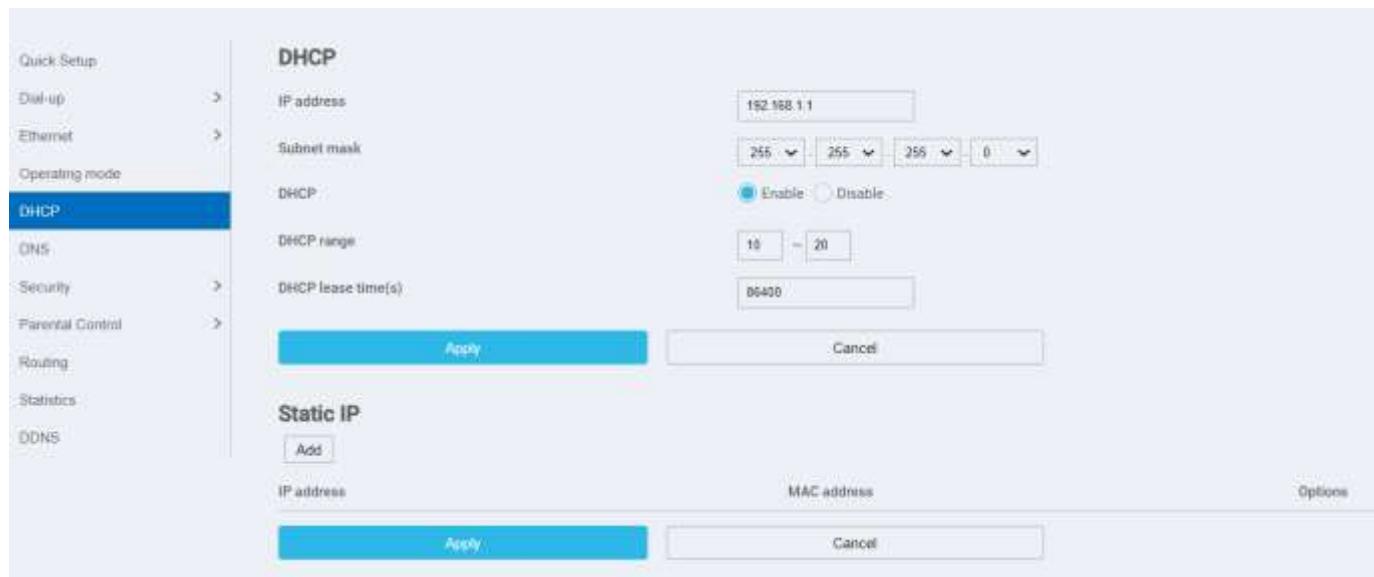


Click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.

8.5 DHCP

DHCP

DHCP assigns LAN IP addresses for connected devices. You can specify an IP address range for the Router to assign from.



IP address: Specify an IP address range for the Router to assign from.

Subnet mask: The subnet mask along with the previously configured IP address defines the network. The default value for subnet mask is 255.255.255.0.

DHCP: Select **Enable** or **Disable** to activate the function.

DHCP range: Type a DHCP range in the fields.

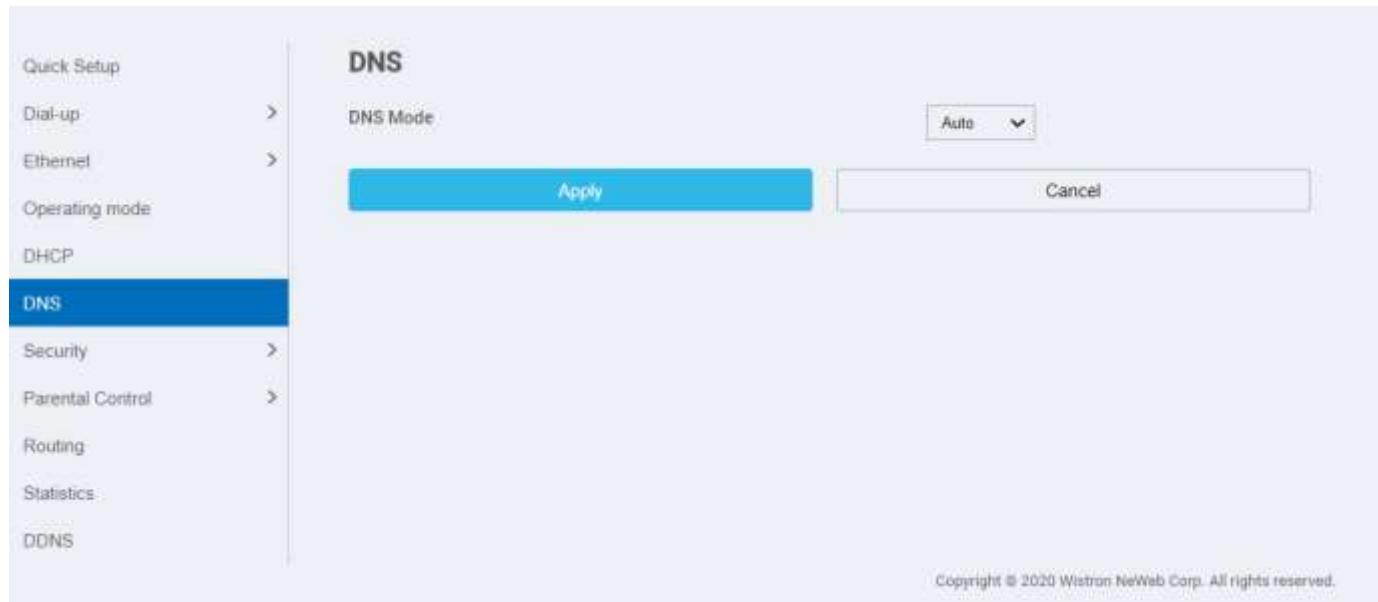
DHCP lease time(s): You can specify a period of time after which an assigned IP address will be retrieved from devices.

Static IP: The Static IP function enables you to assign IP address manually to each device. Click **Add**, and a text field will appear below **IP Address** and **MAC address** for you to manually input an IP address and MAC address for your device. After you have entered the addresses, click **OK** to complete data entry, or click **Cancel** to discard any changes you made.

After entering the settings, click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.

8.6 DNS

Domain Name System (DNS) is an Internet service that translates domain names into IP addresses or vice versa. You may select Auto, Relay or Manual in the DNS mode pull-down menu.



Auto: The device will automatically obtain the DNS server address.

Relay: After selecting this option, enter the primary and secondary DNS addresses of the DNS relay server.

Manual: After selecting this option, enter the primary and secondary DNS addresses

Click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.

8.7 Security

Firewall Switch

This page displays the firewall settings of the Router.

Quick Setup

Dial-up

Ethernet

Operating mode

DHCP

DNS

Security

Firewall Switch

LAN IP Filter

Port Forwarding

DMZ

ALG

UPnP

NAT Settings

DoS Attack

Remote Management

VPN Pass Through

Bandwidth Management

Firewall Switch

Enable Firewall

Security level

Disable WAN port ping

Apply

Cancel

Enable Firewall: The Router has a built-in firewall. To disable the firewall, select **Disable**.

Security Level: Select from one of the three security levels to protect the local network from Internet intrusion.

High Security: All incoming requests from the Internet are blocked by default and the Router allows limited Internet destined traffic from leaving the local network. This mode is the highest level of security. All traffic from the Internet is blocked from reaching the local network, except that which is allowed via port forwarding policies that apply to the local network. A limited set of commonly used services are permitted to be accessed from the local network such as web traffic (HTTP / HTTPS) or file transfer (FTP).

Medium Security: All incoming requests from the Internet are still blocked by default but the computers on the local network can access the Internet without restrictions. This is the default setting and generally the most appropriate security setting for home networks. All traffic from the Internet is blocked from reaching the local network, thus blocking unwanted intrusion from the outside. At the same time local network users are given unrestricted access to the Internet regardless of service or application.

Low Security: This setting opens the firewall for all traffic to and from the Internet. This mode provides unrestricted access from the local network to the Internet and vice-versa. It is not recommended to set the Router's firewall to this mode without additional parental controls as it makes the local network vulnerable to attack from the Internet.

Disable WAN port ping: Disabling WAN port ping will make the Router drop any ICMP ping requests (which is usually used for network diagnostic purposes) to prevent DoS (Denial of Service) attacks.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

LAN IP Filter

Turn the LAN IP Filter on to limit the Internet access on some specified computers.



1. To enable the LAN IP Filter, select **Enable**.
2. At the **Policy** field, select **Whitelist** or **Blacklist** to allow or block an LAN IP address.
3. Click **Add** and type the IP address of the device in the **LAN IP address** field.
4. Type the value range of the LAN port in the **LAN port** field.
5. Type the WAN IP address of the device in the **WAN IP address** field.
6. Type the value range of the WAN port in the **WAN port** field.
7. At the **Protocol** drop-down list, select a protocol. The service uses the following layer-4 protocols: TCP/UDP, TCP, UDP, and ICMP.
8. At the **Status** drop-down list, select **On** or **Off** as the status of the service.
9. Under **Options**, click **OK** to complete data entry, or click **Cancel** to undo the changes.
10. Click **Apply** to confirm your settings, or click **Cancel** to discard any changes you made.

Port Forwarding

Port Forwarding can be used to open certain ports of a device to communicate with an Internet service. If a computer in your LAN is configured as a Web server, a designated port must also be opened for devices from the Internet to communicate with this server.



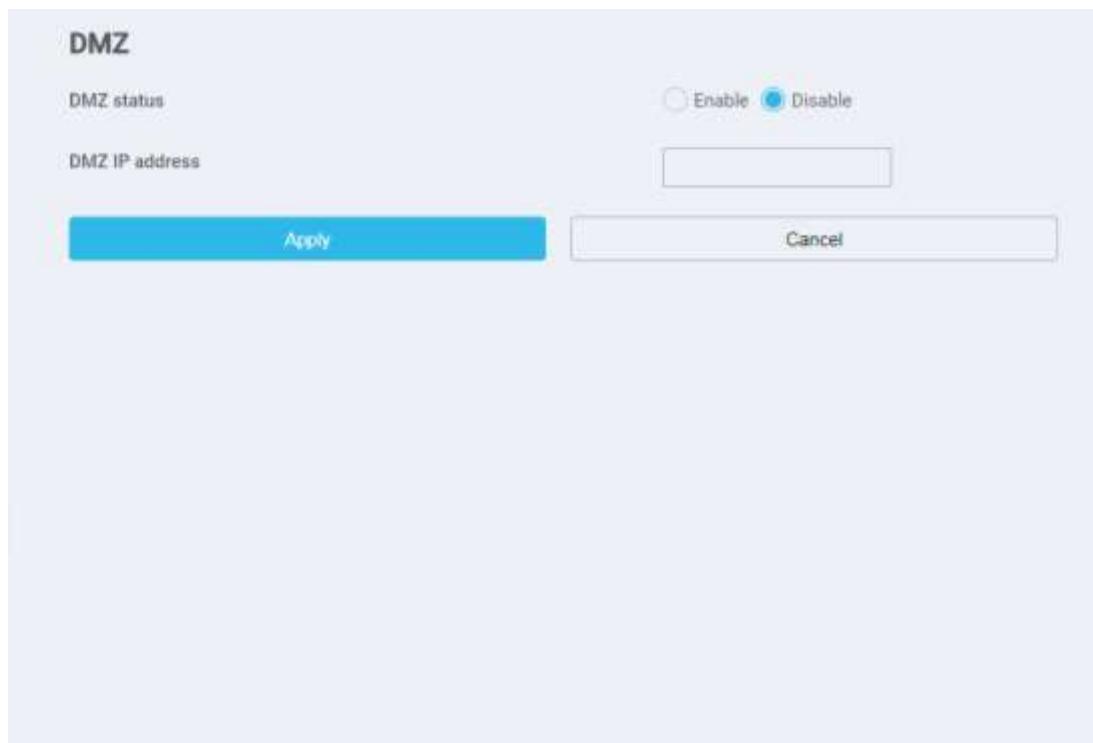
Name	WAN port	LAN IP address	LAN port	Protocol	Status	Options

1. To enable port forwarding, select **Enable**.
2. Click **Add** and type the name of the service for which the port forwarding rule has been created in the **Name** field.
3. Type the value range of the WAN port in the **WAN port** field.
4. Type the IP address of the device in the **LAN IP address** field.
5. Type the value range of the LAN port in the **LAN port** field.
6. At the **Protocol** drop-down list, select a protocol. The service uses the following layer-4 protocols: TCP/UDP, TCP, and UDP.
7. Select **On** or **Off** as the status of the service.
8. Under **Options**, click **OK** to complete data entry, or click **Cancel** to undo the changes.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

DMZ

DMZ (De-Militarized Zone) allows you to specify a DMZ host IP to redirect requests to a virtual DMZ host in order to enhance the security of the local area network.



The screenshot shows a configuration interface for the DMZ function. At the top, the word "DMZ" is displayed in a bold, black font. Below it, the text "DMZ status" is followed by two radio buttons: "Enable" (unselected) and "Disable" (selected, indicated by a blue circle). A text input field for "DMZ IP address" is present, but it is empty. At the bottom of the interface are two buttons: a blue "Apply" button on the left and a white "Cancel" button on the right.

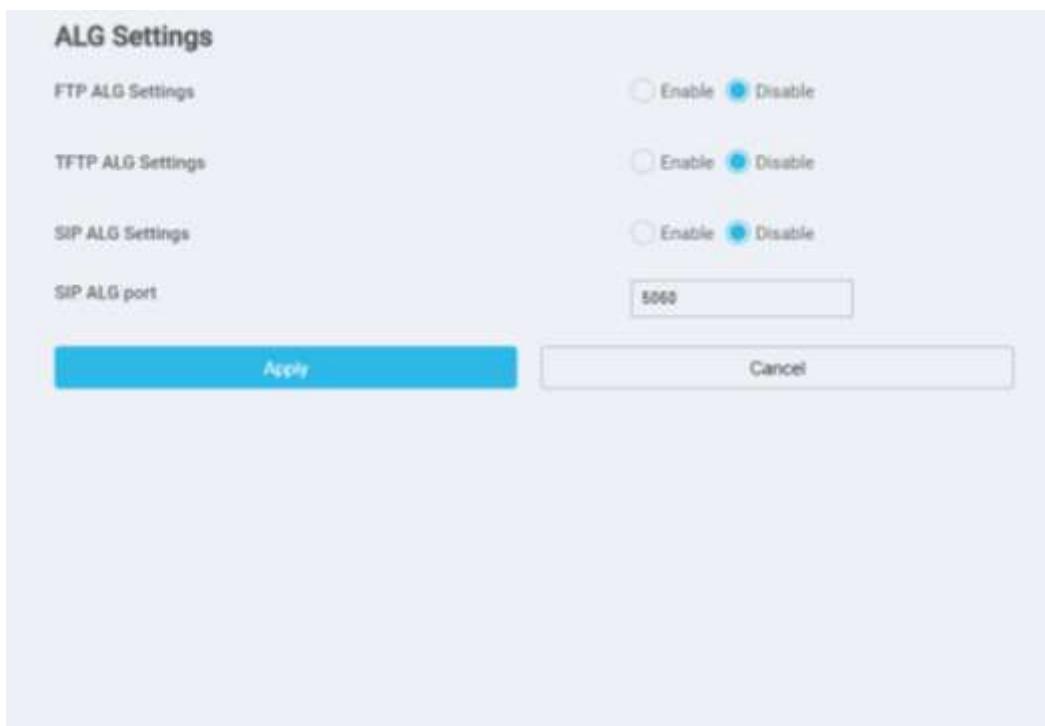
DMZ status: If this function is enabled, threats from external networks will be directed to the DMZ instead of the network.

DMZ IP address: The IP address of the host DMZ.

To designate a device as a DMZ host, enter its IP address in the **DMZ IP Address** text field. Click **Apply** to apply the changes, or click **Cancel** to undo your configuration.

ALG

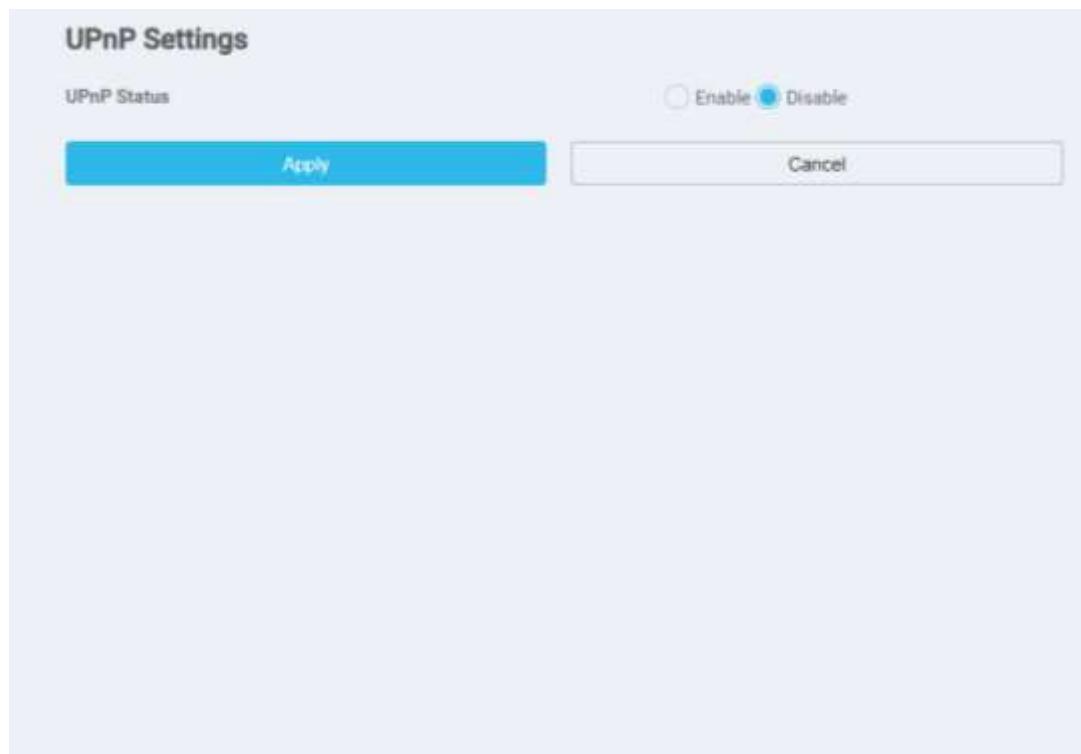
File Transfer Protocol (FTP) is a commonly used method of exchanging files over IP networks. Trivial File Transfer Protocol (TFTP), is a file transfer protocol is used for transferring small files using UDP across networks. The Session Initiation Protocol (SIP) is used to begin, change, or end a session, and an Application Layer Gateway (ALG) is a security component for checking the status of data packages. To complete an FTP, TFTP, or SIP ALG, enable their respective functions on this page.



1. Select **Enable** or **Disable** to activate or deactivate FTP, TFTP, or SIP ALG.
2. In **SIP ALG port**, specify the SIP port number provided by your Internet service provider. Click **Apply**.

UPnP

For devices that support Universal Plug and Play (UPnP), enabling the UPnP function will allow automatic port forwarding that helps your UPnP devices communicate with the Internet.

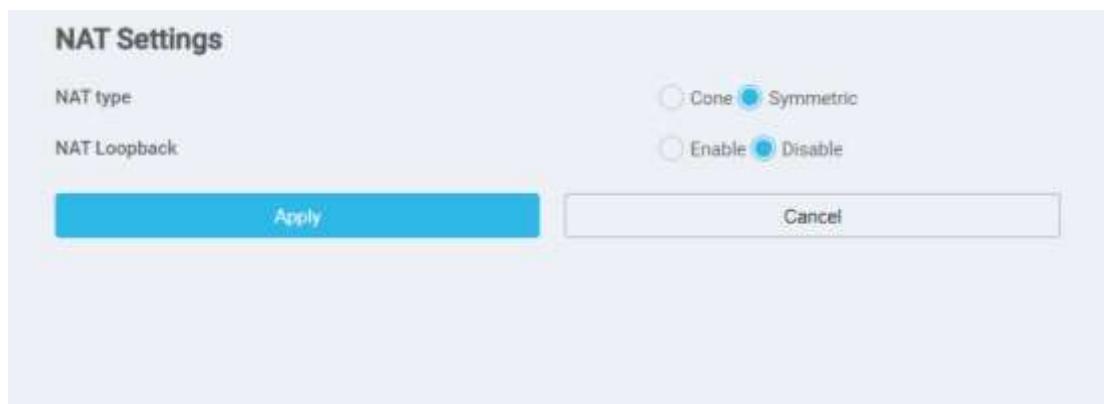


1. At the **UPnP Status**, select **Enable** or **Disable** to enable or disable the UPnP port mapping function.
2. Click **Apply** to apply the settings.

NAT Settings

Network Address Translation (NAT) is a technique which allows several computers on a LAN to share an Internet connection. The computers on the LAN use a “private” IP address range while the WAN port is configured with a single “public” IP address.

Along with connection sharing, NAT also hides internal IP addresses from computers on the Internet.



NAT Type:

Cone: Based on a cone NAT type, the port is permanently open and allows inbound connections from any external host.

Symmetric: Each request from the same internal IP address and port to a specific destination IP address and port is mapped to a unique external source IP address and port. Even if the same internal host sends a packet with the same source address and port but to a different destination, a different mapping is used. Only an external host that receives a packet from an internal host can send a packet back.

Select an **NAT type**, then click **Apply**. Click **Cancel** to undo the settings.

NAT Loopback:

NAT loopback is a feature which allows the access of a service via the WAN IP address from within your local network. Select **Enable** to activate this feature.

DoS Attack

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network by flooding it with traffic, making it inaccessible to its intended users.

The screenshot shows a configuration interface for 'DoS Attack' with the following settings:

- DoS Protection:** Enabled (radio button selected)
- SYN Flood:** Enabled (radio button selected)
Value: 128 packets/sec
- ICMP Flood:** Enabled (radio button selected)
Value: 100 packets/sec

Buttons at the bottom: **Apply** (highlighted in blue) and **Cancel**.

DoS Protection:

Select **Enable** to activate the DoS protection feature.

SYN Flood:

Select **Enable** to activate the SYN Flood protection feature. In the field below, enter the maximum number of SYN packets per second the Router accepts before determining that an SYN Flood Intrusion is occurring. This value can range between 1 and 10,000 SYN packets per second. The default is 128 SYN packets per second.

ICMP Flood:

Select **Enable** to activate the ICMP Flood protection feature. The Router monitors the number of ICMP packets per second, not including ping packets, to determine when to declare an ICMP flood intrusion event. ICMP flood events are not blacklisted. This value can range between 1 and 10,000 ICMP packets per second. The default is 100 ICMP packets per second.

Click **Apply** to apply the settings.

Remote Management

Remote management enables users to access and manage the Router from a remote location.

IMPORTANT: When Remote Management is enabled, the security appliance is accessible to anyone who knows its IP address. Since a malicious WAN user can reconfigure the Router and misuse it in many ways, it is HIGHLY RECOMMENDED that you change the admin and guest passwords before continuing.

The screenshot shows a configuration interface for 'Remote Management'. At the top, there is a section for 'Secured Client IP Address' with two radio button options: 'All IP' (selected) and 'Selected (IP/Subnet)' (unchecked). Below this is a section for 'Remote Port Settings' with two groups. The first group for 'Http' has an 'Enable' radio button (unchecked) and a port field containing '8580'. The second group for 'Https' has an 'Enable' radio button (checked) and a port field containing '8443'. At the bottom of the interface are two buttons: a blue 'Apply' button on the left and a white 'Cancel' button on the right.

Remote Management:

Secured Client IP Address: Select **All IP** to allow all IPs to access and manage the Router remotely. Select **Selected (IP/Subnet)** to assign specific IPs that are authorized to access and manage the Router remotely.

Remote Port Settings:

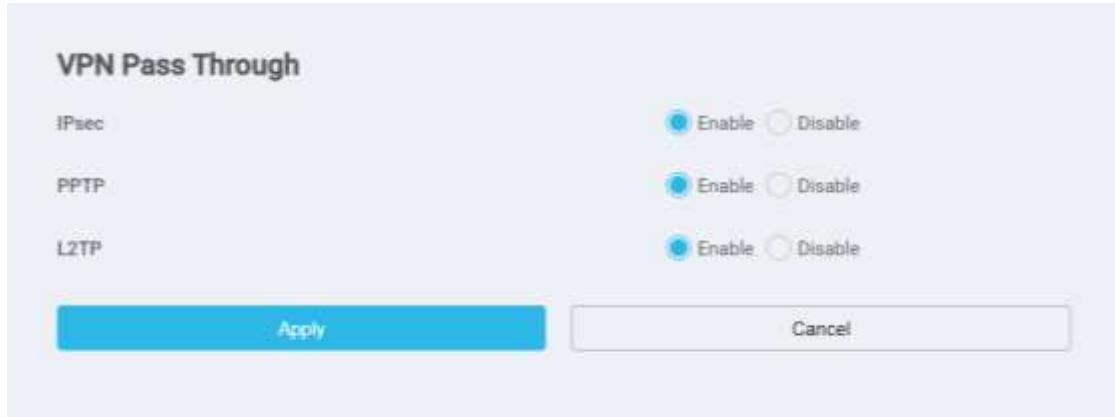
Http: Select **Enable** to allow clients to connect to the Router remotely via Hypertext Transfer Protocol (HTTP). In the field below, enter the port on which remote access is allowed.

Https: Select **Enable** to allow clients to connect to the Router remotely via HyperText Transfer Protocol Secure (HTTPS). In the field below, enter the port on which remote access is allowed.

Click **Apply** to apply the settings, or click **Cancel** to undo the settings.

VPN Pass Through

VPN pass through allows devices connected to the Router to establish outbound VPN connections.



IPsec: Select **Enable** to allow IPSec pass through.

PPTP: Select **Enable** to allow the Point-to-Point Protocol (PPP) pass through.

L2TP: Select **Enable** to allow Layer 2 Tunneling Protocol (L2TP) pass through.

Click **Apply** to apply the settings, or click **Cancel** to undo the settings.

Bandwidth Management

Bandwidth management controls network traffic to provide better service.

Bandwidth Management

Bandwidth Management: **Enable** **Disable**

Default: **Normal**

Profile of Bandwidth Management

Profile	UL (Mbps)	DL (Mbps)
Best effort	50	100
High	30	60
Medium	10	20
Normal	5	10

Bandwidth Management List

Add

MAC address	Profile	Options

Apply Cancel

Bandwidth Management: Select **Enable** to activate bandwidth management.

Default: Use the pull-down menu to set the default bandwidth management mode. The available modes are: Best effort, High, Medium, and Normal.

Profile of Bandwidth Management:

Enter the maximum upload and download data rates for each of the bandwidth management profiles

Bandwidth Management List:

Click **Add** and type the MAC address of the device that requires bandwidth management, and select the profile that will be applied to the device.

Click **Apply** to apply the settings, or click **Cancel** to undo the settings.

8.8 Parental Control

Access Time Restriction

This feature enables parents to set time periods to allow or disable Internet access for specific devices.

Name	MAC address	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	End	Options
									08:00	22:00	

Start: 08:00 End: 22:00

Apply Cancel

Access Time Restriction:

Select **Enable** to activate the access time restriction feature.

Click **Add** to enter the access time restrictions settings for devices.

1. Type the name of the device in the **Name** field.
2. Type the MAC address of the device in the **MAC address** field.
3. Select the days in the week as well as the time period in the day during which access time restrictions will be applied.
4. Under **Options**, click **OK** to complete data entry, or click **Cancel** to undo the changes.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

Domain Name Filter

A domain name filter can be used to block computers from accessing certain websites through the Router.

The screenshot shows a configuration page for a Domain Name Filter. At the top, there is a note: "Limitation: HTTPS webpages cannot be filtered." Below this, there are two main sections: "Domain Name Filter" and "Policy". Under "Domain Name Filter", there is an "Enable" checkbox (unchecked) and a "Disable" checkbox (checked). Under "Policy", there is a "Whitelist" checkbox (unchecked) and a "Blacklist" checkbox (checked). Below these sections is a table with three columns: "Domain Name", "Status", and "Options". A "Add" button is located above the table. At the bottom of the page are two buttons: "Apply" (highlighted in blue) and "Cancel".

1. Select **Enable** to activate the domain name filter feature.
2. At the **Policy** field, select **Whitelist** or **Blacklist** to allow or block a domain name.
3. Click **Add** to create an entry, and type in the domain name in the **Domain Name** text field.
4. Select **On** or **Off** from the **Status** drop-down list.
5. Under **Options**, click **OK** to complete data entry, or click **Cancel** to undo the changes.
6. Click **Apply** to activate your settings.

8.9 Routing

Users may enable or disable static routing and dynamic routing by adjusting the settings on this page.

The screenshot shows a network configuration interface with two main sections: **Static Routing** and **Dynamic Routing**.

Static Routing: This section has a radio button for **Enable** (selected) and **Disable**. Below it is a table with columns: Destination Network, IP Subnet Mask, Network, Gateway, Status, and Options. A large blue **Apply** button is at the bottom left, and a **Cancel** button is at the bottom right.

Dynamic Routing: This section has a radio button for **Enable** (selected) and **Disable**. Below it is a table with columns: Dynamic Routing Protocol (with a dropdown menu showing **RIP** and **RIPv2**), and a large blue **Apply** button is at the bottom left, and a **Cancel** button is at the bottom right.

At the bottom of the interface, a copyright notice reads: Copyright © 2002 MikroTik Corp. All rights reserved.

Static Routing:

1. Select **Enable** to activate static routing.
2. Click **Add** to create an entry, then type in the IP addresses for the **Destination Network** and **IP Subnet Mask**.
3. Select **LAN** or **WAN** from the network pull-down menu.
4. Type in the IP address for the **Gateway**.
5. Select **On** or **Off** as the status of the service.
6. Under **Options**, click **OK** to complete data entry, or click **Cancel** to undo the changes.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

Dynamic Routing:

Select **Enable** to activate dynamic routing.

Dynamic Routing Protocol: Select RIPv1 or RIPv2 as the routing method.

Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

8.10 Statistics

The screenshot shows a user interface for managing network statistics and data plans. The top section, 'Statistics', displays current and total traffic volume and duration. The 'Data Plan' section allows setting a monthly data plan with a start date, monthly limit, and threshold. Buttons for 'Apply' and 'Cancel' are at the bottom.

Statistics	
Current volume	189.68MB
Current duration	01:53:44
Total volume	189.68MB
Total duration	01:53:44

Data Plan

Start Date (1-31)	1
Monthly data plan	1
Threshold	80

Buttons: Clear history, Apply, Cancel.

Statistics

Here you can view the statistics of the Router, including total traffic volume/duration and current traffic volume/duration of the last packets statistic interval.

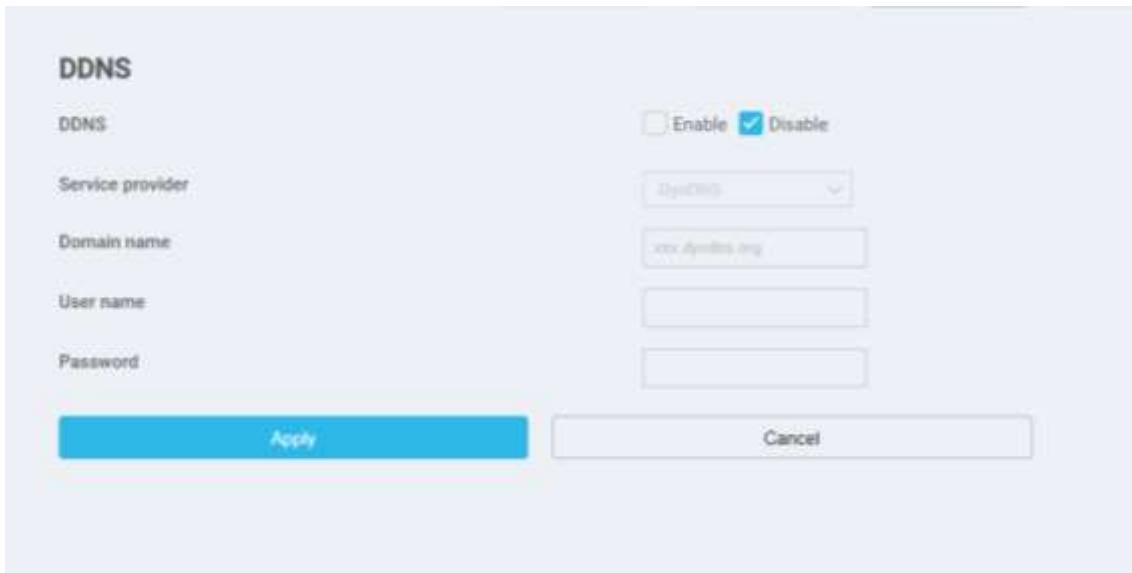
To reset the statistics, click **Clear history**.

Data Plan

You can set the data plan parameters here. Set the data plan parameters and click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.

8.11 DDNS

Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must set up an account with a DDNS provider such as DynDNS.org and fill in the required account details including the Domain name, User name, and Password on this page.



DDNS

DDNS Enable Disable

Service provider: DynDNS

Domain name: www.dynv6.org

User name:

Password:

Apply **Cancel**

DDNS: Select **Enable** or **Disable** to activate or deactivate the service.

Service provider: Select the DNS service that you are subscribed to.

Domain name: Enter the domain name of the DDNS account.

User name: Enter the username of the DDNS account. This will be provided by the DDNS service provider.

Password: Enter the password for the DDNS account.

Click **Apply** to apply the changes, or click **Cancel** to undo your configurations.

9. System

9.1 Device Information

This page displays relevant information of the Router including:

IMEI, ICCID, IMSI, your number, software version, MPSS (Manycore Platform Software Stack), hardware version, LAN MAC address, IPv4 address, IPv6 address, and the band that is currently in use.



Device Information		
Modify Password	IMEI	869257030039693
Diagnosis	ICCID	89886920041030577222
Restore Defaults	IMSI	466924103057722
Reboot	My number	0975438684
Date & Time	Software version	WLD92_v01.07.203131T
	MPSS	EG06ALAR02A07M4G
	Hardware version	01
	LAN MAC address	98:49:14:3E:2A:F2
	IPv4 address	10.142.187.56
	IPv6 address	2001:b400:e3d8:1e5d:99be:baa2:e30:3742/64
	Band	4G 2600MHz (B7)

Copyright © 2020 Wistron NeWeb Corp. All rights reserved.

Refresh: To update device information, click **Refresh**.

9.2 Modify Password

You can change the password used for accessing this Web UI and adjust the session expiration time.

To modify your password, type the current password first. Then input a new password in the **New password** field. Re-type the password in the **Confirm password** field. Click **Apply** to apply the settings. The default auto logout time is 180 seconds. To adjust the login time-out on the Web UI, input a time range between 30 seconds–600 seconds in the **Auto logout time** field. Click **Apply** to set your preferences, or click **Cancel** to discard any changes you made.

The screenshot shows a 'Modify Password' dialog box with the following fields and buttons:

- Current password:** An input field.
- New password:** An input field.
- Confirm password:** An input field.
- Auto logout time:** A numeric input field set to 180, with a dropdown menu showing "seconds".
- Buttons:** Two blue 'Apply' buttons (one for each password section) and two white 'Cancel' buttons (one for each password section and one for the auto logout time section).
- Copyright:** Copyright © 2020 Wistron NeWeb Corp. All rights reserved.

9.3 Diagnosis

If the Router cannot connect to the Internet, you can perform a diagnosis to find out the possible causes.

<Ping>

Select **Ping** from the **Diagnosis method** drop-down list.

1. Enter the IP address or domain name in the **Target IP or domain** text field.
2. Set the **Packet size**.
3. Set the **Timeout period**.
4. Select or clear **Do not fragment**.
5. Click **Apply**. The diagnostics results will then be displayed in the **Result** area at the bottom of the page. Click **Cancel** to discard any changes you made.

The screenshot shows the 'Diagnosis' configuration page. The 'Diagnosis method' dropdown is set to 'Ping'. The 'Target IP or domain' field is empty. The 'Packet size' is set to 32 bytes (1-8000 bytes). The 'Timeout period' is set to 4 seconds (1-10 seconds). The 'Do not fragment' checkbox is unchecked. Below the configuration area, the 'Result' section is titled 'Result' and contains a 'Result' and 'Details' link, with an empty text area for results.

<Traceroute>

Select **Traceroute** from the **Diagnosis method** drop-down list.

1. Enter the IP address or domain name in the **Target IP or domain** text field.
2. Set the **Maximum hops**.
3. Set the **Timeout period**.
4. Click **Apply**. The diagnostics results will then be displayed in the **Result** area at the bottom of the page.
Click **Cancel** to discard any changes you made.

Diagnosis

Diagnosis method

Target IP or domain

Maximum hops 1-100

Timeout period 2-10 seconds

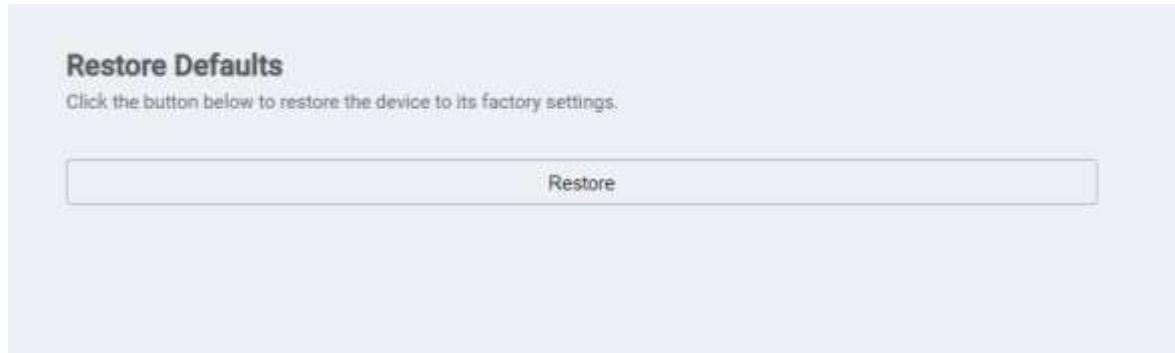
Result

Result

Details

9.4 Restore Defaults

To reset all the Router's settings to the factory default, click **Restore**.

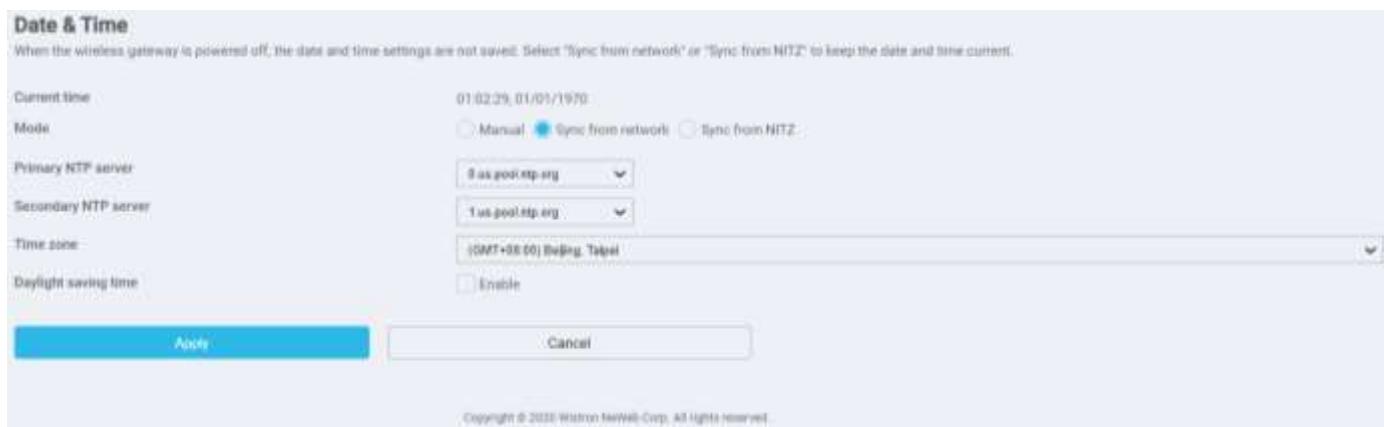


9.5 Reboot

To restart the device, click **Reboot**.



9.6 Date and Time



Date & Time
When the wireless gateway is powered off, the date and time settings are not saved. Select "Sync from network" or "Sync from NITZ" to keep the date and time current.

Current time: 01:02:29, 01/01/1970

Mode: Manual Sync from network Sync from NITZ

Primary NTP server: 0.us.pool.ntp.org

Secondary NTP server: 1.us.pool.ntp.org

Time zone: (CMT+08:00) Beijing, Taipeh

Daylight saving time: Enable

Copyright © 2023 Wistron Network Corp. All rights reserved.

Network Time Protocol (NTP) is a protocol that is used to synchronize the computer clock time among a network of computers. This page allows you to set the date, time, and NTP (Network Time Protocol) servers. Accurate time across a network is important for logging and execution of scheduled upgrades and scheduled policies. Setting the system time correctly is also required to make the firewall schedules work properly.

Current time: Displays the current time of the Router.

Mode: You can set the computer clock time manually or choose to synchronize the time via the network or NITZ.

Primary NTP server: Select an NTP server from the drop-down list to sync. The default server is 0.us.pool.ntp.org.

Secondary NTP server: The second NTP server to sync in case the first server does not respond. Select one from the drop-down list. The default server is 1.us.pool.ntp.org.

Time zone: Select the local time zone.

Daylight saving time: Check **Enable** to turn on the daylight saving function.

If you want to configure the time manually, select **Manual** and enter the local time.

10. Update

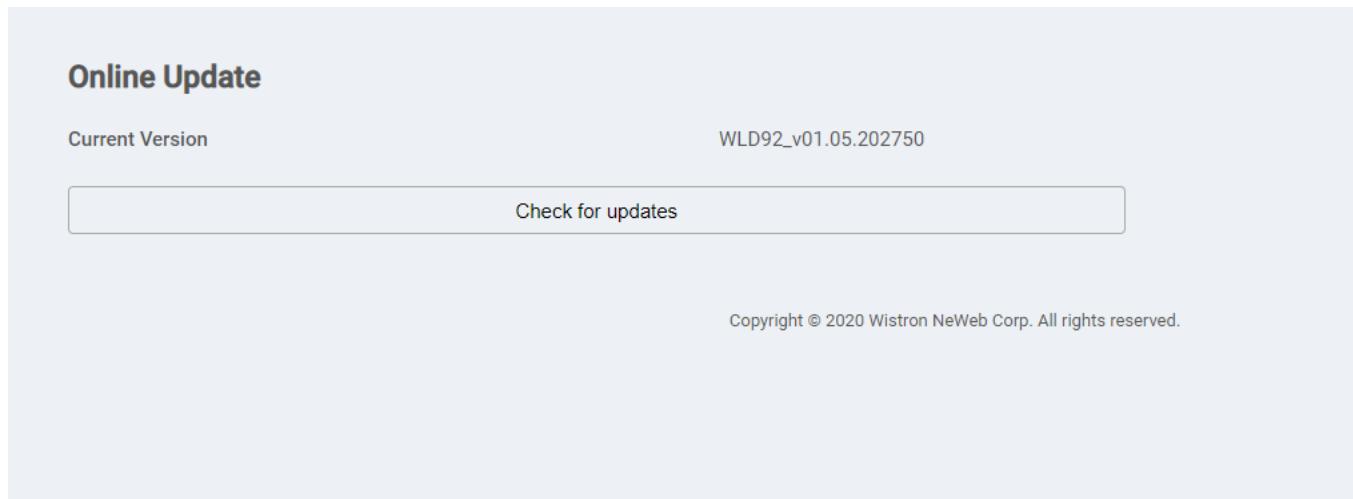
10.1 Local Update

The local update function allows you to select a file locally to perform an update. At the **Select File** field, click **Choose File** and select the update package saved on your computer. Click **Update** to upgrade the firmware.



10.2 Online Update

The online update function enables users to update the firmware of the Router via the Internet. Click **Check for updates** to see if an update is available. If an update is found, the update process will start automatically.



11. Specifications

Hardware and Port Characteristic:

CPU: Qualcomm MDM9240, ARM7 Cortex-A7, 1.2 GHz
Memory: Flash/DDR(4G/2G bits)
Button: Reset/WPS, Power Switch
LED Indication: Power, Internet, 4G Network Mode, 4G Signal, 2.4G/5G Wi-Fi, Ethernet
SIM Card Slot: Push-Push/3FF
Power Adapter: DC 12V/1A
Ethernet Ports: Gigabit LAN × 4 (One for WAN port configuration), Full/Half/Auto

Wi-Fi Features:

DBDC

Antenna: Internal antennas × 2
Chipsets: RTL8192 for 2.4GHz + QCA6174A for 5GHz

Transmission Standard:

802.11 a/b/g/n/ac
DHCP server (up to 32 Wi-Fi clients)
MAC access list/SSID broadcast enable/disable
Multiple SSID/Wireless Protected Setup (WPS)
Security : WPA2-Personal, WPA+WPA2

LTE Features:

Antenna:

Internal antennas × 2
Compliant with 3GPP LTE Release 11

Supported Bands:

NA SKU:

LTE Bands: B2/B4/B5/B12/B66

DL 2CA:

B2 + B2, B2 + B5, B2 + B12
B4 + B4, B4 + B5, B4 + B12
B66 + B5, B66 + B12, B66 + B66

Data Rates:

LTE-FDD: 300 Mbps DL and 50 Mbps UL

LTE WAN:

IPv4/IPv6 dual stack

Ethernet WAN:

Auto/PPPoE/DHCP/static IP

Router Features:

Router/Bridge mode
Port forwarding/Network time Protocol
MAC IP Port filter/URL filter/DoS Protection
UPNP IGD supporting/DNS Relay
L2TP/PPTP/IPSEC VPN pass through
IPv4/IPv6/DMZ/ALG/QoS
Static/Dynamic routing

TR069 Device Management:

TR181, TR104 and TR111 included
Configuration, reporting, provisioning remotely
FOTA via TR069

Applications:

Web UI Configuration
Remote management/ System log location
Parental control
FOTA

Operating Temperature: 0°C–40°C

Operating Humidity: 5%–95% RH

Storage Temperature: -20°C–70°C