# WLD92 Router User Manual

PDF

## **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.	U	UNPACKING INFORMATION	
2.	IN	INTRODUCTION	
2.	.1	SYSTEM LEDS & LED DEFINITIONS	
Ζ.	. Z	BACK PANEL	
3.	IN	INSTALLATION	6
4.	C	CONNECT DEVICES TO THE ROUTER	8
5.	W	WEB USER INTERFACE	11
5.	.1	Accessing the Web User Interface	
5.	.2	Web User Interface Introduction	
6.	н	HOME	
7	١٨		14
/.	~	vvi-ri	
7.	.1	WLAN SETTINGS	
7.	.2	WLAN ADVANCED SETTINGS	
/.	.3		
7.	.4 5	WPS SETTINGS	
/.		CONNECTED DEVICES	
8.	SI	SETTINGS	20
8.	.1	QUICK SETUP	20
8.	.2	DIAL-UP	
8.	.3	ETHERNET	
8.	.4	OPERATING MODE	
8.	.5	DHCP	
8.	.6	DNS	
8.	.7	Security	
8.	.8	PARENTAL CONTROL	45
8.	.9	Routing	
8.	.10	0 STATISTICS	
8.	.11	1 DDNS	
9.	S	SYSTEM	50
9.	.1	DEVICE INFORMATION	50
9.	.2	Modify Password	
9.	.3	DIAGNOSIS	52
9.	.4	Restore Defaults	
9.	.5	Reboot	55
9.	.6	DATE AND TIME	56
10.		UPDATE	57
1(	0.1	1 LOCAL UPDATE	
10	0.2	2 Online Update	
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

0		)
8 9	10	11 12

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	2. Power adapter
3. Notebook, tablet, or smartphone	

#### 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.



1.	Ethernet cable	2.	Computer
	(connect to Ethernet port in wall or other device)		
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.

.

- 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



Descript & 202 Web Same Say of spin-second

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	Click the drop-down list to select a preferred language.
Log-out	
3. Management	Click the icon to access each management function.
Function	
4. Internet Usage	Displays data usage
5. Connection	Provides information including:
Information	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

	WNC	Harrie Wi-H	Settings	and and a second	C. D. Lipstone
WLAN Settings WLAN Advanced Settings WLAN MAC Filter	WLAN Settings				
WPS Settings Connected Devices	Status SSID Security mode Clipher mode Password	Enable: Disable WLD92_2A62 WPA2-PSK AES AES Show Password			
	Broadcast SSID Maximum stations Accep	Enable Disable	) No Cosp. All rights reserve	a.	

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.

<u>None (Open)</u>: This mode allows all Wi-Fi devices to connect to the Router without any security protection. <u>WPA2-PSK</u>: 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.

<u>TKIP+AES</u>: 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.

<u>AES</u>: 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.

# 7.2 WLAN Advanced Settings

Wi-Fi 2:40 Wi-Fi 50	
Channel	Auto 👻
802.11 Mode	Auto bigm 🖌 🛩
Bandwidth	26/401Mrg 🐱
Transmission power	100% 🛩
Fixed Transmission Rate (MC5)	Auto 🗢
Fragmentation Threshold	2347 Dytes
RTS Threshold	2346 bytes
WMM	Enable ① Disable
DTIM Period	3
Guard Interval	Auto 🕒 Long
Preamble type	Cong Preamble 🗍 Short Preamble
Beacon Internal	100

**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:

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

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

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

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

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

## 7.3 WLAN MAC Filter

WiFi246 WiFi60		
MAC filter mode	💭 Enable 💿 Desable	
Policy	🔿 Whitelist 💿 Blacklist	
Add		
MAC address	Name	Optic
Apply	Cancel	

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**:

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

950		
	🔮 Enable 🔘	Disable
	Apply	
vice		
PS association screen		
	vice MP5 association screen	Apply Vice MP5 association screen

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			
W-Fi246	Wi-Fr 50			
IP address		Host name	MAC address	Options
		Copyright 4	2020 Watron NetWeb 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

Quick Setup		APN		
Dial-up	3	Settings		
Ethernet	> APN Config	juration		
Operating mode				
DHCP				Admin
ONS	Authentic ation		There are	
Security	3		intre V	
Parental Control	3 User name			
Bandwidth Management	Password		Show Fassword	
Routing	tP type		(Pv46.Pv6 🗸	
Statistics	IPv6 prefix deleg	ation	🔘 Enetife 🧶 Disatife	
DONS	APN		Laconternet	
				User
				User
	Applied profile		inseriet V	
	Profile Name		Internet	
	Authentication		None 🖌	
	Username			
	Password		Show Patoword	
	IP-type		IPv46/Pv6 👻	
	sPv6 prefix deleg	etion	🔿 Eneble 🧶 Disable	
	APN		Lastcinternet	
		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.

Connection mode:	
LAN Only 👻	
to excitent users a 30 as 40 extends to exceed to the extends	
IN AVAILABLE & JUST OF HIS INFORMATION TO CONSIGN TO THE INFORMATION.	
< Back Next >	

#### 3. WLAN Settings

		WI-FI Settings
WI-FI 2.40 WLD91_3816		
Password:		
WI-F15G WLD91_3816_6G		
Show Password		
< Back	Finish	

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

Quick Setup		Mobile Connection	
Dial-up	>	Mobile connection	Disconnect
Mobile Connection		Data roaming	Crable Olsable
APN Configuration			
Network Settings		Apply	Cancel
Ethernet	>		
Operating mode			
DHCP			
DNS			
Security	2		
Parental Control	>		
Bandwidth Management			
Routing			
Statistics			
DONS			
			Copyright @ 2020 Wistron NeWeb Corp. All righ

**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.

#### APN Configuration

Quick Setup		APN Configuration			
Dial-up					
Mobile Connection					Admin
APN Configuration		Authentication	Nore	v .	
Network Settings		Username			
Ethernet	2				
Operating mode		Password	5h	ow Password	
DHCP		1P type	1714d	urut 🗸	
DNS		IPv6 prefix delegation	() End	atile 🧶 Disotile	
Security	3	APM	value	ternal.	
Parental Control	2				
Bandwidth Management					
Roubing					User
Stubelics		Applied profile	100		
DONS			1		
		Profile Name	ing m	et.	
		Authentication	Norse	~	
		User oame			
		Paraword	() se	ow Paseword	
		IP type	2Py46	ped 🗸	
		IPv6 prefix delegation	Oth	sble 💼 Disable	
		APN	usooin	ternet	
		New Protie	Ann	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).

<u>IPv6</u>: 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).

#### Network Settings

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

Quick Setup Dial-up	5	Band Settings	82 1 84 1 85 1 812 866
Mobile Connection		11250	
APN Configuration		Apply	Cancel
Network Settings		Network Settings	
Ethernet	>	network certaingo	1
Operating mode		Cellular network mode	4G 🛩
DHCP		Network search mode	Auto Manual
DNS		Apply	Cancel
Security	>		
Parental Control	>		
Bandwidth Management			
Routing			
Statistics			
DONS			

#### **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.

# 8.3 Ethernet

#### **Ethernet Settings**

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

Dial-up	>	Connection mode	LAN Only
Ethernet	×		
Ethernet Settings		The system uses a 3G or 4G network to connect to the network.	
Ethernet Status		Apply	
MAC Clone			
Connected Devices			
Operating mode			
HCP			
ONS			
iecurity	×		
Parental Control	2		
Routing			
Statistics			
DDNS			
			Copyright @ 2020 Wistron NeWeb Corp. All rights reserved.

#### <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  $\rightarrow$  Ethernet  $\rightarrow$  Ethernet Settings.

Duration	00:50:00:00
Connection status	Disconnected
MAC Address	00:19:08:91:38:17
Connection mode	LAN Only
P 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
	Refresh

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

#### MAC Clone

Current MAC address	00 19 CB 91 38 17	Rese
Host MAC address	64.48.68.68.68.67	Clone
	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	Heat name	MAC address	
DHCP	192.16E.1.10	T1-1-1-Q-45363	64a95c601da7	

# 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.

<b>Operating mode</b> : Select the desired mode to set up the device as a ro	outer or as a bridge.
--	-----------------------

Quick Setup		Operating mode	
Dial-up	>	Operating mode	Router mode C Bridge mode
Ethernet	>		
Operating mode		Арріу	Cancel
DHOP			
DNS			
Security	>		
Parental Control	>		
Routing			
Statistics			
DDNS			

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

# 8.5 DHCP

#### <u>DHCP</u>

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

Quick Setup		DHCP		
Divi-up	3	IP address	152 168 1 1	
Ethernet	>	Subnet mask	255 - 255 - 255 - 0 -	
Operating mode		DHCP	Enable Disable	
ONS		DHCP range	10 - 20	
Security	>	DHCP lease time(s)	06400	
Parental Control Routing		Apply	Cancel	
Statistics		Static IP		
DDNS		Add		
		IP address	MAC address	Options
		Avery	Cancel	

**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.

Quick Setup		DNS	DNS	DNS
Dial-up	>	DNS Mode	DNS Mode	DNS Mode
Elhernel	>	_		
Operating mode			Apply	Apply
DHCP				
DNS				
Security	>			
Parental Control	>			
Routing				
Statistics				
DONS				

<u>Auto</u>: The device will automatically obtain the DNS server address.

<u>Relay</u>: After selecting this option, enter the primary and secondary DNS addresses of the DNS relay server. <u>Manual</u>: 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.

Juick Setup		Firewall Switch	
)ial-up	>	Enable Firewall	🥥 Enable 🚫 Disable
themet	>	Security level	🔿 High 💿 Medium 🔿 Low
perating mode			
HCP		Disable WAN port ping	👷 Enable 🕖 Disable
INS		Apply	Cancel
Security	>		
Firewall Switch			
LAN IP Filter			
Port Forwarding			
DMZ			
ALG			
UPnP			
NAT Settings			
DoS Attack			
Remote Management			
VPN Pass Through			

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.

<u>High Security</u>: 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).

<u>Medium Security</u>: 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.

<u>Low Security</u>: 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.

#### LAN IP Filter

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

	🗍 Enable 🔵	Disable			
🔘 Whitefair 🛑 Blacklist					
LAN port	WAN IP address	WAN port	Protocul	Status	Options
Apply		Cancel			
	LAN port	LAN port WAN IP address	LAN port WAN IP address WAN port	LAN port WAN IP address WAN port Protocol Cancel	LAN port WAN IP address WAN port Protocol Status

- 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.

Port Forwarding						
Port Forwarding		💭 Enable 🧶 Disable				
Add						
Naime	WAN port	LAN IP address	LAN port	Protocol	Status	Optio
	Apply		Cancel			

- 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 **Protoco**l 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.

#### <u>DMZ</u>

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.

DMZ			
DMZ status	🚫 Enable 🔘 Disable		
DMZ IP address			
Apply	Cancel		

**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.

#### <u>ALG</u>

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.

C facility - Devide
Englie Disable
💭 Enable 🧕 Disable
🔿 Enable 💿 Disable
8060
Cancel

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

#### <u>UPnP</u>

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.

	Enable Disable		
Apply	Cancel		

- 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:

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

<u>Symmetric</u>: 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.

loS Protection	🤵 Enable 🔘 Disable	
IYN Flood	🔵 Enable 🔵 Disable	
	128	packets/sec
CMP Flood	🖲 Enable 🚫 Disable	
	100	packets/sec
Apply	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.

Secured Client IP Address	All IP     Selected (IP/Subnet)
Remote Port Settings	
Http	🔘 Enable 💽 Disable
Http port	8080
Https	💭 Enable 🔮 Disable
Https port	8443
Asoly	Cancel

#### **Remote Management:**

<u>Secured Client IP Address</u>: 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:**

<u>Http</u>: 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 in allowed.

<u>Https</u>: 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 in 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	Enable Disable
PPTP	💿 Enable 🔘 Disable
L2TP	🤵 Enable 💭 Disable
Acoly	Cancel

<u>IPsec</u>: Select **Enable** to allow IPSec pass through.

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

<u>L2TP</u>: 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	Ensble	Dasble		
Default	Normal	*		
Profile of Bandwidth Manage	ment			
	Best effort			High
UE: (Mb/s)	DL: (MIN/N)		10. (99/40	01. (Mb/s)
50	100		м	50
	Medium			Normal
UL: (MIU)	DL: (Mb/s)		UE: (MB/X)	DL: (Mb/s)
10	25		5	10
Bandwidth Management List				
	A12			
MAC address		Profile		Options
		Cancel		

Bandwidth Management: Select Enable to activate bandwidth management.

<u>Default</u>: 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.

Access T	ime Restriction										
Access Time B	esticities		Costler 💼 Disai	R							
Add											
have	SINC address	Max,	Tre.	wei.	7%	PK.	54	245	vtert	End	Options
	A200		Cano	d							

#### 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.

#### Domain Name Filter

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

Acch	Cancel	
Domain Name	Status	Options
A01		
Palicy	💭 Whitelist 🛃 Blacklist	
Domain Name Filter	🔄 Enable 🗹 Disable	
imitation: HTTPS webpages cannot be filtered		
Domain Name Filter		

- 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.

Static Routing		💭 Enstrie 🛢 Disable			
	Add				
Destination Network	IP Subset Mask	Network	Gateway	Status	Options
Ablity		Cancel			
Dynamic Routing					
Dynamic Routing		Enuble Disuble			
Dynamic Routing Protocol					
		Cancel			
- Addr					

#### **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. <u>Dynamic Routing Protocol</u>: Select RIPv1 or RIPv2 as the routing method.

## 8.10 Statistics

ument volume	189.60MB	
urrent duration	01.52.44	
atal volume	189.68MB	
otal duration	01.53-64	
	Clear honory	
Data Plan		
tart Date (1-31)	1	
	1	68
control create breat		

#### **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.

DNS	Enable 🔽 Disable
ervice provider	
lomain name	
iser name	
assword	
Acoly	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.

	WNC			No.	System	() Vieteta
Desce Information	Device Information					
Modify Passivord	(ME)		804227030334683			
Diagnosia	1000		855889000#1030T	77222		
Restore Defaults	textia		466934103057722			
Report	My number		0975438884			
Date & Time	Software version		WLD92, v01 07, 201	1811		
	MPSE		EGONAL ARCEAUTO	45		
	Hardware version		87			
	LAN MAC address		9648143824.FZ			
	IPv4 address		10.142.187.56			
	IPv6 address		2001 5400 e3xill 1e	ht 90e had 400 3743	294	
	Marrid		45-79003342 (87)			
		Reben				
		04	ayagen e söss Wassan Na	etwins Congo Alt register on	ariet.	

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.

current password	
lew password	
Confirm password	
Apply	Cancel
uto logout time	150 seconds
Apply	Cancel

# 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.

Diagnosis	
Diagnosis method	Reg 👻
Target IP or domain	
Packet size	32 1-9000 bytes
Timeout period	4 1-10 seconds
Do not fragment	
404	Cancel
Result	
Result	
Details	

#### <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	
Diagonais method	Trabenute 🛩
Target IP or domain	
Maximum hops	30 1-100
Timesut period	4 2-10 seconds
Apply	Cancel
Result	
Read	
Details	

# 9.4 Restore Defaults

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

Restore	

# 9.5 Reboot

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

Reboot	
NEDOOL	

Click the button below to restart the device.

Reboot

# 9.6 Date and Time

Date & Time When the wireless gateway is powered off, the date and time setting	a are out saves. Select "Sysc from network" or "Sysc from NIT2" to keep the date and tone current.	
Current libe	01.02.29, 01/01/1970	
Mode	📄 Manual 🗮 Sync from natworki 🔅 Sync from NITZ :	
Primary NTP server	Baxpoormpany 👻	
Secondary NTP server	Tus politip arg 🛛 🛩	
Time pone	IGANT-RE COLEMBARY, Talant	1
Daylight saving time	C Enable	
Auto	Cancel	
	Copyright & 2028 Westron Newvell, Copy, All Highla 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.

WNC	ŵ	(in a second sec	*		Update		
Local Update Do not doar the browser or angleg the device when the	uplate is it poper	During the update, the	network convertion m	ay experience tempora	y interceptions. This is normal	The device will extract allo	r The opticity is complete
Current Version	. 16	D92,x01.05.252750					
Select File	1	RUX +ESteam					
	Update						
		eyidir. B. 2020 Michael Na	ning Cog. Al right rear-	et. ;			

# 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.

Online Update	
urrent Version	WLD92_v01.05.202750
	Check for updates
	Consticht @ 2020 Wiston NaWah Com

#### 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, Router/Bridge 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 Standard: 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:** 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