movistar

WLD71-T3 LTE Router
User Manual

Safety Precautions

Please read this user’s manual before operating this product. The information contained in this document is subject to change without notice. Features or specifications may be different depending on the type of product model purchased.

Safe Use of This Product

Carefully follow the warnings and safety notices presented within this manual. Please pay special attention to the following indications of potentially hazardous situations:

Warning: ⚠

Indicates a hazardous situation, which, if not avoided, could result in serious injury.

Caution: ⚠

Indicates a situation, which, if not avoided, could damage this product or other devices.

Note: ⚠

Indicates additional user information to make the user aware of possible problems and to help the user understand, use and maintain the product.

- This product needs only an occasional wipe with a dry cloth.
- Avoid high moisture conditions and keep away from liquids and humidity.
- Do not install or use the product where it is exposed to direct sunlight or heat.

- Care must be taken when using the device in close proximity to personal medical devices, such as pacemakers and hearing aids.
- Do not use this product in environments with a potential explosion hazard.
- The product must be placed horizontally on a hard flat surface. Do not place the product where it may be subject to physical shock or vibration or where the product may drop, topple, slide or shake, which may cause personal injury or damage to the product.
- If lightning is expected, or the product is not going to be used for a long period of time, unplug the power cord from the unit.
- The use of electronic transmitting devices in aircraft, hospitals and petrol stations is forbidden. Please follow the rules and warnings in these conditions.
- The product must ONLY be used with the power supply cord and power adapter supplied by the manufacturer.
- Openings on the housing of the product are required for ventilation. Do not block or obstruct the airflow through these openings.
- Do not operate the product on a soft surface such as a carpet, rug, bed, etc.

FEDERAL COMMUNICATIONS 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 radiates radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

RF Exposure Warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

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

This radio device has been tested to operate with the WWAN external antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna type: Dipole
Antenna peak Gain (dBi)
2.78 dBi (max.) @ 698 MHz to 960 MHz
2.16 dBi (max.) @ 1710 MHz to 2170 MHz
2.77 dBi (max.) @ 2300 MHz to 2690 MHz

Table of Contents

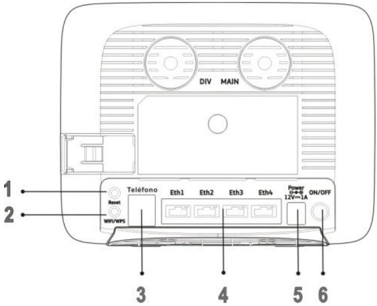
1. Unpacking Information

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

- WLD71-T3 LTE Router × 1
- Power Adaptor: AC 90 V–264 V (47 Hz–63 Hz) input, DC 12 V output (1 A) × 1
- Ethernet Cable × 1
- Telephone Cable × 1
- Quick Start Guide × 1
- Warranty Card × 1

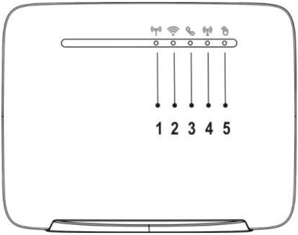
2. Introduction

2.1 Rear Panel

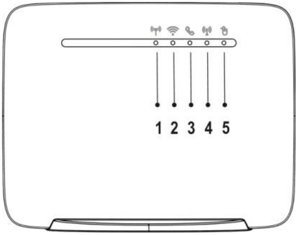


1.	**Reset**	**Reset the Router by pressing this button.** ⓘ **Resetting the router defaults will erase all previous settings.**
2.	**Wi-Fi/WPS**	Connect to other WPS-compatible devices by pressing this button. Wi-Fi function is turned on/off by a long press (for 5 seconds). WPS association window is activated by a short press (less than 3 seconds).
3.	**Phone**	Allows connection to the telephone line.
4.	**Ethernet ports 1–4**	Connect to your devices such as a PC and laptop. ⓘ Eth1 also functions as a WAN port for connecting to a DSL or cable modem.
5.	**12 V**	Connect to the power adapter
6.	**ON/OFF**	Press to turn the power on or off.

2.2 LED Definitions



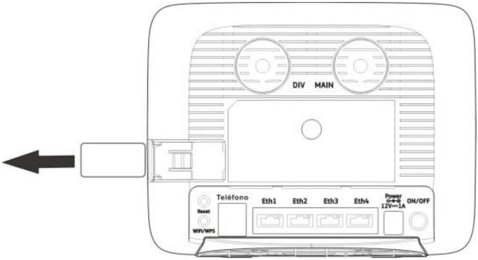
1.	4G/3G/2G Network	**Cyan: Connected to 4G network** Blue: Connected to 3G network Green: Connected to 2G network Blinking red (2 times per second): Connection failure Red: Failure during POST (power-on self-test), or error due to hardware or firmware problems
2.	Signal Strength	Blue: Good coverage Green: Minimum coverage Blinking red: No signal
3.	Telephone	Blue: Off-hook Off: On-hook



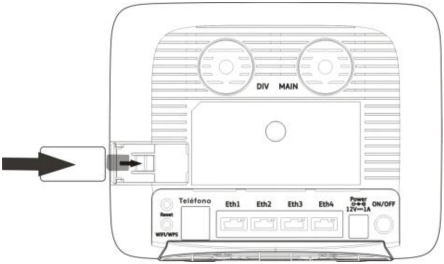
4.	**Wi-Fi/WPS**	Blue: Wi-Fi enabled Blinking blue: A WPS connection is being established. Off: Wi-Fi function off
5.	**Internet**	Blue: Internet connection in progress Off: No internet connection

3. Installation

1. Open the SIM card slot cover.



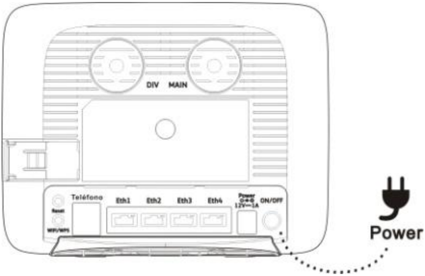
2. Insert a SIM card into the SIM card slot
3. Slide the cover back over the SIM card slot.



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

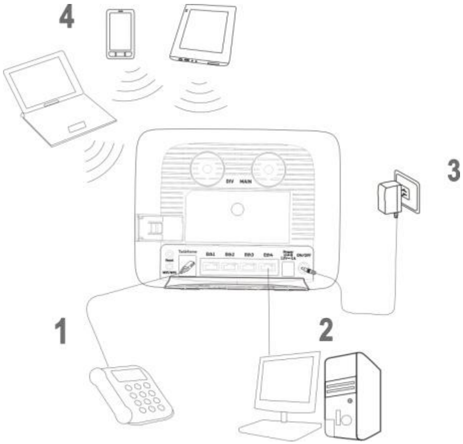
   Note: Always use the adapter that comes with the Router for the power supply.

5. Turn on the power switch of the Router.



4. Connect devices to the Router

Scenario 1: Access the Internet through an LTE, 3G, or 2G network

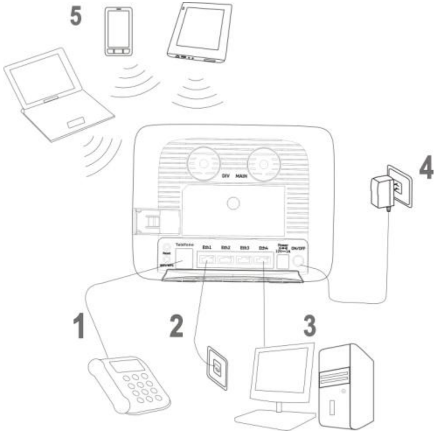


1	Telephone	2	Computer
3	Power adapter	4	Notebook, tablet, or smartphone

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 through another device

You can use the router to access the internet through other access you have at home, such as FTTH or xDSL. To do this, the Eth1 port also functions as a WAN port when connecting to another computer or external socket that provides an Internet connection.



1	Telephone	2	Ethernet wall outlet	3	Computer
4	Power adapter	5	Notebook, tablet, or smartphone		

Scenario 3: Wi-Fi connection

If you want to connect a computer or device wirelessly, make sure the Wi-Fi indicator is lit in blue without blinking, this means that the router's Wi-Fi function is enabled.

To establish the Wi-Fi connection, you can do it manually or automatically via WPS.

Set up a Wi-Fi connection manually

1. Locate the label on the back of the computer that displays all the data needed to connect to the wireless network pre-configured on your computer.
2. Search for wireless networks on your computer or Wi-Fi device.
3. Connect to the network with the same name that appears on the device label.
4. When the password is requested, enter the Wi-Fi key that is on the same label. (Wi-Fi key is case-sensitive). The customer will notify you when you are connected.

ℹ To prevent unauthorized users from accessing your Wi-Fi network, it is recommended that you periodically change your SSID and Wi-Fi password. For detailed information, see the web administration page help.

Establish a Wi-Fi connection automatically using WPS:

If the client supports WPS, it is possible to configure a WPS connection as follows:

1. Ensure that the Wi-Fi feature is enabled on the client.
2. Press and hold the WPS button for 3 seconds. The indicator starts blinking.
3. Activate the WPS connection on the computer or Wi-Fi device within a period of 2 minutes.

ⓘ For instructions on how to enable the WPS connection on your computer or Wi-Fi device, refer to the Wi-Fi user's guide.

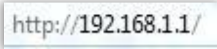
5. Web User Interface

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.

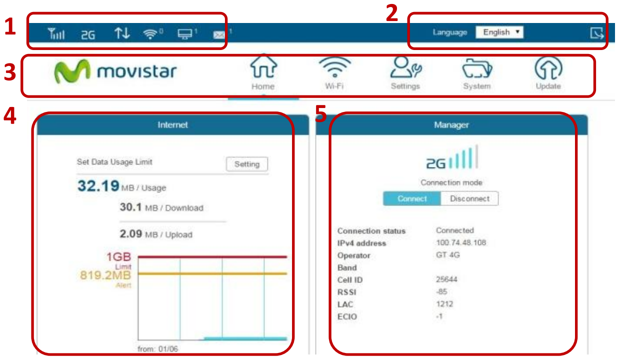


http://192.168.1.1/

3. An authentication screen will appear. Use the default username and password printed on the label on the housing of the Router.
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



Set Data Usage Limit

32.19 MB / Usage

30.1 MB / Download

2.09 MB / Upload

from: 01/06

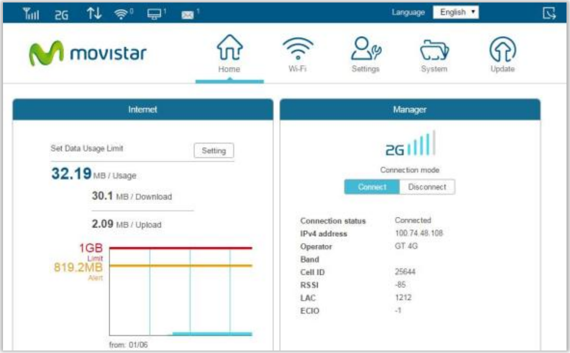
Connection mode

Connection status	Connected
IPv4 address	100.74.48.108
Operator	GT 4G
Band	
Cell ID	25644
RSSI	-85
LAC	1212
ECIO	-1

1.	**Basic Information**	**Provides information including: Signal strength of the connected mobile network, connection mode, Wi-Fi connection status, number of connected devices, and unread SMS.**
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**	Display of data usage
5.	**Connection Information**	Provides information including: Name of the mobile network service provider, connection mode, cell ID, and signal strength indicators

6. Home

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



Set Data Usage Limit

32.19 MB / Usage

30.1 MB / Download

2.09 MB / Upload

2G

Connection mode

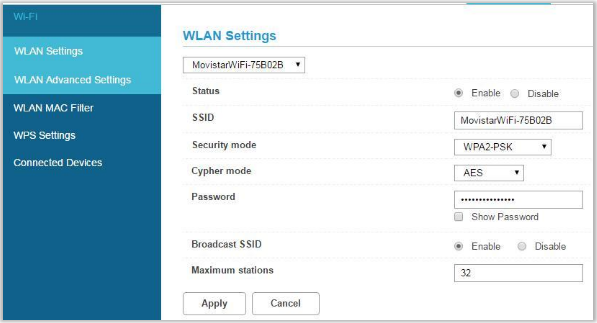
Connection status	Connected
IPv4 address	100.74.48.108
Operator	GT 4G
Band	
Cell ID	25644
RSSI	-85
LAC	1212
ECIO	-1

Internet:
Indicates Internet data usage, including total data usage (download/upload); click **Setting** to view the data plan.

Manager:
Displays the connection mode, connection status, IPv4 address, operator, Band, cell ID, RSSI, LAC, and ECIO

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.



MovistarWiFi-75B02B ▼

Status ● Enable ○ Disable

SSID MovistarWiFi-75B02B

Security mode WPA2-PSK ▼

Cypher mode AES ▼

Password ••••••••••••••••

□ Show Password

Broadcast SSID ● Enable ○ Disable

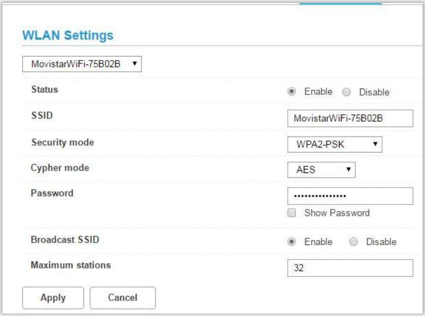
Maximum stations 32

Select the Wi-Fi profile for which you wish to change security settings.

Note:

- The Wi-Fi profile supports establishment of four local wireless networks with different SSIDs. Each profile has its own security mode.

7.1 WLAN Settings



WLAN Settings

MovistarWiFi-75B02B ▾

Status ● Enable ○ Disable

SSID MovistarWiFi-75B02B

Security mode WPA2-PSK ▾

Cypher mode AES ▾

Password •••••••••••••••

□ Show Password

Broadcast SSID ● Enable ○ Disable

Maximum stations 32

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.

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

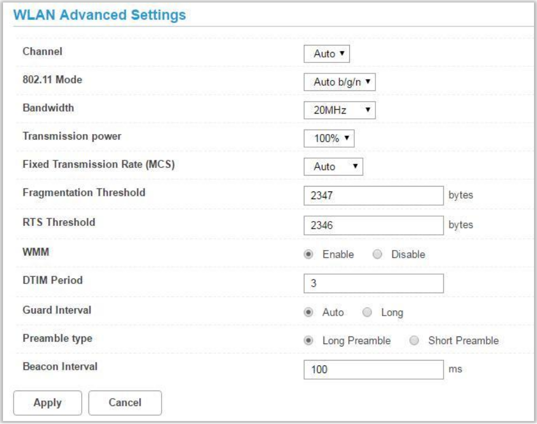
Cipher mode: Select one cipher mode from the drop-down menu.

<u>TKIP+AES</u>: This is what the encryption standards are for WEP2 (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



WLAN Advanced Settings

Channel	Auto ▾
802.11 Mode	Auto b/g/n ▾
Bandwidth	20MHz ▾
Transmission power	100% ▾
Fixed Transmission Rate (MCS)	Auto ▾
Fragmentation Threshold	2347 bytes
RTS Threshold	2346 bytes
WMM	● Enable ○ Disable
DTIM Period	3
Guard Interval	● Auto ○ Long
Preamble type	● Long Preamble ○ Short Preamble
Beacon Interval	100 ms

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:

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.

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 WLD71. 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.

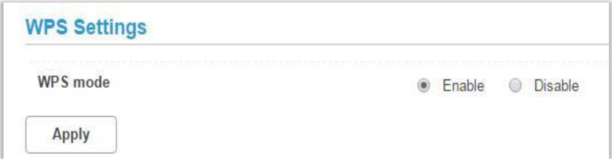
7.3 WLAN MAC Filter

For detailed instructions on the WLAN MAC Filter, please refer to section 8.4.

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.

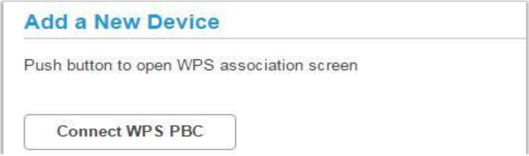
<WPS Settings>


WPS Settings

WPS mode ● Enable ○ Disable

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

<Add a New Device>


Add a New Device

Push button to open WPS association screen

WPS method:

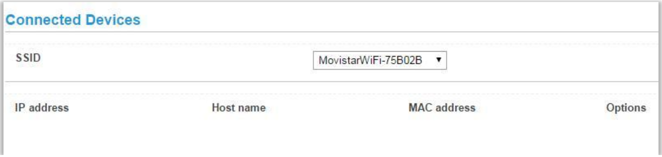
Connect WPS PBC (Push-button configuration**):**

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. Select one SSID from the drop-down menu to see the information of the devices that are connected via Wi-Fi.

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.



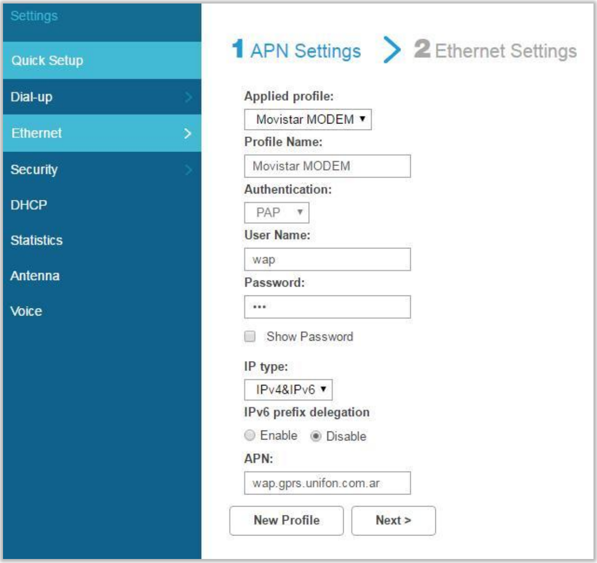
Connected Devices

SSID: MovistarWiFi-75B02B ▼

IP address	Host name	MAC address	Options

8. Settings

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



Applied profile: Movistar MODEM ▾

Profile Name: Movistar MODEM

Authentication: PAP ▾

User Name: wap

Password: •••

□ Show Password

IP type: IPv4&IPv6 ▾

IPv6 prefix delegation

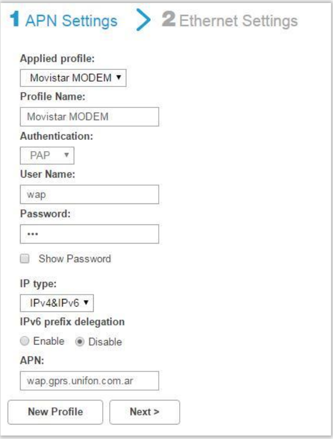
○ Enable ● Disable

APN: wap.gprs.unifon.com.ar

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 > 2 Ethernet Settings



Applied profile: Movistar MODEM

Profile Name: Movistar MODEM

Authentication: PAP

User Name: wap

Password: •••

□ Show Password

IP type: IPv4&IPv6

IPv6 prefix delegation

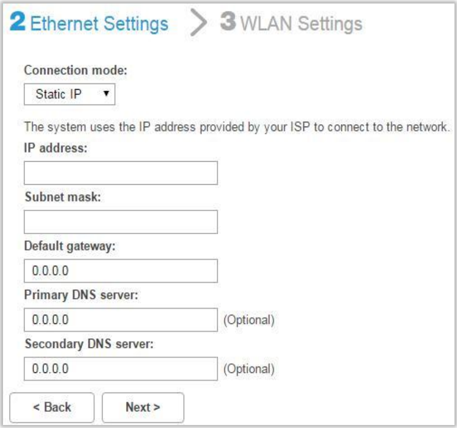
○ Enable ● Disable

APN: wap.gprs.unifon.com.ar

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

2 Ethernet Settings > 3 WLAN Settings

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



Connection mode: Static IP ▾

The system uses the IP address provided by your ISP to connect to the network.

IP address:

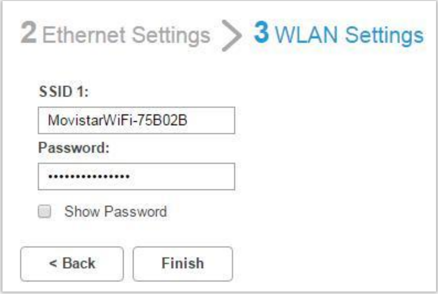
Subnet mask:

Default gateway: 0.0.0.0

Primary DNS server: 0.0.0.0 (Optional)

Secondary DNS server: 0.0.0.0 (Optional)

2 Ethernet Settings > ***3 WLAN Settings***



2 Ethernet Settings > 3 WLAN Settings

SSID 1:

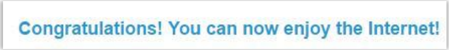
MovistarWiFi-75B02B

Password:

•••••••••••••••

Specify a name and password for your wireless network, then click **Finish**.

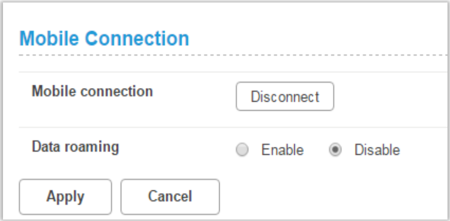
The statements below indicate that all the necessary settings have been performed:



Congratulations! You can now enjoy the Internet!

8.2 Dial-up

Mobile Connection



Mobile Connection

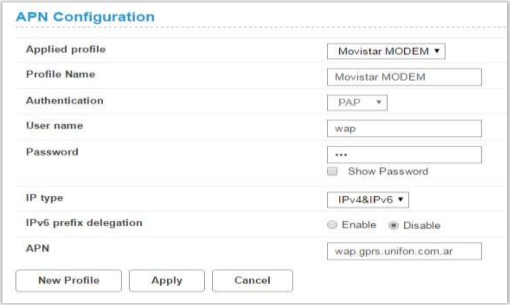
Mobile connection: Disconnect

Data roaming: ○ Enable ● Disable

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

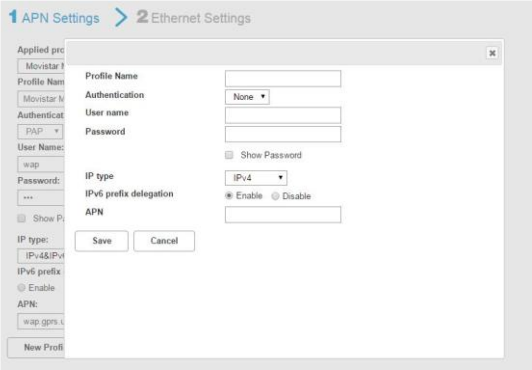


APN Configuration

Applied profile	Movistar MODEM ▾
Profile Name	Movistar MODEM
Authentication	PAP ▾
User name	wap
Password	••• □ Show Password
IP type	IPv4&IPv6 ▾
IPv6 prefix delegation	○ Enable ● Disable
APN	wap.gprs.unifon.com.ar

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.
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).
After the settings are completed, click **Apply**.

To create a new profile, click **New Profile**. The following window will then appear:

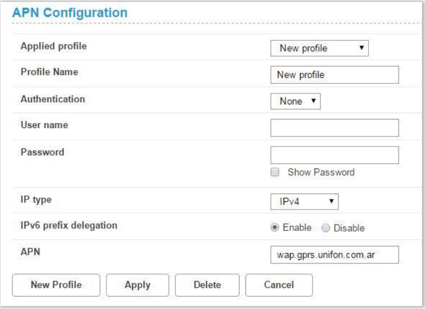


Profile Name	
Authentication	None ▾
User name	
Password	
	□ Show Password
IP type	IPv4 ▾
IPv6 prefix delegation	● Enable ○ Disable
APN	

After you enter the related information, click **Save**.

If you want to delete a particular profile, select the profile you want to delete and then click **Delete**.

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



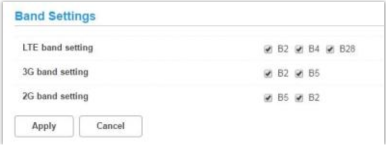
APN Configuration

Applied profile	New profile ▾
Profile Name	New profile
Authentication	None ▾
User name	
Password	 □ Show Password
IP type	IPv4 ▾
IPv6 prefix delegation	● Enable ○ Disable
APN	wap.gprs.unifon.com.ar

Network Settings

<Band Settings>

The section enables you to perform settings for the LTE band, 3G band, and 2G band. Select the appropriate check boxes and click **Apply** to save the changes. Click **Cancel** to discard any changes you made.



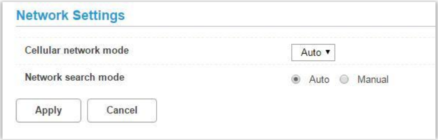
Band Settings

LTE band setting ☑ B2 ☑ B4 ☑ B28

3G band setting ☑ B2 ☑ B5

2G band setting ☑ B5 ☑ B2

<Network Settings>



Network Settings

Cellular network mode Auto ▾

Network search mode ● Auto ○ Manual

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.

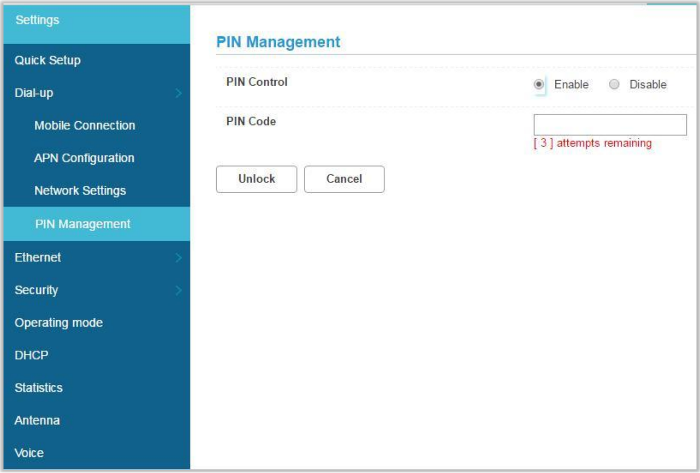
Click **Apply** to save your changes, or click **Cancel** to discard any changes you made.

PIN Management

PIN Control: Select **Enable** to enable PIN protection.
Select **Disable** to disable PIN protection.
PIN Code: Enter your PIN code here, then click **Unlock**.

After you enter the PIN code, click Unlock, or click **Cancel** to undo the changes.

Note: PIN can only be set when PIN control is enabled. When you select **Disable** PIN control, you will not see the **Change PIN Code** option.



PIN Management

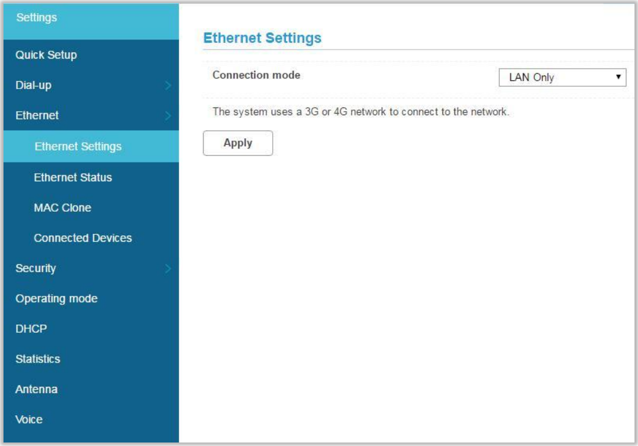
PIN Control ● Enable ○ Disable

PIN Code

[3] attempts remaining

8.3 Ethernet

Ethernet Settings



Ethernet Settings

Connection mode: LAN Only

The system uses a 3G or 4G network to connect to the network.

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. Set **Point-to-Point Protocol over Ethernet (PPPoE)** and the **Dynamic IP** parameters.
3. 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 *1480*. Please do not edit the number unless absolutely necessary.
4. 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 *1480*. 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**, and **DNS address** (optional) provided by your network service provider.
3. Set the **MTU**. The default MTU size is *1480*. Please do not edit the number unless absolutely necessary.
4. Click A**pply** to save your changes.

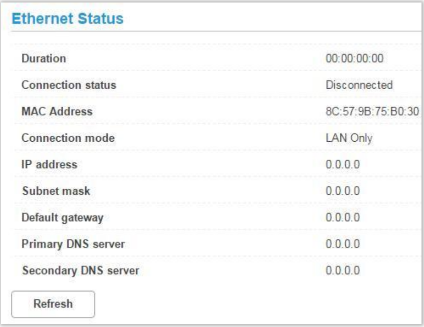
<LAN Only>

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**.



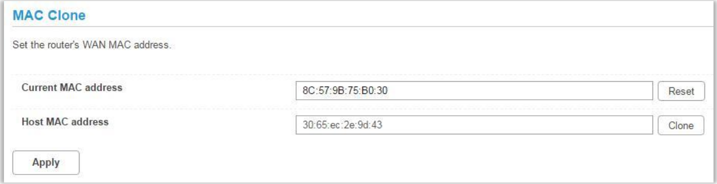
Ethernet Status

Duration	00:00:00:00
Connection status	Disconnected
MAC Address	8C:57:9B:75:B0:30
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

MAC Clone

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.



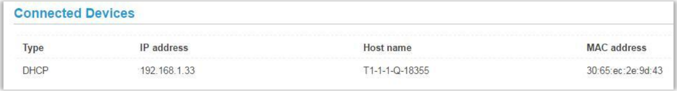
MAC Clone

Set the router's WAN MAC address.

Current MAC address	8C:57:9B:75:B0:30
Host MAC address	30:65:ec:2e:9d:43

Connected Devices

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



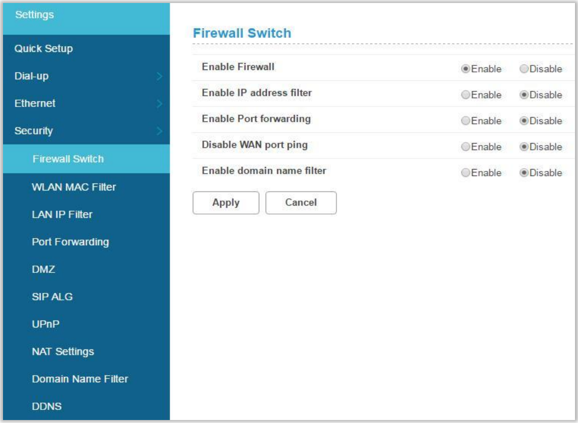
Connected Devices

Type	IP address	Host name	MAC address
DHCP	192.168.1.33	T1-1-1-Q-18355	30:65:ec:2e:9d:43

8.4 Security

Firewall Switch

A firewall is used to prevent traffic from entering and/or leaving the areas of your network.



Firewall Switch

Enable Firewall ● Enable ○ Disable

Enable IP address filter ○ Enable ● Disable

Enable Port forwarding ○ Enable ● Disable

Disable WAN port ping ○ Enable ● Disable

Enable domain name filter ○ Enable ● Disable

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

Enable IP address filter: To limit the Internet access on some specified computers through the router, enable the IP Address Filter.

Enable Port forwarding: Port Forwarding can be used to translate the common service port to a custom port inside your local network such as web or FTP.

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.

Enable domain name filter: Domain name filter can be used to block computers from accessing certain websites through the router.

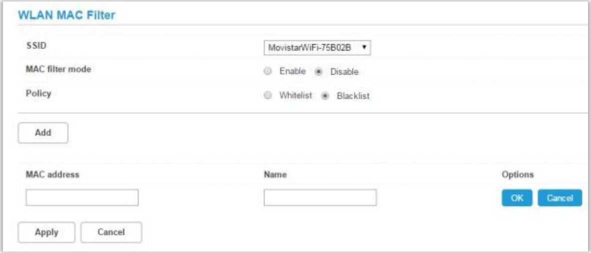
Click **Apply** to activate your settings, or click **Cancel** to discard any changes you made.

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).

1. Select the device **SSID** and 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. Then click **OK** and **Apply**. Click **Cancel** to discard any changes you made.



WLAN MAC Filter

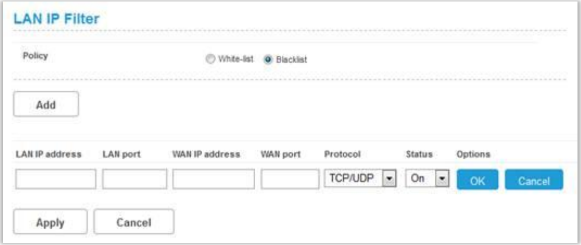
SSID MovistarWiFi-75B02B

MAC filter mode ○ Enable ● Disable

Policy ○ Whitelist ● Blacklist

LAN IP Filter

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



LAN IP Filter

Policy ○ White-list ● Blacklist

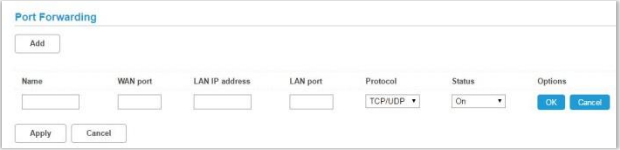
LAN IP address	LAN port	WAN IP address	WAN port	Protocol	Status	Options
				TCP/UDP	On	

1. In the **Policy** field, select **Whitelist** or **Blacklist** if you would like to allow or ban connections, respectively, of a certain device.
2. Click **Add** and type the IP address of the device in the **LAN IP address** field.
3. Type the value range of the LAN port in the **LAN port** field.
4. Type the IP address of the device in the **WAN IP address** field.
5. Type the value range of the WAN port in the **WAN port** field.
6. At the **Protocol** drop-down list, select a protocol. The service uses the following layer-4 protocols: TCP/UDP, TCP, UDP, and ICMP.
7. At the **Status** drop-down list, select **On** or **Off** as the status of the service.

8. At **Options**, click **OK** to complete entry of the information. Click **Cancel** to undo the changes.
9. 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.



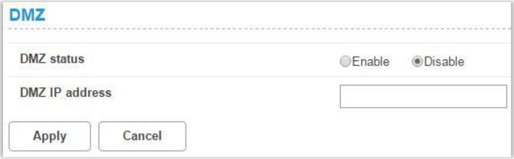
Name	WAN port	LAN IP address	LAN port	Protocol	Status	Options
				TCP/UDP ▾	On ▾	OK Cancel

Name: The name of the service for which the port forwarding rule has been created
WAN port: Type the value range of the WAN port.
LAN IP address: The IP address of the computer on the local network to which the traffic will be forwarded
LAN port: Type the value range of the LAN port.
Protocol: The layer-4 protocol that the service uses. This can be TCP, UDP, or both. If you are unsure, select the **TCP/UDP** option.
Status: Select **On** or **Off** as the status of the service.

1. To add a port forwarding rule, click **Add**.
2. Enter the relevant information for which the port forwarding rule has been created.
3. Select the protocol it uses from the Protocol drop-down list, then select **On** or **Off**.
4. 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.



DMZ

DMZ status ○ Enable ● Disable

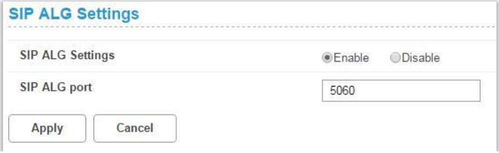
DMZ IP address

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.

SIP ALG

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 SIP ALG, enable the **SIP ALG Settings** function.



SIP ALG Settings

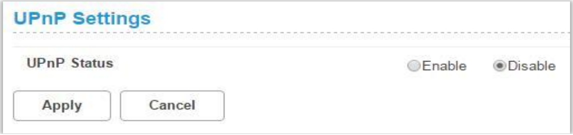
SIP ALG Settings ● Enable ○ Disable

SIP ALG port 5060

1. Select **Enable** to enable the 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.



UPnP Settings

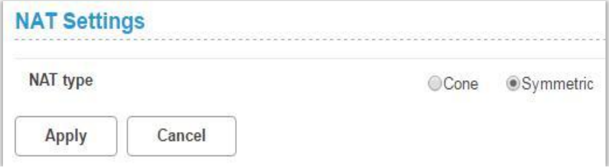
UPnP Status ○ Enable ● Disable

1. At the **UPnP Status**, select **Enable** to enable the UPnP port mapping function.
2. Click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.

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 Settings

NAT type ○Cone ●Symmetric

NAT Type:

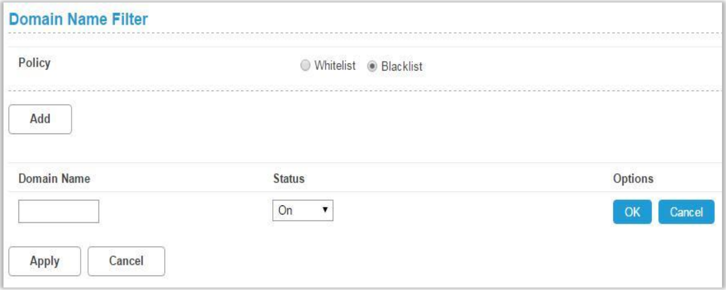
Cone: Based on a cone NAT type, the port is permanently open and allows inbound connections from any external host.

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**, and then click **Apply**. Click **Cancel** to undo the settings.

Domain Name Filter

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



Domain Name Filter

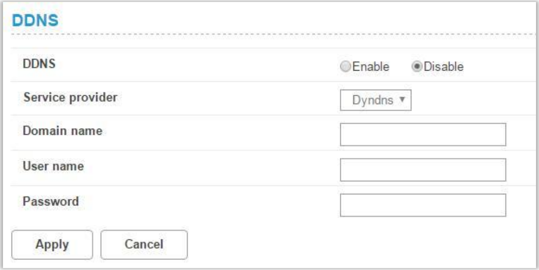
Policy ○ Whitelist ● Blacklist

Domain Name | Status: On | Options

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

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, Username, and Password on this page.



DDNS

DDNS	○ Enable ● Disable
Service provider	Dyndns ▾
Domain name	
User name	
Password	

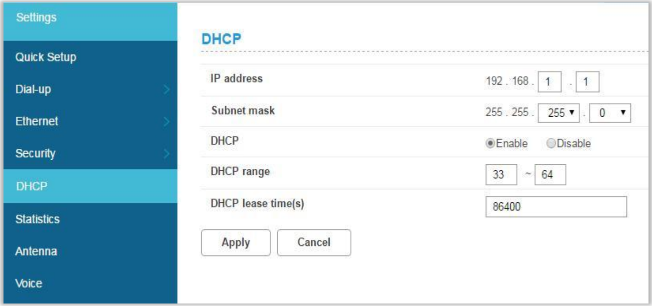
Service provider: Select the DNS service that you are subscribed to.
Domain name: Enter the domain name of the DDNS account.
User name: Enter the username of the DDNS account. This will be provided by the DDNS service provider.
Password: Enter the password for the DDNS account.

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

8.5 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.
Click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.



DHCP

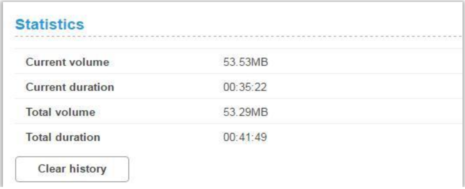
IP address 192 . 168 . 1 . 1
Subnet mask 255 . 255 . 255 ▾ . 0 ▾
DHCP ● Enable ○ Disable
DHCP range 33 ~ 64
DHCP lease time(s) 86400

8.6 Statistics

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**.

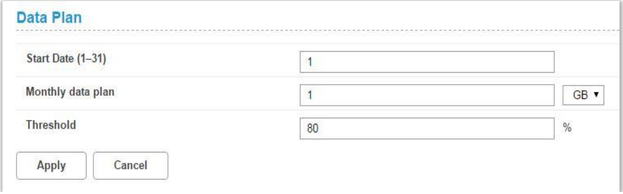


Statistics

Current volume	53.53MB
Current duration	00:35:22
Total volume	53.29MB
Total duration	00:41:49

Data Plan

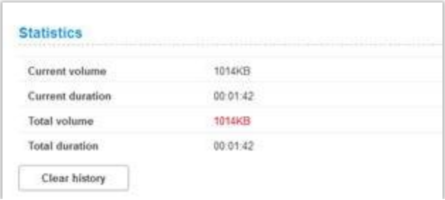
You can set the monthly traffic statistics and view the network traffic of the month. Set the monthly traffic statistics parameters and click **Apply** to apply the settings. Click **Cancel** to discard any changes you made.



Data Plan

Start Date (1–31)	1	
Monthly data plan	1	GB ▾
Threshold	80	%

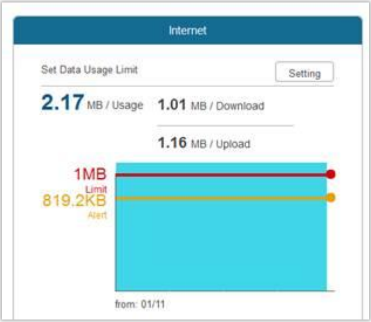
Note: When your data usage exceeds the defined threshold, the total volume will be highlighted in red text.



Statistics

Current volume	1014KB
Current duration	00:01:42
Total volume	1014KB
Total duration	00:01:42

Meanwhile, the blue area that indicates current data usage will exceed the defined threshold indicated by a red line.



Internet

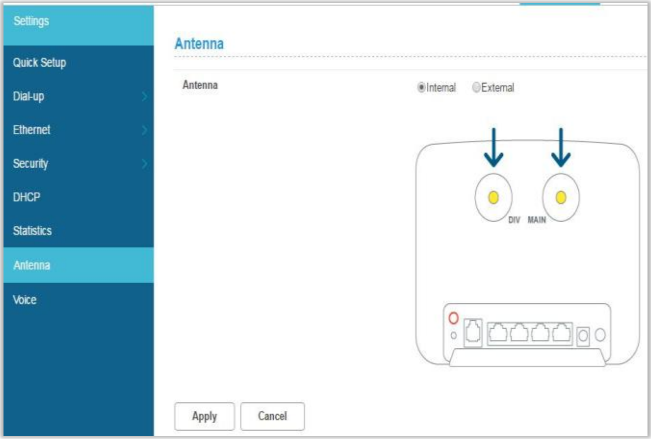
Set Data Usage Limit

2.17 MB / Usage 1.01 MB / Download

1.16 MB / Upload

8.7 Antenna

Antenna: Select **Internal** if you are using an internal antenna with this Router, or select **External** if you are using the Router’s external antenna. Click **Apply** to apply the settings, or click **Cancel** to discard any changes you made.



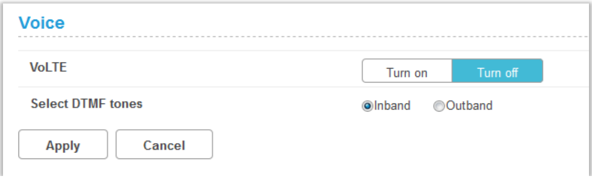
Antenna

Antenna ● Internal ○ External

8.8 Voice

In this section, users can perform settings of voice-related communication features. Supplementary services are also available to enhance telephone services.

DTMF (Dual Tone Multi-Frequency) tones are used during a call to signal to a far-end device; these signals may be for navigating a menu system, entering data, or for other types of manipulation.



Voice

VoLTE: Turn on [✓ Turn off]

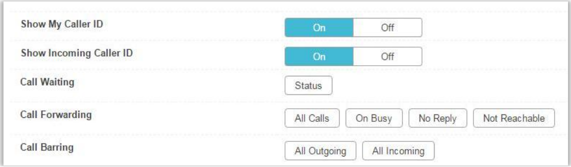
Select DTMF tones: ● Inband ○ Outband

VoLTE: Select **Turn on** to activate VoLTE on the router. Select **Turn off** to use CSFB (Circuit-Switched Fallback).

For the **Select DTMF tones,** select **Inband** or **Outband**. It is recommended that you do not change the default settings.

Users can perform settings on features such as displaying caller ID, call waiting, call forwarding, call barring, and conference calling. Management functions such as activation, deactivation, and simple settings are provided.

When the settings are saved successfully, you will hear the dial tone. If the settings are not successful, you will get a busy tone.



Show My Caller ID [✓ On] Off

Show Incoming Caller ID [✓ On] Off

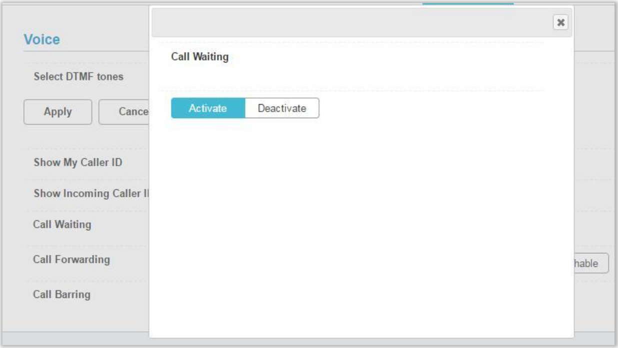
Call Waiting

Call Forwarding

Call Barring

Show My Caller ID: This feature enables you to choose whether to show your own number to the called party's equipment. Click **On** or **Off** to turn on or turn off the function.
Show Incoming Caller ID: The feature allows the calling party to receive a connected party's phone number. Click **On** or **Off** to turn on or turn off the function.

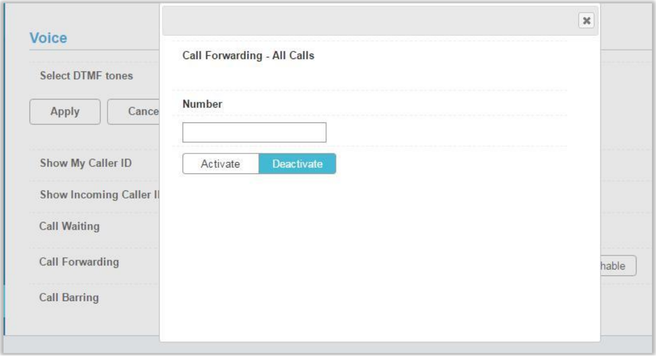
Call Waiting: The call waiting feature allows the user to suspend a phone call that is already ongoing to answer another incoming call. Click **Status** and select **Activate** or **Deactivate** to turn on or turn off the function.



Call Forwarding: The call forwarding feature enables a user to divert incoming calls to the number specified by the user:

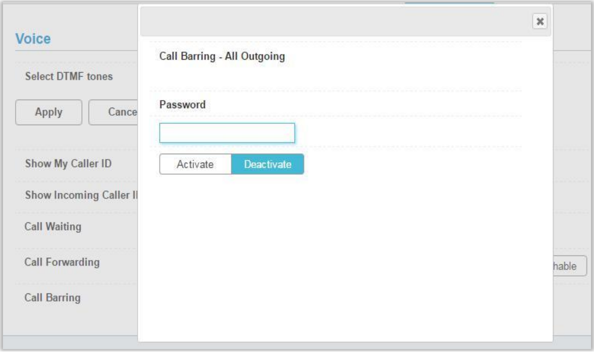
All Calls: All incoming calls will be forwarded to the designated phone number.
On Busy: If the line is busy, incoming calls will be forwarded to the designated phone number.
No Reply: When there is no answer, incoming calls will be forwarded to the designated phone number.
Not Reachable: If you are not in a coverage area of your service provider, incoming calls will be forwarded to the designated phone number.

1. Click on the type of call forwarding you want. A window will appear for you to enter the specified number to which incoming calls will be forwarded.
2. After you enter the number, click **Activate**. To deactivate the feature, click **Deactivate**.



Call Barring: The call barring feature allows the user to bar incoming or outgoing calls.

<u>All Outgoing</u>: All outgoing calls will be barred. Users who activate the feature will not be able to make phone calls.



<u>All Incoming</u>: All incoming calls will be barred. Users who activate the feature will not receive any phone calls.

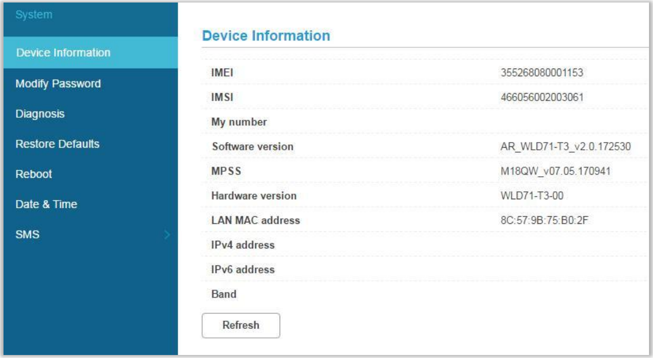
1. Click on the type of call barring you want. A window will appear for you to enter the password to enable the feature.
2. After you enter the password, click **Activate**. To deactivate the feature, click **Deactivate**.

Note: Please ask your operator for the password to enable or disable the feature.

9. System

9.1 Device Information

This page displays relevant information of the Router including: IMEI, 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

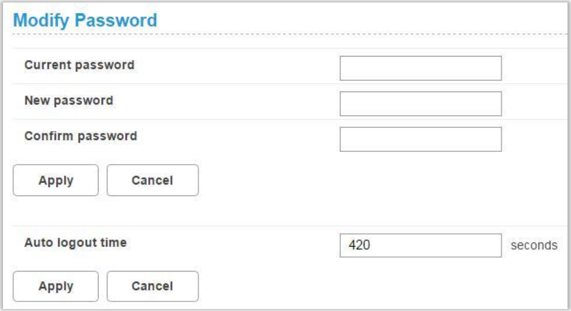
IMEI	355268080001153
IMSI	466056002003061
My number	
Software version	AR_WLD71-T3_v2.0.172530
MPSS	M18QW_v07.05.170941
Hardware version	WLD71-T3-00
LAN MAC address	8C:57:9B:75:B0:2F
IPv4 address	
IPv6 address	
Band	

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 in the **Current password** field. 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, or click **Cancel** to discard any changes you made.
The default auto logout time is 420 seconds. To adjust the login time-out on the Web UI, input a time range between 30 seconds–600 seconds at the **Auto logout time** field. Click **Apply** to set your preferences, or click **Cancel** to discard any changes you made.



Auto logout time: 420 seconds

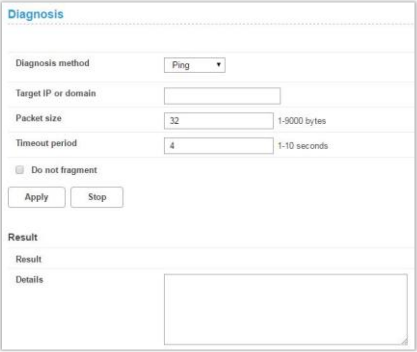
9.3 Diagnosis

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. Clear **Do not fragment** if you set **Packet size** to a value greater than its default value.
6. Click **Apply**. The diagnostics results will then be displayed in the **Result** area at the bottom of the page.



Diagnosis

Diagnosis method: Ping ▾

Target IP or domain:

Packet size: 32 1-9000 bytes

Timeout period: 4 1-10 seconds

□ Do not fragment

Result

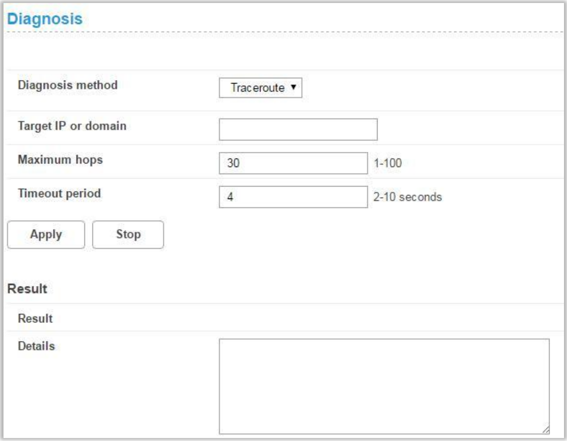
Result

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.



Diagnosis

Diagnosis method	Traceroute ▾	
Target IP or domain		
Maximum hops	30	1-100
Timeout period	4	2-10 seconds

Result

Result

Details

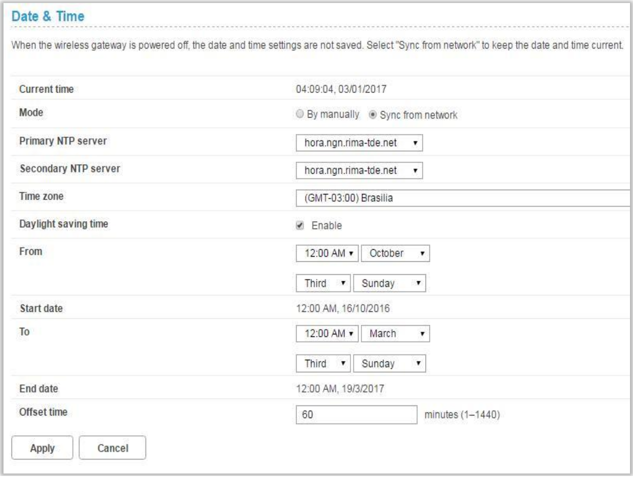
9.4 Restore Defaults

Restore the configuration to factory settings by clicking **Restore**.

9.5 Reboot

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

9.6Date and Time



Date & Time

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

Current time	04:09:04, 03/01/2017
Mode	○ By manually ● Sync from network
Primary NTP server	hora.ngn.rima-tde.net
Secondary NTP server	hora.ngn.rima-tde.net
Time zone	(GMT-03:00) Brasilia
Daylight saving time	☑ Enable
From	12:00 AM October Third Sunday
Start date	12:00 AM, 16/10/2016
To	12:00 AM March Third Sunday
End date	12:00 AM, 19/3/2017
Offset time	60 minutes (1–1440)

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.

Current time: Displays the current time of the Router.
Mode: You can set the computer clock time manually or choose to synchronize the time automatically.

Primary NTP server: Select an NTP server from the drop-down list to sync.
Secondary NTP server: The second NTP server to sync in case the first server does not respond. Select one from the drop-down list.
Time zone: Select the local time zone.
Daylight saving time: Check **Enable** to turn on the daylight saving function.
From: Select from the drop-down lists the time, month, ordinal and day of the week for the start of the daylight saving function.
Start date: Enter the start date on which you wish the synchronization to start.
To: Select from the drop-down lists the time, month, ordinal, and day of the week for the date on which you want the synchronization to end.
End date: Indicates the date on which the synchronization will end.
Offset time: Specify a value between 1–1440 (minutes) as the offset time.

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

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

9.7 SMS

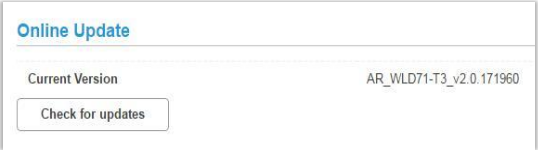
In this section, you can write new messages and view messages saved in your Inbox, Outbox, and Drafts. You may also view the SMSs stored on your SIM.

1.	**New Message**	**You can compose new messages in this section.**
2.	**Inbox**	Displays information about messages stored in the Inbox.
3.	**Outbox**	Displays information about messages stored in the Outbox.
4.	**Drafts**	Displays incomplete messages that have been temporarily saved.
5.	**SIM SMS**	Displays information about the SMS stored on your SIM card.
6.	**SMS Settings**	Enables you to select SMS over IMS or SMS over SGs.

10. Update

10.1 Online Update

Firmware will be continually updated as more features are added and known issues are resolved.
This section shows the current version of your firmware and helps you upgrade the firmware to the latest version online. Click **Check for updates** to see if updates are available.

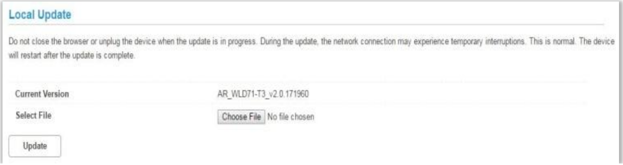


Online Update

Current Version AR_WLD71-T3_v2.0.171960

10.2 Local Update

This section 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.



Local Update

Do not close the browser or unplug the device when the update is in progress. During the update, the network connection may experience temporary interruptions. This is normal. The device will restart after the update is complete.

Current Version AR_WLD71-T3_v2.0.171960

Select File No file chosen

11. Specifications

- **Hardware and Port Characteristics**

Button: Power/Reset/WPS
SIM Card Slot: 3FF (Micro)
Power Adapter: DC 12 V/1 A
Ethernet Port: 4 × Fast Ethernet LAN
RJ11 Port (6P2C) × 1

- **LGA Modules (Cat. 4)**

LTE: 2/4/28, 3G: 2/5 GSM: 2/5
@ supported 20 MHz bandwidth

- **LTE Antenna**

Internal antennas × 2

- **WLAN**

IEEE 802.11b/g/n–compliant

- **Antenna:**

Two internal antennas for Wi-Fi 2.4 G

- **Environmental**

Ambient Operating Temperature: –10 °C to +50 °C
Ambient Operating Humidity: 5% to 95%
Storage Temperature: –25 °C to +70 °C

- **Dimensions**

168 mm × 131.2 mm × 59.1 mm