marsboy

AX1800 Dual Band Wi-Fi 6 Router

User Guide

Contents

1 Get to Know Your Wireless Router 1
1.1 Product Overview 1
1.2 Package Contents 1
1.3 Product Specifications 2
1.4 Appearance 4
1.4.1 Top Panel 4
1.4.2 Back Panel 5
2 Connect the Hardware 6
2.1 Position Your Router 6
2.2 Setup Requirements 6
2.3 Connect Your Router 8
2.3.1 Wired Connection 9
2.3.2 Wireless Connection 9
3 Log in to Your Router 9
4 Set Up Internet Connection 10
4.1 Manually Set Up Your Internet Connection 10
4.1.1 PPPoE 10
4.1.2 PPTP 11
4.1.3 L2TP 11
4.1.4 Static IP 12
4.1.5 DHCP 12
4.2 Set Up Your Wireless Network 13
4.2.1 Configure Your Wi-Fi Network Name (SSID) and Wi-Fi Password 13
4.2.2 Configure Your Wireless Network Name (SSID) and Wireless Network Password 14
4.2.3 Set up the Router as an Access Point (Bridge Mode) 17
4.4 Set up an IPv6 Internet Connection 18
4.4.1 IPv6 (Auto Configured/DHCPv6) 19
4.4.2 IPv6 Static 20
4.4.3 IPv6 Relay 21
5 Guest Network 22
5.1 Create a Network for Guests 22
5.1.1 Enable Guest Network 23
5.1.2 Customize Guest Network 24
6 Security Settings 25
6.1 Firewall Settings 25
6.1.1 Firewall Setting – Low 26
6.1.2 Firewall Setting – Medium 26
6.1.3 Firewall Setting –High 26
6.1.4 Firewall Setting – Set Exception Rules 27
6.1.5 Firewall Setting – Set Filtering Rules 28
6.2 Access Control 29
6.2.1 Wireless Access Control – Add from List 30
6.2.2 Wireless Access Control – Add Manually 31
6.3 Manage Device Access List 32
6.3.1 Manage Device Access List 33
6.4 Filter Control 34
6.4.1 URL Filter Control 35
6.4.2 Block Access Control 36
6.5 Parental Control 36
6.6 Device Access Control 37
6.7 UPnP 38
7 L2TP VPN 39
8 Customize Your Network 40
8.1 Mesh 40
8.1.1 Set up Mesh Connection 41
8.1.2 Mesh Status Display 42
8.2 QoS 42
8.2.1 QoS – Upstream Speed Limit 43
8.2.2 QoS – Downstream Speed Limit 44
8.2.3 QoS – Terminal Device Speed Limit 45
8.2.4 DHCP Static IP Assignment (Address Reservation) 47
8.2.5 DHCP Static IP Assignment – Add by List 48
8.2.6 DHCP Static IP Assignment – Add Manually 49
8.3 Port Forwarding 49
8.3.1 Port Forwarding – Add Rules 50
8.3.2 Port Forwarding – Modify Rules 51
8.3.3 Port Forwarding – Delete Rules 52
8.4 DMZ 52
8.5 UPnP 53
8.6 Wireless Roaming Setting 53
8.7 DDNS 54
8.8 LAN Settings 55
8.8.1 DHCP Server Settings 56
8.8.2 Change Wireless Network Name (SSID) and Wireless Network Password 57
8.8.3 Change Wireless Network Name (SSID) and Wireless Network Password 58
8.8.4 Change Wireless Working Mode 62
8.8.5 Use Repeater to Extend Network 64
8.9 AP Mode (Bridge Mode) 67
8.10 WAN Settings 68
8.10.1 Change Connection Type 69
8.10.2 Change IP Mode 70
9 Manage the Router 71
9.1 Restore Default 71
9.1.1 Manual Restore 71
9.1.2 Setting Page Restore 72
9.2 Change the Web Management Login Password 72
9.3 Set up System Time 73
10 Trouble Shooting 74
11 Warranty Information 79
12 Product Disposal 80

About This Guide

This guide instructs you on the Internet setup, and shows you how to connect your Mardsoy Wireless Router and its accessories. When using this guide, please note that features available of the router may vary by model and software version. Router's availability may also vary by region or ISP. All screenshots, images, steps, parameters and descriptions in this guide are only examples and may not reflect your actual experience.

*Maximum wireless signal rates are the physical rates derived from IEEE Standard 802.11 specifications. Actual wireless data throughput and wireless coverage are not guaranteed and will vary as a result of network conditions, client limitations, and environmental factors, including building materials, obstacles, volume and density of traffic, and client location.

*Use of MU-MIMO and 1024-QAM requires clients to also support those functions.

More Info

After-sales Service:
Email: ad@mandsoytech.com
Live Chat: mandsoy.aftersservice.vip

1 Get to Know Your Wireless Router

1.1 Product Overview

Thank you for purchasing our Mardsoy AX1800 Wireless Router! Equipped with 802.11ax Wi-Fi Technology, the modern-looking Mardsoy AX1800 features 2.4GHz and 5GHz dual bands for an unprecedented wireless HD streaming; the innovative mesh networking function can enable up to 4 times more coverage than a single Wi-Fi router; the Gigabit Ethernet provides up to 10% power-saving solution. It's also backwards compatible with 802.11a/b/g/n/ac.

1.2 Package Contents

NOTE:

- If any of the items are damaged or missing, contact Mardsoy for technical inquiries and support. Refer to the Mardsoy Support Contact at the back of this user manual.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Product Specifications

- Specifications:

Product Name	Mardsoy Dual Band AX1800 Wi-Fi 6 Router
DC Power Adapter	DC Output: 12V with max 1A current;
Operating Temperature	0°C ~ +40°C (32°F ~ 104°F)
Storage Temperature	-20°C ~ +70°C (-4°F ~ 158°F)
Operating Humidity	10% ~ 90% RH (No condensation)
Storage Humidity	5% ~ 95% RH (No condensation)

NOTE:

- Use only the adapter that came with your package. Using other adapters may damage the device.
- Keep a minimum gap of 15cm around the equipment, and do not cover it with newspapers and other items.
- The equipment must not be exposed to water droplets or splashes. Do not place objects filled with liquids, such as vases, on the equipment.
- Please place the router away from humidity, exposure to the sun, high temperature, other similar environments, as well as magnetic objects.
- Please avoid scratching the case or interface. And also please avoid dropping the device due to falling, throwing or being subjected to strong impact.
- Please do not try to disassemble this product by yourself. Maintenance work can only be carried out by staff authorized by the company.
- Please use the products with AC or DC power switch. "■" means power off, "□" means power off.
- This product has an external power adapter as a power disconnect device. Please pay attention to safe plugging and unplugging, and the disconnect device should be easy and convenient to operate.

1.4 Appearance

1.4.1 Top Panel

The router's LED Crows from left to right) are located on the Front, You can check the router's working status by the following LED Explanation table.

LED Explanation

Status	Explanation
Solid on in red	The router system is starting or failed to connect to the network.
Flashing in green	The router is performing WPS or Mesh connection.
Solid on in green	The router has been successfully connected to the Internet.

1.4.2 Back Panel

Button and Port Explanation

Item	Description
Power ON/OFF Button	Press this button to power on or off the router.
POWER Port	For connecting the router to a power socket via the provided power adapter.
WPS Button	Press the button for 5 seconds to activate mesh networking.
RESET Button	Press and hold the button for at least 5 seconds to reset the router to its factory default settings.
LAN1/LAN2 LAN3/LAN4	For wired connection to devices via cables.
Antennas	Used for wireless operation and data transmission. Adjust for the best Wi-Fi performance.

2 Connect the Hardware

2.1 Position Your Router

For the best wireless signal transmission between the wireless router and the network devices connected to it, ensure that you:

1. The router should not be located in a place where it will be exposed to moisture or excessive heat.
2. Place the router in a location where it can be connected to multiple devices as well as to a power source.
3. Make sure the cables and power cords are safely placed out of the way so that they do not create a tripping hazard, or have a chance of being worn or damaged.
4. Keep the router away from devices with strong electromagnetic interference, such as Bluetooth devices, cordless phones and microwaves.

2.2 Setup Requirements

To set up your wireless network, you need a computer that meets the following minimum requirements:

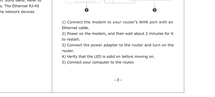
1. Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000BaseTX)
2. IEEE 802.11a/b/g/n/ac wireless capability An installed Network Interface Card (NIC)
3. Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome

NOTE:

- If your computer does not have built-in wireless capabilities, you can add a NIC to it to connect to the Mardsoy WLAN adapter to your computer to connect to the network.
- With its dual band technology, your wireless router supports 2.4GHz and 5GHz wireless signals simultaneously. This allows you to carry out Internet-related activities such as Ethernet surfing or reading / writing e-mail messages using the 2.4GHz band while simultaneously streaming high definition audio/video such as movie or music using the 5GHz band.
- Some IEEE 802. 11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications. The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

2.3 Connect Your Router

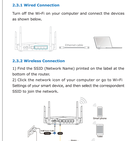
Before you start, please turn off your modem if any. Hold the antennas from the base and mave the antennas vertically. Use the provided network cable to connect your modem directly from the wall instead of through a DSL/Cable/Satellite modem, connect the Ethernet cable to the router's WAN port, and then follow step 3 to complete the hardware connection.



1) Connect the modem to your router's WAN port with an Ethernet cable.
2) Power on the modem, and then wait about 2 minutes for it to restart.
3) Connect the power adapter to the router and turn on the power switch.
4) Verify that the LED is solid on before moving on.
5) Connect your computer to the router.

2.3.1 Wired Connection

Turn off the Wi-Fi on your computer and connect the devices as shown below.



2.3.2 Wireless Connection

1) Find the SSID (Network Name) printed on the label at the bottom of the router.
2) Click the network icon of your computer or go to Wi-Fi Settings of your smart device, and then select the corresponded SSID to join the network.

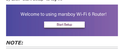
NOTE:

- WPS is NOT supported by iOS devices.
- The WPS function cannot be configured if the wireless function is disabled or configured to WEP. It must be set to disabled if your wireless encryption is WEP. Please make sure the wireless function is enabled and is configured with the appropriate encryption before configuring the WPS.

3 Log in to Your Router

With a web-based utility, it is easy to configure and manage the router. The web-based utility can be used on any Windows, MacOS or UNIXOS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari. Follow the Steps below to login to your router.

1) Set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer.
2) Open the browser and visit 192.168.100.1 or router.mardsoy.com
3) Click "Start Setup" to log in.



NOTE:

- If the login window does not appear, please refer to the FAQ section.
- You can also scan the QR code to enter the web-based utility login page.

4 Set Up Internet Connection

4.1 Manually Set Up Your Internet Connection

In this part, you can check and modify your current internet connection settings. You can also modify the settings according to the service information provided by your ISP.
After logging in to the web-based utility of your router, you can select your internet connection type from the drop-down list.

4.1.1 DHCP

Select DHCP (Dynamic Host Configuration Protocol) if your ISP doesn't provide any information for internet connection. It will assign a unique IP address automatically to your device. Then click **Next** to enter the next step.

4.1.2 PPPoE

If you choose PPPoE, enter the username and password provided by your ISP. PPPoE users usually have DSL cable modems.
Then click **Next** to enter the next step.

NOTE:

- If you forget your Username or Password, follow the suggestions below:
1) Consult ISP and obtain username and password.
2) Use an Ethernet cable to connect the WAN port of RX4-1800 to the LAN port of the old router, click "Get from old router" in this page. After obtaining this information, replace the original router with the RX4-1800.

4.1.3 Static IP

If you choose Static IP, enter the information provided by your ISP in the corresponding fields.
Then click **Next** to enter the next step.

NOTE:

- After finishing modifications and clicking **Next**, you will enter the **Set Your Wireless Network page**.
- You can take a screenshot to keep the information for future use.

4.2 Set Up Your Wireless Network

4.2.1 Configure Your Wi-Fi Network Name (SSID) and Wi-Fi Password

In this step, you can follow the instructions below to configure your wireless network.
1) Change the router name (SSID) for your preference, or keep the original one.
2) Enter password with digits between 8-24.
3) Click **Next** to enter the next step.

NOTE:

- If you select "Unify 2.4GHz & 5GHz", then 2.4G and 5G Wi-Fi will use the same network name. Meanwhile, the router will automatically select the best Wi-Fi network for the terminal devices.

- However, due to differences of terminal devices, the network may be interrupted for a short time when the signal source is automatically switched, or the connection may even be dropped.

4.2.2 Configure Your Web Login Password

In this step, you may follow the instructions below to configure the login password of your web-based utility page.
1) Enter the password you would like to set. There is no default password.
2) By clicking "Apply", the last configuration for your Wi-Fi network and web-based utility page is finished.

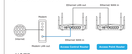
NOTE:

- If you select "Same with Wi-Fi password", it means the password for the web-based configuration login page will be the same with the Wi-Fi network password in the last step.
- You can take a screenshot of this page to keep the information for future use.

4.3 Set up the Router as an Access Point (Bridge Mode)

The router can work as an access point, transforming your existing wired network to a wireless one or expand your wireless network.
Before installation, please complete the following settings:
1) After disconnecting the WAN port on the router, connect a device (such as a PC or phone) to your Mardsoy router and launch a web browser. Then, log in to your router.

2) Go to **Basic > WAN > WAN Mode (Link Mode)**, Select **Bridge** from the **Link Mode** drop-down list. Then, click **Apply** to finish your setting.



3) Connect the router to your existing wired router via an Ethernet cable. Please refer to the instruction above below.

NOTE:

- If you want to enjoy seamless roaming, please make sure that the wireless settings of all your wireless devices are consistent (to have a unified SSID and password).

4.4 Set up an IPv6 Internet Connection

Your ISP provides information about one of the following IPv6 internet connection types: IPv6 (Auto Configured), IPv6 Static.

4.4.1 IPV6 (Auto Configured/DHCPv6)

1) After logging in to your router, go to **Basic > WAN > IP Mode**.
2) Select **IPv6** from the drop-down list.
3) Then, set **IPv6 Address** to **Auto Configured or DHCPv6**, **DNS** to **Auto**, and fill in **IPv6 Address** and **Default IPv6 Gateway** as required.
Click **Apply** to finish your setting.

4.4.2 IPV6 Static

1) After logging in to your router, go to **Basic > WAN > IP Mode**.
2) Select **IPv6** from the drop-down list.
3) Then, set **IPv6 Address** to Static, and fill in **IPv6 Address** and **Default IPv6 Gateway** as required.
Click **Apply** to finish your setting.

4.4.3 IPV6 Relay

1) After logging in to your router, go to **Basic > WAN > IP Mode**.
2) Select **IPv6** from the drop-down list.
3) Then, set **IPv6 Address** to Static, and fill in **IPv6 Address** and **Default IPv6 Gateway** as required.
Click **Apply** to finish your setting.

5 Guest Network

The Guest Network function allows you to provide Wi-Fi access for guests without disclosing your home network. When you have guests in your house, apartment or workplace, you can create a guest network for them.

5.1 Create a Network for Guests

1) After logging in to your router, click **Basic > WAN > Guest Network**.

2) Click the **Enable Guest Network** button for the 2.4GHz or 5GHz wireless network.
3) Customize your Guest Network's Wi-Fi name and key. 4) You can also modify Authentication Mode (WPA-PSK/WPA2-PSK is recommended).

5) Click **Save** to finish your settings. Now your guest can access your guest network using the SSID and password you set.

6.1.1 WAN Access Control

The Firewall protects the router from cyber attacks and validates the traffic that is passing through the router based on protocol. When Firewall is enabled, the state-based firewall rules will establish security protection between the router and the Internet to prevent associated connections and DoS attacks from the WAN side.
This function is enabled by default and it is recommended to keep the default settings. If the Firewall is disabled, the protection will be lost and the router will face the risk of cyber attacks.

6 Security Settings

This section guides you on how to protect your home network from unauthorized users by implementing network security functions. You can create a personalized network that caters to your needs by setting firewall rules, blocking access to websites using Keyword Filtering, block or allow specific client devices to access your network using Access Control, or block inappropriate websites at specified time using Parental Control.

6.1.1 Firewall Setting – Low

After logging in to your router, go to **Basics > Security > Firewall**.

NOTE:

- This feature is enabled by default, and the initial state is Low. Also, this mode provides low-level conventional protection, and the protection rules cannot be customized.

6.1.2 Firewall Setting – Medium

1) After logging in to your router, go to **Basics > Security > Firewall**.
2) Select Medium from the **Firewall Level** drop-down list.
3) Click **Apply** to finish your setting.

NOTE:

- This mode provides medium-level network protection, the most suitable network protection without affecting your normal use, but meanwhile the protection rules cannot be customized.

6.1.3 Firewall Setting –High

1) After logging in to your router, go to **Basics > Security > Firewall**.
2) Select **High** from the **Firewall Level** drop-down list.
3) Click **Apply** to finish your setting.

NOTE:

- This mode provides the highest level of network protection, which will affect the normal use of the network, especially some software that requires the use of specific network

- Please clarify the port usage before customizing the rules, and disable the corresponding rules if the port is not in use or compromised, please go to the network security page and change the **Firewall Level** to **Medium** or **Low**.

6.1.4 Firewall Setting – Set Exception Rules

You may follow the instructions below to add Firewall exception rules.
1) After logging in to your router, go to **Basics > Security > Firewall**.
2) Select **High** from the **Firewall Level** drop-down list.
3) Click **Add** in **Firewall exception rules**.
4) After filling in the necessary information, click **Add** in **Firewall exception rules**.

NOTE:

- If it affects your normal use and needs to close this rule, click the Remove button next to the corresponding rule.
- The following screenshot shows an example of the rules.

6.1.5 Firewall Setting – Set Filtering Rules

The protocol filtering rules is used to block IP and its protocol packets derived from the LAN side. You may follow the instructions below to add protocol filtering rules.
1) After logging in to your router, go to **Basics > Security > Firewall**.
2) Select **High** from the **Firewall Level** drop-down list.
3) Click **Add** in **Filter Rules**.
4) After filling in the necessary information, click **Add** in **Protocol Filter Rules**.

NOTE:

- If it affects your normal use and needs to close this rule, click the Remove button next to the corresponding rule.
- The following screenshot shows an example of the rules.

6.2 Wireless Access Control

Wireless Access Control blocks or allows terminal devices to access your network (via wired or wireless) based on a list of blocked devices (Blacklist) or a list of allowed devices (Whitelist). There are two ways to setting wireless access control: adding from list, or adding manually.

6.2.1 Wireless Access Control – Add from List

You may follow the instructions below to block or allow devices to access your wireless network with the method of adding from list.
1) After logging in to your router, go to **Basics > Security > Wireless Access Control.**
2) Select the wireless name you want to be set from the SSID drop-down list.
3) Click the **Enable** button (to the green status).
4) Select the access **Mode** (to block or allow the device).
5) Select the device, select **Block List**, and then click **Save**.

6.2.2 Wireless Access Control – Add Manually

You may follow the instructions below to block or allow devices to access your wireless network with the method of adding manually.
1) Obtain the MAC address of the device that you do NOT want to access the specified SSID from its product label or product description.
2) After enabling Wireless Access Control, click **Add Manually** in the Device List section.
3) Fill in the prepared MAC address in the **MAC Address** field. 4)Click **Add** to finish your setting.

1) Click **Add from List** in the **Device List** section. You will see the connected devices in the Device List section.
2) Turn the selection box next to the device(s) you want to block, and then select **Add** to finish your setting.

1) Then, devices in the **Device List** will NOT be allowed to access the current SSID (wireless network).

NOTE:

- If you want to restore connection permissions for this device, click the Remove button next to the corresponding rule.

6.3 Manage Device Access List

This page is used to manage devices that can log in to the router setting interface.
1) If this feature is turned on, the router can be configured only from devices in the following MAC address list.
2) Turn the selection box next to the device that sits thruter for the first time and be in the list.
3. If you accidentally delete all the management devices, please press the RESET button and hold for 10 seconds to restore factory settings.
4) Access Management is based on MAC address. There are two ways to get the MAC address: in the device interface of the homepage; from product label or product description. In the following, an example of adding a Mac from PC or mobile phone to the **Management device access list**.

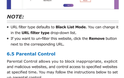
New the device has been added to the management list! If you want to cancel the management authority of this device, click the **Remove** button next to the corresponding rule.

6.4 URL Filter Control

URL Filter Control is used to block or allow specific URL to access your network (via wired or wireless) based on a list of keywords. Keywords can be set up in advance in Keyword Filtering. You may follow the instructions below to set the URL filter.
1) After logging in to your router, go to **Basics > Security > URL filter control.**

2) Click **Add** at the bottom of the URL **filter control** section. Fill in the target URL in the **URL address** field in the pop-up interface, and then click **Add** to finish your setting.

New the blocked URL appears in the **URL filter control section**!



NOTE:

- URL filter type defaults to **Black List Mode**. You can change it in the **URL filter type** drop-down list.
- If you want to unfilter the website, click the **Remove** button next to the corresponding URL.

6.5 Parental Control

Parental Control allows you to block inappropriate, explicit and malicious websites, and control access to specified websites at specified time. You may follow the instructions below to set Parental Control.
1) Obtain the MAC address of the device you want to manage. You can get the MAC address of the connected device in **Device List** section in **Device Lists**.
2) After logging in to your router, go to **Basics > Security > Parent Control**.
3) Fill in the MAC address of the device you want to add in the **Device MAC** field.
4) Select the **Blocking Days** and the **Blocking Duration** to your preference.

NOTE:

- If you want to cancel the management authority of this device, click the **Remove** button next to the corresponding rule.
- Only devices that have previously been connected to your router's network appears in the **Device List**. If you are unable to find the device you want to add, connect the device to your router's network and then try again.

6.6 Device Access Control

Device Access Control manages network access of a device based on its MAC address.
1) Obtain the MAC address of the device you want to manage.
2) Find the MAC address of the connected device in the **Device List**.
3) After logging in to your router, go to **Basics > Security > Device Access Control**.

4) Select the control mode from **Access Control Mode** drop-down list and then **Save** to finish your setting.

5) Click **Add**, and then fill in your device's **MAC address** in the MAC Address field in the pop-up interface.
6) Click **Add** to finish your setting.

NOTE:

- If you want to cancel the management authority of this device, click the Delete button next to the corresponding rule.

7 VPN Server

The VPN (Virtual Private Networking) Server allows you to access your home network in a secured way through internet when you are away from home. This section instructs you on setting up VPN connection in L2TP connection mode.

7.1 L2TP VPN

1) After logging in to your router, go to **Advanced > VPN**.
2) Click **Add** in the **VPN** section.
3) Fill in the fields according to the information provided by the VPN provider based on the L2TP protocol.

NOTE:

- VPN user name, password, server address, protocol type and pre-shared authentication need to be obtained from the VPN service provider.
- The server address can be domain name or IP address, which is provided by the service provider.
- Optional. After completing the VPN setup, you can manage your VPN network by **SmartSpot VPN Streaming**.

8 Customize Your Network

This section guides you on how to configure advanced network features.

8.1 Mesh

Mesh connection mode can be quickly achieved via WPS button.

8.1.1 Set up Mesh Connection

1) Connect your router's WAN port to the LAN port of the ar-router's LAN port.
2) Set up the router whose WAN port is unavailable, enable it to access the Internet normally (please note that the wireless network must be set to the properly encrypted state and password has been set).
3) Press the WPS button on both routers for at least 5 seconds.
4) After about 30 seconds until the lights on both routers change from flashing to steady green, the setting is complete. By now the mesh network is established and can be used normally.

NOTE:

- If you want to continue adding mesh devices, get another Mardsoy router to build the mesh network. Press the WPS button on the new device and the main router in the mesh network for at least 5 seconds, and wait for the mesh network to complete.
- Devices that log in through the mesh network can only access the main router and view sub devices in Advance > Mesh.
- If failed, please reset both routers/and follow the setting steps again.

8.1.2 Mesh Status Display

After pressing the WPS button on the main router for at least 5 seconds, Mesh page is displayed as follows: (no following devices is connected yet)
Note: Controller
Status: Waiting for pairing

After about 30 seconds, the link diagram will be displayed in the status diagram as follows:

NOTE:

- After successful pairing, you can only log in to the main router to connect/view the device is connected to the mesh.
- Generally, signal strength higher than -50 can be acceptable, if it is lower than -74, please adjust the placement of the device.

8.2 QoS

QoS (Quality of Service) allows you to prioritize the internet traffic of specific device.

8.2.1 QoS – Upstream Speed Limit

You may follow the instructions below to check and control the router speed limit.
1) After logging in to your router, go to **Advanced > QoS**.
2) Select **Terminal device speed limit** section, click **Set Speed Limit**.
3) Enter the maximum upload and download speed you want to set in the corresponding fields. Then, click **Apply** to finish your setting.
4) If you want to modify the terminal speed limit, click **Set Speed Limit** to modify the limit values, and click **Apply** to finish your setting.

NOTE:

- If set to 0, the network speed of the device will NOT be restricted.

8.2.2 QoS – Terminal Device Speed Limit

You may follow the instructions below to check and control terminal device speed limit.
1) After logging in to your router, go to **Advanced > QoS**.
2) Select **Terminal device speed limit** section, click **Set Speed Limit**.
3) Enter the maximum upload and download speed you want to set in the corresponding fields. Then, click **Apply** to finish your setting.
4) If you want to modify the terminal speed limit, click **Set Speed Limit** to modify the limit values, and click **Apply** to finish your setting.

NOTE:

- If set to 0, the network speed of the device will NOT be restricted.

8.2.3 DHCP Static IP Assignment (Address Reservation)

This function is used to assign a fixed IP address to your specific terminal device. Address reserve requires a fixed IP, such as network printers, IP cameras.
It is recommended to connect the device to the router first, so that it will be more convenient to obtain the MAC address of the device.

8.2.4 DHCP Static IP Assignment – Add by List

1) After logging in to your router, click **Advanced > DHCP**.
2) Click **Add by List**, and select the device whose IP needs to be fixed from the drop-down list. Then, click **Add** to finish your settings.
3) If you want to modify the settings, click the **Remove** button next to the corresponding rule.

8.2.5 DHCP Static IP Assignment – Add Manually

You may follow the instructions below to set up DHCP static IP assignment manually.
1) Obtain the MAC address of the device you want to assign IP address.
2) Click **Add Manually**, and fill in this device's MAC address and IP address. Then, click **Add** to finish your settings.
3) If you want to modify the settings, click the **Remove** button next to the corresponding rule.

8.2.6 LAN Port Forwarding

A virtual server is a server using a device on the LAN side, which can be accessed directly from the external network.
1) After logging in to your router, go to **Advanced > Application**.
2) Click **Add** button in the **Port Forwarding** section.
3) Fill in the **Protocol, Internal IP Address** and **Internal Port**, and select **Protocol Type** from the drop-down list.
4) If you want to modify the settings, click the Delete button next to the corresponding rule.

8.5 DMZ

DMZ maps the internal IP address of an internal host to a public IP address. When a user accesses a port of a host that provides a mapped port, the server transfers the request to the host corresponding to the port service in the LAN. With this function, you can map multiple ports of a host with an external IP address to different ports on different internal hosts on the internal