802.11ax Wave 2 Router User Guide

- 2020/5/21

Table of Contents

1 Hardware Setup

1.1 Getting To Know Your WiFi Router

This product is designed for the In-Home and Business WiFi services for Spectrum customers. With a custom industrial design, this WiFi Router can be placed in a central location to deliver superior WiFi network coverage.

The WiFi Router provides:

1. High performance:
    - Qual-Core A53 up to 2.2G/2GB DDR RAM.
    - Dual-Band wireless up to AX3500 (2.4G 287M * 4 + 5G 600M * 4).
    - Three 1Gigabit LAN Port + One 2.5Gigabit WAN Port.
2. High security: Firewall/VPN supported.
3. Ease of setting up: Friendly wizard, visual setup & maintenance (Basic Mode), complete functions (Advanced Mode).

The WiFi Router is an ideal choice for residential and SMB (Small Business) users who can enjoy a variety of wireless applications and services.

This chapter contains the following contents:

- Unpacking the WiFi Router’s Box
- Hardware Features
- Positioning Your WiFi Router

1.2 Unpacking the WiFi Router’s Box

Open the box and remove the WiFi Router, power adapter, Quick Start Guide, WiFi Network Name and Password sticker, and Ethernet cable.

WiFi Router Power Adapter

Figure 1. Check the box contents

The box contains the following items:

- WiFi Router
- AC power adapter
- Quick Start Guide
- WiFi Network Name and Password Sticker
- Ethernet cable

If any items are missing or damaged, please contact Charter Communications. Please keep the original packaging materials in case you need to return the product for repairing.

1.3 Hardware Features

Before you cable your router, take a moment to become familiar with the front and rear panels. Pay particular attention to the LEDs on the front panel.

1.3.1 Front Panel

The WiFi Router front and back panels feature the status LED and buttons as shown in the following figures.

Figure 2. WiFi Router front view

Front panel LED status

- **Off** Device off.
- **Blue** *Blinking* with 600ms interval Booting up
- **Blue** *Breathing* with 5s interval Connecting to the Internet

- **Blue** *Solid* — Connected to the Internet.
- **Red** *Breathing* with 5s interval — Connectivity issues (no Internet connection).
- **Red** and **Blue** cycle breathing with 2.5s interval — Updating firmware (or any scenario where device must not be restarted).
- **Red** *Solid* — Critical issues (hardware or otherwise).

1.3.2 Rear Panel

The Ethernet and buttons are shown in the following figure.

Figure 3. WiFi Router rear view

- **Factory Reset (Reset)**: Press and hold the Reset button for over 5 seconds, the

WiFi Router will reset to factory setting.

- **Ethernet (LAN) Port**: Connect network cables into these ports to establish LAN connection.
- **Internet (WAN) Port**: Connect a network cable into this port to establish WAN connection.
- **Power**: Use the bundled AC adapter to connect your WiFi Router to a power source.

1.4 Positioning Your WiFi Router

The WiFi Router lets you access your network from virtually anywhere within the operating range of your wireless network. However, the wireless communicating distance varies significantly due to placement of the WiFi Router. For example, the thickness and number of walls the wireless signal passes through can affect and limit the range. For best results, WiFi Router is likely to be placed as follow:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- Accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a shelf, keeping the number of walls and ceilings between the WiFi Router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves, computers, the base of a cordless phone, or a 2.4 GHz cordless

phone.

Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick and concrete can also affect your wireless signal.

2 Sign-In Your WiFi Router Web GUI

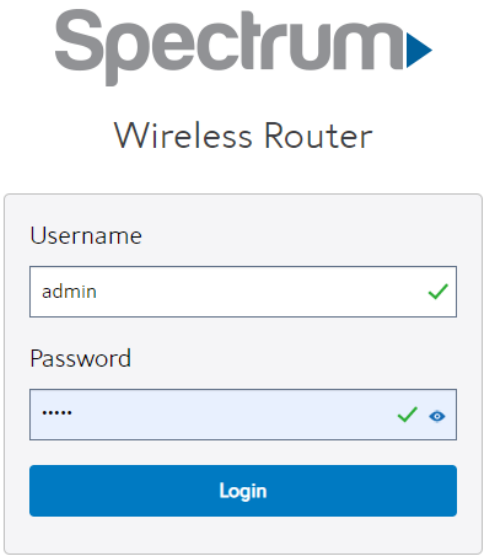
The WiFi Router contains an intuitive graphical user interface (GUI) based on web, which lets administrator easily configure its features through a web browser.

2.1 Sign-In

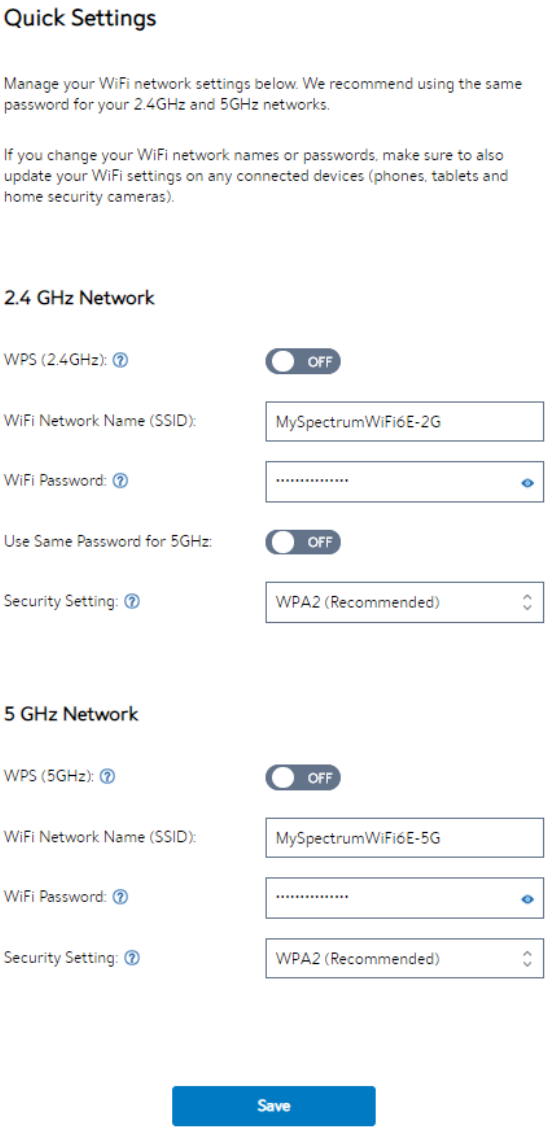
1. Open a web browser, then key in the WiFi Router's default IP address:

https://192.168.1.1, and click **Enter** key in the keyboard;

2. On the sign in webpage, type in its Username and password: **admin** (admin)**,** then click **Login** button.



After administrator has logged in the WiFi Router, some quick setting information will be displayed by the browser. You can quickly set up Wifi information.



WPS(2.4GHz):enable(ON) or disable(OFF) WPS.

Wifi Network Name(SSID):you should set your Wifi Name for connecting.

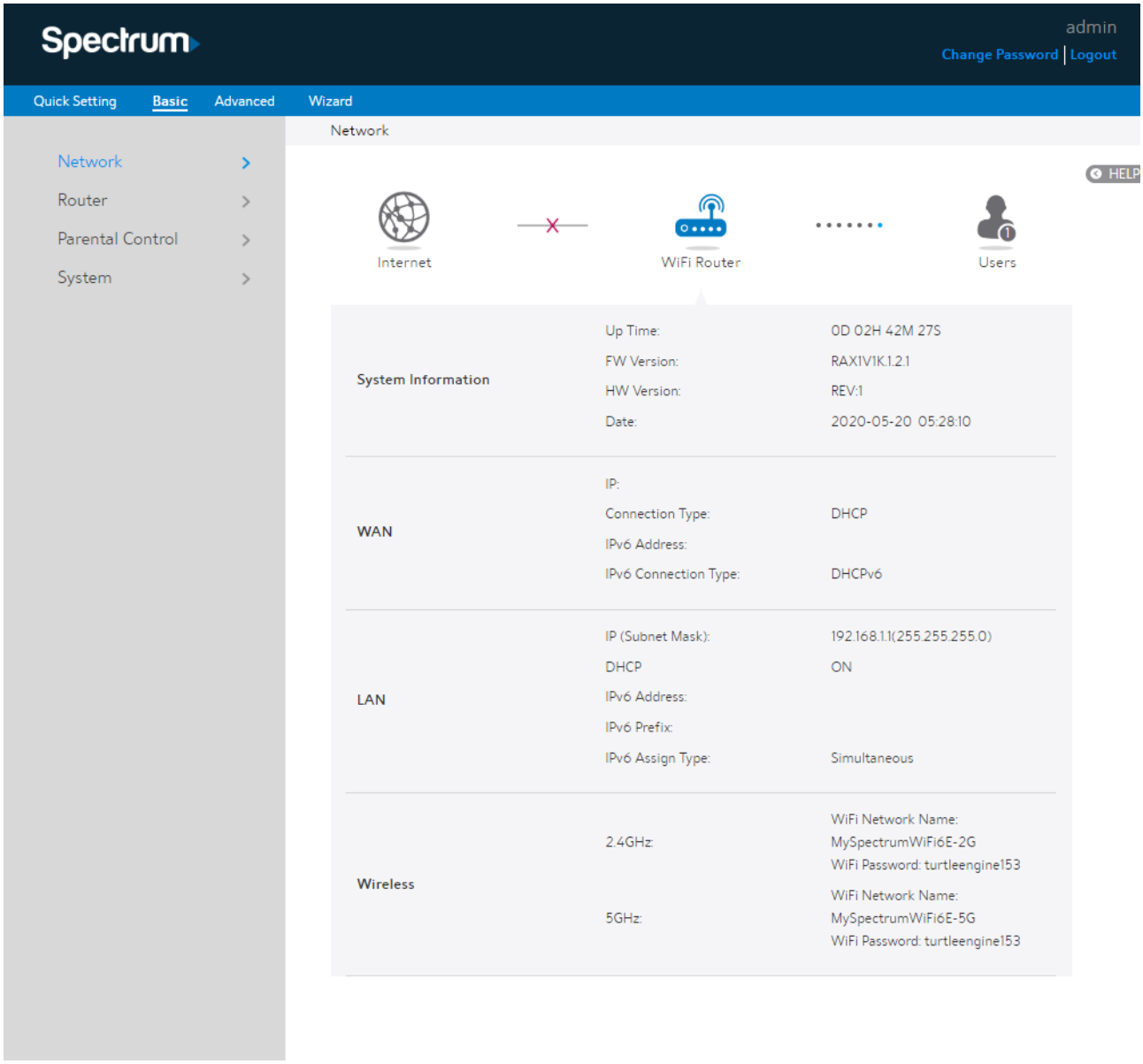
Password:Password.

Use Same Password for 5G:ON or OFF.

Security Settings:Select agreement.

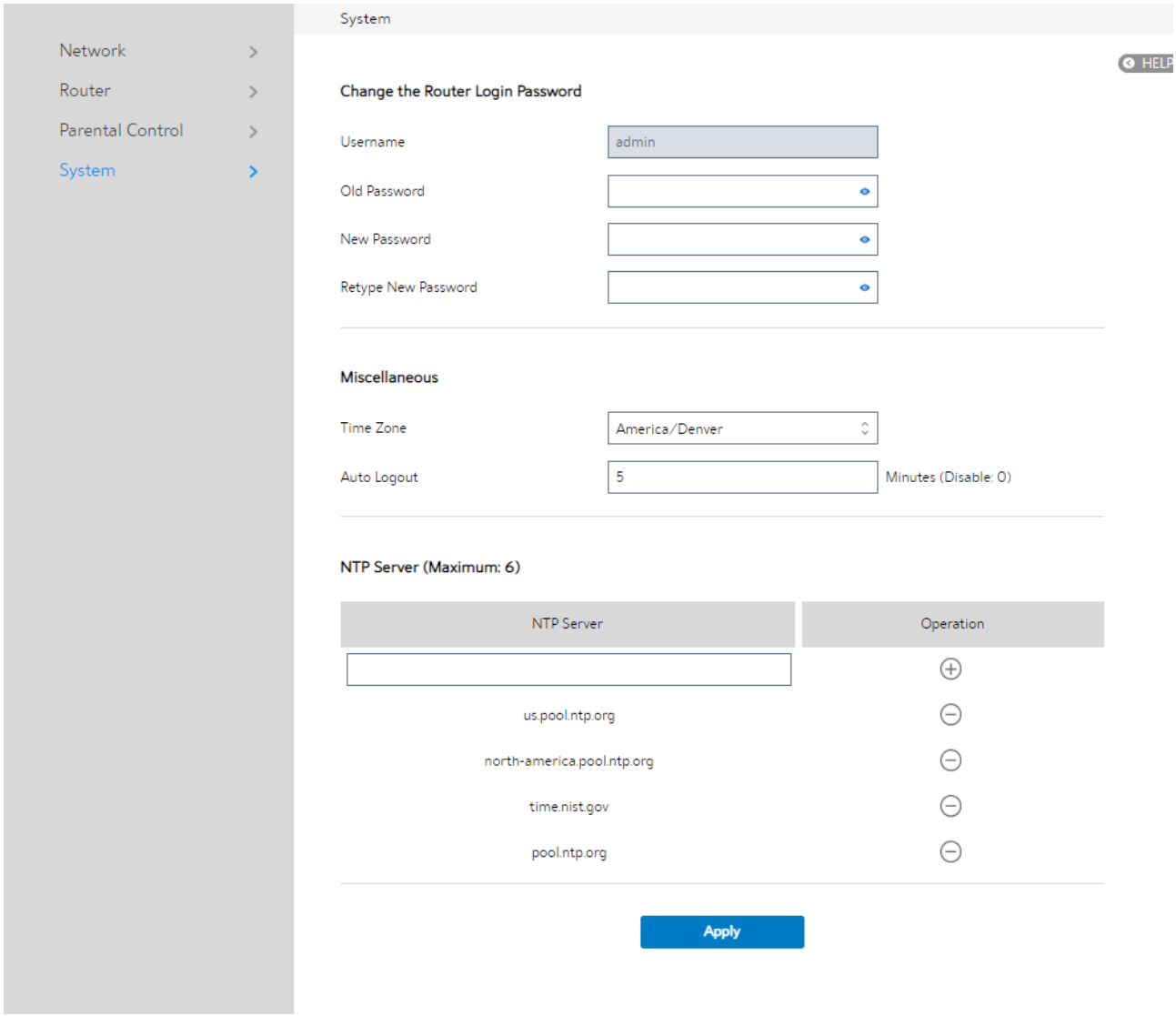
5GHz Network: It is the same as up here.

Go to **Basic** to view more information about the Network.



On the right top side, there are two command buttons: **Change Password** and **Logout**. Click the **Logout** button when administrator intends to leave the Web GUI.

When the **Change Password button** has been clicked on**,** the browser will navigate administrator to corresponding webpage.



On this page, user should 1) enter old password in “Old Password”, 2) enter new password in “New Password” and 3) retype New Password, then click **Apply** button. Web GUI user sign in password will be changed.

2.2 Wizard Setup

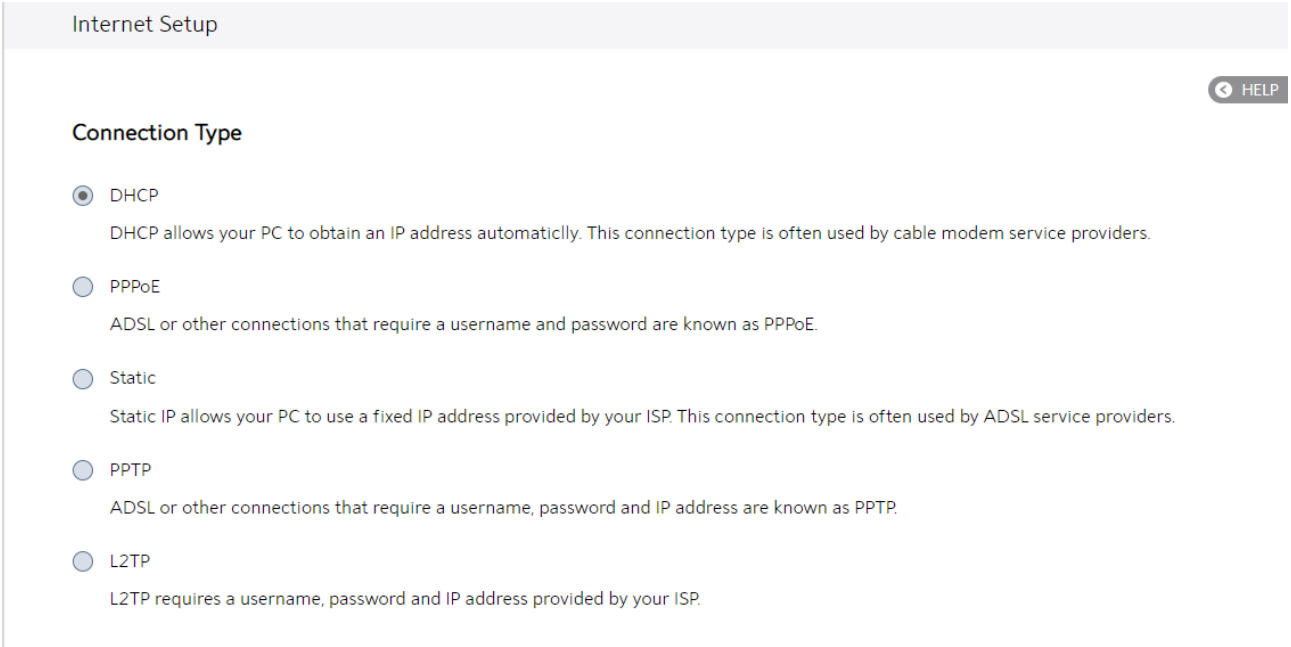
The wizard can navigate administrator to configure basic settings for WiFi Router, which makes it become easy enough to set up the WiFi Router.

Internet Setup

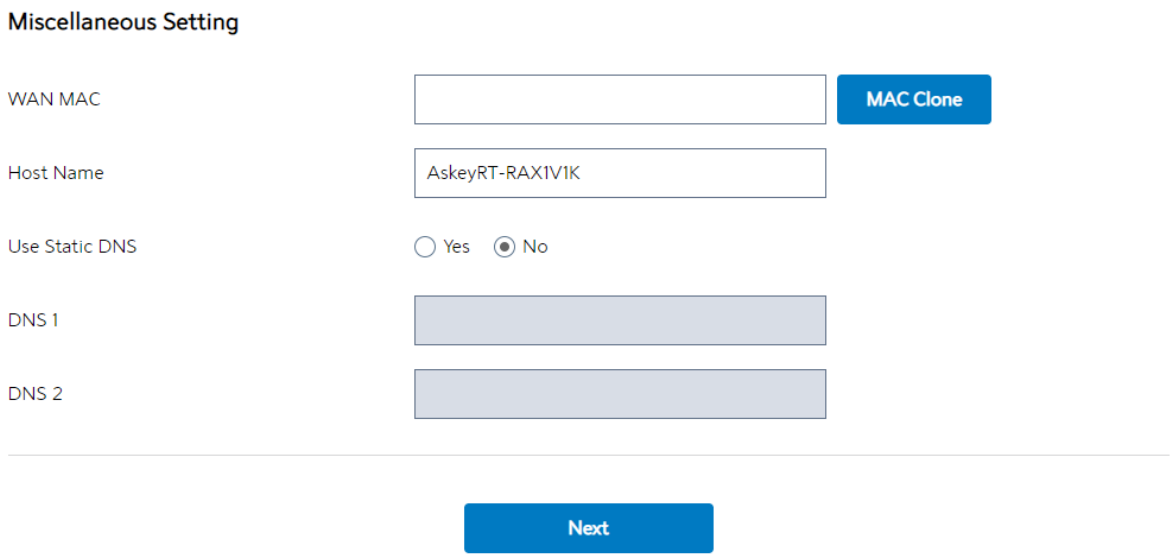
After administrator has clicked the **Wizard** button, the **Internet Setup** page will come up.

Connection Type:

There are 5 kinds of connection types: **DHCP**, **PPPoE**, **Static, PPTP and L2TP**.



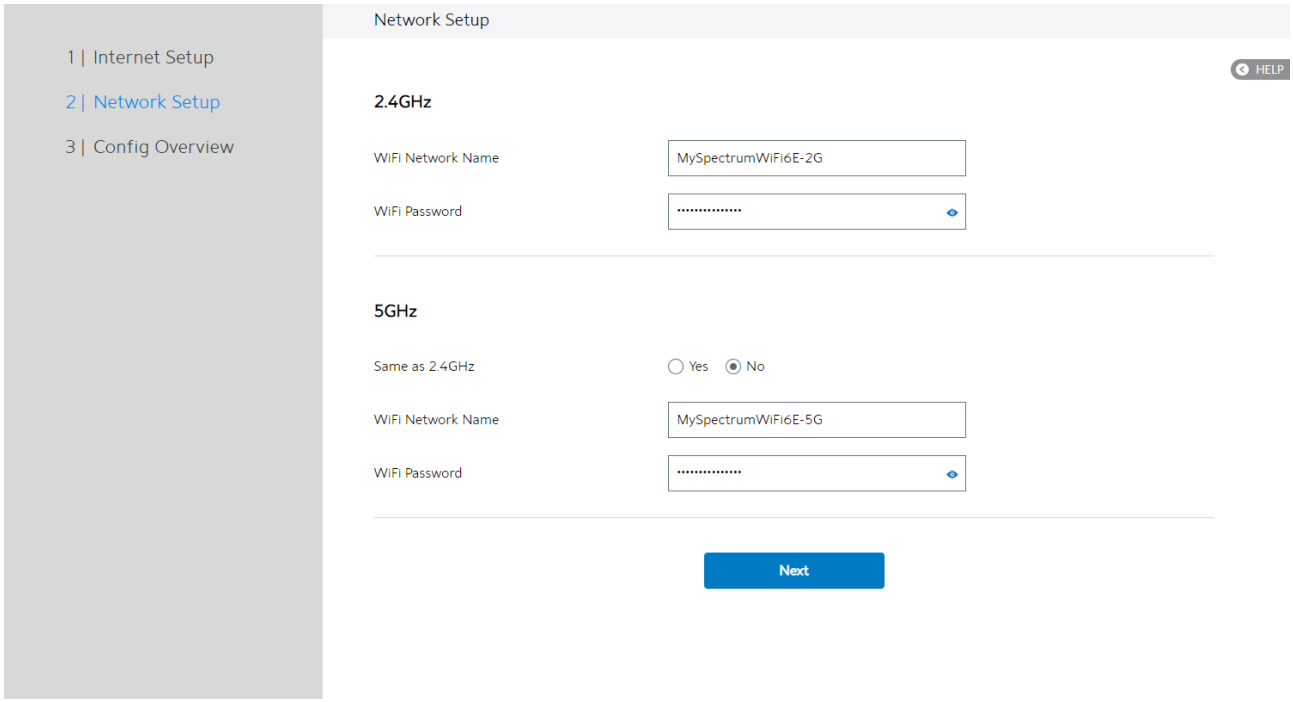
1. **DHCP:** Enable WiFi Router to obtain IP addresses automatically. This setting is the default for Spectrum services. More types of settings, refer to **2.3.4 WAN Setup**.



- **WAN MAC**: MAC address of WAN port.
- **Host Name**: This field lets administrator provide a name for WiFi Router.
- **DNS 1 & DNS 2:** Either of them indicates the IP address of a DNS Server.
- Click **Next**.

Network Setup

After you have clicked **Next icon** in Internet Setup page, the following webpage will appear.

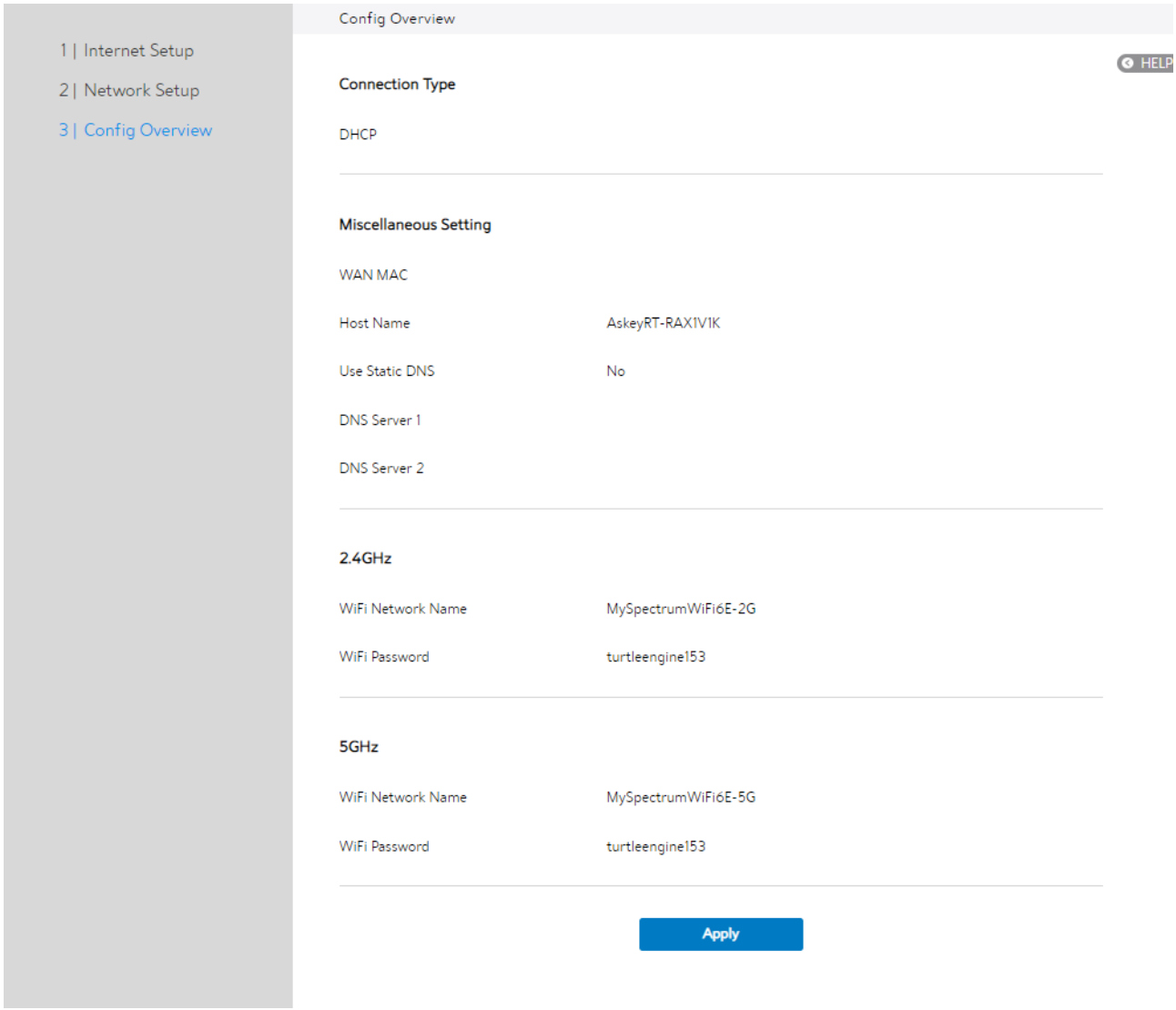


1. **WiFi Network Name**: Name of a wireless network, that's to say it's used to identify the wireless network. WiFi devices automatically detect all networks within its communication range. These are defaulted from the printed WiFi network name on the back of the WiFi Router. You can change them here, but they would no longer match the sticker on your WiFi Router.
2. **WiFi Password**: A password used by WiFi Router to authenticate wireless connections. These are defaulted from the printed WiFi password on the back of the WiFi Router. You can change it here, but they would no longer match the sticker on your router.
3. When done, click **Next**.

Config Overview

After click the **Next icon**, administrator comes to **Config Overview** page, which

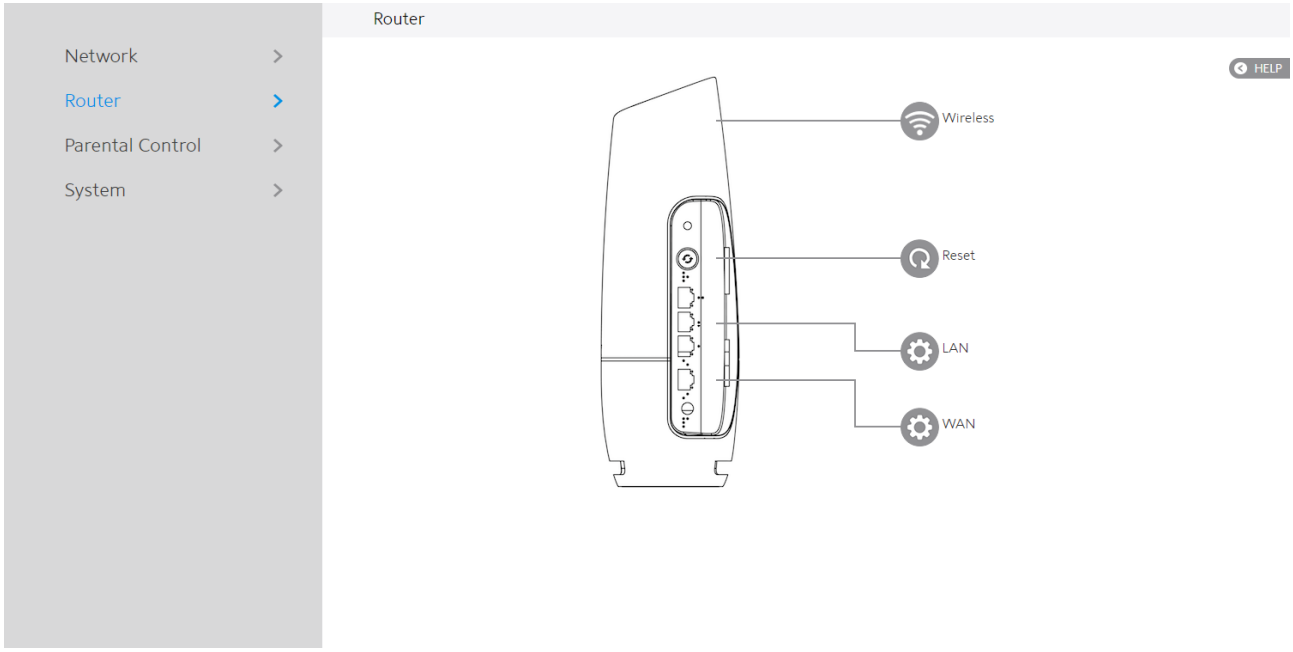
displays a summary of configuration information. If the settings are all correct, administrator should click **Apply** icon.



2.3 Basic Setup

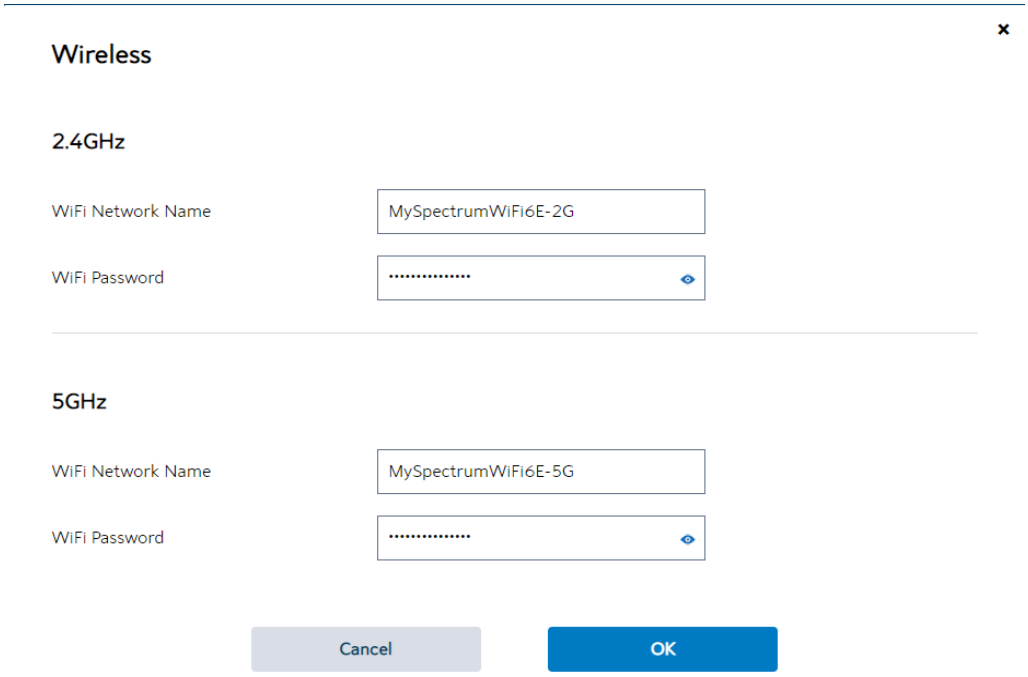
2.3.1 Router

From the navigation panel, go to **Basic > Router**.



NOTE: Clicking on the **Reset** icon in the Web GUI will restart the **WiFi Router.** If the WiFi Router hardware **Factory Reset (pinhole)** button is pressed and hold over 5 seconds, the WiFi Router will reset to factory setting.

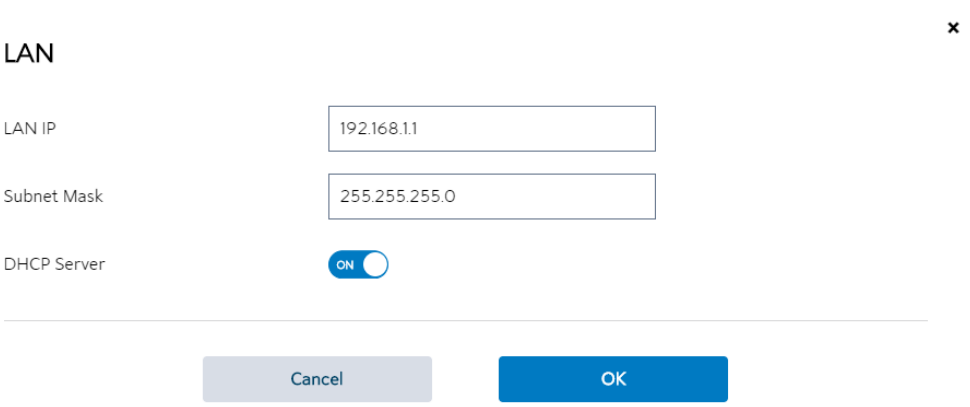
Wireless: This module is implemented to configure some basic settings for WiFi Router's wireless connection.



1. **WiFi Network Name**: A unique name that identifies the wireless network. Wireless device can automatically detect all networks within its communication range. The maximum length of a network name (SSID) is 32 characters.
2. **WiFi Password**: A string used for connection authentication. Its length ranges from 8 to 63 characters (letters, numbers or a combination) or from 8 to 64 hex digits.
3. Click **OK**.

2.3.3 LAN Setup

This module makes it easier for administrator to modify the default LAN IP Address.



Steps to modify LAN IP settings:

1. From the navigation panel, go to **Basic** > **Router.**
2. **LAN IP**: The LAN IP address of the WiFi Router. Its default value is 192.168.1.1. In IP-based networks, packets are sent to the network devices' specific IP addresses.
3. **Subnet Mask**: Subnet mask of WiFi Router. Its default value is 255.255.255.0
4. **DHCP Server**: DHCP (Dynamic Host Configuration Protocol) is mostly used to allocate IP address for LAN-side devices. And a DHCP server can inform LAN-side devices of DNS server's address, default gateway IP and etc. This WiFi Router can allocate 253 IP addresses at most.

NOTE: It's recommended for administrator to select **DHCP Server** for LAN IP setting. If not, administrator has to assign IP address to LAN-side device manually.

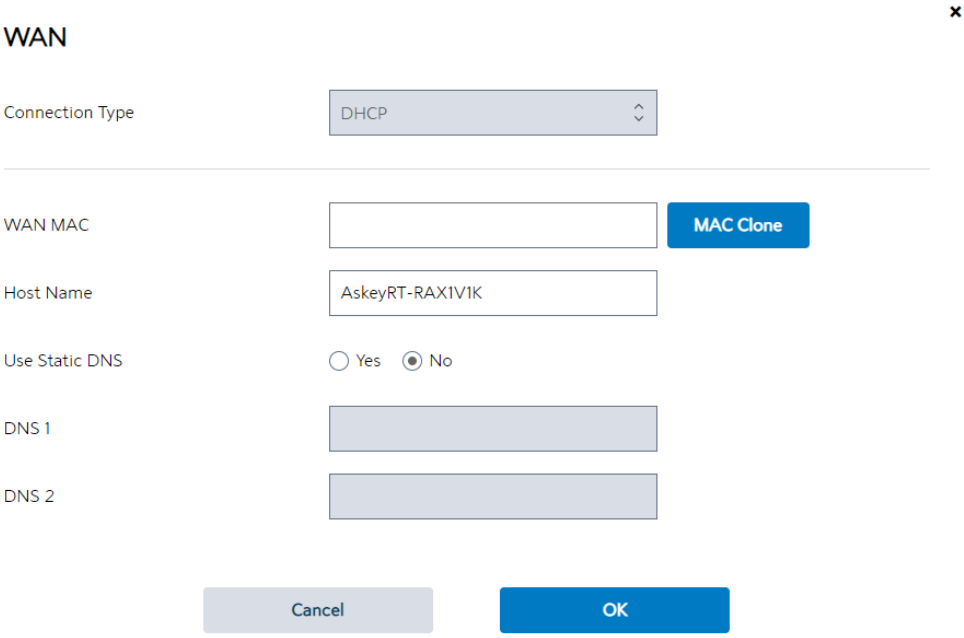
---

5. Click **OK**.

2.3.4 WAN Setup

Click **WAN** button to configure the WAN connection settings:

1. **Connection Type**: There are five options are DHCP, PPPoE, Static, PPTP and L2TP. Consult your Internet Service Provider (ISP) if To use the WPS button, follow the steps below:



2. The admin user default is **DHCP,** and cannot choose other options, below show the steps to set

   - **WAN MAC**: MAC (Media Access Control) address is a unique identifier that identifies your computer or device in the network. ISPs monitor the MAC addresses of devices that connect to their services, and would disallow Internet connection for new MAC addresses.

     To fix this issue, you can do either of the following:

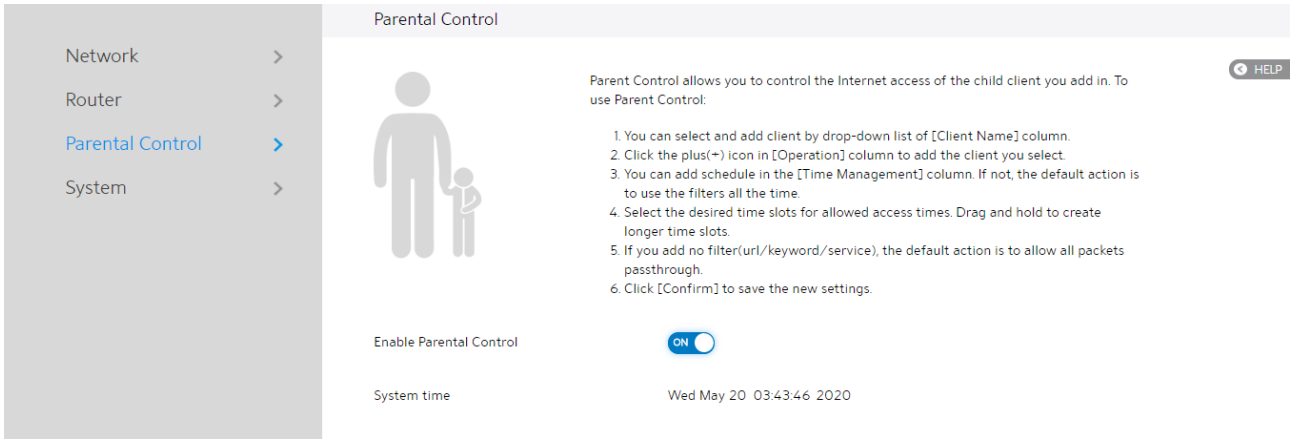
     * Contact your ISP and request to update the MAC address associated with your ISP subscription.

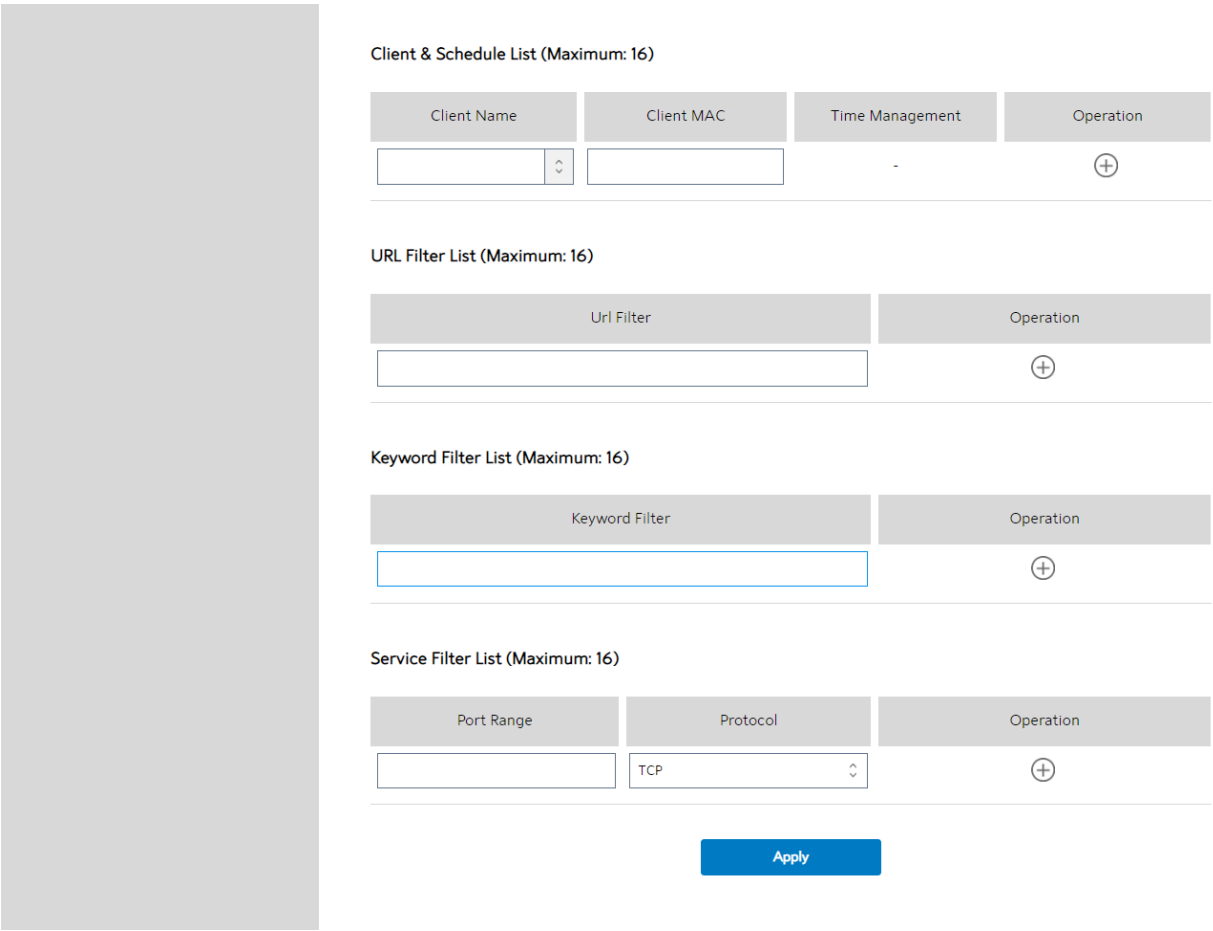
* Clone or change the MAC address of the new device to match the MAC address of the original device.

- **Host Name**: This field lets you provide a host name for WiFi Router. Usually it's provided by ISP.
- **DNS 1** & **DNS 2:** Either of them indicates IP address of a DNS server.
- Click **OK**.

2.3.5 Parental Control

Parental Control lets administrator control the Internet access of the client.





Steps to set parental control function:

1. From the navigation panel, go to **Basic** > **Parental Control.**
2. **Enable Parental Control**: Select **On** to enable parental control, Select **Off** to disable parental control.
3. **Client & Schedule List**
   - **Client Name**: Select client from the list. The name in the list stands for the client that is communicating with the WiFi Router.
   - **Client MAC**: MAC address of the selected client.

NOTE: **Client Name** just makes it easier for technician to distinguish LAN-side devices. The **Client MAC** in fact specify the device with the **Client**

Name.

- **Time Management**: Click , then setup the client's schedule timetable to allow or deny client's access to Internet.
- **Add/Delete:** Click or to add/delete the profile.

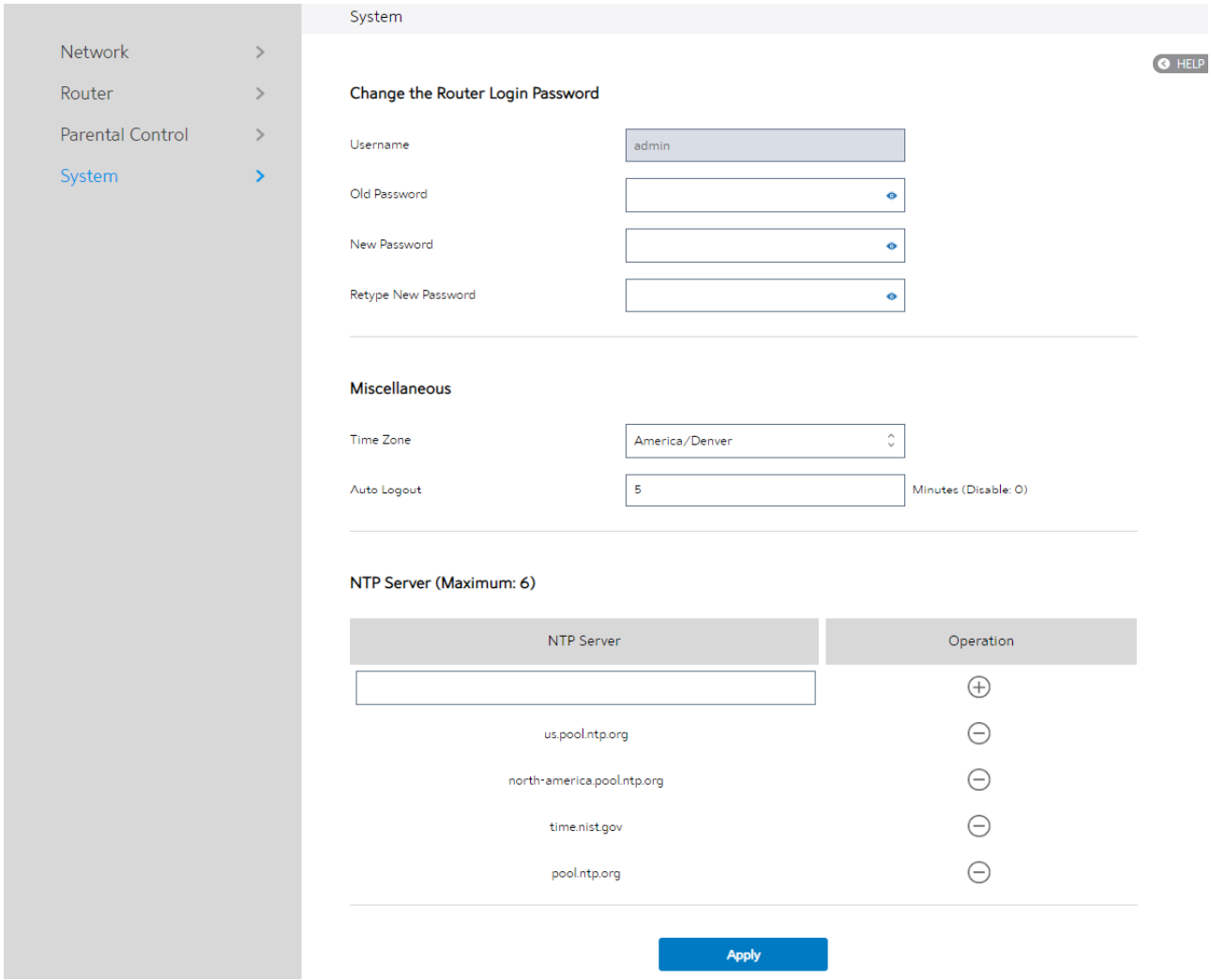
4. **URL Filter List**
   - **URL Filter List**: WiFi Router prevents LAN-side device from accessing the URL in list.
   - **URL Filter**: WEB URLs which contain the URLs defined by user. For example, the filter "abc" can filter both "www.abc.com"
   - **Add/Delete:** Click or to add/delete the profile.
5. **Keyword Filter List**
   - **Keyword Filter List**: WiFi Router prevents LAN-side device from accessing to webpages contain the keyword in list.
   - **Keyword Filter**: WEB URLs which contain the keywords defined by user. For example, the filter "abc" can filter both "www.abc.com"
   - **Add/Delete:** Click or to add/delete the profile.
6. **Service Filter List**
   - **Service Filter List**: WiFi Router prevents LAN-side device from communicating with remote device with user defined Port Range and Protocol.
   - **Port Range:** Defines the range of port in LAN side. The Port Range can be a single port like "xxxx", or a port range like "xxxx:xxxx".
   - **Protocol:** Select the type of protocol that the Service Filter will use.

- **Add/Delete:** Click ⊕ or ⊖ to add/delete the profile.

7. Click **Apply**.

2.3.6 System

This module lets user do some settings, such as changing your sign in password, selecting time-zone and adding NTP server. If you changed the password, the user password to sign in SSH will be changed.



Steps to set the System settings:

1. From the navigation panel, go to **Basic** > **System**.

2. **Username**: Name used to sign in WiFi Router.

3. **Old Password:** Password used to sign in WiFi Router.
4. **New Password**: New sign in password for WiFi Router.
5. **Retype New Password**: Retype new sign in password for WiFi Router.
6. **Time Zone**: The time zone used by default.
7. **Auto Logout**: Auto sign out after a specified period of time.
8. **NTP Server**: DNS of an NTP (Network Time Protocol) server.
9. Click **Apply**.

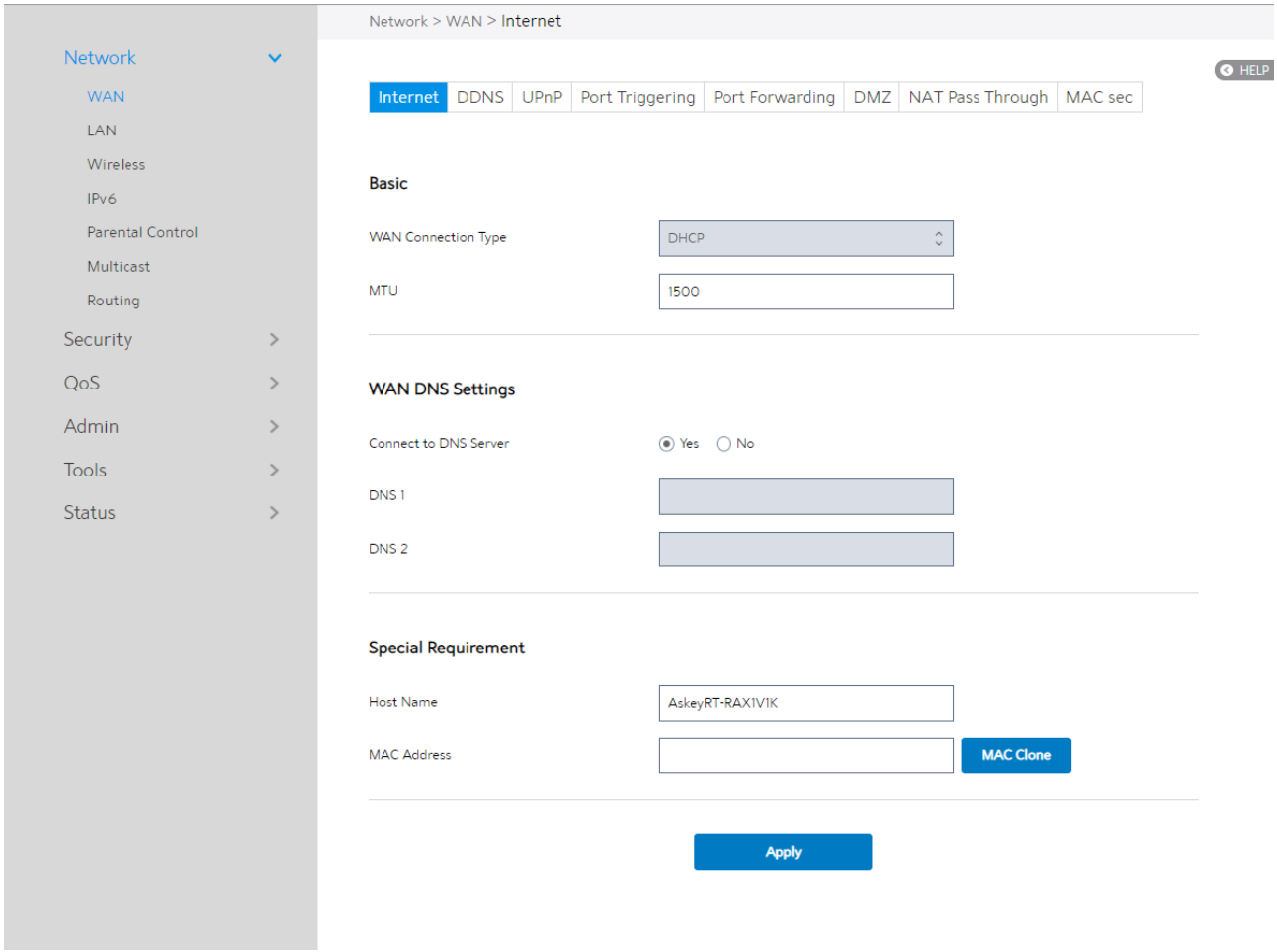
2.4 Advanced Setup

2.4.1 Network

2.4.1.1 WAN Settings

2.4.1.1.1 Internet Settings

WiFi Router supports several WAN connection types. Select the type from the WAN Connection Type dropdown menu.



Steps to configure WAN connection settings:

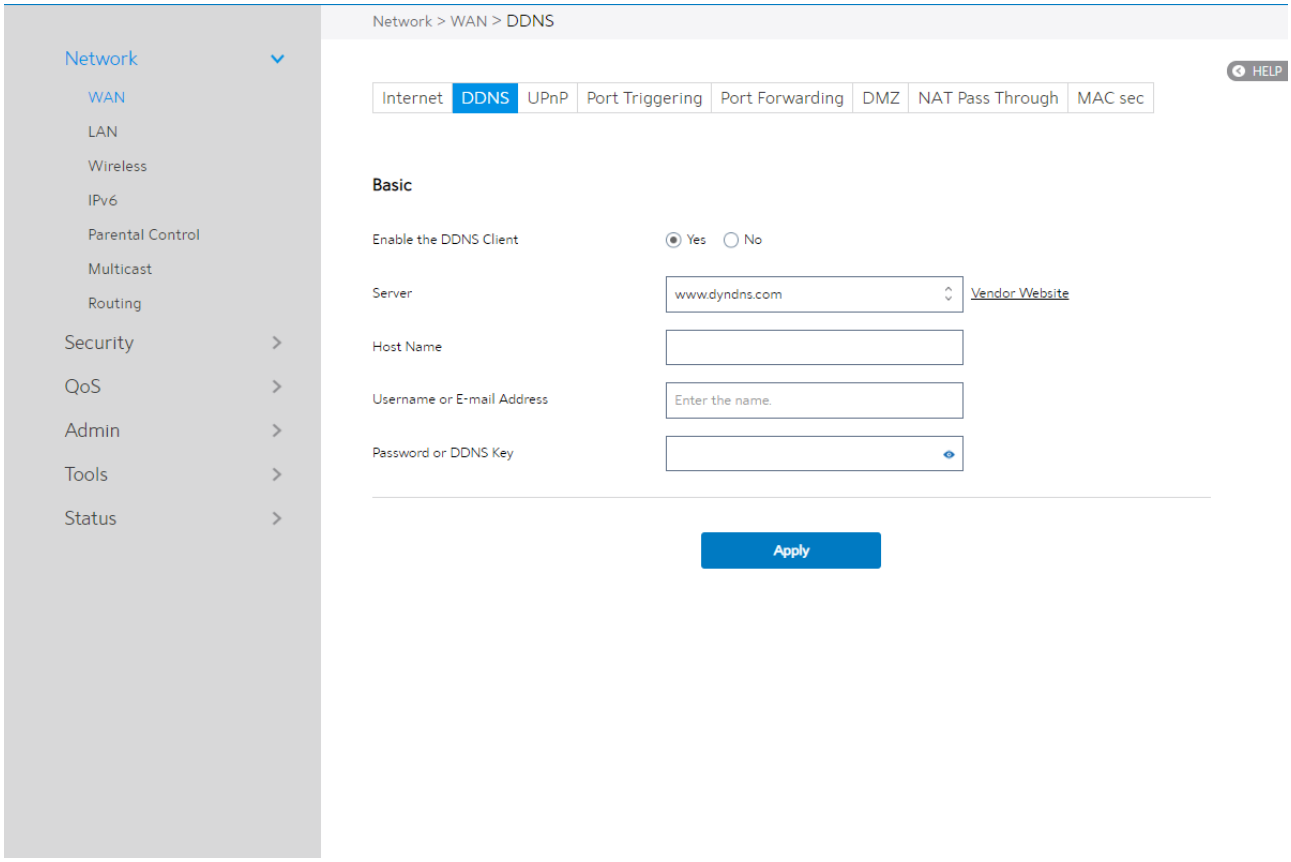
1. From the navigation panel, go to **Advanced** > **Network** > **WAN** > **Internet.**
2. **WAN Connection Type**: Choose the Internet Service Provider type. There are 5 options: **DHCP, PPPoE, Static, PPTP and L2TP**. If you are unsure which type to

select, please consult your ISP.

3. **MTU:** Maximum Transmission Unit value, which defines the maximum length of a packet.
4. **Connect to DNS Server**: Lets WiFi Router get IP address from the DNS Server automatically. DNS Server is a host on the Internet that translates Internet names to numeric IP addresses.
5. **DNS 1 & DNS 2:** Either of them indicates an IP address of a DNS server.
6. **Host Name:** This field allows you to provide a host name for your router. It is usually provided by ISP.
7. **MAC Address:** MAC address identifies a device in the network. ISPs monitor the MAC addresses of devices that connect to their services, and would disallow Internet connection for new MAC addresses. To fix this issue, you can do either of the following: * Contact your ISP and request to update the MAC address associated with your ISP subscription. * Clone or change the MAC address of the new device to match the MAC address of the original device.
8. Click **Apply**.

2.4.1.1.2 DDNS

DDNS (Dynamic DNS）allows administrator to get access to WiFi Router, even though it’s working within a local network.



Steps to set up DDNS:

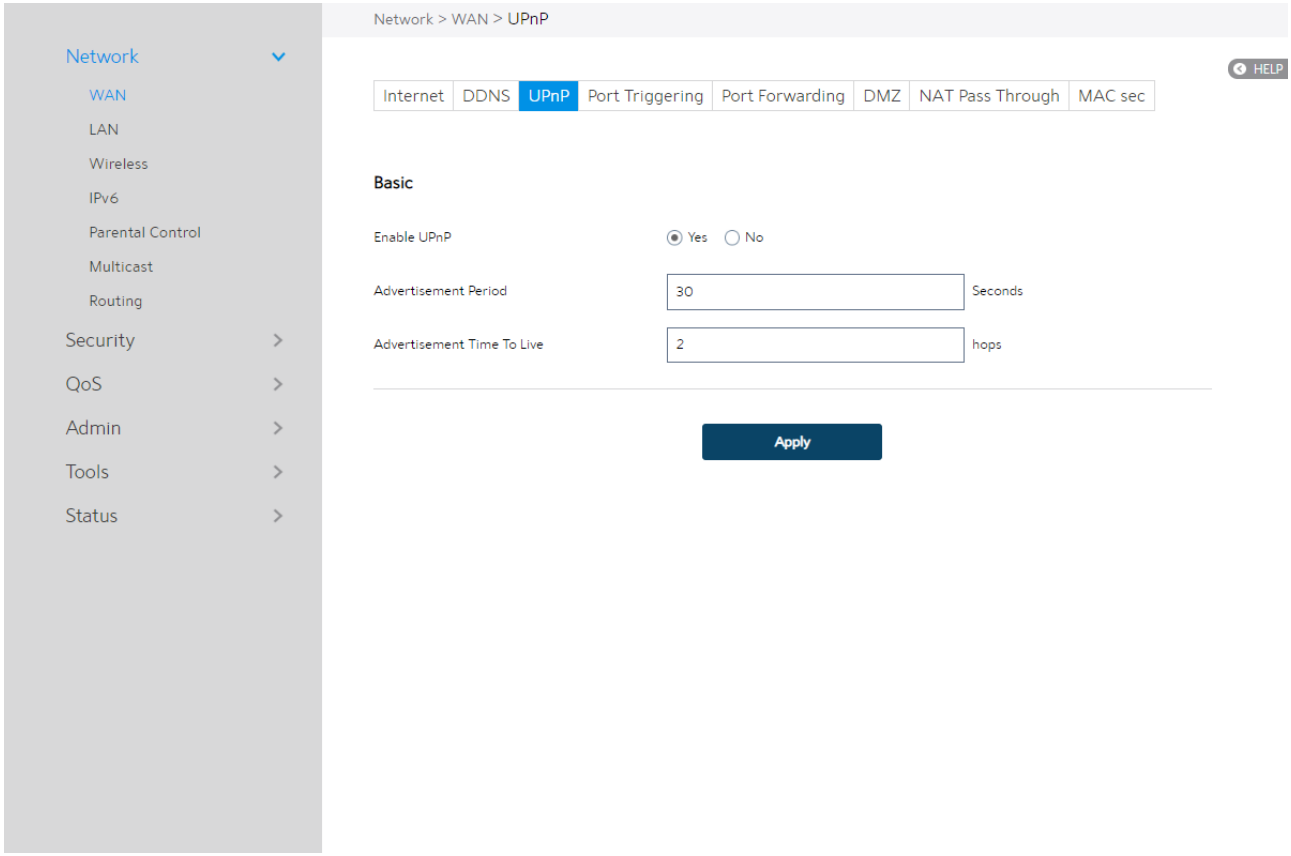
1. From the navigation panel, go to **Advanced > Network > WAN > DDNS.**
2. **Enable the DDNS Client**: **Yes** means enable DDNS function, **No** means disable DDNS function.
3. **Server**: Select supported DDNS service provider's URL from the list.
4. **Host Name**: URL that has been registered in the specified Vendor.
5. **Username or E-mail Address**: Username or email address which has been registered in the specified vendor.
6. **Password or DDNS Key**: Password which has been registered in the specified vendor.
7. Click **Apply**.

NOTES: DDNS service will not work properly under these conditions:

- When the WiFi Router is using a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x), as indicated by yellow text.
- The WiFi Router works on a network who uses multiple NAT tables.

2.4.1.1.3 UPnP

UPnP (Universal Plug and Play) let devices (such as routers, televisions, stereo systems) be controlled via an IP-based network with or without a central control unit. Under the help of UPnP, one device can be discovered once it has connected to network, then device can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, UPnP automatically configures the WiFi Router to accept incoming connections and direct requests to a specific PC on the local network.



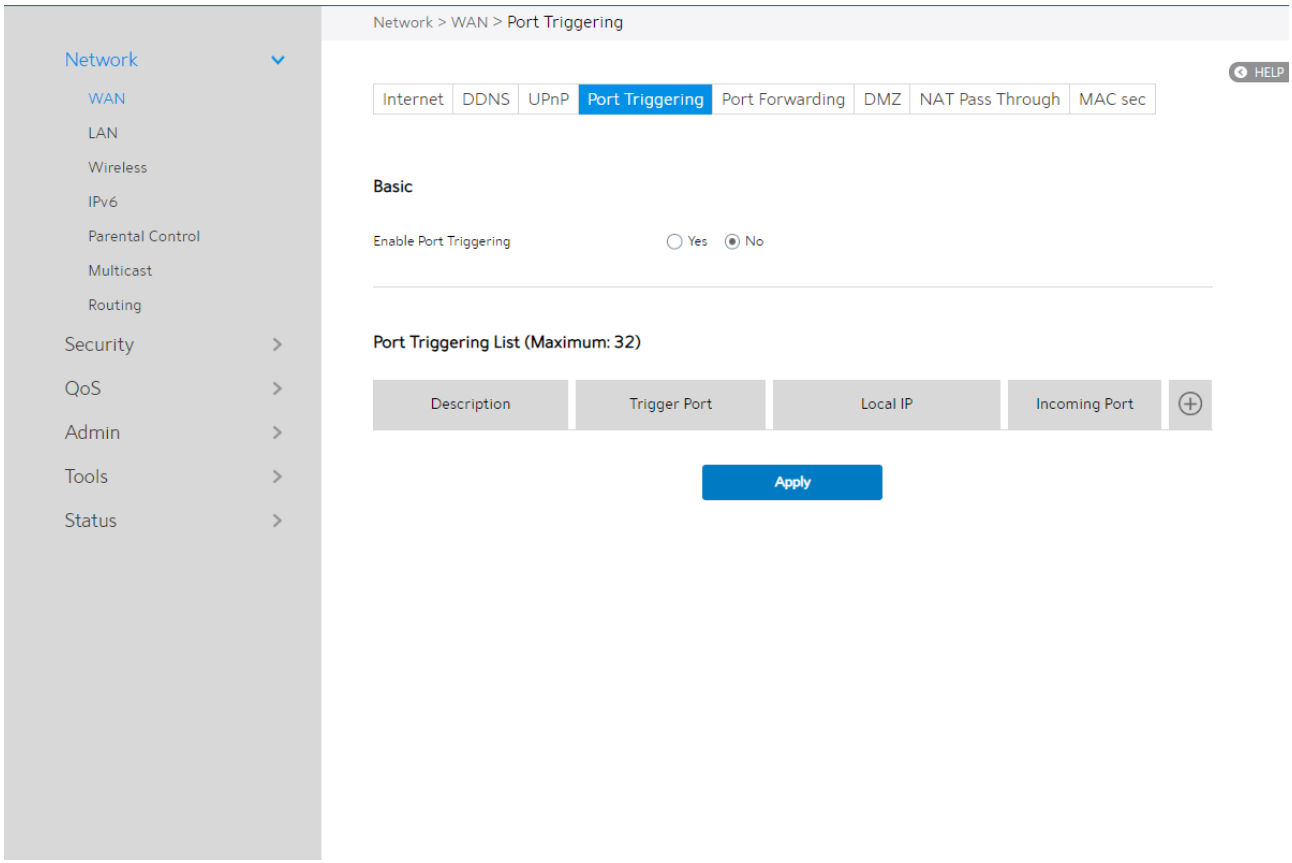
Steps to set up UPnP：

1. From the navigation panel, go to **Advanced > Network > WAN > UPnP**.
2. **Enable UPnP**: **Yes** means enable UPnP and **No** means disable it.
3. **Advertisement Period**: WiFi Router will broadcast its UPnP information to all devices every advertisement-period second.
4. **Advertisement Time To Live**: Number of hops that an advertisement will be transmitted.
5. Click Apply.

2.4.1.1.4 Port Triggering

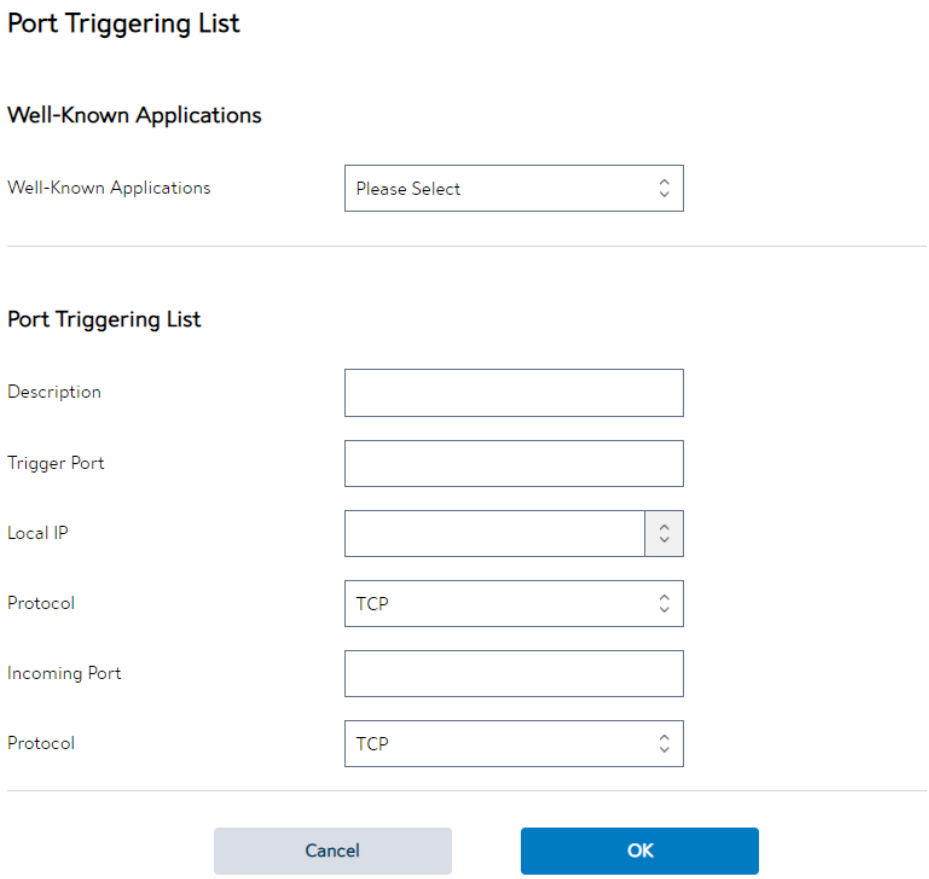
Port triggering mechanism forwards the packets from the **Incoming Port** to the local

client when the local client makes an outgoing connection through a predetermined port/port range (**Triggering Port**).



Steps to set up Port Triggering:

1. From the navigation panel, go to **Advanced > Network > WAN > Port Triggering**.
2. **Enable Port Triggering**: Check to enable or disable Port Triggering.



3. **Well-Known Applications**: Select popular games and web services to add to the Port Triggering List.
4. **Description**: A brief description for application.
5. **Triggering Port**: When there is incoming data from LAN-side application to this port, the **Port Triggering** mechanism will be activated.
6. **Local IP**: Local host's IP address.
7. **Protocol**: Select the type of protocol that the application will use.
8. **Incoming Port**: Defines the range of port. After Port triggering mechanism has been activated, the data from port within this range will be forwarded to the corresponding port of the application which has activated Port triggering mechanism.

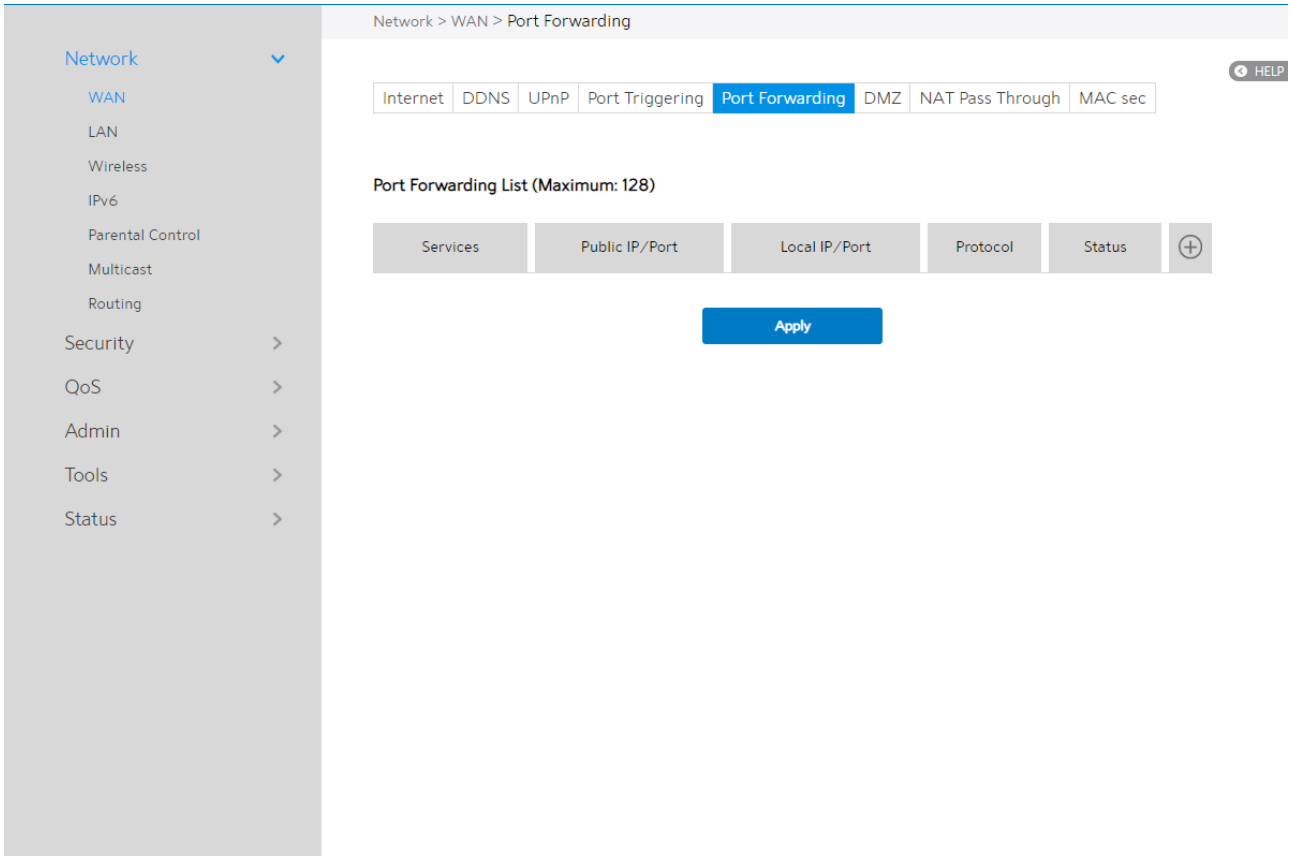
9. **Operation**: Add, Edit or Delete operation for this item.

10. Click **Apply**.

NOTE: Triggering Port element in the list is regarded as a triggering, that's to say when data comes to this port, the Port Triggering mechanism will be activated.

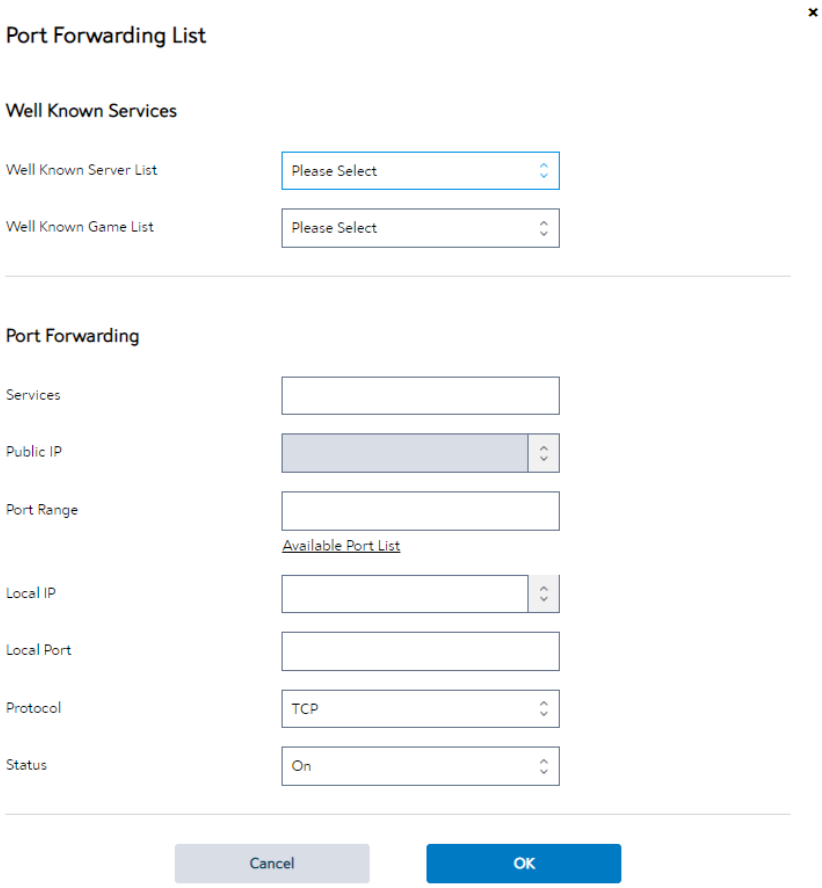
2.4.1.1.5 Port Forwarding

Port forwarding lets remote computers access a specific service within a LAN-side network. It can redirect a network request from one address/ports (**Public IP/Port**) to another (**Local IP/Port**).



Steps to set up Port Forwarding:

1. From the navigation panel, go to **Advanced> Network> WAN>Port Forwarding**.
2. Click the Add button to add the port forwarding rules.



3. **Well Known Server List**: Select a pre-defined Server list from the drop-down menu and the Port Forwarding List will be auto-filled.
4. **Well Known Game List**: Select a game from the Server list and the Port Forwarding List will be auto-filled.
5. **Services**: A short description about this service.
6. **Public IP**: IP address of WAN Port.
7. **Port Range**: Defines the range of port in WAN side.

NOTE: A network makes use of ports in order to exchange data, with each port assigned a port number and a specific task. For example, port 80 is used for HTTP. A specific port can only be used by one application or service at a time. Hence, two PCs attempting to access data through the same port at the same time would fail. For example, you cannot set up Port Forwarding for port 100 for two PCs at the same time.

8. **Local IP**: The client's LAN IP address.
9. **Local Port**: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
10. **Protocol**: The required protocol. Refer to the documentation for the service that you are hosting.
11. **Status**: the status of this rule, on or off.
12. Click **OK**.

Steps to check whether Port Forwarding module has been activated successfully:

- Ensure that your server or application is set up and running.
- You will need a client outside your LAN which has Internet access (referred to as "Internet client"). This client should not be connected to the WiFi Router.
- On the Internet client, use the WiFi Router's WAN IP to access the server. If port forwarding has been successful, you should be able to access available/specified

files or applications.

Differences between port triggering and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the WiFi Router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering lets multiple computers run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the triggering port.

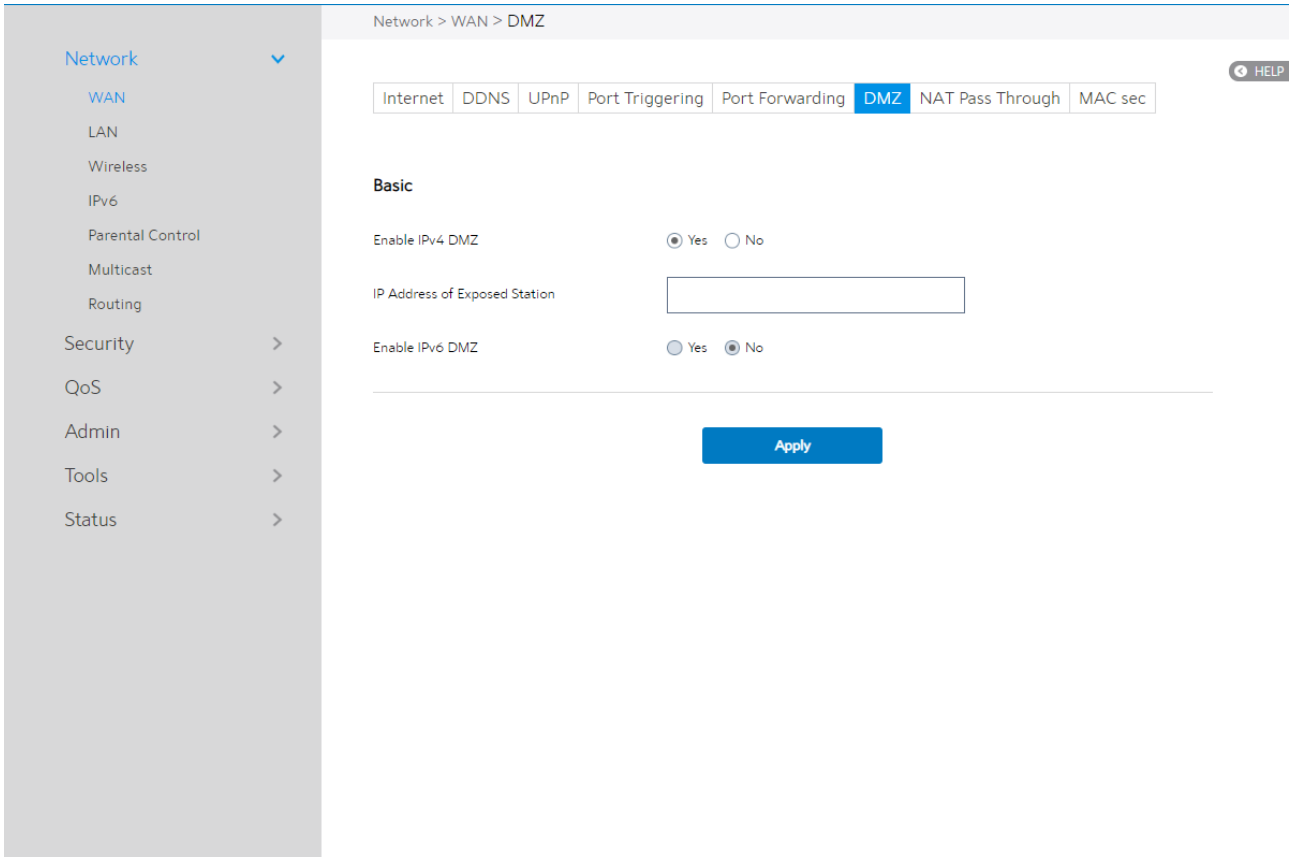
2.4.1.1.6 DMZ

Virtual DMZ module exposes one client to the Internet, allowing this client to receive all inbound packets directed to a Local Area Network. For IPv4, inbound traffic from the Internet is usually discarded and routed to a specific client only if port forwarding or a port trigger has been configured on the network. For IPv6, inbound traffic from the Internet is usually discarded and routed to a specific client address or a prefix only the ipv6 firewall have the rules to let them in. In a DMZ configuration, one network client receives all inbound packets.

CAUTION: Opening all of the client’s ports to Internet makes the network

---

vulnerable to outside attacks. Please be aware of the security risks involved in using DMZ.



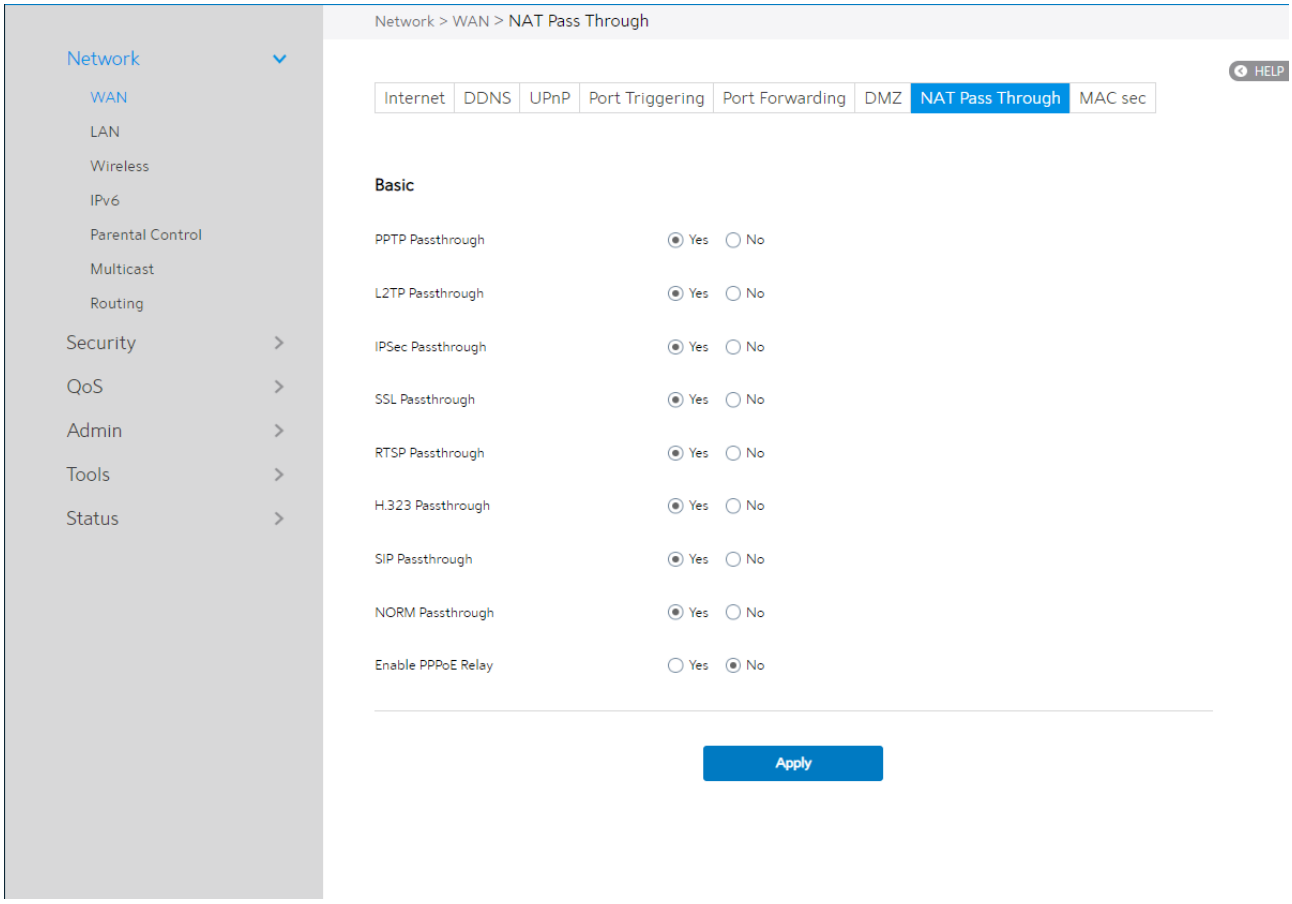
Steps to set up DMZ:

1. From the navigation panel, go to **Advanced** > **Network** > **WAN** > **DMZ.**
2. **Enable IPv4 DMZ**: Check to enable or disable DMZ.
3. **IP Address of Exposed Station**: LAN IP address of a client who can provide DMZ service. This makes the device with this IP address expose to Internet. Make sure that the server client has a static IP address.
4. **Enable IPv6 DMZ**: Check to enable or disable IPv6 DMZ.
5. **IPv6 Address of Exposed Station**: The client's LAN IPv6 address that will provide the DMZ service and be exposed on the Internet.

6. **IPv6 prefix for DMZ setting**: The IPv6 DMZ address must be in the range of IPv6 prefix. Show it for user to set valid DMZ address.
7. Click **Apply**.

2.4.1.1.7 NAT Pass Through

NAT Pass Through lets a Virtual Private Network (VPN) connection pass through the WiFi Router to the network server.



Steps to set up NAT Pass Through:

1. To configure NAT Pass Through settings, go to **Advanced** > **Network** > **WAN** > **NAT Pass Through.**
2. **PPTP Passthrough**: Enable or disable. Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks.
3. **L2TP Passthrough**: Enable or disable. In computer networking, Layer 2 Tunneling

Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself.

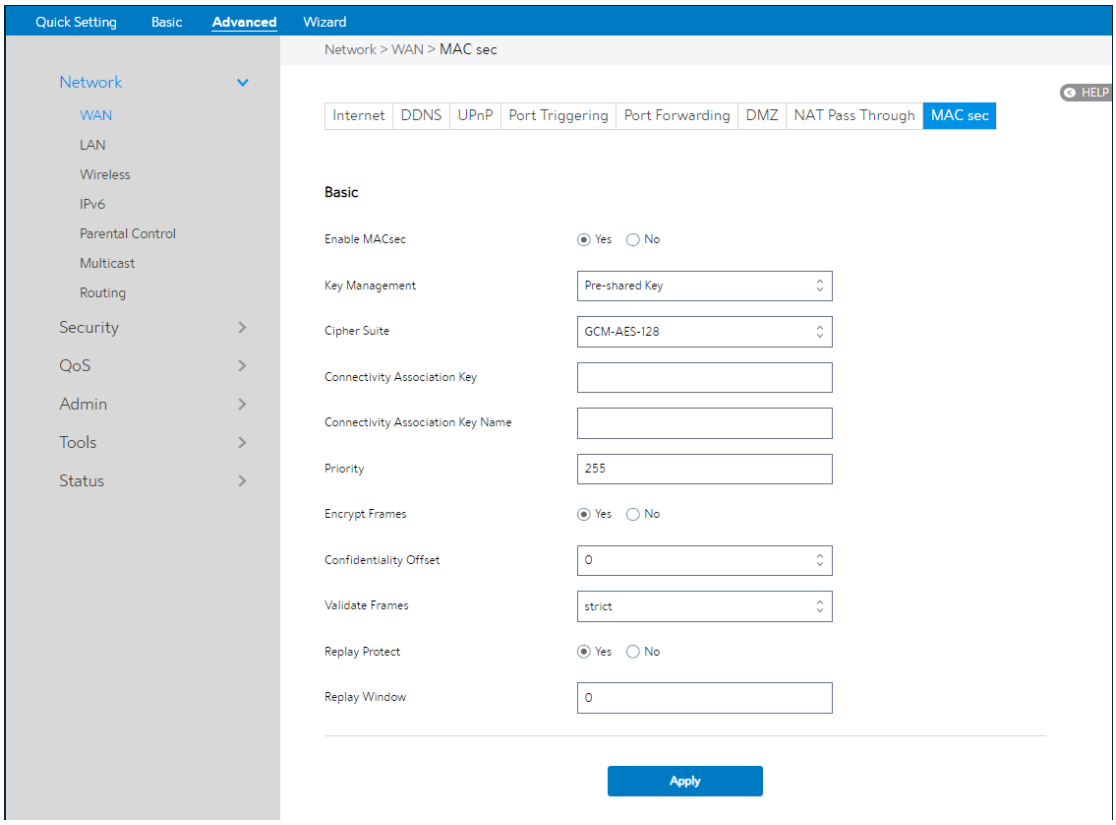
4. **IPSec Passthrough**: Enable or disable. Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
5. **SSL Passthrough**: Secure Sockets Layer (SSL) is cryptographic protocols that provide communications security over a computer network.
6. **RTSP Passthrough**: Enable or disable. The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.
7. **H.323 Passthrough**: Enable or disable. H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network.
8. **SIP Passthrough**: Enable or disable. The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging all over Internet Protocol (IP) networks.
9. **NORM Passthrough**: Enable or disable. NACK-Oriented Reliable Multicast (NORM) Transport Protocol, which is able to provide end-to-end reliable transport of bulk data objects or streams over generic IP multicast routing and forwarding services.

10. **Enable PPPoE Relay**: PPPoE relay lets devices in LAN establish an individual PPPoE connection that passes through NAT.

11. When done, click **Apply**.

2.4.1.1.8 MACsec

The basic configuration of MACsec:



Steps to set up MACsec:

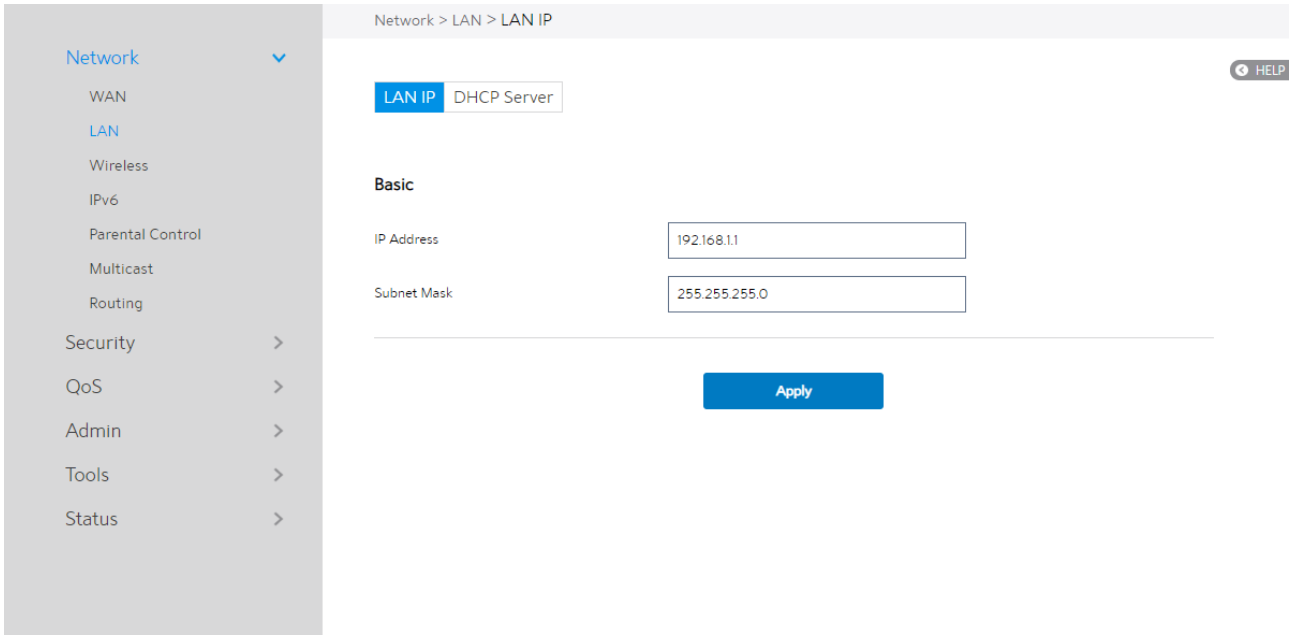
1. From the navigation panel, go to **Advanced** > **Network** > **WAN** > **MACsec**
2. **Enable MACsec: Yes** means enable MACsec function, **No** means disable MACsec function.
3. **Key Management:** Select the key management protocol of Macsec.
4. **Cipher Suite:** Select the cipher suite of Macsec.
5. **Connectivity Association Key:** Set the pre-shared Connectivity Association Key(CAK).

6. **Connectivity Association Key Name:** Set the pre-shared Connectivity Association Key Name(CKN).
7. **Priority:** The priority of MACsec.
8. **Encrypt Frames: Yes** means Open Encrypt Frames, **No** means close Encrypt Frames.
9. **Confidentiality Offset:** Select the MACsec confidentiality offset.
10. **Validate Frames:** The validate frames mode of MACsec.
11. **Replay Protect: Yes** means enable replay protect of MACsec, **No** means disable replay protect of MACsec.
12. **Replay Window:** Set the replay protection window size of MACsec

2.4.1.2 LAN Settings

2.4.1.2.1 LAN

The LAN IP module lets administrator modify LAN-side IP address of the router.



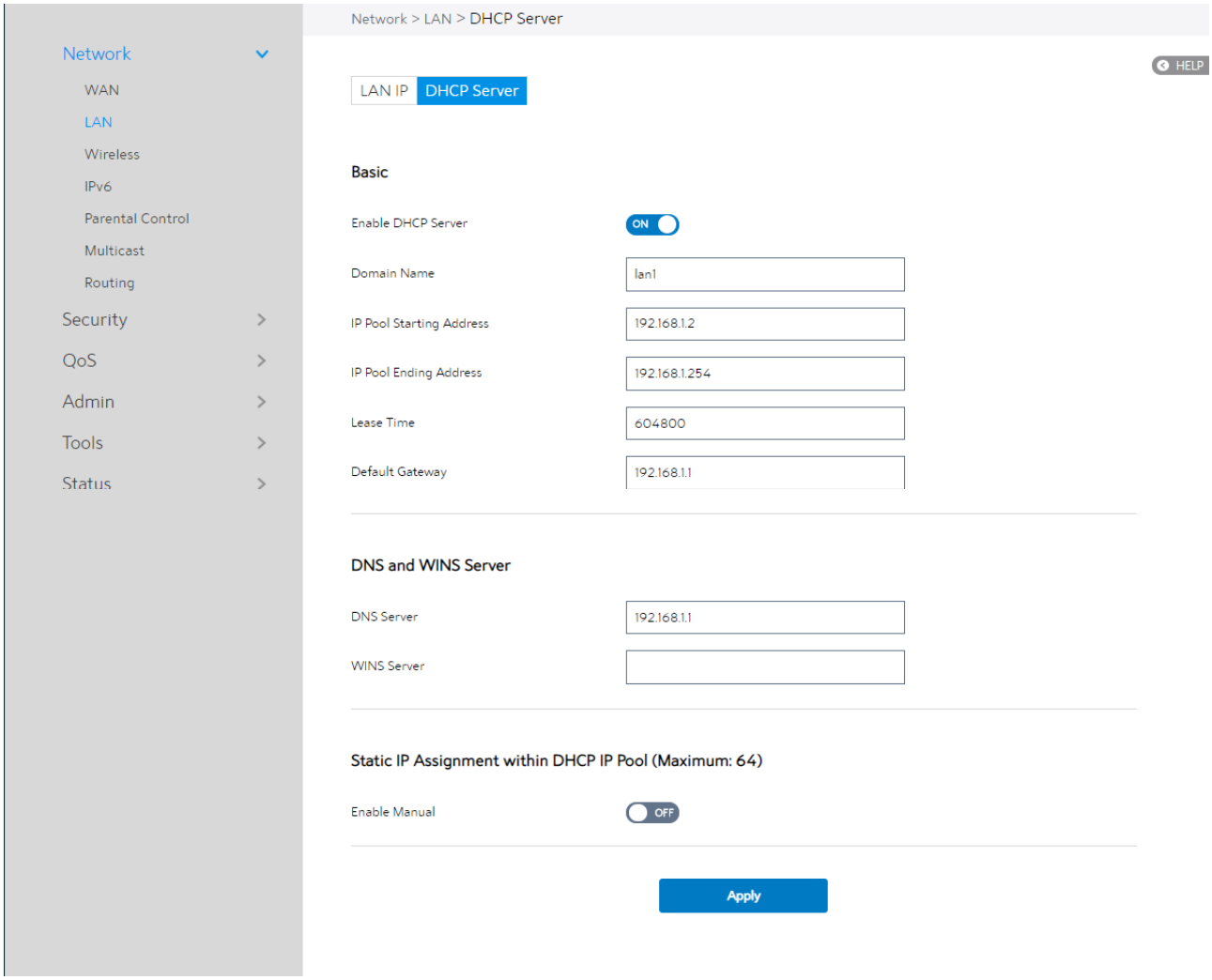
Steps to modify the LAN IP settings:

1. From the navigation panel, go to **Advanced > Network > LAN > LAN IP.**
2. **IP Address**: The LAN IP address of WiFi Router. The default value is 192.168.1.1. In IP-based networks, data packets are sent to the network devices' specific IP addresses.
3. **Subnet Mask**: The LAN subnet mask of WiFi Router. Its default value is **255.255.255.0**
4. Click **Apply.**

NOTE: Any change to the LAN IP module will affect router’s DHCP settings.

2.3.1.2.2 DHCP Server

DHCP server can assign each client an IP address and informs the client of DNS server's IP, default gateway's IP and etc. This WiFi Router can allocate up to 253 IP addresses for LAN-side devices.



Steps to configure the DHCP server:

1. From the navigation panel, go to **Advanced** > **Network** > **LAN** > **DHCP Server**.
2. **Enable DHCP Server**: Enable DHCP server function which lets WiFi Router act as a DHCP server to automatically assign IP addresses to network clients. If this function is disabled, administrator has to manually set LAN devices.

3. **Domain Name**: Domain Name for clients who request IP Address from DHCP Server. This field only contains alphanumeric characters and dash symbols.
4. **IP Pool Starting Address**: Starting address that can be allocated to LAN-side devices.
5. **IP Pool Ending Address**: Ending address that can be allocated to LAN-side devices.
6. **Lease Time**: Defines the time that LAN-side devices can use the assigned IP address. When the lease time expires, the network client will either send renew or rebind message to a DHCP server.
7. **Default Gateway**: IP address of the gateway for LAN.
8. **DNS Server**: IP address of a DNS server. DNS Server is used to resolve a DNS into a numerical IP Address. By default, the WiFi Router will act as a DNS server.
9. **WINS Server**: Windows Internet Naming Service manages interactions of each PC with the Internet. If you use a WINS server, enter the IP Address of server here.
10. **Enable Manual**: Assign fixed IP address for clients.
11. **MAC**: MAC address of LAN-side device.
12. **IP**: IP address within DHCP IP Pool for LAN-side device.
13. **Add/Delete**: Add/Delete static IP.
14. Click **Apply.**

NOTES:

• We recommend that administrator use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when

---

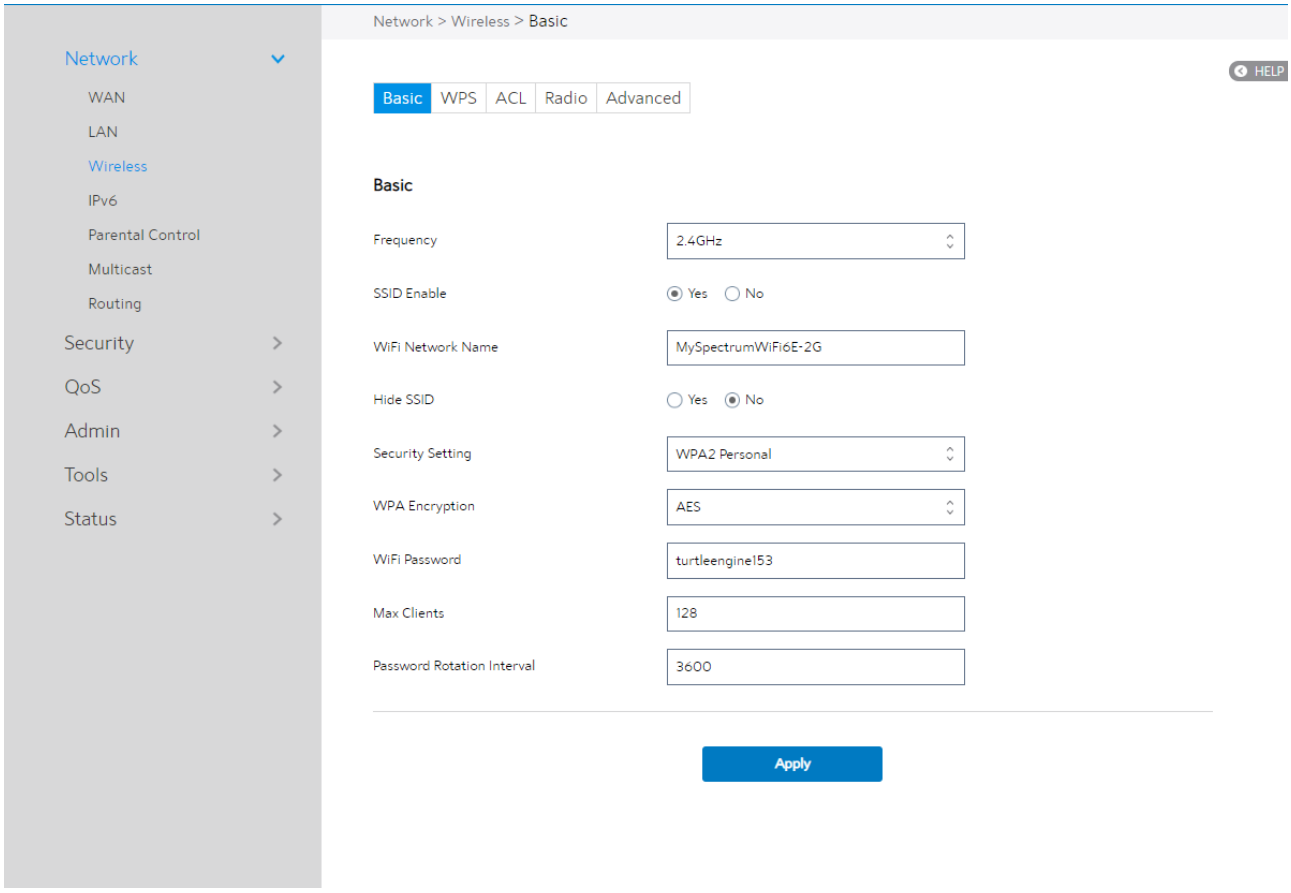
specifying an IP address range.

- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.

2.4.1.3 Wireless

2.4.1.3.1 Basic

Basic settings allow you to set up the basic wireless settings.



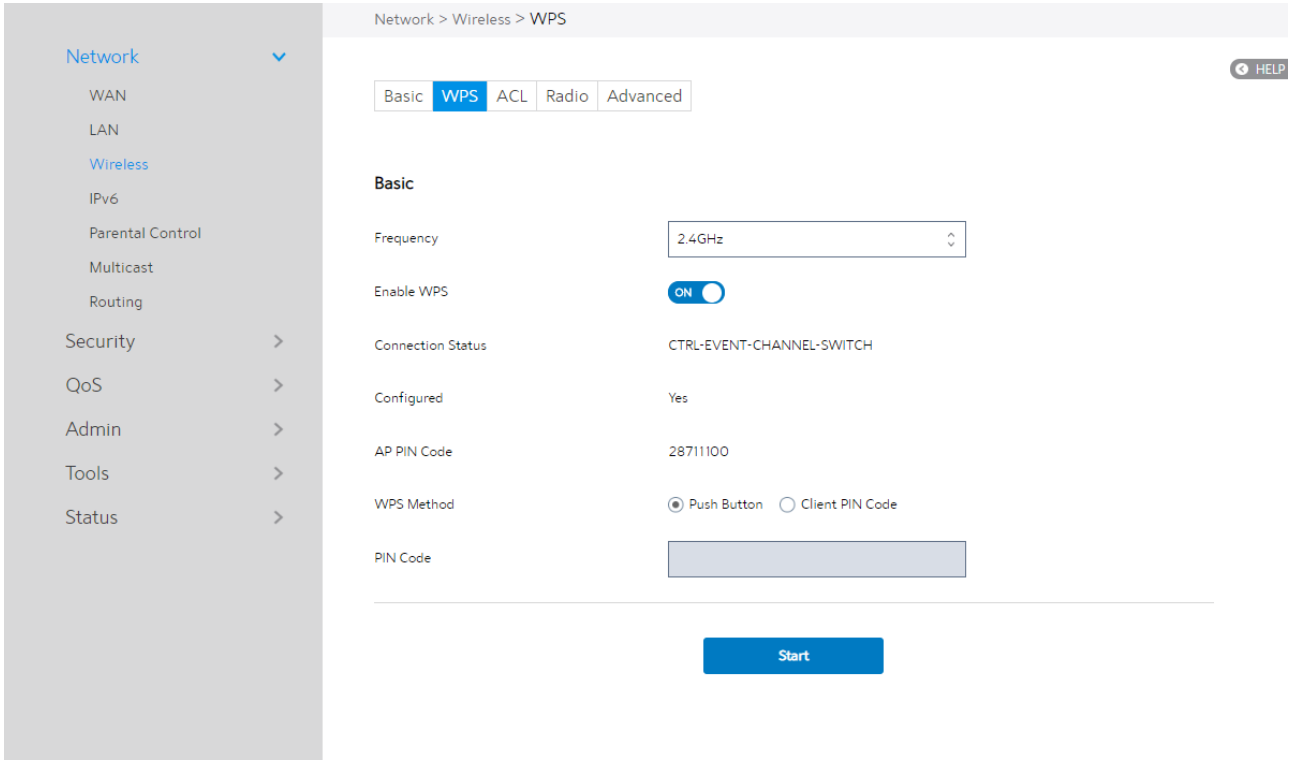
Steps to set up the basic wireless settings:

1. From the navigation panel, go to **Advanced** > **Network** > **Wireless** > **Basic.**
2. **Frequency**: Select the frequency band to configure.
3. **SSID Enable**: Switch the SSID on/off (enable/disable).

4. **WiFi Network Name**: A name whose length is less than 32 characters is used to identify a wireless network. WiFi devices automatically detect all networks within its communication range.
5. **Hide SSID**: If [**Yes**] is selected, network name (SSID) does not show in site surveys by wireless mobile clients and they can only connect to WiFi Router by manually entering network name (SSID).
6. **Security Setting**: This field enables authentication methods for wireless clients.
7. **WPA Encryption**: Enable WPA Encryption to encrypt data.
8. **WiFi Password**: Requires a password of 8-63 characters (letters, numbers or a combination) or 8 - 64 hex digits to start the encryption process.
9. **Protected Management Frames**: Protected Management Frames is a feature to protect some types of management frames like deauthorization, disassociation and action frames.
10. **Max Clients**: The maximum number of clients allowed.
11. **Password Rotation Interval**: This field specifies the interval (in seconds) after which a WPA group password is changed. Enter [0] (zero) to indicate that a periodic key-change is not required. Please input the value between 600 to 86400 (seconds).
12. Click **Apply**.

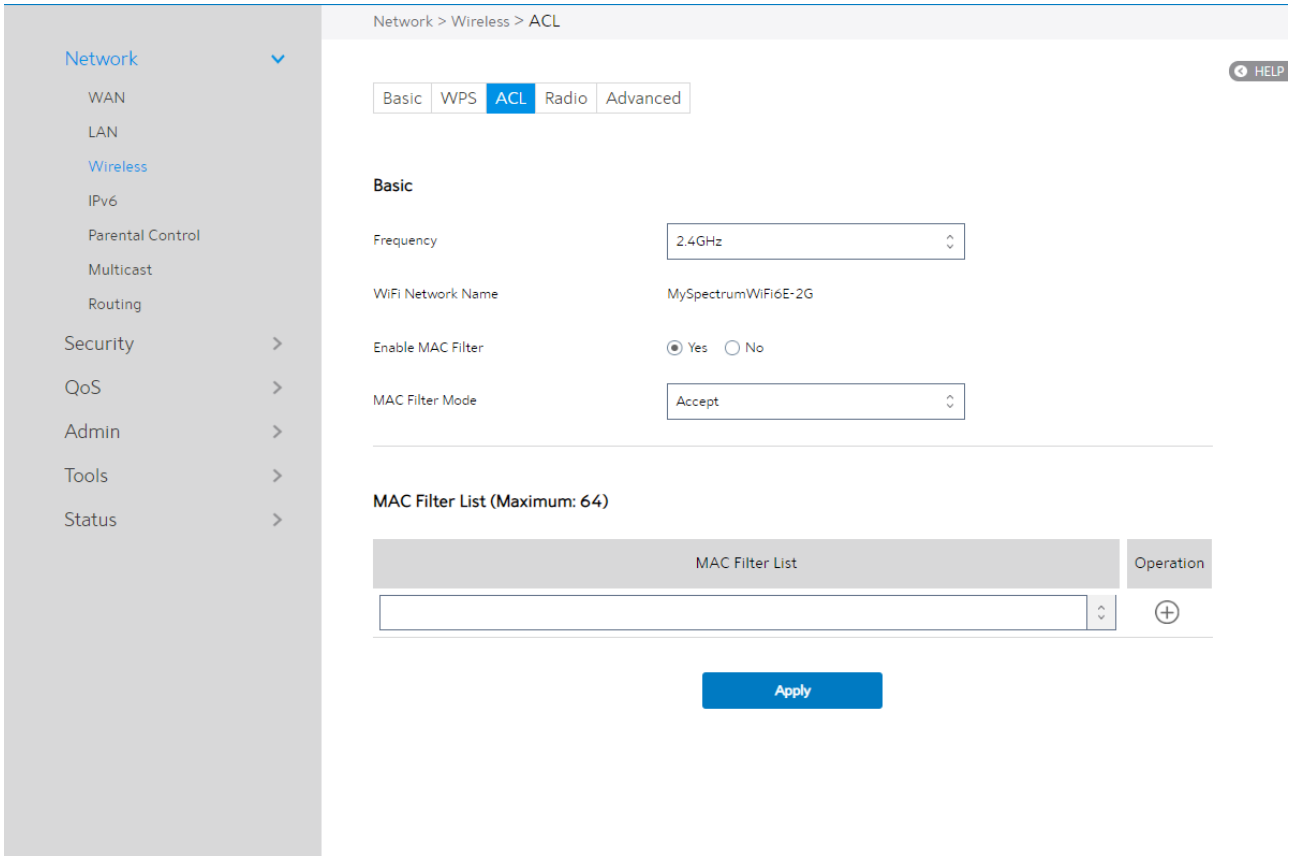
2.4.1.3.2 WPS

WPS (WiFi Protected Setup) is a wireless security standard that lets you easily connect devices to a wireless network. You can trigger the WPS function via the PIN code or WPS button. Reference 2.3.2 WPS Setup



2.4.1.3.3 ACL

ACL can be used to allow or disallow one device to associate to the AP/ Router.



Steps to set up the ACL:

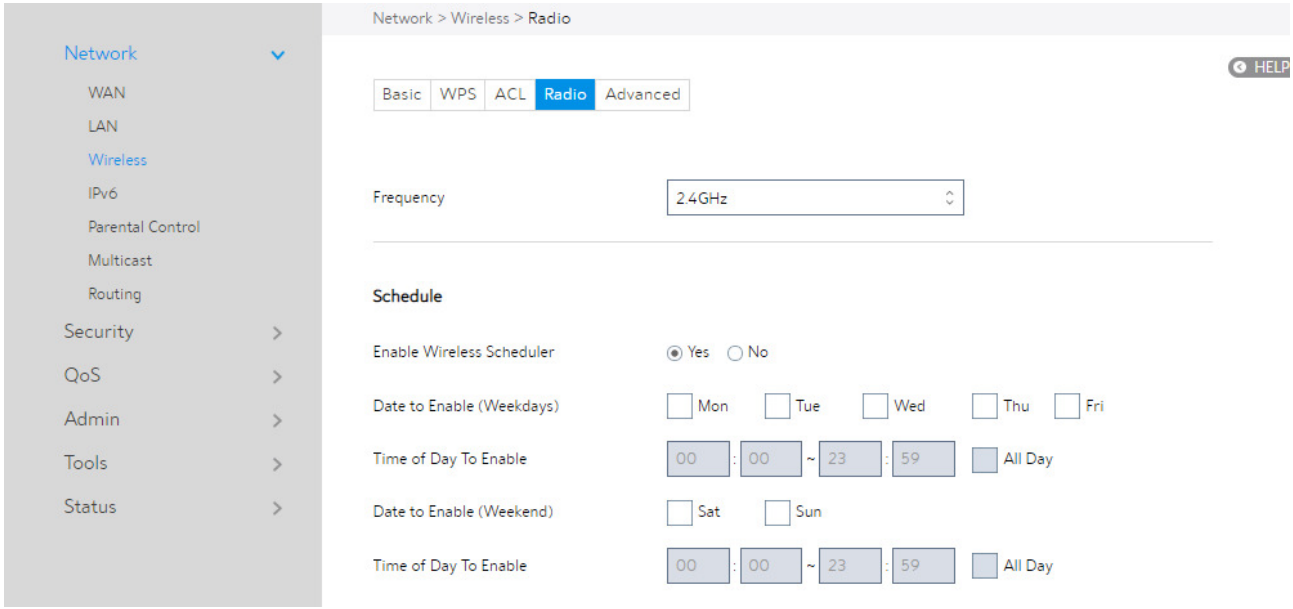
1. From the navigation panel, go to **Advanced** > **Network** > **Wireless** > **ACL**.
2. **Frequency:** In the frequency field, select the frequency band that you want to use for the ACL settings.
3. **WiFi Network Name**: A name whose length is less than 32 characters is used to identify a wireless network.
4. **Enable MAC Filter**: Enable MAC filter or disable.
5. **MAC Filter Mode**: Select **Accept** to allow devices in the MAC filter list to associate to the AP/ Router, select **Reject** to prevent devices in the MAC filter list from

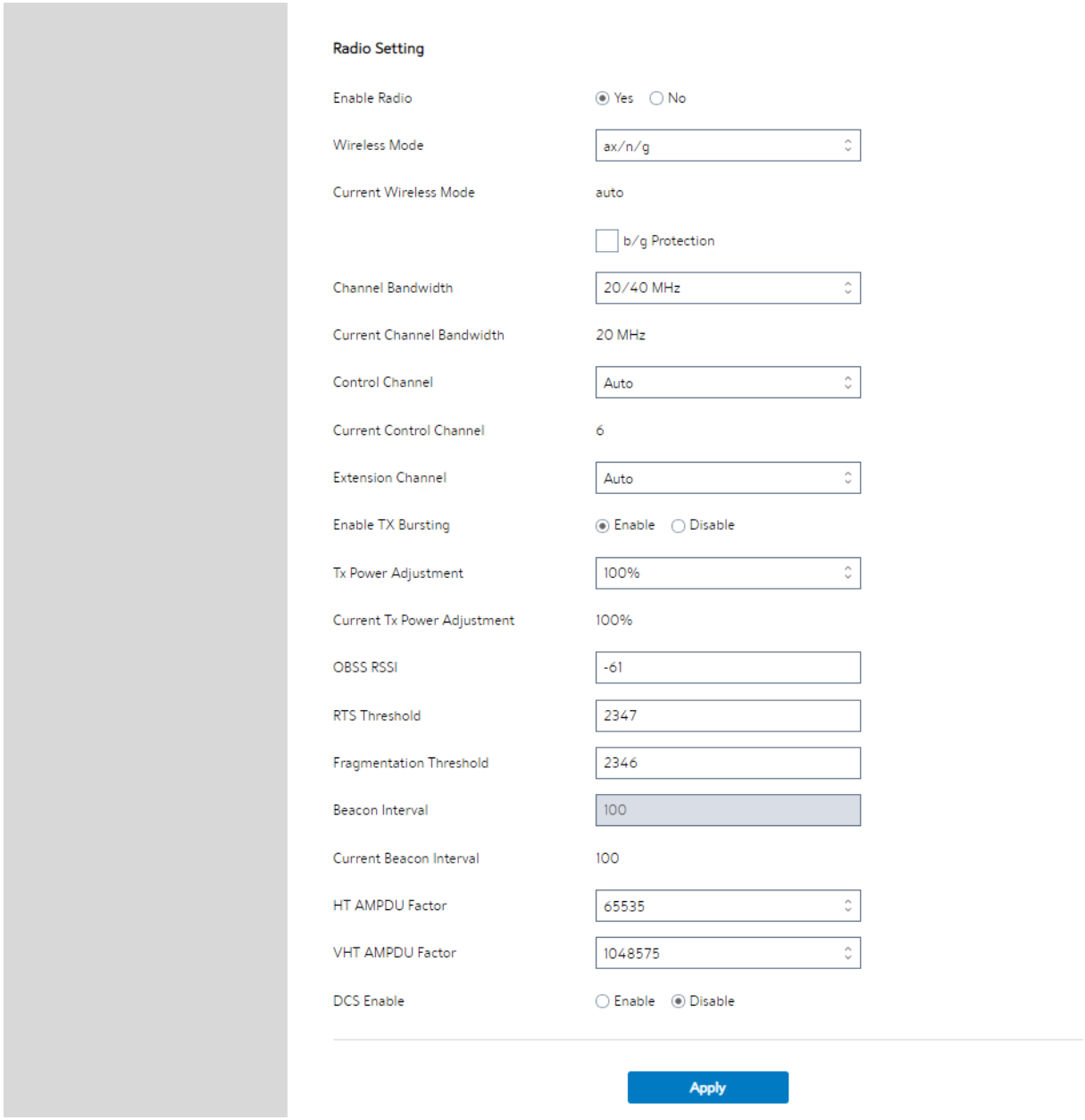
associating to the AP /Router.

6. **MAC Filter List**: Enter the MAC address of the wireless device. MAC filtering lets users either limit specific MAC addresses from associating with the AP/Router, or specifically indicates which MAC addresses can associate with the AP/Router.
7. When done, click **Apply**.

2.4.1.3.4 Radio

Administrator can set some advanced feature for radio of the WiFi Router.





Steps to set Radio:

1. From the navigation panel, go to **Advanced** > **Network** > **Wireless** > **Radio**.
2. **Frequency:** Selecting the frequency band that the WiFi Router is running.
3. **Enable Wireless Scheduler**: Switch wireless schedule on or not.
4. **Date to Enable (Weekdays)**: Select weekdays to enable Wi-Fi.
5. **Time of Day To Enable**: Set weekday time to enable Wi-Fi.

6. **Date to Enable (Weekend)**: Select weekend days to enable Wi-Fi.
7. **Time of Day To Enable**: Set weekend time to enable Wi-Fi.
8. **Enable Radio**: Select "**Yes**" or "No" to enable/disable wireless radio (wireless network).
9. **Wireless Mode**: Select a Wireless Mode of your 802.11 interface.
10. **Current Wireless Mode:** The Mode is to represent the current state.
11. **Channel Bandwidth:** Sets manual channel bandwidth.
12. **Current Channel Bandwidth:** This mode represents the current state.
13. **Control Channel**: The radio channel for wireless connection operation.
14. **Current Control Channel:** This mode represents the current state.
15. **Extension Channel**: Extension (Secondary) channel is above/below the control (Primary) channel.
16. **Enable TX Bursting**: TX Bursting improves transmission speed between WiFi Router and 802.11 devices.
17. **Tx Power Adjustment**: Set the capability for transmission power. The maximum value is 100%. You can save power and increase security if you don't require full wireless range.
18. **Current Tx Power Adjustment**: This mode represents the current state.

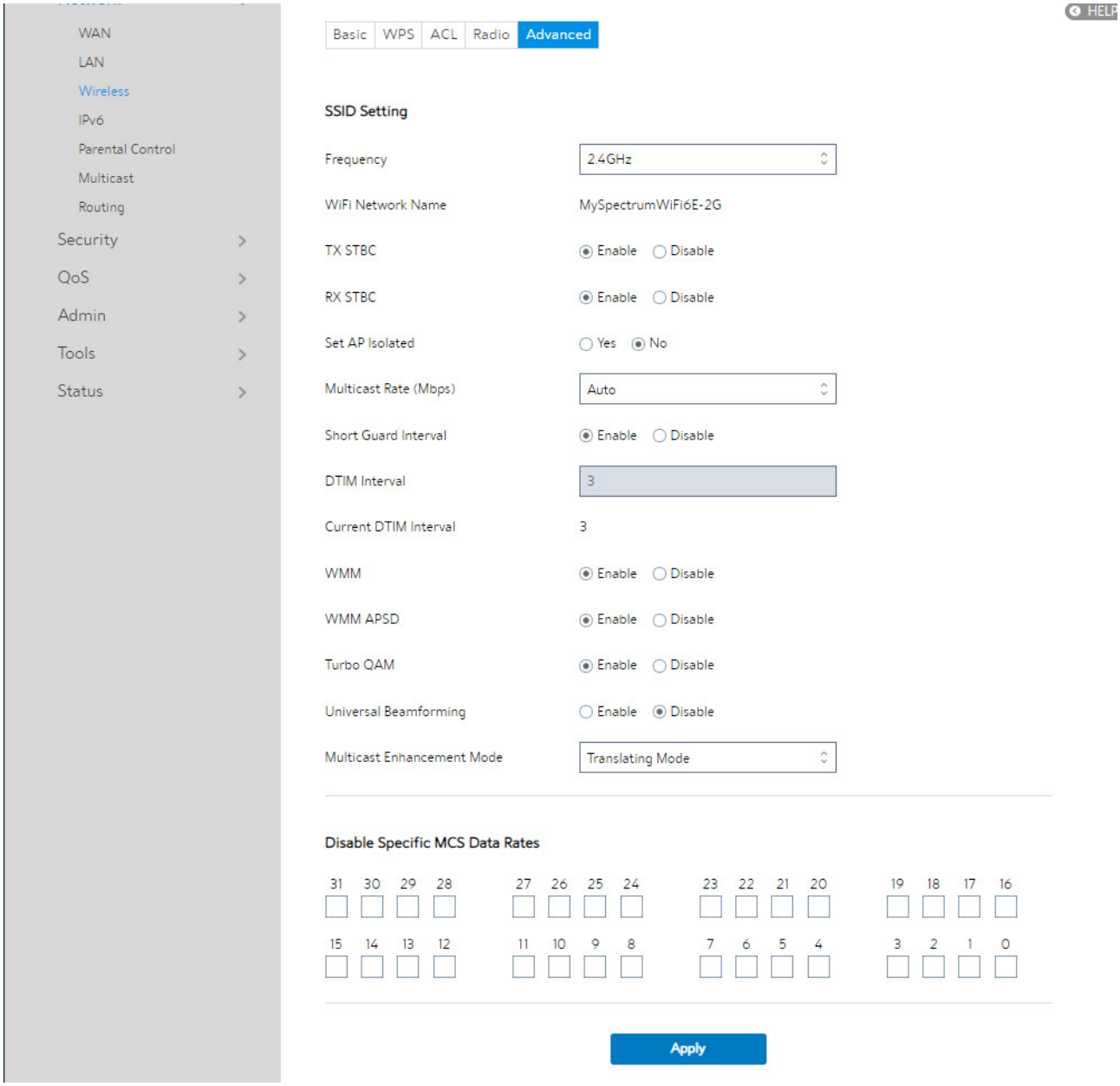
NOTE: Increasing the Transmission Power adjustment values may affect the stability of the wireless network.

---

19. **OBSS RSSI**: Configure OBSS RSSI threshold. If OBSS RSSI is greater than configured value, then only move to 20 Mhz.
20. **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
21. **Fragmentation Threshold**: Set the fragmentation threshold, which is the maximum fragment size.
22. **Beacon Interval**: Beacon Interval means the period of time between one beacon and the next one. The default value is 100 (the unit is millisecond, or 1/1000 second). Lower the Beacon Interval to improve transmission performance in unstable environment or for roaming clients, but it will be power consuming.
23. **Current Beacon Interval:** This Mode represents the current status.
24. **HT AMPDU Factor**: Enables or disables Tx AMPDU aggregation for the entire interface. Receiving aggregate frames will still be performed, but no aggregate frames will be transmitted if this is disabled.
25. **VHT AMPDU Factor**: Set VHT capability field, Maximum A-MPDU length exponent. Value range is 0 to 7. Maximum A-MPDU length exponent indicates the maximum length of A-MPDU that the station can receive.
26. **DCS Enable**: Enable or disable DCS function which is a feature to detect and avoid CW interference.
27. When done, click **Apply.**

2.4.1.3.5 Advanced

The Professional module provides advanced configuration options.



NOTE: We recommend that administrators use the default settings.

In this module, administrator can configure the followings:

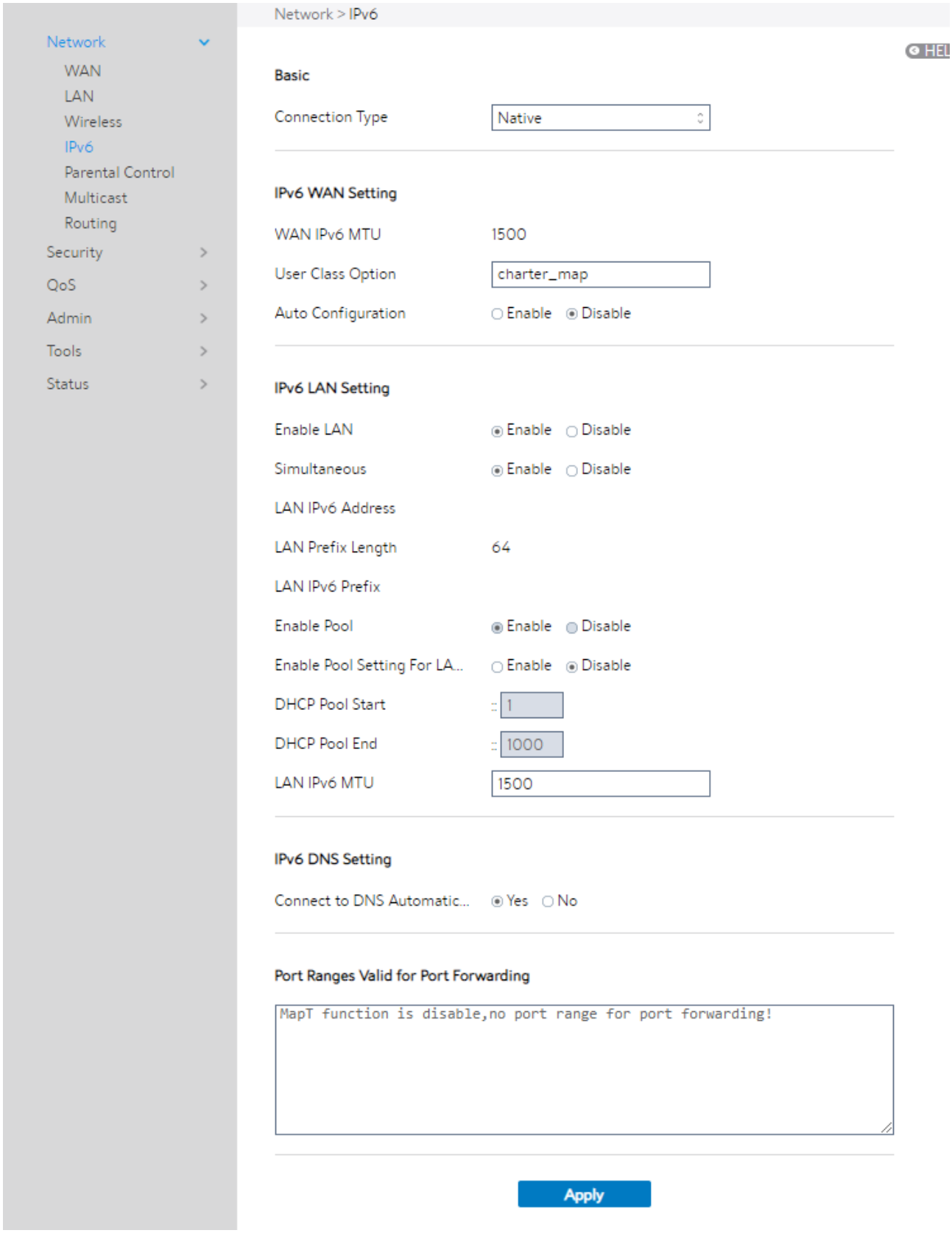
1. From the navigation panel, go to **Advanced** > **Network** > **Wireless** > **advanced.**

2. **Frequency**: Select the frequency band to configure professional settings.
3. **WiFi Network Name**: A name whose length is less than 32 characters is used to identify a wireless network.
4. **TX STBC**: Enables or disables the Space Time Coding Block (STBC) feature, as described in 802.11 specification, in transmitting (TX) direction.
5. **RX STBC**: Enables or disables the Space Time Coding Block (STBC) feature, as described in 802.11 specification, in receiving (RX) direction.
6. **Set AP Isolated**: Prevent wireless devices from communicating with each other via WiFi Router. This feature is useful if many guests frequently join or leave your network. Select [**Yes]** to enable this feature or select [**No]** to disable.
7. **Multicast Rate (Mbps)**: Setting transmission rate for multicast.
8. **Short Guard Interval**: Defines the length of time that the WiFi Router spends for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Enable** for a busy wireless network with high network traffic.
9. **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.
10. **Current DTIM Interval：** The article represent a current state.
11. **WMM**: Enables or disables WMM capabilities in the driver. The WMM capabilities perform special processing for multimedia stream data including voice and video data.

12. **WMM APSD**: Enable WMM APSD (WiFi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.
13. **Turbo QAM**: 256-QAM (MCS 8/9) support. Wireless Mode must be set to auto.
14. **Universal Beamforming**: For legacy wireless network adapters which do not support beamforming, the WiFi Router estimates the channel and determines the steering direction to improve the downlink speed. (Also known as Implicit Beamforming.)
15. **Multicast Enhancement Mode**: The Multicast Enhancement Mode comes in three modes. They are a) “Disable Multicast Enhancement”, b) “Enable Multicast Enhancement” (which uses Tunneling Mode), and c) “Translating Mode”. But “Enable Multicast Enhancement”, which uses Tunneling Mode in the OL chip, is not supported.
16. **Disable Specific MCS Data Rates**: Disabling specific MCS data rates per SSID.
17. Click **Apply**.

2.4.1.4 IPv6

The module is used to set some basic functions related to IPv6. For IPv6 service is not yet widely available, contact your ISP to make sure whether IPv6 service is provided.



Steps to set up IPv6:

1. From the navigation panel, go to **Advanced > Network > IPv6**.
2. **Connection Type**: Select IPv6 connection type to configure Disable, Native and Static IPv6.
3. **WAN IPv6 Address**: Set the WAN interface's ipv6 address.
4. **WAN Prefix Length:** Set the WAN interface's ipv6 prefix length.
5. **WAN IPv6 Gateway:** Set the WAN interface's ipv6 gateway.
6. **WAN IPv6 MTU**: Set the WAN interface's IPv6 MTU (Maximum Transmission Unit).
7. **User Class Option**: The user class option (15) of ORO that DHCPv6 clients send to the DHCPv6 server by solicit message.
8. **Auto Configuration:** The WAN interface's address assign type (SLAAC). Enable: WAN interface can get ipv6 address by SLAAC. Disable: WAN interface gets the ipv6 address only by Stateful.
9. **Enable LAN**: Enable/Disable WiFi Router allocating IPv6 addresses for LAN-side devices.
10. **LAN IPv6 Address**: Set LAN interface's IPv6 address.
11. **Simultaneous**: The mode which hosts connected to the LAN interface can get IPv6 addresses. When enabled, hosts get IPv6 address by simultaneous Stateless and Stateful (requires address between DHCP pool start and end values). When disabled, hosts do not get IPv6 addresses simultaneously, and a mode must be selected instead (SLAAC + RDNSS, SLAAC + Stateless DHCPv6, Stateful DHCPv6).
12. **LAN Prefix Length**: Set LAN interface's IPv6 prefix length.
13. **LAN IPv6 Prefix**: Set LAN interface's prefix.

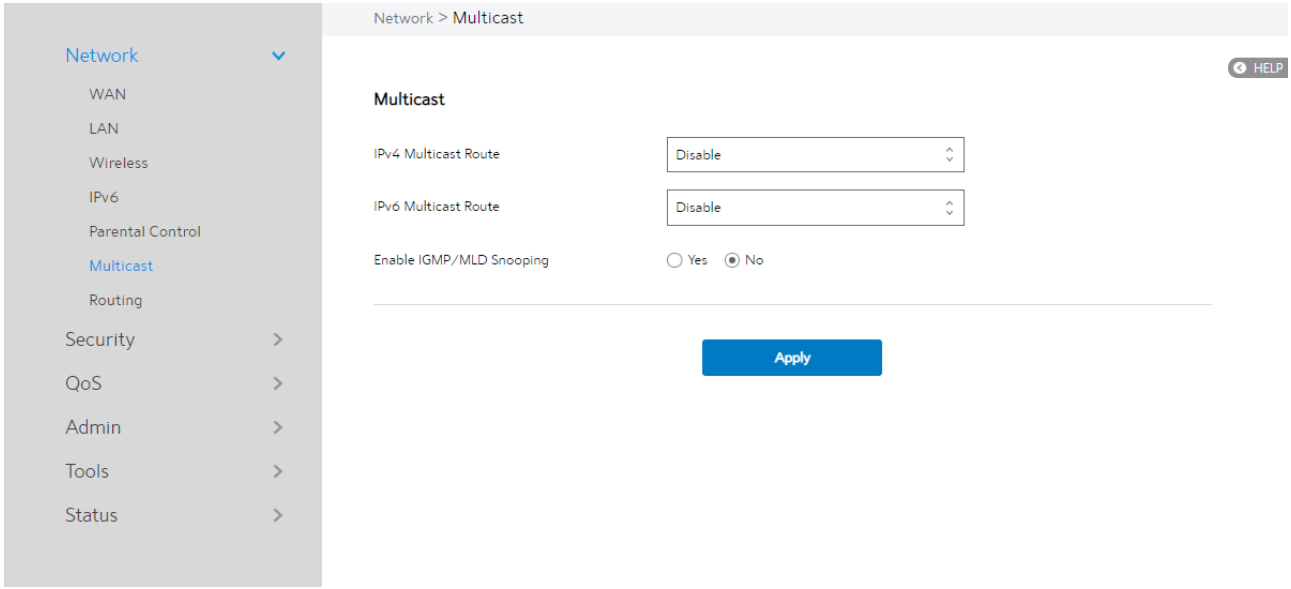
14. **Enable pool:** Enable/Disable ipv6 pool.
15. **Enable Pool Setting For Lan Host**: Enable to set DHCP pool start and end values for client IPv6 address assign range, it's disable by default.
16. **DHCP Pool Start**: DHCP pool start values for client IPv6 address.
17. **DHCP Pool End**: DHCP pool end values for client IPv6 address.
18. **PD-Valid Lifetime**: Prefix delegation for valid lifetime.
19. **PD-Preferred Lifetime**: Prefix delegation for preferred lifetime.
20. **LAN IPv6 MTU:** Set MTU for LAN-side devices.
21. **Connect to DNS Server Automatically**: Choose to acquire the DNS from uplink.
22. **IPv6 DNS Server 1**: IPv6 address for DNS server.
23. **IPv6 DNS Server 2**: IPv6 address for DNS server.
24. **IPv6 DNS Server 3**: IPv6 address for DNS server.
25. **Port Ranges Valid for Port Forwarding**: The "port ranges" are set by Map-T mode, and the port setting for port forwarding must be in these ranges.
26. Click **Apply**.

2.4.1.5 Parental Control

Refer to 2.3.5 Parental Control for relevant setting descriptions.

2.4.1.6 Multicast

Enable multicast. The sender and receiver can implement point-to-multipoint connections.



Steps to set up Multicast:

1. From the navigation panel, go to **Advanced > Network > Multicast.**
2. **IPv4 Multicast Route**: Select an IPv4 Multicast Route.

   *IGMP Proxy: IGMP Proxy enables hosts in a unidirectional link routing (UDLR) environment that are not directly connected to a downstream WiFi Router to join a multicast group sourced from an upstream network.

   *PIM: PIM-Source-specific multicast (SSM) is used in IPv4/IPv6 and is a method of delivering multicast packets in which the only packets that are delivered to a receiver are those originating from a specific source address requested by the receiver. By limiting the source, SSM reduces demands on the network and improves security.
3. **IPv6 Multicast Route**: Select an IPv6 Multicast Route.

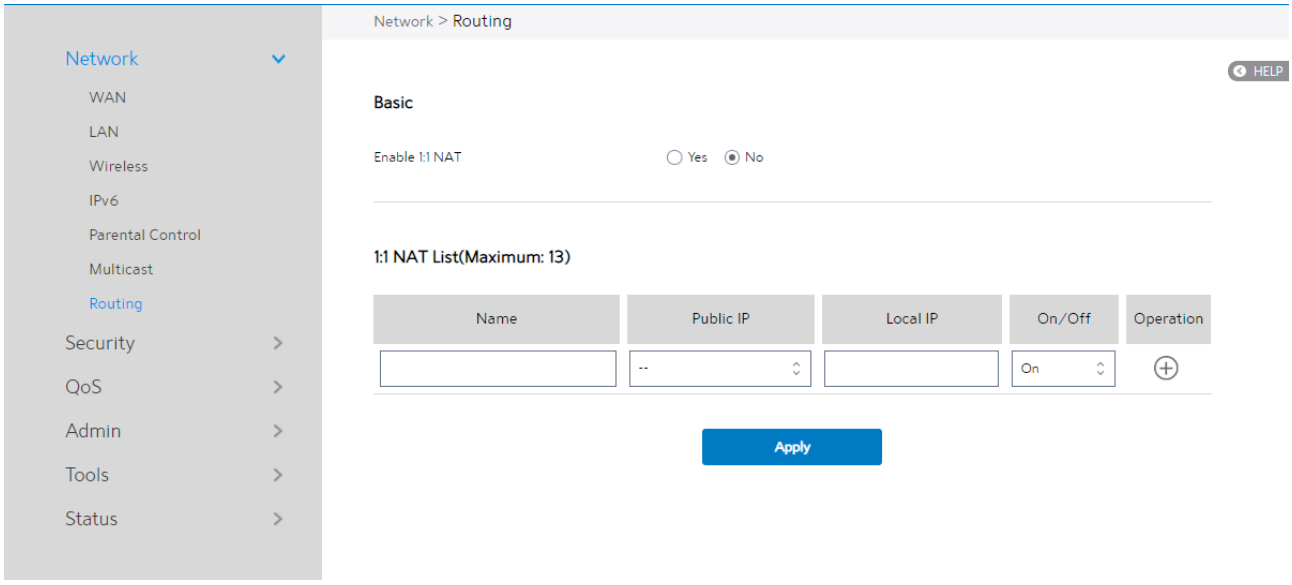
   *MLD Proxy: The MLD proxy is used in IPv6 environments. This feature enables a device to learn proxy group membership information, and forward multicast

packets based upon that information. If a device is acting as RP for route proxy entries, MLD membership reports for these entries can be generated on user specified proxy interface.

4. **Enable IGMP/MLD Snooping:** Check [**Yes**] to enable snooping and Check [**No**] to disable snooping. IGMP/MLD snooping is the process of listening to Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD) network traffic. The feature lets a network switch listen in on the IGMP/MLD conversation between hosts and WiFi Routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
5. When done, click **Apply**.

2.4.1.7 Routing

This module can be used to build a static NAT table between WAN IP address and LAN IP address.



Steps to set up Routing:

1. From the navigation panel, go to **Advanced** > **Network** > **Routing.**
2. **Enable 1:1 NAT**: Check [**Yes**] to enable this function, check [**No**] to disable this function.
3. **Name**: A brief description for application.
4. **Public IP**: IP address from Charter supplied public IP subnets.
5. **Local IP**: Key in the client's LAN IP address, not limited to the subnet for the directly connected LAN interface
6. Click **On/Off** to enable/disable the rule.
7. Click [**+**] to add this item to the 1:1 NAT List.
8. Click **Apply**.

NOTE: This module only works only when WAN port is in static mode!

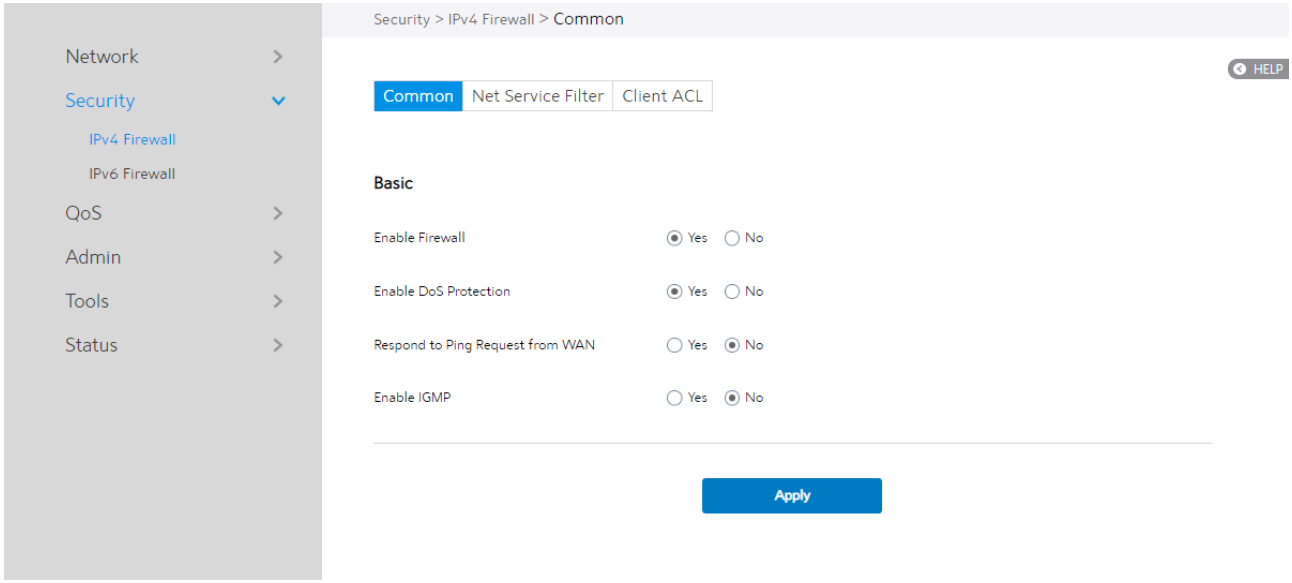
2.4.2 Security

2.4.2.1 IPv4 Firewall

Enable the firewall to protect local area network against attacks from outside. Firewall filters the incoming and outgoing packets based on rules.

NOTE: Firewall is enable by default.

2.4.2.1.1 Common



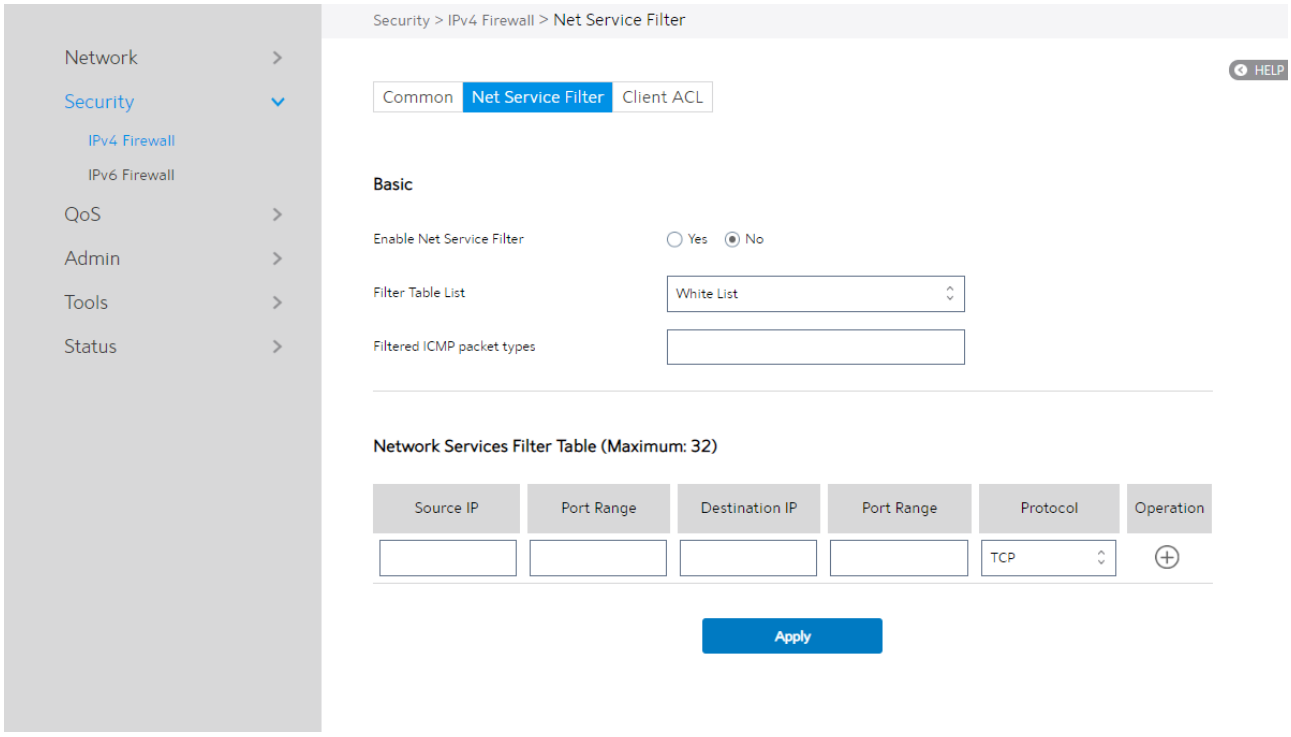
Steps to set up basic Firewall settings:

1. From the navigation panel, go to **Advanced > Security > IPv4 Firewall > Common**.
2. **Enable Firewall**: Disabling the firewall will deactivate all related functions.
3. **Enable DoS Protection**: A "denial-of-service" attack is an explicit attempt to deny legitimate users from using a service or computer resource. Enabling this feature can protect the WiFi Router from DoS attack but it would increase the WiFi Router's workload.

4. **Respond to Ping Request from WAN**: This feature lets WiFi Router make a response to ping request from WAN.
5. **Enable IGMP**: Check [Yes] to allow IGMP packages to be transferred to the WiFi Router. Check No to deny IGMP packages.
6. Click **Apply**.

2.4.2.1.2 Net Service Filter

Net Service Filter can work in either **White List** or **Black List** mode. When running in **White List** mode, it only lets certain packets get through the WiFi Router. While in **Black List** mode, it only blocks certain packets passthrough.



Steps to set **Net Service Filter**:

1. From the navigation panel, go to **Advanced** > **Security** > **IPv4 Firewall** > **Net**

Service Filter.

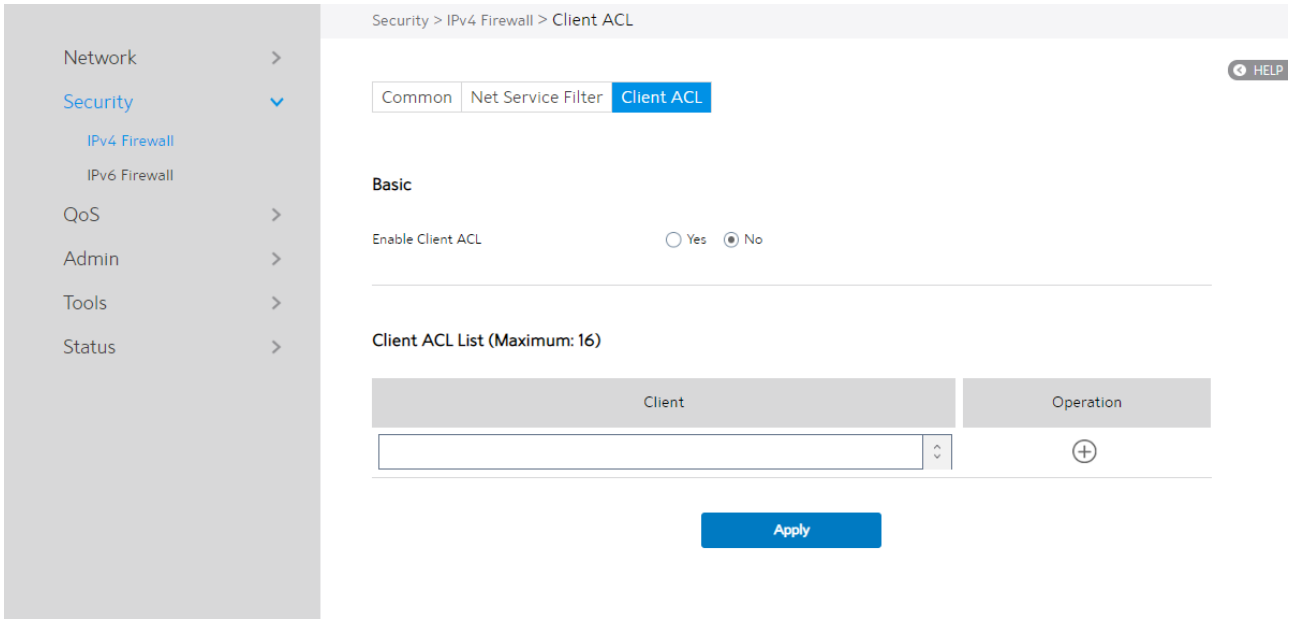
2. **Enable Net Service Filter**: Enable or disable this module.
3. **Filter Table List**: There are two kinds of filter list: White List, Black List. White List can make WiFi Router serve the specified service defined in the list, Black List make WiFi Router deny serving the specified service.
4. **Filtered ICMP packet types**: This field defines a list of LAN to WAN ICMP packets type that will be filtered. For example, if you would like to filter Echo (type 8) and Echo Reply (type 0) ICMP packets, you need to enter a string with numbers separated by blank, such as [0 8].
5. **Source IP**: For source or destination IP address, you can: (a) enter a specific IP address such as "192.168.122.1"; (b) enter IP addresses within one subnet or within the same IP pool such as "192.168.123.*" or "192.168.*.*"; or (c) enter all IP addresses as "*.*.*.*".
6. **Port Range**: For source or destination port range, you can either: a) enter a specific port, such as "95"; or b) enter ports within a range such as "103:315", ">100", or "<65535".
7. **Destination IP**: For source or destination IP address, you can: (a) enter a specific IP address such as "192.168.122.1"; (b) enter IP addresses within one subnet or within the same IP pool such as "192.168.123.*" or "192.168.*.*"; or (c) enter all IP addresses as "*.*.*.*".
8. **Port Range**: For source or destination port range, you can either: a) enter a specific port, such as "95"; or b) enter ports within a range, such as "103:315",

">100", or "<65535".

9. **Protocol**: The protocol of service used to transport the packages. (UDP, TCP)
10. **Add/Delete:** Click ⊕ or ⊖ to add/delete the profile.
11. When done, click **Apply**.

2.4.2.1.3 Client ACL

Client ACL can forbid the client from accessing to the WiFi Router. The client in the **Client ACL List** can't visit the resource of WiFi Router and the internet.



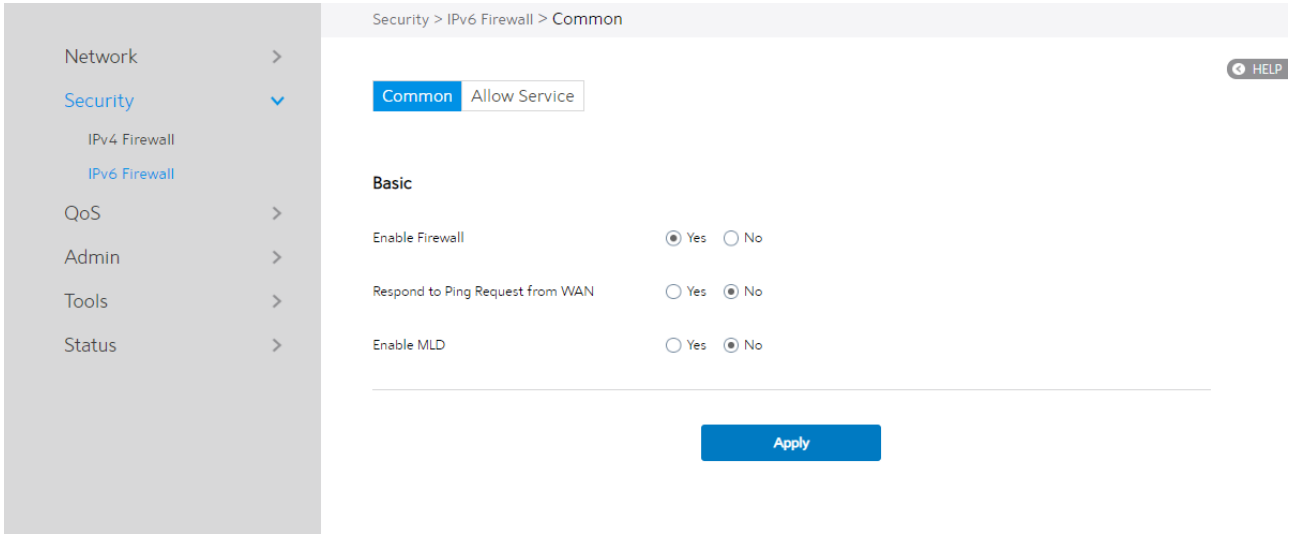
Steps to set up **Client ACL**:

1. From the navigation panel, go to **Advanced** > **Security** > **IPv4 Firewall** > **Client ACL**.
2. **Enable Client ACL**: Enable or disable **Client ACL** function.
3. **Client**: MAC address of LAN-side devices.
4. **Add/Delete:** Click [+] or [-] to add/delete the profile.

5. When done, click **Apply**.

2.4.2.2 IPv6 Firewall

2.4.2.2.1 Common

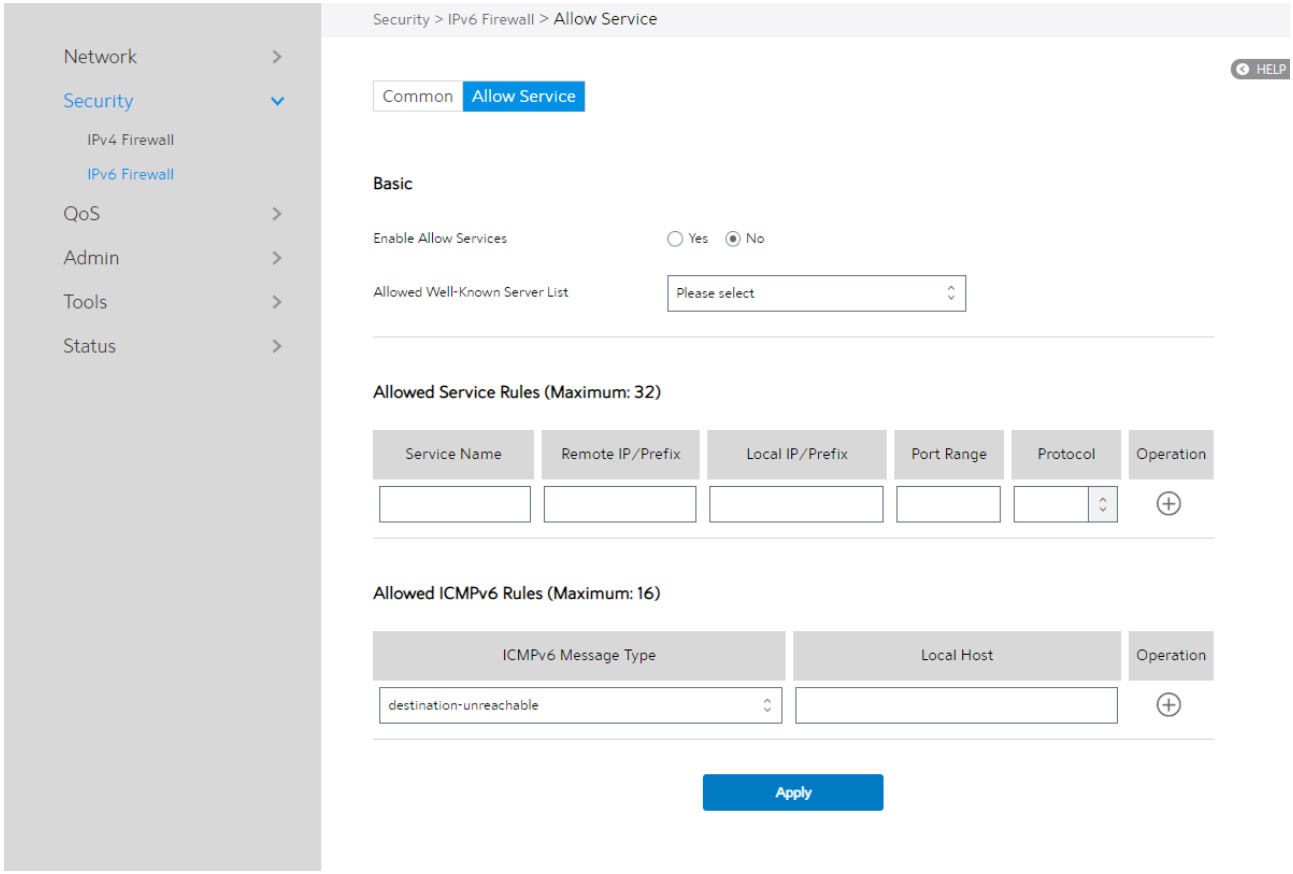


Steps to set up common **IPv6 Firewall**:

1. From the navigation panel, go to **Advanced** > **Security** > **IPv6 Firewall** > **Common.**
2. **Enable Firewall**: Enable or disable the IPv6 firewall. When disabled, all IPv6 packages can input WiFi Router, output WiFi Router and forward without any limitation.
3. **Respond to Ping Request from WAN**: This feature lets WiFi Router make a response to ping request from WAN.
4. **Enable MLD**: Check [**Yes**] to allow MLD packages to be transferred to the WiFi Router. Check [**No**] to deny MLD packages.
5. Click **Apply**.

2.4.2.2.2 Allow Services

Allow Services allows various types of service rules including protocol like TCP/UDP and ICMPv6 Message Type. It will allow certain packets and drop the other IPv6 packets from WAN-side to LAN-side.



Steps to set up **IPv6 Firewall**:

1. From the navigation panel, go to **Advanced** > **Security** > **IPv6 Firewall** > **Allow Services**.
2. **Enable Allow Services**: Enable or disable the IPv6 Allow Services feature. When Allow Services is enabled, the Allowed Service Rules will be allowed.
3. **Allowed Well-Known Server List**: List of well-known servers to be allowed. For example: ftp, samba.
4. **Service Name**: The name of the service which will add IPv6 firewall rule.

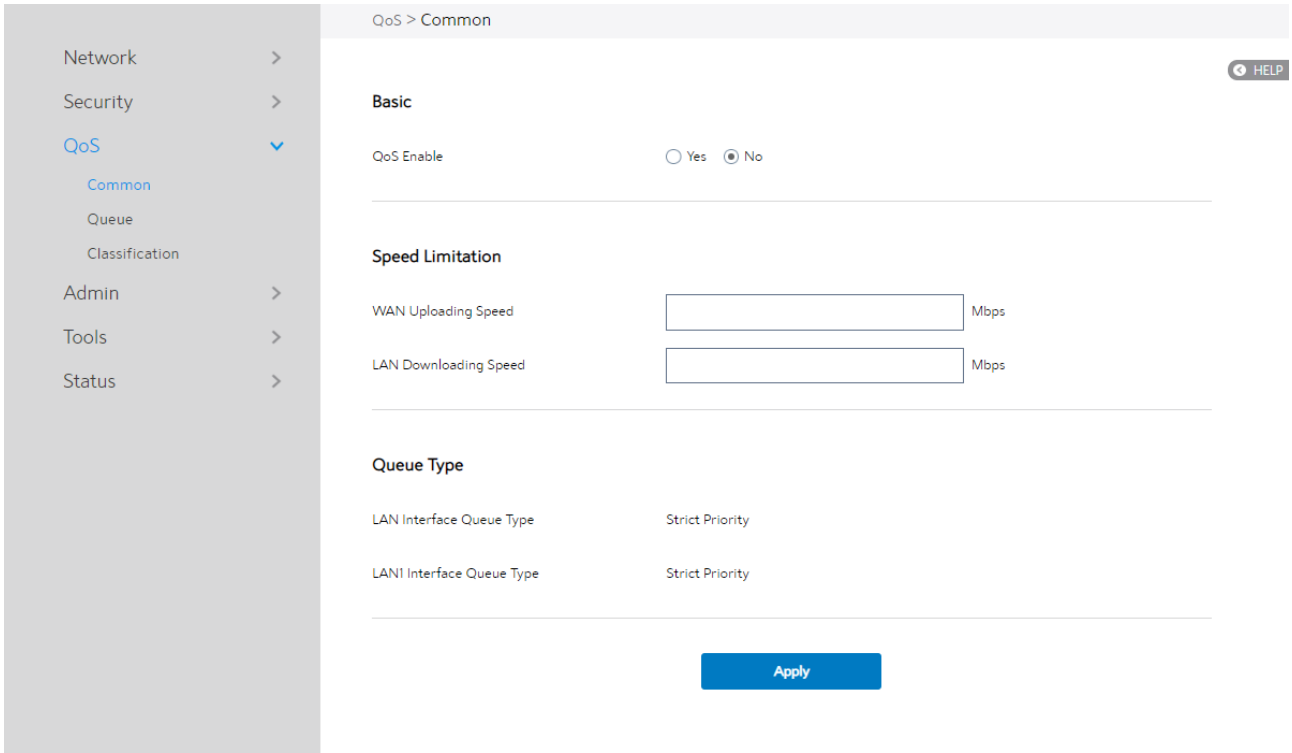
5. **Remote IP/Prefix**: IPv6 address or Prefix of a remote server.
6. **Local IP/Prefix**: IPv6 address or Prefix of a LAN-side client.
7. **Port Range**: Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024, 3021).
8. **Protocol**: The protocol the service uses to transport the number of packages e.g. (17=UDP, 6=TCP).
9. **ICMPv6 Message Type**: Make WiFi Router process the defined types of ICMPv6 packet from specified host.
10. **Local Host:** IPv6 address of the host.
11. **Add/Delete:** Click [+] or [-] to add/delete the profile.
12. When done, click **Apply**.

2.4.3 QoS

The Quality of Service (QoS) module provides different services according to the priority of applications, users, or data flows. In a word, it can guarantee a certain level of performance to a data flow.

2.4.3.1 Common

The Common module is for setting the up and down queue type. The user may choose the queue type, depending on his/her need, as well as set the uplink and the downlink limit to limit the uplink and downlink transmission rate.



Steps to set it:

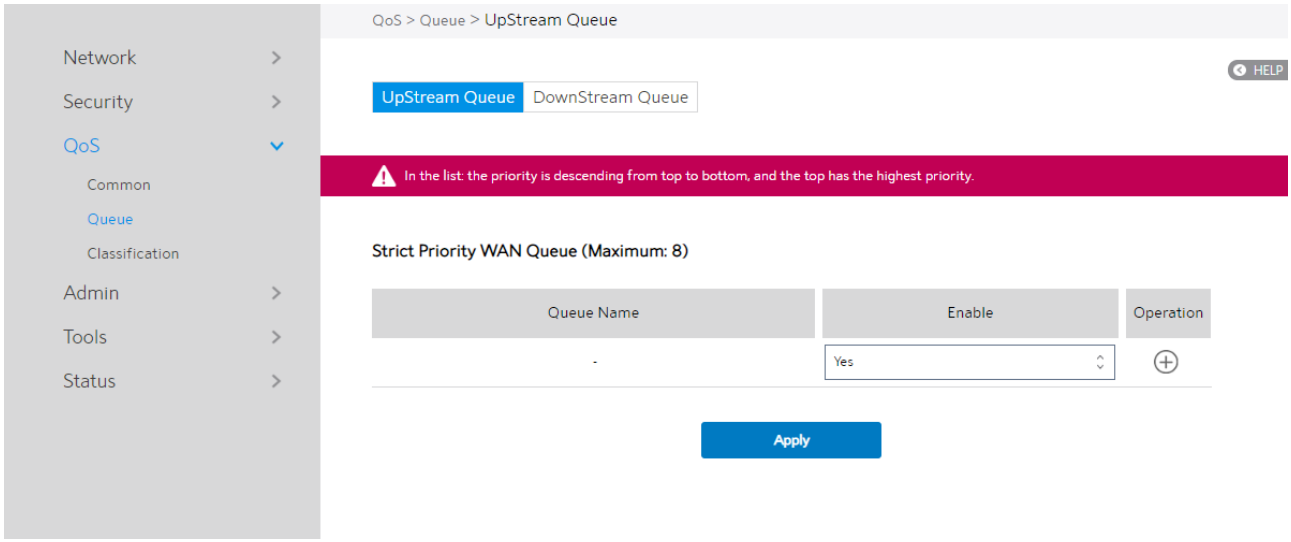
1. From the navigation panel, go to **Advanced** > **QoS** > **Common**.
2. **QoS Enable**: Set the switch of WiFi Router QoS function through Web page.

3. **WAN Uploading Speed**: The speed of the uplink data limit.
4. **LAN Downloading Speed**: The downstream limit of the subnet LAN.
5. **LAN Interface Queue Type**: For setting Downstream QoS queue (Strict Priority / Weighted Round Robin / Weighted Fair Queuing), for Subnet LAN.
6. **LAN1 Interface Queue Type**: Downstream QoS queue type should to be set to Strict Priority/Weighted Round Robin/Weighted Fair Queuing for Subnet LAN1.
7. Click **Apply**.

2.4.3.2 Queue

Create upstream queue and downstream queues to classify traffic of different types into the upstream or downstream queue. Select up queue and down queue type based on common page selection. In the Queue webpage, user may add, delete, or modify Queue settings.

2.4.3.2.1 UpStream Queue

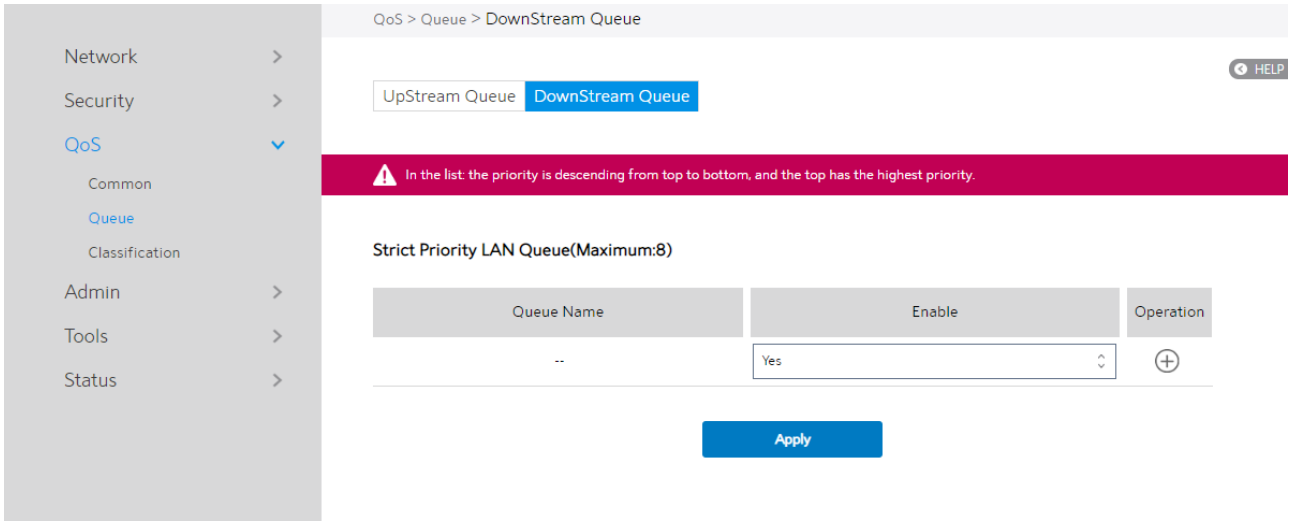


Steps to set queue:

1. From the navigation panel, go to **Advanced > QoS > Queue > UpStream Queue**.
2. **Enable**: Enables or disables this queue.
3. **Operation**: Add, Edit or Delete operation for this item.
4. Click **Apply**.

2.4.3.2.2 DownStream Queue

Steps to set queue:



Steps to set Queue:

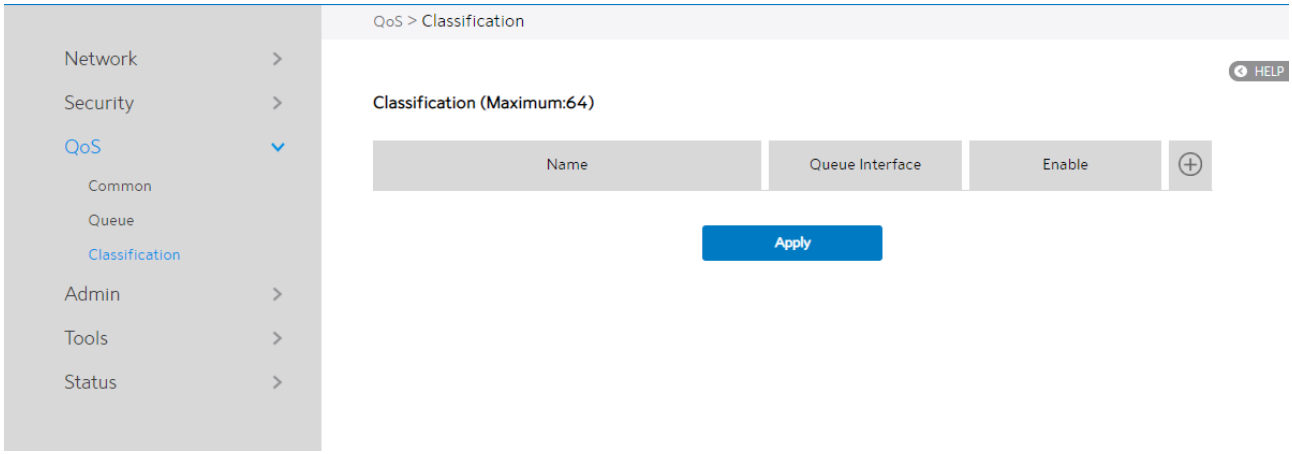
1. From the navigation panel, go to **Advanced > QoS > Queue > DownStream Queue**.
2. **Enable**: Enables or disables this queue.
3. **Operation**: Add, Edit or Delete operation for this item.
4. Click **Apply**.

2.4.3.3 Classification

According to the characteristics of the data flow, traffic is classified and then queued to the specified upstream or downstream queues.

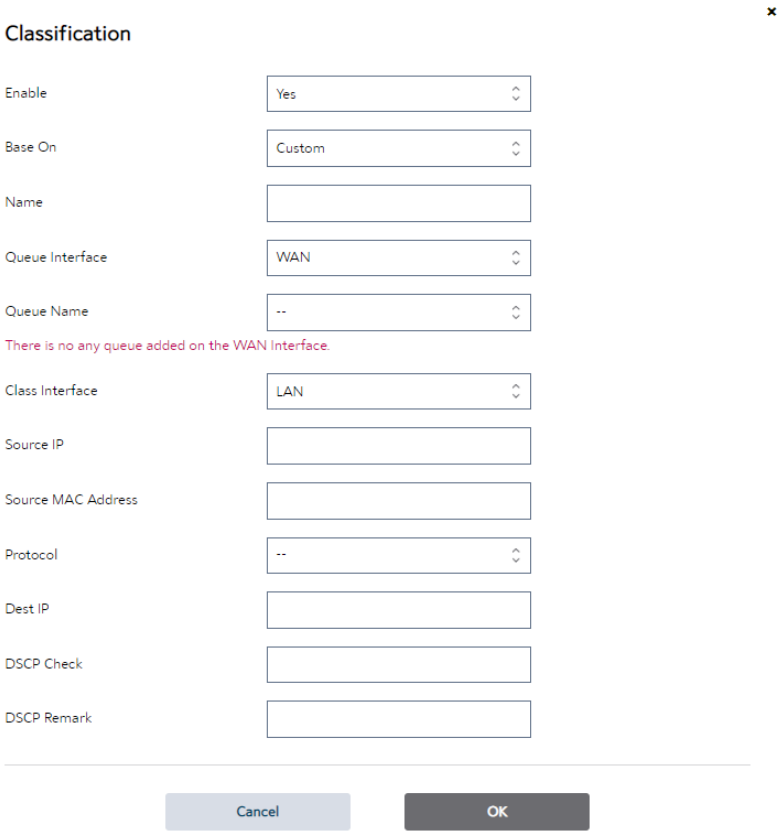
Classification Display page:

Display classification table (Simple information).



Steps to set up **Classification:**

1. From the navigation panel, go to **Advanced** > **QoS** > **Classification**.
2. Classification is displayed. Click **Add** to set up.
3. **Name**: Classification name.
4. **Queue Interface**: The queue that represents the current entry selection.
5. **Enable**: Display the entry's status.
6. **Edit/Delete**: Modify or delete this entry.



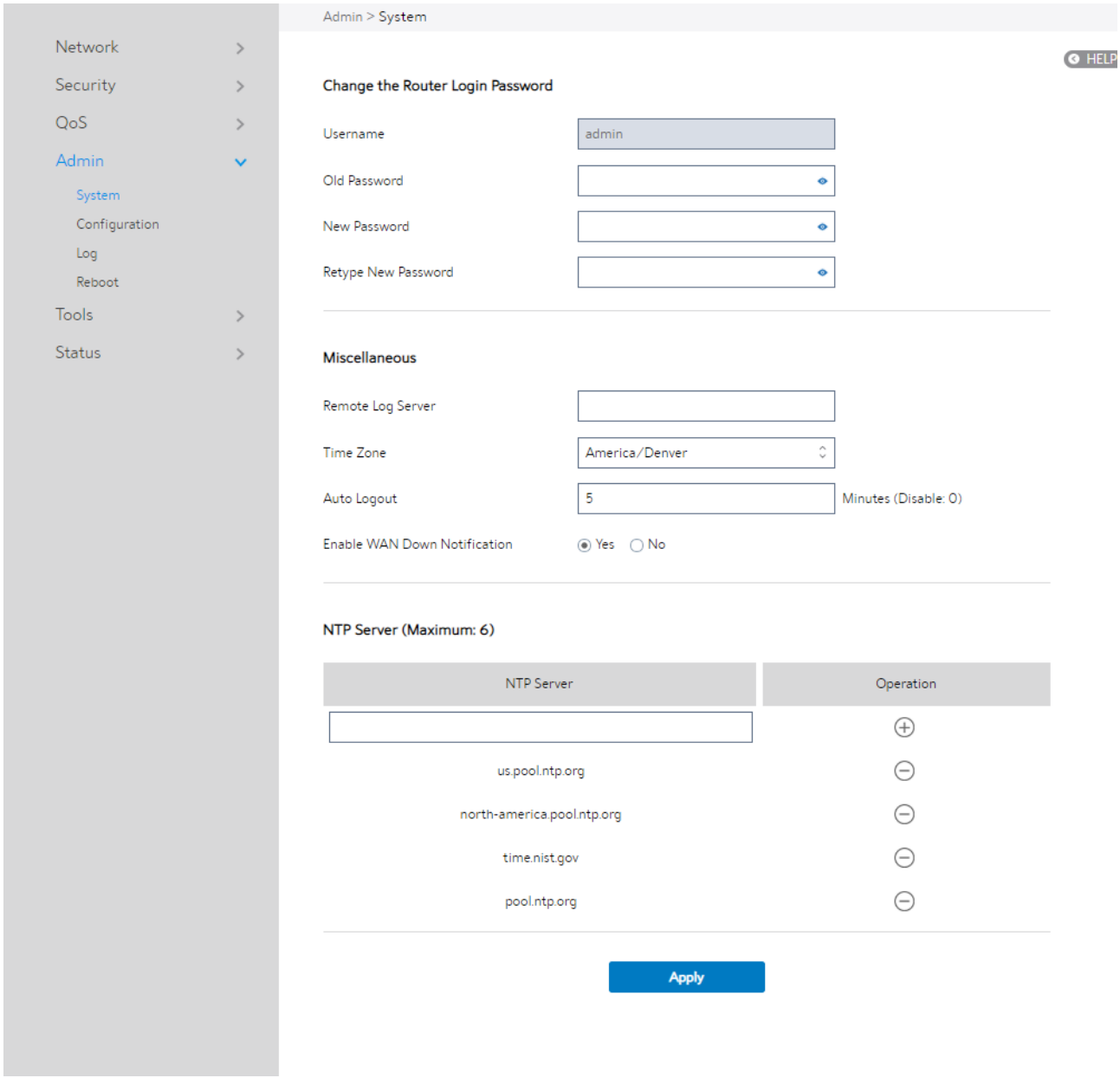
7. **Enable**: Disable or enable this classification function.
8. **Base On**: It is a fast classification, (can be based on Client, Custom, Server, SSID, APP).
9. **Name**: Define this classification alias name.
10. **Queue Interface**: Select the existing queue (upstream or downstream).
11. **Queue Name**: Only display. Indicates the index number of the queue type selected by the user.
12. **Class Interface**: This specifies the ingress interface associated with the entry
13. **Source IP**: Source IP address. An empty string indicates this criterion is not used for classification.

14. **Source MAC Address**: Source MAC Address. An empty string indicates this criterion is not used for classification.
15. **Protocol**: Protocol
16. **Dest IP**: Destination IP address, an empty string indicates this criterion is not used for classification.
17. **DSCP Check**: DSCP number (0~63), base on it filter.
18. **DSCP Remark**: Remark new DSCP number.
19. When done, click **OK**.

2.4.4 Admin

2.4.4.1 System

The System page lets you configure your WiFi Router settings. The Web GUI sign in password is the same as SSH sign in password.

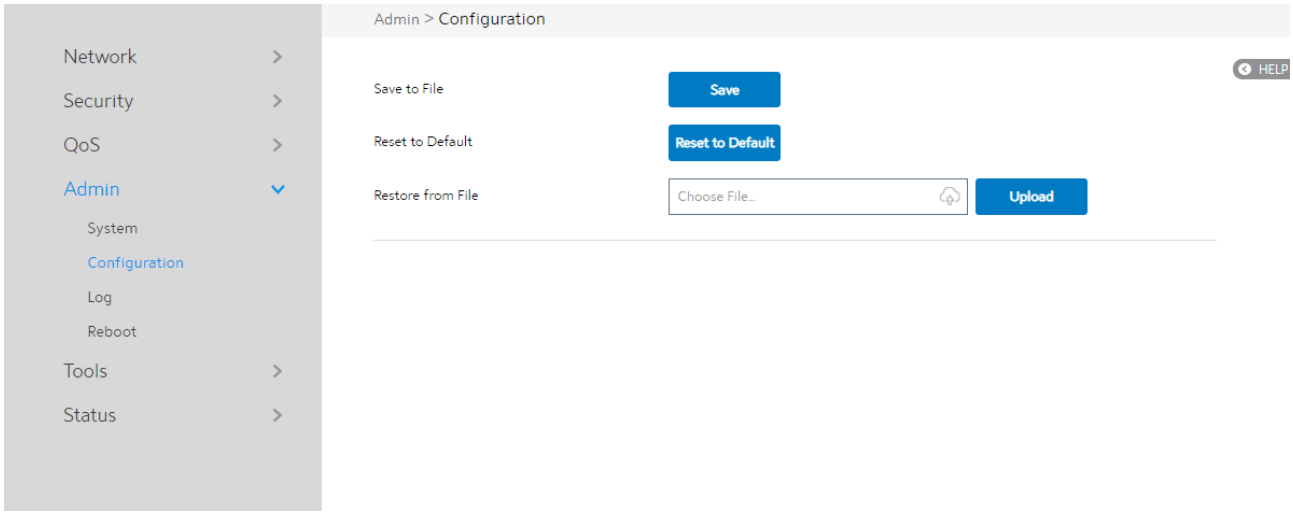


Steps to set **System**:

1. From the navigation panel, go to **Advanced** > **Admin** > **System.**

2. **Username**: WiFi Router's sign in name.
3. **Old Password:** WiFi Router's sign in password.
4. **New Password**: New password.
5. **Retype New Password**: Retype new password.
6. **Remote Log Server**: IP address of a syslog server to which log messages will be sent in addition to the local destination.
7. **Time Zone**: Default time-zone is USA/Denver.
8. **Auto Logout**: Auto sign out after a specified time.
9. **Enable WAN Down Notification**: When there is no Internet access, redirect to local notification.
10. **NTP Server**: WiFi Router can access a NTP (Network Time Protocol) server in order to synchronize the time automatically.
11. Click **Apply**.

2.4.4.2 Configuration

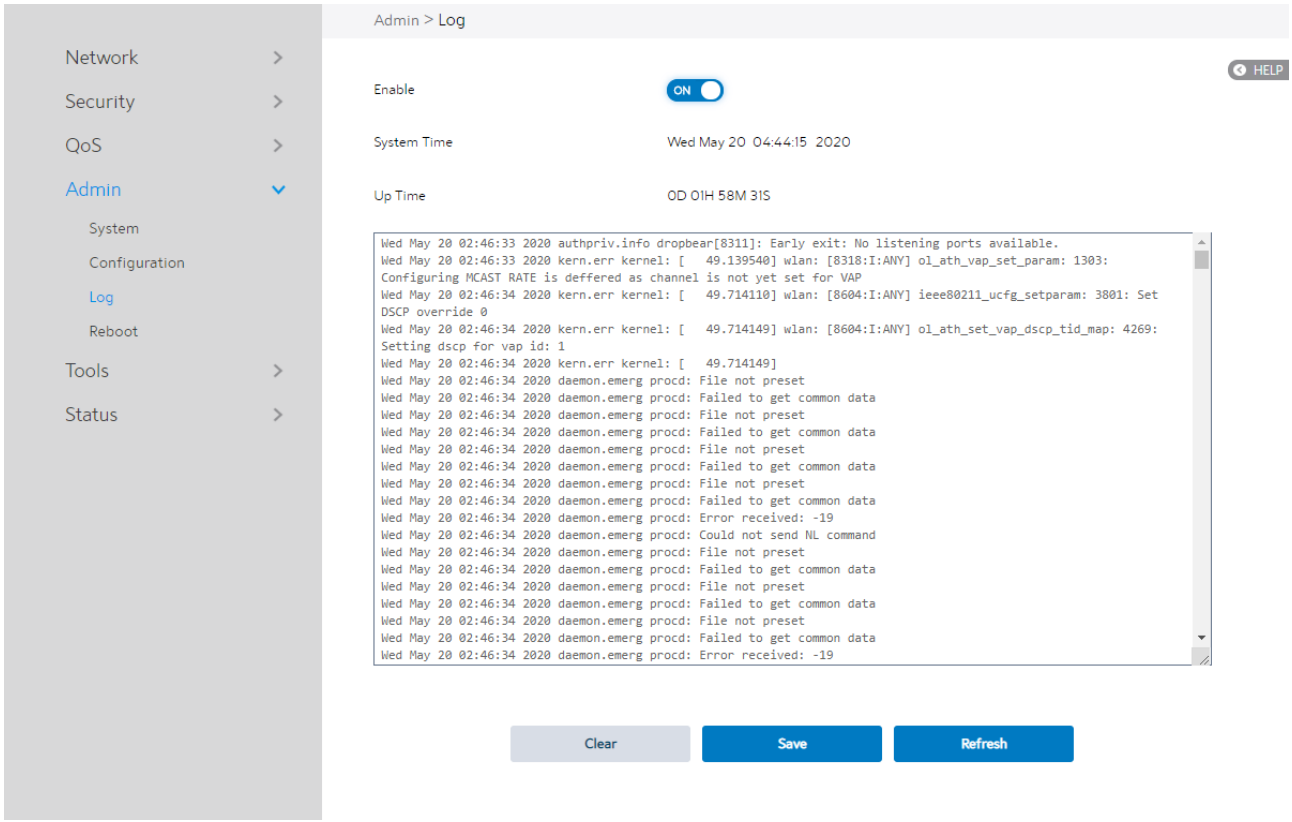


Steps to “Save to File”, “Reset to Default” and “Restore from File”:

1. From the navigation panel, go to **Advanced > Admin > Configuration.**
2. Click **Save,** and then the browser will automatically download WiFi Router’s setting files.
3. Click **Reset to Default,** this will resets all settings to factory default settings.
4. Click to select setting file, then click **Upload** button, this will set the WiFi Router to run “Restore from File”.

2.4.4.3 Log

System Log contains logs on network activities in the WiFi Router.

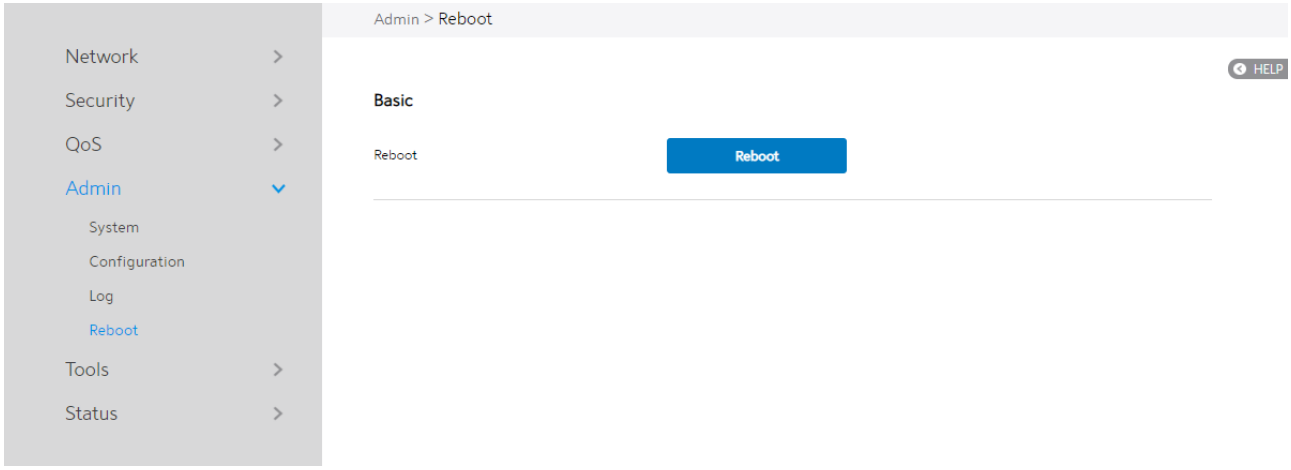


Steps to set System log:

1. From the navigation panel, go to **Advanced** > **Admin** > **Log**.
2. **Clear**: Clear contents in log file.
3. **Save**: Download log file from WiFi Router.
4. **Refresh**: Refresh the log window to show the latest log.

2.4.4.4 Reboot

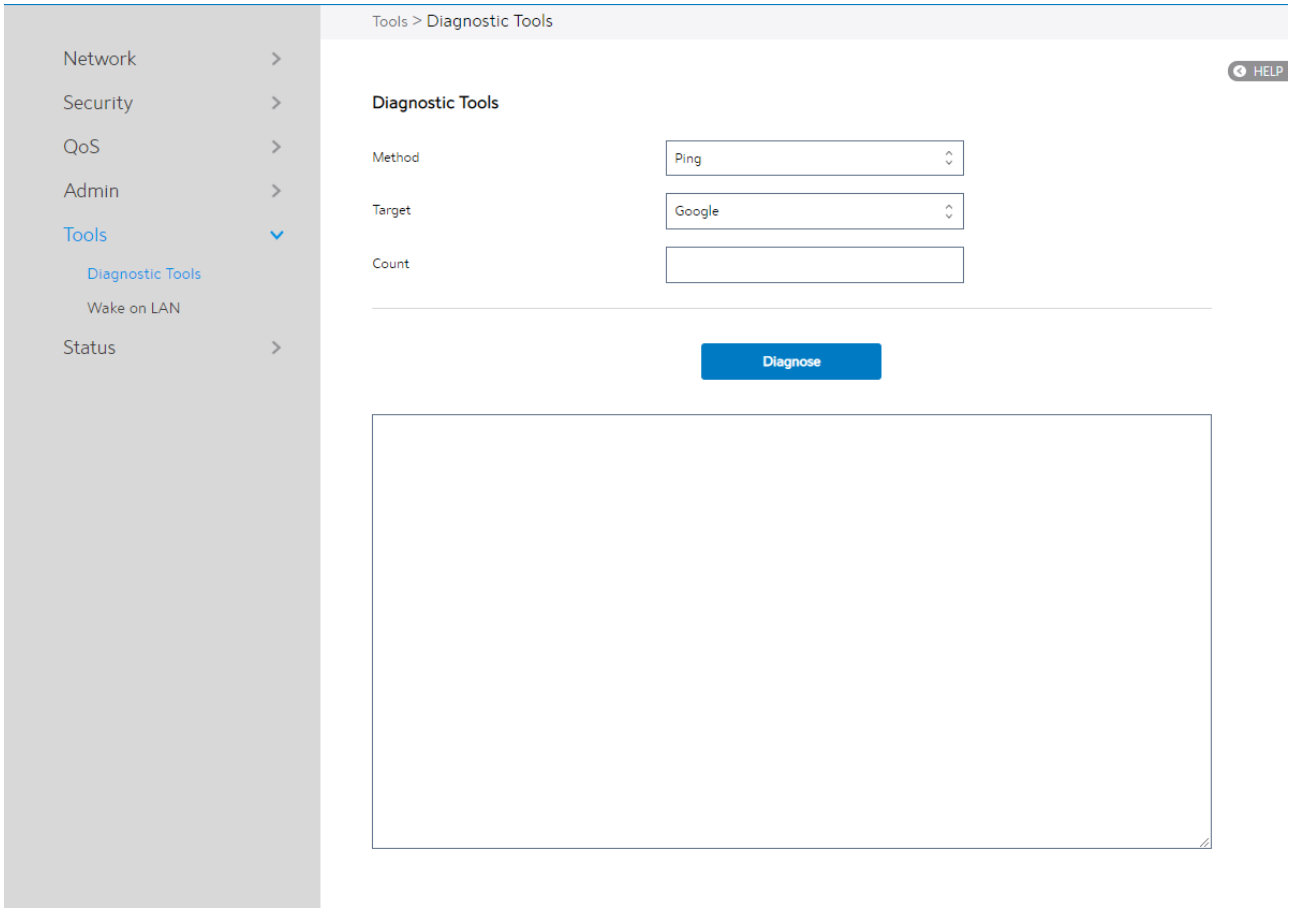
Click the **Reboot** button, the WiFi Router will restart.



2.4.5 Tools

2.4.5.1 Diagnostic Tools

Various diagnostic tools are available such as “ping”, “ping6”, “traceroute” and “nslookup”.

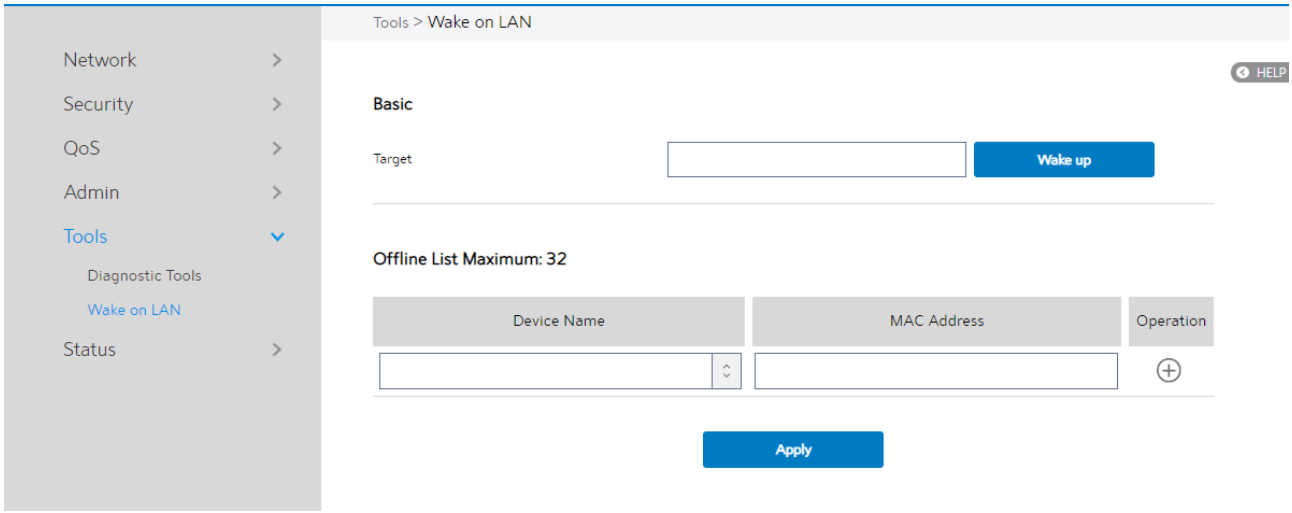


Steps to use Diagnostic Tools:

1. From the navigation panel, go to **Advanced** > **Tools** > **Diagnostic Tools**
2. **Method**: Choose a specified method to test network.
3. **Target**: Choose target for the test.
4. **Count**: Number of times to test.
5. Click **Diagnose**.

2.4.5.2 Wake on LAN

Wake on LAN is a power management function. It lets network admins wake up LAN side devices from standby or hibernation mode. This function requires motherboard support on LAN-side devices.



Steps to set Wake on LAN:

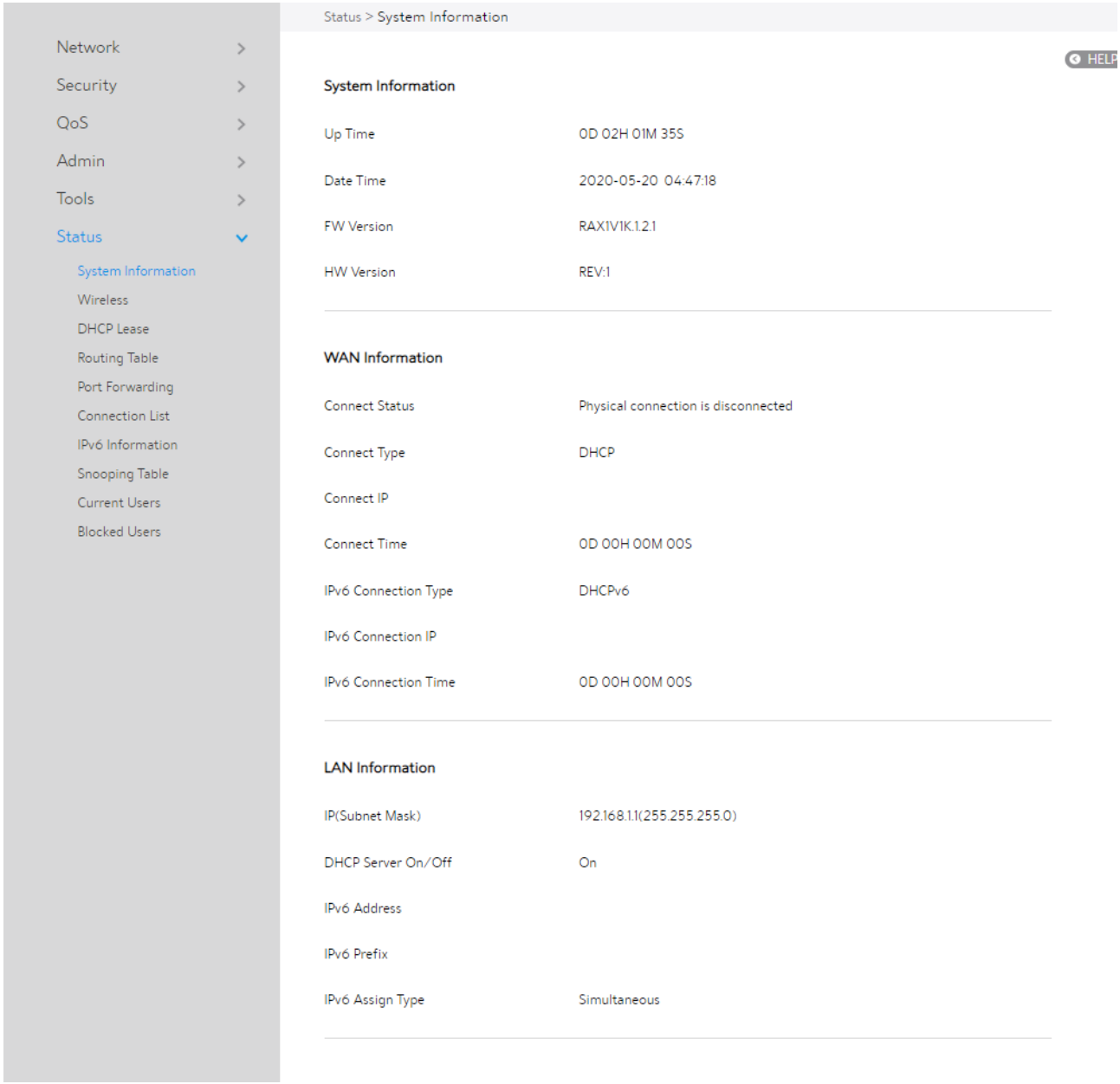
1. From the navigation panel, go to **Advanced> Tools> Wake on LAN**.
2. **Target**: Enter the MAC address of the device to be woken up, or select the device name from the list.
3. **Device Name**: Name of device.
4. **MAC Address**: The format for the MAC address is six groups of two hexadecimal digits, separated by colons (:), in transmission order (e.g. 12:34:56:aa:bc:ef).
5. When done, click **Apply**.

2.4.6 Status

2.4.6.1 System Information

System Information displays basic System, WAN, LAN and USB information.

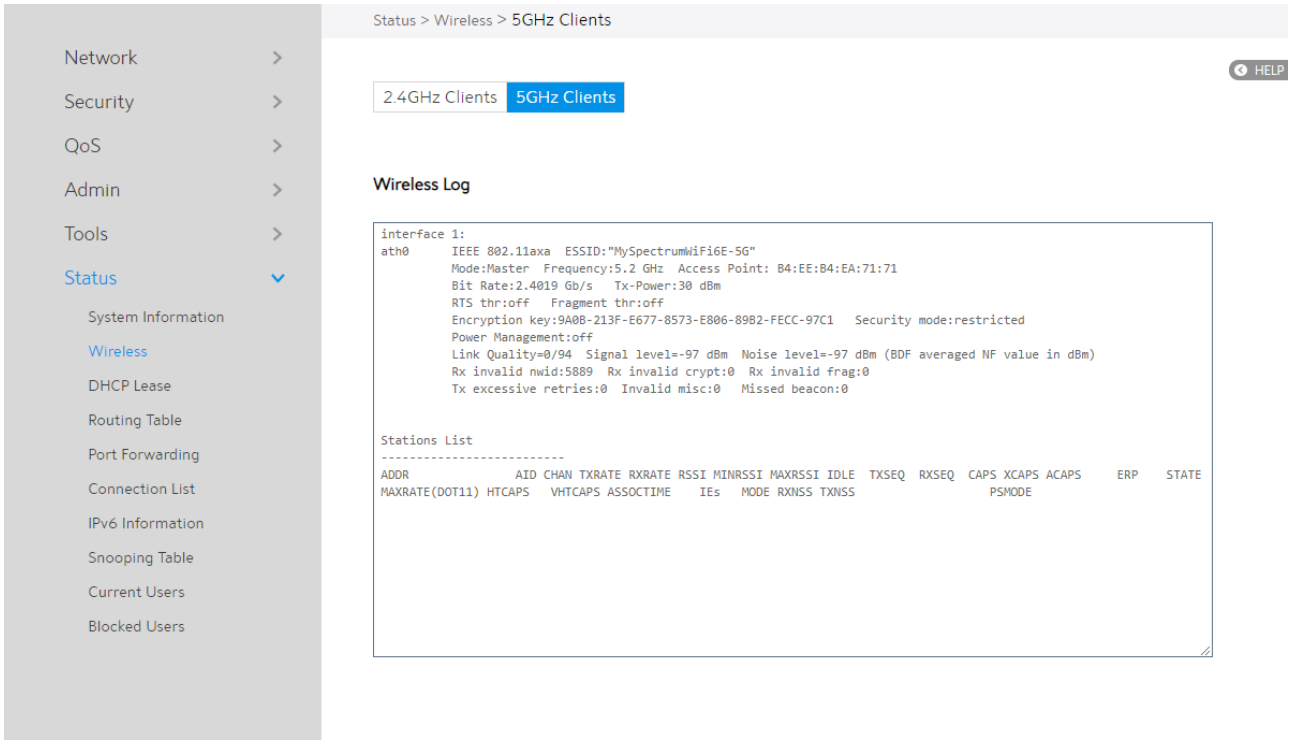
From the navigation panel, go to **Advanced** > **Status** > **System Information**.



2.4.6.2 Wireless

Wireless shows status information for wireless clients.

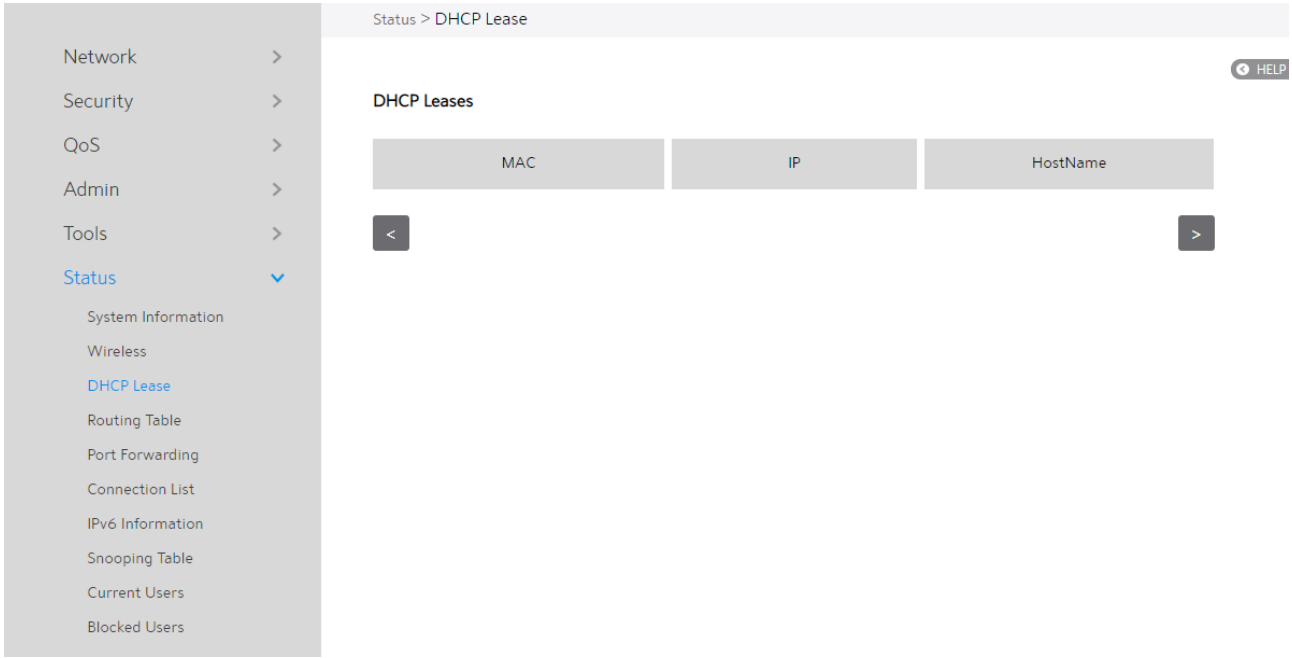
From the navigation panel, go to **Advanced** > **Status** >**Wireless**.



2.4.6.3 DHCP Lease

Show DHCP Lease status information, including MAC, IP and Hostname information.

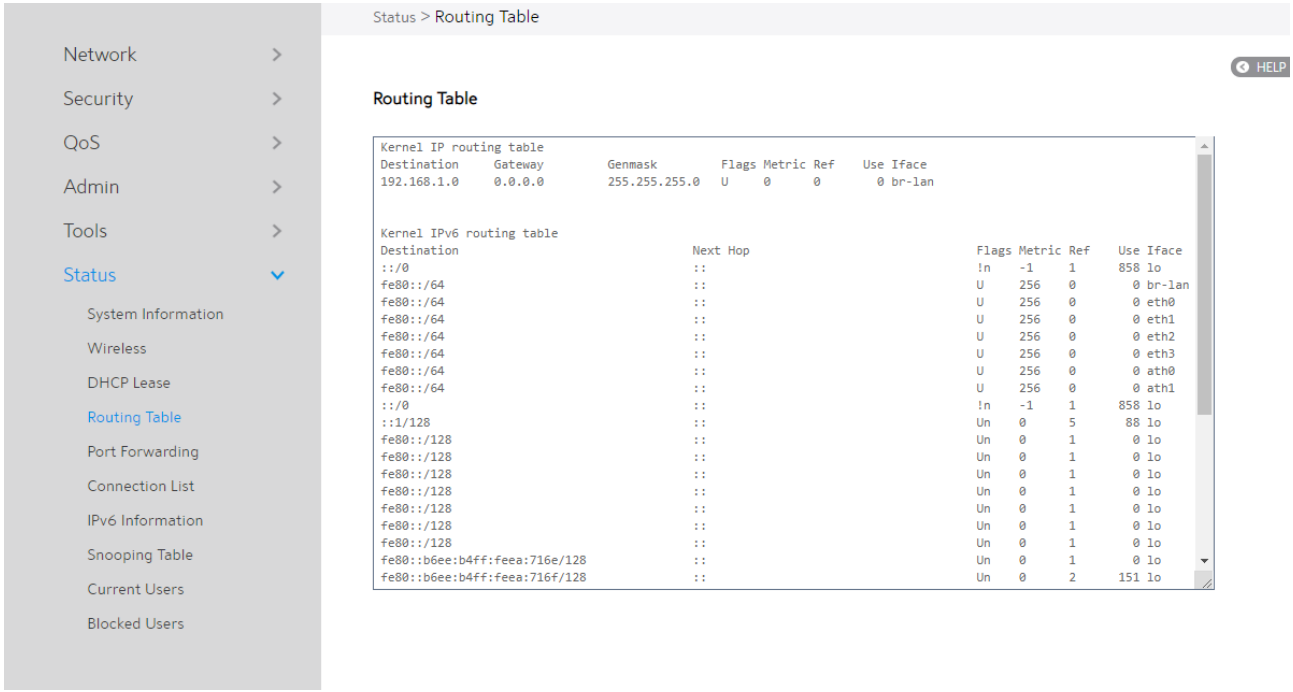
From the navigation panel, go to **Advanced** > **Status** > **DHCP Lease.**



2.4.6.4 Routing Table

Shows IPv4 and Ipv6 routing table and status information.

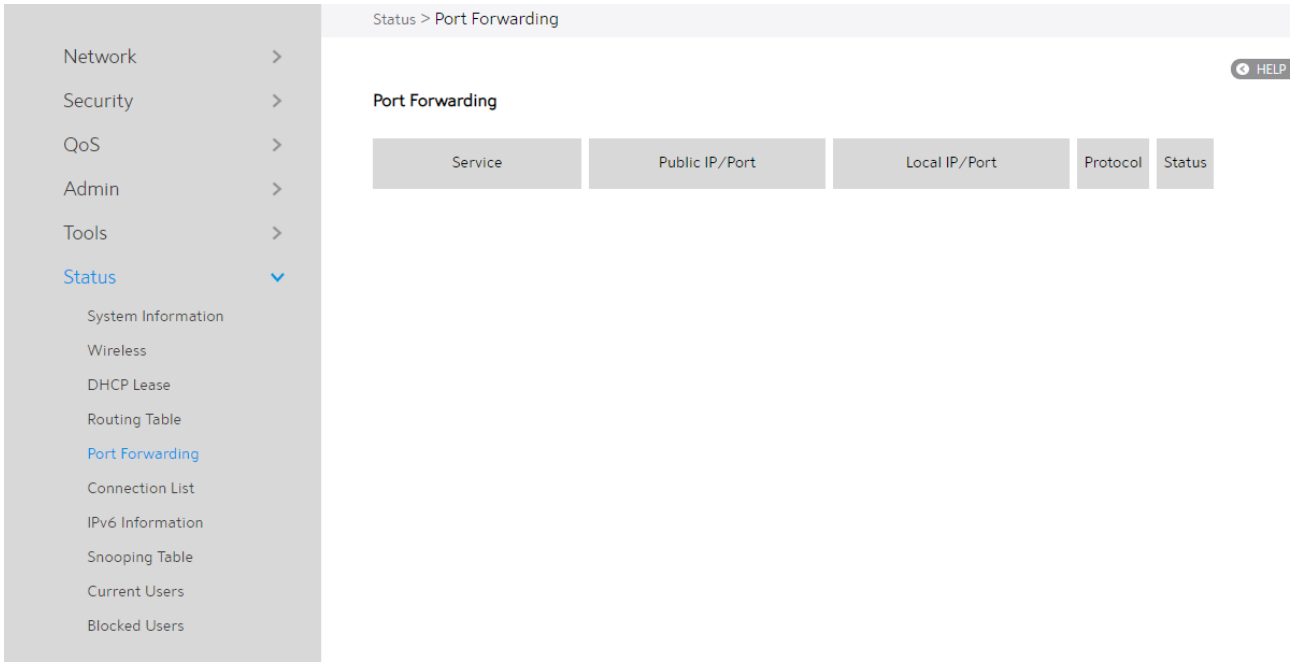
From the navigation panel, go to **Advanced** > **Status > Routing Table.**



2.4.6.5 Port Forwarding

This module is used to show the WiFi Router's port forwarding rules information, which contains both Port Forwarding module's rules and UpnP module's rules.

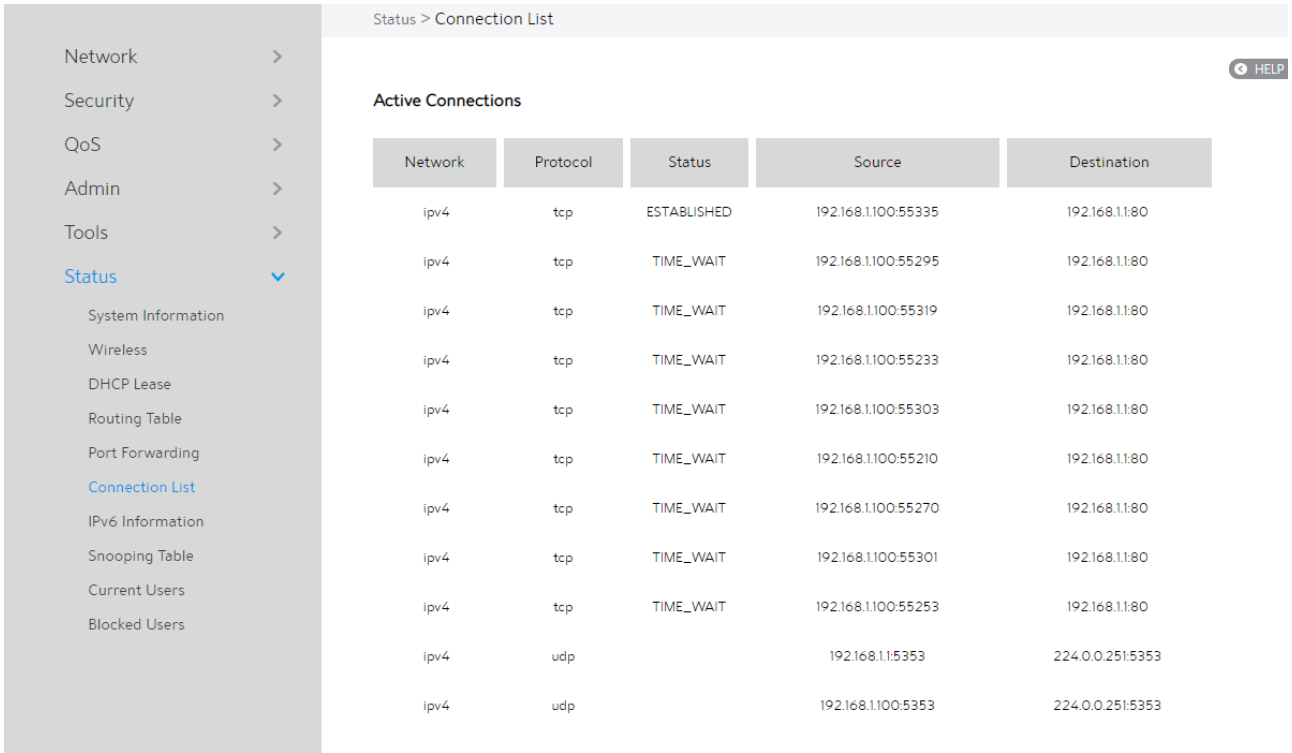
From the navigation panel, go to **Advanced** > **Status** > **Port Forwarding.**



2.4.6.6 Connection List

Show active connections status information.

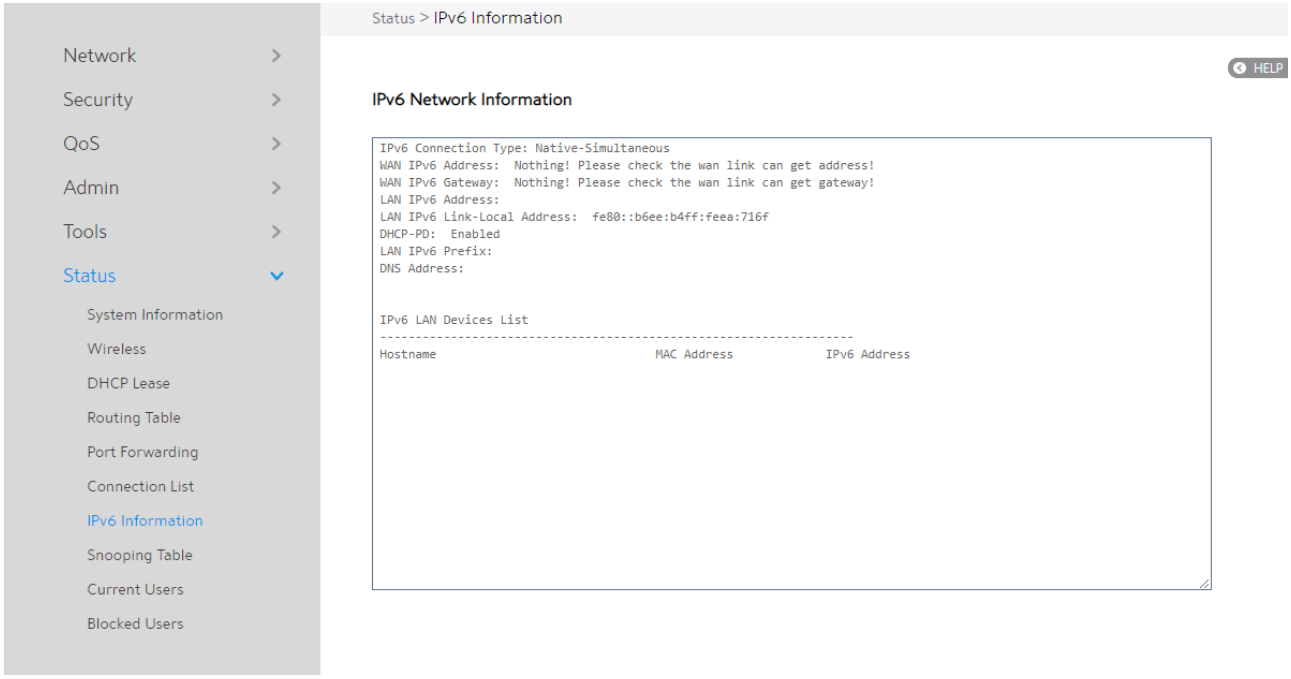
From the navigation panel, go to **Advanced** > **Status** > **Connection List.**



2.4.6.7 Ipv6 Information

This module displays details on WAN and LAN IPv6 information.

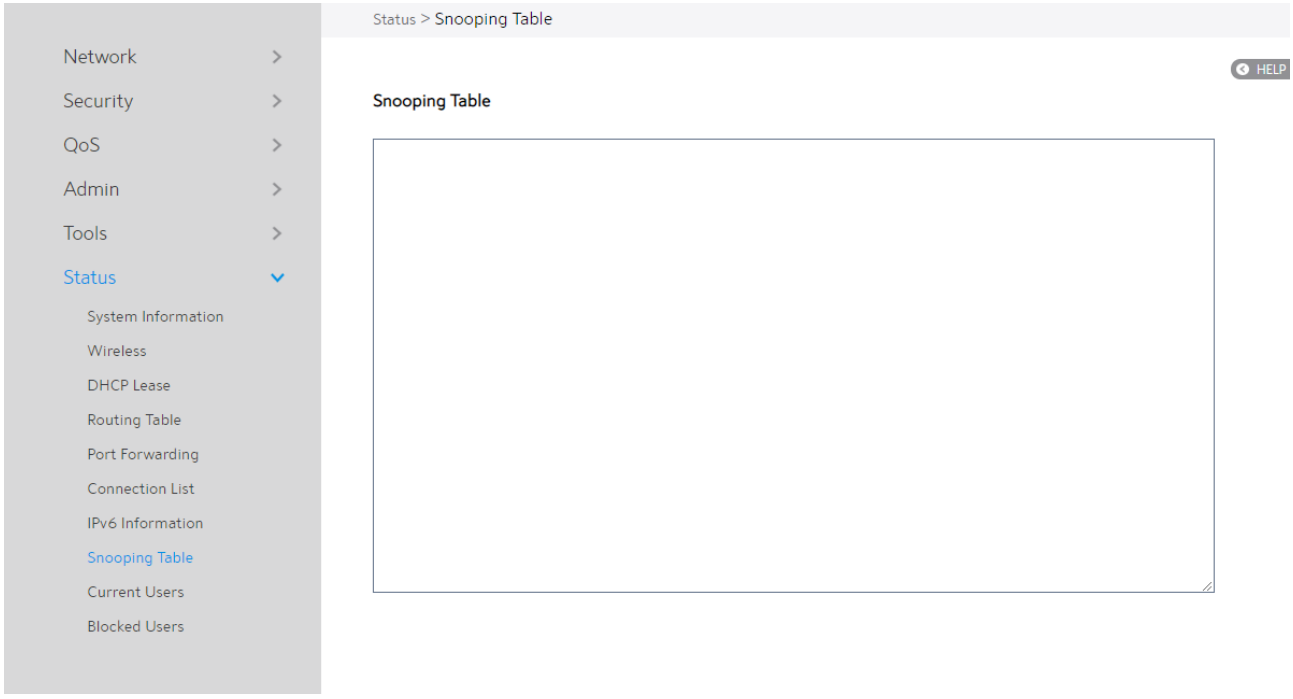
From the navigation panel, go to **Advanced** > **Status** > **IPv6 Information.**



2.4.6.8 Snooping Table

This module displays snooping table for client joins/leaves for both wired and wireless client streams.

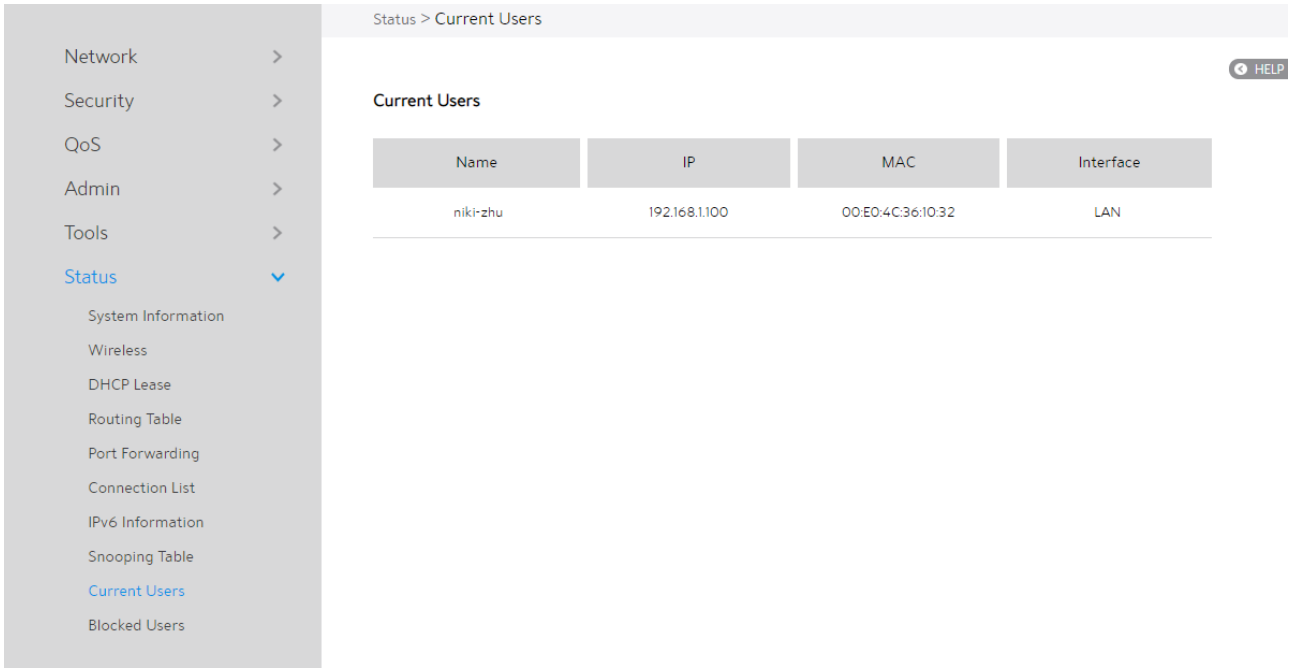
From the navigation panel, go to **Advanced** > **Status** > **Snooping Table.**



2.4.6.9 Current Users

This module displays current users who are permitted to get access to Internet through the router.

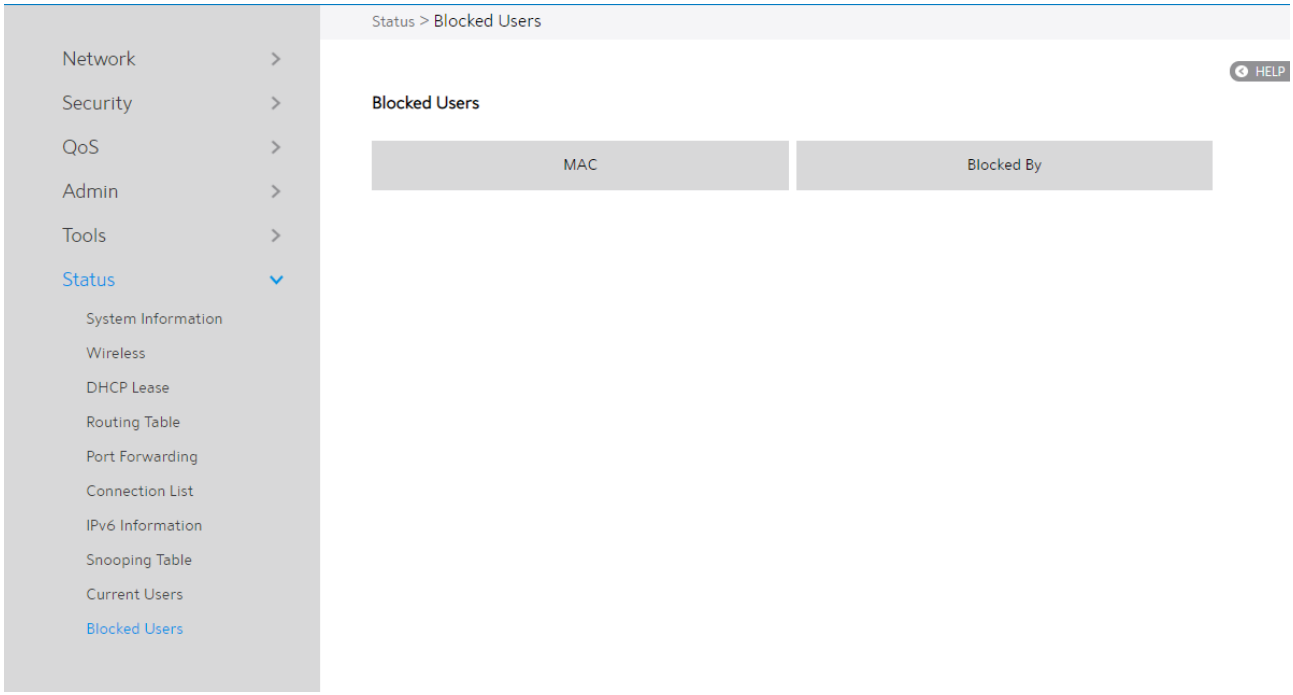
From the navigation panel, go to **Advanced** > **Status** > **Current Users.**



2.4.6.10 Blocked Users

This module displays blocked users who are not permitted to get access to Internet through the router.

From the navigation panel, go to **Advanced** > **Status** > **Blocked Users.**



3 FCC Statement

Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this 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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is restricted for indoor use.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24 cm between the radiator & your body.