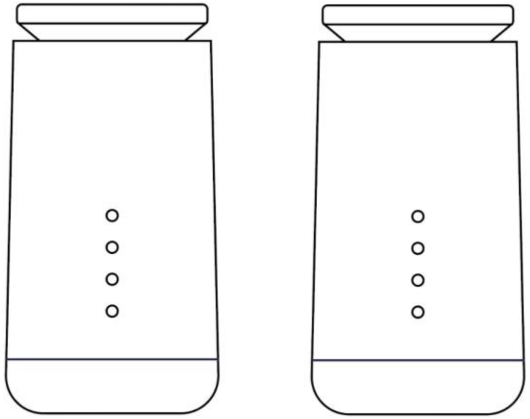
Mesh WiFi System 2 Pack

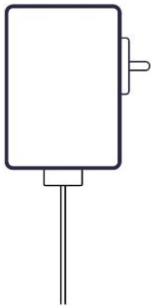
AXE10200 Tri-band Mesh WiFi 6E System

Table of Contents

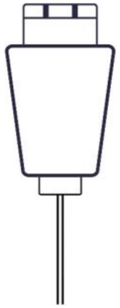
1. Package contents



Router x2



Power Adapter x2

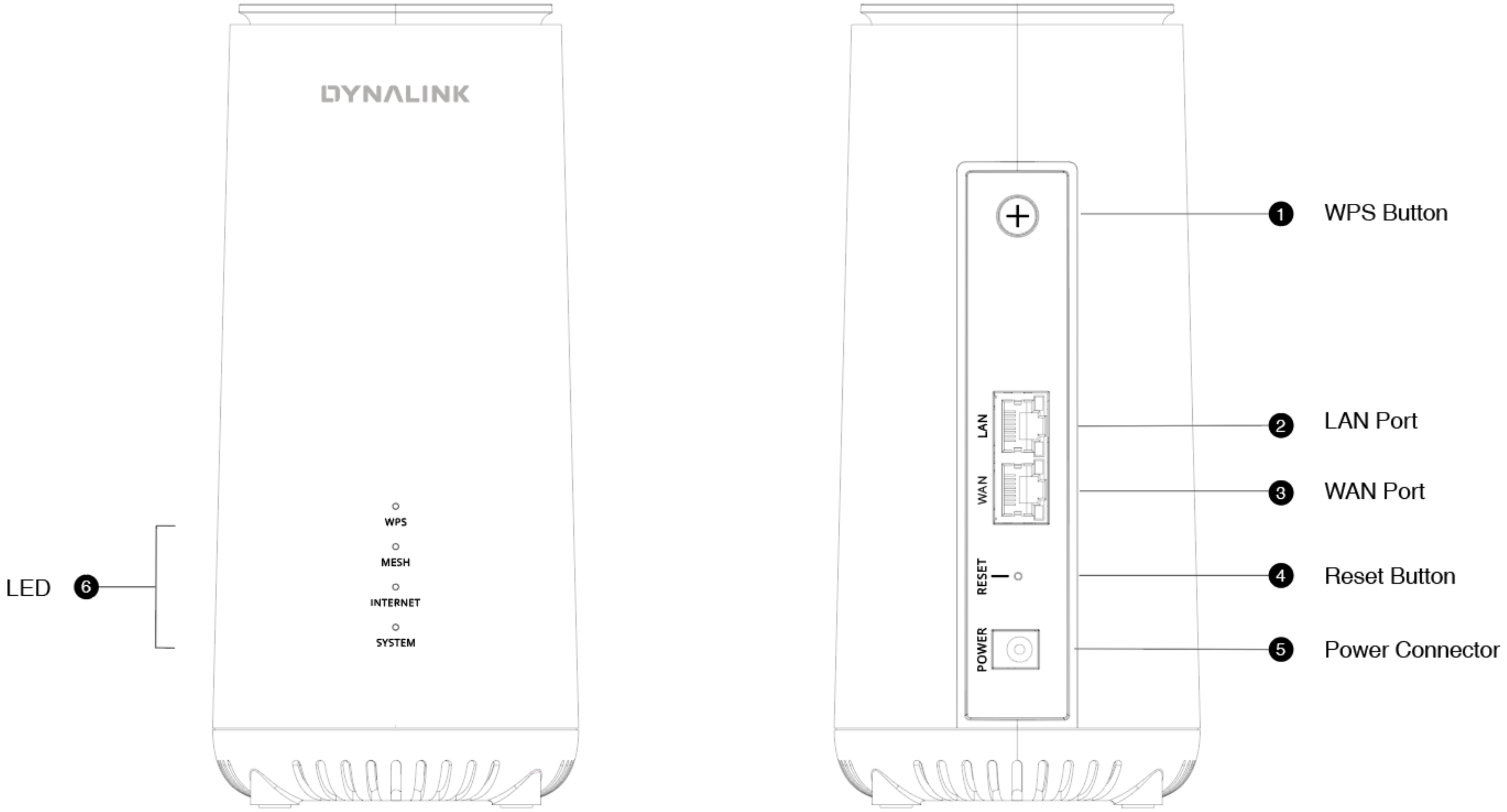


Ethernet Cable

Start Guide

2. Device description

Indicators and Connectors



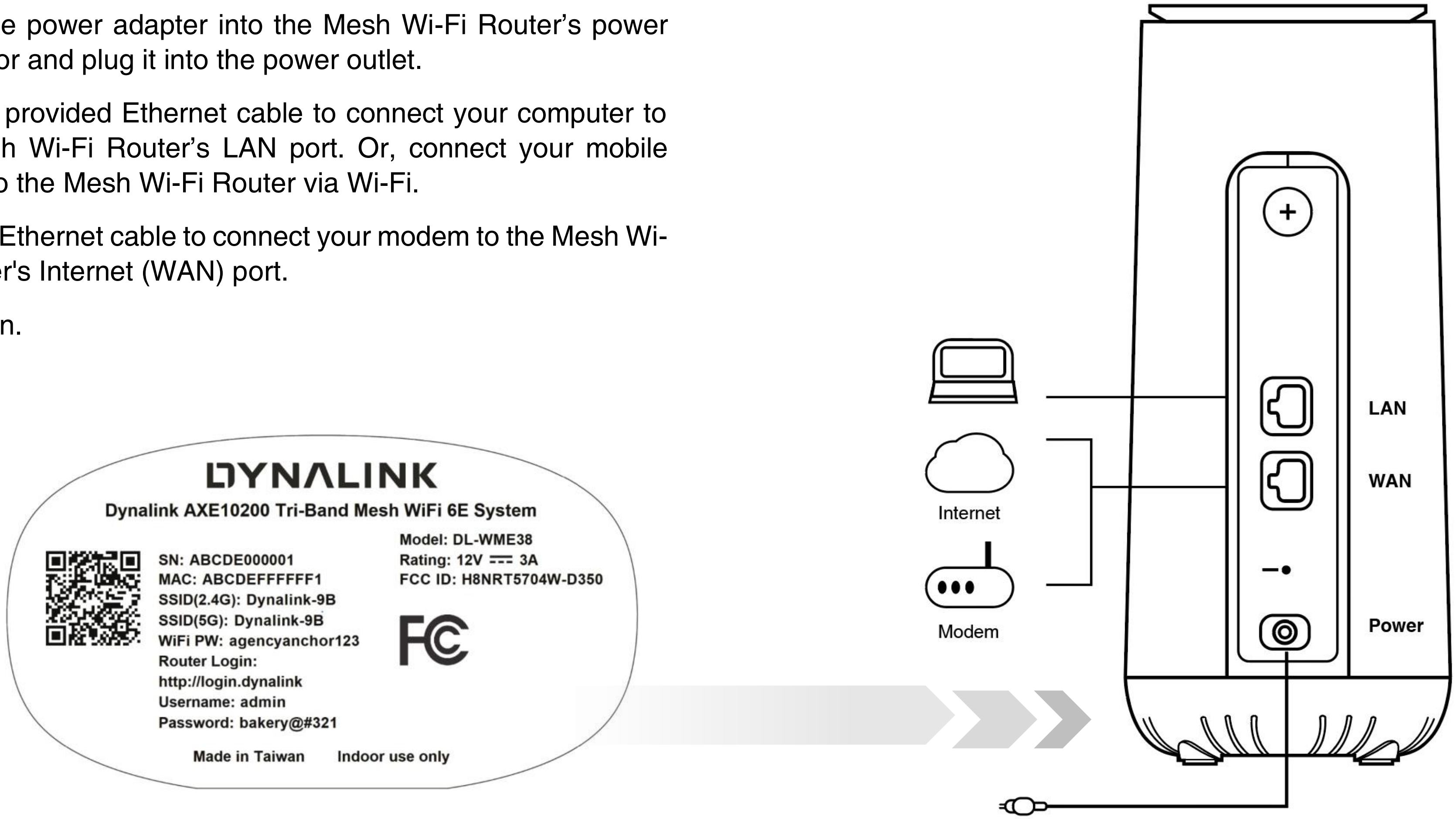
LED Behavior

The LEDs indicate the Mesh Wi-Fi Router’s power and connection.

LED Name	Color status		Time	Description
WPS (Only functional on the Main Router when pairing)	Green	Blinking	Every 0.5 sec.	Press WPS button, LED start to blink green, until WPS pairing success or fail or 2 minute timeout.
	Green	Solid on		WPS paring success, change to solid green for 10 seconds, then change to off.
	Red	Solid on	Continue for 10 sec.	WPS pairing failure or timeout, LED become solid Red for 10 seconds, then change to off.
Mesh	Orange	Blinking	Every 2 sec.	Waiting to be paired (default mode).
	Green	Blinking	Every 0.5 sec.	Paring is going on.
	Green	Solid		Paired and signal quality is good.
	Orange	Solid		Paired but signal quality is not good.
	Red	Solid	Last for 5 seconds and off.	Paring failed, will show RED for 5 seconds, and go back to previous mode. If this device is in default mode, will go back to blinking orange.
	OFF			Not paired and not in pairing mode.
Internet	Green			Device is Wifi Router and is connected to Internet.
Internet	Orange			Device is Wifi Router but not connected to Internet.
Internet	OFF			Device is Wifi Point or is in factory default mode.
System (Power on/Reboot)	Green	Blinking	Every 1 sec.	Power on (Booting). LED will blink blue for a while and become solid blue when boot process is done successfully.
	Red	Solid		Device failure.
	Green	Solid on		Power on Success.
System (Firmware Upgrade)	Green	Blinking	Every 0.5 sec.	Firmware upgrade process, LED will blink green till upgrade is done, then LED off and reboot.
System (Reset to Default)	Green	Blinking	Every 0.5 sec.	Press reset for 7+ seconds till LED start blinking, LED will blink green for 5 seconds to start reset process. Then LED off and reboot.

3. Let‘s get started

1. Insert the power adapter into the Mesh Wi-Fi Router's power connector and plug it into the power outlet.
2. Use the provided Ethernet cable to connect your computer to the Mesh Wi-Fi Router's LAN port. Or, connect your mobile device to the Mesh Wi-Fi Router via Wi-Fi.
3. Use the Ethernet cable to connect your modem to the Mesh Wi-Fi Router's Internet (WAN) port.
4. Power on.



DYNALINK

Dynalink AXE10200 Tri-Band Mesh WiFi 6E System

SN: ABCDE000001
MAC: ABCDEFFFFFF1
SSID(2.4G): Dynalink-9B
SSID(5G): Dynalink-9B
WiFi PW: agencyanchor123
Router Login:
http://login.dynalink
Username: admin
Password: bakery@#321

Model: DL-WME38
Rating: 12V ⎓ 3A
FCC ID: H8NRT5704W-D350

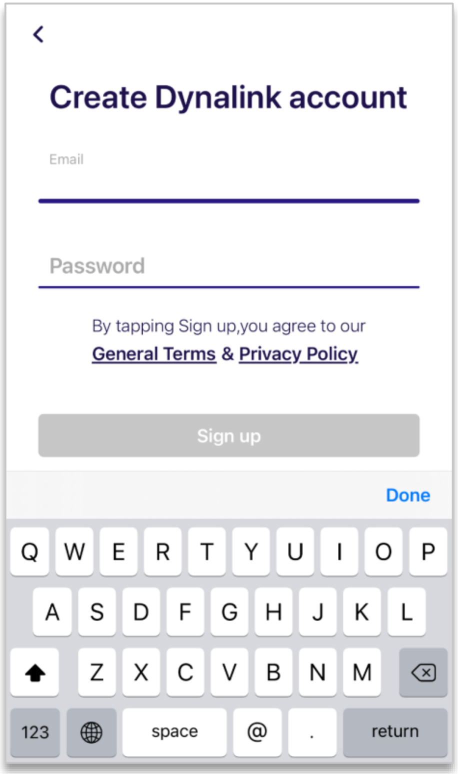
Made in Taiwan   Indoor use only

4. Configure your Mesh Wi-Fi Router

You can configure your Mesh Wi-Fi Router's network settings by using either your smartphone or computer.

4.1 How to access the configuration utility via mobile App

1. Install Dynalink Wi-Fi APP from Google Play or APP store.
2. Create Dynalink account with user's email account.
3. Refer to the label on the bottom of your Mesh Wi-Fi Router. Connect your mobile to router via Wi-Fi, there are 2 ways.
    - ✓ User can enter the SSID and Wi-Fi password on the label.
    - ✓ User can use APP to scan the QR_CODE on the label.
4. Follow the instruction on APP to setup internet connection.
5. We highly recommend you to upgrade to the latest APP version when you set up the first time. So as to achieve maximum performance and enable more features. Please navigate to the Settings page on the APP to update the firmware.



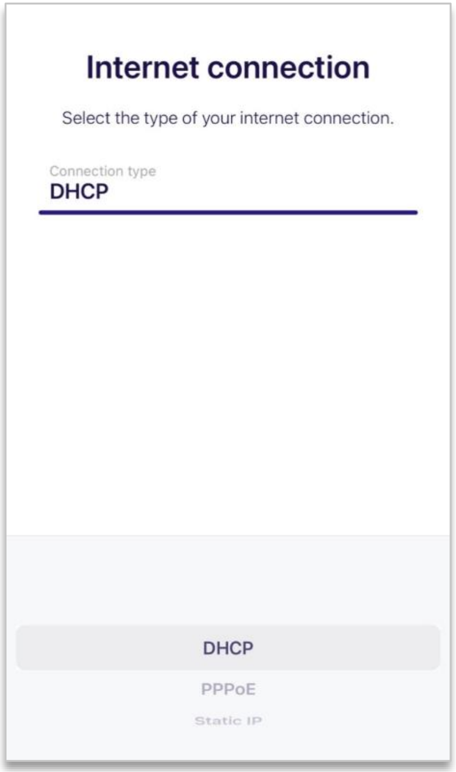
Create Dynalink account

Email

Password

By tapping Sign up,you agree to our General Terms & Privacy Policy

Sign up



Internet connection

Select the type of your internet connection.

Connection type
DHCP

4.2 How to access the configuration utility via Web browser

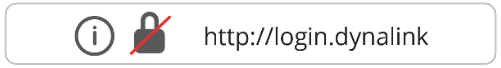
1. On your computer, scan available Wi-Fi networks.

2. Select the Wi-Fi Network Name (SSID) found on the white sticker on the bottom of your Mesh Wi-Fi Router.

3. Enter the unique password found on the white sticker on the bottom of your Mesh Wi-Fi Router.

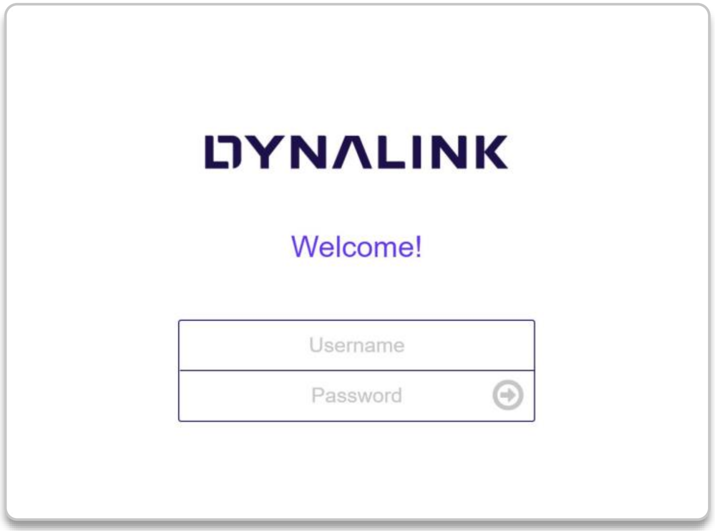
4. If preferred, you can use an Ethernet cable to connect your computer to the Mesh Wi-Fi Router's LAN port for configuration instead of following step1 to step3.

5. Launch your web browser and enter the Mesh Wi-Fi Router's domain name **http://login.dynalink** or IP address: **http://192.168.216.1** in the address bar.



http://login.dynalink

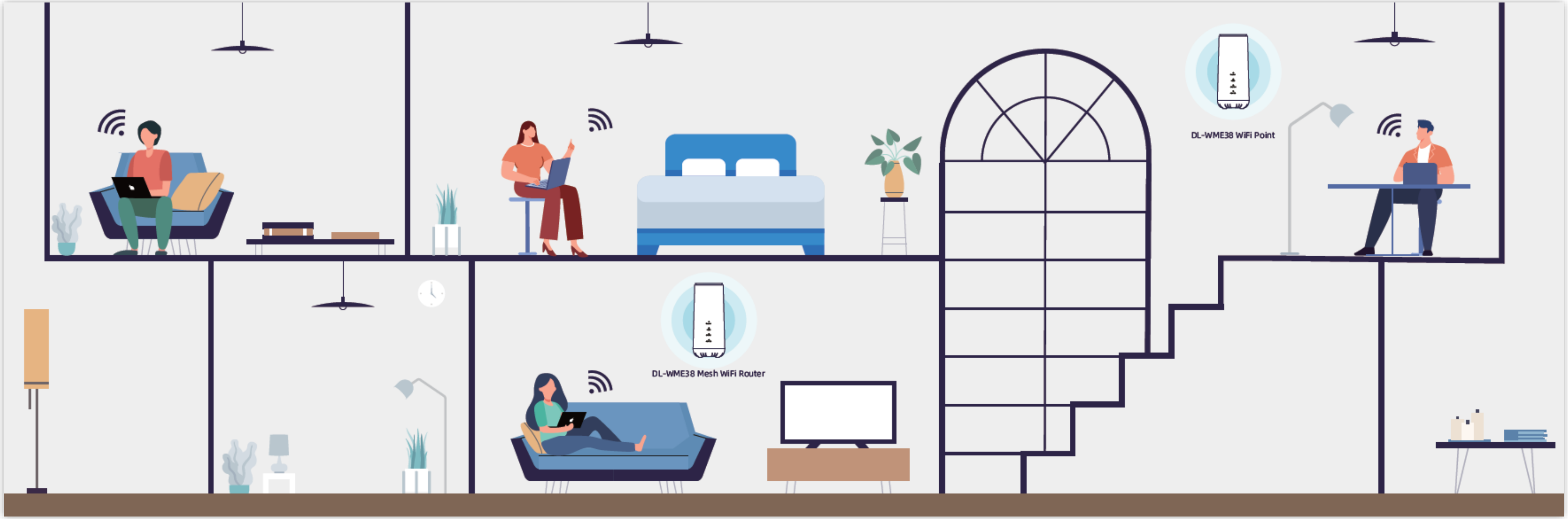
6. Enter the default username (admin) and password (check admin password on the label) to log in to your Mesh Wi-Fi Router's management page.



5. Set up a Mesh Wi-Fi system

Your DL-WME38 Router pair is a smart Mesh Wi-Fi system that enhances the Wi-Fi signal quality and extends its coverage with the use of a Mesh Wi-Fi Router paired with the Wifi Point. Follow these basic guidelines and start to establish your own smart Mesh Wi-Fi system.

1. Place two of your DL-WME38 in a short distance and power on. One of the DL-WME38 will be configured as the Mesh Wi-Fi Router which needs to be connected to the Internet firstly, and the other DL-WME38 will be configured the Wifi point.
2. Follow the Dynalink APP step-by-step instructions to finish the internet connection setup. When setup is successfully, your Mesh Wi-Fi Router INTERNET LED indicator shows green.
3. Then the APP proceeds to the step to add a Wifi Point, both Mesh Wi-Fi Router and Wifi Point will blink green on the WPS LED indicators. Your DL-WME38 will start to sync the Wi-Fi signal. And then both become solid green when successfully paired.
4. After the Mesh Wi-Fi system has been set up successfully, you can move your Wifi Point anywhere in your home to extend the Wi-Fi coverage. In case of setup trouble, follow the LED behavior on chapter 2 or see FAQ on chapter 7 for more information.

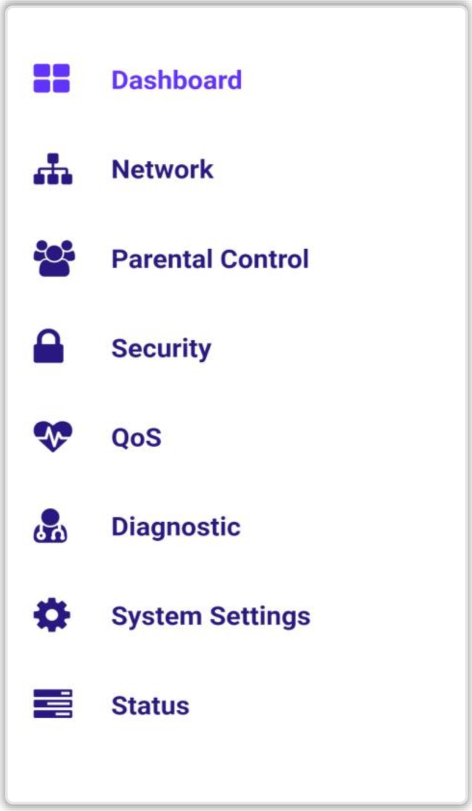


6. Specify Your Mesh Wi-Fi Router Settings

Your Mesh Wi-Fi Router comes with an intuitive Web User Interface (Web UI) that allows you to easily set up its feature.

Menu

Displays all the Mesh Wi-Fi Router functions.



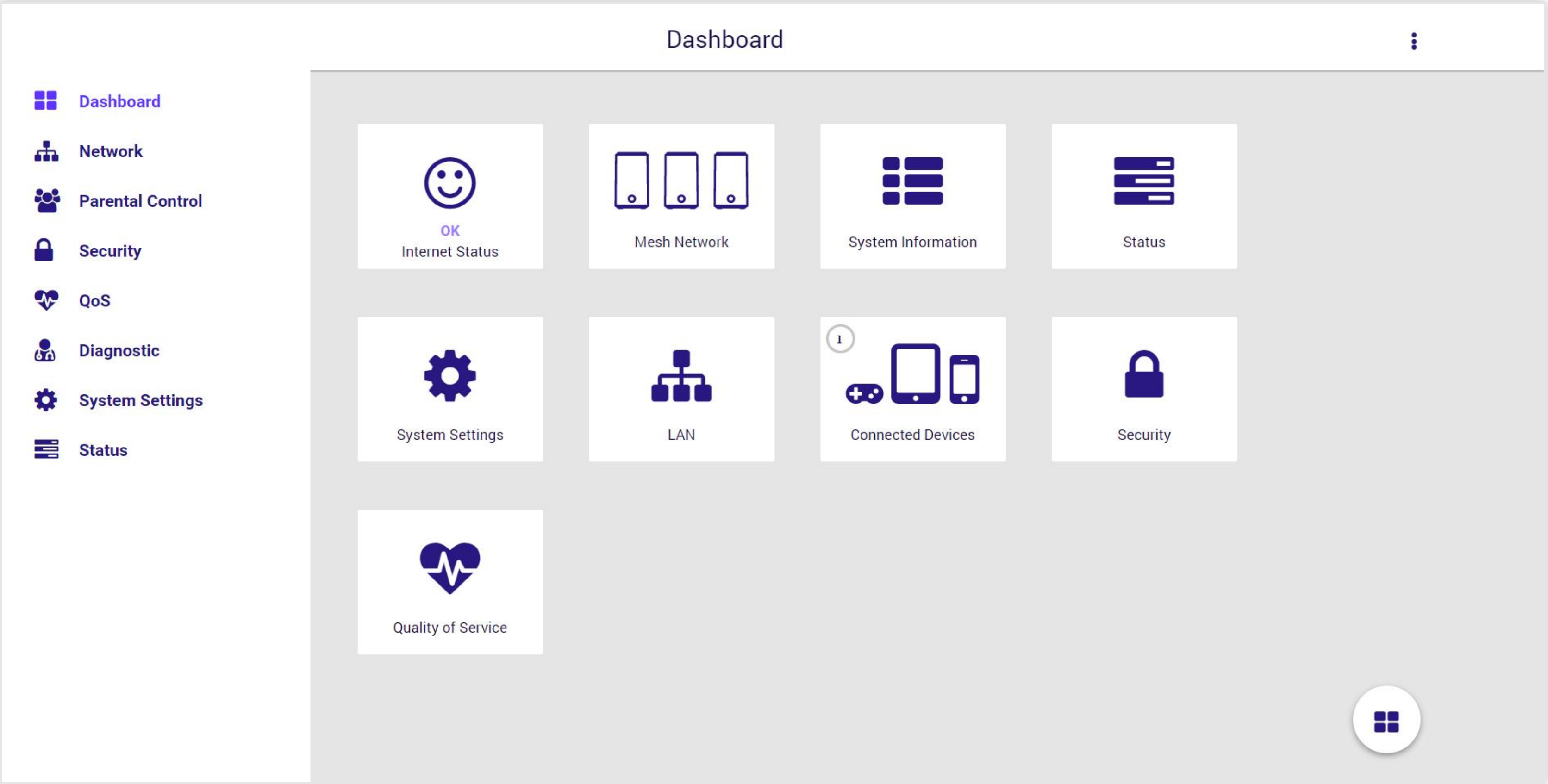
Save

Remember to save your settings with the save button after making changes.

Cancel
Save

6.1 Dashboard

The Dashboard shows a snapshot of your network status with quick links to key features of your Mesh Wi-Fi Router.



Click any of the icons on the dashboard: Internet Status, Mesh Network, System Information, Status, System Settings, LAN, Connected Devices, Security, and Quality of Service to access more information and navigate to the setting pages.

Internet Status shows the WAN, LAN, Ethernet, and Wi-Fi connection status of Mesh Wi-Fi Router. Navigate to the corresponding setting page by clicking the icons.

Mesh Network directly navigates to **Network > WiFi** and allows you to see the AP mode, Wi-Fi Settings, and Topology.

System Information comprehensively displays the information of router feature and status.

Status navigates to **Status > Wireless** and allows you to see detailed router status**.**

System Settings directly navigates to **System Settings > Password & Timezone** for you to configure system settings.

LAN navigates to **Network > LAN** for you to manage LAN setting.

Connected Devices displays the connection type, IP, MAC address, and manufacturer of all devices connected to your router.

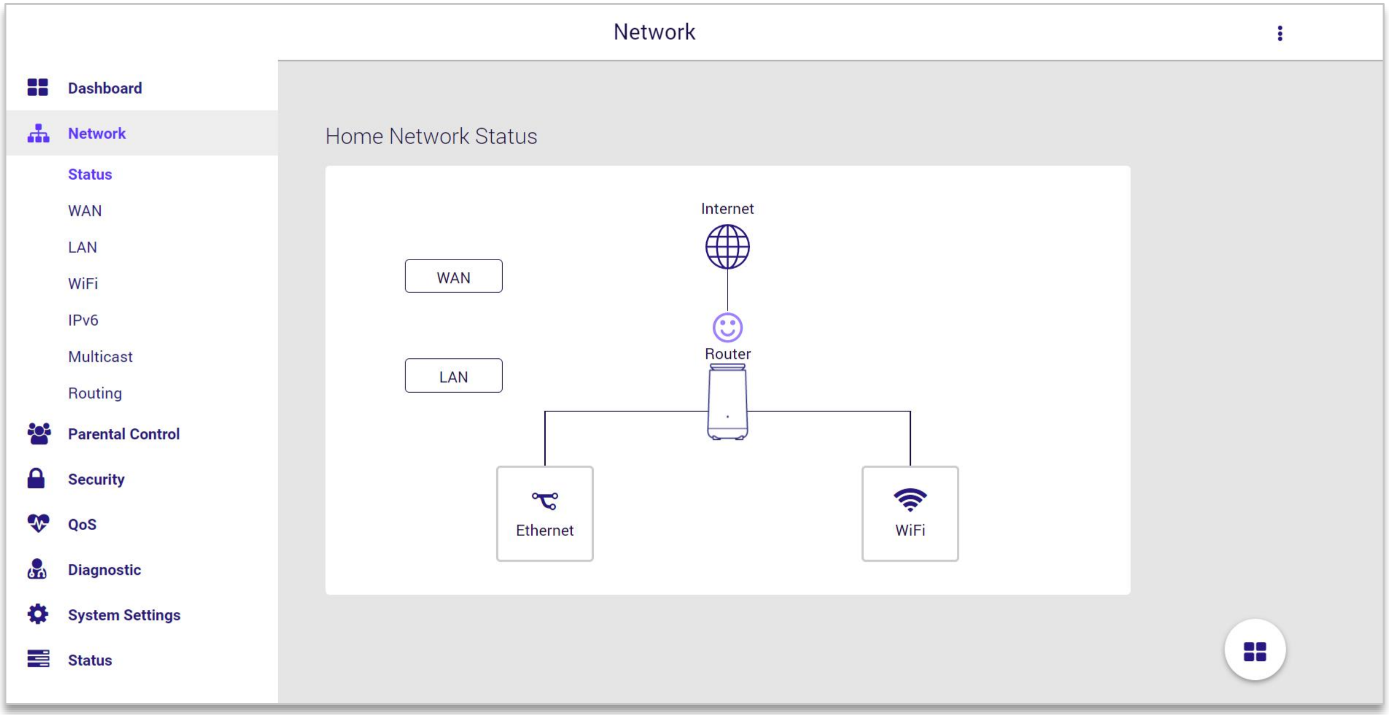
Security prompts out navigation of Firewall IPv4, Firewall IPv6, and VPN settings.

Quality of Service takes you to **QoS > Basic** directly**.**

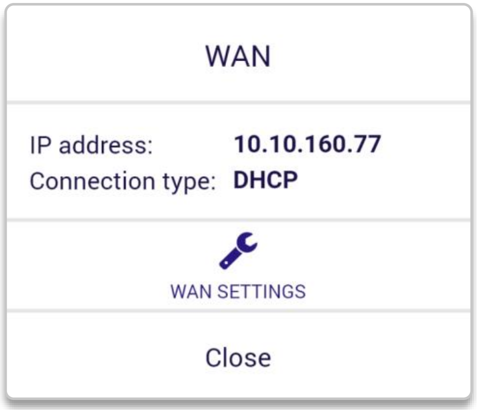
6.2 Network

6.2.1 Status

The panel shows a visual overview of connection status between Internet, router, and devices. Click the **WAN**, **LAN**, **Ethernet**, and **Wi-Fi** icons to access more information and quickly navigate to the corresponding setting pages.



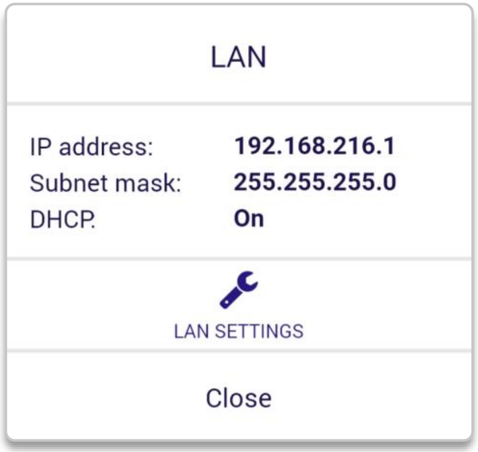
WAN: Displays IP address, connection type, and navigation link of the Mesh Wi-Fi Router's Wide Area Network (WAN) configuration page.



WAN

IP address: **10.10.160.77**
Connection type: **DHCP**

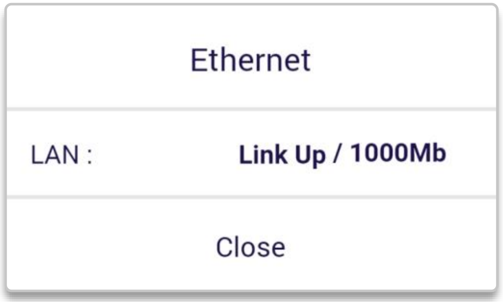
LAN: Displays IP address, subnet mask, DHCP status, and navigation link of the Mesh Wi-Fi Router's Local Area Network (LAN) configuration page.



LAN

IP address: **192.168.216.1**
Subnet mask: **255.255.255.0**
DHCP. **On**

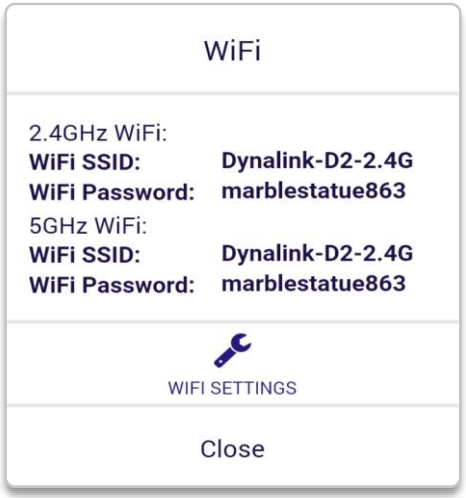
Ethernet: Displays the link up/down status and the capability of each LAN port.



Ethernet

LAN : **Link Up / 1000Mb**

Wi-Fi: Displays the status, SSID name, password, and the navigation link of Wi-Fi configuration page.



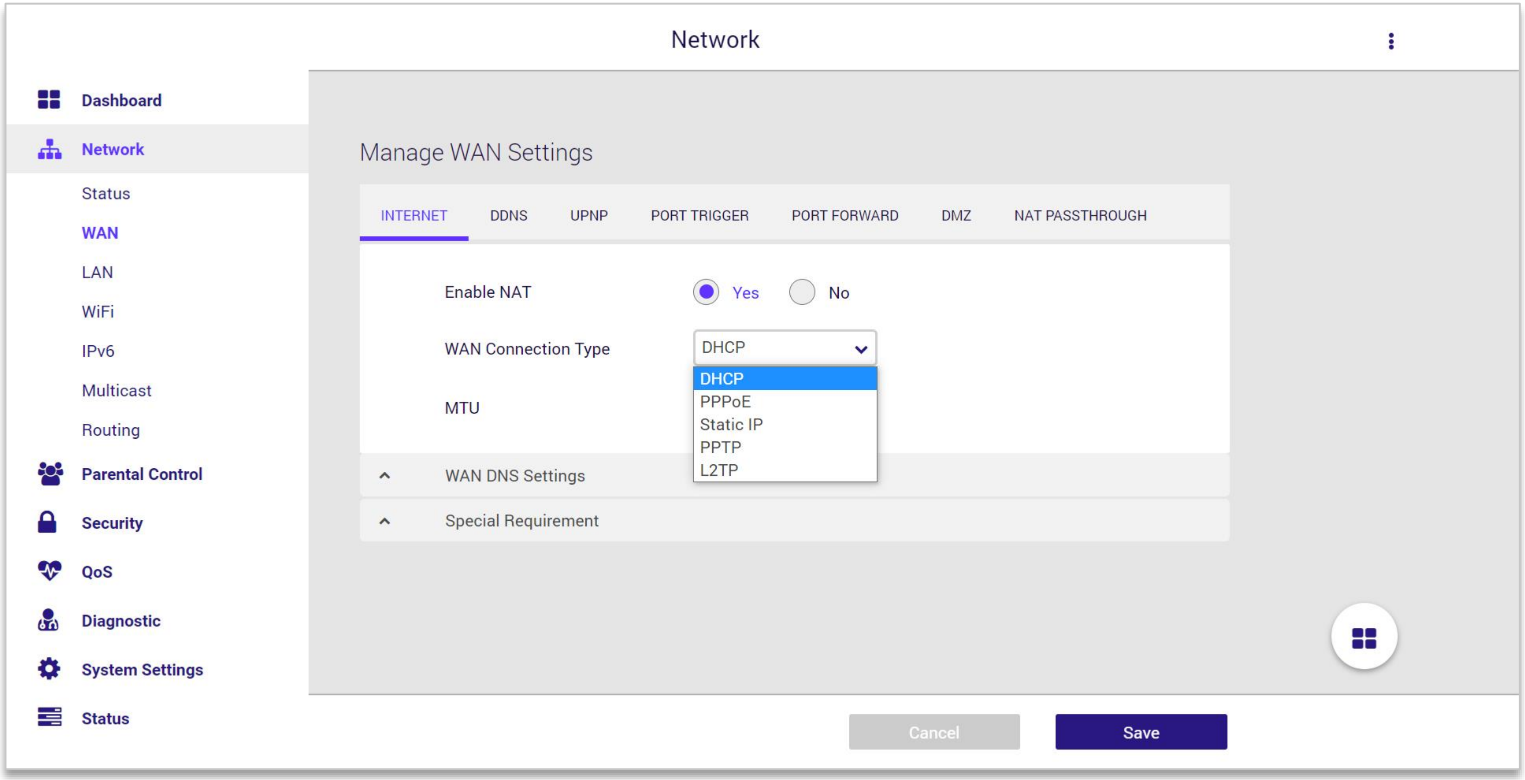
WiFi

2.4GHz WiFi:
WiFi SSID: **Dynalink-D2-2.4G**
WiFi Password: **marblestatue863**
5GHz WiFi:
WiFi SSID: **Dynalink-D2-2.4G**
WiFi Password: **marblestatue863**

6.2.2 WAN

6.2.2.1 Internet

The feature allows you to configure the settings of various WAN connection types.



Network

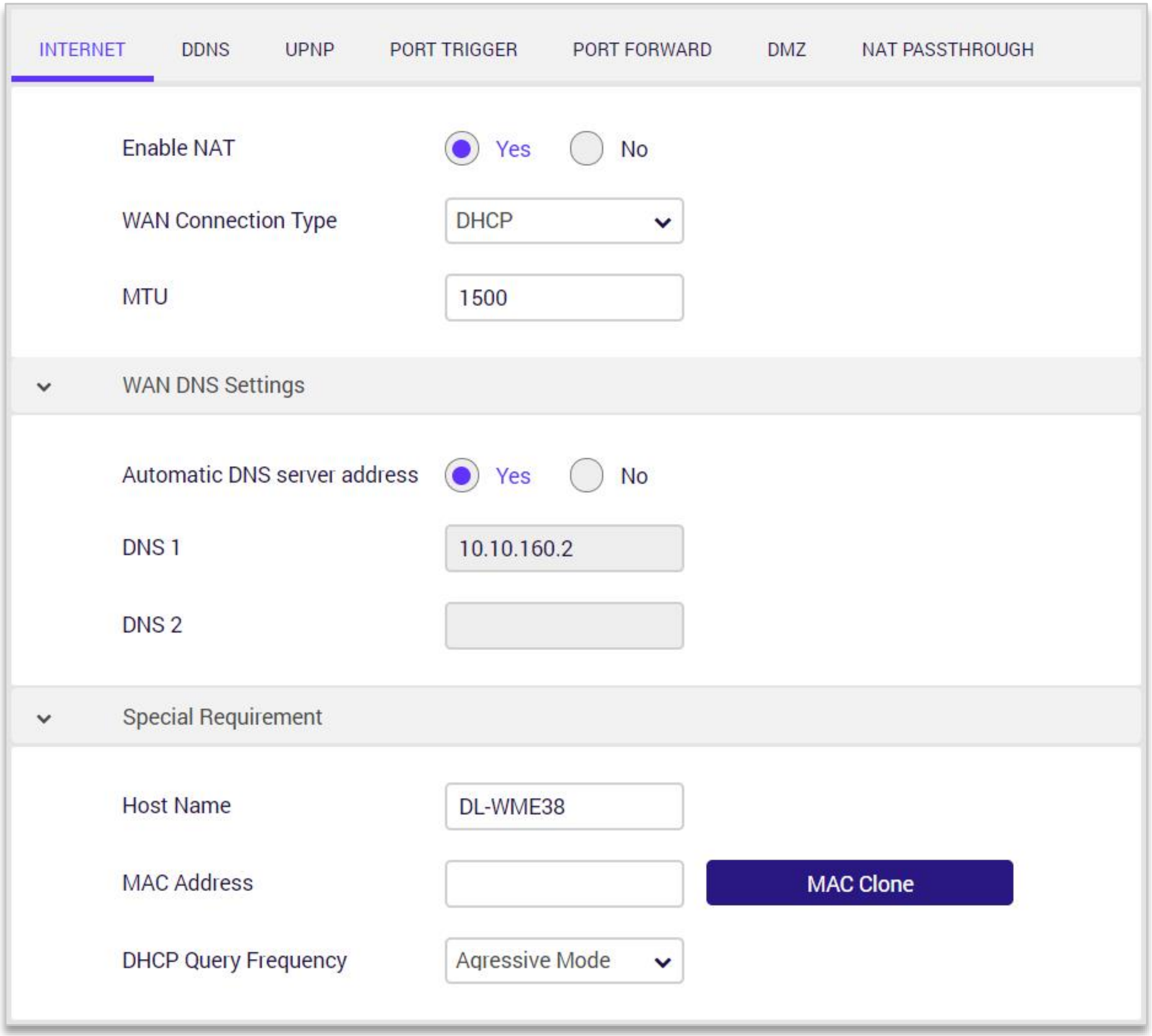
Manage WAN Settings

Enable NAT ● Yes ○ No

WAN Connection Type: DHCP

MTU

WAN Connection Type 1 - DHCP



Enable NAT ● Yes ○ No

WAN Connection Type: DHCP

MTU: 1500

WAN DNS Settings

Automatic DNS server address ● Yes ○ No

DNS 1: 10.10.160.2

DNS 2:

Special Requirement

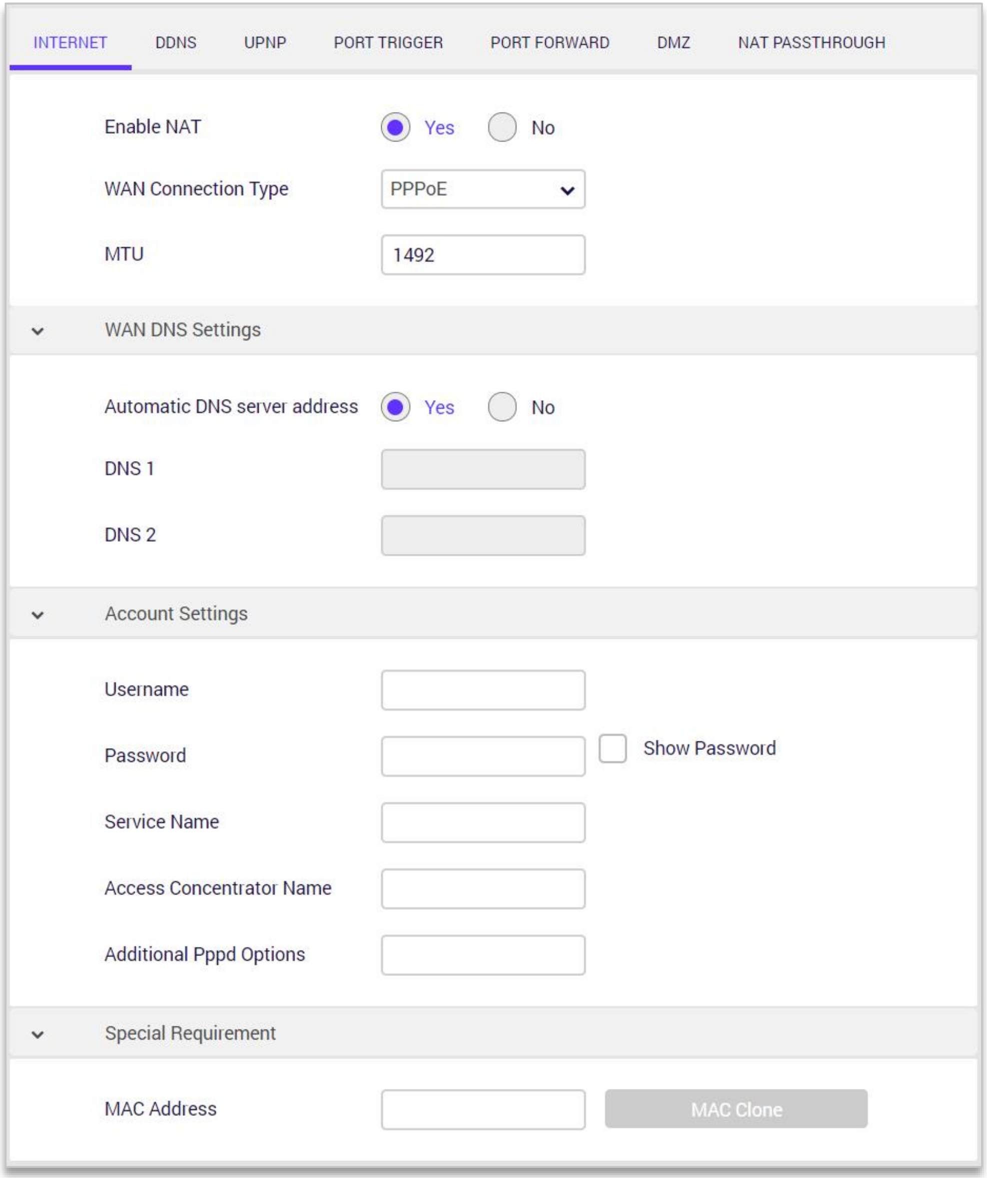
Host Name: DL-WME38

MAC Address:

DHCP Query Frequency: Aqressive Mode

DHCP	
Enable NAT	Network Address Translation (NAT) is a method to substitute the information of IP address space from private IP to public IP when the devices which connected to the router access to the Internet. The router records the source/destination address on table and maps the IP while receiving packages from Internet.
WAN Connection Type	The connection type to access the Internet.
MTU	Maximum transmission unit (MTU) is the largest data packet for the router capable to transmit and receive. The data packets exceed MTU will be fragmented while transmitting and be reassembled once the packets reach the destination.
WAN DNS Settings	
Automatic DNS server address	Allows your router to get Domain name Service (DNS) IP address from the Internet Service Provider (ISP) automatically.
DNS1	Enter an IP address as the primary domain name server.
DNS2	Enter an IP address as the secondary domain name server.
Special Requirement	
Host Name	Enter a host name for your router.
MAC Address	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.
DHCP Query Frequency	Some Internet Service Providers might block MAC addresses if the device makes DHCP queries too often. To prevent this, change the DHCP query frequency. In the default Aggressive mode, if router does not get a response from the ISP, it sends another query after 20 seconds and makes three more attempts. In Normal mode, if router doesn’t get a response from the ISP, it makes a second query after 120 seconds and makes two more attempts.

WAN Connection Type 2 - PPPoE



Enable NAT ● Yes ○ No

WAN Connection Type: PPPoE

MTU: 1492

WAN DNS Settings

Automatic DNS server address ● Yes ○ No

DNS 1

DNS 2

Account Settings

Username

Password □ Show Password

Service Name

Access Concentrator Name

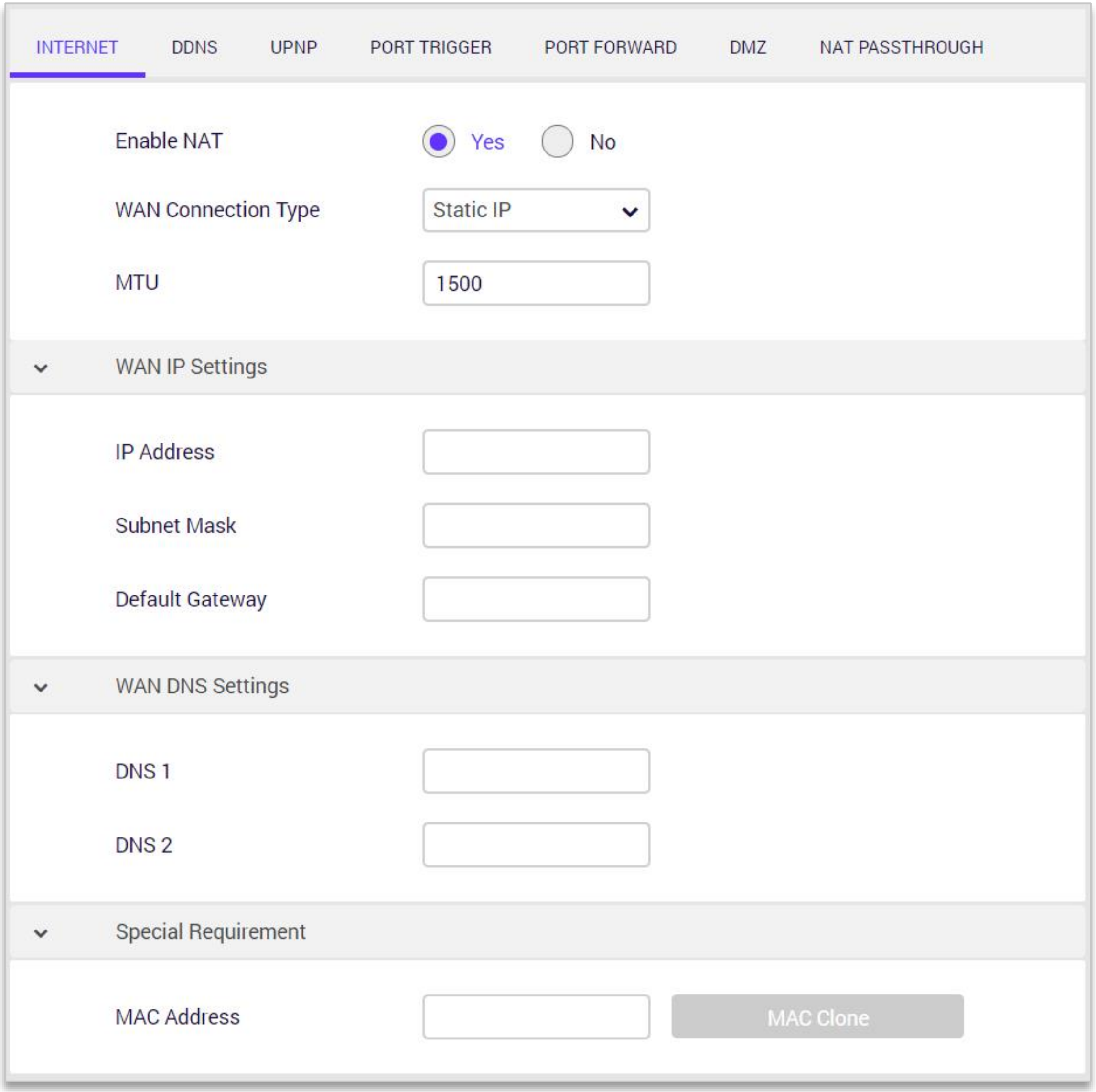
Additional Pppd Options

Special Requirement

MAC Address

PPPoE	
Enable NAT	Network Address Translation (NAT) is a method to substitute the information of IP address space from private IP to public IP when the devices which connected to the router access to the Internet. The router records the source/destination address on table and maps the IP while receiving packages from Internet.
WAN Connection Type	The connection type to access Internet.
MTU	Maximum transmission unit (MTU) is the largest data packet for the router capable to transmit and receive. The data packets exceed MTU will be fragmented while transmitting and be reassembled once the packets reach the destination.
WAN DNS Settings	
Automatic DNS server address	Allows your router to get Domain name Service (DNS) IP address from the Internet Service Provider (ISP) automatically.
DNS1	Enter an IP address as the primary domain name server.
DNS2	Enter an IP address as the secondary domain name server.
Account Settings	
Username	Enter username provided by your ISP.
Password	Enter password provided by your ISP.
Service Name	This field is optional and may be specified by some ISPs. Check with your ISP and fill them in if required.
Access Concentrator Name	This field is optional and may be specified by some ISPs. Check with your ISP and fill them in if required.
Additional Pppd Options	This item may be specified by some ISPs. Check with your ISP and fill them in if required.
Special Requirement	
MAC Address	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.

Connection Type 3 - Static IP



Enable NAT ● Yes ○ No

WAN Connection Type: Static IP

MTU: 1500

WAN IP Settings

IP Address

Subnet Mask

Default Gateway

WAN DNS Settings

DNS 1

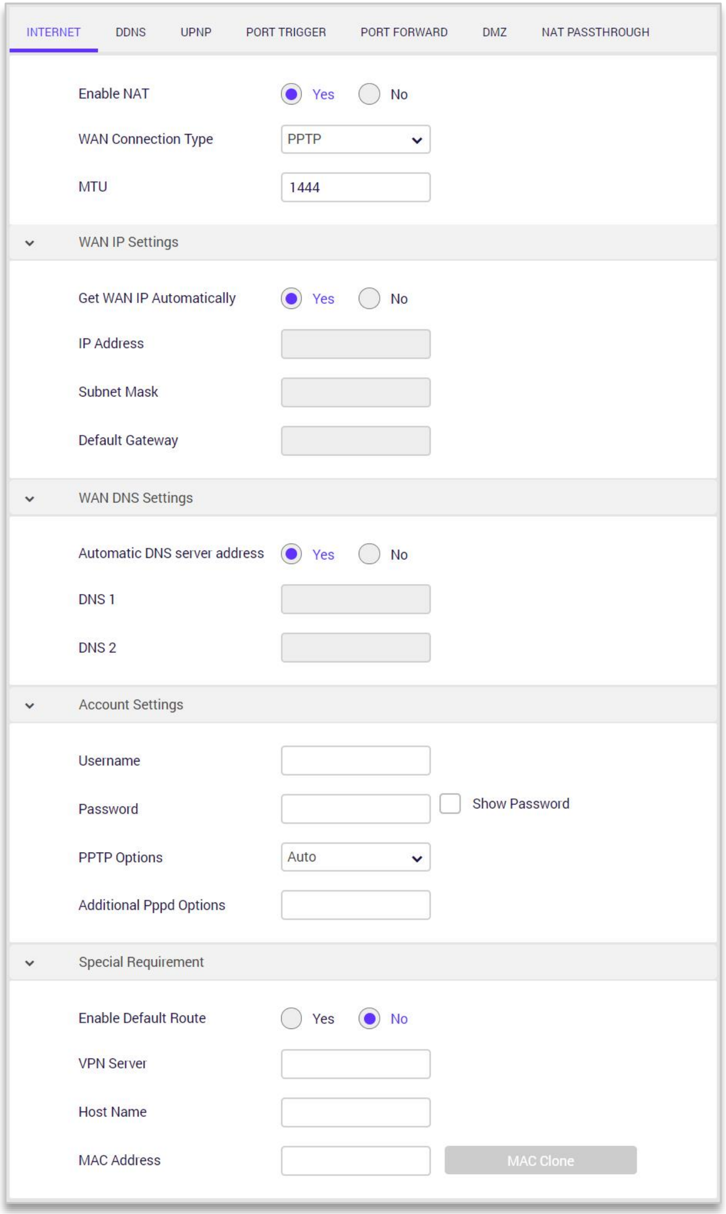
DNS 2

Special Requirement

MAC Address

Static IP	
Enable NAT	Network Address Translation (NAT) is a method to substitute the information of IP address space from private IP to public IP when the devices which connected to the router access to the Internet. The router records the source/destination address on table and maps the IP while receiving packages from Internet.
WAN Connection Type	The connection type to access Internet.
MTU	Maximum transmission unit (MTU) is the largest data packet for the router capable to transmit and receive. The data packets exceed MTU will be fragmented while transmitting and be reassembled once the packets reach the destination.
WAN IP Settings	
IP Address	If your WAN connection requires a static IP address, key in the IP address in this field.
Subnet Mask	If your WAN connection requires a static IP address, key in the subnet mask in this field.
Default Gateway	If your WAN connection requires a static IP address, key in the gateway IP address in this field.
WAN DNS Settings	
Automatic DNS server address	Allows your router to get Domain name Service (DNS) IP address from the Internet Service Provider (ISP) automatically.
DNS1	Enter an IP address as the primary domain name server.
DNS2	Enter an IP address as the secondary domain name server.
Special Requirement	
MAC Address	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.

WAN Connection Type 4 - PPTP



Enable NAT	● Yes ○ No
WAN Connection Type	PPTP
MTU	1444

WAN IP Settings

Get WAN IP Automatically	● Yes ○ No
IP Address	
Subnet Mask	
Default Gateway	

WAN DNS Settings

Automatic DNS server address	● Yes ○ No
DNS 1	
DNS 2	

Account Settings

Username	
Password	□ Show Password
PPTP Options	Auto
Additional Pppd Options	

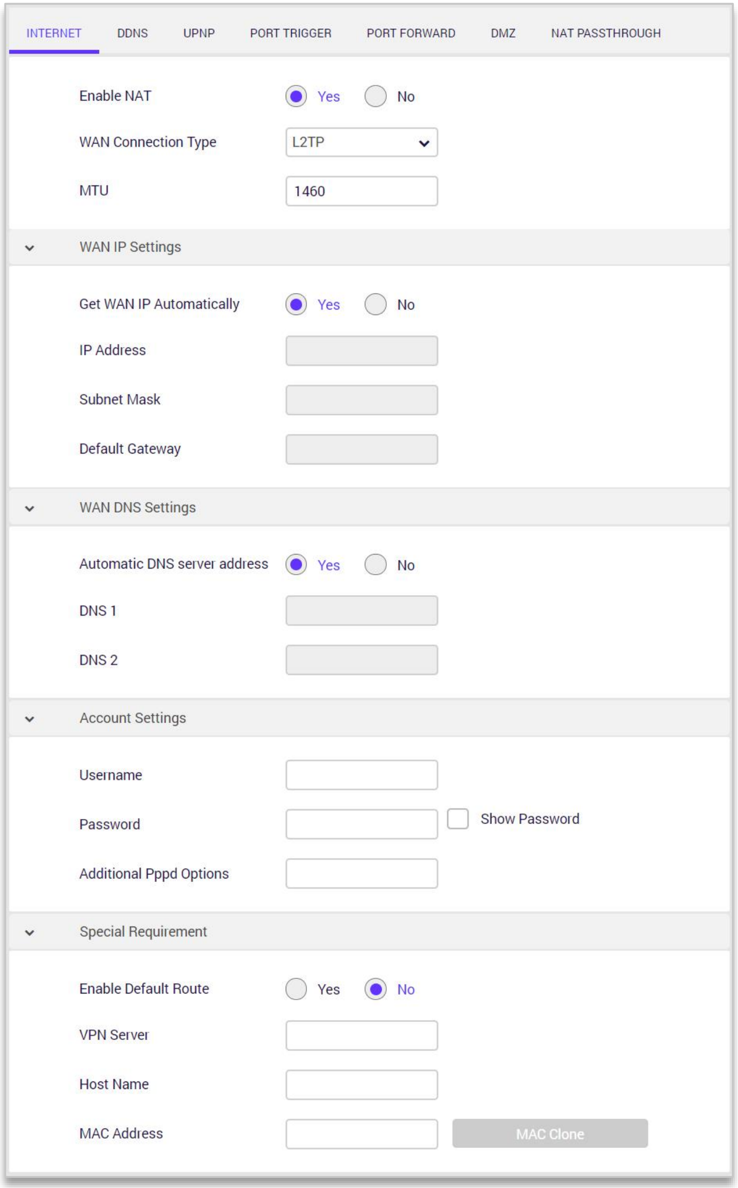
Special Requirement

Enable Default Route	○ Yes ● No
VPN Server	
Host Name	
MAC Address	MAC Clone

PPTP	
Enable NAT	Network Address Translation (NAT) is a method to substitute the information of IP address space from private IP to public IP when the devices which connected to the router access to the Internet. The router records the source/destination address on table and maps the IP while receiving packages from Internet.
WAN Connection Type	The connection type to access Internet.
MTU	Maximum transmission unit (MTU) is the largest data packet for the router capable to transmit and receive. The data packets exceed MTU will be fragmented while transmitting and be reassembled once the packets reach the destination.
WAN IP Settings	
Get WAN IP Automatically	Automatically get WAN IP address from the ISP.
IP Address	If your WAN connection requires a static IP address, key in the IP address in this field.
Subnet Mask	If your WAN connection requires a static IP address, key in the subnet mask in this field
Default Gateway	If your WAN connection requires a static IP address, key in the gateway IP address in this field.
WAN DNS Settings	
Automatic DNS server address	Allows your router to get Domain name Service (DNS) IP address from the Internet Service Provider (ISP) automatically.
DNS1	Enter an IP address as the primary domain name server.
DNS2	Enter an IP address as the secondary domain name server.
Account Settings	
Username	Enter username provided by your ISP.
Password	Enter password provided by your ISP.
PPTP Options	This item may be specified by some ISPs. Check with your ISP and fill them in if required.
Additional Pppd Options	This item may be specified by some ISPs. Check with your ISP and fill them in if required.

Special Requirement	
Enable Default Route	Enable default route if requires.
VPN Server	If your WAN connection type is PPTP or L2TP, please enter the server name or server IP of the VPN Server.
Host Name	You can provide a host name for your router. It’s usually requested by your ISP.
MAC Address	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.

WAN Connection Type 5 - L2TP



Enable NAT ● Yes ○ No

WAN Connection Type: L2TP

MTU: 1460

WAN IP Settings

Get WAN IP Automatically ● Yes ○ No

IP Address

Subnet Mask

Default Gateway

WAN DNS Settings

Automatic DNS server address ● Yes ○ No

DNS 1

DNS 2

Account Settings

Username

Password □ Show Password

Additional Pppd Options

Special Requirement

Enable Default Route ○ Yes ● No

VPN Server

Host Name

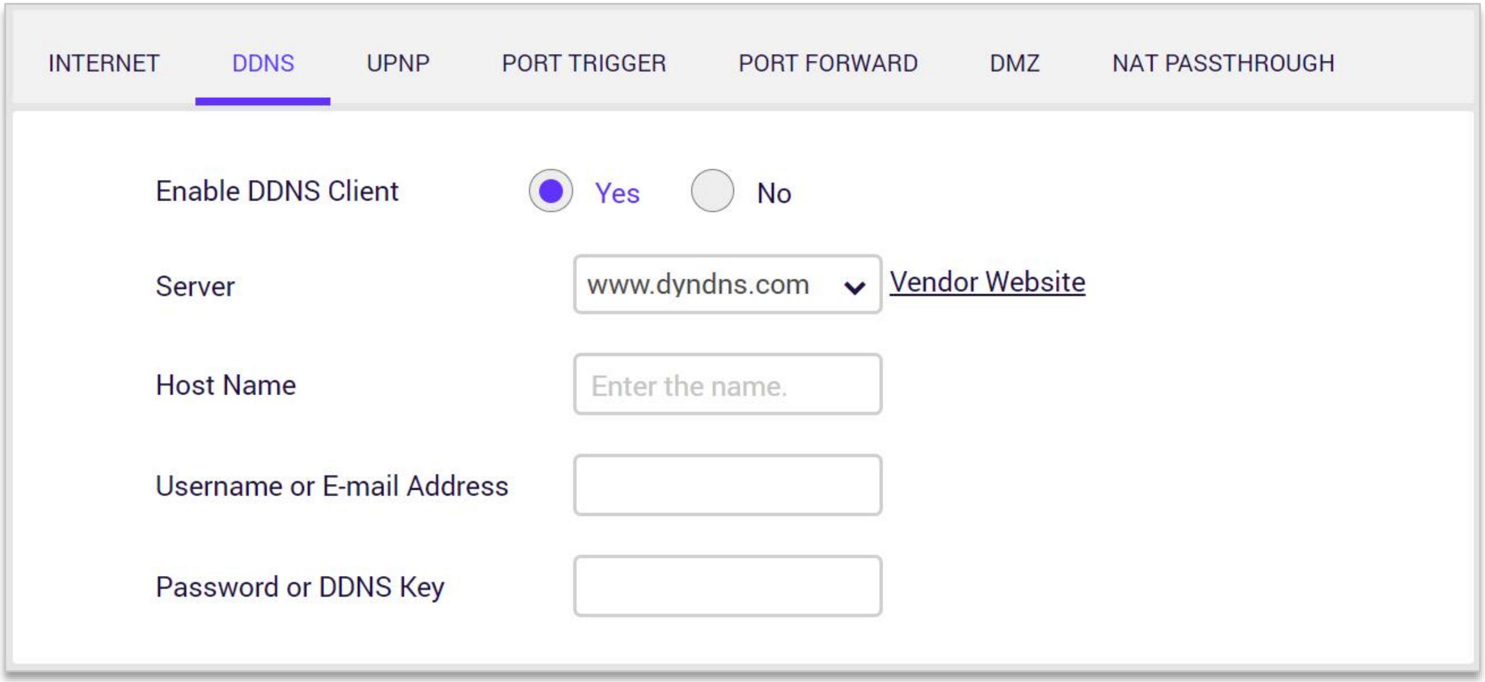
MAC Address

L2TP	
Enable NAT	Network Address Translation (NAT) is a method to substitute the information of IP address space from private IP to public IP when the devices which connected to the router access to the Internet. The router records the source/destination address on table and maps the IP while receiving packages from Internet.
WAN Connection Type	The connection type to access Internet.
MTU	Maximum transmission unit (MTU) is the largest data packet for the router capable to transmit and receive. The data packets exceed MTU will be fragmented while transmitting and be reassembled once the packets reach the destination.
WAN IP Settings	
Get WAN IP Automatically	Automatically get WAN IP address from the ISP.
IP Address	If your WAN connection requires a static IP address, key in the IP address in this field.
Subnet Mask	If your WAN connection requires a static IP address, key in the subnet mask in this field
Default Gateway	If your WAN connection requires a static IP address, key in the gateway IP address in this field.
WAN DNS Settings	
Automatic DNS server address	Allows your router to get Domain name Service (DNS) IP address from the Internet Service Provider (ISP) automatically.
DNS1	Enter an IP address as the primary domain name server.
DNS2	Enter an IP address as the secondary domain name server.
Account Settings	
Username	Enter username provided by your ISP.
Password	Enter password provided by your ISP.
Additional Pppd Options	This item may be specified by some ISPs. Check with your ISP and fill them in if required.

Special Requirement	
Enable Default Route	Enable default route if requires.
VPN Server	If your WAN connection type is PPTP or L2TP, please enter the server name or server IP of the VPN Server.
Host Name	You can provide a host name for your router. It’s usually requested by your ISP.
MAC Address	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.

6.2.2.2 DDNS

Dynamic DNS (DDNS) feature allows network clients to access your Mesh Wi-Fi Router through a specific domain name. Despite the WAN public IP of the router assigned randomly, you can always use one domain name to access your Mesh Wi-Fi Router from Internet as long as the domain name of your Mesh Wi-Fi Router is successfully registered on DDNS server.



Enable DDNS Client ● Yes ○ No

Server www.dyndns.com

Host Name Enter the name.

Username or E-mail Address

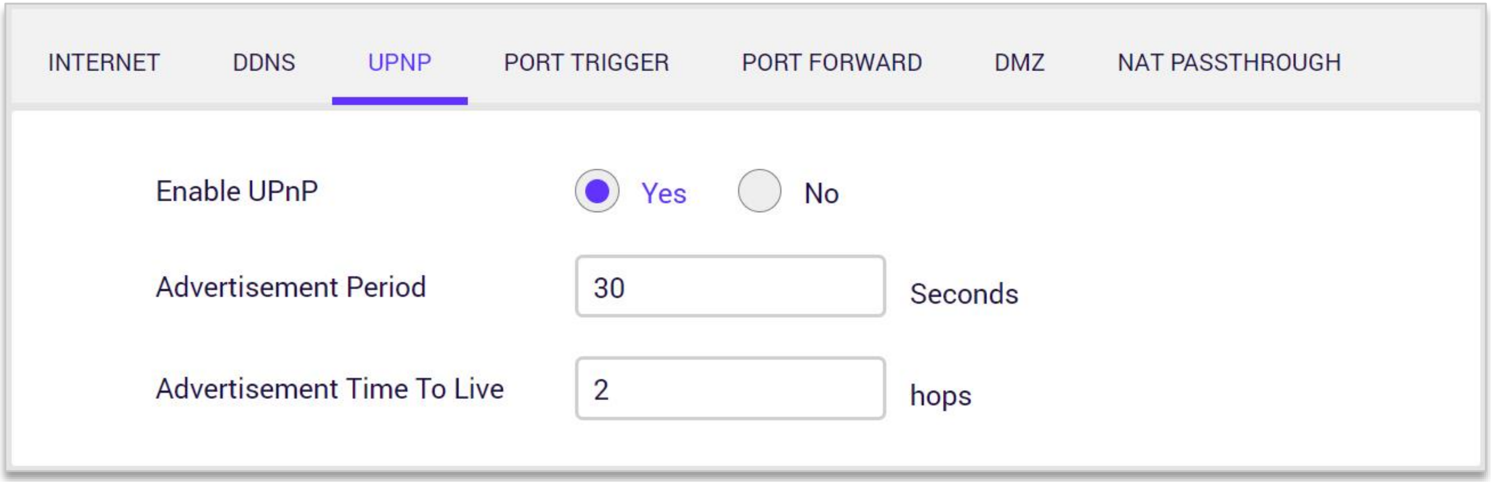
Password or DDNS Key

Enable/Disable DDNS Client	Enable or disable DDNS Client.
Server	The dropdown menu displays the vendors of DDNS Server. Clicking the hyperlink to access the website, then register a domain name for your router.
Host Name	Enter the domain name you registered on DDNS server.
Username or E-Mail Address	Enter the username you registered on DDNS server.
Password or DDNS Key	Enter the password you registered on DDNS server.

6.2.2.3 UPnP

Universal plug-and-play (UPnP) allows network devices, such as computers, printers, mobile devices etc. to discover each other's presence on network automatically. A UPnP-enabled device communicates directly with other connected UPnP devices and establishes functional network service. It's typically used for data sharing, communications and entertainment purposes. Despite there is a disadvantage of consideration for security concerns, this set of networking protocols sometimes can be useful when the application operated properly.

Enable/Disable UPnP	Set UPnP to active or inactive by selecting the radio button according to your requirements.
Advertisement Period	Enter the time period to decide the frequency of your router to advertise UPnP information.
Advertisement Time To Live	Enter the number of hops for each advertisement when the UPnP packet sent.



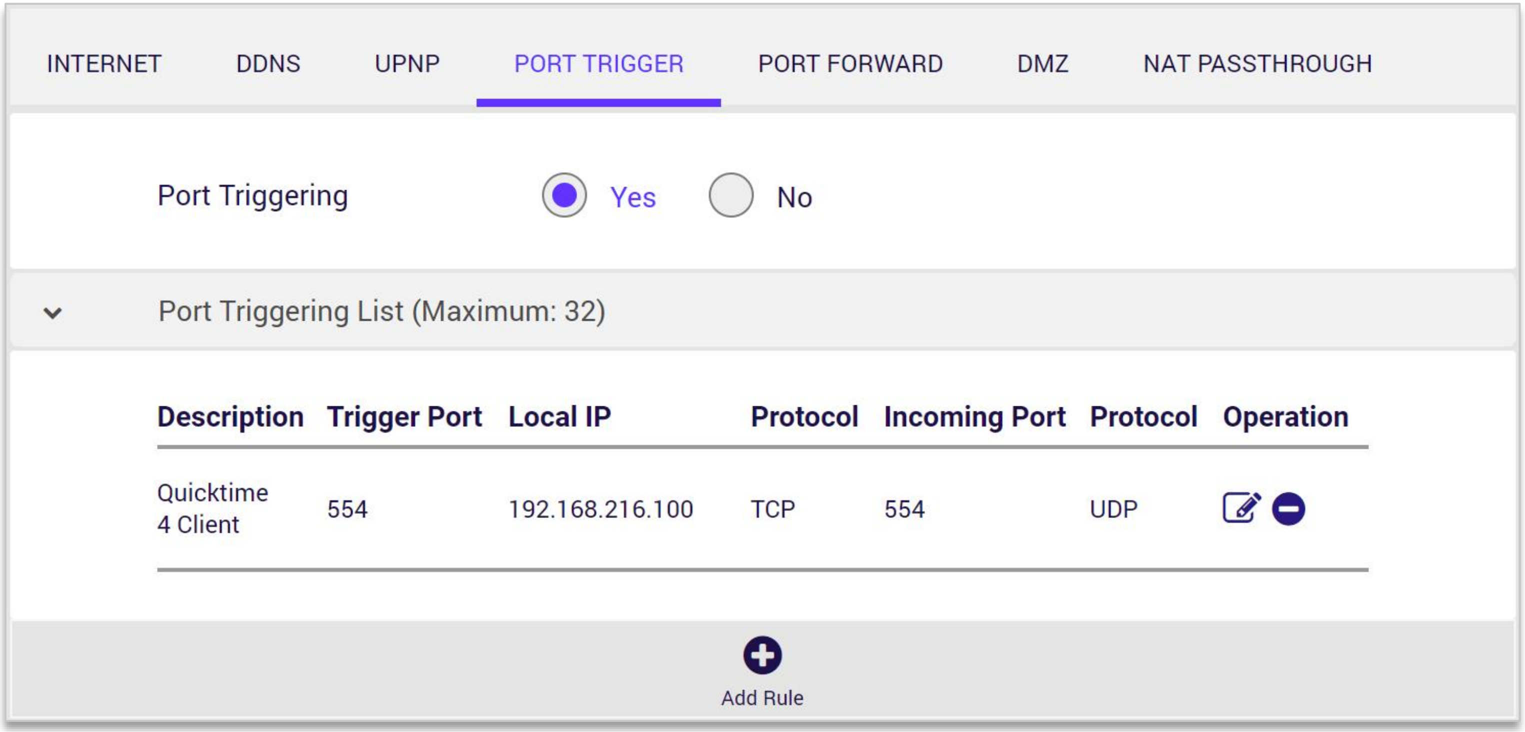
Enable UPnP ● Yes ○ No

Advertisement Period 30 Seconds

Advertisement Time To Live 2 hops

6.2.2.4 Port Trigger

Port trigger allows you to define the specific inbound and outbound TCP/UDP ports for LAN devices to communicate with Network devices unrestrictedly. The Incoming Ports are not activated until the corresponding Trigger Port is triggered by detecting packets transmission.



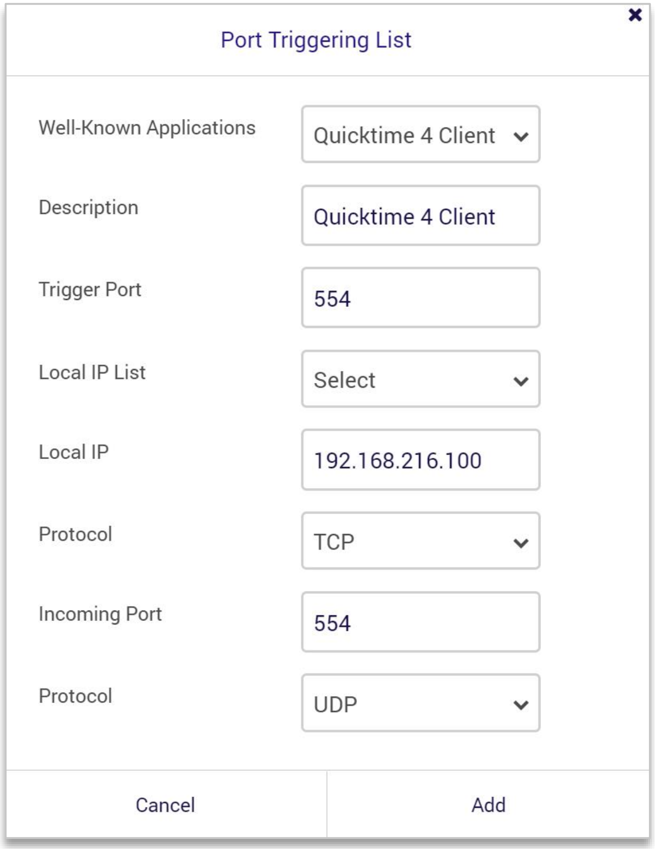
Port Triggering ● Yes ○ No

Port Triggering List (Maximum: 32)

Description	Trigger Port	Local IP	Protocol	Incoming Port	Protocol	Operation
Quicktime 4 Client	554	192.168.216.100	TCP	554	UDP	

1. Select the radio button to enable/disable port trigger.
2. Click **Add Rule ⊕**. Enter the parameters in accordance with your requirements.
3. Click **Add** to have the rule created on port triggering list and then click Save to apply your changes. You can remove or edit any port trigger rule by using the ⊖ and ✎ icons.

   Note: The maximum number on port triggering list is 32 rules.



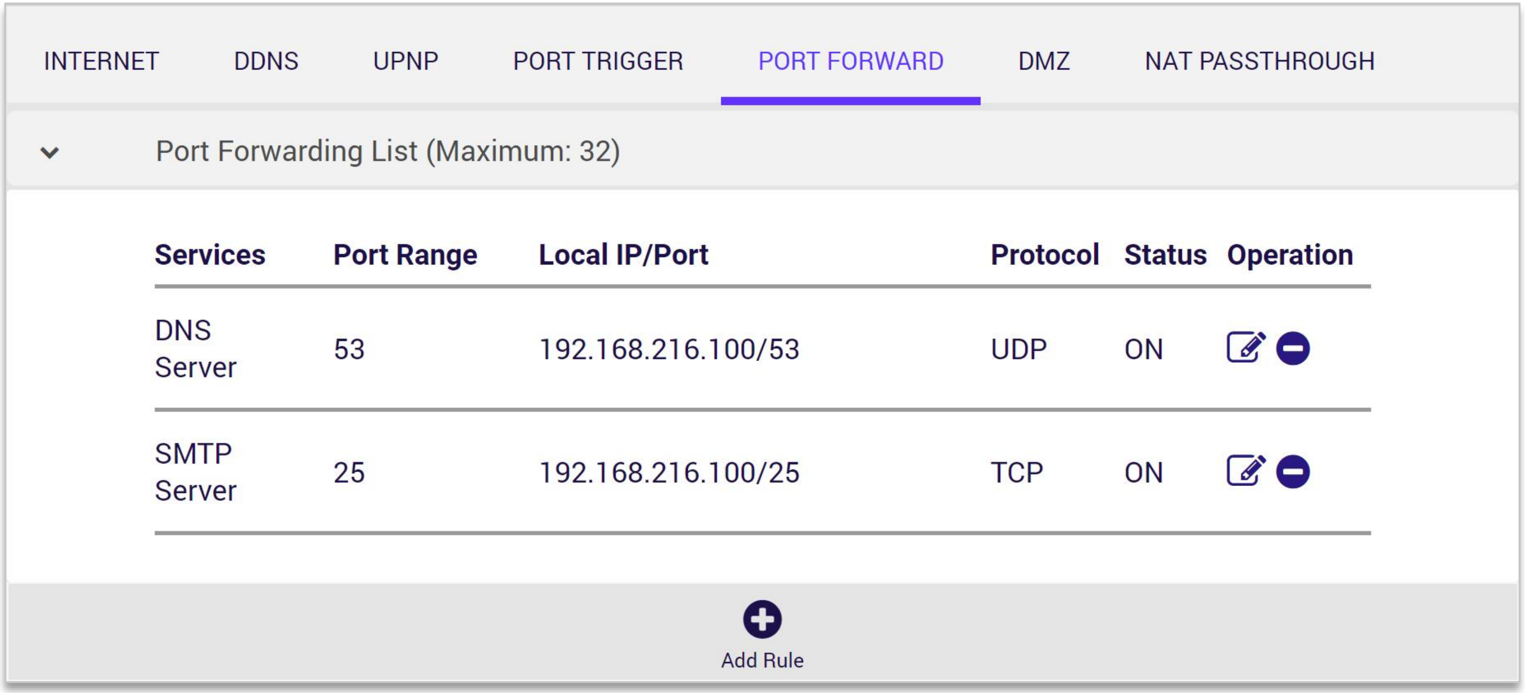
Port Triggering List

Well-Known Applications	Quicktime 4 Client
Description	Quicktime 4 Client
Trigger Port	554
Local IP List	Select
Local IP	192.168.216.100
Protocol	TCP
Incoming Port	554
Protocol	UDP

Well-known Applications	Select a well-known application from the dropdown menu to set up the corresponding settings automatically.
Description	Name the rule according to your requirement.
Trigger port	Define the port number or the port range for triggering the incoming ports.
Local IP list	Select the IP address in the dropdown menu which automatically detected by your router.
Local IP	Enter the IP address of the device connecting to your router.
Protocol	Select TCP or UDP in the dropdown menu.
Incoming port	Define the port number or the port range to be open while detecting port triggered event.
Protocol	Select the TCP or UDP in the dropdown menu.

6.2.2.5 Port Forward

Port forward allows you to set up an Internet service on a local computer, without exposing the local computer to the Internet. Internet traffic directed to a specific port or range of ports on this router is redirect to a device or devices on your local network. You can also build various sets of port redirection, to provide various Internet services on different local computers via a single Internet IP address. It also allows PCs outside the network to access services provided by a computer in the local network.

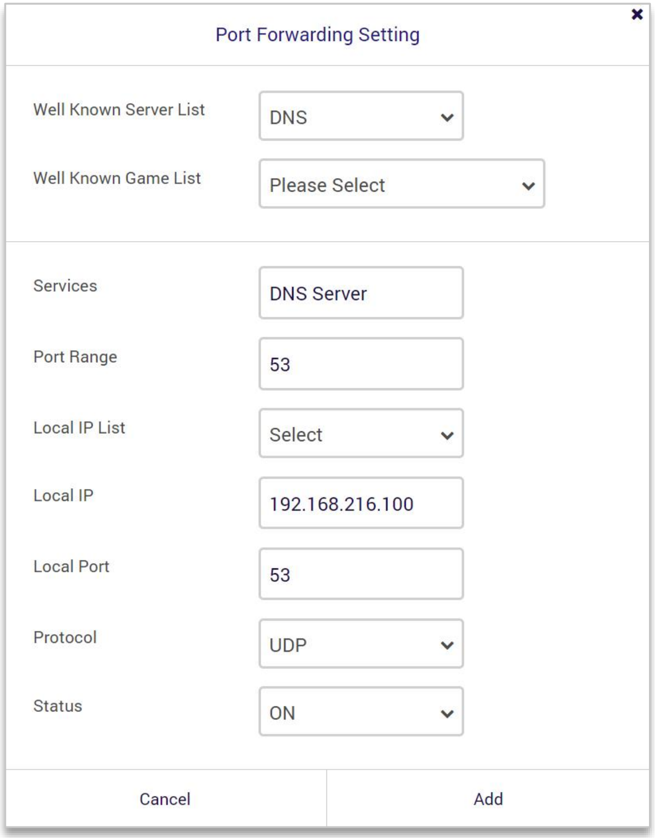


Port Forwarding List (Maximum: 32)

Services	Port Range	Local IP/Port	Protocol	Status	Operation
DNS Server	53	192.168.216.100/53	UDP	ON	✎ ⊖
SMTP Server	25	192.168.216.100/25	TCP	ON	✎ ⊖

1. Click **Add Rule** ⊕. Enter the parameters in accordance with your requirements to set up a port forwarding rule.
2. Click **Add** to have the rule created on port forwarding list and then click Save to apply your changes. You can remove or edit any port forwarding rule by using the ⊖ and ✎ icons.

   Note: The maximum number on port forwarding list is 32 rules



Port Forwarding Setting

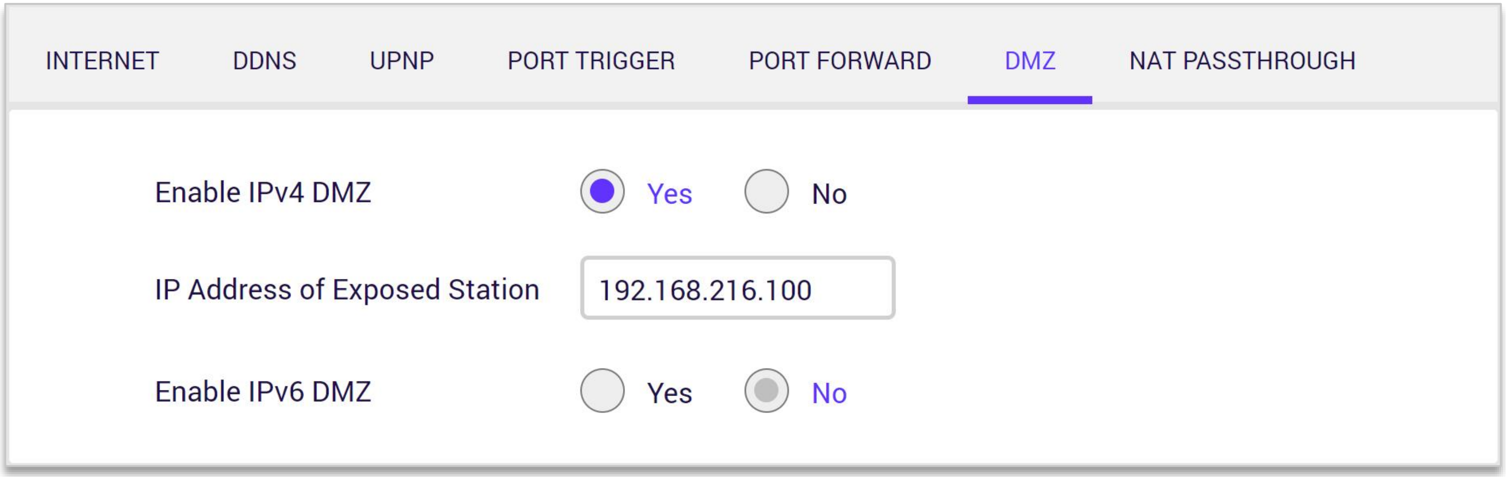
Well Known Server List	DNS
Well Known Game List	Please Select
Services	DNS Server
Port Range	53
Local IP List	Select
Local IP	192.168.216.100
Local Port	53
Protocol	UDP
Status	ON

Well Known Server List	Select a well-known service from the dropdown menu to set up the corresponding settings automatically.
Well Known Game List	Select a well-known game from the dropdown menu to set up the corresponding settings automatically.
Services	Specify the name of the service e.g. HTTP, POP3 etc.
Port Range	Define the number or a range of external ports.
Local IP List	Select the IP address in the dropdown menu which automatically detected by your router.
Local IP	Enter the IP address of the device connecting to your router.
Local Port	Define the number or a range of internal ports.
Protocol	Select TCP, UDP or BOTH in the dropdown menu.
Status	Configure the default status of this rule.

6.2.2.6 DMZ

A Demilitarized Zone (DMZ) is an isolated device in your local network where a computer outside the firewall can access directly. This can provide an extra layer of security to the rest of the network but still provide service to devices outside firewall without problems due to NAT firewall. However, since it opens the device up to unrestricted two-way access, this device is vulnerable to outside attack. DMZ should be configured only by expert network users aware of the security risks.

Enable DMZ	Enable or disable DMZ function.
IP Address of Exposed Station	Enter an IP address to become DMZ Host.



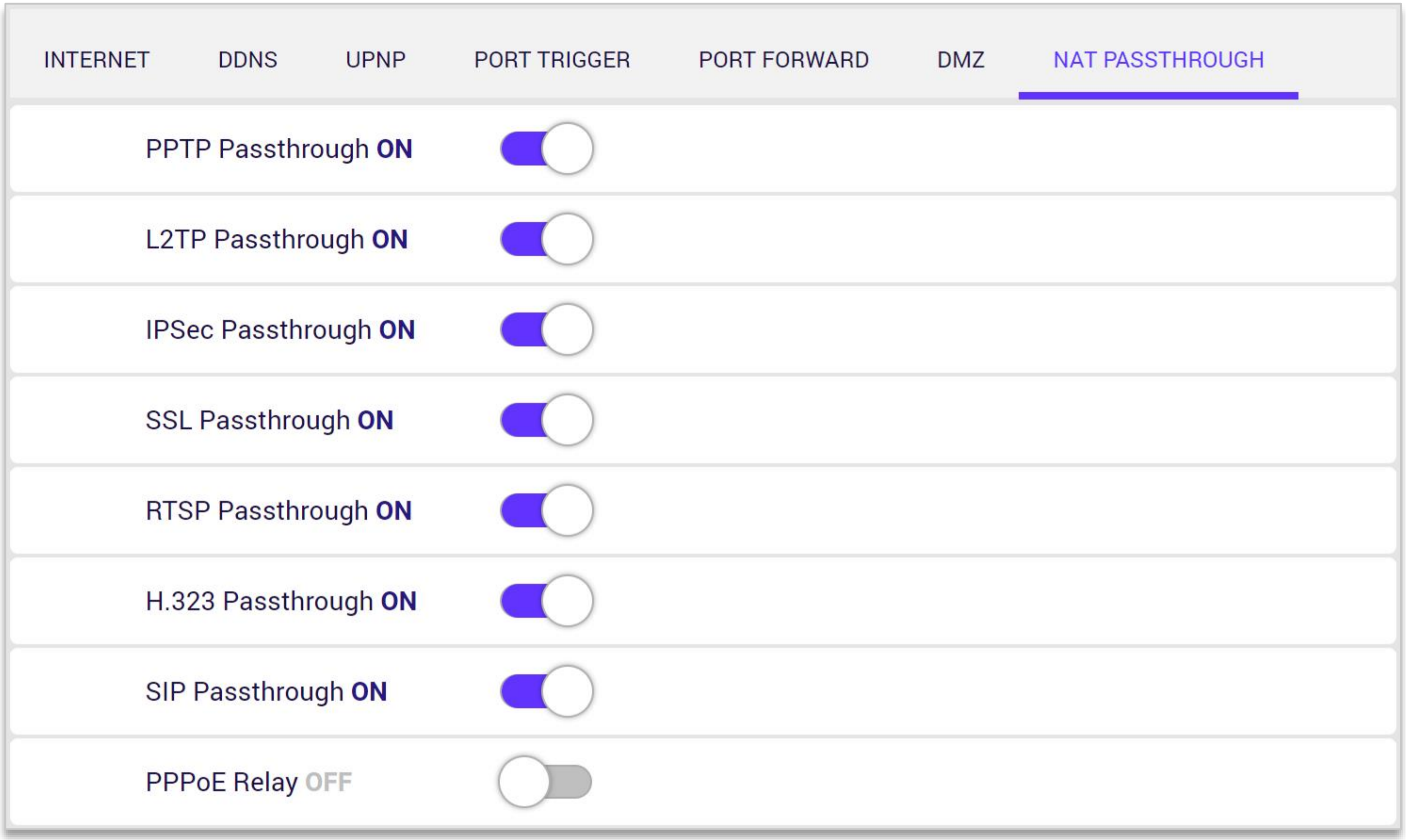
Enable IPv4 DMZ ● Yes ○ No

IP Address of Exposed Station 192.168.216.100

Enable IPv6 DMZ ○ Yes ● No

6.2.2.7 NAT Passthrough

NAT Passthrough allows an incoming Virtual Private Network (VPN) connection to pass through the router to the network clients.



PPTP Passthrough **ON**

L2TP Passthrough **ON**

IPSec Passthrough **ON**

SSL Passthrough **ON**

RTSP Passthrough **ON**

H.323 Passthrough **ON**

SIP Passthrough **ON**

PPPoE Relay **OFF**

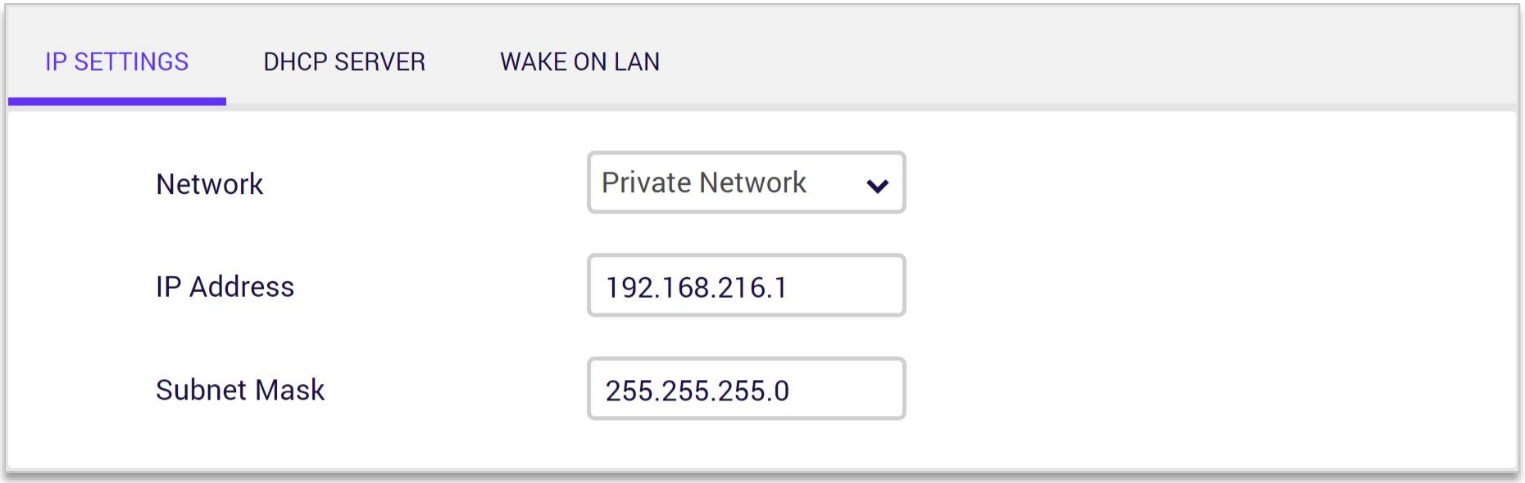
NAT Passthrough	
PPTP Passthrough	Point-to-Point Tunneling Protocol (PPTP) is a module for implementing virtual private networks.
L2TP Passthrough	Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.
IPSec Passthrough	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.
SSL Passthrough	SSL (Secure Sockets Layer) is a standard security protocol for encryption algorithms between a server to server or between server and a client to safeguard sensitive data.
RTSP Passthrough	Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The protocol is used for establishing and controlling media sessions between end points.
H.323 Passthrough	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. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.
SIP Passthrough	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.
PPPoE Relay	Enable PPPoE relay allows devices in LAN to establish an individual PPPoE connections that pass through NAT.

6.2.3 LAN

6.2.3.1 IP Settings

Manage IP settings for your local area network.

1. **Network**: Select Private Network or Guest Network to configure LAN settings.
2. **IP address**: Specify an IP address. The default IP address of Private Network is “**192.168.216.1**” and “**192.168.217.1**” is for Guest Network.
3. **Subnet Mask**: Modify the subnet mask or remain default settings “**255.255.255.0**”.



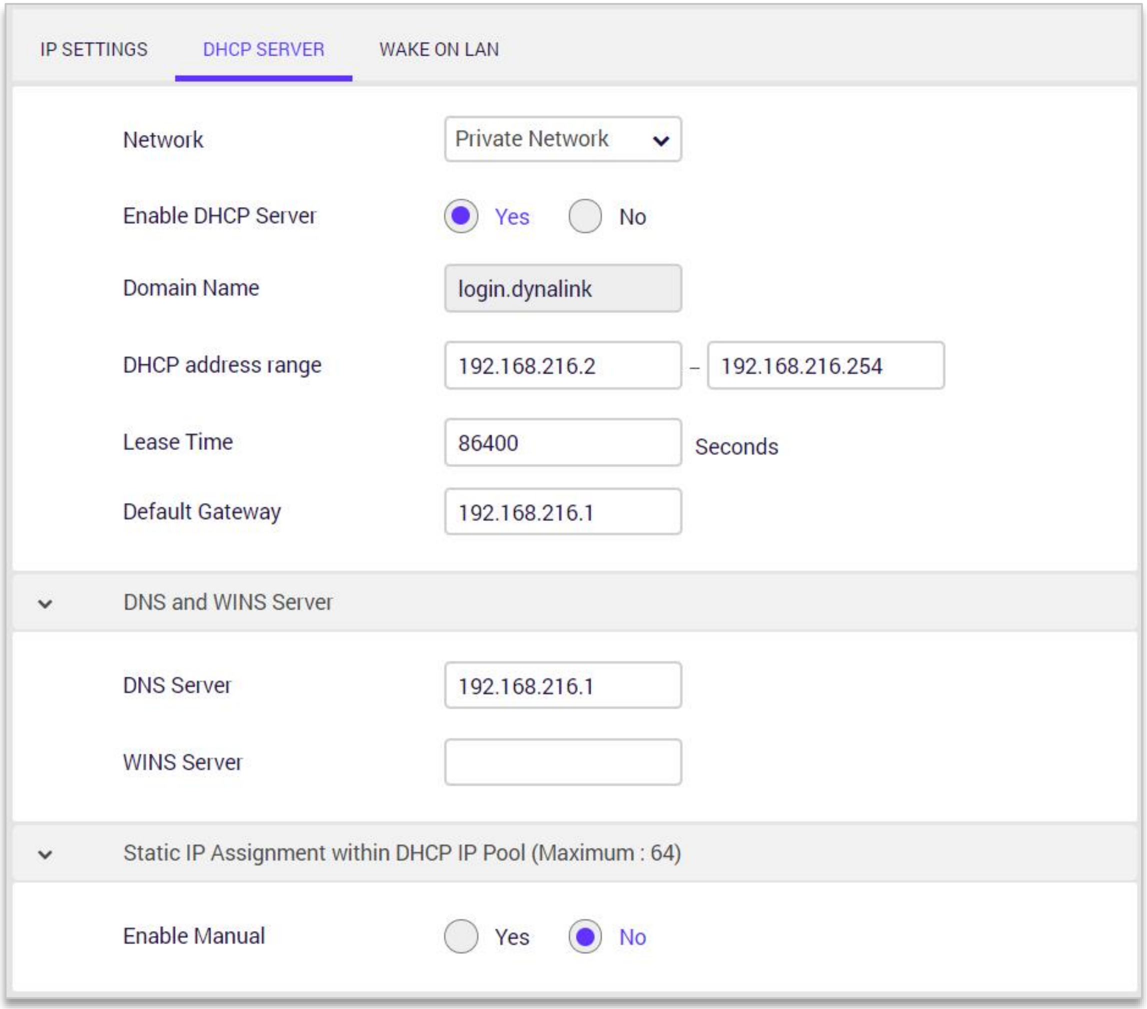
Network: Private Network

IP Address: 192.168.216.1

Subnet Mask: 255.255.255.0

6.2.3.2 DHCP Server

This page allows you to configure your router as a DHCP server which automatically assigns IP addresses to the devices connecting your LAN.



Network: Private Network

Enable DHCP Server: ● Yes ○ No

Domain Name: login.dynalink

DHCP address range: 192.168.216.2 – 192.168.216.254

Lease Time: 86400 Seconds

Default Gateway: 192.168.216.1

DNS and WINS Server

DNS Server: 192.168.216.1

WINS Server:

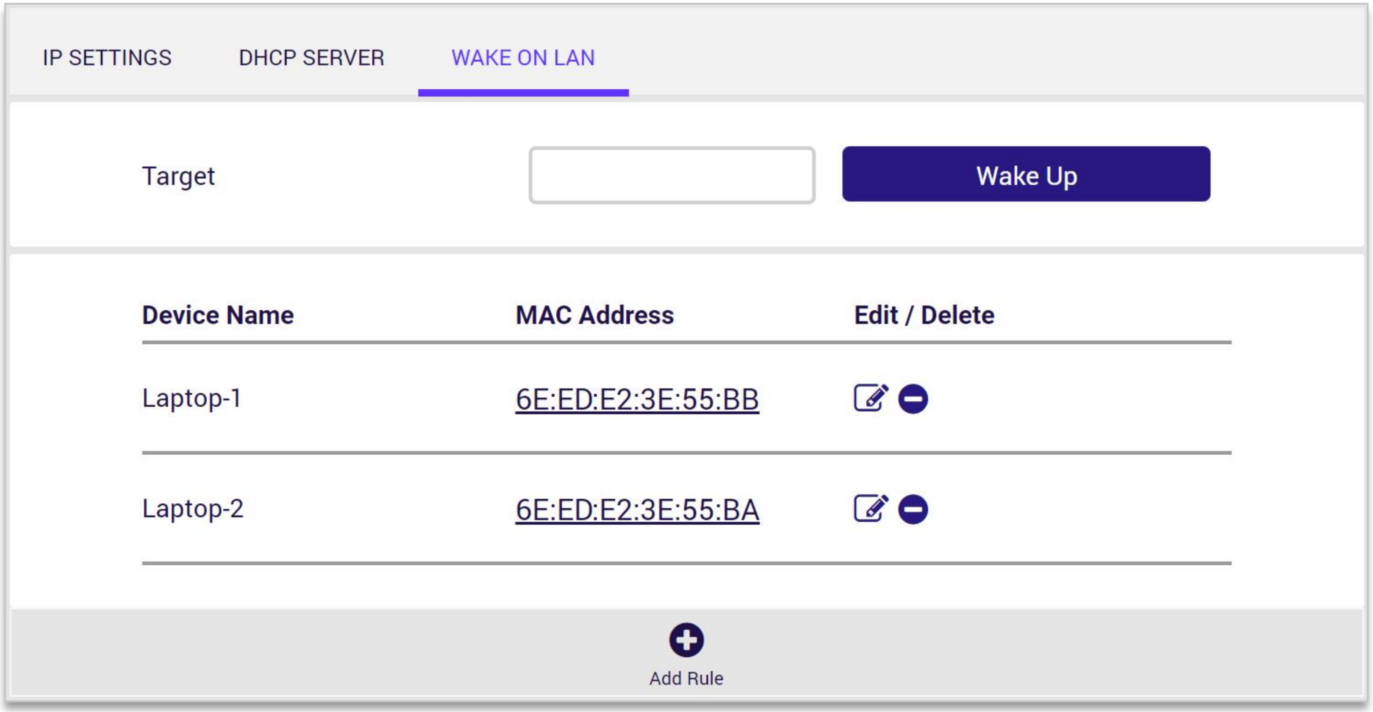
Static IP Assignment within DHCP IP Pool (Maximum : 64)

Enable Manual: ○ Yes ● No

DHCP Server	
Network	Select Private Network or Guest Network in the dropdown menu to configure DHCP server.
Enable DHCP Server	Select the radio button to enable or disable DHCP server.
Domain Name	Enter the domain name of the network or remain default settings.
DHCP address Range	Define the start and end of the IP address range that the DHCP server will assign to the LAN devices connecting to your router.
Lease Time	Enter the lease time in seconds that DHCP server will renegotiate with the LAN devices to release and renew IP addresses.
Default Gateway	The router uses the IP address of default gateway to communicates with LAN devices and other networks.
DNS and WINS Server	
DNS Server	Enter a Domain Name Server address.
WINS Server	Enter a Windows Internet Name Service address.
Static IP Assignment within DHCP IP Pool (Maximum: 64)	
Enable Manual	Select the radio button to enable/disable static IP assignment within DHCP IP pool.

6.2.3.3 Wake on LAN

Wake on LAN is a standard protocol that allows your computer to be turned on or awakened remotely whether it is hibernating, sleeping, or completely powered off. Click **Add Rule** ⊕ and enter the name/MAC of the computer. To turn on a specific computer, enter the MAC address in the text field and click [Wake Up] button. You can also use ✎ and ⊖ button to manage the control list.



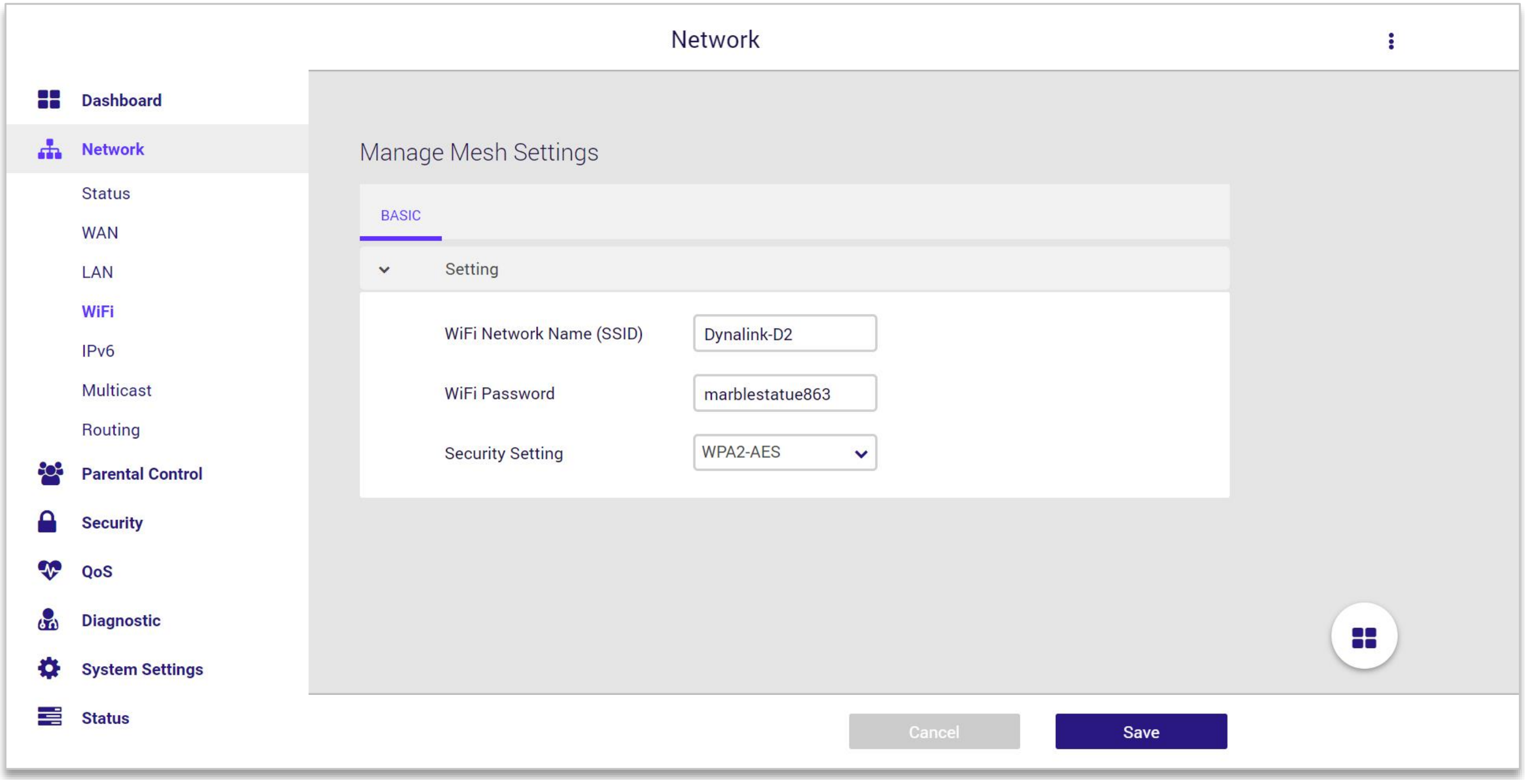
Device Name	MAC Address	Edit / Delete
Laptop-1	6E:ED:E2:3E:55:BB	✎ ⊖
Laptop-2	6E:ED:E2:3E:55:BA	✎ ⊖

6.2.4 WiFi

6.2.4.1 Basic

This page shows the mode of your Mesh Wi-Fi Router and allows you to configure the corresponding Wi-Fi settings.

Note: You will retain only one Wi-Fi network name and password on both 2.4GHz and 5GHz network.



WiFi Network Name (SSID): Dynalink-D2

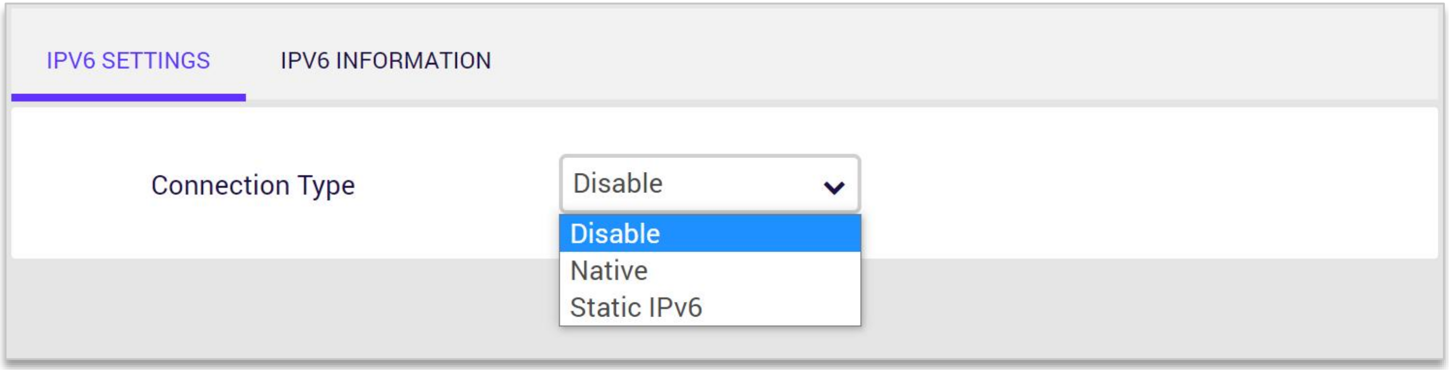
WiFi Password: marblestatue863

Security Setting: WPA2-AES

6.2.5 IPv6

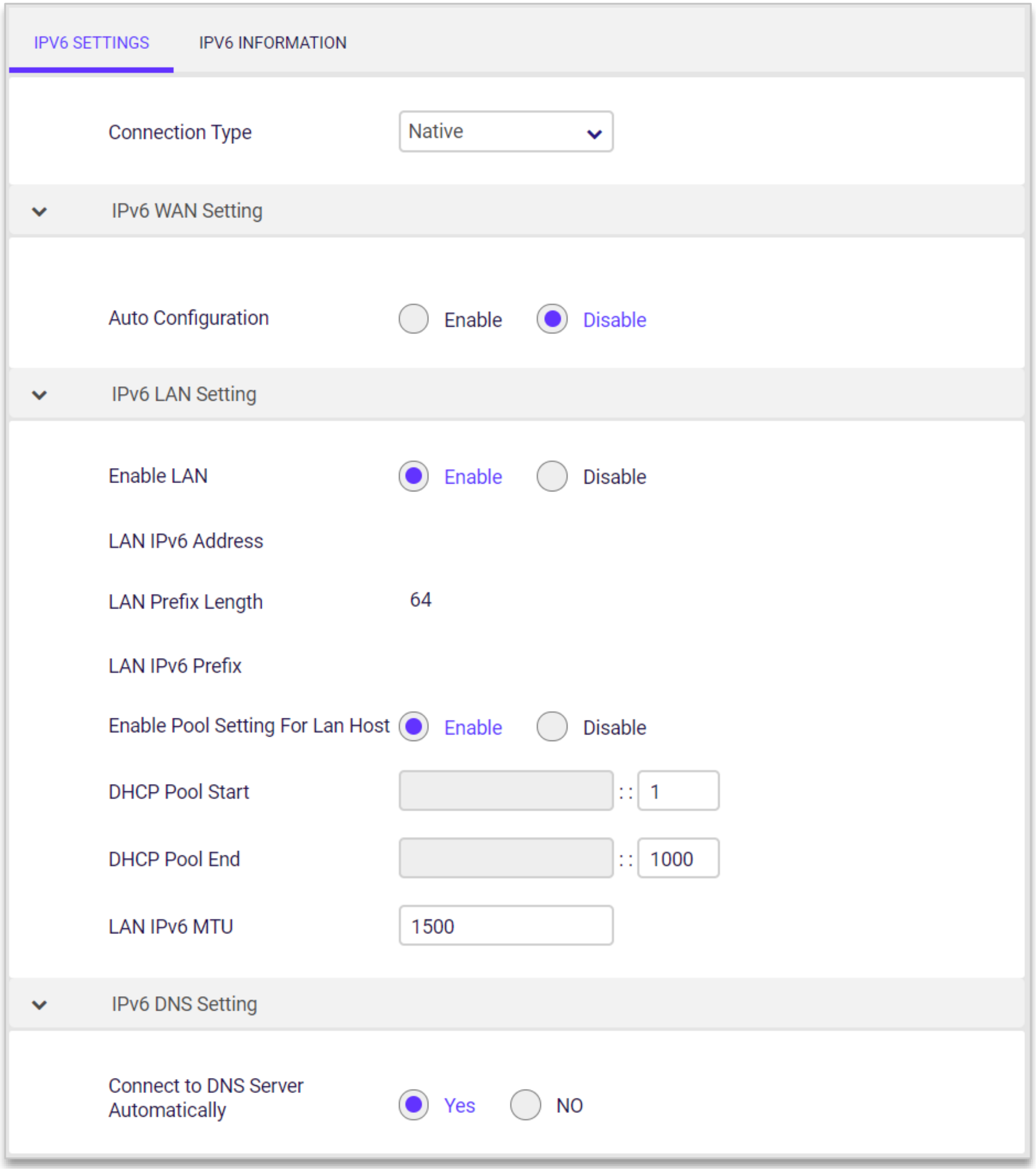
6.2.5.1 IPv6 Settings

IPv6 (Internet Protocol Version 6) is a next-generation IP protocol designed by the IETF (Internet Engineering Task Force) to replace the current version of the IP protocol (IPv4). With the shortage of IPv4 resources, IPv6 will become the standard of the next generation of Internet addresses in the near future. Compared with IPv4, IPv6 has rich IP address resources. Select Disable, Native, or Static IPv6 on dropdown menu.



Connection Type: Disable

Connection Type 1 - Native



Connection Type: Native

IPv6 WAN Setting

Auto Configuration ○ Enable ● Disable

IPv6 LAN Setting

Enable LAN ● Enable ○ Disable

LAN IPv6 Address

LAN Prefix Length 64

LAN IPv6 Prefix

Enable Pool Setting For Lan Host ● Enable ○ Disable

DHCP Pool Start :: 1

DHCP Pool End :: 1000

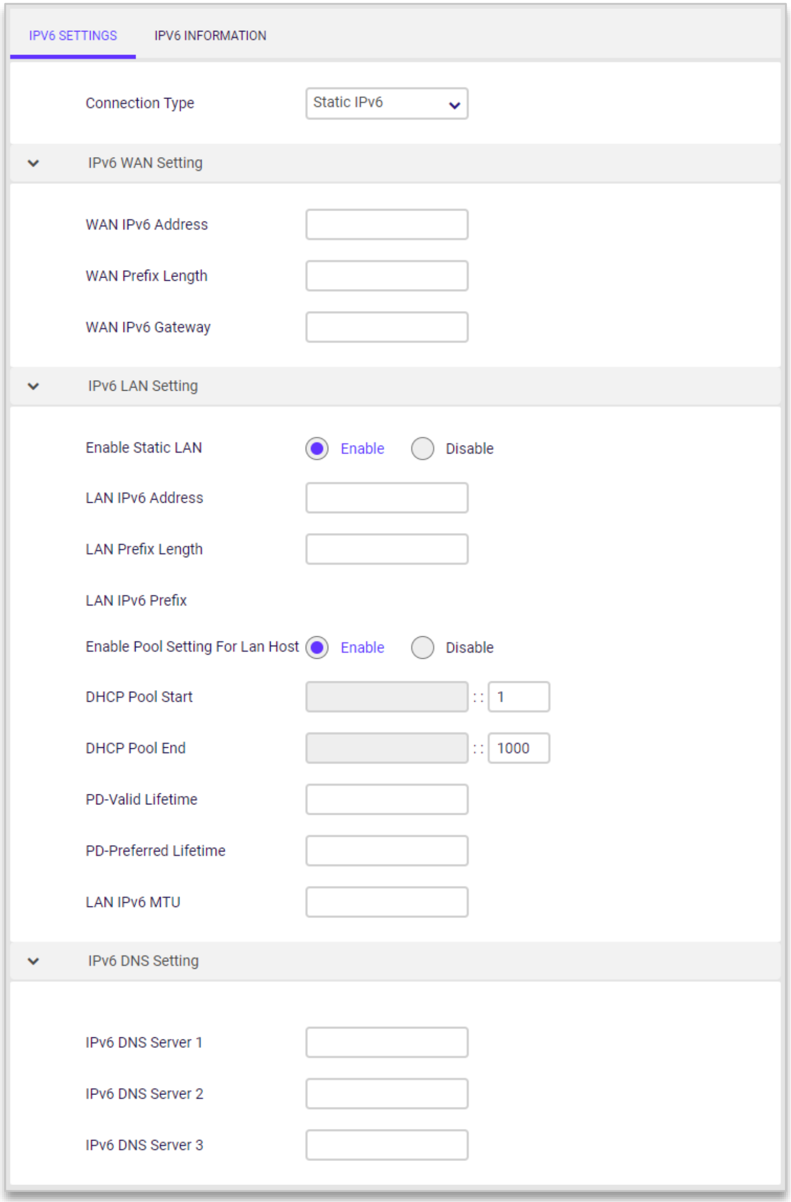
LAN IPv6 MTU 1500

IPv6 DNS Setting

Connect to DNS Server Automatically ● Yes ○ NO

Native	
Connection Type	Native.
IPv6 WAN Setting	
Auto Configuration	Enable or remain default.
IPv6 LAN Setting	
Enable LAN	Toggle the switch to enable or disable IPv6 LAN.
LAN IPv6 Address	Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network.
LAN Prefix Length	IPv6 Prefix Length is used to identify how many bits of a Gobal Unicast IPv6 Address are there in a network packet.
LAN IPv6 Prefix	The leftmost fields of the IPv6 address along with the network bits length represented in CIDR format is known as the network prefix.
Enable Pool Setting For Lan Host	Toggle the switch to enable or disable IPv6 LAN DHCP Pool.
DHCP Pool Start	Enter the start IPv6 address of the DHCP Pool.
DHCP Pool End	Enter the end IPv6 address of the DHCP Pool.
LAN IPv6 MTU	MTU (Maximum Transmission Unit) is the single largest frame or packet of data that can be transmitted across a network.
IPv6 DNS Setting	
Connect to DNS Server Automatically	Toggle the switch to connect to DNS server or not.
IPv6 DNS Server 1	Enter a DNS Server address manually.
IPv6 DNS Server 2	Enter a second DNS Server address manually.
IPv6 DNS Server 3	Enter a third DNS Server address manually.

Connection Type 2 - Static IPv6



IPV6 SETTINGS IPV6 INFORMATION

Connection Type	Static IPv6

IPv6 WAN Setting

WAN IPv6 Address	
WAN Prefix Length	
WAN IPv6 Gateway	

IPv6 LAN Setting

Enable Static LAN	● Enable ○ Disable
LAN IPv6 Address	
LAN Prefix Length	
LAN IPv6 Prefix	
Enable Pool Setting For Lan Host	● Enable ○ Disable
DHCP Pool Start	:: 1
DHCP Pool End	:: 1000
PD-Valid Lifetime	
PD-Preferred Lifetime	
LAN IPv6 MTU	

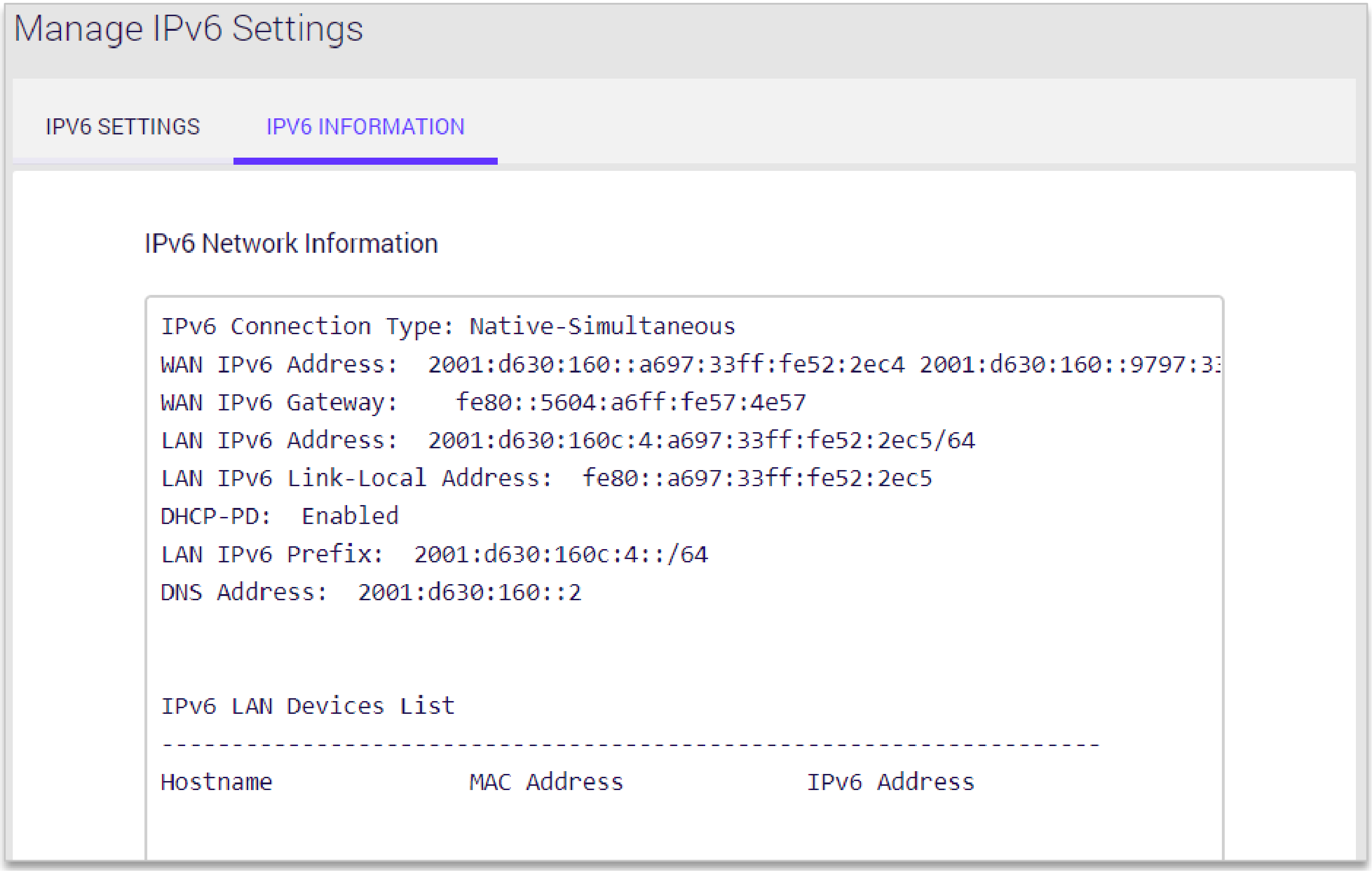
IPv6 DNS Setting

IPv6 DNS Server 1	
IPv6 DNS Server 2	
IPv6 DNS Server 3	

Static IPv6	
Connection Type	Static IPv6
IPv6 WAN Setting	
WAN IPv6 Address	Enter Static IPv6 address.
WAN Prefix Length	Enter IPv6 prefix length.IPv6 Prefix Length is used to identify how many bits of a Gobal Unicast IPv6 Address are there in a network packet.
WAN IPv6 Router	Enter IPv6 router.
IPv6 LAN Setting	
Enable Static LAN	Toggle the switch to enable or disable IPv6 LAN.
LAN IPv6 Address	Internet Protocol Version 6 (IPv6) is a network layer protocol that enables data communications over a packet switched network. IPv6 uses 128-bit numbering scheme (2^{128}) which has big enough address space for many decades to come.
LAN Prefix Length	IPv6 Prefix Length is used to identify how many bits of a Gobal Unicast IPv6 Address are there in network part.
LAN IPv6 Prefix	The leftmost fields of the IPv6 address along with the network bits length represented in CIDR format is known as the network prefix.
DHCP Pool Start	Enter the start IPv6 address of the DHCP Pool.
DHCP Pool End	Enter the end IPv6 address of the DHCP Pool.
PD-Valid Lifetime	Prefix Delegation valid lifetime.
PD-Preferred Lifetime	Prefix Delegation preferred lifetime.
LAN IPv6 MTU	MTU (Maximum Transmission Unit) is the single largest frame or packet of data that can be transmitted across a network.
IPv6 DNS Setting	
IPv6 DNS Server1	Enter a DNS Server address manually.
IPv6 DNS Server2	Enter a second DNS Server address manually.
IPv6 DNS Server3	Enter a third DNS Server address manually.

6.2.5.2 IPv6 Information

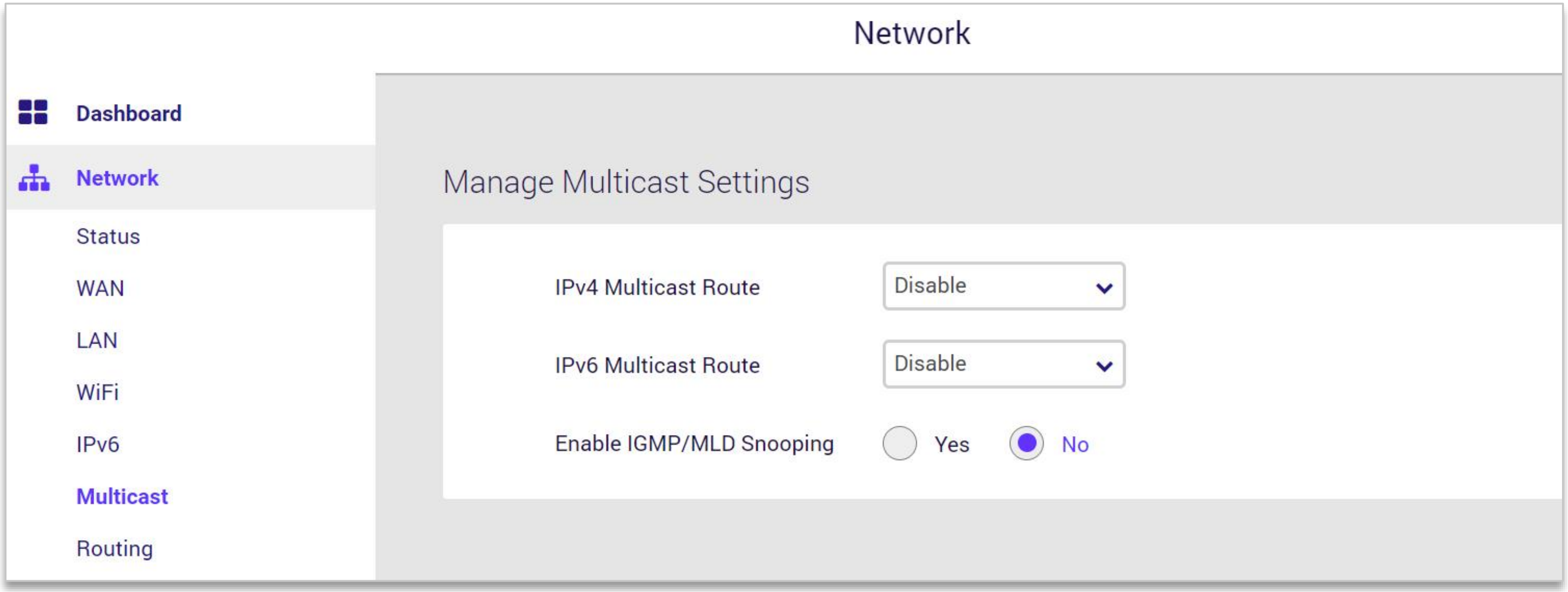
The IPv6 status displayed as below:



```
IPv6 Connection Type: Native-Simultaneous
WAN IPv6 Address:  2001:d630:160::a697:33ff:fe52:2ec4 2001:d630:160::9797:3
WAN IPv6 Gateway:    fe80::5604:a6ff:fe57:4e57
LAN IPv6 Address:  2001:d630:160c:4:a697:33ff:fe52:2ec5/64
LAN IPv6 Link-Local Address:  fe80::a697:33ff:fe52:2ec5
DHCP-PD:  Enabled
LAN IPv6 Prefix:  2001:d630:160c:4::/64
DNS Address:  2001:d630:160::2


IPv6 LAN Devices List
-------------------------------------------------------------------
Hostname                 MAC Address              IPv6 Address
```

6.2.6 Multicast

IPv4/IPv6 Multicast Route allows you to configure the router to deliver traffic flows with efficient method.



Manage Multicast Settings

IPv4 Multicast Route: Disable

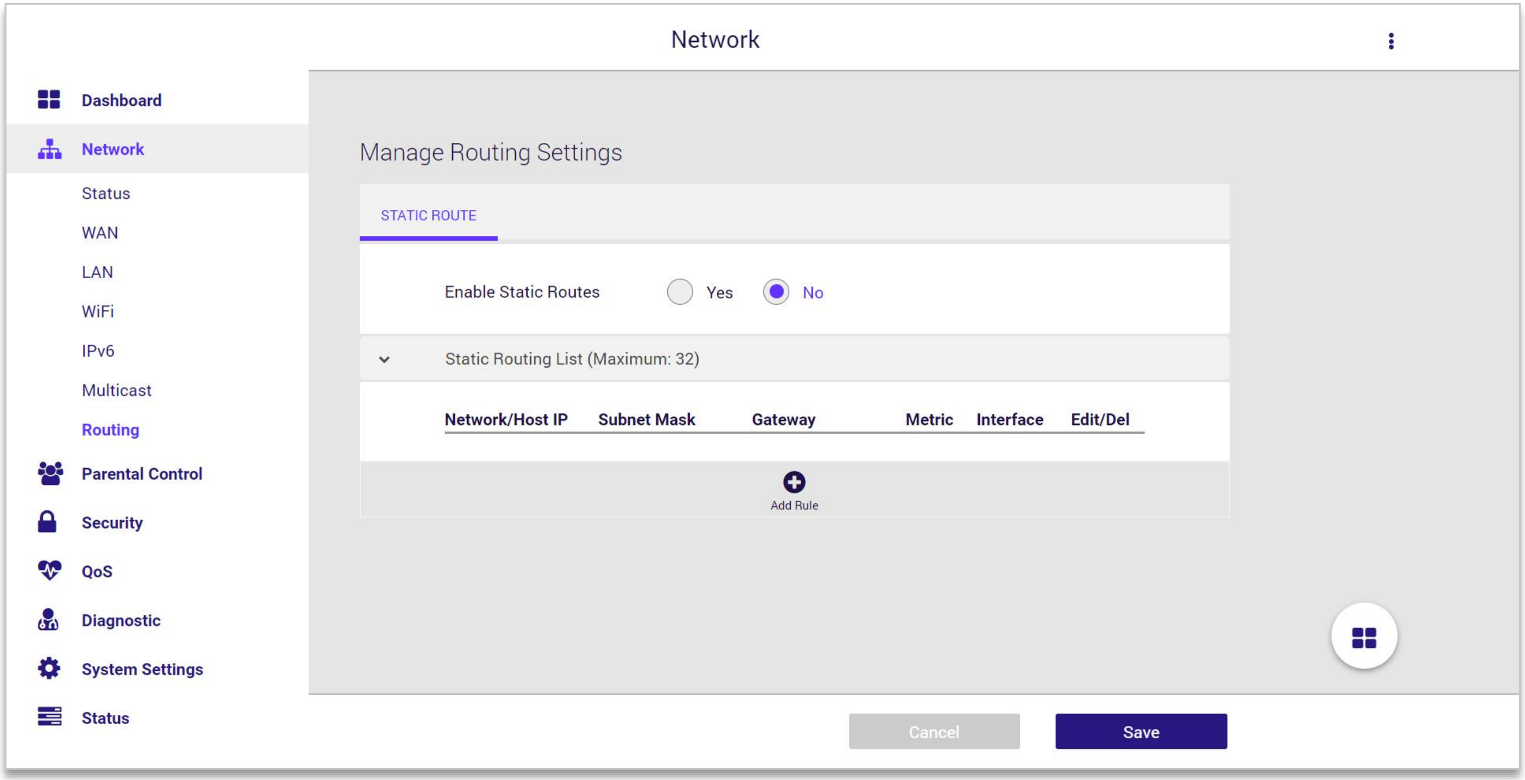
IPv6 Multicast Route: Disable

Enable IGMP/MLD Snooping ○ Yes ● No

6.2.7 Routing

6.2.7.1 Static Route

Failover mode allows you configure the default router of device data flow. When you choose WAN as your preferred line, all the data flow of your router will go through Ethernet WAN interface. The default router will change to WAN again after WAN interface is back on line.



Manage Routing Settings

Enable Static Routes ○ Yes ● No

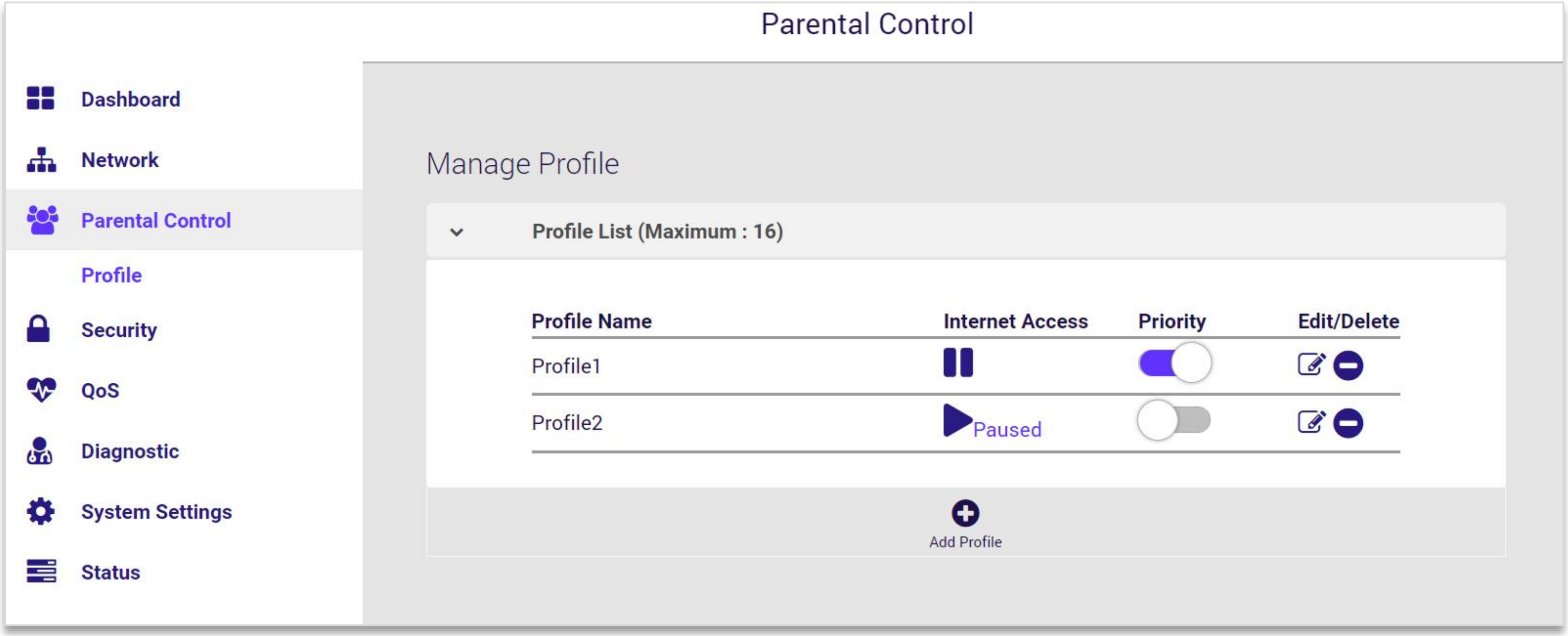
Static Routing List (Maximum: 32)

Network/Host IP	Subnet Mask	Gateway	Metric	Interface	Edit/Del

6.3 Parental Control

6.3.1 Profile

Parental control is a set of tools that allow parents to manage their child’s Internet use and restrict the access to certain content.



Parental Control

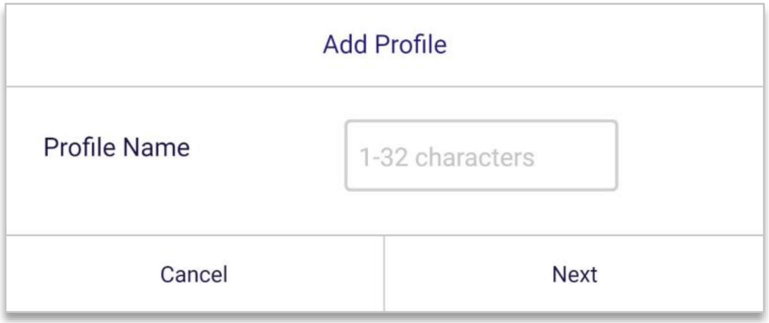
Manage Profile

Profile List (Maximum : 16)

Profile Name	Internet Access	Priority	Edit/Delete
Profile1	❚❚	●	✎ ⊖
Profile2	▶ Paused	○	✎ ⊖

1. **Create a profile,** in order to use the parental control features, first you need to create a profile with one device or multiple devices. You add devices by selecting them from a list of connected devices.

1.1 Click **Add Profile ⊕** and enter a unique name.

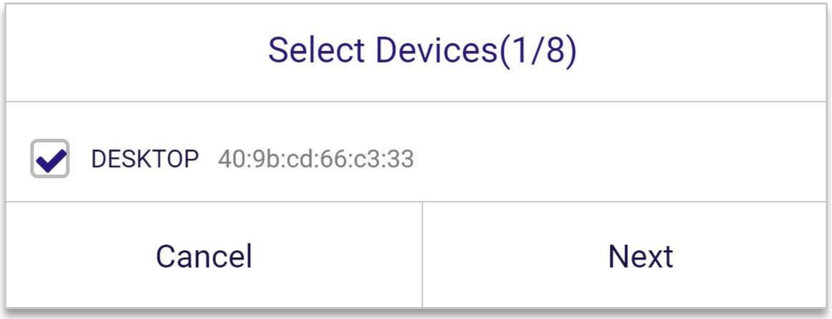


Add Profile

Profile Name 1-32 characters

Cancel Next

1.2 Select the devices you would like to apply to this profile.



Select Devices(1/8)

☑ DESKTOP 40:9b:cd:66:c3:33

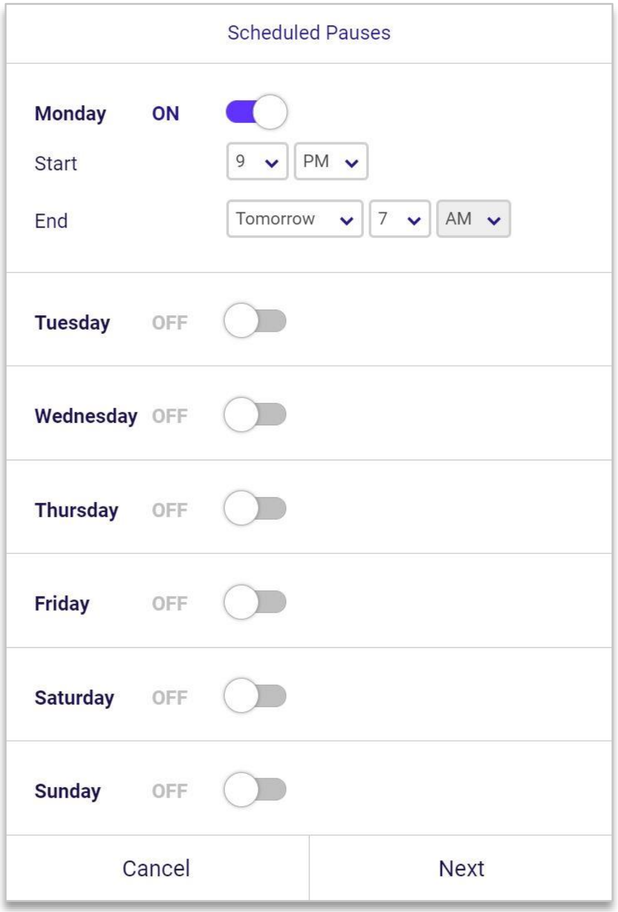
Cancel Next

Note: A device can only belong to one profile.

2. **Internet access button,** to manually pause the Internet access of the device(s) in a Profile, click **❚❚,** immediately the specific device(s) will be restricted from accessing the Internet and their services will be blocked. To restart internet access of the profile, click **▶,** the specific device(s) will be allowed to access Internet, unless you had configured partial restrictions such as time schedule or website block.
3. **Priority,** indicates higher bandwidth priority. When QoS is enabled and the Download/Upload Bandwidth are set properly, QoS assign higher priority for data traffic to and from high priority devices.

4. **Time schedule**, we can pause the Internet access for a specific time of day, such as sleeping time.
5. **Website block**, using specific keywords of the website URL and block its access.

4.1 Configure the time schedule of a Profile to control the Internet access of the device(s) at particular times of the day.

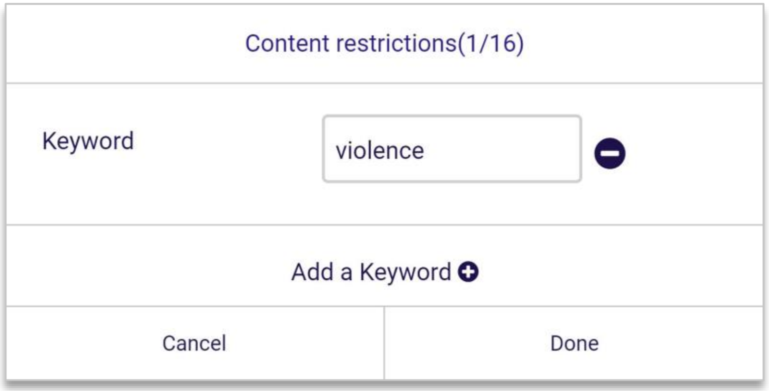


Scheduled Pauses

Monday ON
Start 9 PM
End Tomorrow 7 AM

Tuesday OFF
Wednesday OFF
Thursday OFF
Friday OFF
Saturday OFF
Sunday OFF

5.1 Enter the keyword contained in the website URL to block the Profile device(s) from access any matching website.



Content restrictions(1/16)

Keyword: violence

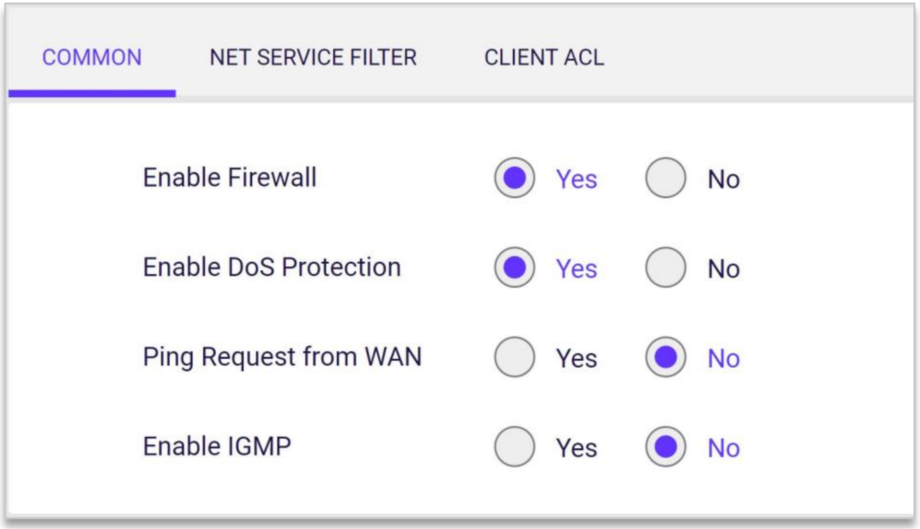
6.4 Security

Use the Security menu to configure various security functions if needed, including IPv4 Firewall and IPv6 Firewall.

6.4.1 Firewall IPv4

6.4.1.1 Common

- **Enable Firewall**- Display the status of firewall function.
- **Enable DoS Protection** Denial-of-Service (DoS) is a common form of malicious attack against a network. The router's firewall can protect against such attacks by filtering unreasonable packets that could flood and disable network with large amounts of traffic.
- **Ping Request from WAN** When inactive the feature the router will not answer IPv4 ping requests from the Internet. This can increase security as ping is a common method used by hackers to test networks.
- **Enable IGMP-** Switch to turn on/off IGMP service.



Enable Firewall ● Yes ○ No

Enable DoS Protection ● Yes ○ No

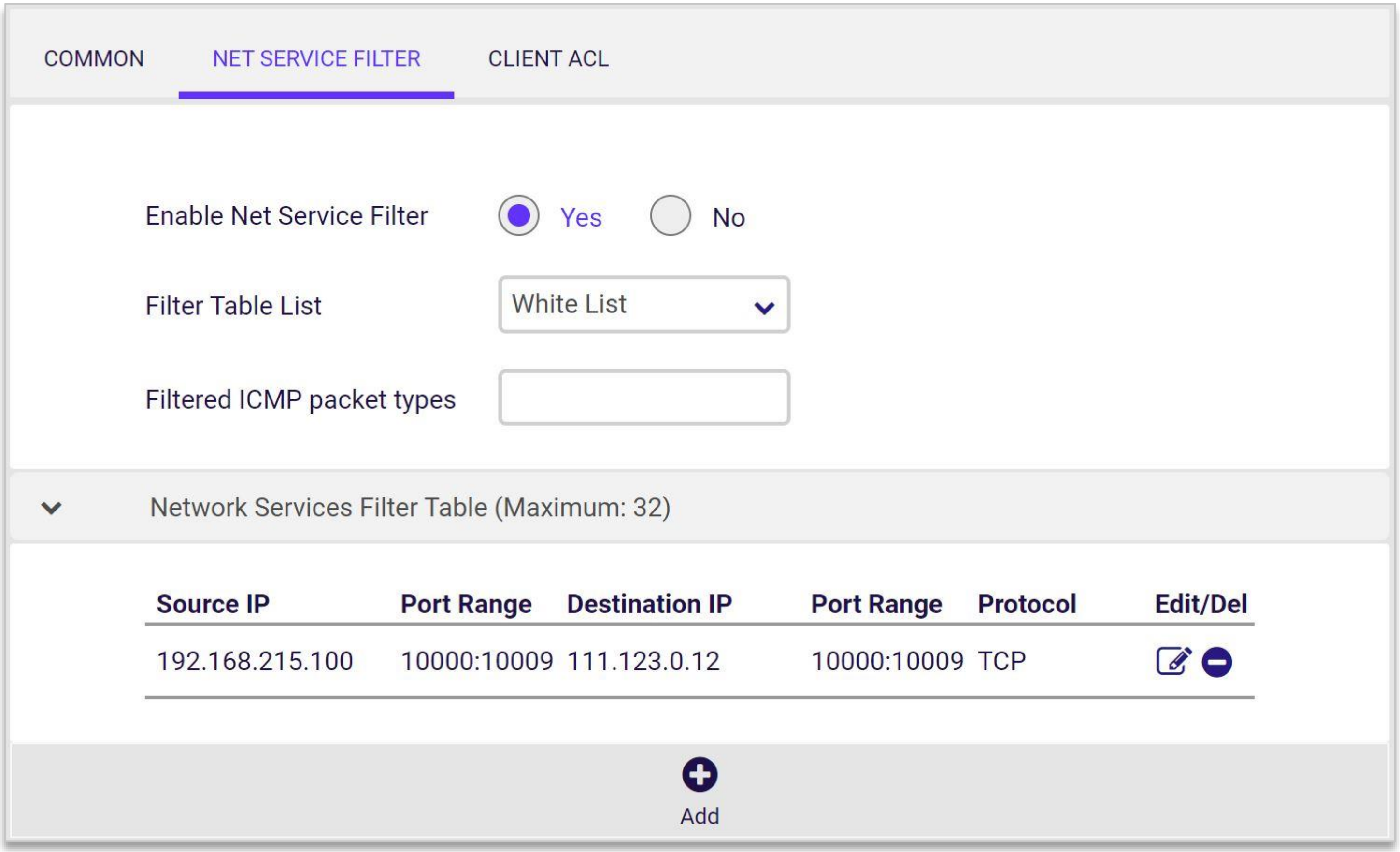
Ping Request from WAN ○ Yes ● No

Enable IGMP ○ Yes ● No

6.4.1.2 Net Service Filter

The Net Service filter blocks LAN to WAN packet exchanges by setting filter rules. Black List blocks the specified network service. White List limits access to only the specified network services.

To specify a network service to filter, enter the Source IP, Destination IP, Port Range, and Protocol.



Enable Net Service Filter ● Yes ○ No

Filter Table List: White List

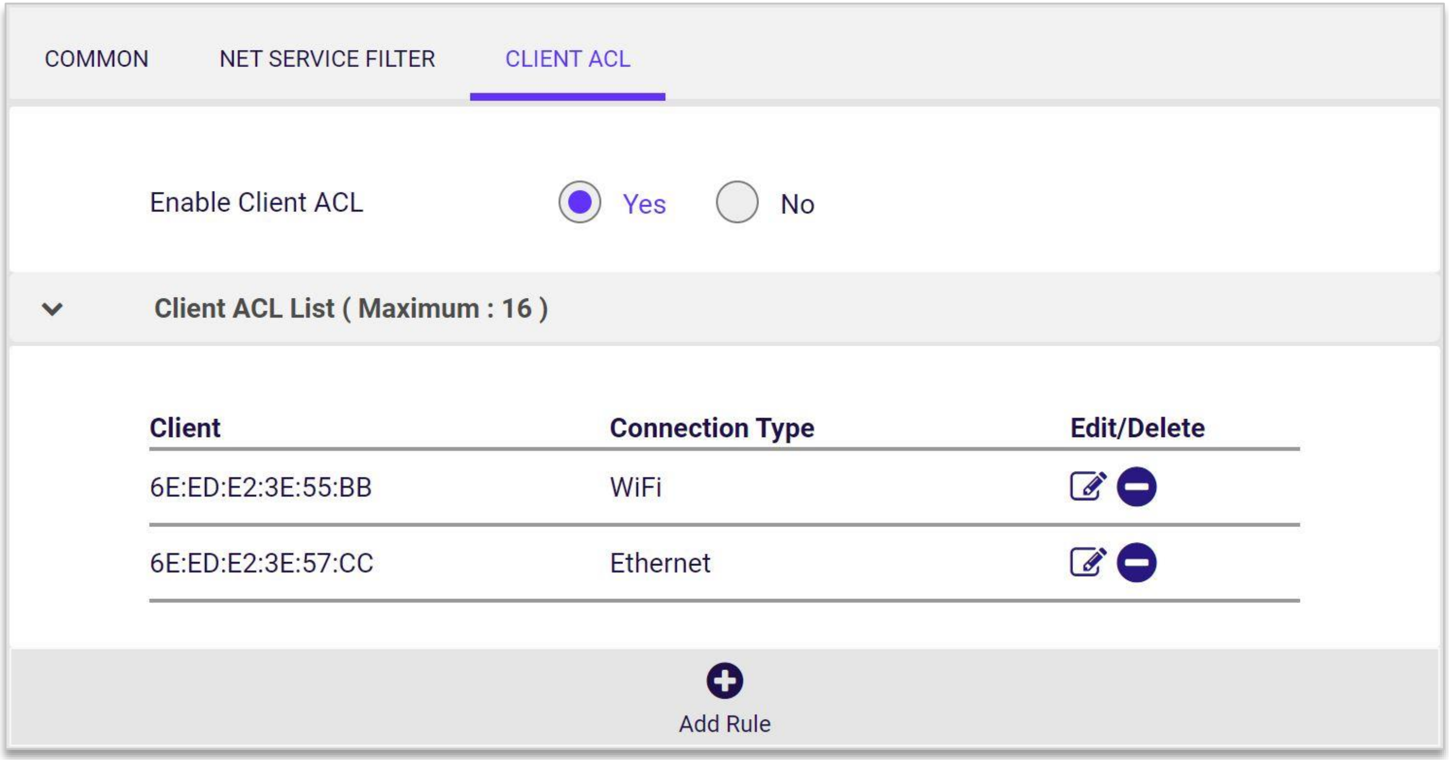
Filtered ICMP packet types:

Network Services Filter Table (Maximum: 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Edit/Del
192.168.215.100	10000:10009	111.123.0.12	10000:10009	TCP	

6.4.1.3 Client ACL

Client Access Control is a security feature that can help to prevent unauthorized users from connecting to your router. You can define a list of network devices permitted to connect to the router. Devices are each identified by their unique MAC address.



Enable Client ACL ● Yes ○ No

Client ACL List (Maximum : 16)

Client	Connection Type	Edit/Delete
6E:ED:E2:3E:55:BB	WiFi	✎ ⊖
6E:ED:E2:3E:57:CC	Ethernet	✎ ⊖

1. Select ● Yes to enable Client ACL.

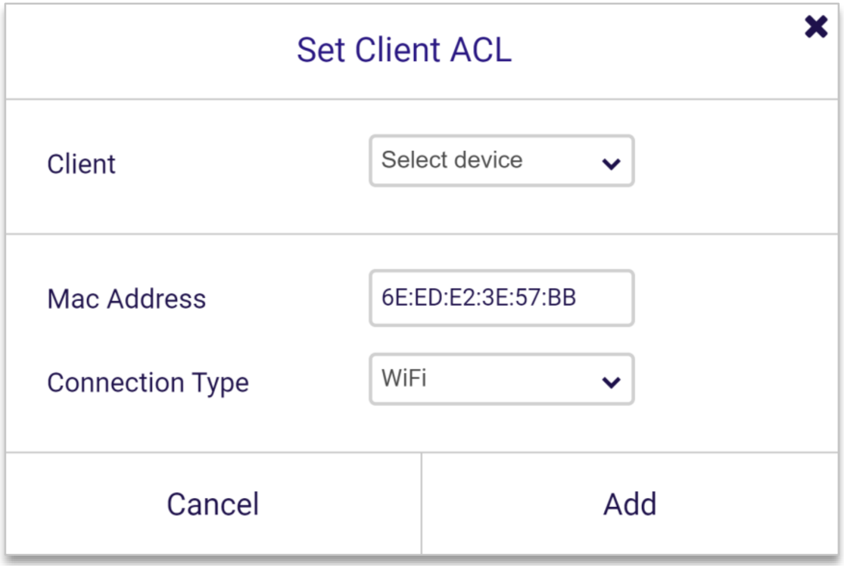
2. Click **Add Rule** ⊕.

3. Select a device from the Client menu or enter the MAC address manually.

4. Click **Add** and Save to save the rule.

5. Click the ✎ or ⊖ icon beside any entry in your ACL list to remove or edit the entry.

Note: Device will work as "allow all" even though "Net Service Filter" enabled on White or Black List without any filtering rule.



Set Client ACL

Client: Select device

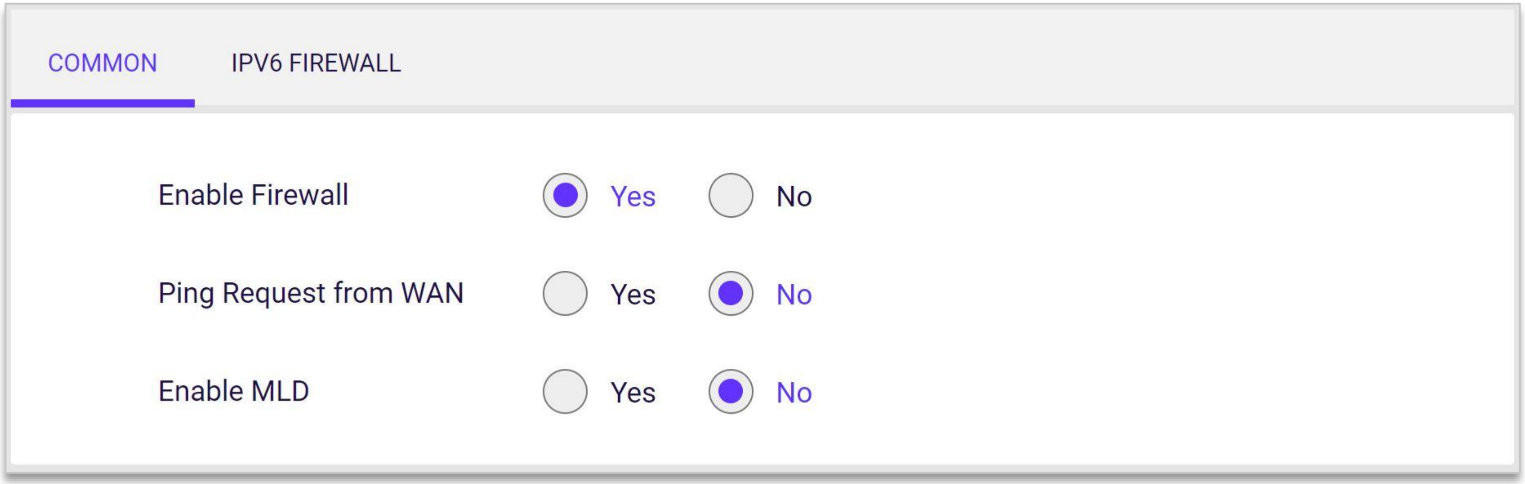
Mac Address: 6E:ED:E2:3E:57:BB

Connection Type: WiFi

6.4.2 Firewall IPv6

6.4.2.1 Common

- **Enable Firewall-** Switch to turn on/off Firewall service.
- **Ping Request from WAN-** When inactive the feature Wi-Fi router will not answer IPv6 ping requests from the Internet. This can increase security as pinging is a common method used by hackers to test networks.
- **Enable MLD**- Multicast Listener Discover, a network protocol used in multicast technology.



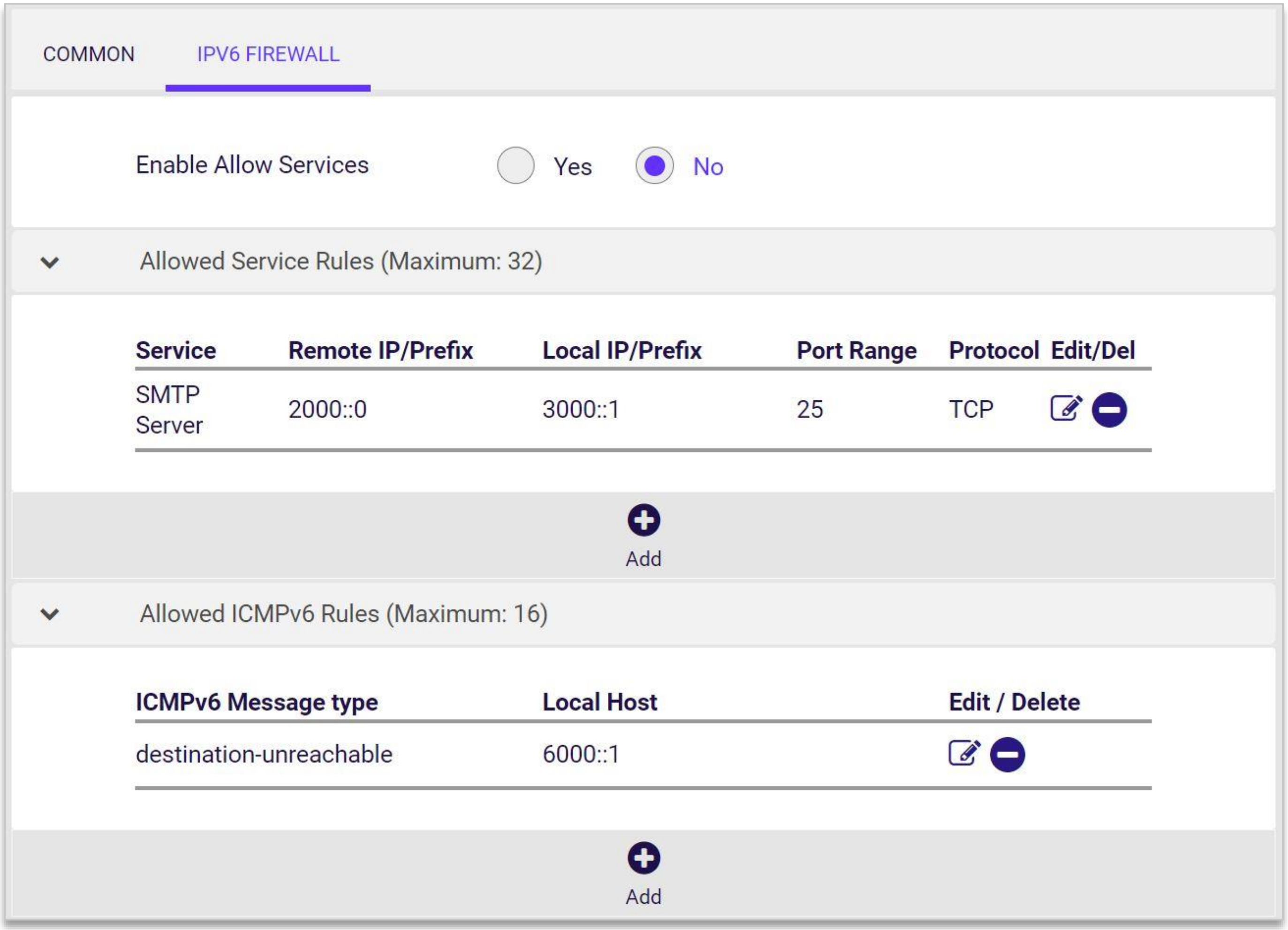
Enable Firewall ● Yes ○ No

Ping Request from WAN ○ Yes ● No

Enable MLD ○ Yes ● No

6.4.2.2 IPv6 Firewall

Enable IPv6 Firewall Services will only allow IPv6 services specified in service rules list.



Enable Allow Services ○ Yes ● No

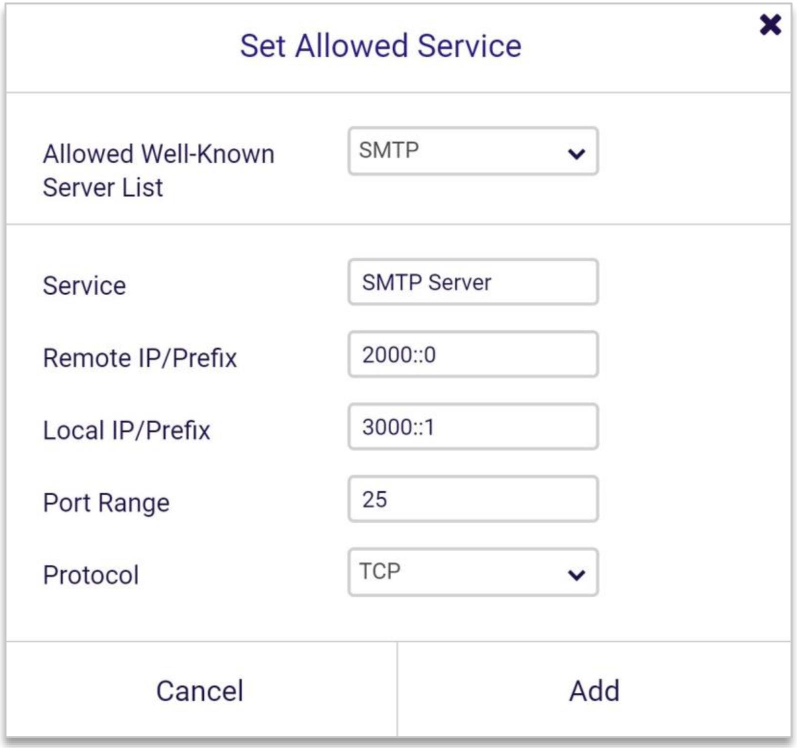
Allowed Service Rules (Maximum: 32)

Service	Remote IP/Prefix	Local IP/Prefix	Port Range	Protocol	Edit/Del
SMTP Server	2000::0	3000::1	25	TCP	

Allowed ICMPv6 Rules (Maximum: 16)

ICMPv6 Message type	Local Host	Edit / Delete
destination-unreachable	6000::1	

1. Click **Add** ⊕ on Allowed Service Rules (Maximum: 32).
2. Select an IPv6 service rule from the well-known server list or input your own rule.
3. Input service name, remote IP/prefix, local IP/prefix, port range and protocol.
4. Click **Add** and Save to save the allowed service rule.



Set Allowed Service

Allowed Well-Known Server List: SMTP

Service: SMTP Server

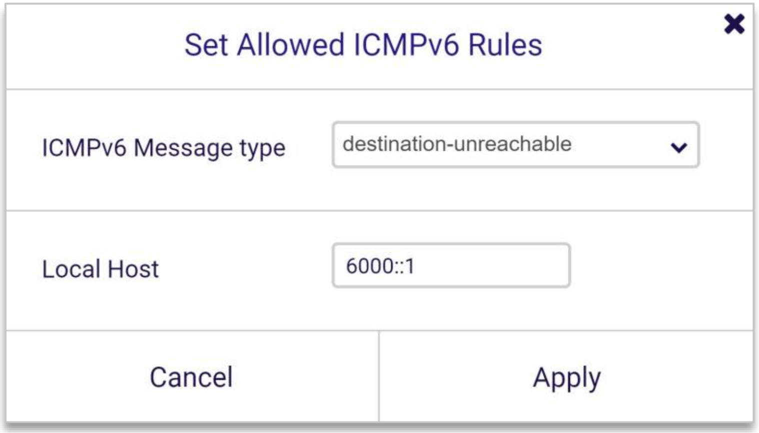
Remote IP/Prefix: 2000::0

Local IP/Prefix: 3000::1

Port Range: 25

Protocol: TCP

5. Click **Add** ⊕ on Allowed ICMPv6 Rules (Maximum: 16).
6. Select the ICMPv6 message type from the list
7. Input local host address.
8. Click **Add** and Save to save the allowed ICMPv6 rule.



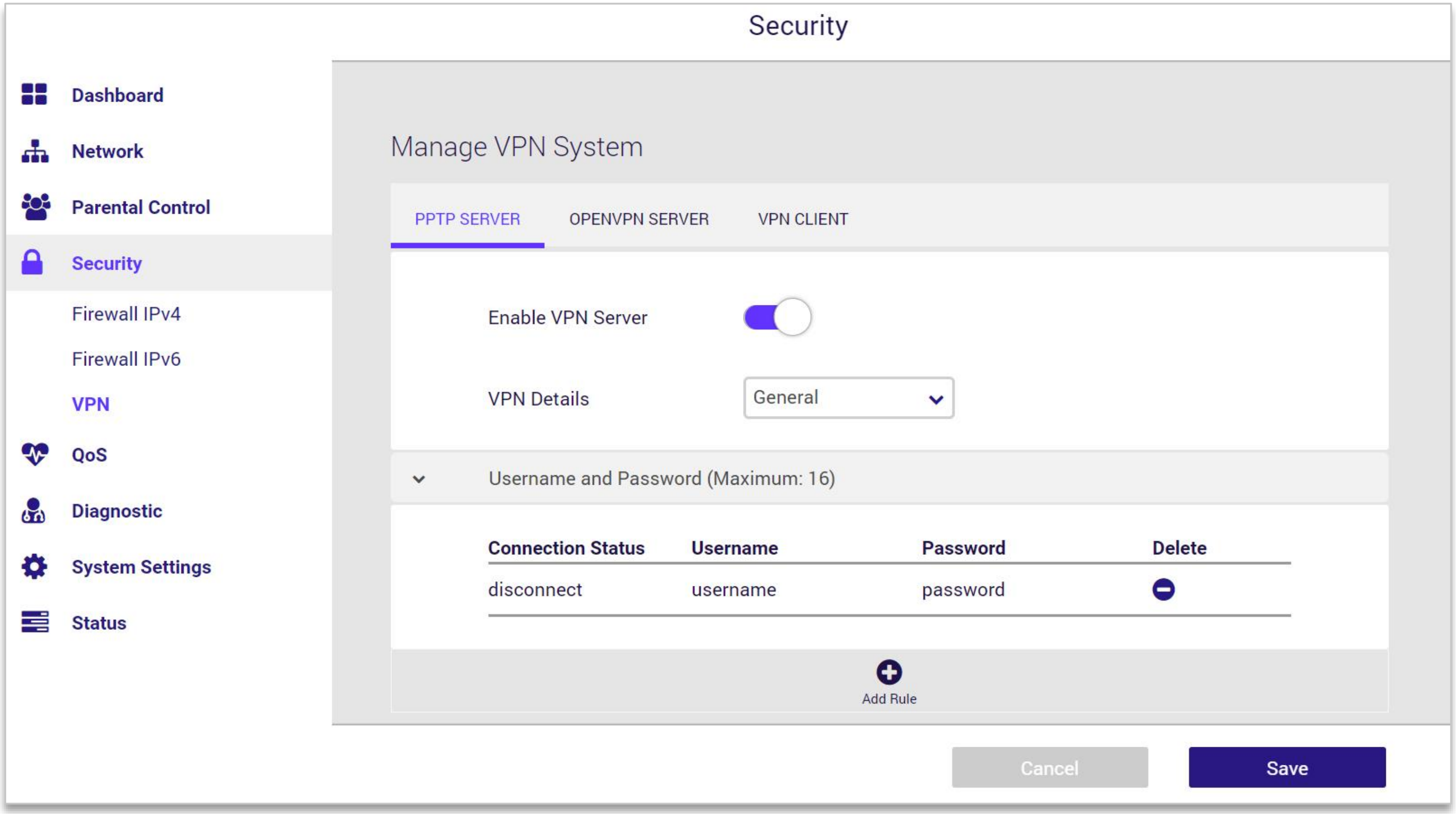
Set Allowed ICMPv6 Rules

ICMPv6 Message type: destination-unreachable

Local Host: 6000::1

6.4.3 VPN

VPN stands for Virtual Private Network. When you use a VPN, you can extend that Private Network, making it Virtual. Through a VPN, packets are sent over the Internet through an encrypted tunnel. This tunnel makes it appear as though you are directly connected to the private network.



Manage VPN System

Enable VPN Server ●

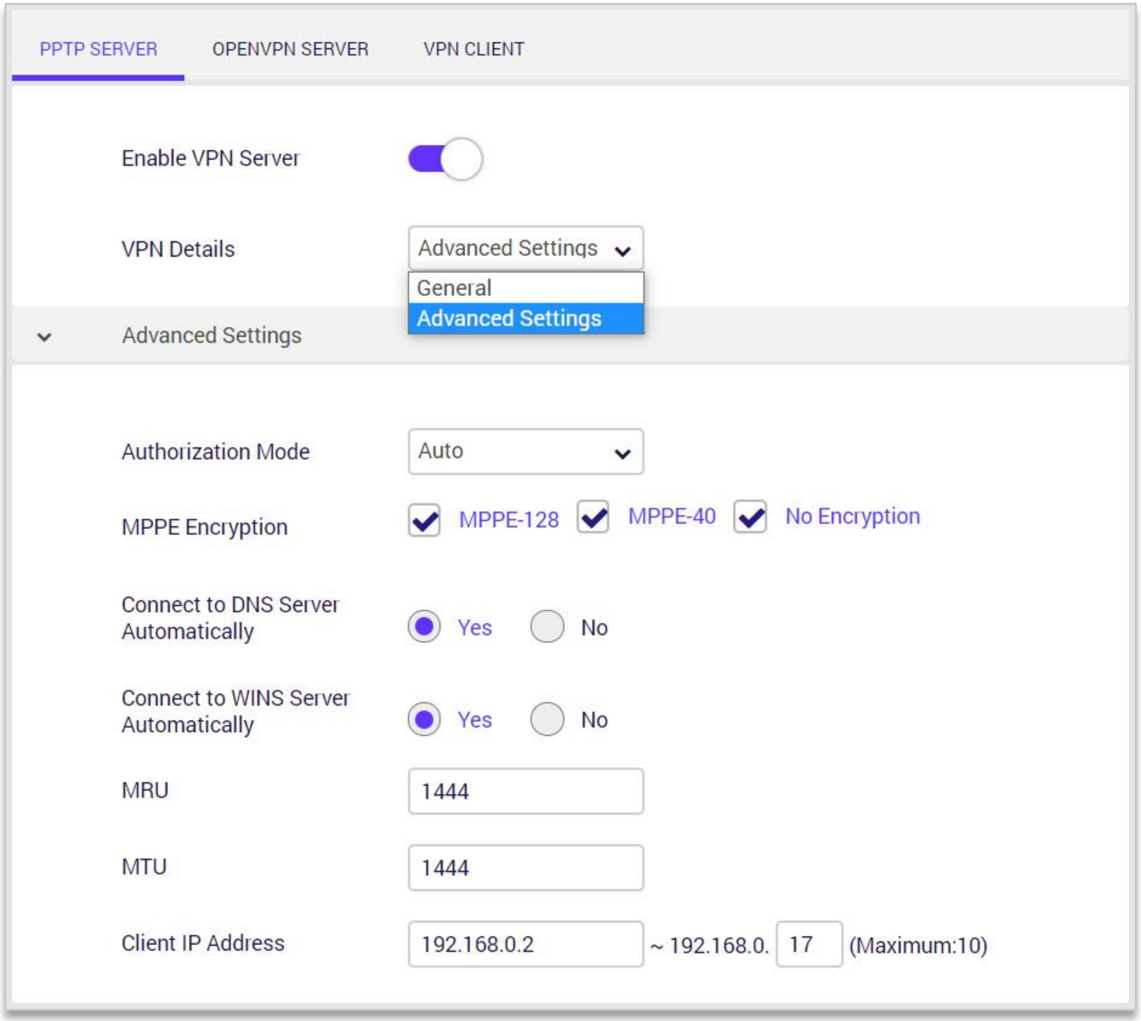
VPN Details: General

Username and Password (Maximum: 16)

Connection Status	Username	Password	Delete
disconnect	username	password	⊖

6.4.3.1 PPTP Server

PPTP VPN or point to point tunneling protocol is a legacy vpn protocol. It’s still commonly used and natively supported by a large scale of routers and clients. PPTP has a low data encryption compared to other VPN protocols. But it is quite safe to use for browsing activities and accessing blocked sites. **Enable the VPN Server** and then select General or Advance Settings from the **VPN Details** dropdown menu to configure the VPN settings.



Enable VPN Server ●

VPN Details: Advanced Settings

Advanced Settings

Authorization Mode: Auto

MPPE Encryption: ☑ MPPE-128 ☑ MPPE-40 ☑ No Encryption

Connect to DNS Server Automatically: ● Yes ○ No

Connect to WINS Server Automatically: ● Yes ○ No

MRU: 1444

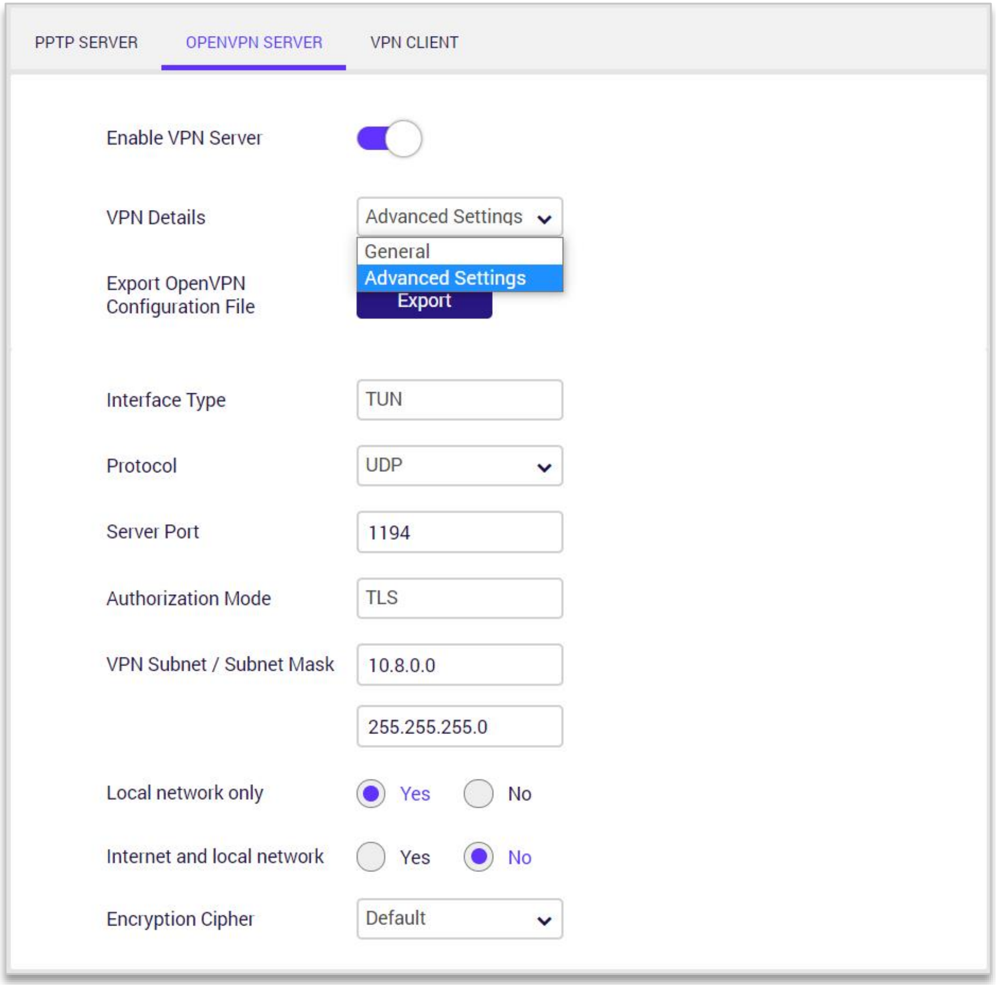
MTU: 1444

Client IP Address: 192.168.0.2 ~ 192.168.0. 17 (Maximum:10)

PPTP Server	
Enable VPN Server	Enable or disable the VPN Server.
VPN Details	Select General or Advanced settings.
Username and Password	Select General and click the Add Rule button. Input the username and password to authenticate the devices to the VPN server. Then click the Save button.
Advanced Settings	
Authorization Mode	Select Auto, MS-CHAPv1, or MS-CHAPv2.
MPPE Encryption	Select the MPPE Encryption type “MPPE-128, MPPE-40, or No Encryption”.
Connect to DNS Server Automatically	Select Yes or No to connect to the DNS Server automatically.
Connect to WINS Server Automatically	Select Yes or No to connect to the WINS Server automatically.
MRU	The Maximum Receive Unit (MRU) sizes are sent to the client as part of the PPTP parameters to use during the PPTP session. We recommend that you do not change the MRU values. The incorrect MRU values cause the traffic through the PPTP VPN to fail.
MTU	The Maximum Transmission Unit (MTU) sizes are sent to the client as part of the PPTP parameters to use during the PPTP session. We recommend that you do not change the MTU values. The incorrect MTU values cause the traffic through the PPTP VPN to fail.
Client IP Address	The IP address range of PPTP clients.

6.4.3.2 OpenVPN Server

OpenVPN is a robust and highly flexible tunneling application that uses all of the encryption, authentication, and certification features of the OpenSSL library to securely tunnel IP networks over a single TCP/UDP port. **Enable the VPN Server** and then select General or Advance Settings from the **VPN Details** dropdown menu to configure the VPN settings. You can use the Export button to export the configuration file.



Enable VPN Server: ●

VPN Details: Advanced Settings

Export OpenVPN Configuration File: Export

Interface Type: TUN

Protocol: UDP

Server Port: 1194

Authorization Mode: TLS

VPN Subnet / Subnet Mask: 10.8.0.0
255.255.255.0

Local network only: ● Yes ○ No

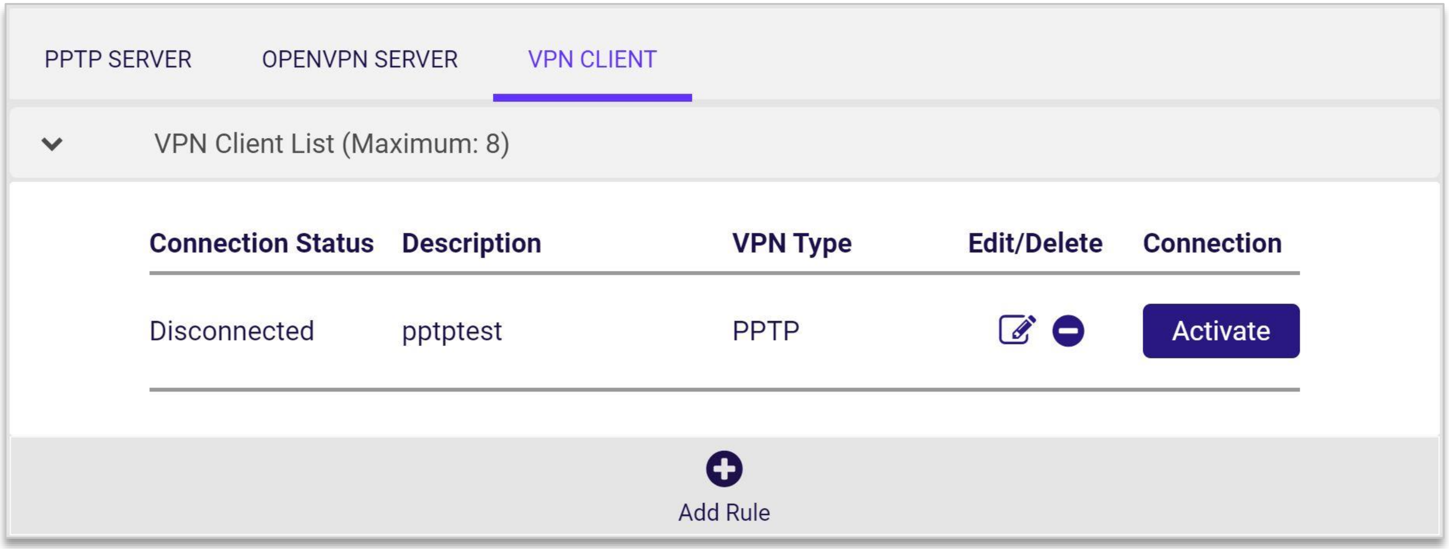
Internet and local network: ○ Yes ● No

Encryption Cipher: Default

OpenVPN Server	
Enable VPN Server	Enable or disable the VPN Server.
VPN Details	Select General or Advanced settings.
Export OpenVPN Configuration File	Export the configuration file.
Username and Password	Select General and click the Add Rule button. Input the username and password to authenticate the devices to the VPN server. Then click the Save button.
Advanced Settings	
Interface Type	Select TUN to create a routed IP tunnel.
Protocol	Select TCP or UDP.
Server Port	The TCP/UDP port which OpenVPN server will listen on.
Authorization Mode	Select the authorization mode.
VPN Subnet / Subnet Mask	Configure the VPN subnet and subnet mask settings.
Local network only	Select Yes or No according to the requirement.
Internet and local network	Select Yes or No according to the requirement.
Encryption Cipher	Select a cryptographic method. This configuration item must be copied to the client configure file as well.

6.4.3.3 VPN Client

VPN clients are used to connect to a specific VPN server and access private resources securely over a public network. This feature routes all traffic from devices in the home network through the VPN, without having to install VPN software on each device. To start a VPN connection, please follow the steps below:



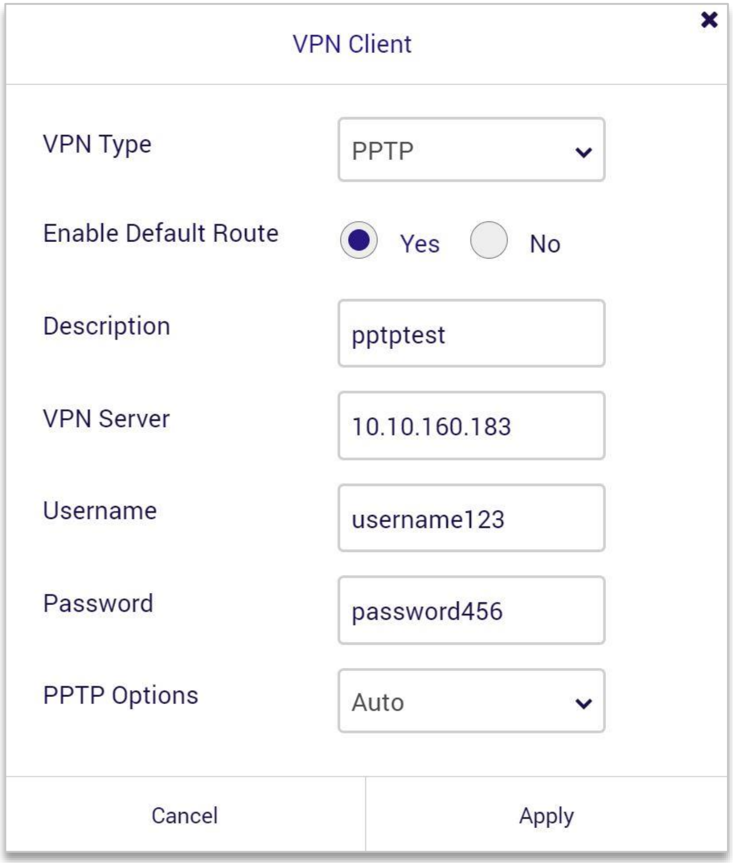
Connection Status	Description	VPN Type	Edit/Delete	Connection
Disconnected	pptptest	PPTP	✎ ⊖	Activate

1. Click **Add Rule** ⊕. Enter the parameters in accordance with your requirements.

2. Click **Apply** to have the rule created on VPN client list and then click Save to apply your changes. You can modify or remove the rules by using the ✎ and ⊖ icons. Click the Activate button to activate the connection.

   Note: The maximum number on VPN Client list is 8 rules

VPN Type - PPTP



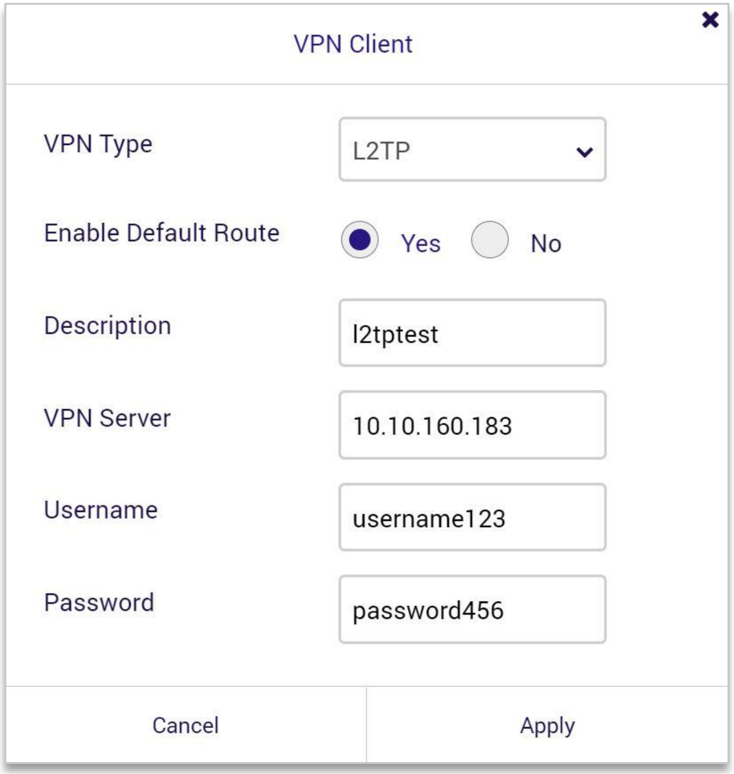
VPN Client ✕

VPN Type	PPTP
Enable Default Route	● Yes ○ No
Description	pptptest
VPN Server	10.10.160.183
Username	username123
Password	password456
PPTP Options	Auto

Cancel Apply

VPN Type	Select the VPN Type **PPTP** from the dropdown menu.
Enable Default Route	Enable default route if requires.
Description	Specify the name.
VPN Server	Enter the server name or server IP of the VPN Server.
Username	Enter the username.
Password	Enter the password.
PPTP Options	Select the PPTP Options **Auto/No Encryption/MPPE 40/ MPPE 128** from the dropdown menu.

VPN Type - L2TP

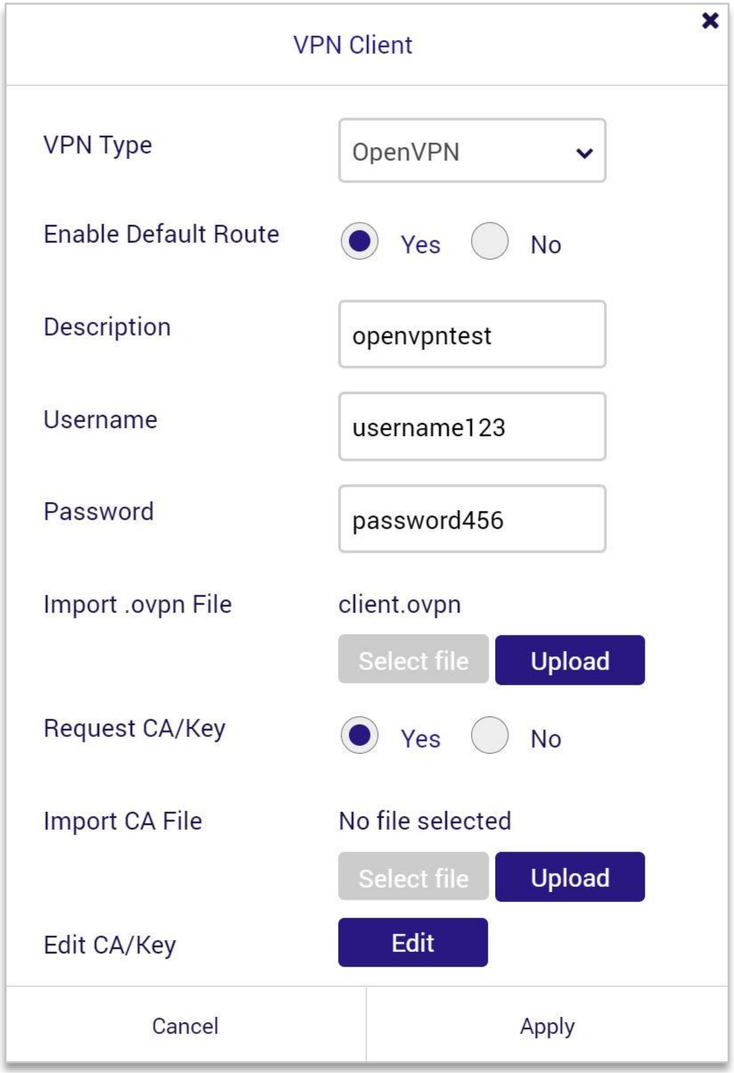


VPN Client

VPN Type	L2TP
Enable Default Route	● Yes ○ No
Description	l2tptest
VPN Server	10.10.160.183
Username	username123
Password	password456

VPN Type	Select the VPN Type **L2TP** from the dropdown menu.
Enable Default Route	Enable default route if requires.
Description	Specify the name.
VPN Server	Enter the server name or server IP of the VPN Server.
Username	Enter the username.
Password	Enter the password.

VPN Type - OpenVPN



VPN Client

VPN Type: OpenVPN

Enable Default Route: ● Yes ○ No

Description: openvpntest

Username: username123

Password: password456

Import .ovpn File: client.ovpn

Request CA/Key: ● Yes ○ No

Import CA File: No file selected

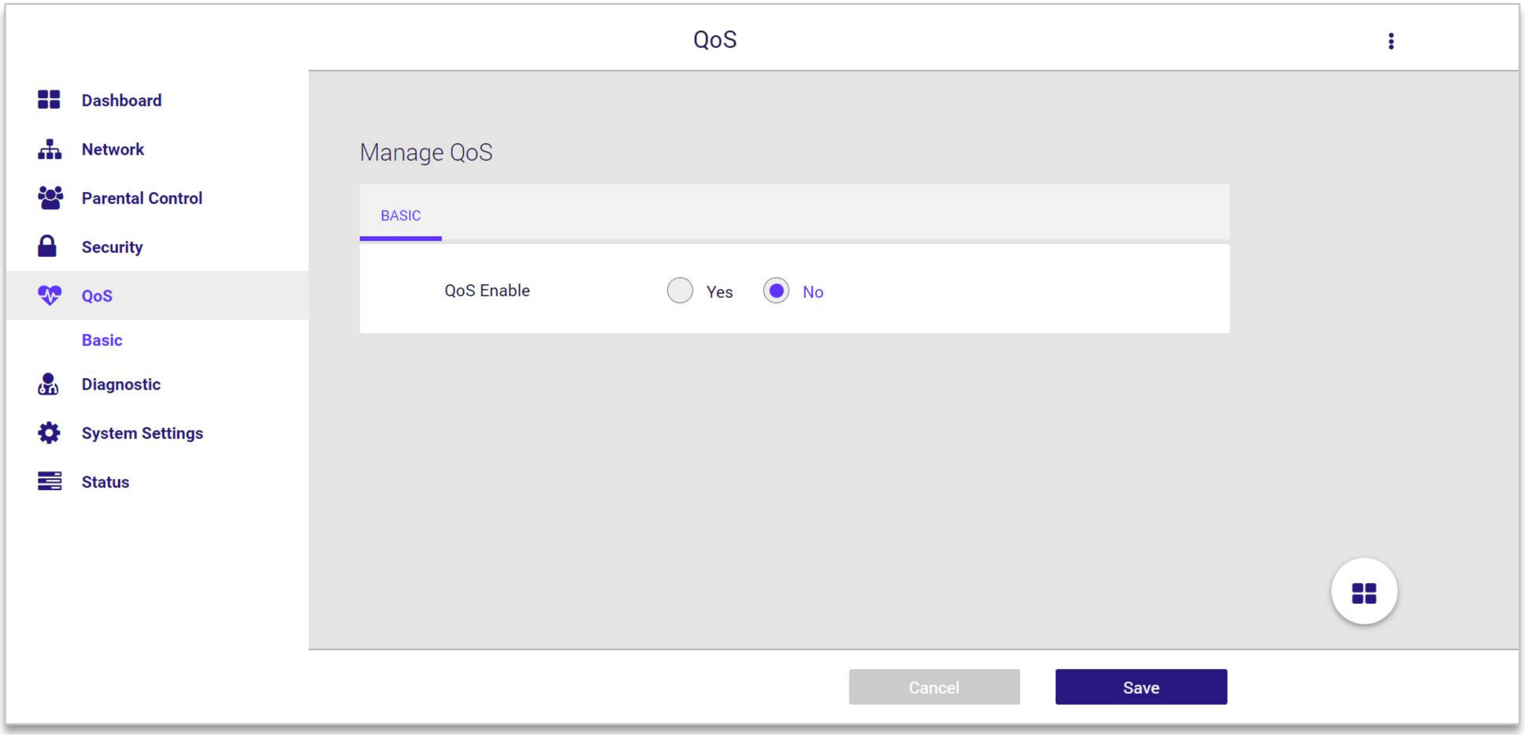
Edit CA/Key

VPN Type	Select the VPN Type **OpenVPN** from the dropdown menu.
Enable Default Route	Enable default route if requires.
Description	Specify the name.
Username	Enter the username.
Password	Enter the password.
Import .ovpn File	Select the file exported from the OpenVPN server. Then click the **Upload** button.
Request CA/Key	Use the Yes/No radio button to request the CA/Key if requires. Then configure the detailed options.
Import CA File	Select the specific CA file you would like to import. Then click the **Upload** button.
Edit CA/Key	Manually edit the content of **Certificate Authority**, **Client Certificate**, **Client Key**, and **Static Key**.

6.5 QoS

Quality of Service (QoS) is a feature that gives different priority to different traffic stream. So when you have a lot of family members using Internet at the same time, the person with QoS priority will have a guaranteed Internet experience.

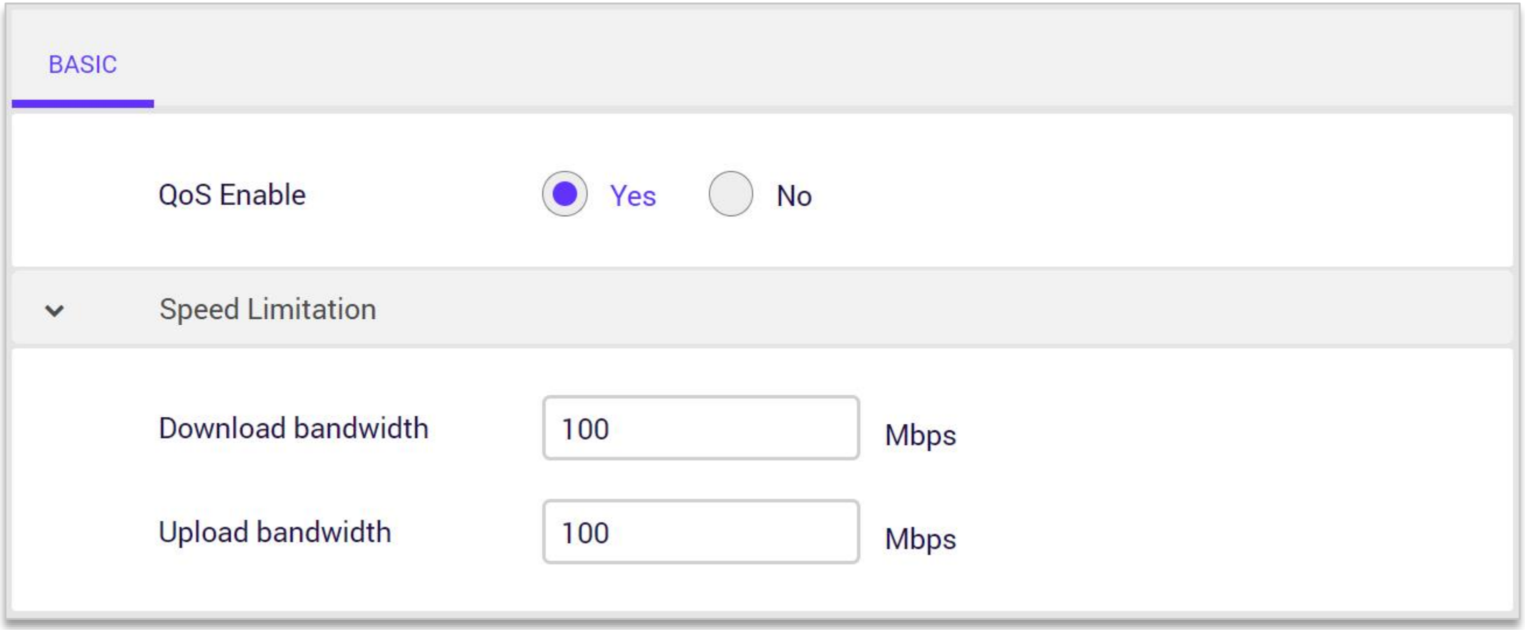
QoS does not really give you a bigger Internet bandwidth. It works by slowing down low priority traffic to yield the bandwidth to high priority traffic. So if you give everyone high priority, then no one has priority. This mechanism works best if only one person at home with critical task get the priority. For example, if Dad works from home with important business video call while everyone else is playing games, then you can give Dad the priority to make sure his meeting is smooth. Or maybe one kid is playing real time online game and he gets a big jitter delay and can't win often. Then you can give him the priority, so he can win the game.



QoS Enable ○ Yes ● No

6.5.1 Basic

To enable QoS feature in Dynalink router, you can configure from both, APP or Web UI. First you should enable the master QoS setting and specify maximum upload and download bandwidth. So the QoS logic can start to drop low priority traffic when total bandwidth is approaching the limit. If the maximum bandwidth number is set too high, QoS will not kick in, if the number is set too low, QoS logic will start to drop packets too early. The more accurately the max bandwidth is set, the better the QoS function works. We suggest to use a speed test tool. There are many free tools on the Internet you can use or you can check with your ISP.

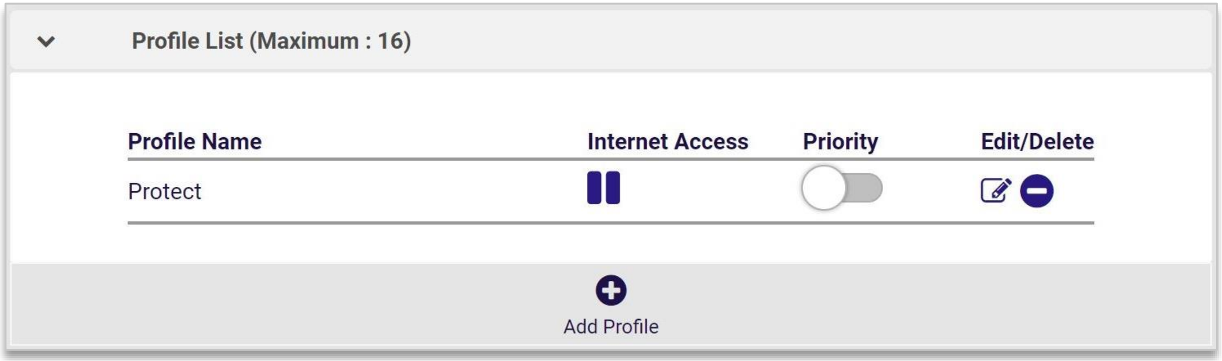


QoS Enable ● Yes ○ No

Download bandwidth 100 Mbps

Upload bandwidth 100 Mbps

After you enable the master QoS setting, you have to go to Parental Control profiles to choose which ones will be granted priority access to bandwidth. Slide on/off the priority switch for each profile.



Profile List (Maximum : 16)

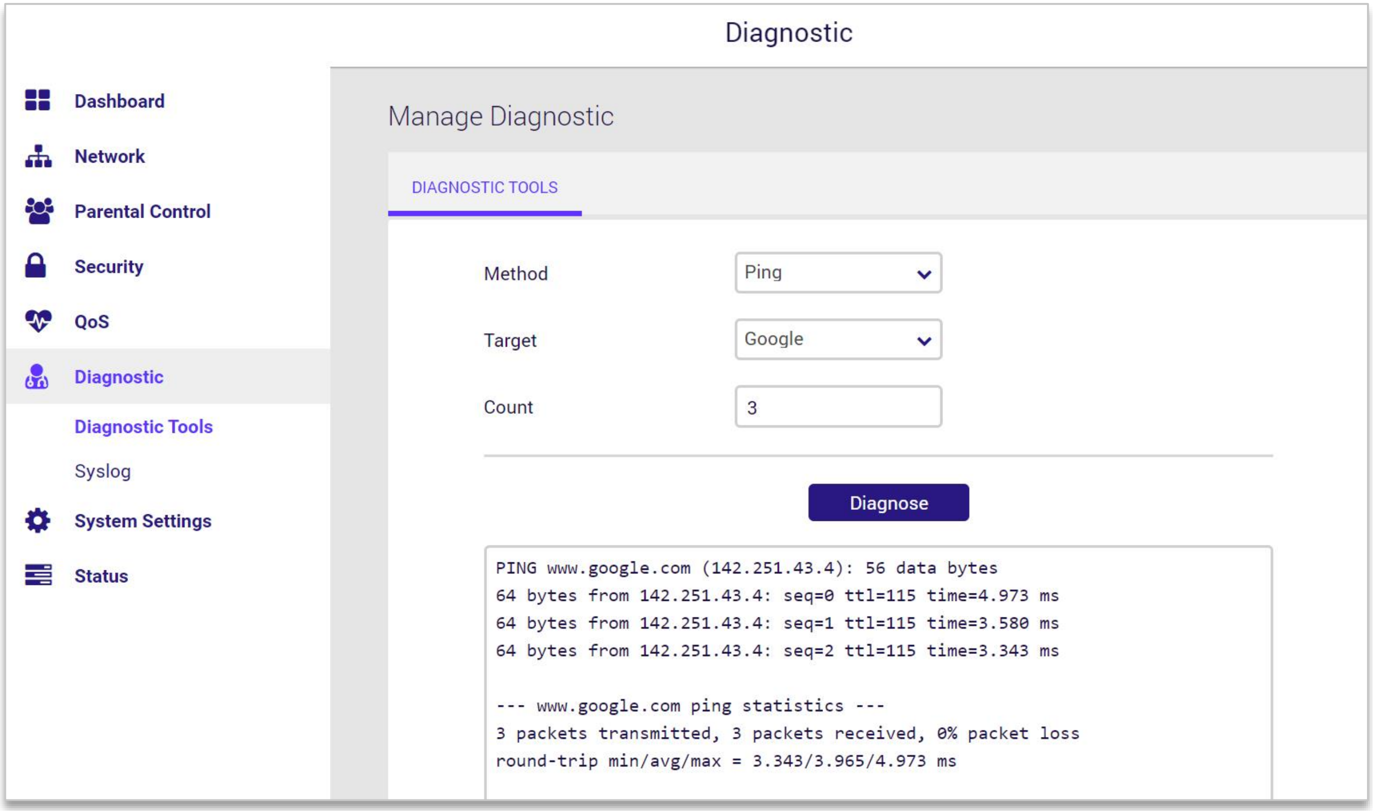
Profile Name	Internet Access	Priority	Edit/Delete
Protect	❚❚	○	✎ ⊖

Note: If you want to disable QoS and give everyone a fair priority, you simply need to disable the master QoS setting. Remember that QoS effectiveness is higher if less devices have the priority function, pay attention to the amount of devices per profile.

6.6 Diagnostic

6.6.1 Diagnostic Tools

Diagnostic tools allows you to run a **Ping**, **Traceroute**, **Nslookup** and **Ping6** tests with the router. Enter the IP address to use for the test and then click Diagnose, results are displayed in the diagnostic box.



Method: Ping

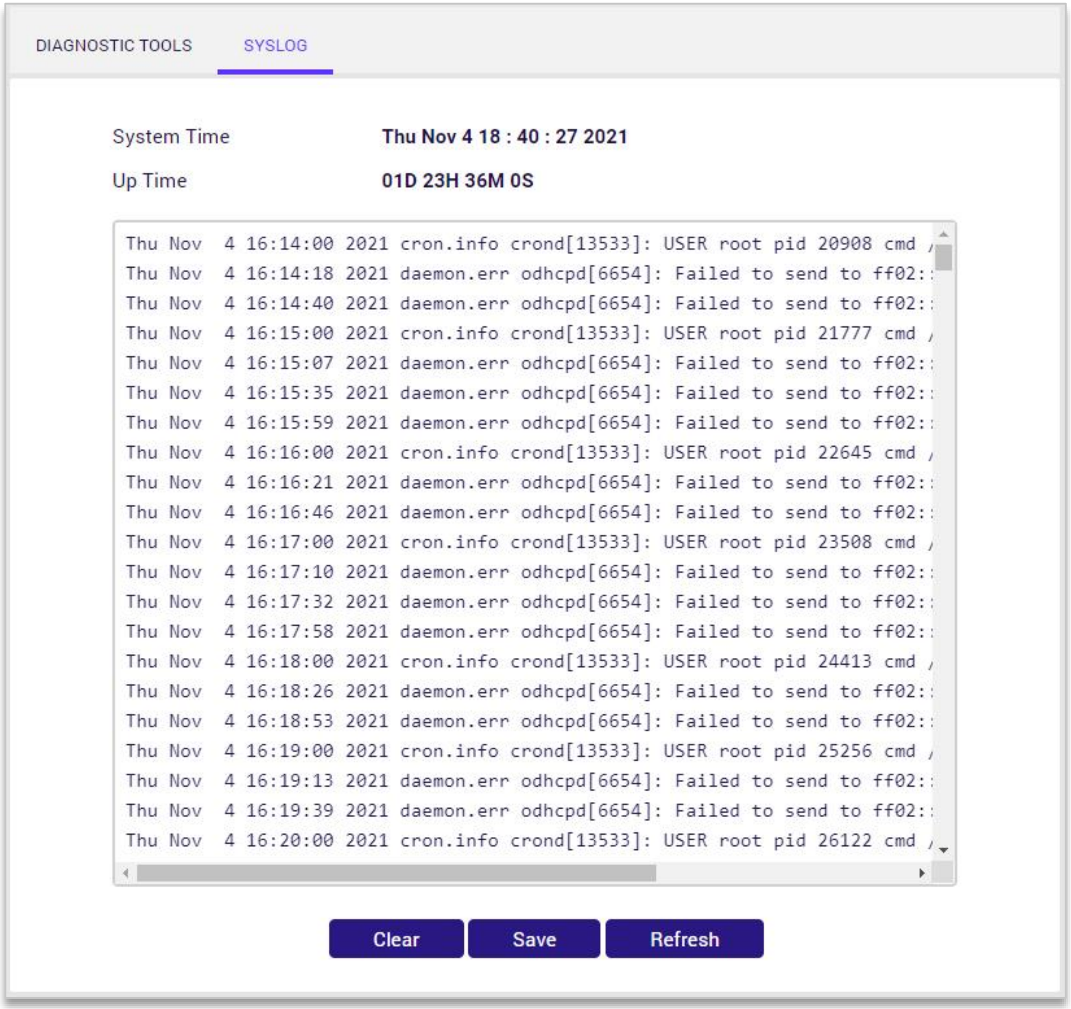
Target: Google

Count: 3

```
PING www.google.com (142.251.43.4): 56 data bytes
64 bytes from 142.251.43.4: seq=0 ttl=115 time=4.973 ms
64 bytes from 142.251.43.4: seq=1 ttl=115 time=3.580 ms
64 bytes from 142.251.43.4: seq=2 ttl=115 time=3.343 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3.343/3.965/4.973 ms
```

6.6.2 Syslog

System logs, track local events on your Mesh Wi-Fi Router. You can click Cear to clear the content of the system logs. You can save logs by clicking Save or Click Refresh to update the logs content.



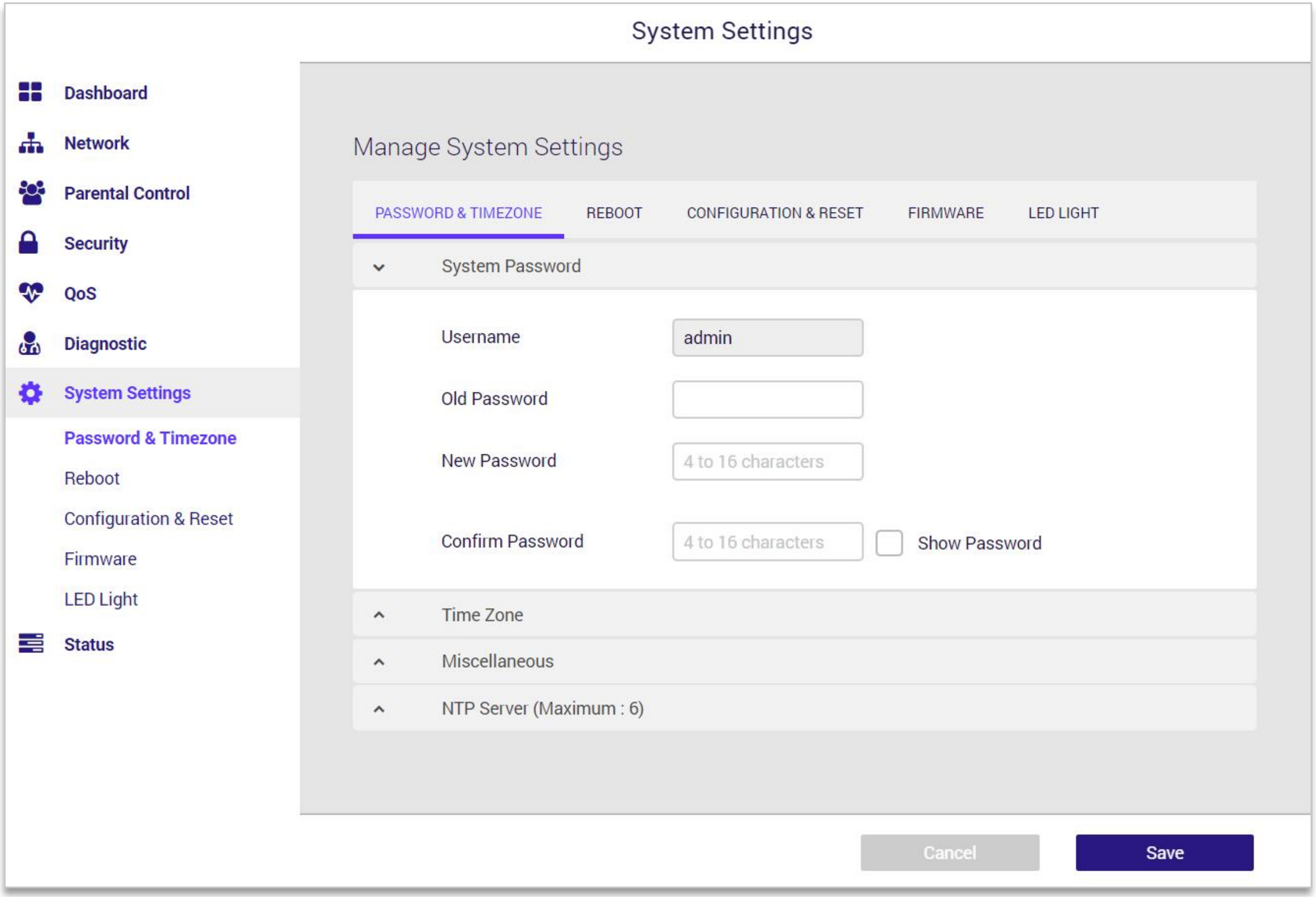
System Time Thu Nov 4 18 : 40 : 27 2021

Up Time 01D 23H 36M 0S

```
Thu Nov  4 16:14:00 2021 cron.info crond[13533]: USER root pid 20908 cmd /
Thu Nov  4 16:14:18 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:14:40 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:15:00 2021 cron.info crond[13533]: USER root pid 21777 cmd /
Thu Nov  4 16:15:07 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:15:35 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:15:59 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:16:00 2021 cron.info crond[13533]: USER root pid 22645 cmd /
Thu Nov  4 16:16:21 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:16:46 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:17:00 2021 cron.info crond[13533]: USER root pid 23508 cmd /
Thu Nov  4 16:17:10 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:17:32 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:17:58 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:18:00 2021 cron.info crond[13533]: USER root pid 24413 cmd /
Thu Nov  4 16:18:26 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:18:53 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:19:00 2021 cron.info crond[13533]: USER root pid 25256 cmd /
Thu Nov  4 16:19:13 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:19:39 2021 daemon.err odhcpd[6654]: Failed to send to ff02::
Thu Nov  4 16:20:00 2021 cron.info crond[13533]: USER root pid 26122 cmd /
```

6.7 System Settings

Various administrative functions of your router can be configured from the System Settings menu, including the Web UI login password, date & time settings, backup, firmware and system logs.



System Settings

Manage System Settings

Username: admin

Old Password:

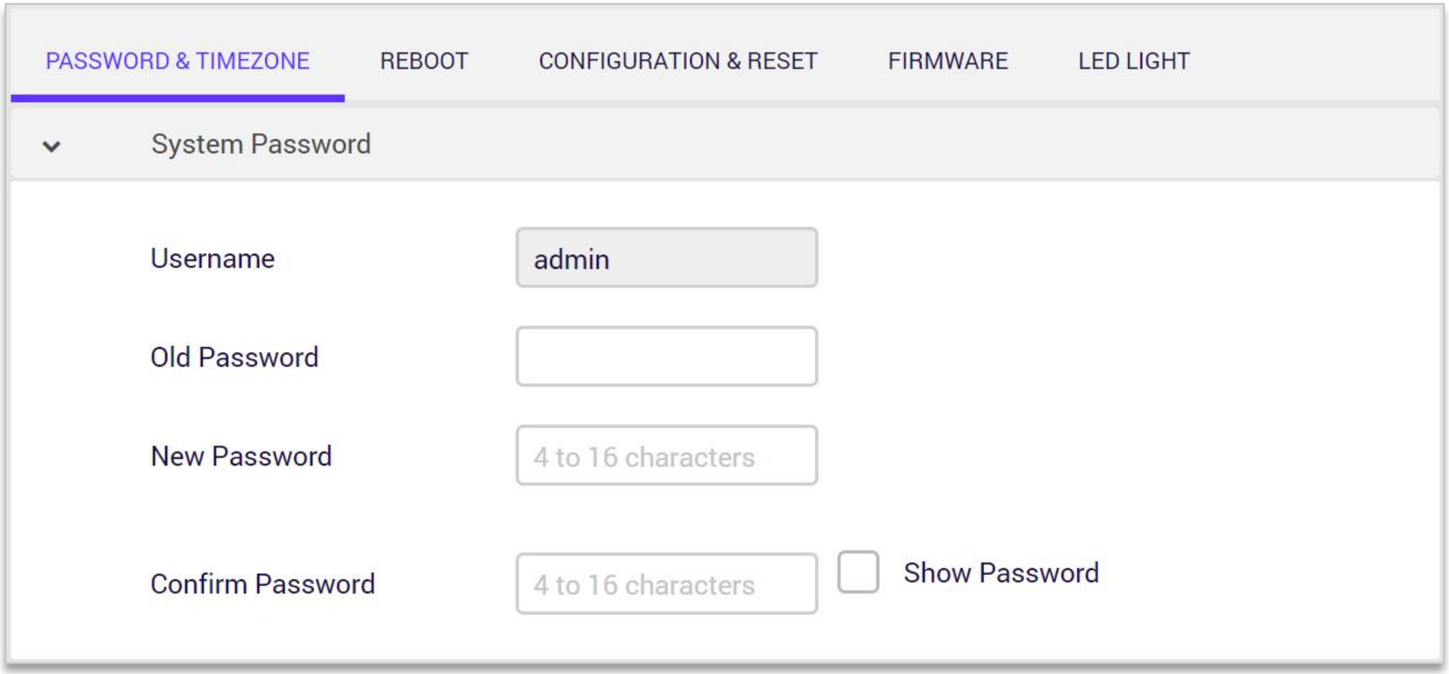
New Password: 4 to 16 characters

Confirm Password: 4 to 16 characters □ Show Password

6.7.1 Password & Timezone

System Password- The password function allows you to change the login password for the router's Web UI. It's essential to change this password for the security of your router. Use hard-to-guess password which include combinations of numbers, letters and symbols, and change your password regularly.

1. Enter the old password for authentication.
2. Enter your new password in the New Password field and again to confirm, and select Save to save the new settings.



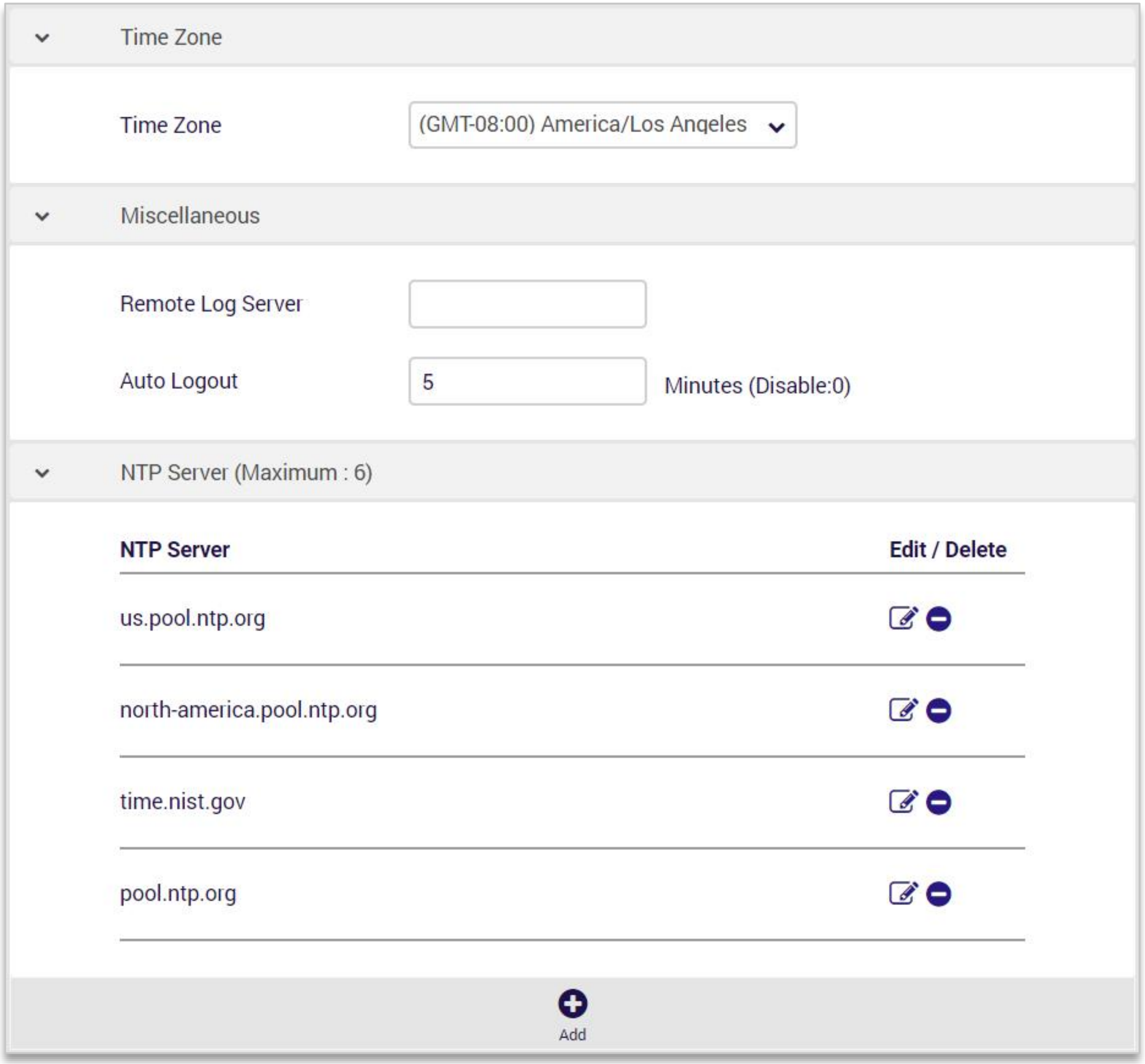
System Password

Username	admin
Old Password	
New Password	4 to 16 characters
Confirm Password	4 to 16 characters

□ Show Password

Time Zone- Set the time zone for your router. You can use a Network Time Protocol (NTP) which synchronizes the date and time with public time servers, or the router can get the date and time automatically based on your selected time zone.

1. Select your time zone from the drop-down menu.
2. If you want to use NTP to synchronize date and time with public time servers, enter the NTP Servers and Save settings.
3. Set the Time Zone back to Automatic to use the selected time zone automatically, and save the settings.



Time Zone

Time Zone: (GMT-08:00) America/Los Angeles

Miscellaneous

Remote Log Server:

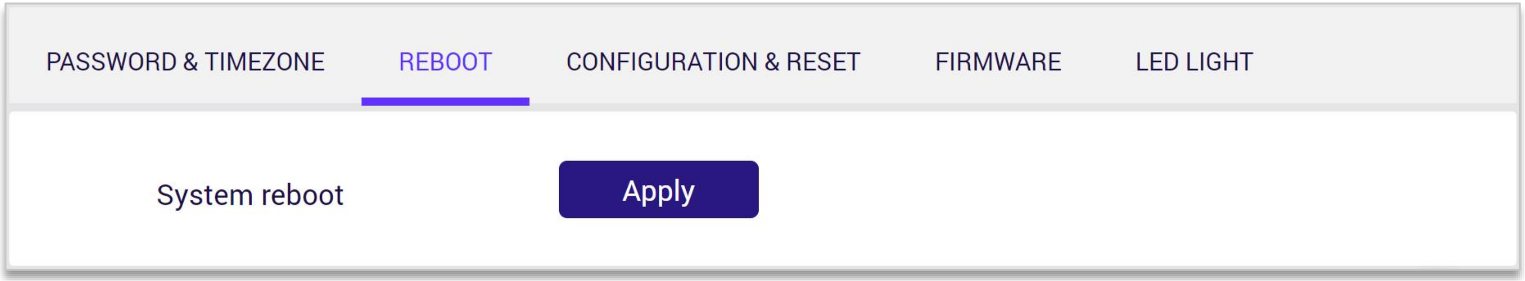
Auto Logout: 5 Minutes (Disable:0)

NTP Server (Maximum : 6)

NTP Server	Edit / Delete
us.pool.ntp.org	
north-america.pool.ntp.org	
time.nist.gov	
pool.ntp.org	

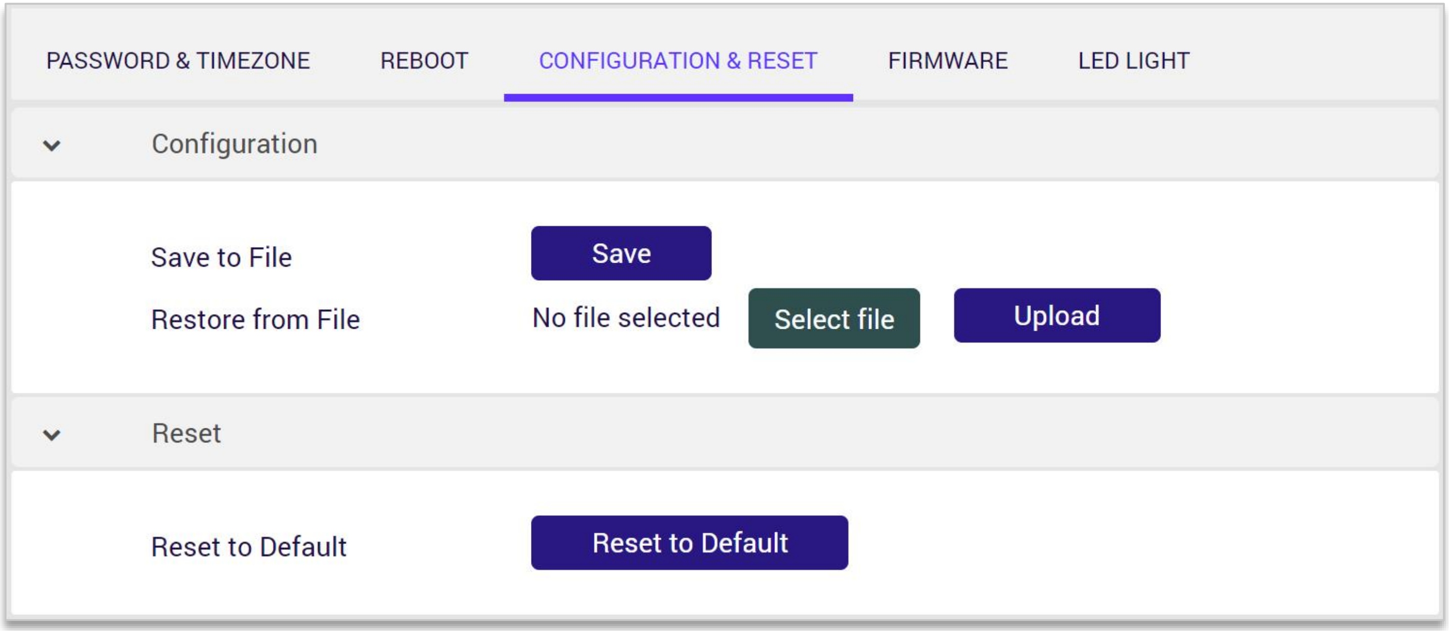
6.7.2 Reboot

Reboot the router by press Apply button.



6.7.3 Configuration & Reset

The Configuration & Reset page enables you to save/upload the router's current settings as a file to your local computer, or upload your router to previously saved settings by loading a backed up file. You can also reset the router back to factory default settings. If the router malfunctions or is not responding, then it is recommended that you first reboot the device (press the reset button for 1 second), and if still experiencing problems reset the device back to its factory default settings. You can reset the router back to its default settings using the Reset button on the back of the router (press and hold for **7+** seconds).



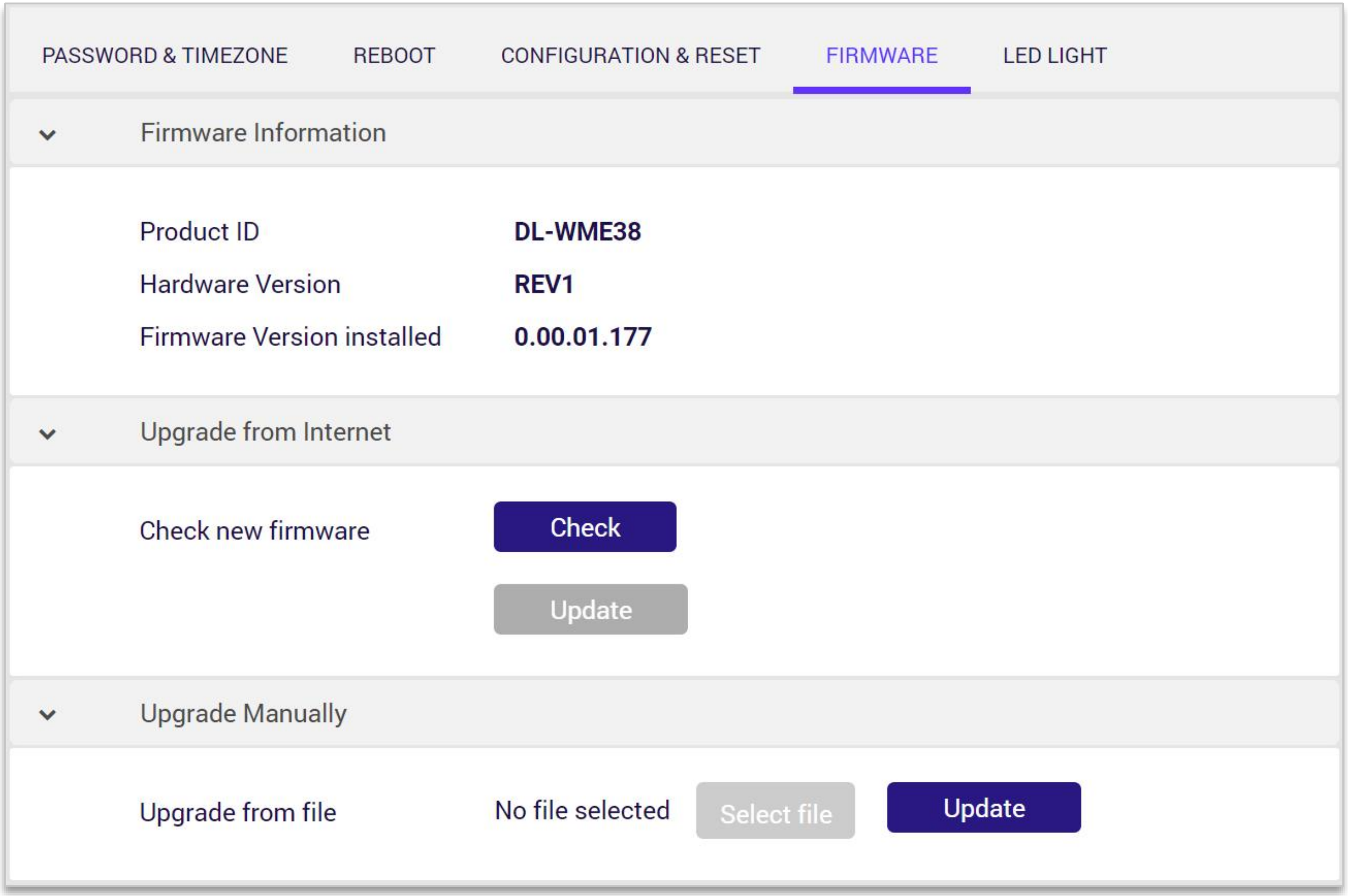
Note:

1. Reboot the device – press the reset button for 1 second;
2. Reset the device back to its factory default settings – press and hold for **7+** seconds.

Configuration	
Save to File	Click the Save button to copy of your current settings and download configuration file to your local computer.
Restore from File	Restore saved settings from a configuration file. Choose Select File to locate a previously saved settings file on your computer. Select it to restore to your router.
Reset	
Reset to default	Revert all the settings to factory default values. Select Reset to default button to revert your router to the factory default configuration. This resets all settings.

6.7.4 Firmware

The Firmware page displays your router’s firmware version and hardware version information and can upload firmware manually when select a valid firmware to update it.



Product ID DL-WME38

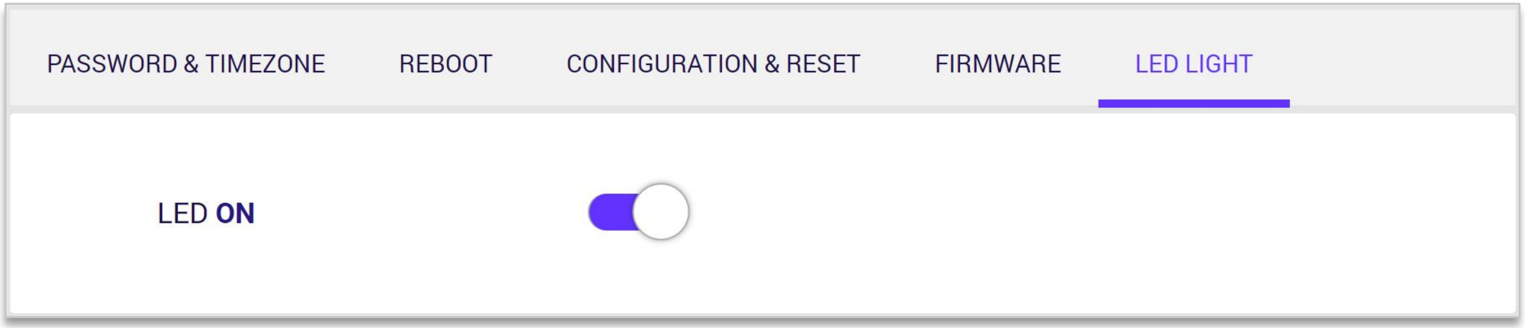
Hardware Version REV1

Firmware Version installed 0.00.01.177

No file selected

6.7.5 LED Light

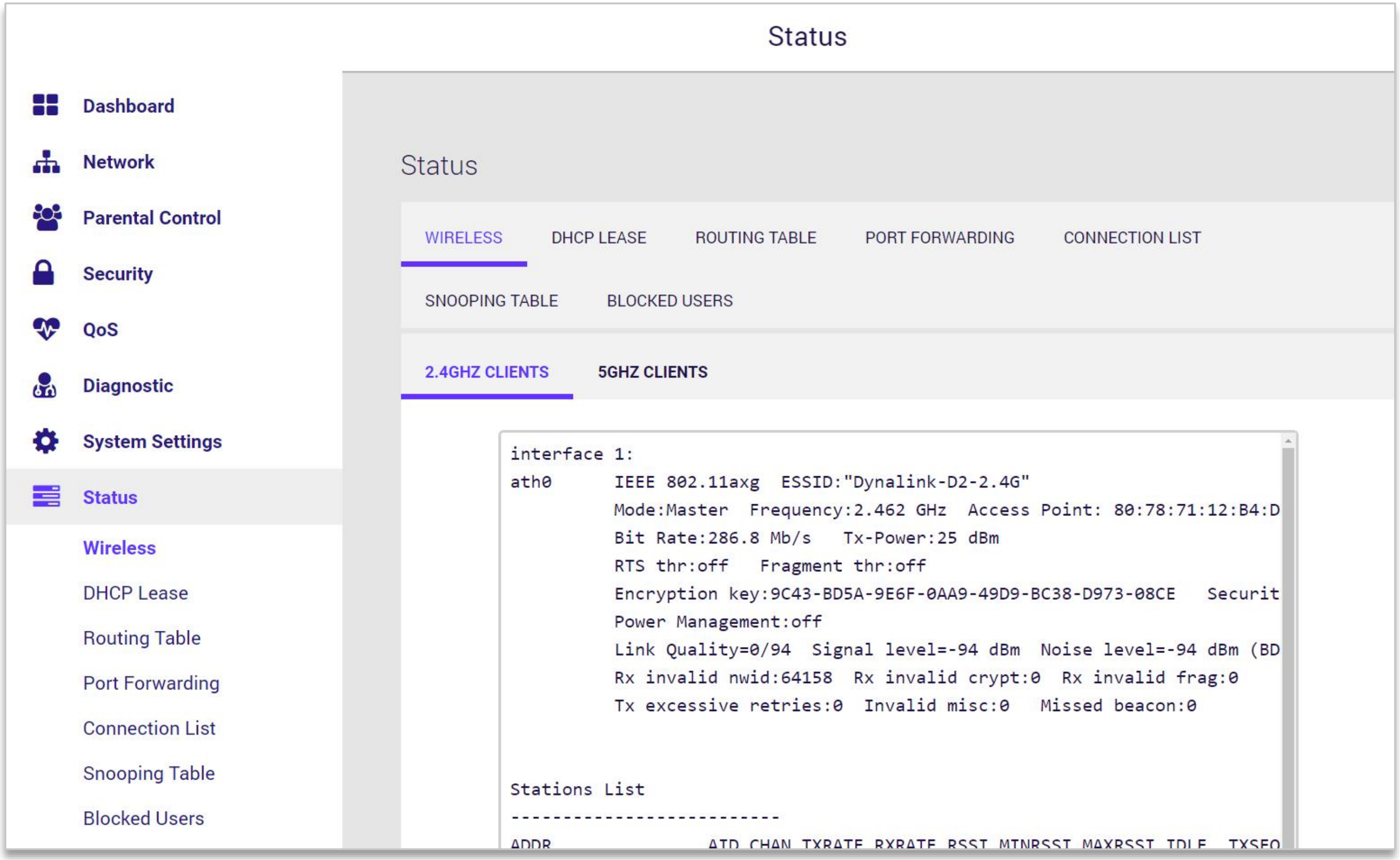
This page allows you to enable or disable the LED on your router.



LED **ON**

6.8 Status

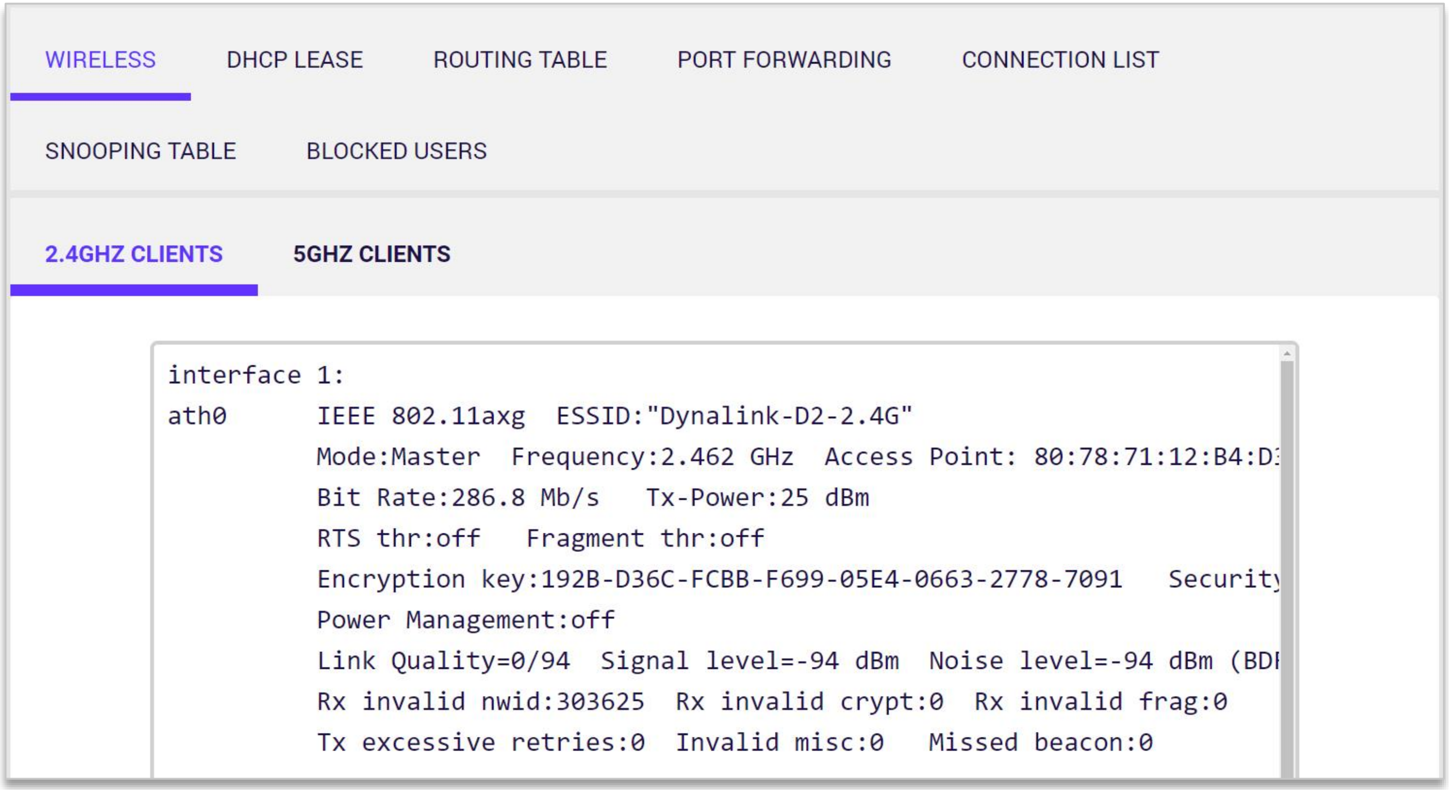
Network Status displays the status of the network across 7 categories: **Wireless**, **DHCP Lease**, **Routing Table**, **Port Forwarding**, **Connection List**, **Snooping Table**, **Blocked Users**. Information is listed in Network Status for reference as described below:



```
interface 1:
ath0      IEEE 802.11axg  ESSID:"Dynalink-D2-2.4G"
          Mode:Master  Frequency:2.462 GHz  Access Point: 80:78:71:12:B4:D
          Bit Rate:286.8 Mb/s   Tx-Power:25 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:9C43-BD5A-9E6F-0AA9-49D9-BC38-D973-08CE   Securit
          Power Management:off
          Link Quality=0/94  Signal level=-94 dBm  Noise level=-94 dBm (BD
          Rx invalid nwid:64158  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0


Stations List
--------------------------
ADDR               AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE  TXSEQ
```

6.8.1 Wireless

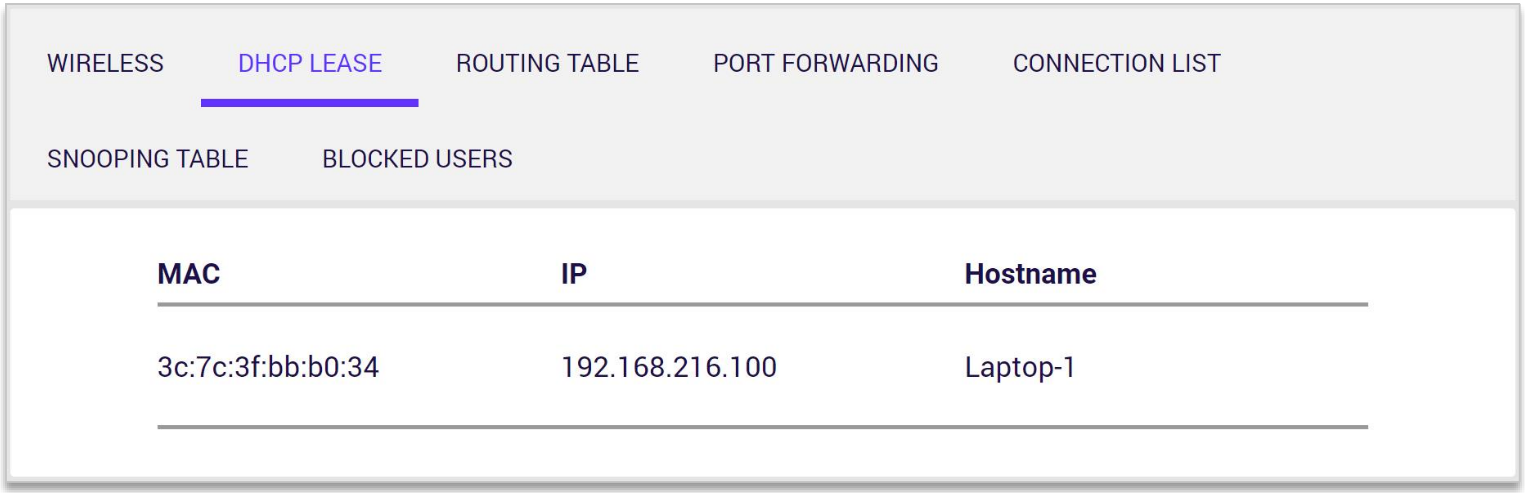
Displays your router's Wi-Fi information for both 2.4GHz & 5GHz frequencies. Includes network name (SSID) and radio & channel information. To edit these Wi-Fi settings go to Network > Mesh Settings.



```
interface 1:
ath0      IEEE 802.11axg  ESSID:"Dynalink-D2-2.4G"
          Mode:Master  Frequency:2.462 GHz  Access Point: 80:78:71:12:B4:D
          Bit Rate:286.8 Mb/s   Tx-Power:25 dBm
          RTS thr:off   Fragment thr:off
          Encryption key:192B-D36C-FCBB-F699-05E4-0663-2778-7091   Securit
          Power Management:off
          Link Quality=0/94  Signal level=-94 dBm  Noise level=-94 dBm (BD
          Rx invalid nwid:303625  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

6.8.2 DHCP Lease

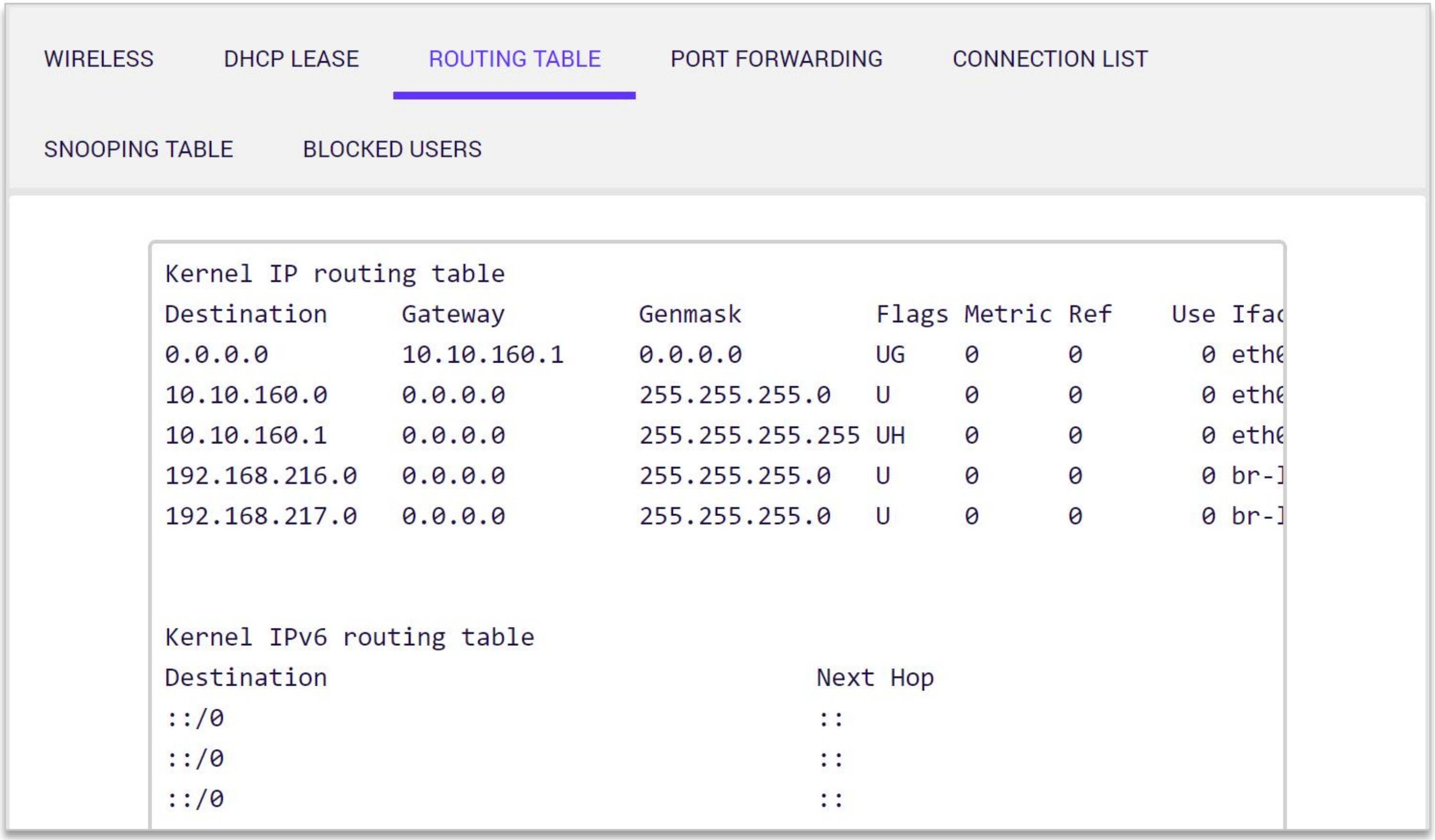
Displays the DHCP address allocation, including MAC, IP and Hostname.



MAC	IP	Hostname
3c:7c:3f:bb:b0:34	192.168.216.100	Laptop-1

6.8.3 Routing Table

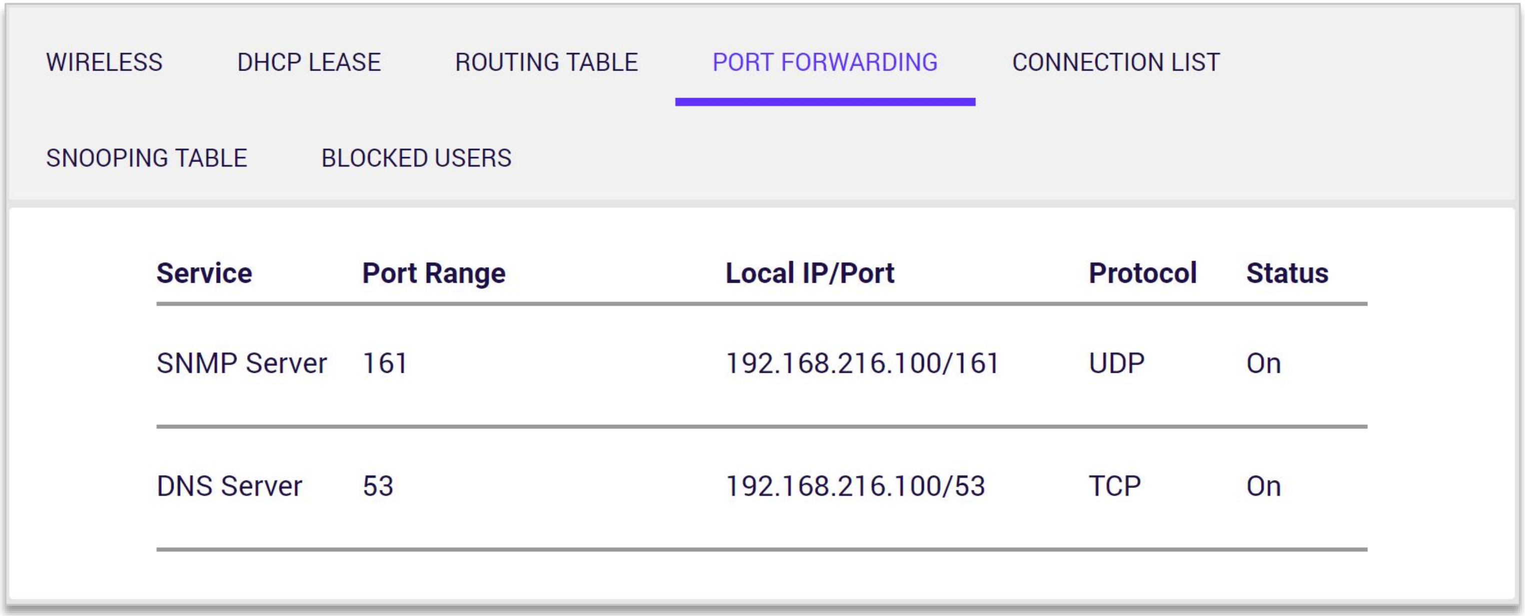
Displays the Wi-Fi router’s routing table information including IPv4 and IPv6 routing table.



```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Ifac
0.0.0.0         10.10.160.1     0.0.0.0         UG    0      0        0 eth0
10.10.160.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
10.10.160.1     0.0.0.0         255.255.255.255 UH    0      0        0 eth0
192.168.216.0   0.0.0.0         255.255.255.0   U     0      0        0 br-l
192.168.217.0   0.0.0.0         255.255.255.0   U     0      0        0 br-l


Kernel IPv6 routing table
Destination                                 Next Hop
::/0                                        ::
::/0                                        ::
::/0                                        ::
```

6.8.4 Port Forwarding

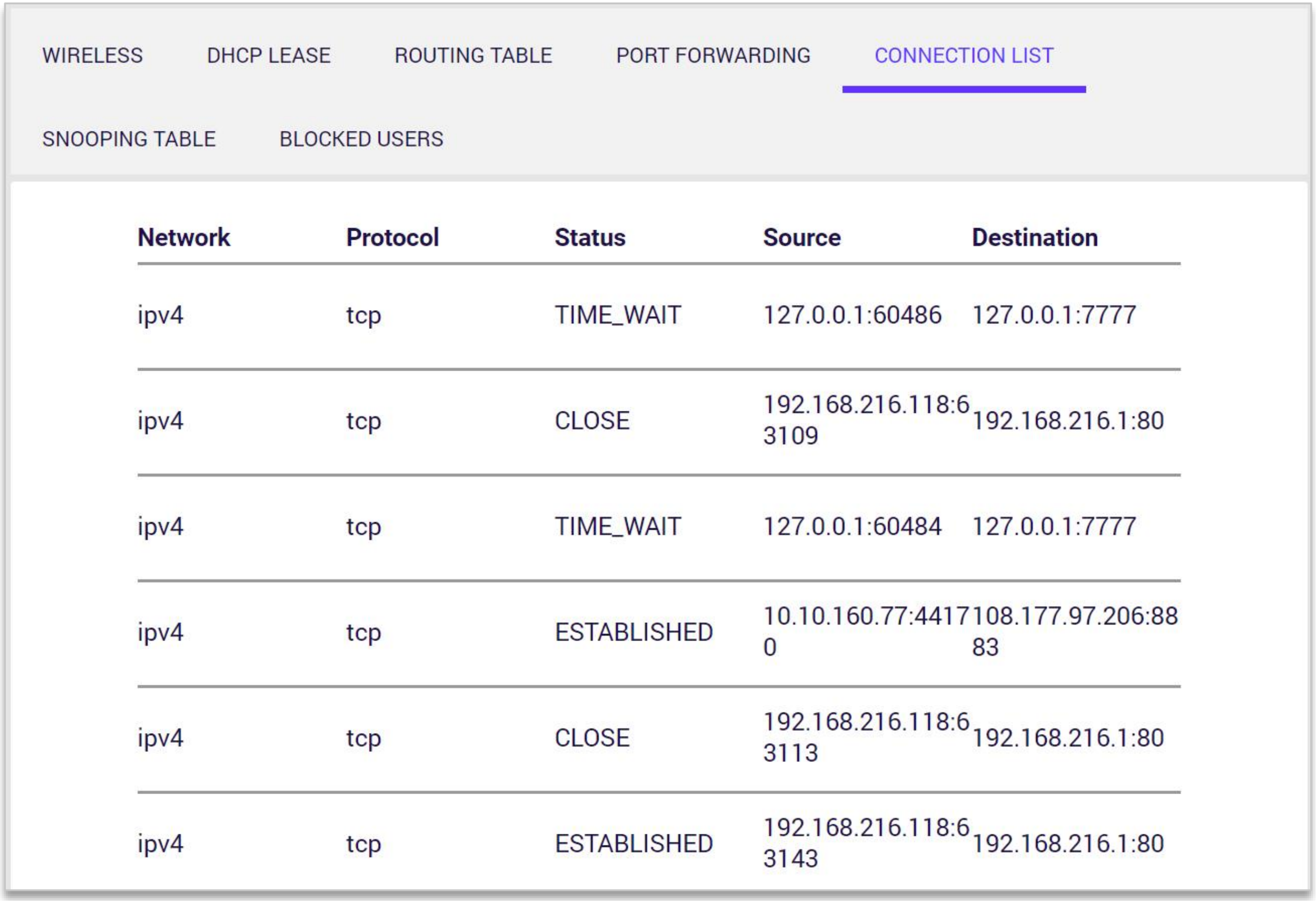
Displays the router’s Port Forwarding Rule including service, port range, local IP/port, protocol and status. To edit port forwarding settings go to Network > WAN > Port Forwarding.



Service	Port Range	Local IP/Port	Protocol	Status
SNMP Server	161	192.168.216.100/161	UDP	On
DNS Server	53	192.168.216.100/53	TCP	On

6.8.5 Connection List

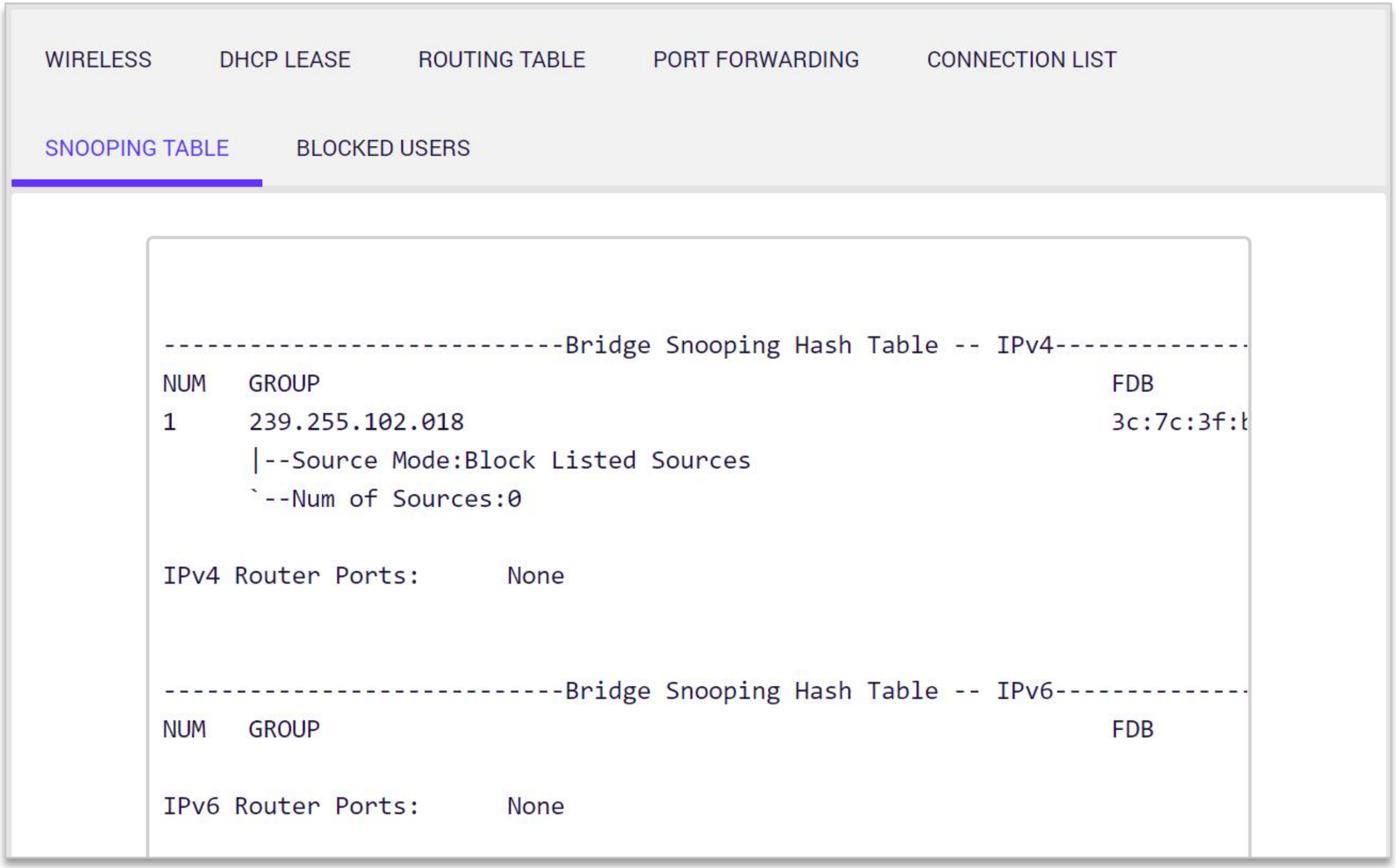
Displays Network, protocol, status, source and destination of the device connected to router.



Network	Protocol	Status	Source	Destination
ipv4	tcp	TIME_WAIT	127.0.0.1:60486	127.0.0.1:7777
ipv4	tcp	CLOSE	192.168.216.118:63109	192.168.216.1:80
ipv4	tcp	TIME_WAIT	127.0.0.1:60484	127.0.0.1:7777
ipv4	tcp	ESTABLISHED	10.10.160.77:44170	108.177.97.206:8883
ipv4	tcp	CLOSE	192.168.216.118:63113	192.168.216.1:80
ipv4	tcp	ESTABLISHED	192.168.216.118:63143	192.168.216.1:80

6.8.6 Snooping Table

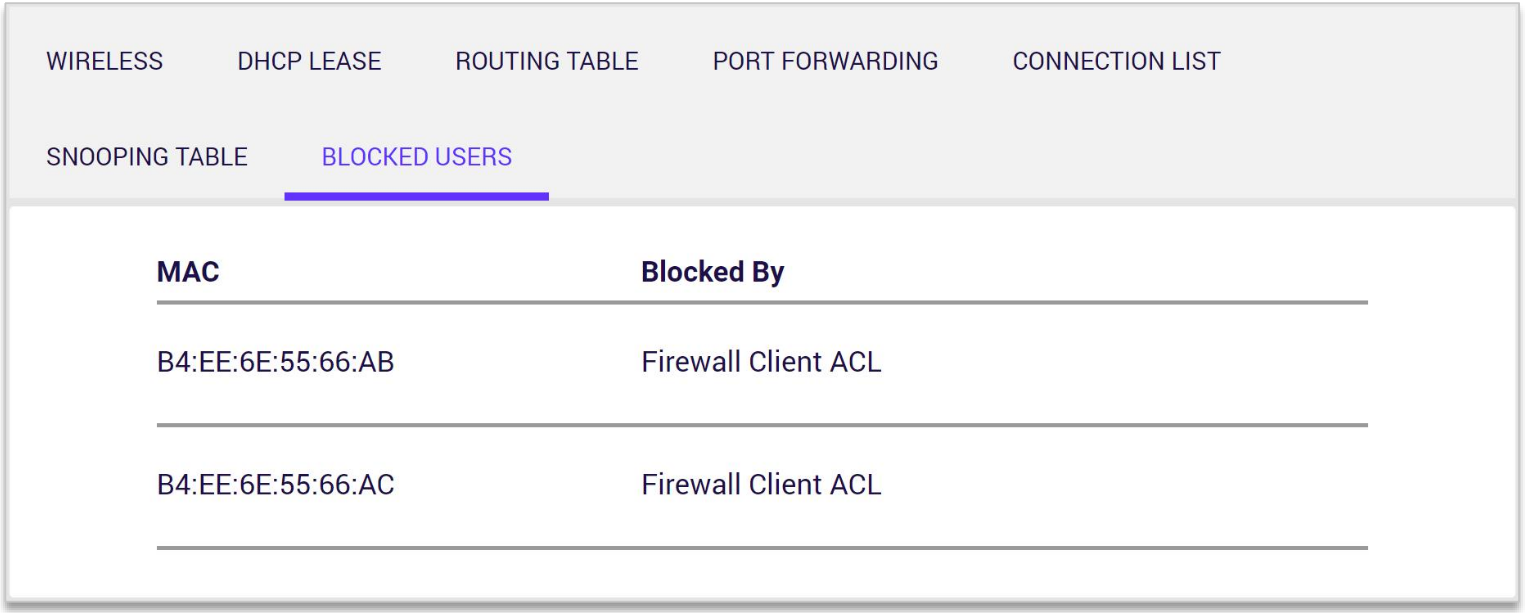
Enable Multicast (Network > Multicast) first and see the status of delivering traffic flows.



```
---------------------------Bridge Snooping Hash Table -- IPv4-------------
NUM    GROUP                                                         FDB
1      239.255.102.018                                               3c:7c:3f:t
       |--Source Mode:Block Listed Sources
       `--Num of Sources:0

IPv4 Router Ports:      None


---------------------------Bridge Snooping Hash Table -- IPv6-------------
NUM    GROUP                                                         FDB

IPv6 Router Ports:      None
```

6.8.7 Blocked Users

Displays the router’s block users.



MAC	Blocked By
B4:EE:6E:55:66:AB	Firewall Client ACL
B4:EE:6E:55:66:AC	Firewall Client ACL

7. FAQ

• What is Wi-Fi 6?

Starting in 2019, in order to simplify the name, WFA (Wi-Fi Alliance) used numbers to name the new standard, so the name Wi-Fi 6 appeared.

802.11ax (11ax), which is also known as Wi-Fi 6. 11ax features 1024-QAM which provides high-throughput in both 2.4 GHz and 5 GHz bands, and supports MU-MIMO & Orthogonal Frequency Division Multiple Access (OFDMA) to improve the channel capacity and efficiency, enabling more clients to access the AP.

• What is the difference between Wi-Fi 6 and Wi-Fi 5?

Institute of Electrical and Electronics Engineers (IEEE) wireless Wi-Fi 6 (802.11ax) standard is the successor to the IEEE Wi-Fi 5 (802.11ac) standard. Wi-Fi 6 addresses the increasing number of devices in individual networks. Wi-Fi 6 operates in the 2.4 and 5 GHz bands and features improvements in throughput, multiple-device support, and Wi-Fi spectrum efficiency.

Published Year	Wi-Fi	Wi-Fi Standard	Frequency Band
1997	1st generation	IEEE 802.11 (Wi-Fi 1)	2.4GHz
1999	2nd generation	IEEE 802.11a IEEE 802.11b (Wi-Fi 2)	5GHz 2.4GHz
2003	3rd generation	IEEE 802.11g (Wi-Fi 3)	2.4GHz
2009	4th generation	IEEE 802.11n (Wi-Fi 4)	2.4GHz or 5GHz
2013	5th generation	IEEE 802.11ac **(Wi-Fi 5)**	5GHz
2019	6th generation	IEEE 802.11ax **(Wi-Fi 6)**	2.4GHz or 5GHz

• How to reset DL-WME38 router to factory default settings?

A factory reset will restore all the settings to default status just like you firstly got the router. Make sure you have already backed up the configuration before using the process of reset to default to fix other issues. Factory reset could be done via the reset button on the back side of the router (See **3. Let‘s get started** for the location of each interface). Press and hold the button for 7 seconds. You will see the power LED starts flashing blue and then lights off in a few seconds. After that, the router will reboot automatically. You can see all the configurations become default status when the process is completed. In another way, you can also reset the router to default via Web UI and APP. Go to **System Settings > Configuration & Reset** and click the **Reset to Default** button. The router will automatically start the factory reset process.

• What if I forgot my login password?

If you forget the default login password (you haven't changed the password before), please refer to the product label which is located on the bottom of the router. Use the username, password, and url to access the web UI. But, if you changed the default password before, you will first need to reset the router to default. All settings will be lost. Then use the default password to access the web UI.

• How to update the operating system to the latest firmware version?

Launch a browser and log in to the web user interface. Navigate to **System Settings > Firmware** and see the configuration settings of **Upgrade from Internet**. Use the **Check** button to inspect the latest firmware version. An information prompt will help you to check if the router needs to be upgraded or not. Then click the **Update** button and proceed to firmware update process. This will cause the router to reboot in a few seconds. When all the loading process is completed, log in to the web user interface again. You will see the firmware version is up to date.

Note: If you have problems resolving router issues by the solution described above, please contact Dynalink's technical support via this website https://dynalink.life/.

8. Troubleshooting

If you are having problems with your router, try these basic steps in this section before looking for further solutions.

• Computer is disconnected from the router.

Your computer might have lost the connection to the router due to interference, system updates, or any number of reasons. If your computer is still not connected, try to disconnect and establish the connection to the router’s Wi-Fi again and make sure the Wi-Fi password is correct. Or use an Ethernet cable to connect to the router’s LAN port directly. Follow the steps in **4. Configure your Router** for more help.

• Can‘t connect your computer or mobile to the Wi-Fi network.

The Wi-Fi signal strength is an influential Factor that affects the connection stability between your devices and router. Try to use the following solutions to improve the Wi-Fi connection quality:

- Move your devices closer to the router to boost Wi-Fi signal. On the other side, you may avoid placing the router close to household appliances that may cause interference on your 802.11 wireless network, e.g. microwave ovens, radio transmitters, cellular transmitters, or wireless devices operate at 2.4GHz/5GHz that emit electromagnetic waves. Also, some types of barrier will weaken Wi-Fi signal, such as metal, bulletproof glass, concrete, plaster, marble, brick objects and appliances.

- When you start to use Dynalink APP, the step-by-step instruction direct you to complete router setup including establishing Wi-Fi connection between your mobile and router. For your convenience, Dynalink APP allows you to scan the QR code located at the bottom of Router to establishing Wi-Fi connection without entering password. However, if the default SSID has been modified, you will need to operate manually instead.

- Try to avoid using special characters when you configure wireless network name and password. It is suggested to use a combination of only English letters and numbers.

9. Technical Specification

- Wireless 10200Mbps: 4800 Mbps (6 GHz) + 4800 Mbps (5 GHz) + 600 Mbps (2.4 GHz)
- 4X4 MU-MIMO, OFDMA, 1024-QAM, BSS-Coloring, WPA3, IPv6
- 1 Gigabit L AN Ports + 1 Gigabit WAN Port
- Support Protocol 802.11a/g/n/ac/ax/k/v
- Antenna: 2x2 2.4G/6G dual-band antenna, 4x4 5G single-band antenna, 2x2 6G single-band antenna.
- Support 160MHz on 5GHz and 6GHz Radio
- Power, Reset to default, WPS Button
- Dimensions: W 90.8 x H 197 x D 122.8 mm
- Operating Voltage: 12V/3A DC adaptor (100V~240V, 50 Hz ~ 60 Hz)
- Maximum Power Consumption: 25.2 Watts
- Temperature: Operating: 0 °C ~ 40 °C, Storage: -40 °C ~ 85 °C
- Humidity: Operating: 5% ~ 90% RH, Storage: 5% ~ 95% RH

10. Regulatory Compliance Notices

Class B Equipment

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 or more of the following measures:

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

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.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet.

Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

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 20cm between the radiator & your body.