

User Guide

DL-WRX36

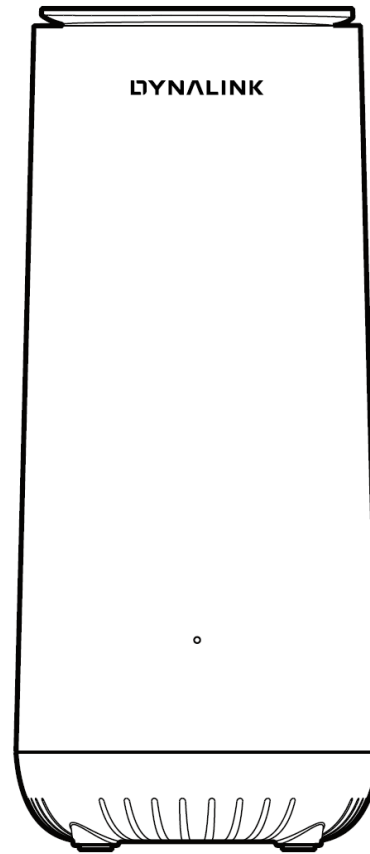


Contents

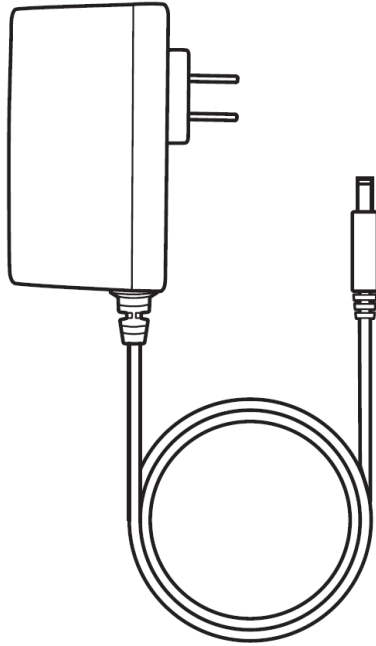
1. What's in the box	4
2. Device description	4
3. Let's get started	6
4. Configure your Router	7
4.1 How to set up your device from mobile App	7
4.2 How to set up your device from web	8
5. General Settings	9
5.1 Dashboard	10
5.2 Network	12
5.3 Parental control	50
5.4 Service	58
5.5 Security	61
5.6 QoS	75

5.7	Diagnostic	84
5.8	System Settings	85
5.9	Status	92
6.	Troubleshooting	100
7.	Tips & tricks	102
8.	Technical Specification	103

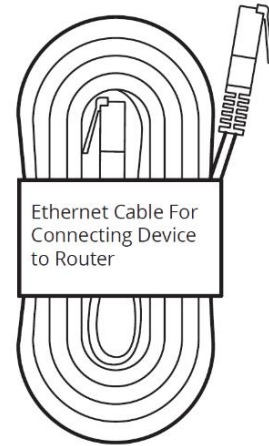
1. What's in the box



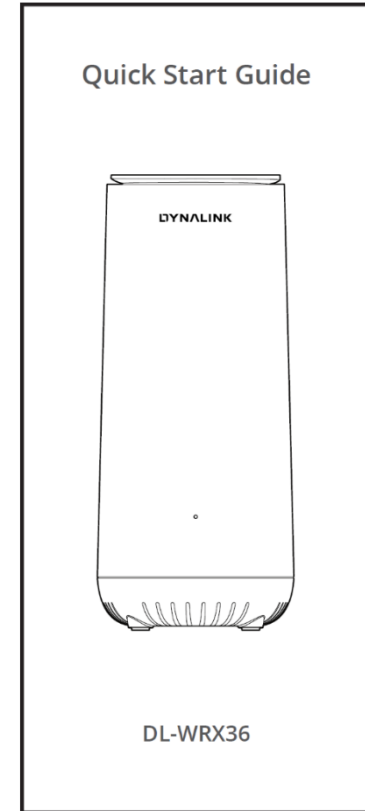
DL-WRX36



1 Power Adaptor

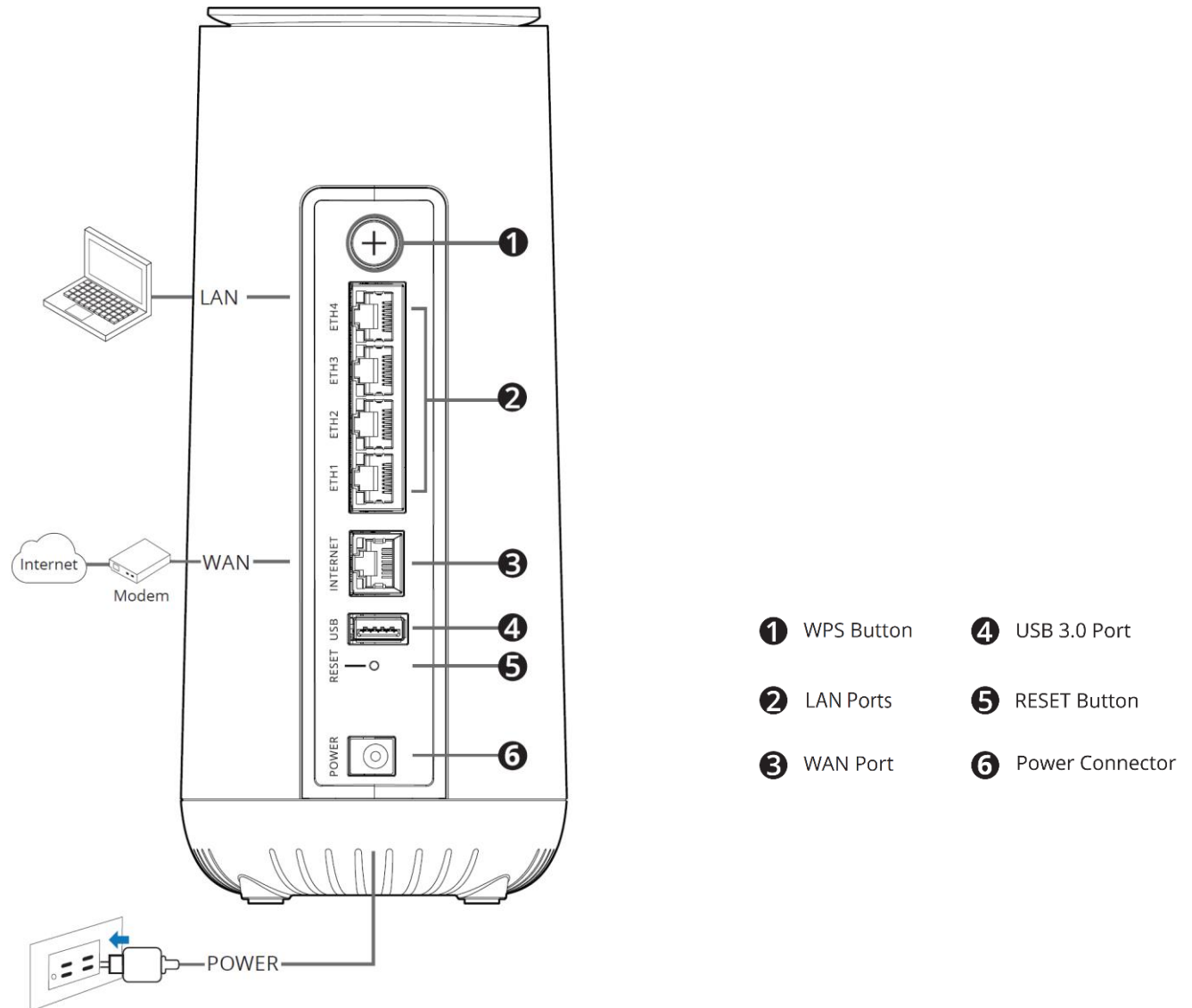


1 Ethernet cable











2. Device description

Physical interfaces



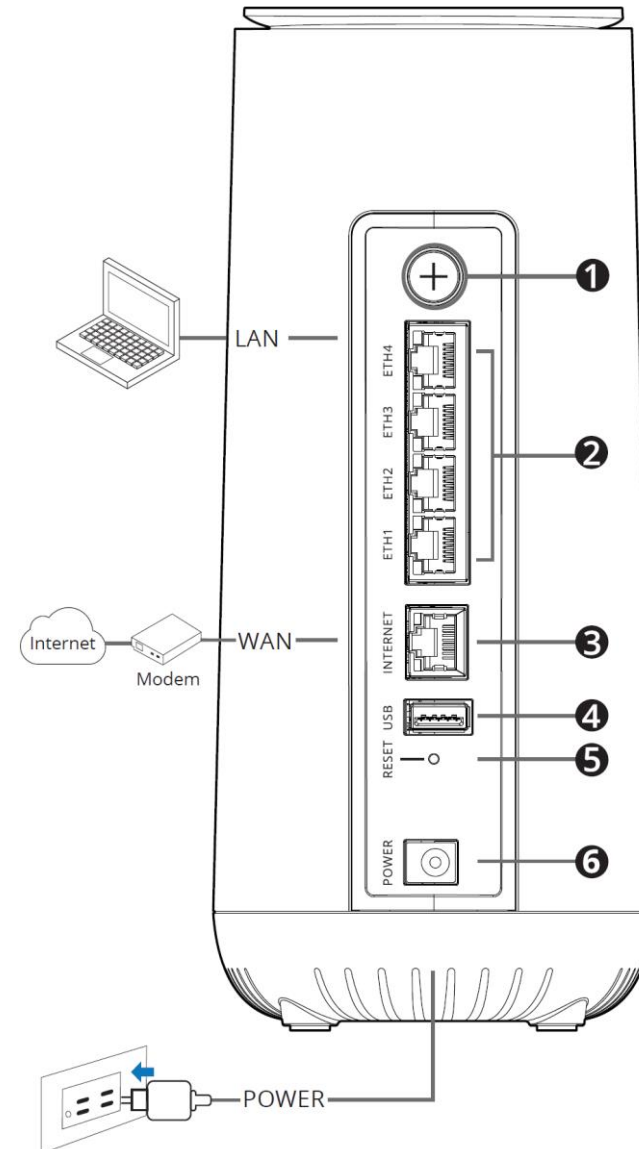
LEDs

The LEDs indicate the router's power and connection.

Function	Color status	Description
WPS	 Fast blink	Press WPS button, LED start to blink Magenta, until WPS pairing success or fail or 2 minute timeout.
	 Blue Solid on	WPS paring success, change to solid Blue.
	 Continue for 5 sec	WPS pairing failure or timeout, LED become solid Magenta for 5 seconds, then change to solid Blue.
Power on/ Reboot	 Slow blink	Power on (Booting). will show solid magenta first, then LED will continue to blink blue, and become solid blue when boot process is done successfully.
	 Red Solid	Device failure.
	 Blue Solid on	Power on Success.
Firmware Upgrade	 Fast blink	Firmware upgrade process, LED will blink blue till upgrade is done, then LED off and reboot.
Reset to Default	 Fast Blink	Press reset for 7+ seconds, LED will blink blue for 5 seconds to start reset process. Then LED off and reboot.

3. Let's get started

1. Insert the Power Adapter into the WiFi Router's Power Port and plug it into the power outlet.
2. connect your Computer or mobile device to the router via WiFi or use Ethernet cable to connect your computer to the Router's LAN port.
3. Use the provided Ethernet Cable and connect it to the WiFi Router's Internet (WAN) Port.
4. Power on.



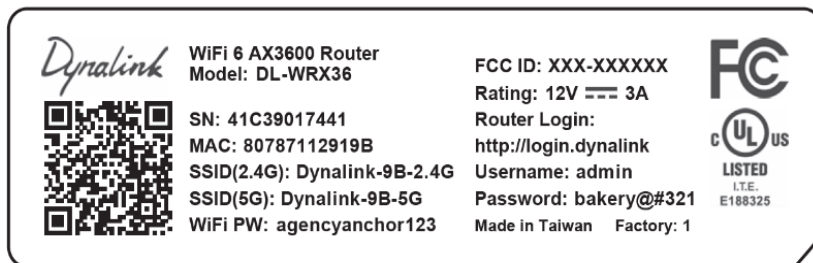
4. Configure your Router

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

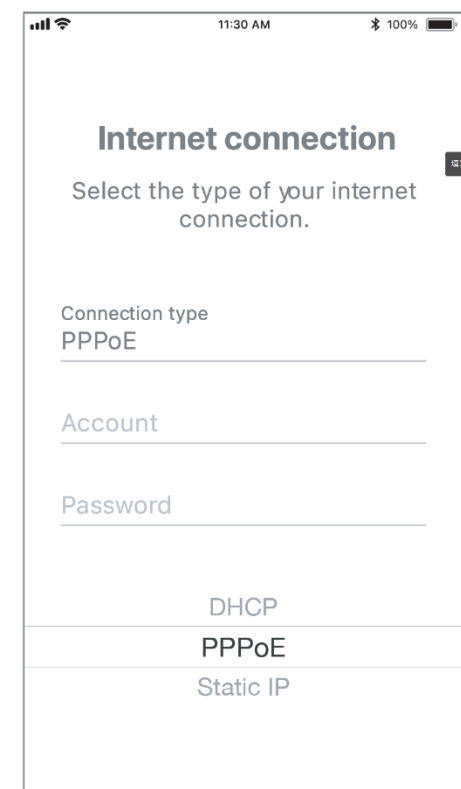
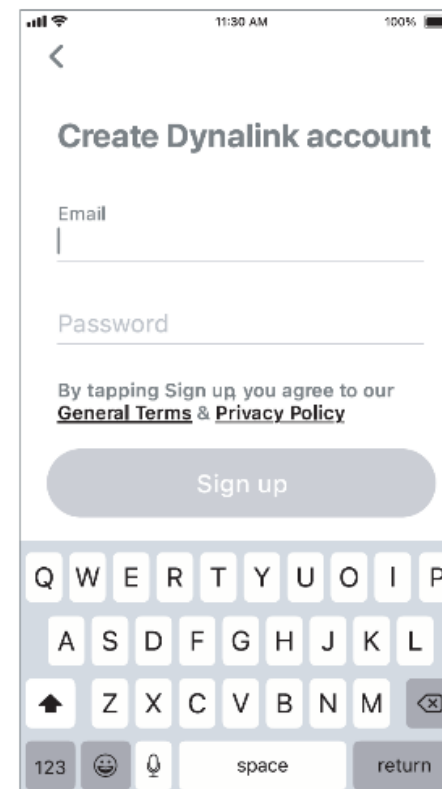
4.1 How to set up your device from mobile App



1. Install Dynalink WiFi APP from Google Play or APP store.
2. Create Dynalink account with user's email account.
3. Connect your device to router via WiFi, there are 2 ways.
 - ✓ User can enter the WIFI SSID and password on the label at bottom of device to manually connect to device
 - ✓ User can use APP to scan the QR_CODE on the label at bottom of device to connect to device.



4. Follow the APP to setup internet connection.
5. We highly recommend you to upgrade to the latest Firmware when you setup the first time to achieve maximum performance and enable more features. Please use the FOTA page on the APP to upgrade the firmware.

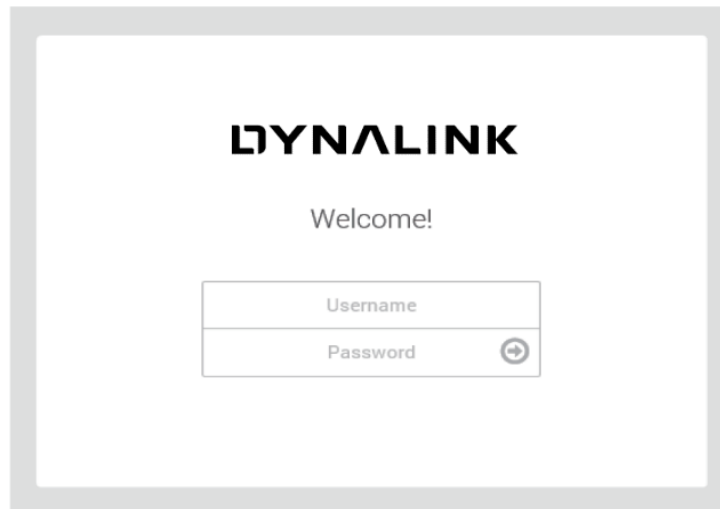


4.2 How to set up your device from web

1. On your computer, scan available Wi-Fi networks.
2. Select the Wi-Fi Network Name on the bottom of your Router.
3. Enter the unique password found on the white sticker on the bottom of your Router.
4. If preferred, you can use an Ethernet cable to connect your computer to the Router's LAN port for configuration.
5. Launch your web browser and enter the WiFi router's domain name `http://login.dynalink` in the address bar.



6. Enter the default user name (admin) and password (check admin password on the label) to login to your device's management page.

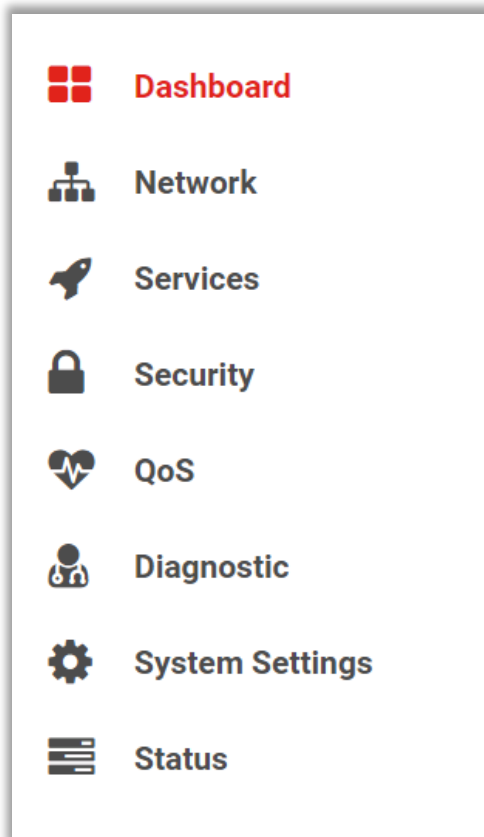


5. General Settings

Your router comes with an intuitive Web User Interface (Web UI) that allows you to easily setup its feature.

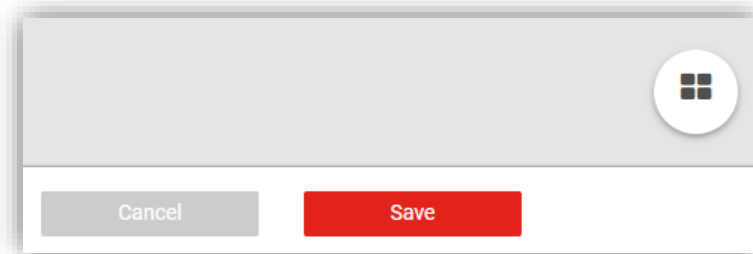
Menu

Select the **General** tab in the menu:



Save

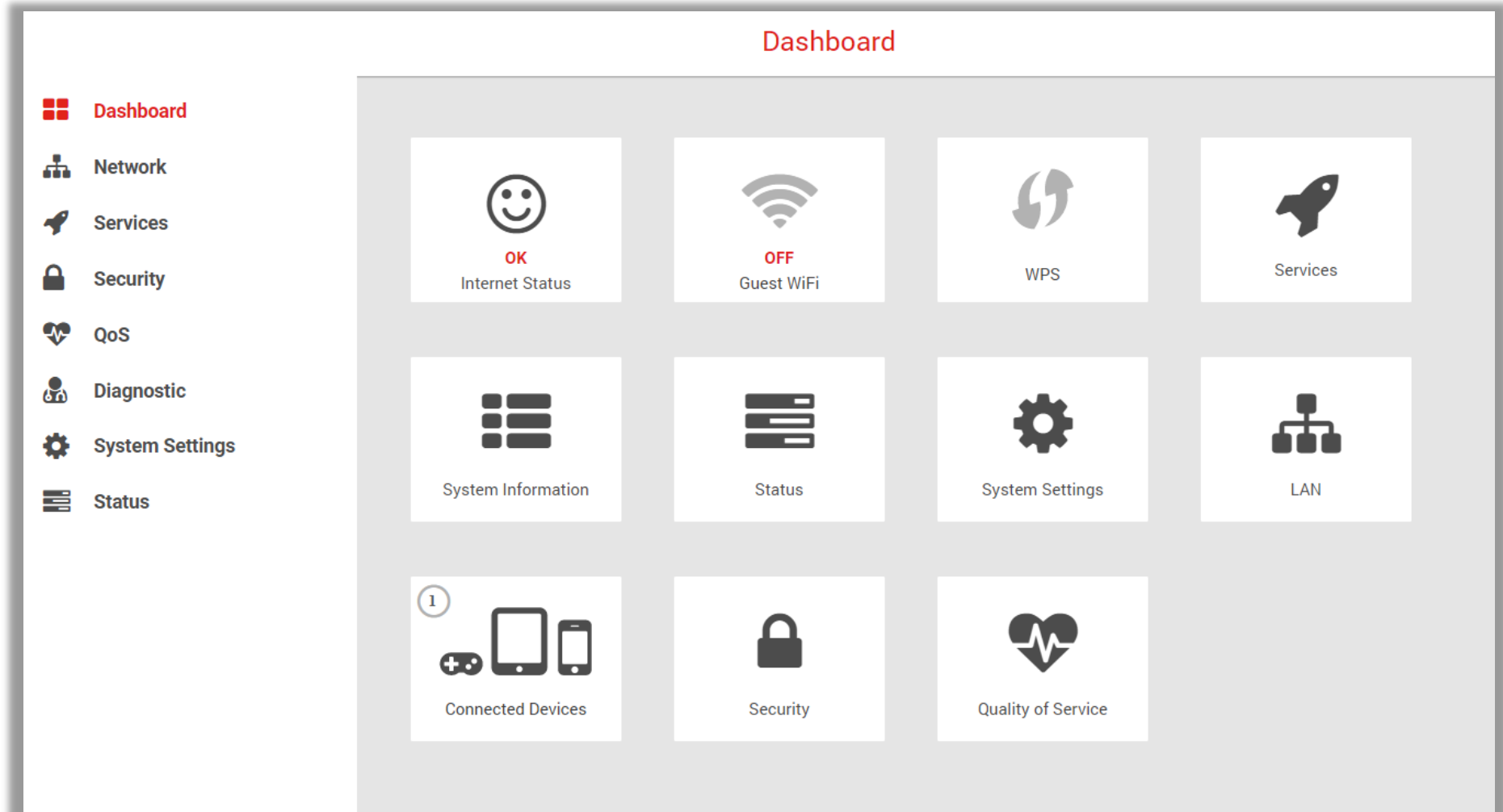
Remember to save your settings with the save button after making changes.



5.1 Dashboard

General > Dashboard

The Dashboard shows a snapshot of your network status with quick links to key features of your router.



Select any icon on the dashboard: **Internet Status, Guest Wi-Fi, WPS, Service, System Information, Status, System Settings, LAN, Connected Devices, Security, Quality of Service** to access more information and settings.

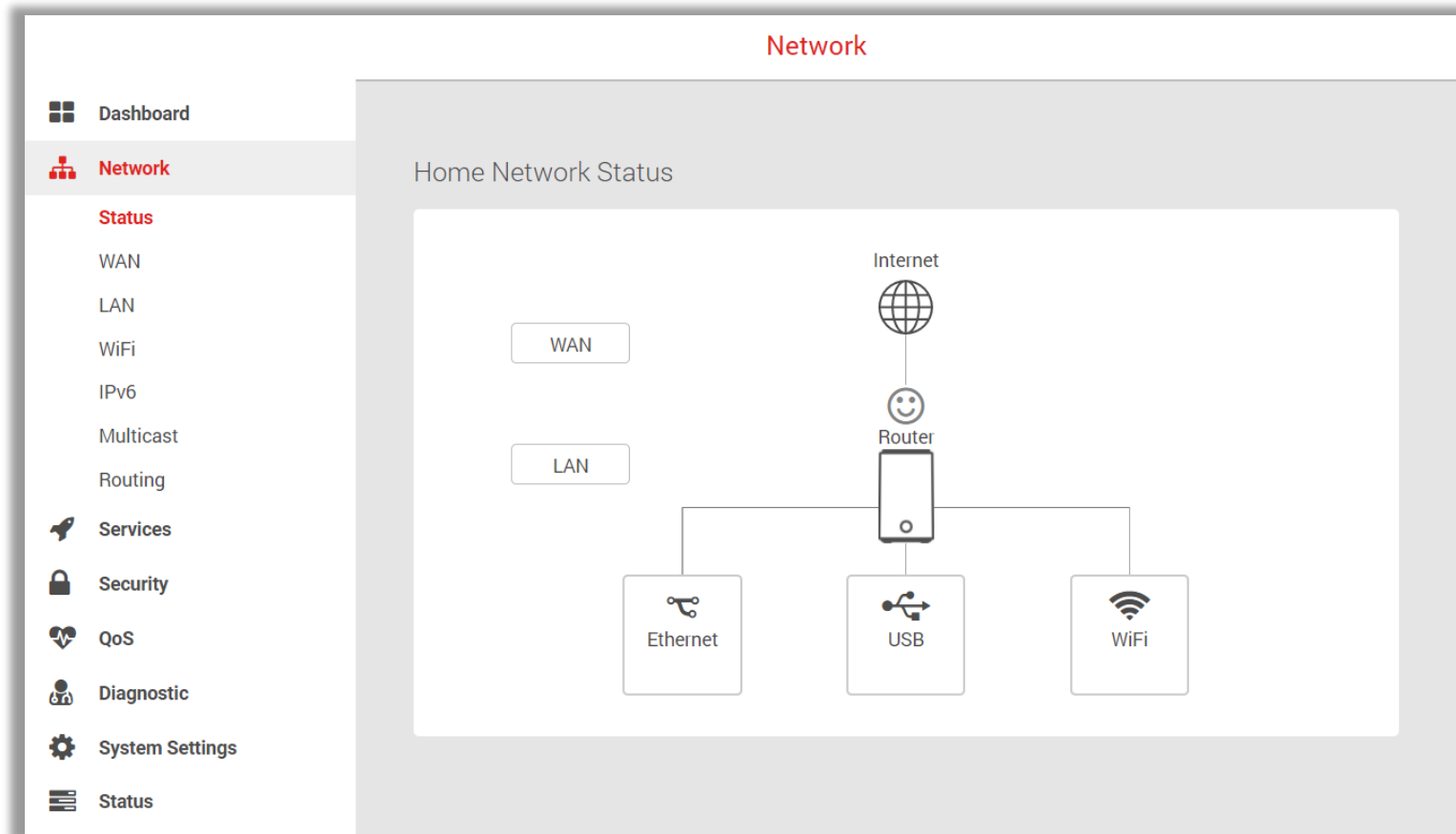
- **Internet Status** displays the connecting status between **Internet, Router, and Device**. Navigate to the corresponding setting page by clicking the WAN, LAN, STORAGE, WIFI SETTINGS icons.
- **Guest Wi-Fi** straightly configure guest Wi-Fi on/off, name, and password settings.
- **WPS** prompt out a button for you to quickly trigger WPS function.
- **Service** takes you to **General > Service > Manage Services** directly.
- **System Information** displays detailed information of router feature and status.
- **Status** takes you to **General > Status** settings directly.
- **System Settings** takes you to **General > System Settings > Manage System Settings** directly.
- **LAN** takes you to **General > Network > LAN > Manage LAN Settings** directly.
- **Connected Devices** displays Connection type, IP, MAC address, and Manufacturer of devices connecting to Router.
- **Security** prompt out Firewall IPv4 and IPv6 buttons for you to navigate to **General > Security > Manage Firewall**.
- **Quality of Service** takes you to **General > QoS > Manage QoS** directly.

5.2 Network

5.2.1 Status

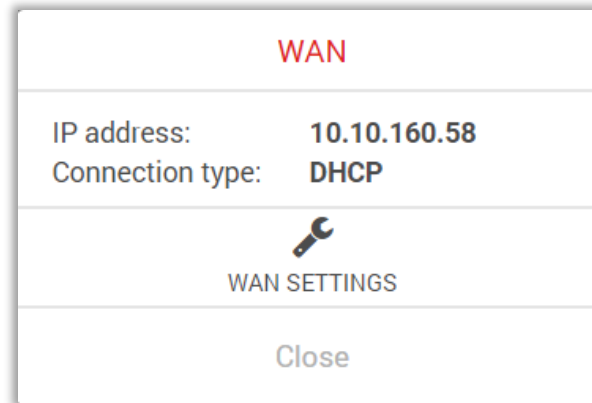
General > Network > Status

The network map provides a visual overview and status information of the network and devices on the network, with quick links to wireless security settings and client lists. It's important to check and configure security settings.

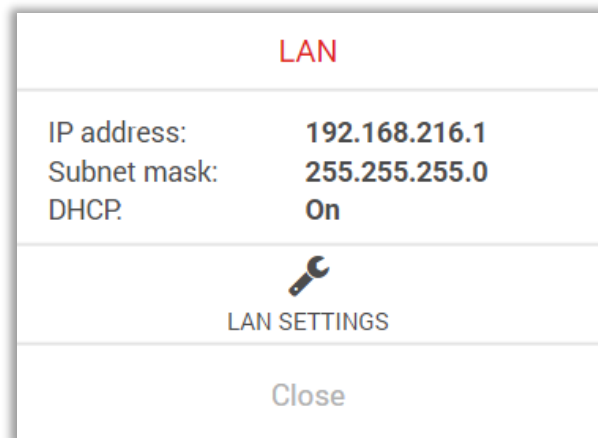


Select icons on the dashboard for more information and settings, as displayed below:

WAN displays the router's Wide Area Network (WAN).



LAN displays the router's Local Area Network (LAN) IP Address and Subnet Mask. Click LAN Settings to modify the settings.



5.2.2 WAN

General > Network > WAN

5.2.2.1 Internet

The Internet feature allows you to configure the WAN Interface Mode. You can specify a static IP address for your router, or request the address from a DHCP Server.

The screenshot shows the 'Network' configuration page for the WAN interface. The left sidebar contains a navigation menu with the following items: Dashboard, Network (selected), Status, WAN, LAN, WiFi, IPv6, Multicast, Routing, Services, Security, QoS, Diagnostic, System Settings, and Status. The main content area is titled 'Network' and 'Manage WAN Settings'. It features several tabs: INTERNET (selected), DDNS, UPNP, PORT TRIGGER, PORT FORWARD, DMZ, and NAT PASSTHROUGH. The 'INTERNET' tab is active and contains the following settings:

- Enable NAT: Yes No
- WAN Connection Type: DHCP (selected from a dropdown menu)
- MTU: 1500 (text input field)
- WAN DNS Settings (expanded section):
 - Automatic DNS server address: Yes No
 - DNS 1: 10.10.160.2 (text input field)
 - DNS 2: (empty text input field)
- Special Requirement (expanded section):
 - Host Name: (empty text input field)
 - MAC Address: (empty text input field) with a red 'MAC Clone' button to its right
 - DHCP Query Frequency: Aggressive Mode (selected from a dropdown menu)

WAN Connection Type- DHCP

INTERNET	DDNS	UPNP	PORT TRIGGER	PORT FORWARD	DMZ	NAT PASSTHROUGH
Enable NAT	<input checked="" type="radio"/> Yes	<input type="radio"/> No				
WAN Connection Type	DHCP ▼					
MTU	1500					
▼ WAN DNS Settings						
Automatic DNS server address	<input checked="" type="radio"/> Yes	<input type="radio"/> No				
DNS 1	10.10.160.2					
DNS 2						
▼ Special Requirement						
Host Name	<input type="text"/>					
MAC Address	<input type="text"/>	<input type="button" value="MAC Clone"/>				
DHCP Query Frequency	Agressive Mode ▼					

Basic	
Enable NAT	NAT (Network Address Translation) is a process used in routers to map local devices with private IP address to router IP address and port combination when sending the packet outside.
WAN Connection Type	The connection type of broadband.
Automatic MTU	Use default MTU value.
MTU	MTU (Maximum Transmission Unit) is the Maximum packet size(in bytes) to be transmitted out of the device
WAN DNS Settings	
Automatic DNS Server Address	Allows this router to get the DNS IP address from the ISP automatically.
DNS1	Manually assign a Domain Name Server address.
DNS2	Manually assign a second Domain Name Server address.
Special Requirement	
Host Name	Enter a host name for your router.
MAC	MAC (Media Access Control) address is a unique identifier that identifies your device in the network.
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 to avoid the problem.

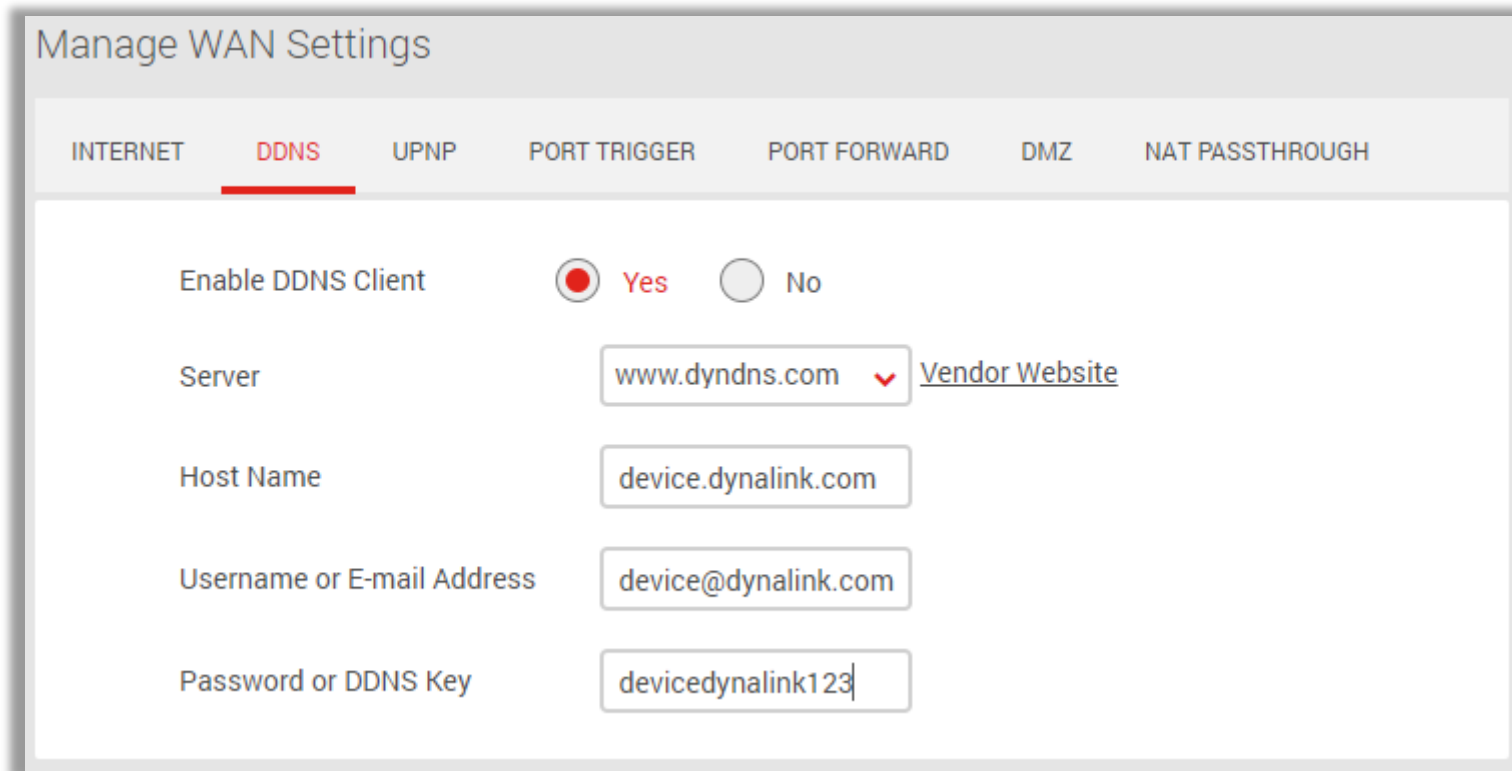
WAN Connection Type- Static IP

INTERNET	DDNS	UPNP	PORT TRIGGER	PORT FORWARD	DMZ	NAT PASSTHROUGH
Enable NAT	<input checked="" type="radio"/> Yes	<input type="radio"/> No				
WAN Connection Type	Static IP <input type="button" value="v"/>					
MTU	1500					
<input type="button" value="v"/>	WAN IP Settings					
IP Address	10.10.160.33					
Subnet Mask	255.255.255.0					
Default Gateway	10.10.160.1					
<input type="button" value="v"/>	WAN DNS Settings					
DNS 1	10.10.160.2					
DNS 2	10.10.160.3					
<input type="button" value="v"/>	Special Requirement					
MAC Address	<input type="text"/>	<input type="button" value="MAC Clone"/>				

Basic	
Enable NAT	NAT (Network Address Translation) is a process used in routers to replace the address information of network packets with new address information.
WAN Connection Type	The connection type broadband WAN get access internet.
MTU	MTU (Maximum Transmission Unit) is the single largest frame or packet of data that can be transmitted across a network.
WAN IP Settings	
IP Address	Enter WAN static IPv4 address provided by ISP.
Subnet Mask	Enter correct subnet mask.
Default Router	Enter default router provided by ISP.
WAN DNS Settings	
DNS1	Enter a Domain Name Server address.
DNS2	Enter a second Domain Name Server address.
Special Requirement	
MAC	MAC (Media Access Control) address is a unique identifier that identifies your computer or device in the network.

General > Network > WAN**5.2.2.2 DDNS**

Dynamic DNS (DDNS) feature allows you to access your router through a domain name at any time, no matter what the device's WAN public IP is.



The screenshot shows the 'Manage WAN Settings' interface with the 'DDNS' tab selected. The settings are as follows:

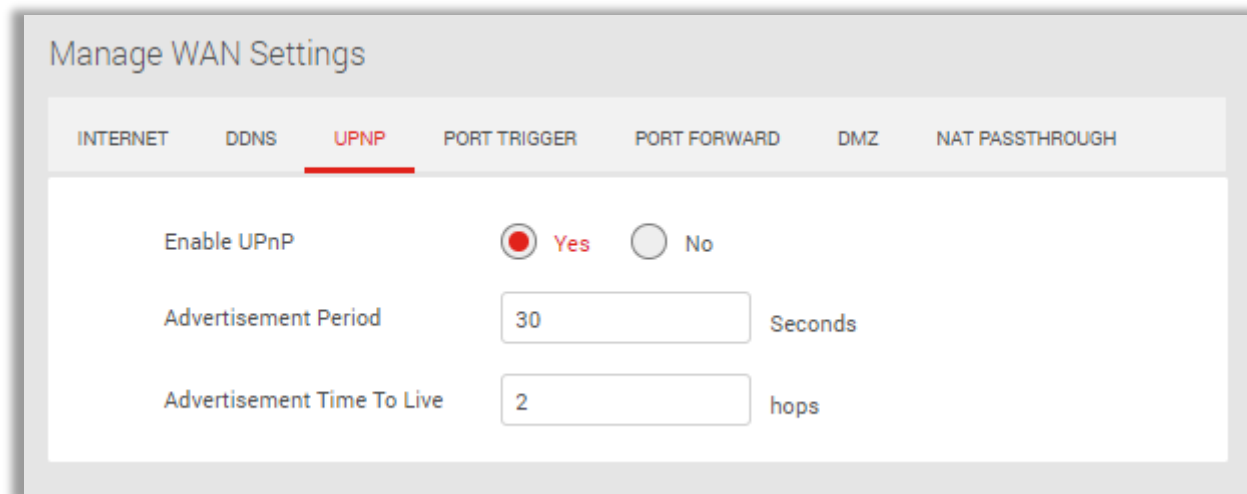
Setting	Value
Enable DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	www.dyndns.com Vendor Website
Host Name	device.dynalink.com
Username or E-mail Address	device@dynalink.com
Password or DDNS Key	devicedynalink123

DDNS	
Enable/Disable DDNS Client	Toggle the switch to enable or disable DDNS Client.
Server	Select a DDNS Server.
Host Name	Enter a domain name you applied for the device from domain name management agency.
Username or E-Mail Address	Enter your username registered on the DDNS server.
Password or DDNS Key	Enter your password registered on the DDNS server.

General > Network > WAN**5.2.2.3 UPNP**

Universal plug-and-play (UPnP) is a set of networking protocols which enables network devices to communicate and automatically establish working configurations with each other, such as computers, printers, mobile devices etc.

It's typically used for data sharing, communications and entertainment purposes, although sometimes not preferred due to security concerns. Some devices may require UPnP to be enabled to function properly. Use the switch to set UPnP to active or inactive, according to your requirements.



The screenshot shows the 'Manage WAN Settings' interface. At the top, there are several tabs: INTERNET, DDNS, UPNP (which is selected and underlined in red), PORT TRIGGER, PORT FORWARD, DMZ, and NAT PASSTHROUGH. Below the tabs, the 'UPnP' configuration is shown. It includes a radio button for 'Enable UPnP' which is currently set to 'Yes'. Below this, there are two input fields: 'Advertisement Period' set to '30' with the unit 'Seconds', and 'Advertisement Time To Live' set to '2' with the unit 'hops'.

General > Network > WAN**5.2.2.4 Port trigger**

Port trigger allows the router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the router, so that when the requested data returns through the router, the data is routed back to the proper device.

Manage WAN Settings

INTERNET DDNS UPNP **PORT TRIGGER** PORT FORWARD DMZ NAT PASSTHROUGH

Port Triggering Yes No

Port Triggering List (Maximum: 32)

Description	Trigger Port	Local IP	Protocol	Incoming Port	Protocol	Operation
Port Trigger	65534	192.168.1.118	TCP	65535	TCP	

Add Rule

1. Click **Add Rule** and enter the parameters to set up a port trigger rule.
2. Click **Add** to add the rule to port trigger list and click **Save** to save your port trigger rules. You can remove or edit any port trigger rule using the icons.

Port Triggering List ✕

Well-Known Applications	<input type="text" value="Please Select"/>
Description	<input type="text" value="Quicktime 4 Client"/>
Trigger Port	<input type="text" value="554"/>
Local IP List	<input type="text" value="Select"/>
Local IP	<input type="text"/>
Protocol	<input type="text" value="TCP"/>
Incoming Port	<input type="text" value="6970:32000"/>
Protocol	<input type="text" value="UDP"/>

Cancel
Apply

Well-known Applications	Select pre-defined application rules.
Description	Description of the rule.
Trigger port	Enter the trigger port.
Local IP list	Select the IP address of the computer on your local network.
Local IP	Enter the IP address of the computer on your local network.
Protocol	Selected trigger protocol.
Incoming port	Enter the open port.
Protocol	Select open protocol.

General > Network > WAN

5.2.2.5 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.

The screenshot displays the 'Network' configuration page in the router's web interface. The 'Expert' mode is selected. The 'Network' menu is active, and the 'PORT FORWARD' tab is selected under 'Manage WAN Settings'. The 'Port Forwarding List (Maximum: 32)' is shown with the following entries:

Services	Port Range	Local IP/Port	Protocol	Status	Operation
DNS Server	53	192.168.1.118/53	UDP	ON	
SMTP Server	25	192.168.1.118/25	TCP	ON	

An 'Add Rule' button is visible at the bottom of the list.

1. Click **Add Rule** and enter the parameters to set up a port forwarding rule.
2. Click **Add** to add the rule to port forward list and click **Save** to save your port forward rules. You can remove or edit any port forward rule using the icons.

Port Forwarding Setting ✕

Well Known Server List

Please Select ▼

Well Known Game List

Please Select ▼

Services

DNS Server

Port Range

53

Local IP List

Select ▼

Local IP

192.168.12.214

Local Port

53

Protocol

UDP ▼

Status

ON ▼

Cancel

Apply

Services	Specify the service type e.g. HTTP, POP3 etc.
Port Range	Enter external port or external port start: external port end.
Local IP List	Select the IP address of the computer on your local network.
Local IP	Enter the IP address of the computer on your local network.
Local Port	Specify the internal/private port you wish to use on the computer in your local network.
Protocol	Select the connection protocol: TCP, UDP or Both.
Status	Enable or disable the rule.

General > Network > WAN

5.2.2.6 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.

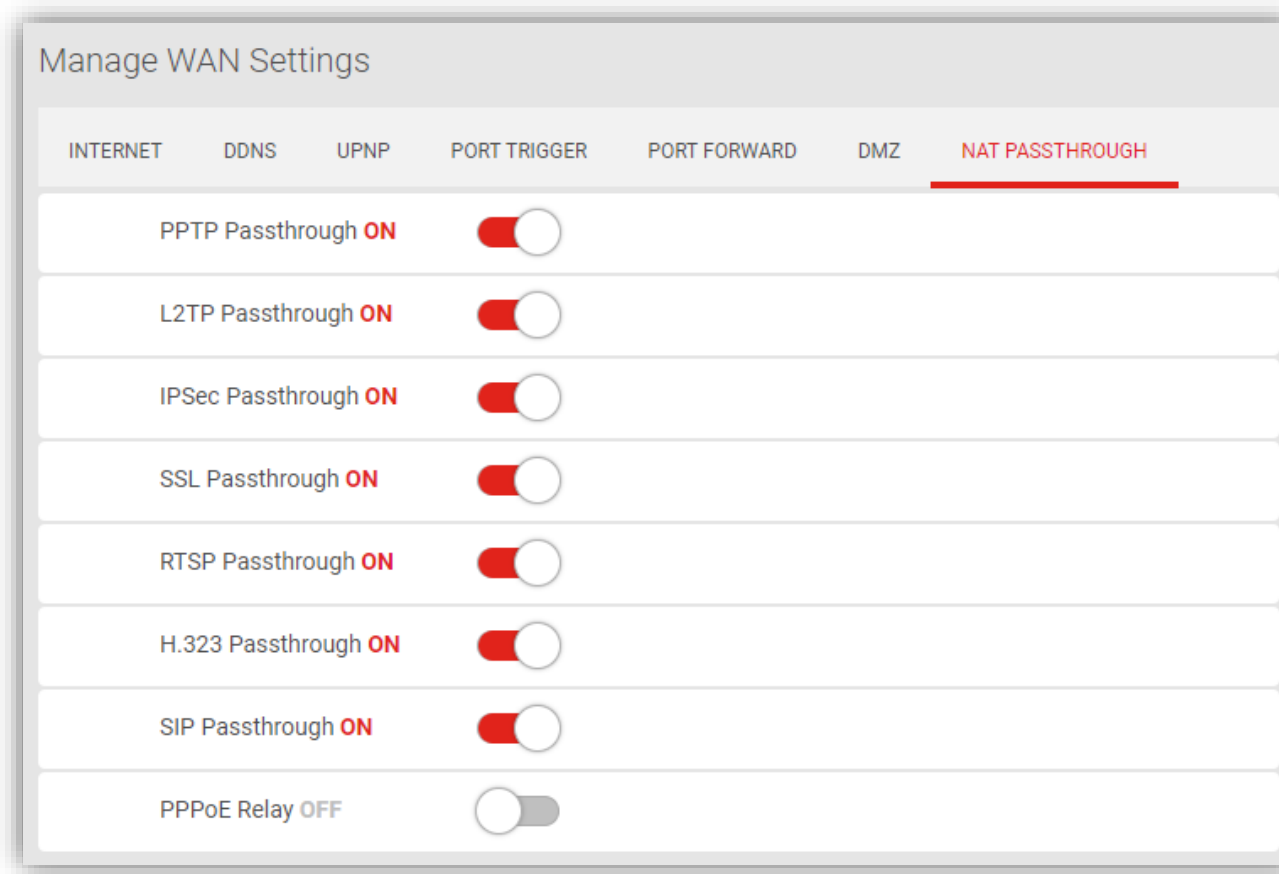
The screenshot shows the 'Manage WAN Settings' interface with the 'DMZ' tab selected. A warning message states: 'IPv6 feature is not enabled. So now the IPv6 DMZ can not be enabled.' The configuration options are as follows:

- Enable IPv4 DMZ:** Radio buttons for 'Yes' (selected) and 'No'.
- IP Address of Exposed Station:** Text input field containing '192.168.12.214'.
- Enable IPv6 DMZ:** Radio buttons for 'Yes' and 'No' (selected).

Enable IPv4 DMZ	Enable or disable DMZ function.
IP Address of Exposed Station	DMZ Host.

General > Network > WAN**5.2.2.7 NAT Passthrough**

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



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 establishing encrypted links between a web server and a browser in an online communication.
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.

5.2.3 LAN

General > Network > LAN

5.2.3.1 IP SETTINGS

Configure/Change IP Address for Private or Guest Network: This page allows you to configure your router on your LAN.

Manage LAN Settings

IP SETTINGS
DHCP SERVER
DEVICE LIST
WAKE ON LAN

Network	<input style="width: 90%;" type="text" value="Private Network"/>
IP Address	<input style="width: 90%;" type="text" value="192.168.216.1"/>
Subnet Mask	<input style="width: 90%;" type="text" value="255.255.255.0"/>

IP Settings	
IP Address	Specify the IP address here.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0

General > Network > LAN**5.2.3.2 DHCP server**

This page allows you to configure your router as a DHCP server to assign IP addresses to other devices on your LAN.

Manage LAN Settings

IP SETTINGS **DHCP SERVER** DEVICE LIST WAKE ON LAN

Network	<input type="text" value="Private Network"/>
Enable DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
Domain Name	<input type="text" value="Askey.com"/>
DHCP address range	<input type="text" value="192.168.216.2"/> - <input type="text" value="192.168.216.254"/>
Lease Time	<input type="text" value="86400"/> Seconds
Default Gateway	<input type="text" value="192.168.216.1"/>

▼ DNS and WINS Server

DNS Server	<input type="text" value="192.168.216.1"/>
WINS Server	<input type="text"/>

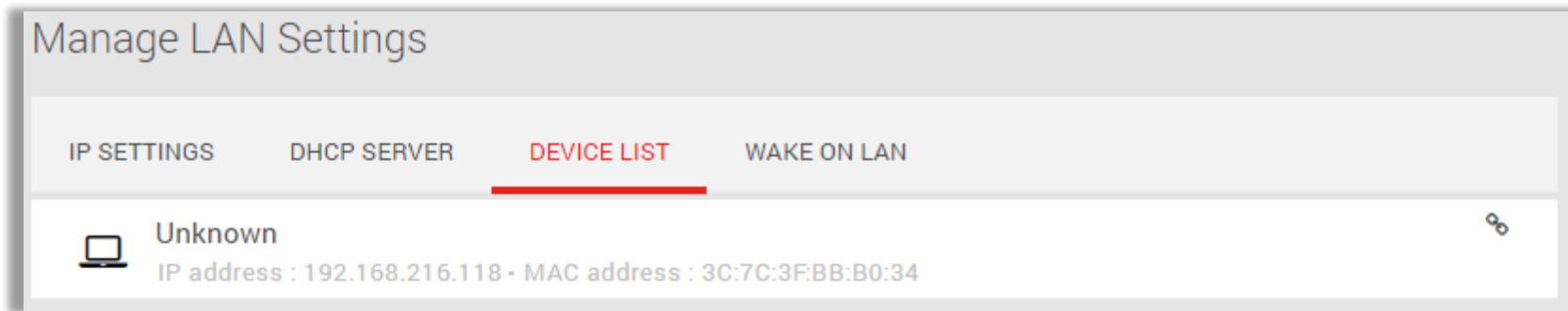
▼ Static IP Assignment within DHCP IP Pool (Maximum : 64)

Enable Manual	<input type="radio"/> Yes <input checked="" type="radio"/> No
---------------	---

DHCP SERVER	
DHCP Server	Dynamic Host Configuration Protocol Server. Server that assign IP to clients.
Network	Select one of the networks as DHCP server network
Enable/Disable DHCP Server	Toggle the switch to enable or disable DHCP server.
DHCP Address Range	Enter the start and end IP address of the IP address range which your router's DHCP server will assign to devices on the network.
Lease Time	Enter an address lease time in seconds. IP addresses will be assigned for this period of time before being reassigned.
DNS Server	Enter a Domain Name Server address.
WINS Server	Enter a Windows Internet Name Service address.
Enable Manual	Toggle the switch to enable or disable Static IP Assignment

General > Network > LAN**5.2.3.3 Device list**

This page displays all devices (clients) connected to your router, by Ethernet (LAN) or Wi-Fi (wireless) e.g. laptops, smartphones. The device name, MAC address and IP address is listed for each device.



General > Network > LAN**5.2.3.4 Wake on LAN**

To startup the devices (clients) connected to your router remotely. Add a name/MAC of device which you want to be controlled and **Save**. Then select the MAC address to trigger Wake up function. Use Edit and Delete to modify the device list.

Manage LAN Settings

IP SETTINGS DHCP SERVER DEVICE LIST **WAKE ON LAN**

Target [Wake Up](#)

Device Name	MAC Address	Edit / Delete
809097-P2	3C:7C:3F:BB:B0:34	✎ -

[+](#)
Add Rule

5.2.3 WiFi

General > Network > WiFi

5.2.3.1 Basic

The **Wi-Fi** screen displays basic settings for your router's Wi-Fi. Your router is dual-band and uses two Wi-Fi frequencies (2.4GHz & 5GHz) for better wireless performance on your devices. You can edit advanced settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.

The screenshot displays the router's web interface for the Network > WiFi settings. The left sidebar contains a navigation menu with the following items: Dashboard, Network (highlighted), Status, WAN, LAN, WiFi, IPv6, Multicast, Routing, Services, Security, QoS, Diagnostic, System Settings, and Status. The main content area is titled "Network" and "Manage WiFi Settings". It features several tabs: BASIC (selected), WPS, ACL, RADIO, ADVANCED, and BAND STEERING. The settings are as follows:

Setting	Value
Frequency	2.4 GHz
Network	Private Network
WiFi Network	ON
WiFi Network Name (SSID)	Askey-099AD
Broadcast SSID	ON
Security Setting	WPA2 Personal
WPA Encryption	AES
WiFi Password <input type="checkbox"/> Show Password

2.4 / 5 GHz Wi-Fi Settings	
Wi-Fi is active/inactive	Enable or disable this Wi-Fi band.
Wireless Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as "SSID". The SSID can consist of any combination of up to 32 alphanumeric characters.
Wireless Password	Enter your Wi-Fi password. A complex, hard-to-guess key is recommended. The Wi-Fi password must be 8 characters or longer.
Security	Select a Wi-Fi security type from the drop-down menu. WPA2 personal is the default setting and the most secure. Security can be disabled by selecting None but this is not recommended.
Version	Select which version of security type to use. WPA2 is the most secure but not supported by all wireless clients. Selecting Mixed WPA/WPA2, WPA2/WPA3 ensures wireless client compatibility.
Encryption	Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is default for Mixed WPA/WPA2.

General > Network > WiFi

5.2.4.2 WPS

Press **WPS** button, you can quickly and securely establish wireless connections without configuring tedious parameters.

1. With WPS Enabled, PC or smart phone can connect router without input Wi-Fi password.
2. If the PC or smart phone has a WPS button, press the button and then select push button, start it in web UI.
3. If the PC or smart phone has a PIN code, type the number into the router PIN box, then start it.
4. PC or smart phone type the AP PIN code and start it.

The screenshot shows the 'Manage WiFi Settings' web interface with the 'WPS' tab selected. The interface includes a navigation bar with tabs for BASIC, WPS, ACL, RADIO, ADVANCED, and BAND STEERING. A red warning icon and text state: 'Note: ACL will only take effect when WPS is disabled.' The main configuration area contains the following settings:

Frequency	2.4 GHz
Enable WPS : ON	<input checked="" type="checkbox"/>
Connection Status	WPS-ENROLLEE-SEEN
Configured	Yes
AP PIN Code	20694739
WPS Method	<input checked="" type="radio"/> Push Button <input type="radio"/> Client PIN Code
PIN Code	<input type="text"/>

A red 'Start' button is located at the bottom of the configuration area.

General > Network > WiFi**5.2.4.3 ACL**



Access control list can allow or deny devices with one or more specified MAC addresses to connect to the wireless network.

1. Enable ACL, select frequency and network.
2. Select MAC Filter Mode to Accept/Reject.
3. Add a rule, type a MAC address.
4. PC or smart phone with matched MAC address can or deny access to wireless network.

The screenshot shows the 'Manage WiFi Settings' interface with the 'ACL' tab selected. The settings are as follows:

- Frequency: 2.4 GHz
- Network: Private Network
- WiFi Network Name (SSID): Askey-099AD
- Enable MAC Filter: Yes (selected)
- MAC Filter Mode: Accept

Below these settings is a section titled 'MAC Filter List (Maximum: 64)'. It contains a table with one entry:

MAC Filter List	Edit / Delete
AA:AA:AA:AA:AA:AA	 

At the bottom of the page, there is a button labeled 'Add Rule' with a plus sign icon.

General > Network > WiFi**5.2.4.4 Radio**

The Wi-Fi screen displays radio settings for your router's Wi-Fi. You can edit radio settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.

The screenshot shows the 'Manage WiFi Settings' interface with the 'RADIO' tab selected. The settings are as follows:

Setting	Value
Frequency	2.4 GHz
Schedule	
Wireless Scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No
Setting	
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	ax/n/g
Channel Bandwidth	20/40 MHz
Control Channel	Auto
Current Channel : 6	
Tx Power Adjustment	100%

2.4 / 5 GHz Channel Settings	
Mode	2.4GHz: Select the wireless mode used for the router's Wi-Fi. Include g, g/n, n, ax/n/g/b . 5GHz: Select the wireless mode used for the router's Wi-Fi. Include a, n/a, ac, ac/n/a, ax/ac/n/a .
Channel	Select a wireless radio channel or use the default "Auto" setting from the drop-down menu. Changing radio channel can improve Wi-Fi signal depending on how crowded the channel is with other radio signals and interference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (better performance but likely more interference), or Auto (automatically select based on interference level).

General > Network > WiFi

5.2.4.5 Advanced

The Wi-Fi screen displays advanced settings for your router's Wi-Fi. You can edit radio settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.

The screenshot shows the 'Manage WiFi Settings' interface with the 'ADVANCED' tab selected. The settings are as follows:

- Frequency:** 2.4 GHz (dropdown menu)
- Setting:** (expanded dropdown menu)
- Network:** Private Network (dropdown menu)
- WiFi Network Name (SSID):** Askey-099AD
- Set AP Isolated:** Radio buttons for 'Yes' (unselected) and 'No' (selected).

2.4 / 5 GHz Advanced Settings	
AP Isolated	After it is enabled, all connected computers cannot be accessed by each other, and play a role of isolation to protect data security between different users.
TX STBC	Transmit rate.
RX STBC	Receive rate.
DTIM	DTIM indicates for how many beacon interval that the AP will cache the package for the Station (for example, when the Station is sleeping).
Fragmentation Threshold	The threshold of the packet size. When the data packet size exceeds this threshold, the 802.11 protocol will automatically split the data packet.

General > Network > WiFi**5.2.4.6 Band Steering**

Band Steering is a feature that encourages dual-band capable wireless clients to connect to the faster 5GHz Wi-Fi, and leave the 2.4GHz Wi-Fi less-crowded for those clients who support 2.4GHz only; therefore, to improve Wi-Fi performance for all the clients.

Manage WiFi Settings

BASIC WPS ACL RADIO ADVANCED **BAND STEERING**

⚠ Enable Band steering will sync all radio wifi settings same with the setting in this page.

Band Steering **ON**

▼ Sync Wifi Setting

WiFi Network Name (SSID)	<input type="text" value="Askey-099AD"/>
Security Setting	<input type="text" value="WPA2 Personal"/>
WPA Encryption	<input type="text" value="AES"/>
WiFi Password	<input type="text" value="12345678"/>

5.2.5 IPv6

General > Network > IPv6

5.2.5.1 IPv6 SETTINGS

The device supports Ipv6 function only when WAN Interface Mode is configured as WAN. You can go to General > Network > WAN to change it.

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.

Manage IPv6 Settings

IPv6 SETTINGS
IPv6 INFORMATION

Connection Type	Native
IPv6 WAN Setting	
Auto Configuration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
IPv6 LAN Setting	
Enable LAN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
LAN IPv6 Address	2001:d630:160c:5:8278:71ff:fe31:1ae
LAN Prefix Length	64
LAN IPv6 Prefix	2001:d630:160c:5::
Enable Pool Setting For Lan Host	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DHCP Pool Start	<input type="text" value="2001:d630:160c:5"/> <input type="text" value="::"/> <input type="text" value="1"/>
DHCP Pool End	<input type="text" value="2001:d630:160c:5"/> <input type="text" value="::"/> <input type="text" value="1000"/>
LAN IPv6 MTU	<input type="text" value="1500"/>
IPv6 DNS Setting	
Connect to DNS Server Automatically	<input checked="" type="radio"/> Yes <input type="radio"/> NO

IPv6 Settings	
Connection Type	Native.
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 Global 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	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.

The screenshot shows the 'Network' configuration page for a DL-WRX36 router. The left sidebar contains a navigation menu with the following items: Dashboard, Network (highlighted), Status, WAN, LAN, WiFi, IPv6, Multicast, Routing, Services, Security, QoS, Diagnostic, System Settings, and Status. The main content area is titled 'Network' and 'Manage IPv6 Settings'. It features two tabs: 'IPv6 SETTINGS' (active) and 'IPv6 INFORMATION'. The settings are organized into sections: 'IPv6 WAN Setting' with a 'Connection Type' dropdown set to 'Native'; 'IPv6 LAN Setting' with 'Auto Configuration' set to 'Disable', 'Enable LAN' set to 'Enable', 'LAN IPv6 Address' set to '2001:d630:160c:5:8278:71ff:fe31:1ae', 'LAN Prefix Length' set to '64', 'LAN IPv6 Prefix' set to '2001:d630:160c:5::', 'Enable Pool Setting For Lan Host' set to 'Enable', 'DHCP Pool Start' set to '2001:d630:160c:5 :: 1', 'DHCP Pool End' set to '2001:d630:160c:5 :: 1000', and 'LAN IPv6 MTU' set to '1500'; and 'IPv6 DNS Setting' with 'Connect to DNS Server Automatically' set to 'Yes'.

Network

Manage IPv6 Settings

IPv6 SETTINGS IPv6 INFORMATION

Connection Type Native

IPv6 WAN Setting

Auto Configuration Enable Disable

IPv6 LAN Setting

Enable LAN Enable Disable

LAN IPv6 Address 2001:d630:160c:5:8278:71ff:fe31:1ae

LAN Prefix Length 64

LAN IPv6 Prefix 2001:d630:160c:5::

Enable Pool Setting For Lan Host Enable Disable

DHCP Pool Start 2001:d630:160c:5 :: 1

DHCP Pool End 2001:d630:160c:5 :: 1000

LAN IPv6 MTU 1500

IPv6 DNS Setting

Connect to DNS Server Automatically Yes NO

IPv6 Settings	
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 Global 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 Global 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.

General > Network > IPv6**5.2.5.1 IPv6 Information**

The IPv6 status displayed as below:

Manage IPv6 Settings

IPv6 SETTINGS **IPv6 INFORMATION**

IPv6 Network Information

```
IPv6 Connection Type: Native-Simultaneous
WAN IPv6 Address: 2001:d630:160::d2
WAN IPv6 Gateway: fe80::d296:fbff:fe8d:2fa7
LAN IPv6 Address: 2001:d630:160c:5:8278:71ff:fe31:1ae/64
LAN IPv6 Link-Local Address: fe80::8278:71ff:fe31:01ae
DHCP-PD: Enabled
LAN IPv6 Prefix: 2001:d630:160c:5::/64
DNS Address: 2001:d630:160::2
```

IPv6 LAN Devices List

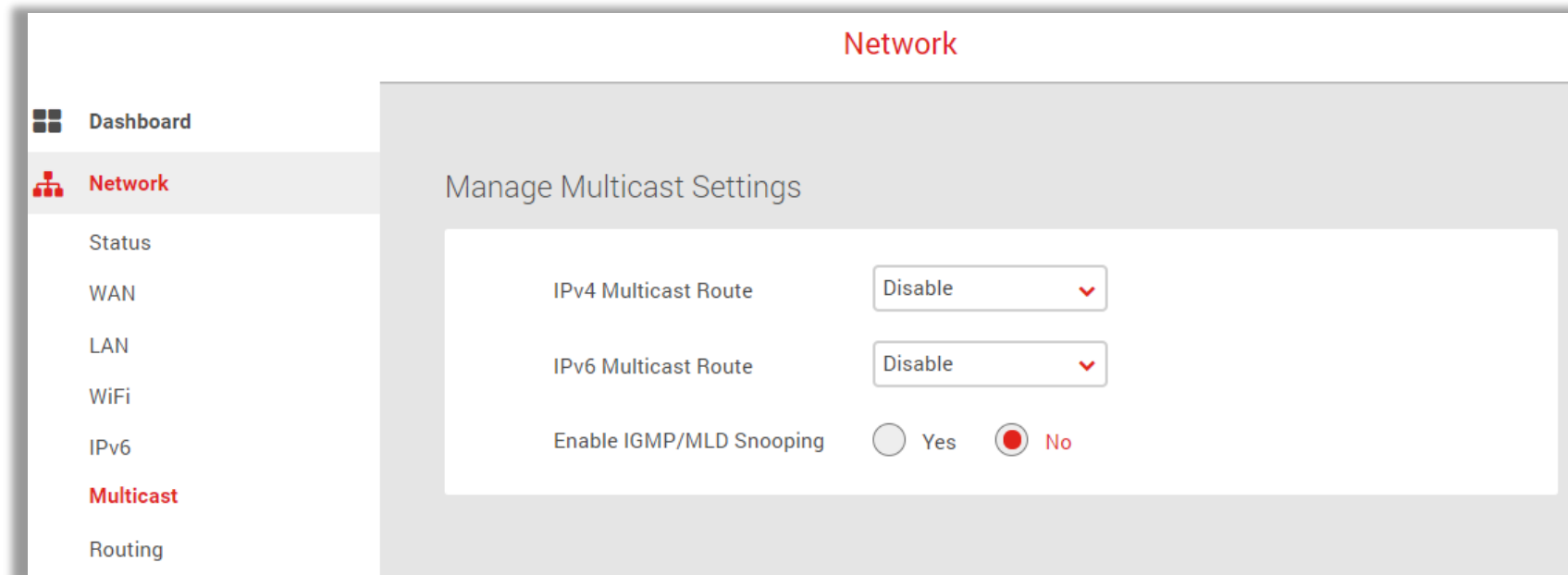
Hostname	MAC Address	IPv6 Address
----------	-------------	--------------

5.2.6 Multicast

General > Network > Multicast

5.2.6.1 Manage Multicast Settings

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



5.2.6 Routing

General > Network > Routing

5.2.7.1 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.

The screenshot shows the 'Network' settings page with the 'Routing' section selected. The 'Static Route' tab is active, displaying the 'Manage Routing Settings' interface. The 'Enable Static Routes' option is currently set to 'No'. Below this, there is a 'Static Routing List (Maximum: 32)' section with a table header and an 'Add Rule' button.

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

+ Add Rule

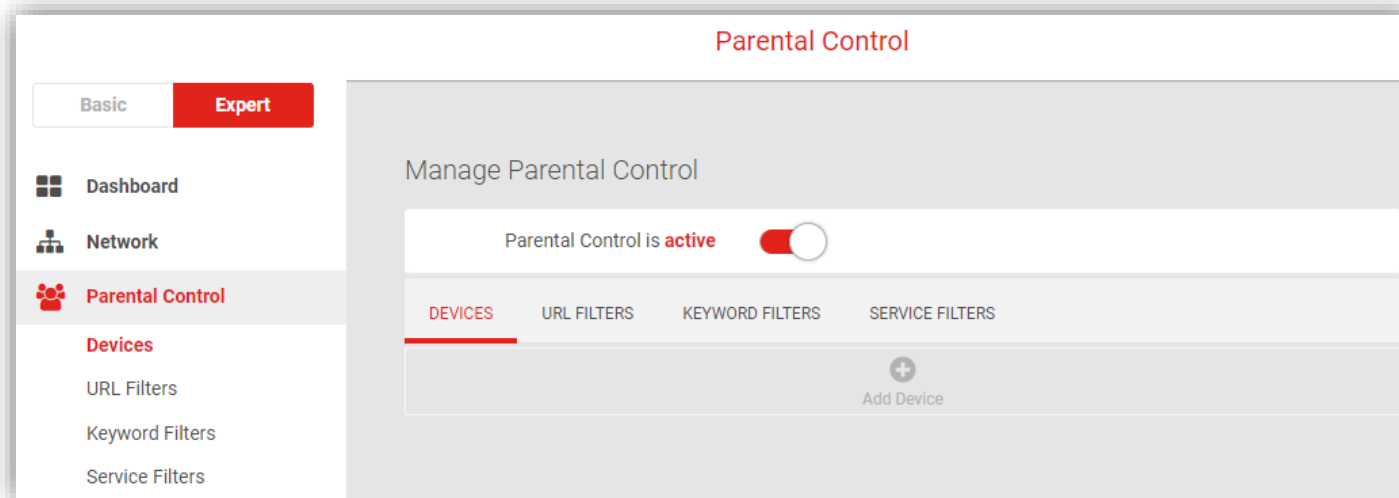
5.3 Parental control

5.3.1 Device

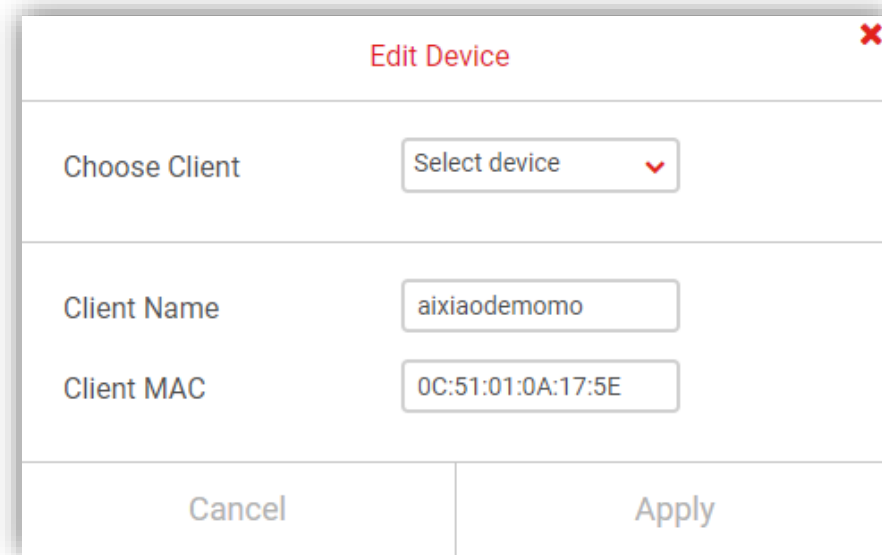
General > Parental control > Device

The Parental Control feature allows you to restrict Internet access to select devices on your network at specified times e.g. disabling Internet access for a child's smartphone.

1. Set the slider to active to enable parental control.



2. Click ADD Device to add and setup a new device for parental controls.
3. Select a device from the Client menu or enter the MAC address manually.
4. Specify a Client Name for the device easy reference.
5. Click Add button then click Save to save the device.



The image shows a dialog box titled "Edit Device" with a red close button in the top right corner. The dialog contains three input fields: "Choose Client" with a dropdown menu showing "Select device", "Client Name" with the text "aixiaodemomo", and "Client MAC" with the text "0C:51:01:0A:17:5E". At the bottom, there are two buttons: "Cancel" and "Apply".

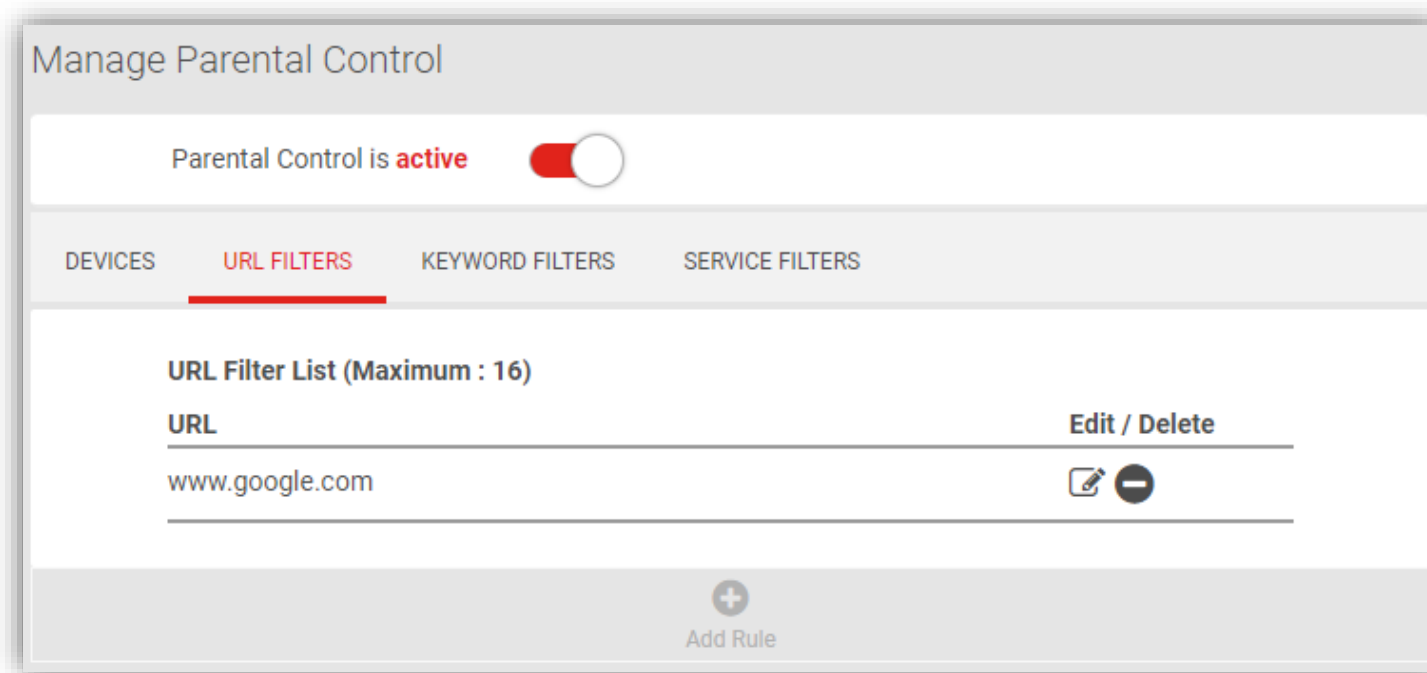
6. Click the **SCHEDULE** icon beside the new device to setup the schedule for Internet access.
7. Click and drag to fill in the red blocks on the schedule by day and hour. The red blocks indicate the time blocks during which Internet access is not allowed.
8. Click **SAVE SCHEDULE** to save the schedule and the device's Internet access will be restricted according to the schedule.

The screenshot shows the 'Manage Parental Control' interface. At the top, it indicates 'Parental Control is active' with a toggle switch. Below this, there are tabs for 'DEVICES', 'URL FILTERS', 'KEYWORD FILTERS', and 'SERVICE FILTERS'. The 'DEVICES' tab is selected, showing a device named 'aixiaodemomo' with MAC address 'Mac 0C:51:01:0A:17:5E'. To the right of the device name are icons for 'Edit Device', 'Schedule', and 'Remove'. The main area is a schedule grid with days of the week (S, M, T, W, T, F, S) as columns and hours (00 to 24) as rows. A legend indicates that white boxes represent 'Allow' and red boxes represent 'Controlled'. The grid shows red blocks for internet access restriction: from 00:00 to 06:00 on Sunday and Saturday; from 12:00 to 14:00 on Monday, Tuesday, Wednesday, and Thursday; and from 22:00 to 24:00 on Friday and Saturday. To the right of the grid are icons for moon (night) and gear (settings). At the bottom, there are buttons for 'Save Schedule' (with a checkmark icon), 'Clear Schedule' (with an 'x' icon), and 'Add Device' (with a plus icon).

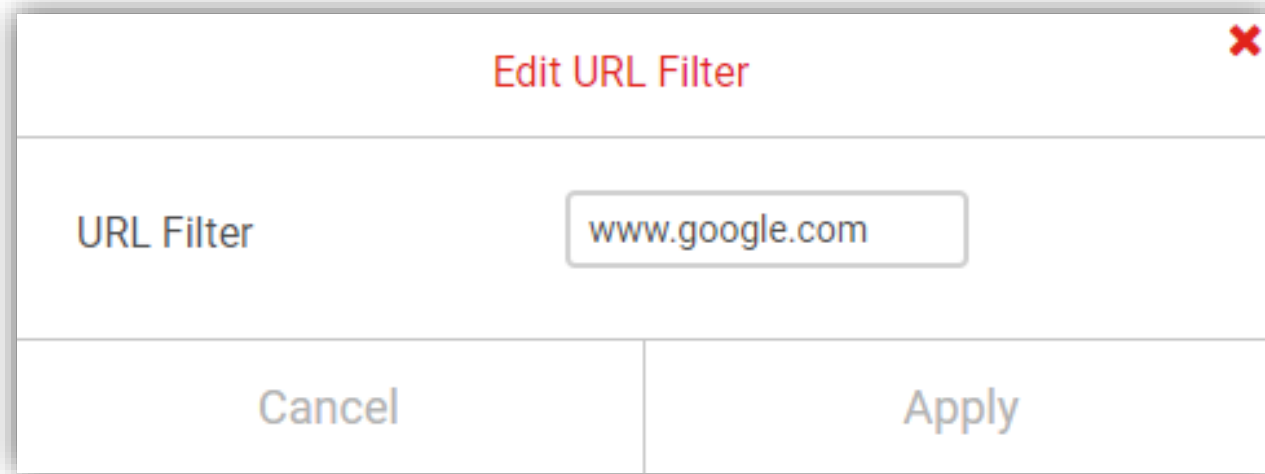
5.3.2 URL Filters

General > Parental control > URL Filters

1. Set the slider to active to enable parental control.



2. Click **Add Rule** to add URL Filter.
3. Input an URL and add it.
4. Save it and the device's Internet access will be restricted according to the URL filter.

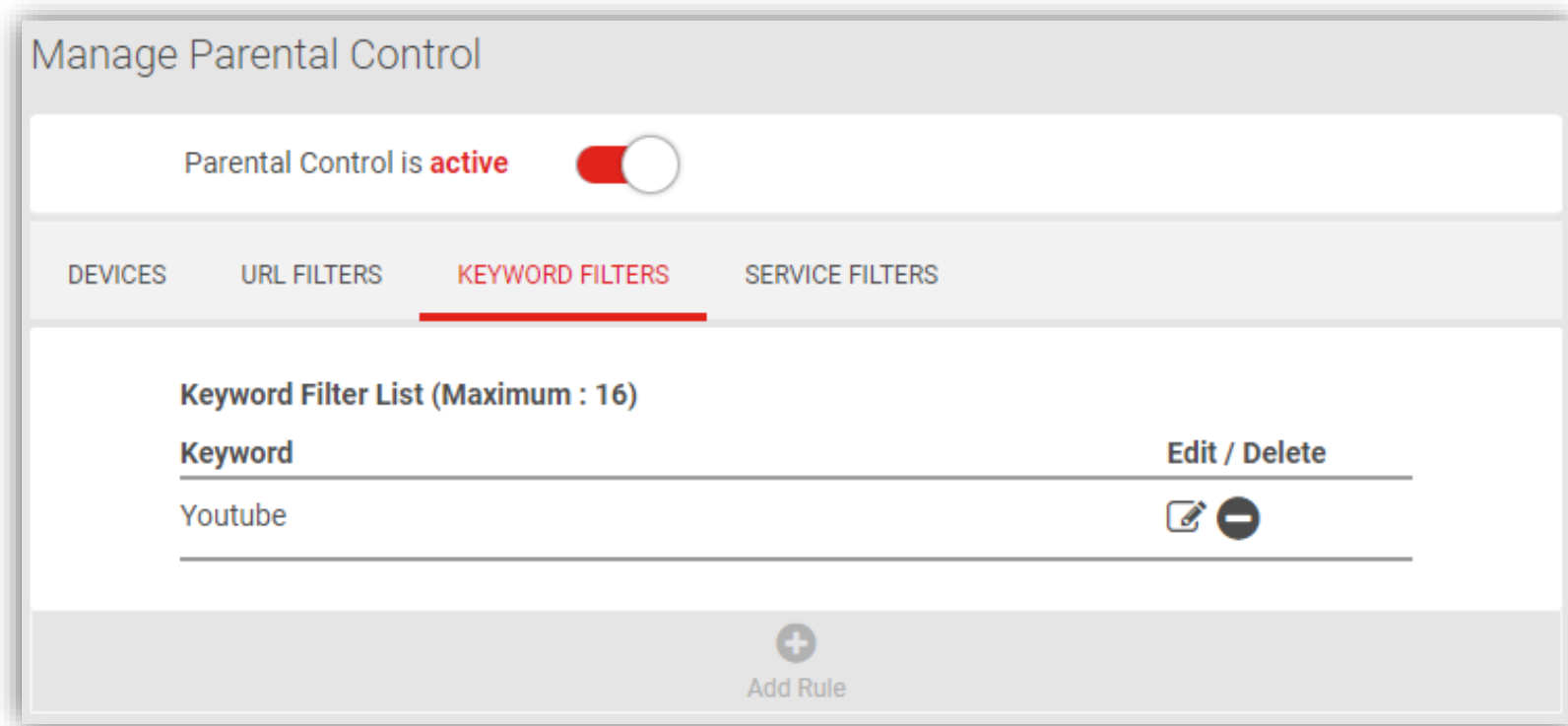


The image shows a dialog box titled "Edit URL Filter" with a red close button in the top right corner. The dialog is divided into three horizontal sections. The top section contains the title. The middle section contains a label "URL Filter" on the left and a text input field containing "www.google.com". The bottom section contains two buttons: "Cancel" on the left and "Apply" on the right.

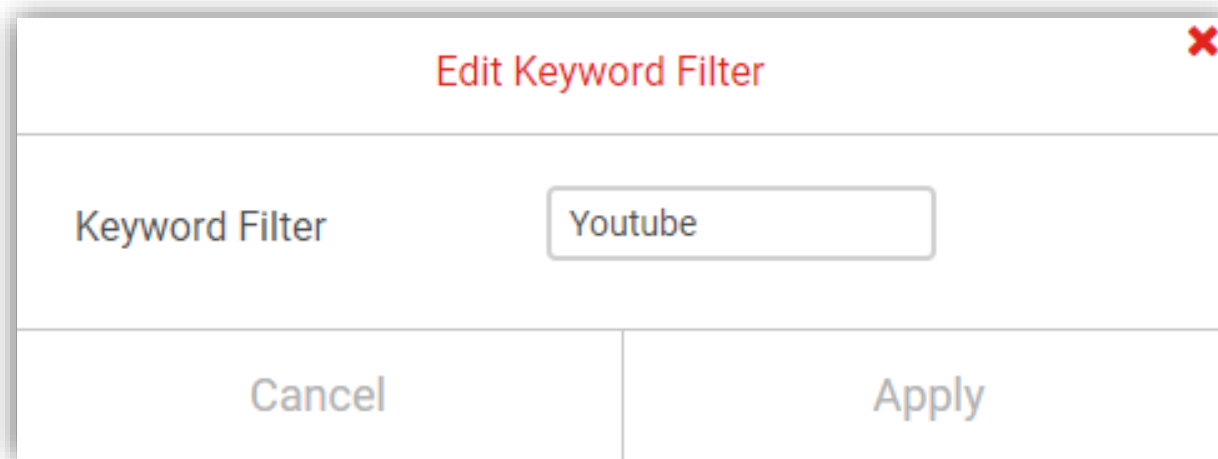
5.3.3 Keyword Filters

General > Parental control > Keyword Filters

1. Set the slider to active to enable parental control based on keyword on the URL.



2. Click **Add Rule** to add Keyword Filter.
3. Input a Keyword and add it.
4. Save it and the device's Internet access will be restricted according to the Keyword filter.



Edit Keyword Filter

Keyword Filter

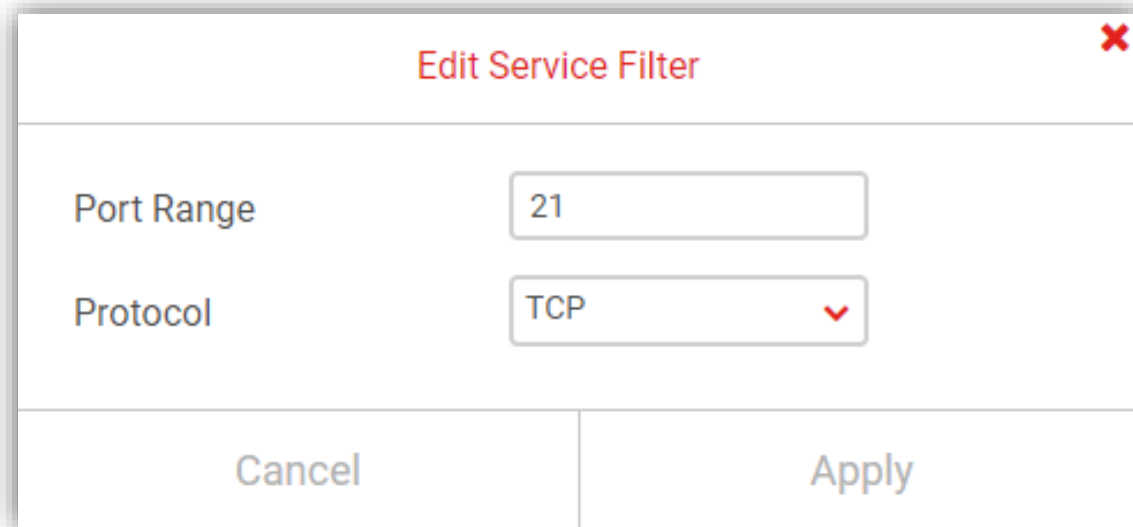
Cancel

Apply

5.3.4 Service Filters

General > Parental control > Service Filters

1. Set the slider to active to enable parental control.
2. Click **Add Rule** to add Service Filter.
3. Input a port range, protocol and add it.
4. Save it and the device's Internet access will be restricted according to the Service filter.



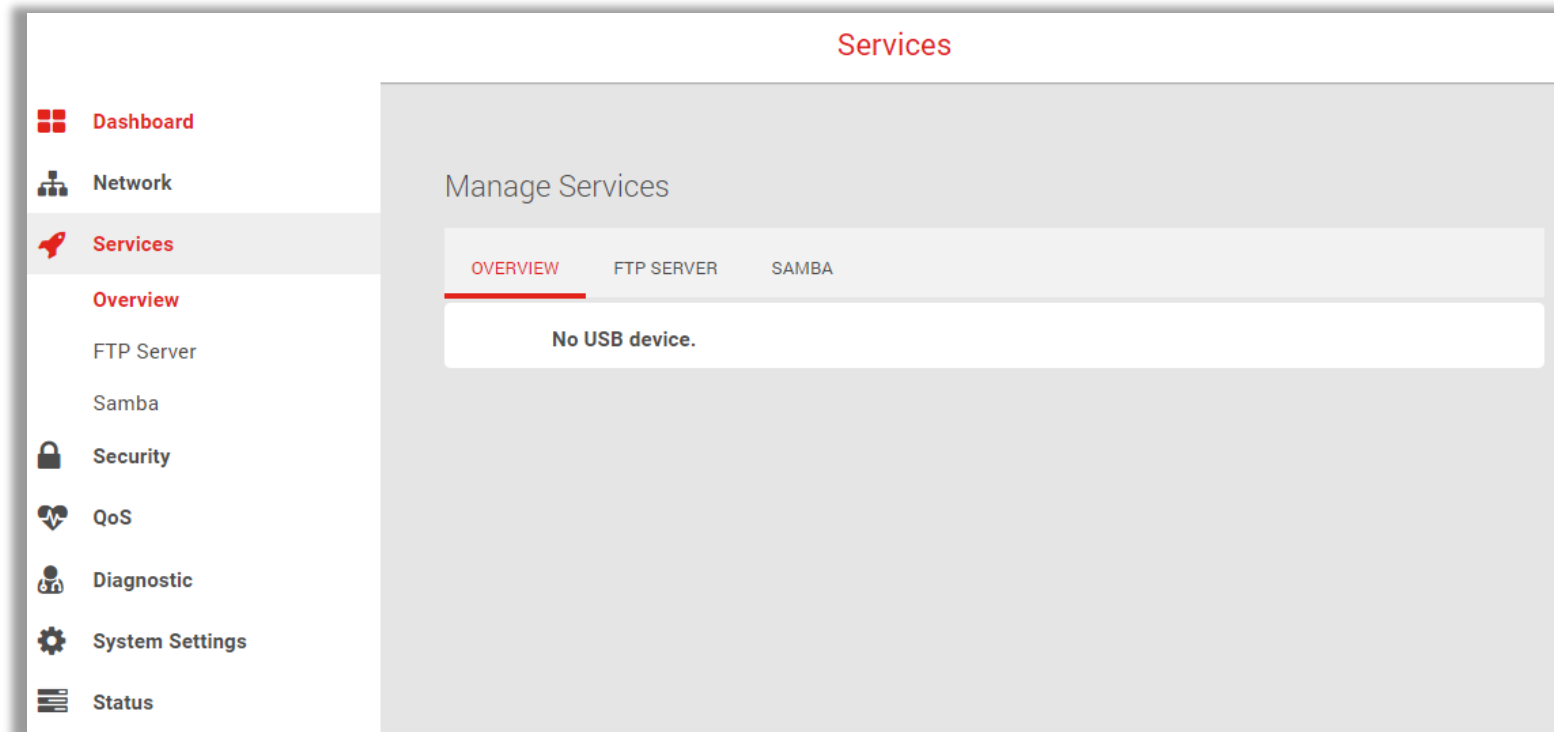
The screenshot shows a dialog box titled "Edit Service Filter" with a red close button in the top right corner. The dialog contains two input fields: "Port Range" with the value "21" and "Protocol" with a dropdown menu showing "TCP". At the bottom, there are "Cancel" and "Apply" buttons.

5.4 Service

5.4.1 Overview

General > Service > Overview

You can attach USB drives (including a thumb drive or a high-capacity external drive) to the USB port on your router. You can then use the drive as network storage, as a FTP server. You can also specify which users can access the content on the drive.



5.4.2 FTP Server

General > Service > FTP Server

1. Insert USB drive or thumb drive or a high-capacity external drive.
2. Enable FTP.
3. Run FTP client software in PC.
4. Access FTP server with anonymous or correct username and password to download/upload files.

Manage Services

OVERVIEW **FTP SERVER** SAMBA

No USB device.

Enable FTP

Max number of Connections

Allow Anonymous Login Yes No

Enable Outside Access Yes No

Local Access Method ftp://192.168.216.1

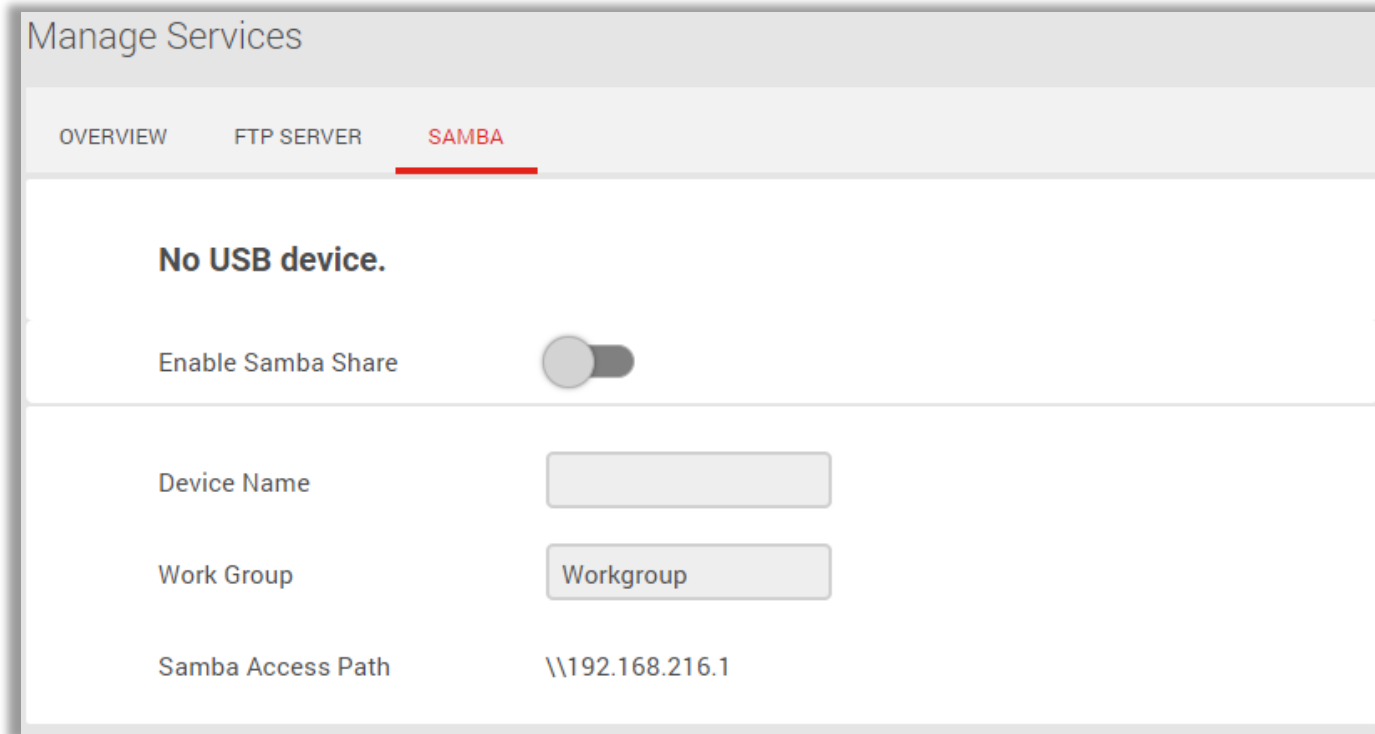
Local Access Method (IPv6) ftp://[2001:d630:160c:5:8278:71ff:fe31:1ae]

5.4.3 Samba

General > Service > Samba

Computers (through network shared directories, network neighborhoods) can securely and conveniently access data in USB storage devices and easily achieve file sharing.

1. Insert USB drive or thumb drive or a high-capacity external drive.
2. Enable SAMBA.
3. Configure the device name and work group. Enter the path in the computer's network share, and you can read or write the data.



The screenshot displays the 'Manage Services' configuration page for a router. The 'SAMBAs' tab is selected, indicated by a red underline. The page shows a message 'No USB device.' and a toggle switch for 'Enable Samba Share' which is currently turned off. Below this, there are input fields for 'Device Name', 'Work Group' (set to 'Workgroup'), and 'Samba Access Path' (set to '\\192.168.216.1').

Service	Status
OVERVIEW	FTP SERVER
SAMBAs	

No USB device.

Enable Samba Share

Device Name

Work Group

Samba Access Path

5.5 Security

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

5.5.1 Firewall IPv4

General > Security > Firewall IPv4

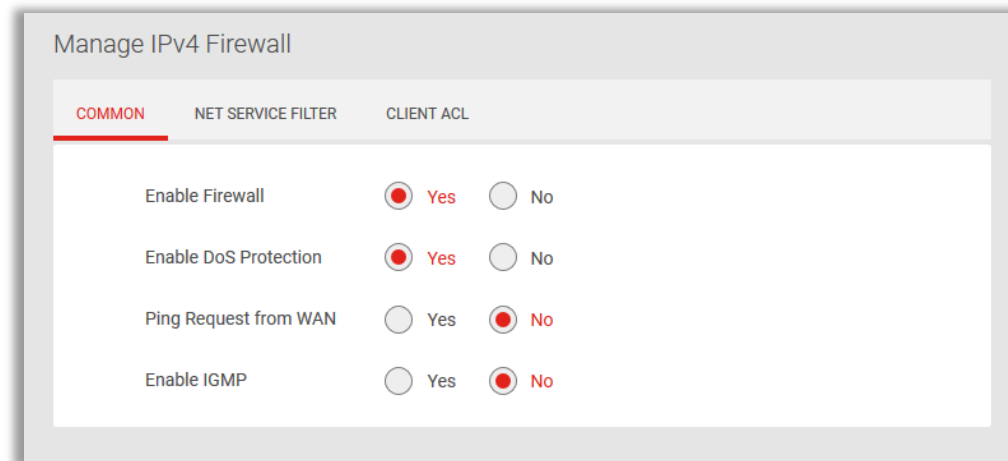
5.5.1.1 Common

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 Internet 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- When disable IGMP, IGMP function is disabled.



Manage IPv4 Firewall

COMMON NET SERVICE FILTER CLIENT ACL

Enable Firewall	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Enable DoS Protection	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Ping Request from WAN	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Enable IGMP	<input type="radio"/> Yes	<input checked="" type="radio"/> No

General > Security > Firewall IPv4

5.5.1.2 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.

Manage IPv4 Firewall



COMMON **NET SERVICE FILTER** CLIENT ACL


Enable Net Service Filter Yes No

Filter Table List

Filtered ICMP packet types

Network Services Filter Table (Maximum: 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Edit/Del
192.168.0.100	10000:10009	111.123.0.12	10000:10009	TCP	 

 Add

General > Security > Firewall IPv4**5.5.1.3 Client ACL**

The Net Service filter blocks L



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.


Manage IPv4 Firewall

COMMON NET SERVICE FILTER **CLIENT ACL**

Enable Client ACL Yes No

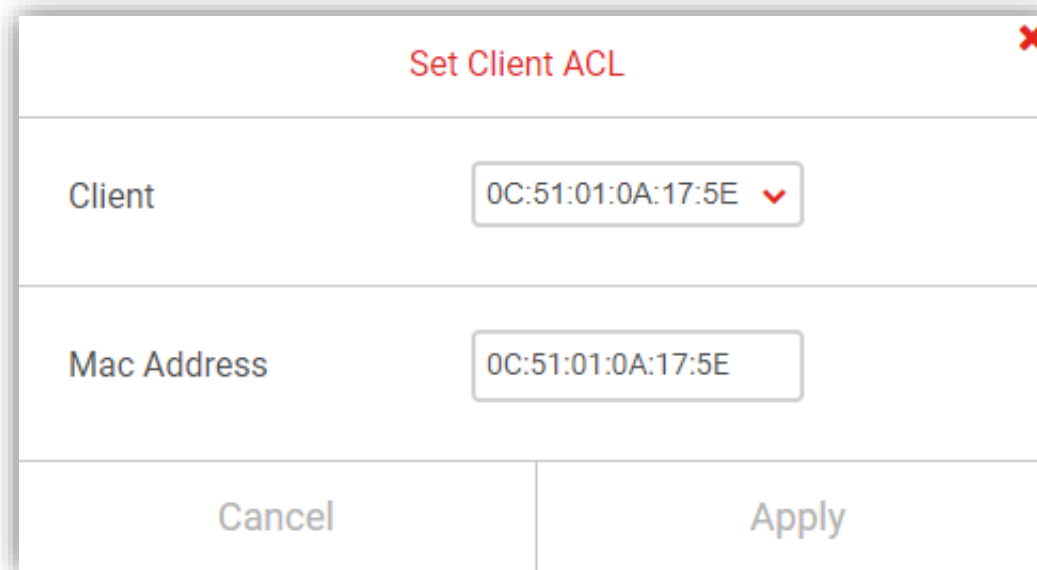
▼ Client ACL List (Maximum : 16)

Client	Edit/Delete
AA:AA:AA:AA:AA:AA	 

 Add Rule

1. Switch Access Control on using the switch.
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 REMOVE or EDIT 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.



The screenshot shows a dialog box titled "Set Client ACL" with a red close button in the top right corner. The dialog is divided into three horizontal sections. The first section is labeled "Client" and contains a dropdown menu with the value "0C:51:01:0A:17:5E" and a small red downward arrow. The second section is labeled "Mac Address" and contains a text input field with the same value "0C:51:01:0A:17:5E". The third section at the bottom contains two buttons: "Cancel" on the left and "Apply" on the right.

5.5.2 Firewall IPv6

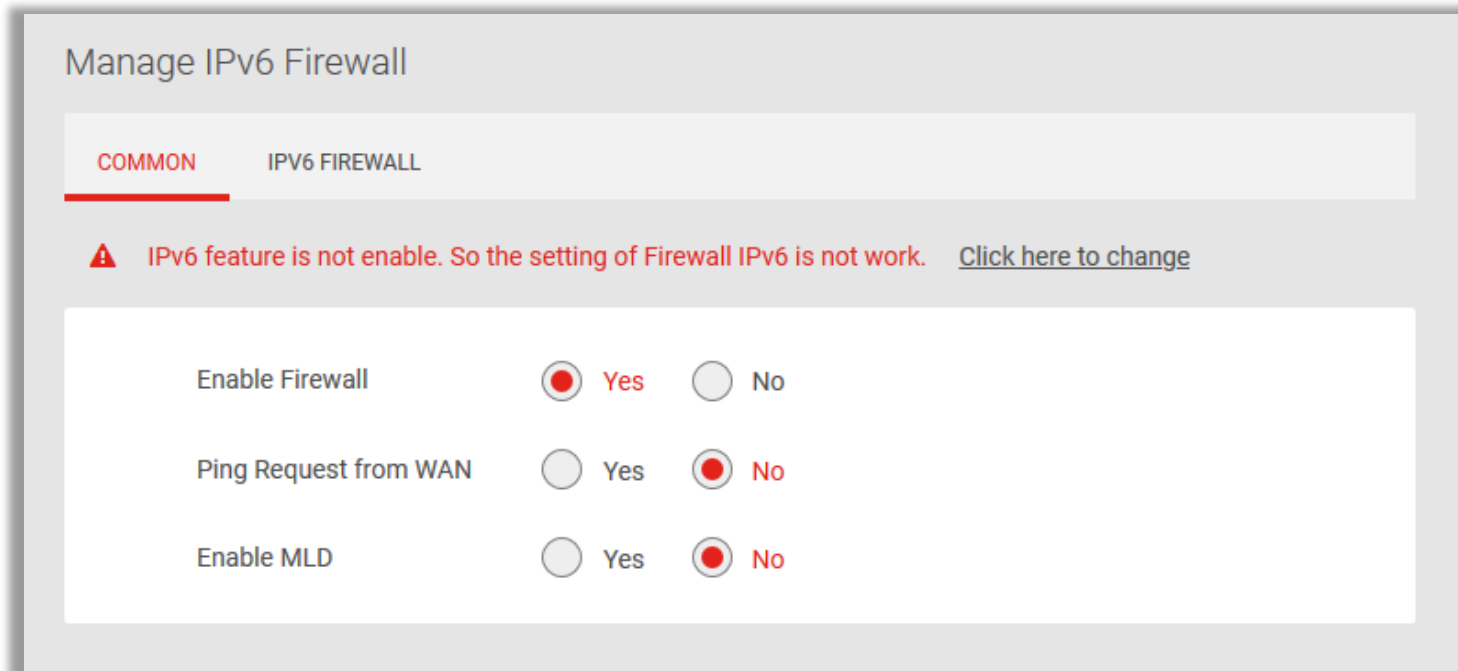
General > Security > Firewall IPv6

5.5.2.1 Common

Enable Firewall- Display the status of firewall function.

Ping Request from WAN- When inactive the feature Wi-Fi gateway will not answer IPv6 ping requests from the Internet. This can increase security as pingging is a common method used by hackers to test networks.

Enable MLD- Multicast Listener Discover, a network protocol used in multicast technology. When disable MLD, MLD function is disabled.



Manage IPv6 Firewall

COMMON IPV6 FIREWALL

⚠ IPv6 feature is not enable. So the setting of Firewall IPv6 is not work. [Click here to change](#)

Enable Firewall	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Ping Request from WAN	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Enable MLD	<input type="radio"/> Yes	<input checked="" type="radio"/> No

General > Security > Firewall IPv6**5.5.2.2 IPv6 Firewall**


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

Manage IPv6 Firewall


COMMON **IPv6 FIREWALL**

Enable Allow Services Yes No

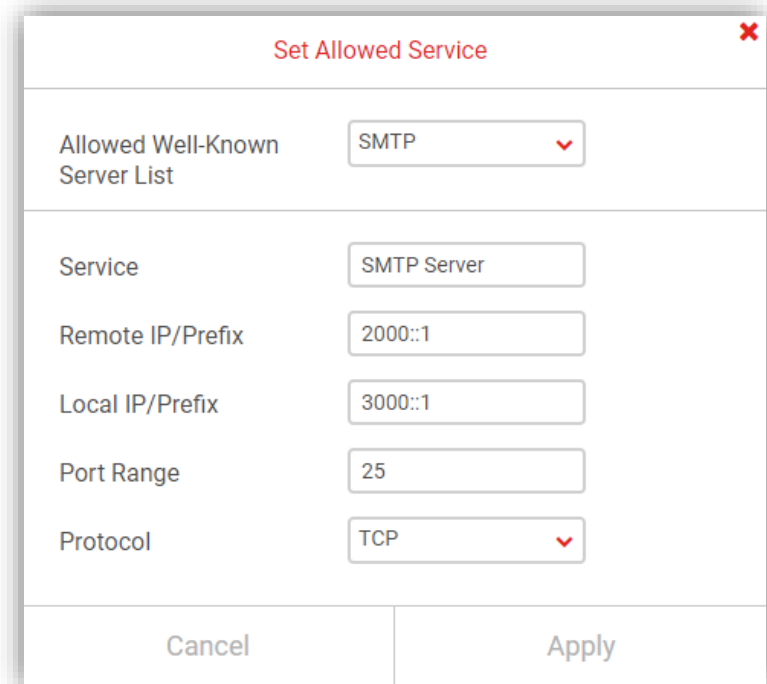
Allowed Service Rules (Maximum: 32)

Service	Remote IP/Prefix	Local IP/Prefix	Port Range	Protocol	Edit/Del
 Add					

Allowed ICMPv6 Rules (Maximum: 16)

ICMPv6 Message type	Local Host	Edit / Delete
 Add		

1. Click Add to add an IPv6 service rule.
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.

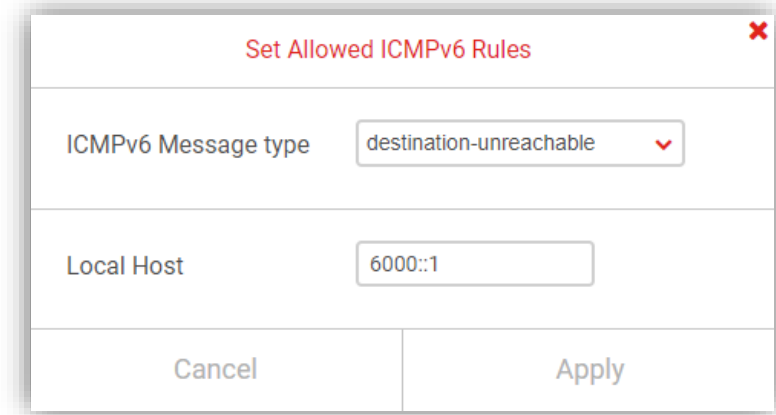


The screenshot shows a dialog box titled "Set Allowed Service" with a red close button in the top right corner. The dialog contains several input fields and dropdown menus:

- Allowed Well-Known Server List:** A dropdown menu with "SMTP" selected.
- Service:** A text input field containing "SMTP Server".
- Remote IP/Prefix:** A text input field containing "2000::1".
- Local IP/Prefix:** A text input field containing "3000::1".
- Port Range:** A text input field containing "25".
- Protocol:** A dropdown menu with "TCP" selected.

At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Apply" on the right.

1. Click Add to add an ICMPv6 rule.
2. Select the ICMPv6 message type from the list
3. Input local host address.
4. Click Add and Save to save the allowed ICMPv6 rule.



Set Allowed ICMPv6 Rules

ICMPv6 Message type destination-unreachable

Local Host 6000::1

Cancel Apply

5.5.3 VPN

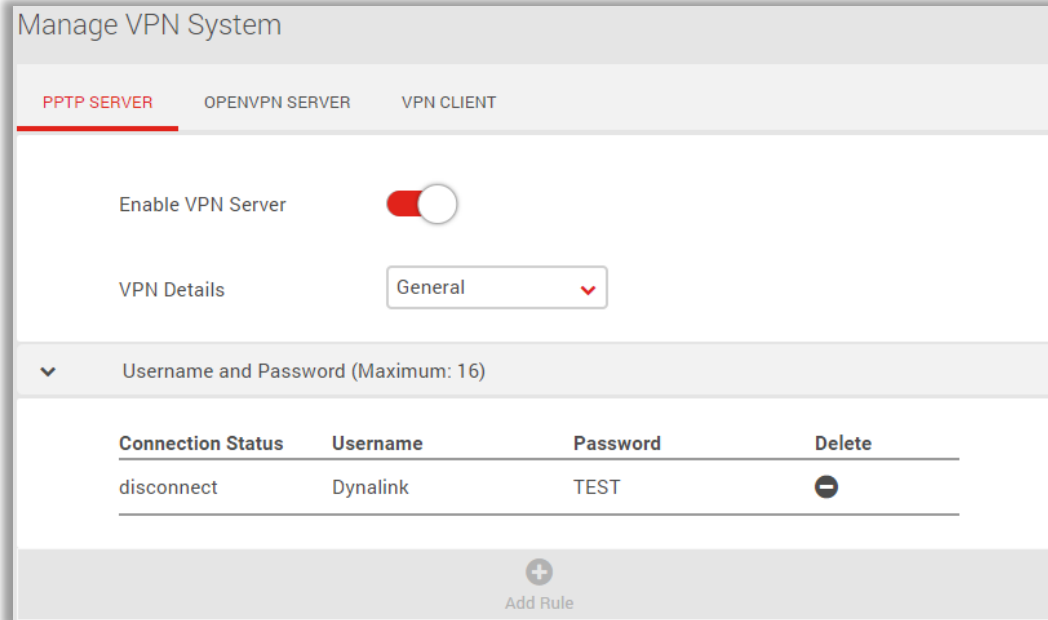
A VPN (Virtual Private Network) uses a public network such as the Internet to provide secure communications between a remote computer and another network. Corporations often provide VPN access to their networks to enable employees to work from remote offices or while traveling, most corporates VPNs use the Internet.

General > Security > VPN

5.5.3.1 PPTP Server

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. The VPN server accepts VPN requests initiated by clients.

1. Enable PPTP Server.



The screenshot displays the 'Manage VPN System' interface. It features three tabs: 'PPTP SERVER' (selected), 'OPENVPN SERVER', and 'VPN CLIENT'. The 'Enable VPN Server' toggle is turned on. Below this, the 'VPN Details' dropdown is set to 'General'. A section titled 'Username and Password (Maximum: 16)' is expanded, showing a table with one entry:

Connection Status	Username	Password	Delete
disconnect	Dynalink	TEST	⊖

At the bottom, there is an 'Add Rule' button with a plus sign icon.

2. Add a username and password.
3. Set up PPTP client dialing on the PC.
4. After the terminal is successfully connected, the WEB UI will display information such as the connection status.
5. PPTP VPN settings are successfully connected, VPN clients can access the Internet and access the company's internal network.

Username and Password
(Maximum: 64)

Username	<input type="text" value="askeytest"/>
Password	<input type="text" value="askeytest"/>

Cancel	Add
--------	-----

General > Security > VPN**5.5.3.2 OpenVPN Server**

OpenVPN implements a virtual private network (VPN) solution in a router or bridge configuration and remote access device to create a secure point-to-point or site-to-site connection.

1. Enable OpenVPN Server.

Manage VPN System

PPTP SERVER **OPENVPN SERVER** VPN CLIENT

Enable VPN Server

VPN Details General ▾

▼ Username and Password (Maximum: 16)

Connection Status	Username	Password	Delete
	askeytest	askeytest	⊖

+
Add Rule

2. Add a username and password.
3. Set up OpenVPN on the PC.
4. After the terminal is successfully connected, the WEB UI will display information such as the connection status.
5. OpenVPN settings are successfully connected, VPN clients can access the Internet and access the company's internal network.

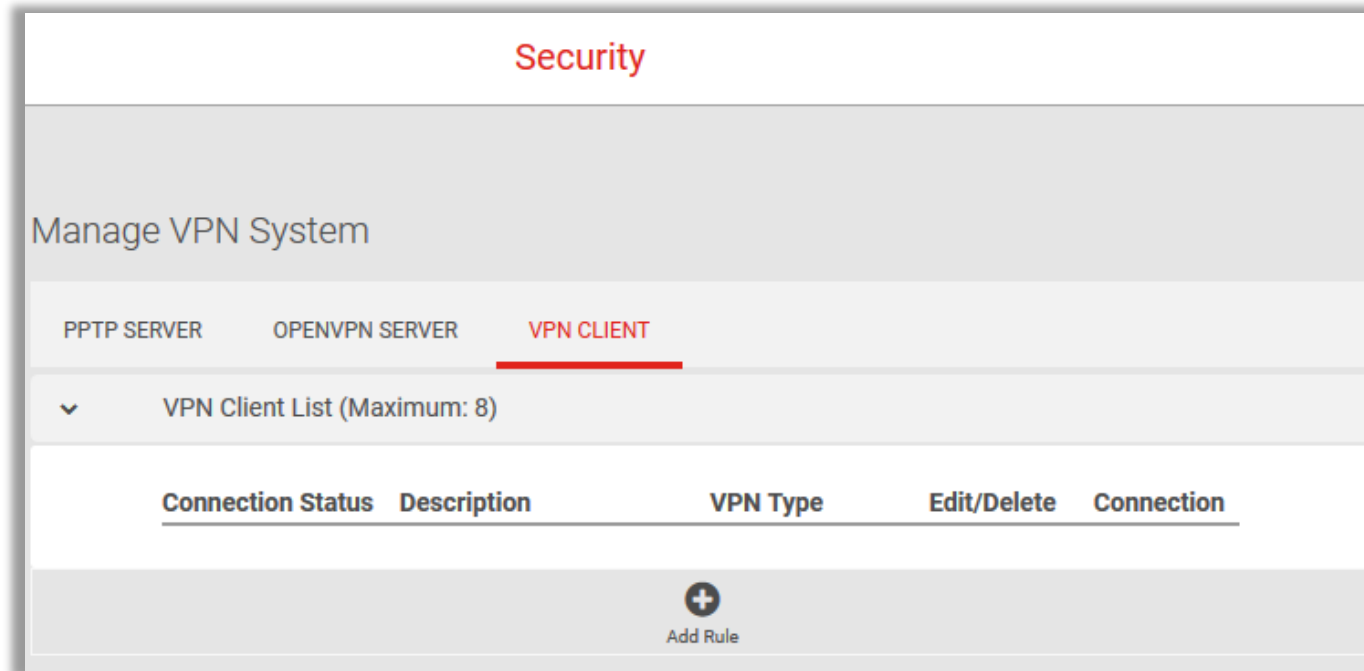
Username and Password
(Maximum: 64)

Username	<input type="text" value="askeytest"/>
Password	<input type="text" value="askeytest"/>

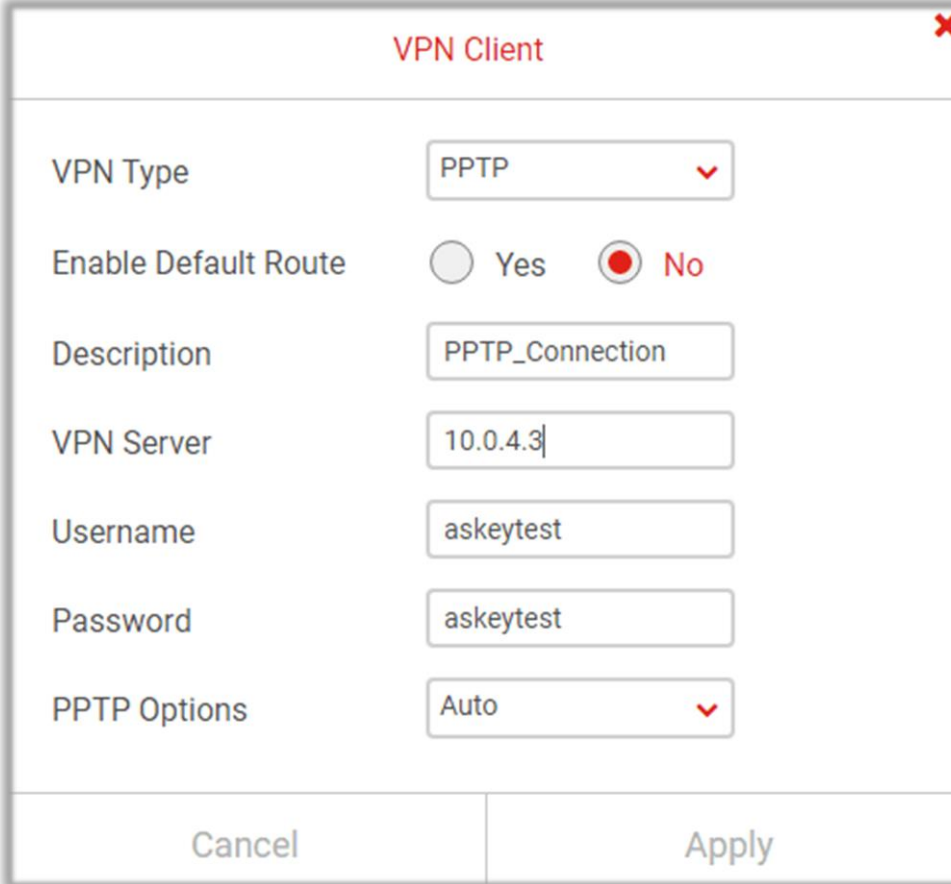
Cancel	Add
--------	-----

General > Security > VPN**5.5.3.2 OpenVPN Server**

1. Add a VPN Client rule.



2. Select VPN type, type VPN server IP, username and password.
3. Gateway can access the Internet and access the company's internal network.



The image shows a configuration window titled "VPN Client" with a red close button in the top right corner. The window contains the following fields and options:

- VPN Type:** A dropdown menu set to "PPTP".
- Enable Default Route:** Radio buttons for "Yes" (unselected) and "No" (selected).
- Description:** A text box containing "PPTP_Connection".
- VPN Server:** A text box containing "10.0.4.3".
- Username:** A text box containing "askeytest".
- Password:** A text box containing "askeytest".
- PPTP Options:** A dropdown menu set to "Auto".

At the bottom of the window, there are two buttons: "Cancel" on the left and "Apply" on the right.

5.6 QoS

Quality of Service (QoS) is a feature to manage Internet bandwidth efficiently. Some applications require more bandwidth than others to function properly, and QoS allows you to ensure that sufficient bandwidth is available. Maximum bandwidth can be set for specified devices on the network, ensuring that sufficient bandwidth is available for others – or priority numbering can be used to prioritize devices on the network for bandwidth. QoS can improve performance for applications such as gaming or entertainment streaming.

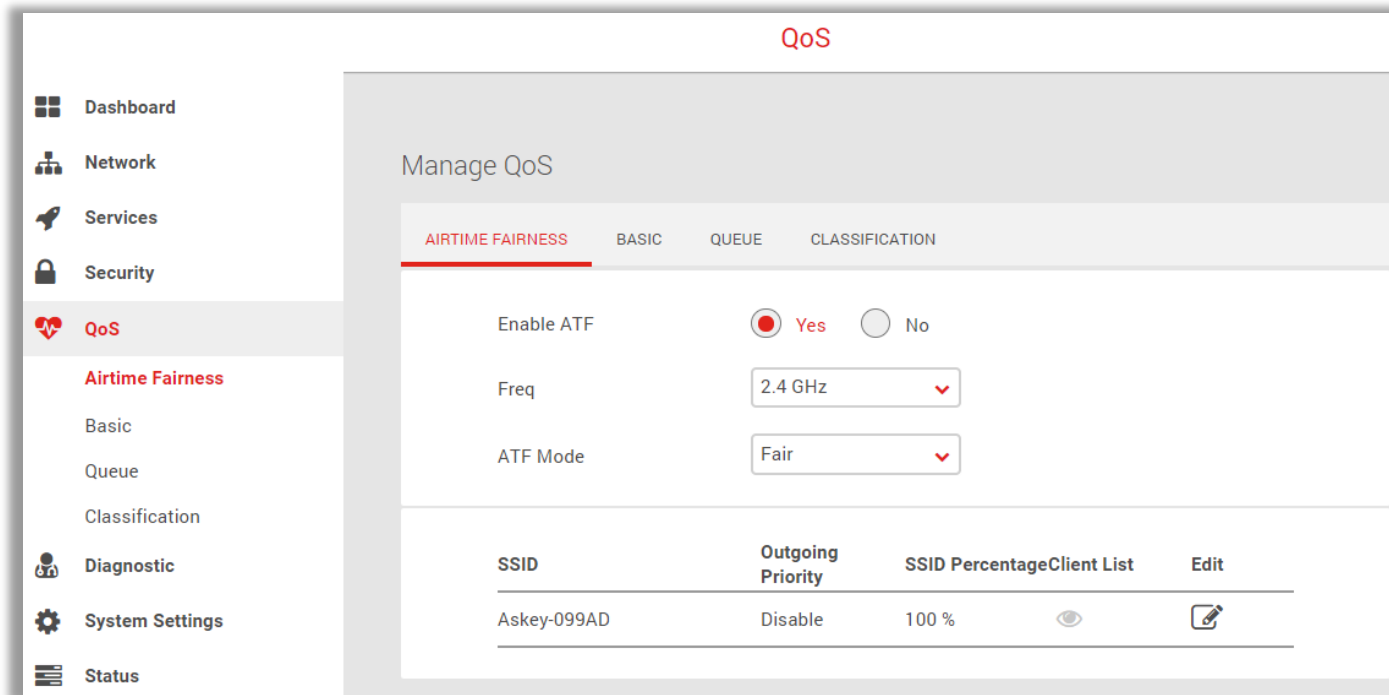
5.6.1 Airtime Fairness

General > QoS > Airtime Fairness

Airtime Fairness is a feature that boost the overall network performance by sacrifice a little bit of network time on your slowest devices. Note: The relatively “slow” Wi-Fi speed devices can be slow from either long physical distance, weak signal strength, or simply being a legacy device with older technology.

When your router is connected to a large number of wireless clients at the same time, enabling Airtime Fairness can better balance bandwidth allocation between devices, avoid bandwidth waste and slow devices slow down the entire network. In addition, if some of your devices (such as mobile phones) are often far away from the router and the signal is not good, you should also enable Airtime Fairness to ensure the network quality of other devices.

Remark: The device supports Basic, Queue and Classification function only when WAN Interface Mode is configured as WAN. You can go to Expert > Network > WAN to change it.



Airtime Fairness	
Enable ATF	Toggle the switch to enable or disable ATF.
Freq	Wireless frequency 2.4GHz or 5GHz.
ATF Mode	Fair or strict.

5.6.2 Basic

General > QoS > Basic

Basic setting allows configure WAN interface upload bandwidth. Bandwidth management helps properly allocate bandwidth resources. It has two queue type: weighted round robin and weighted fair queuing.

1. Enable QoS.
2. Design Speed Limitation for Upstream & Downstream.

WAN Upload (LAN-to-WAN) =50Mbps

Private Network Download (WAN-to-LAN) =100Mbps

Note: Once incoming stream rate exceeds Speed Limitation (congestion), QoS competition mechanism would be triggered and started to follow Egress Queue algorithm (Strict Priority or WRR or WFQ)

3. Configure Queue Type and select general “Strict Priority” algorithm on both WAN Interface (LAN-to-WAN) & Private Network (WAN-to-LAN).

Strict Priority: That’s, “Higher Queue streams MUST be guaranteed to higher opportunity than lower one while traffic congestion occurs”.

The screenshot shows the 'Manage QoS' configuration page. At the top, there are four tabs: 'AIRTIME FAIRNESS', 'BASIC' (which is selected and underlined in red), 'QUEUE', and 'CLASSIFICATION'. Below the tabs, there are several configuration sections:

- QoS Enable:** A radio button labeled 'Yes' is selected, and a radio button labeled 'No' is unselected.
- Speed Limitation:** A dropdown arrow is visible to the left of the section title. Below it, there are two rows:
 - 'WAN Upload' with a text input field containing '50' and 'Mbps' to its right.
 - 'Private Network Download' with a text input field containing '100' and 'Mbps' to its right.
- Queue Type:** A dropdown arrow is visible to the left of the section title. Below it, there are two rows:
 - 'WAN Interface Queue Type' with a dropdown menu showing 'Strict Priority' and a red downward arrow.
 - 'Private Network Queue Type' with a dropdown menu showing 'Strict Priority' and a red downward arrow.

5.6.3 Queue

General > QoS > Queue

Queue page displays the WAN queue priority list, the priority is descending from top to bottom, and the top has the highest priority.

4. Define suitable queue numbers

Upstream (LAN-to-WAN) queue numbers: up to 8 queues

Suppose to create specific 4-queues in upstream (Priority Level: cpe-1 > cpe-2 > cpe-3 > cpe-4)

Manage QoS

AIRTIME FAIRNESS BASIC **QUEUE** CLASSIFICATION

⚠ In the list: the priority is descending from top to bottom, and the top has the highest priority.

UPSTREAM QUEUE DOWNSTREAM QUEUE

Strict Priority WAN Queue (Maximum: 8)

Queue Name	Enable	Operation
cpe-1	Yes	
cpe-2	Yes	
cpe-3	Yes	
cpe-4	Yes	

Add

Downstream (WAN-to-LAN) queue numbers: up to 8 queues

Suppose to create specific 4-queues in downstream (Priority Level: cpe-5 > cpe-6 > cpe-7 > cpe-8)









Manage QoS


AIRTIME FAIRNESS BASIC **QUEUE** CLASSIFICATION

⚠ In the list: the priority is descending from top to bottom, and the top has the highest priority.

UPSTREAM QUEUE **DOWNSTREAM QUEUE**

▼ Strict Priority WAN Queue (Maximum: 8)

Queue Name	Enable	Operation
cpe-1	Yes	 
cpe-2	Yes	 
cpe-3	Yes	 
cpe-4	Yes	 

 Add

5.6.4 Classification

General > QoS > Classification

5. Create 3-level classification rules for individual US & DS (mapping to planned 3-plays services), also bind “Based On” & “Queue Interface” & previous “Queue Name” & “Class Interface” & the remaining filtering parameters.

e.g. According to IP Destination (or IP Source) parameter binding various fields, if all conditions are met, packets will be put into expected Queues, and then enter competition.

Manage QoS

AIRTIME FAIRNESS BASIC QUEUE **CLASSIFICATION**

⚠ Guest Network is not enabled now, so Guest Network relative settings in this page are not working.

Classification (Maximum:64)

Name	Queue Interface	Enable	Edit/Delete
VoIP_DS	Private Network	Yes	
IPTV_DS	Private Network	Yes	
Internet_DS	Private Network	Yes	
VoIP_US	WAN	Yes	
IPTV_US	WAN	Yes	
Internet_US	WAN	Yes	

Add Rule

(1) For Upstream rule

VoIP_US

Based on: Client (Client/App/SSID/Server)

Queue Name: cpe-1

Queue Interface: WAN (for Upstream)

Class Interface: Private Network (for LAN Network)

Source IP: 10.1.1.2

IPTV_US

Based on: Client (Client/App/SSID/Server)

Queue Name: cpe-2

Queue Interface: WAN (for Upstream)

Class Interface: Private Network (for LAN Network)

Source IP: 10.1.1.3

Internet_US

Based on: Client (Client/App/SSID/Server)

Queue Name: cpe-3

Queue Interface: WAN (for Upstream)

Class Interface: Private Network (for LAN Network)

Source IP: 10.1.1.4

Classification ✕

Enable	<input type="text" value="Yes"/>
Base On	<input type="text" value="Custom"/>
Name	<input type="text" value="VoIP_US"/>
Queue Interface	<input type="text" value="WAN"/>
Queue Name	<input type="text" value="cpe-1"/>
Class Interface	<input type="text" value="Private Network"/>
Source IP	<input type="text" value="10.1.1.2"/>
Source MAC Address	<input type="text"/>
Source Port	<input type="text"/>
Protocol	<input type="text" value="--"/>
Dest IP	<input type="text"/>
Dest MAC Address	<input type="text"/>
Dest Port	<input type="text"/>
DSCP Check	<input type="text"/>
DSCP Remark	<input type="text"/>

Cancel
Apply

(2) For Downstream rule

VoIP_DS

Based on: Server (Client/App/SSID/Server)

Queue Name: cpe-5

Queue Interface: Private Network (for Downstream)

Class Interface: Private Network (for LAN Network)

Dest IP: 10.1.1.2

IPTV_DS

Based on: Server (Client/App/SSID/Server)

Queue Name: cpe-6

Queue Interface: Private Network (for Downstream)

Class Interface: Private Network (for LAN Network)

Dest IP: 10.1.1.3

Internet_DS

Based on: Server (Client/App/SSID/Server)

Queue Name: cpe-7

Queue Interface: Private Network (for Downstream)

Class Interface: Private Network (for LAN Network)

Dest IP: 10.1.1.4

Classification ✖

Enable	<input type="text" value="Yes"/>
Base On	<input type="text" value="Custom"/>
Name	<input type="text" value="VoIP_DS"/>
Queue Interface	<input type="text" value="Private Network"/>
Queue Name	<input type="text" value="cpe-5"/>
Class Interface	<input type="text" value="Private Network"/>
Source IP	<input type="text"/>
Source MAC Address	<input type="text"/>
Source Port	<input type="text"/>
Protocol	<input type="text" value="--"/>
Dest IP	<input type="text" value="10.1.1.2"/>
Dest MAC Address	<input type="text"/>
Dest Port	<input type="text"/>
DSCP Check	<input type="text"/>
DSCP Remark	<input type="text"/>

Cancel
Apply

6. Streams with higher queue SHALL be satisfied on top priority, even without packet losses
 - (1) US dealing priority: VoIP> IPTV> Internet
 - (2) DS dealing priority: VoIP> IPTV> Internet

5.7 Diagnostic

5.7.1 Diagnostic tools

General > Diagnostic > Diagnostic tools

You can run Ping, Traceroute, Nslookup and Ping6 tests with the gateway. Enter the IP address to use for the test and click Diagnose, results are displayed in the box. You can run **Ping**, **Traceroute**, **Nslookup** and **Ping6** tests with the router. Enter the IP address to use for the test and click **Diagnose**, results are displayed in the box.

The screenshot shows the 'Diagnostic' page in the router's web management console. The page title is 'Diagnostic'. On the left is a navigation menu with the following items: Dashboard, Network, Services, Security, QoS, Diagnostic (highlighted), Diagnostic Tools, System Settings, and Status. The main content area is titled 'Manage Diagnostic' and contains a section for 'DIAGNOSTIC TOOLS'. This section has three input fields: 'Method' set to 'Ping', 'Target' set to 'Google', and 'Count' set to '3'. Below these fields is a red 'Diagnose' button. Underneath the button is a text box containing the following output:

```
PING www.google.com (172.217.160.68): 56 data bytes
64 bytes from 172.217.160.68: seq=0 ttl=116 time=14.250 ms
64 bytes from 172.217.160.68: seq=1 ttl=116 time=18.180 ms
64 bytes from 172.217.160.68: seq=2 ttl=116 time=16.104 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 14.250/16.178/18.180 ms
```

5.8 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.

The screenshot displays the 'System Settings' web interface. The main heading is 'System Settings' in red. Below it is a sub-heading 'Manage System Settings'. There are four tabs: 'PASSWORD & TIMEZONE' (selected), 'REBOOT', 'CONFIGURATION & RESET', and 'FIRMWARE'. The 'PASSWORD & TIMEZONE' section is expanded, showing three sub-sections: 'System Password', 'Time Zone', and 'Miscellaneous'. The 'System Password' section includes fields for 'Username' (admin), 'Old Password', 'New Password' (4 to 16 characters), and 'Confirm Password' (4 to 16 characters), along with a 'Show Password' checkbox. The 'Time Zone' section has a dropdown menu set to 'America/Los Angeles'. The 'Miscellaneous' section includes 'Remote Log Server' and 'Auto Logout' (0 Minutes (Disable:0)).

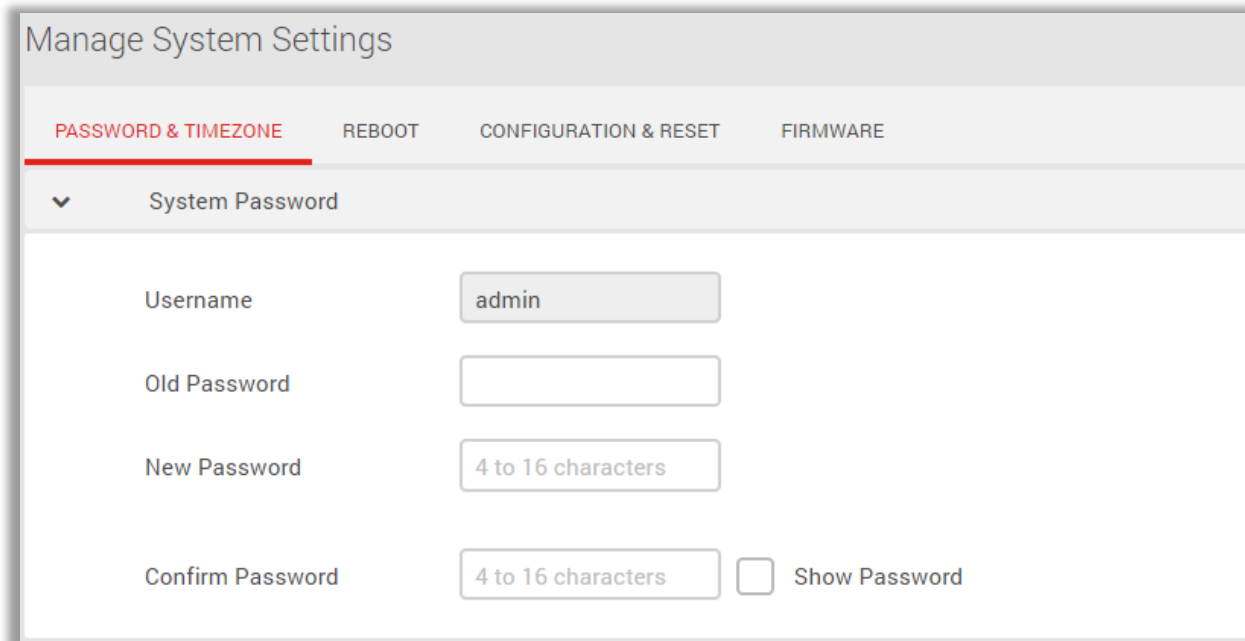
Manage System Settings	
PASSWORD & TIMEZONE	
System Password	
Username	admin
Old Password	
New Password	4 to 16 characters
Confirm Password	4 to 16 characters <input type="checkbox"/> Show Password
Time Zone	
Time Zone	America/Los Angeles
Miscellaneous	
Remote Log Server	
Auto Logout	0 Minutes (Disable:0)

5.7.1 Password & Timezone

General > System Settings > 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 choose **Save** to save the new settings.



The screenshot displays the 'Manage System Settings' web interface. At the top, there are four tabs: 'PASSWORD & TIMEZONE' (highlighted in red), 'REBOOT', 'CONFIGURATION & RESET', and 'FIRMWARE'. Below the tabs, a dropdown menu is open, showing 'System Password'. The main content area contains four input fields: 'Username' with the value 'admin', 'Old Password' (empty), 'New Password' with the placeholder '4 to 16 characters', and 'Confirm Password' with the placeholder '4 to 16 characters'. To the right of the 'Confirm Password' field is a checkbox labeled 'Show Password'.

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

The screenshot displays the configuration interface for the DL-WRX36 Router, organized into three main sections:

- Time Zone:** A dropdown menu is set to "America/Los Angeles".
- Miscellaneous:** Includes a "Remote Log Server" text input field and an "Auto Logout" section with a numeric input field set to "0" and the label "Minutes (Disable:0)".
- NTP Server (Maximum : 6):** A table listing four NTP servers, each with an edit icon and a delete icon.

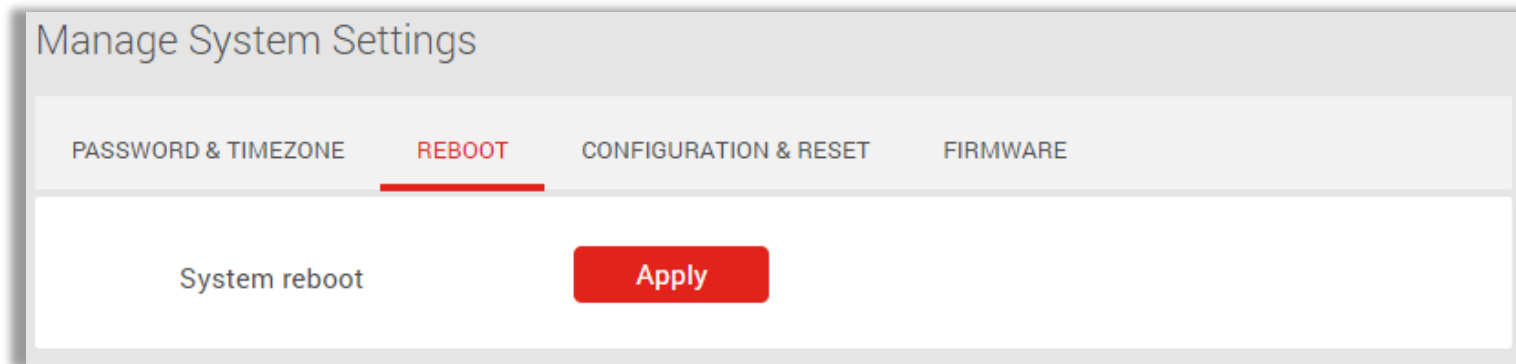
NTP Server	Edit / Delete
us.pool.ntp.org	
north-america.pool.ntp.org	
time.nist.gov	
pool.ntp.org	

At the bottom of the NTP Server section, there is a button with a plus sign and the text "Add".

5.7.2 Reboot

General > System Settings > Reboot

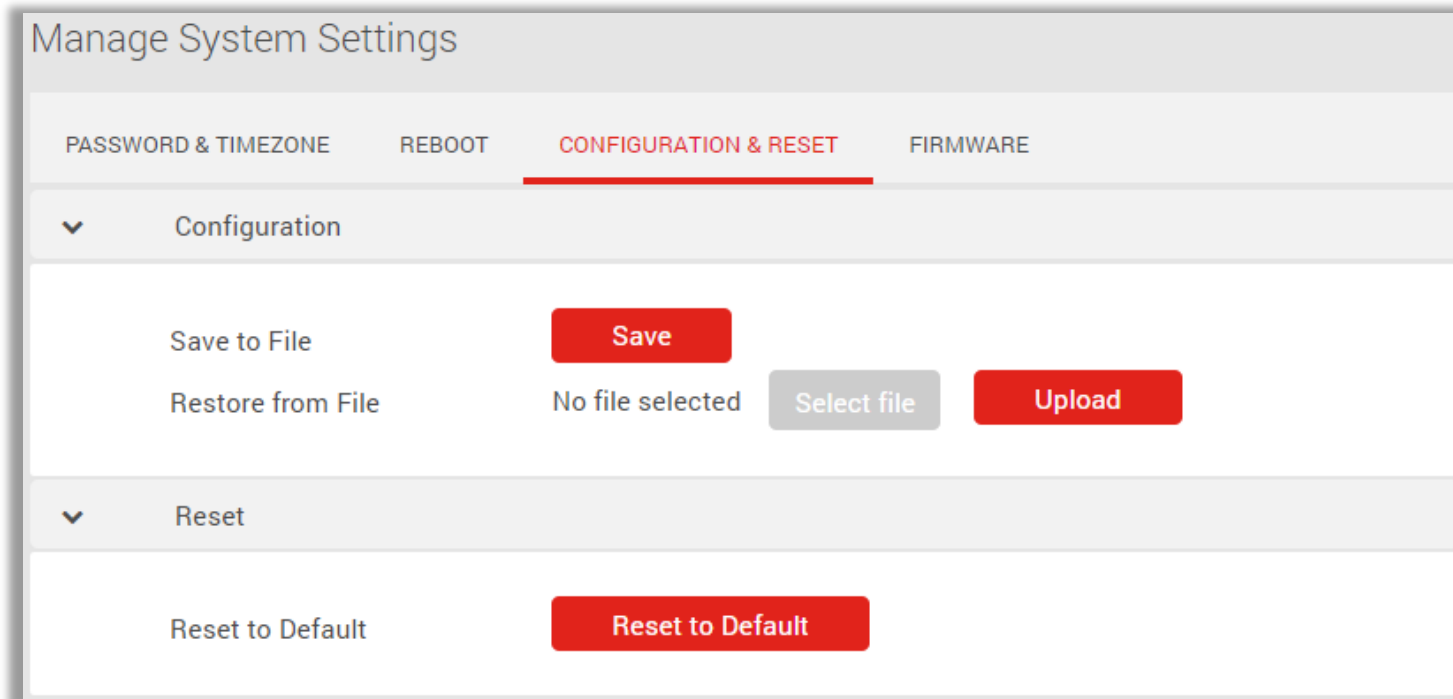
Reboot the router by press **Apply** button.



5.7.3 Configuration & Reset

General > System Settings > Configuration & Reset

The Configuration & Reset page enables you to save/upload the gateway's current settings as a file to your local computer, or upload your gateway to previously saved settings by loading a backed up file. You can also reset the gateway back to factory default settings. If the gateway 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 gateway back to its default settings using the Reset button on the back of the gateway (press and hold for 4+ seconds).



Notice:

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 4+ seconds.

Save to File	
Save a copy of your current settings	Click the Backup button to save the settings file to your local computer.
Restore from File	
Restore saved settings from a file	Choose Select File to locate a previously saved settings file on your computer and select it to load the file to your router.
Reset	
Revert all the settings to their default values.	Select Factory Restore to revert your router to it's original factory default state. This resets all settings.

5.7.3 Firmware

General > System Settings > 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.

The screenshot displays the 'Manage System Settings' interface with the 'FIRMWARE' tab selected. It is divided into two main sections: 'Firmware Information' and 'Upgrade from internet'.

Manage System Settings			
PASSWORD & TIMEZONE	REBOOT	CONFIGURATION & RESET	FIRMWARE
▼ Firmware Information			
Product ID			
Hardware Version		Unknown	
Firmware version installed		0.00.1.267	
▼ Upgrade from internet			
Check new firmware		Check	
Version:		Update	

5.9 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:

The screenshot shows the router's web interface. On the left is a navigation menu with the following items: Dashboard, Network, Services, Security, QoS, Diagnostic, System Settings, and Status (highlighted). Under 'Status', there are sub-links: Wireless (highlighted), DHCP Lease, Routing Table, Port Forwarding, Connection List, Snooping Table, and Blocked Users.

The main content area is titled 'Status' and has several tabs: WIRELESS (selected), DHCP LEASE, ROUTING TABLE, PORT FORWARDING, CONNECTION LIST, SNOOPING TABLE, and BLOCKED USERS. Below these tabs, there are two more sub-sections: 2.4GHZ CLIENTS (selected) and 5GHZ CLIENTS.

The '2.4GHZ CLIENTS' section displays the following information for 'interface 1':

```

interface 1:
ath1      IEEE 802.11axg  ESSID:"Askey-099AD"
          Mode:Master  Frequency:2.437 GHz  Access Point: 00:03:7F:12:34:57
          Bit Rate:573.5 Mb/s  Tx-Power:29 dBm
          RTS thr:off  Fragment thr:off
          Encryption key:2163-E7C0-0F1B-D907-D6E6-23F7-68B5-CFEB  Security
          Power Management:off
          Link Quality=0/94  Signal level=-96 dBm  Noise level=-96 dBm (BDF
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0
  
```

Below this, there is a 'Stations List' section with a header row:

```

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

5.9.1 Wireless

General > Status > 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 General > Network > Wi-Fi Settings.

The screenshot shows the 'Status' page of a router, specifically the 'Wireless' section. The '2.4GHZ CLIENTS' tab is selected. The main content area displays the configuration and status for 'interface 1: ath1'. Below this, a 'Stations List' table is partially visible, showing columns for ADDR, AID, CHAN, TXRATE, RXRATE, RSSI, MINRSSI, MAXRSSI, IDLE, TXSEQ, RXSEQ, CAPS, and XCAPS.

```

Status
-----
WIRELESS  DHCP LEASE  ROUTING TABLE  PORT FORWARDING  CONNECTION LIST
-----
SNOOPING TABLE  BLOCKED USERS

2.4GHZ CLIENTS  5GHZ CLIENTS
-----
interface 1:
ath1      IEEE 802.11axg  ESSID:"Askey-099AD"
          Mode:Master  Frequency:2.437 GHz  Access Point: 00:03:7F:12:34:57
          Bit Rate:573.5 Mb/s  Tx-Power:29 dBm
          RTS thr:off  Fragment thr:off
          Encryption key:2163-E7C0-0F1B-D907-D6E6-23F7-68B5-CFEB  Security
          Power Management:off
          Link Quality=0/94  Signal level=-96 dBm  Noise level=-96 dBm (BDF
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0  Missed beacon:0

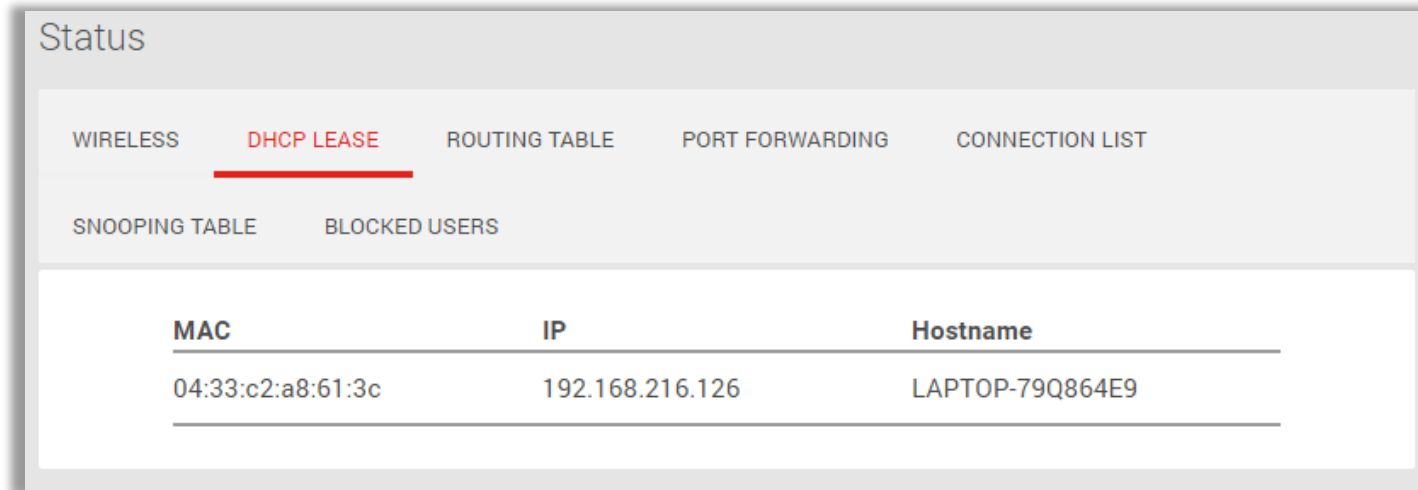
Stations List
-----
ADDR AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE TXSEQ RXSEQ CAPS XCAPS

```

5.9.2 DHCP Lease

General > Status > DHCP Lease

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



The screenshot shows a web interface titled "Status" with several navigation tabs: WIRELESS, DHCP LEASE (highlighted with a red underline), ROUTING TABLE, PORT FORWARDING, CONNECTION LIST, SNOOPING TABLE, and BLOCKED USERS. Below the tabs is a table with three columns: MAC, IP, and Hostname. The table contains one entry: MAC 04:33:c2:a8:61:3c, IP 192.168.216.126, and Hostname LAPTOP-79Q864E9.

MAC	IP	Hostname
04:33:c2:a8:61:3c	192.168.216.126	LAPTOP-79Q864E9

5.9.3 Routing Table

General > Status > Routing Table

Displays the Wi-Fi gateway's routing table information including IPv4 and IPv6 routing table.

The screenshot shows the 'Status' page of the DL-WRX36 Router. The 'ROUTING TABLE' tab is selected. The page displays the following routing information:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use I
0.0.0.0	10.10.160.1	0.0.0.0	UG	0	0	0 e
0.0.0.0	0.0.0.0	0.0.0.0	U	2048	0	0 4
10.10.160.0	0.0.0.0	255.255.255.0	U	0	0	0 e
10.10.160.1	0.0.0.0	255.255.255.255	UH	0	0	0 e
192.168.216.0	0.0.0.0	255.255.255.0	U	0	0	0 b

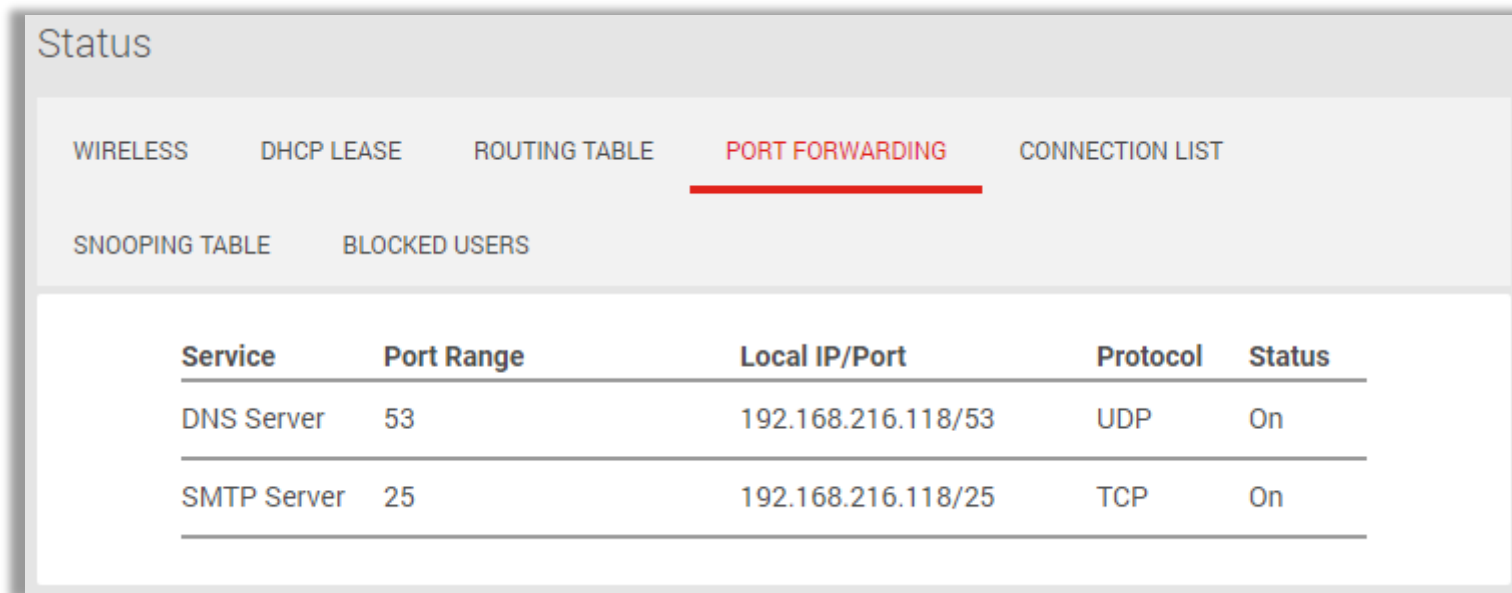
Kernel IPv6 routing table

Destination	Next Hop
2001:d630:160::7411:8810:77ee:fc0c/128	::
::/0	::
::/0	fe80::5604:a6ff:fe57:4e57
::/0	fe80::5604:a6ff:fe57:4e57
2001:d630:160::/64	::
2001:d630:160c:5::/64	::
2001:d630:160c:5::/64	::
2001:d630:160c:5::/64	::
fe80::/64	::
fe80::/64	::
fe80::/64	::
fe80::/64	::
fe80::/64	::
fe80::/64	::
fe80::/64	::
fe80::/64	::
::/0	fe80::d296:fbff:fe8d:2fa7
::/0	fe80::230:88ff:fe80:e7fe
::/0	fe80::5604:a6ff:fe57:4e57
::/0	::

5.9.4 Port Forwarding

General > Status > Port Forwarding

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



The screenshot shows the 'Status' page of a router. At the top, there are several menu items: WIRELESS, DHCP LEASE, ROUTING TABLE, PORT FORWARDING (which is highlighted with a red underline), and CONNECTION LIST. Below these, there are two more menu items: SNOOPING TABLE and BLOCKED USERS. The main content area displays a table of port forwarding rules.

Service	Port Range	Local IP/Port	Protocol	Status
DNS Server	53	192.168.216.118/53	UDP	On
SMTP Server	25	192.168.216.118/25	TCP	On

5.9.5 Connection List

General > Status > Connection List

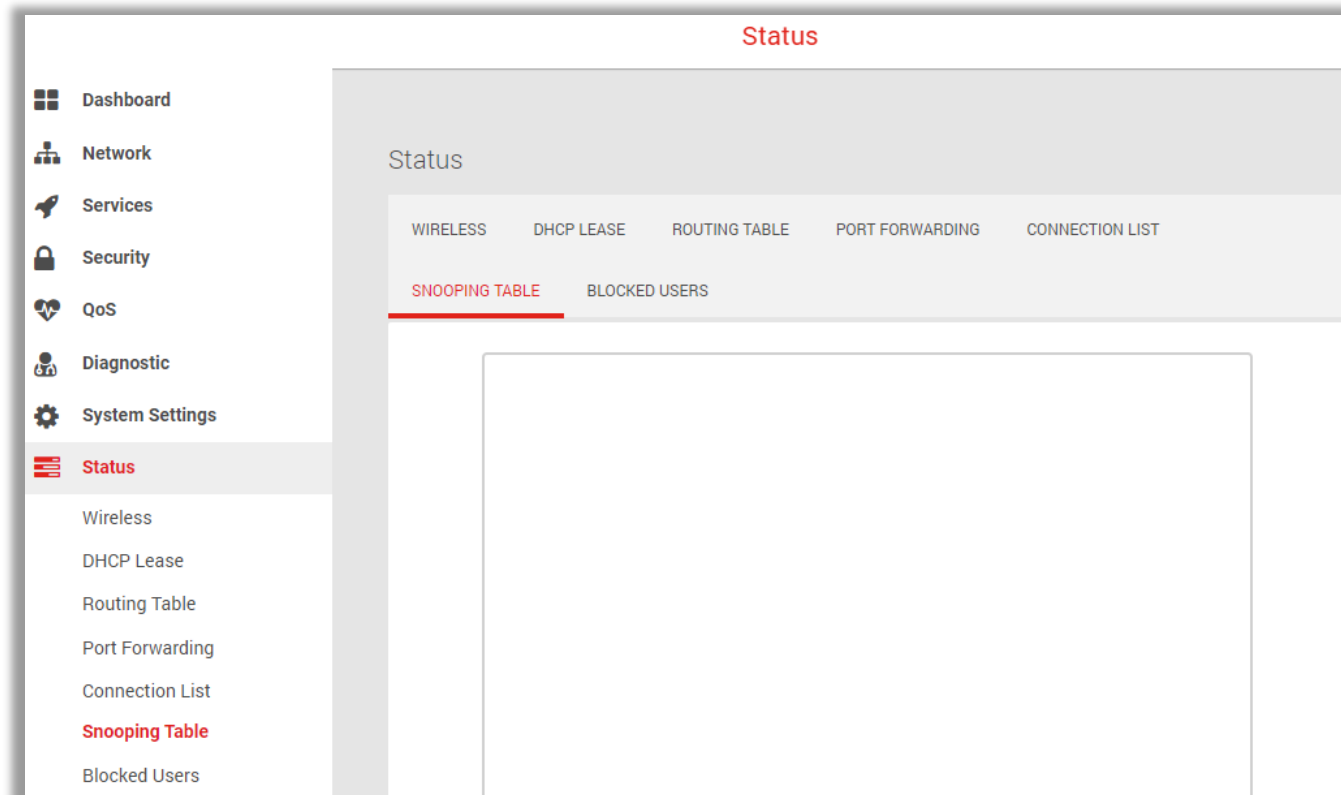
Displays Network, protocol, status, source and destination of the device connected to router.

Status						
WIRELESS		DHCP LEASE		ROUTING TABLE	PORT FORWARDING	CONNECTION LIST
SNOOPING TABLE		BLOCKED USERS				
Network	Protocol	Status	Source	Destination		
ipv4	tcp	ESTABLISHED	192.168.216.11 8:64433	192.168.216.1:8 0		
ipv4	tcp	TIME_WAIT	192.168.216.11 8:64403	192.168.216.1:8 0		
ipv4	udp		192.168.216.1:4 4039	192.168.216.11 8:137		
ipv6	udp		fe80:0000:0000: 0000:f037:3f67:1 1d9:c063:5353	ff02:0000:0000:0 000:0000:0000:0 000:00fb:5353		

5.9.5 Snooping Table

General > Status > Snooping Table

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



5.9.5 Blocked Users

General > Status > Blocked Users

Displays the router's Block Users.

The screenshot displays the router's web interface. On the left is a navigation sidebar with the following items: Dashboard, Network, Services, Security, QoS, Diagnostic, System Settings, Status (highlighted in red), Wireless, DHCP Lease, Routing Table, Port Forwarding, Connection List, Snooping Table, and Blocked Users (highlighted in red). The main content area is titled 'Status' and contains a sub-menu with the following options: WIRELESS, DHCP LEASE, ROUTING TABLE, PORT FORWARDING, CONNECTION LIST, SNOOPING TABLE, and **BLOCKED USERS** (highlighted with a red underline). Below the sub-menu is a table header with two columns: MAC and **Blocked By**. The table body is currently empty.

6. 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 you're not connected, reconnect to the router's Wi-Fi and make sure the password is correct, or use an Ethernet cable to connect directly to the router's LAN port. Follow the steps in **4. Configure your Router** for more help.

Cannot find the Wi-Fi network or cannot connect to the router.

If you can't see your router's Wi-Fi when scanning available networks, or if you can't establish a connection, try the following:

- Refresh the list of available Wi-Fi networks on your device.
- Switch the router off and back on again with the power switch.
- Move the router closer to your device, or move your device closer to the router.
- Restart your device or computer.

If you still can't find the Wi-Fi network or establish a connection, then try to reset your router back to factory default settings. To do this, press and hold the reset button on the back of the router for at least 4 seconds and wait for the router to restart. Then repeat the connection process as described in **4. Configure your Router**.

Can't access the Web User Interface to configure settings.

If you can't access the Web UI, it might be an issue with your device or computer's proxy or IP address settings. Make sure that proxy settings are disabled and that your device or computer can be allocated an IP address on the network by the router's DHCP server. You'll need to check the support for your device or computer's operating system e.g. Windows, macOS, for detailed instructions how to do this.

7. Tips & tricks

Get the best Wi-Fi signal

Where you place the router can affect your wireless coverage. For the best Wi-Fi performance, your router needs open spaces, away from walls, obstructions and heavy-duty appliances or electronics.

Surf the Internet faster

Have you thought of changing your network frequency band to enjoy a faster connection? Your router is dual-band (2.4GHz & 5GHz), so you'll likely get better speed by switching to the 5GHz band instead of the more commonly used and congested 2.4GHz band. Make sure your 5 GHz Wi-Fi is active at General > Network > Wi-Fi in the router's Web UI, and connect your Wi-Fi device or computer to the 5GHz band instead of 2.4GHz.

Network security

Your router is pre-set with the recommended WPA2 security type, but you should immediately change the default Wi-Fi password, as well as the Web UI login password. You can do so at General > Network > Wi-Fi and General > System Settings > Password & Timezone in the Web UI. It's not recommended to change Wi-Fi security type: WPA2 with AES is the most secure. And it's **never recommended** to disable Wi-Fi security (no security type), this means your network is open and anybody within range can connect by Wi-Fi.

8. Technical Specification

Memory

FLASH: NAND 256MB RAM: DDR4 1GB

Interface

Wireless 2.4GHz and 5GHz Dual-Band Concurrent
4 Gigabit LAN Port + One 2.5 Gigabit WAN Port

Standard

IEEE802.11a/b/g/n/ac/ax

IEEE802.3, 10BASE-T_e/100BASE-TX/1000BASE-T/2500BASE-T

Wireless Frequency Range

2.4 GHz: 2.412 GHz ~ 2.4835 GHz

5 GHz: 5.15 GHz ~ 5.35 GHz, 5.47 GHz ~ 5.85 GHz

Antenna

4-internal for 2.4 GHz

4-internal for 5 GHz

Maximum Output Power (with RF combine power)

29 dBm for 2.4 GHz

29 dBm for 5 GHz

Dimensions

W 100 x H 230.25 x D 150 mm

Button

Power, Reset to default, WPS

Indication

LED Indicators (2-color) Blue/Red

Operating Voltage

12V/2.5A DC adaptor (100V~240V, 50 Hz ~ 60 Hz)

Maximum Power Consumption

26.8 Watts

Temperature

Operating: 0oC ~ 40oC

Storage: -40oC ~ 85oC

Humidity

Operating: 5% ~ 90% RH

Storage: 5% ~ 95% RH