# **User Guide**

802.11ac Wave 2 Router

Model Number RAC2V1K



# Spectrum

# Table of Contents

	2
1 Hardware Setup	2
1.1 Getting To Know Your WiFi Router	
1.2 Unpack WiFi Router's box	3
1.3 Hardware Features	4
1.3.1 Front Panel	4
1.3.2 Rear Panel	5
1.4 Position Your WiFi Router	6

### 2 Login to your WiFi Router Web GUI

2.1 Login	7
2.2 Wizard Setup	
2.3 Basic Setup	
2.3.1 Router	
2.3.2 WPS Setup	
2.3.3 LAN Setup	
2.3.4 WAN Setup	
2.3.5 Parental Control	
2.3.6 Services	25
2.3.7 System	
2.4 Advanced Setup	
2.4.1 Network	
2.4.2 Services Config	66
2.4.3 Security	79
2.4.4 QoS	
2.4.5 Admin	
2.4.6 Tools	
2.4.7 Status	
	113
CC Statement	

# **1 Hardware Setup**

## 1.1 Getting To Know Your WiFi Router

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

WiFi Router provides:

- 1. High performance:
  - Dual-Core ARM up to 1.7G/1GB DDR RAM.
  - Dual-Band wireless up to AC2350 (2.4G 150M \* 4 + 5G 433M \* 4).
  - Gigabyte 1 x WAN/ 4x LAN Ethernet ports.
- 2. High security:

7

- 3. Easy to setup:
- 4. USB-based services: File/media/printer sharing. The WiFi Router is an ideal choice for residential and SMB (Small Business) users who can enjoy a variety of wireless applications and services.

This chapter contains the following contents:

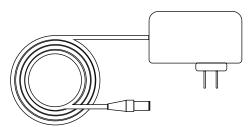
- Unpack Your WiFi Router
- Hardware Features
- Position Your WiFi Router

Firewall/VPN supported. Friendly wizard, visual setup & maintenance (Basic Mode), complete functions (Advanced Mode).

### 1.2 Unpack WiFi Router's box

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







Power Adapter

Figure 1. Check the package contents

The box contains the following items:

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

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

### **1.3 Hardware Features**

Before setup please take a moment to become familiar with the Front Panel and Rear Panel of your WiFi Router. Pay particular attention to the LED on the front panel. You should know the surface structure of your WiFi Router only.

### 1.3.1 Front Panel

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



Front panel LED status

- Off:
- Blue Flashing (0.4 second intervals):
- Blue Pulsing 1 second intervals:
- Blue solid:
- Red Flashing:
- Red and Blue alternate Pulsing: •
- Red solid:
- LED on front of device will dim to low (65%) when there is no settings activity or connectivity issues for 120 hours.
- brightness.

Figure 2. WiFi Router front view

Device off.

Booting up.

Connecting to Internet.

Connected to Internet.

Connectivity issues (no Internet connection).

Updating firmware (or any scenario where device must not be restarted).

Critical issues (hardware or otherwise).

• If any settings are changed or connectivity issues occur LEDs will return to normal (100%)

### 1.3.2 Rear Panel

There are Ethernet and USB connections and buttons shown in the following figure.



Figure 3. WiFi Router rear panel

•	Factory Reset (pinhole):	Press the pinhole and hold over 5 seconds, the WiFi Router will reset to factory.
•	WPS Button:	Push the button more than 1 second to activate WPS. Reference 2.3.2 WPS Setup.
•	Ethernet (LAN) Port:	Connect Ethernet cables for LAN (local area network) connections, e.g. network switch, hub, personal computer or Internet devices.
•	Internet (WAN) Port:	Connect Ethernet cable for WAN (Wide Area Network) connection to modem. This connects the Ethernet and other access lines e.g. modem.
•	USB (3.0) Port:	Connect a USB Printer, U-Disk or USB drive. For printer and folder sharing, reference 2.3.6 Services.
•	Power:	Use the bundled AC adapter to connect your WiFi Router to a power source.

# **1.4 Position Your WiFi Router**

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

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- •
- the WiFi Router and your other devices to a minimum.
- computers, the base of a cordless phone, or a 2.4 GHz cordless phone.
- concrete can also affect your wireless signal.

5

So it is accessible to an AC power outlet and near Ethernet cables for wired computers. In an elevated location such as a shelf, keeping the number of walls and ceilings between

Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves,

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

# 2 Sign-In Your WiFi Router Web GUI

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

# 2.1 Sign-In

- 1. Open a web browser, then key in the WiFi Router's default IP address: http://192.168.1.1, and click Enter key in the keyboard;;
- 2. On the sign in webpage, type in its Username and password: admin (admin), then click Login button.

# Spectrum-WiFi Router Username admin

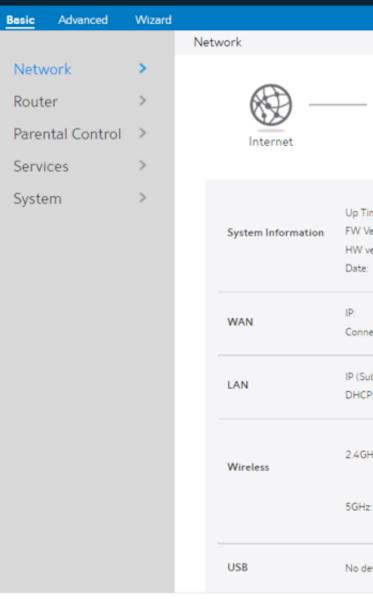
Password

After the administrator has logged into the WiFi Router, some basic information about	it wil
be displayed in the browser.	

Login

.....

# Spectrum



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

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

		a	d	m	in	
hange	Password	I	Le	ogo		

HELP





. . . .



ne:	OD OH 14M 41S
rsion:	1.0.11
ersion:	REV:1
	2018-03-15 20:41:11
	192.168.11.218
ction Type:	DHCP
onet Mask):	192.168.1.1(255.255.255.0)
	On
	WiFi Network Name: MySpectrumWiFi8d
Z	-2G WiFi Password: reasonanchor876
	WIFI Password: reasonanchor870
	WIFi Network Name: MySpectrumWiFi8d
	-5G WiFi Password: reasonanchor876
	WiFi Password: reasonanchor876

Basic	Advanced	Wizard				
			System			
Netw	vork	>				
Route	er	>	Change the Route	r Login Password		( HELP
Parer	ntal Control	>	Username	admin		C
Servi	ces	>	New Password			
Syste	m	>	Retype New Password		Show Password	
			Miscellaneous Time Zone Auto Logout	America/Denver	C Minutes (Disable: 0)	
			NTP Server(Maxir			
			NTP Ser	ver	Add/Delete	
					0	
			us.pool.nt	p.org	0	
			north-america.p	pool.ntp.org	.0	
			time.nist	.gov	0	
			pool.ntp	org	0	
				Apply		

On this page, user should just type in new password in New Password and Retype New Password, then click Apply button. Web GUI user sign in password will be changed.

### 2.2 Wizard Setup

The wizard can navigate the administrator to configure basic settings for the WiFi Router, which makes the set up of the WiFi Router much easier.

### **Internet Setup**

After the administrator has clicked the Wizard button, the Internet Setup page will be displayed.

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

Basic	Advanced	Wizard		
			Inter	net Setup
1   Int	ternet Setup			
2  Ne	etwork Setu	o	С	onnection Type
3   Co	onfig Overvi	ew	۲	DHCP DHCP allows your PC to obtain service providers.
			0	PPPoE ADSL or other connections that
			0	Static Static IP allows your PC to use a service providers.
			0	PPTP ADSL or other connections that
			0	L2TP L2TP requires a username,passe

 -		
	1	5

#### G HELP

n an IP address automaticIly. This connection type is often used by cable modem

at require a username and password are known as PPPoE.

a fixed IP address provided by your ISP. This connection type is often used by ADSL

at require a username, password and IP address are known as PPTP.

sword and IP address provided by your ISP.

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

WAN MAC		MAC Clone
Host Name		
Use WAN DNS		
DNS 1	10.7.46.1	
DNS 2	61.139.2.69	

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

### Network Setup

After you have clicked Next icon in Internet Setup page, you can come here or you will refer to the below picture.

Spectrum			admin Change Password   Logout
Basic Advanced <mark>Wizar</mark>	d		
	Network Setup		
1   Internet Setup			
2  Network Setup	2.4GHz		G HELP
3   Config Overview	WiFi Network Name	MySpectrumWiFi8d-2G	
	WiFi Password	reasonanchor876	
	<b>5GHz</b> Same as 2.4GHz WiFi Network Name WiFi Password	MySpectrumWiFi8d-5G reasonanchor876 Apply	

1. WiFi Network Name:

Name for a wireless network, that's to say it's used to identify the wireless network. WiFi devices automatically detect all networks within its communication range. These are defaulted from the printed WiFi network name on the back of the WiFi Router. You can change them here, but they would no longer match the sticker on your WiFi Router.

- - sticker on your router.
- 3. When done, click Apply.

#### Config Overview

After click the Apply icon, administrator comes to Config Overview page, which displays a summary of configuration information. If the settings are all correct, administrator should click Apply icon.

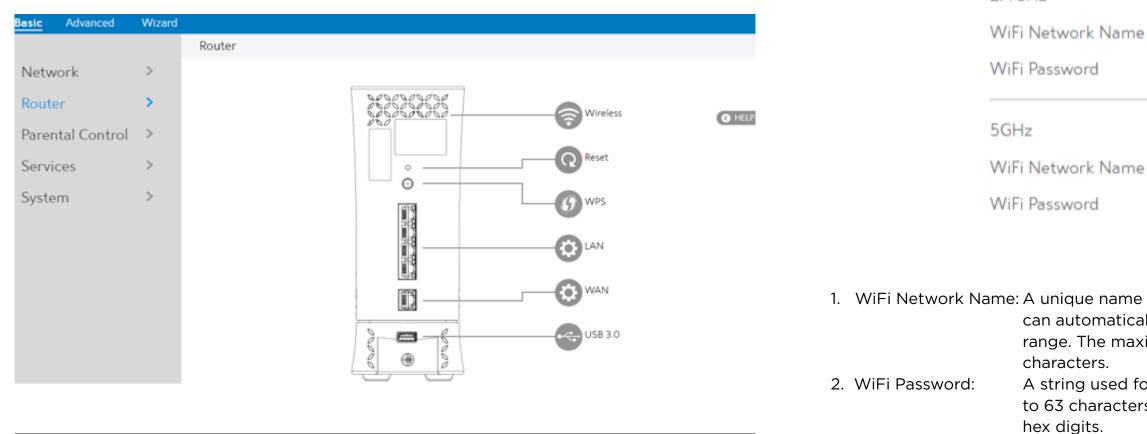
Spectrum			admin Change Password   Logout
Basic Advanced <u>Wizerd</u>			
	Config Overview		
1  Internet Setup			
2  Network Setup	Connection Type		G HELP
3  Config Overview	DHCP		
	DHCP Setting		
	WAN MAC		
	Host Name		
	Use Static DNS	No	
	DNS Server 1		
	DNS Server 2		
	2.4GHz		
	WiFi Network Name	MySpectrumWiFi8d-2G	
	WiFi Password	reasonanchor876	
	5GHz		
	WiFi Network Name	MySpectrumWiFi8d-5G	
	WiFi Password	reasonanchor876	

2. WiFi Password: A password used by WiFi Router to authenticate wireless connections. These are defaulted from the printed WiFi password on the back of the WiFi Router. You can change it here, but they would no longer match the

### 2.3 Basic Setup

### 2.3.1 Router

From the navigation panel, go to Basic > Router.



NOTE: Click Reset Icon in the Web GUI is used to restart the WiFi Router. The WiFi Router hardware Factory Reset (pinhole) was pressed and hold over 5 seconds, it will reset to factory.

3. Click Apply.

Wireless:

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

Wireless

2.4GHz

WiFi Network Name

	anchor870	4	
reason	anchorozo	5	
MySpe	ctrumWiF	i8d-5G	
reason	anchor87	6	

1. WiFi Network Name: A unique name that identifies the wireless network. Wireless device can automatically detect all networks within its communication range. The maximum length of a network name (SSID) is 32

> A string used for connection authentication. Its length ranges from 8 to 63 characters (letters, numbers or a combination) or from 8 to 64

### 2.3.2 WPS Setup

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

Frequency	2.4GHz
Enable WPS	On
Connection Status	WPS-ENROLLEE-SEEN
Configured	Yes
AP PIN Code	10625958
WPS Method	Push Button O Client PIN Code
PIN Code	

- 8. PIN Code: The WPS PIN code which clients use to connect with the WiFi Router.
- go to step 10. If you select Client PIN code, go to step 11.
- 10. Using with WPS button please following these steps:

  - logo.
- 11. To set up WPS using the Client's PIN code, follow these steps:
  - a) Locate the WPS PIN code in wireless device's in Web GUI.
  - b) Key in the Client PIN code on the text box.
- 12. Click Start.

Steps to enable WPS (WiFi Protected Setup):

- 1. From the navigation panel, go to Basic > Router.
- Selecting operating band (2.4 GHz or 5 GHz) for WPS function. Each 2. Frequency: one is enabled separately.
- Selecting [On] to run WPS, which simplifies the process of connecting 3. Enable WPS: any device to the WiFi network.

NOTE: Authentication method supported by WPS is: WPA2-Personal. Not supported methods are: Shared Key, WPA-Enterprise, WPA2-Enterprise and RADIUS.

9. In the WPS Method field, select Push Button or Client PIN code. If you select Push Button, a) Click Start or press the WPS button located on at the rear of the WiFi Router. b) Press the WPS button on your wireless device. This is normally identified by the WPS

### 2.3.3 LAN Setup



LAN	
LAN IP	192.168.1.1
Subnet Mask	255.255.255.0
✓ DHCP Server	
	Apply

Steps to modify LAN IP settings:

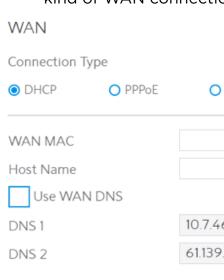
- 1. From the navigation panel, go to Basic > Router.
- 2. LAN IP: The LAN IP address of the WiFi Router. Its default value is 192.168.1.1. In IP-based networks, packets are sent to the network devices' specific IP addresses.
- 3. Subnet Mask: Subnet mask of WiFi Router. Its default value is 255.255.255.0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

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

5. Click Apply.

### 2.3.4 WAN Setup

Click WAN button to configure the WAN connection settings: 1. Connection Type: Choose the Internet Service type. There are five options are DHCP, PPPoE, Static, PPTP and L2TP. Consult your ISP if you are unsure what kind of WAN connection types to select.





- 2. If you select DHCP, below show the steps to set
- WAN MAC:
- Internet connection for new MAC addresses.

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

- subscription.
- original device.
- Host Name: provided by ISP.
  - DNS1&DNS2:
- Click Apply.

Static	O PPTP	O L2TP
		MAC Clone
6.1		
.2.69		
Apply		

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

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

• Clone or change the MAC address of the new device to match the MAC address of the

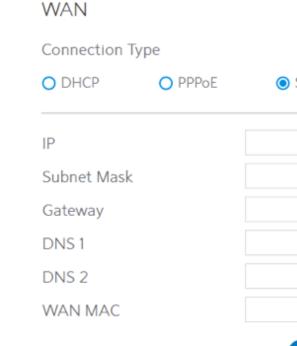
This field lets you provide a host name for WiFi Router. Usually it's

Either of them indicates IP address of a DNS server.

### 3. If you select PPPoE, below show the steps to set

Connection <sup>-</sup>	Туре			
O DHCP	PPPoE	O Static	O PPTP	O L2TP
Username				
Password				Show Password
Connect to [	ONS Server	Yes O No		
DNS 1				
DNS 2				

4. If you select Static, below show the steps to set



- Username: This field is only available when you set the WAN Connection Type as PPPoE, PPTP or L2TP.
- Password: This field is only available when you set WAN Connection Type as PPPoE, PPTP or L2TP.
- DNS1 & DNS2: Either of them indicates IP address of a DNS server that WiFi Router will contact.
- Click Apply.

NOTE: All of the parameters mentioned above are provided. If you need assistance, please contact Charter customer service.

- IP: this field. • Subnet Mask: this field. • Gateway:
  - address in this field.
- DNS 1 & DNS 2: Either of them indicates IP address of a DNS server.
- WAN MAC: 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.
- original device.
- Click Apply.

Static	O PPTP	O L2TP
		MAC Clone
Apply		

If WAN connection requires a static IP address, key in the IP address in

If WAN connection requires a static IP address, key in the subnet mask in

If WAN connection requires a static IP address, key in the gateway IP

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

• Clone or change the MAC address of the new device to match the MAC address of the

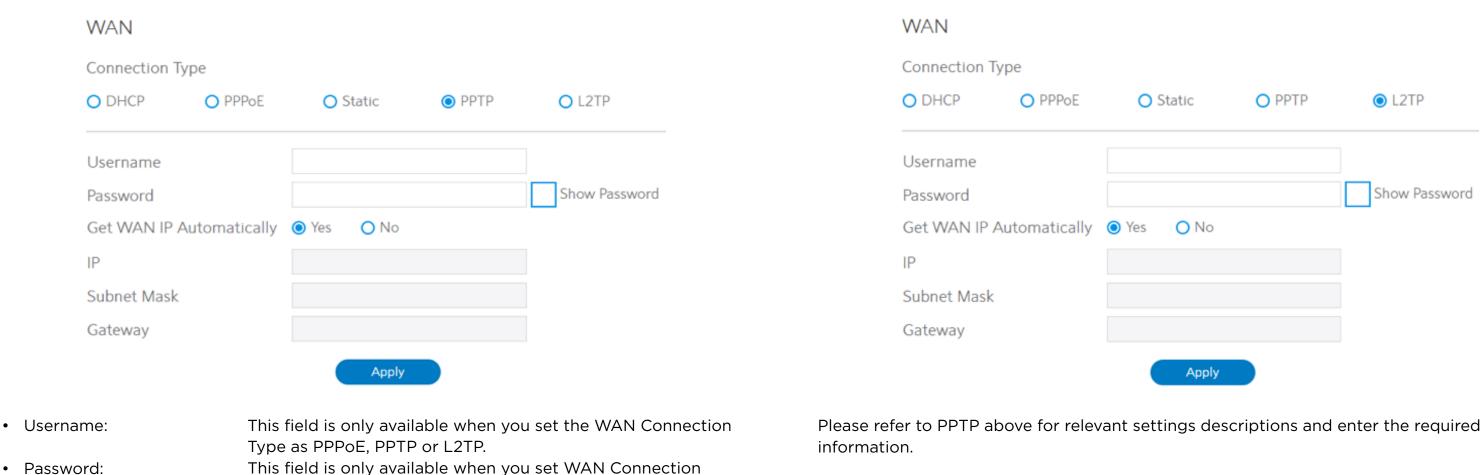
#### 5. If you select PPTP, below show the steps to set

• IP:

• Subnet Mask:

• Gateway:

Click Apply.



If WAN connection requires a static IP address, key in the IP

If WAN connection requires a static IP address, key in the

If WAN connection requires a static IP address, key in the

Type as PPPoE, PPTP or L2TP. • Get WAN IP Automatically: Select Yes to get WAN IP automatically and No to enter IP

manually below.

address in this field.

subnet mask in this field.

gateway IP address in this field.

itatic	О РРТР	● L2TP
		Show Password
O No		
Apply		

### 2.3.5 Parental Control

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

Basic Advanced	Wizard		
		Parental Control	
Network	>		
Router	>		Parent Control allows you to control the Internet access of the child client you add in. To use Parent Control:
Parental Control	>		1. You can select and add client by drop-down list of [Client Name] column.
Services	>		<ol> <li>Click the plus(+) icon in [Add/Delete] column to add the client you select.</li> <li>You can add schedule in the [Time Management] column. If not, the default action is to use the filters all the time.</li> </ol>
System	>	9	<ol> <li>Select the desired time slots for allowed access times. Drag and hold to create longer time slots.</li> </ol>
			<ol> <li>If you add no filter(url/keyword/service), the default action is to allow all packets passthrough.</li> <li>Click [Confirm] to save the new settings.</li> </ol>
		Enable Parental Co	ntrol On
		System time	Sun Feb 12 22: 51: 50 2017

### Client & Schedule List (Maximum: 16)

Client Name	Client MAC	Time Management	Add / Delete
\$		-	Φ

### URL Filter List (Maximum: 16)

URL Filter	Add / Delete
	0

### Keyword Filter List (Maximum: 16)

Keyword Filter	Add / Delete
	0

### Service Filter List (Maximum: 16)

Port Range	Protocol		Add / Delete
	ТСР	0	Φ
	Apply		

Steps to set parental control function:

- 1. From the navigation panel, go to Basic > Parental Control.
- 2. Enable Parental Control: Select On to enable parental control, Select Off to disable parental control.
- 3. Client & Schedule List: communicating with the WiFi Router.
  - •Client MAC: MAC address of the selected client.

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

- client's access to Internet.
- •Add/Delete: Click or to add/delete the profile.
- 4. URL Filter List

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

•Client Name: Select client from the list. The name in the list stands for the client that is

•Time Management: Click , then setup the client's schedule timetable to allow or deny

•URL Filter List: WiFi Router prevents LAN-side device from accessing the URL in list.

•Keyword Filter List: WiFi Router prevents LAN-side device from accessing to webpages

•Keyword Filter: WEB URLs which contain the keywords defined by user. For example, the

•Port Range: Defines the range of port in LAN side. The Port Range can be a single port

### 2.3.6 Services

### 2.3.6.1 USB Printer Sharing

USB Printer sharing lets administrator plug a USB printer to WiFi Router's USB port and set up the printer server.

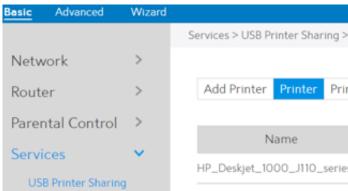
#### Basic Advanced Wizard Services > USB Printer Sharing > Add Printer > Network Add Printer Printer Print Jobs Router > O HELP Parental Control > Available Printers Services $\sim$ USB Printer Sharing HP Deskjet 1000 J110 series

Steps to set up USB Printer sharing:

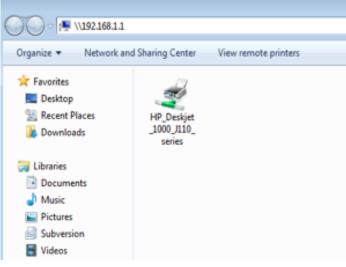
- 1. From the navigation panel, go to Basic > Service > USB Printer sharing.
- 2. Plug in the USB interface of the printer to the WiFi Router. Confirm your printer has been detected and click Continue.
- 3. Select one of the following modes to install the printer driver, and click Add printer.
- Auto select: Automatically searches for the appropriate printer driver and installs. If there is no corresponding printer driver, the system displays add a printer error; please select the correct printer driver manually.
- Select printer driver: Manually select the corresponding Printer brand and model.
- Choose PPD File: If the above methods are unable to correctly install the printer driver, then you can upload a PPD File. Select your PPD file and click the upload button.

Basic Advanced	Wizard			
		Services > USB Printer Sharing	> Add Printer	
Network	>			
Router	>	Add Printer Printer Pr	int Jobs	G HELP
Parental Control	>			G HEDP
Services	~	Available Print	ers	
USB Printer Sharin	g	Name	HP_Deskjet_1000_J110_series	
FTP Server		Description	HP_Deskjet_1000_J110_series	
Samba		Choose Model	HP Deskjet 1000 j110 Serie 🗘	
WebDAV			The Deskjet 1000 Jillo Serie V	
DLNA			Add Printer	
AFP			Additimet	

below.



for the printer in Windows Finder.



6. Double-click the printer icon and if you see the status interface as shown below, the then return to Add Printer settings and select the correct driver.

🖶 HP_Deskjet_1000_J110_series on 192.168.1.1					
Printer Document View					
Document Name	Status	Owner	Pages	Size	Sut
•					•
					÷t.

4. Printer tab displays whether your printer is operating correctly with the print server, as

Pri	nter			
nt Jo	obs			G HELP
	Details	Status	Operation	
s	HP_Deskjet_1000_J110_series	Idle	/0	

5. To check whether your printer is working correctly or not, input the LAN address (192.168.1.1)

	-	×
• 49 Search 192.168.1.1		Q
	•	0

installation was successful. If an error message prompts that the driver cannot be found,

#### 7. You can view print status information in the Print Jobs tab.

Basic	Advanced	Wizard		
			Services > USB Printer Sharing > Print Jobs	
Netw	vork	>		
Route	er	>	Add Printer Printer Print Jobs	HELP
Parer	ntal Control	>		
Servi	ces	×	Search	
US	B Printer Sharing	1	All Jobs	
FTF	P Server			
Sar	nba		Print Jobs List	
We	bDAV		PRINTER SIZE FILENAME STATUS CONTROL	L
DU	NA			

- All active jobs, including processing and pending jobs. Active:
- Processing: The job currently processing/communicating print data.
- All Jobs: All print jobs.

### 2.3.6.2 FTP

FTP Server enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet. This page shows information about the FTP Server and enable or disable it. If you want to set more configurations, please go to Advanced > Servers > FTP.

Basic	Advanced	Wizard	
			Services > FTP Server
Netw	vork	>	
Route	er	>	Generic_UDISK
Parer	ntal Control	>	Kingston_DataTraveler_3
Servi	ces	×	
US	B Printer Sharing	,	FTP
FTF	Server		Enable FTP
Sar	nba		
We	bDAV		Maximum number of Conne
DL	NA		Enable Outside Access
AFI	p		Outside Access
NF	S		Local Access Method
Syste	m	>	Outside Access Method

Display information on FTP Server:

- 1. From the navigation panel, go to go to Basic > Services > FTP.
- 2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your device will be displayed here.
- 3. Enable FTP:

6. Outside Access:

7. Safely Remove Disk:

- Click On/Off to enable/disable Internet access to FTP service.
- 4. Maximum number of Connections: The maximum number of concurrent connections for the Network Neighborhood or FTP Server.
- 5. Enable Outside Access:
- Select On/Off to enable/disable access to FTP server by wide area network.
- The numbers of external service ports
- (default value: 8021).
- Click to safely remove USB devices. When the USB disk is ejected successfully, the USB status shows 'No device '.

_0		Safely Remove Disk
	On	
ections	20	
	Yes	
	8021	
	ftp://192.168.1.1	
	ftp://10.8.4.187:8021	

### 2.3.6.3 Samba

Samba Share lets you set up the accounts and permissions for the Samba service. This page shows information about the Samba Server and enable or disable it. If you want to set more configurations, please go to Advanced > Servers > Samba.

Basic Advanced	Wizard			
		Services > Samba		
Network	>			
Router	>	SanDisk_Extreme	Safely Remove Disk	( HELP
Parental Control	>	Kingston_DataTraveler_	.3_0 Safely Remove Disk	
Services	×	This setting has already been cor	nfigured in Advanced Settings. You can view the details in Advanced Settings.	
USB Printer Sharing	3	Samba		
FTP Server		Salliba		
Samba		Enable Share	On	
WebDAV		Device Name	RAC2V1K	
DLNA		Work Group	Workgroup	
AFP		Account	admin	
NFS		Samba Access Path	\\192.168.1.1	
System	>			

- From the navigation panel, go to Basic > Services > Samba.
- Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your device will be displayed here.
- Enable Share: Click the On/Off to enable/disable Internet access to Samba service.
- Device Name: Enter a name for your device and you can use this name in your web browser's URL field to quickly access the device as a Network Place service.
- Work Group: Group name of the WiFi Router in Network Neighborhood.
- Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.

### 2.3.6.4 WebDAV

The client can write operations in WebDAV directory with appropriate permissions. This page shows information about the WebDAV Server and enable or disable it. If you want to set more configurations, please go to Advanced > Servers > WebDAV.

asic Advanced	Wizard		
		Services > WebDAV	
Network	>		
Router	>	Generic_UDISK	
Parental Control	>	Kingston_DataTraveler_3_0	
Services	<b>v</b>		
USB Printer Sharing	3	WebDAV	
FTP Server		Enable WebDAV	On
Samba		HTTP Access Port	80
WebDAV DLNA		HTTPS Access Port	443
AFP		Enable Outside Access	Yes
NFS		Outside Access HTTP	8080
System	>	Outside Access HTTPS	8443
		LAN	
		WebDAV HTTP Access Path	http://192.168.1.1:80/UUU
		WebDAV HTTPS Access Path	https://192.168.1.1:443/UUU
		WebDAV HTTP Access Path	http://192.168.1.1:80/BING
		WebDAV HTTPS Access Path	https://192.168.1.1:443/BING

WebDAV HTTP Access Path WebDAV HTTPS Access Path WebDAV HTTP Access Path WebDAV HTTPS Access Path

- 1. From the navigation panel, go to Basic > Services > WebDAV.
- 2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your device will be displayed here.
- 3. HTTP Access Port:
- 4. HTTPS Access Port:
- 5. Enable Outside Access: Select On/Off to enable/disable access to WebDAV server by wide area network.

The port to access the WebDAV server for HTTP protocol in the

The port to access the WebDAV server for HTTPS protocol in the

local area network (default value: 80).

http://10.8.4.187:8080/UUU

https://10.8.4.187:8443/UUU

http://10.8.4.187:8080/BING

https://10.8.4.187:8443/BING

local area network (default value: 443).

30

- 6. Outside Access HTTP: The port number of external service ports via HTTP (default value: 8080).
- 7. Outside Access HTTPS: The port number of external service ports via HTTPS (default value: 8443).
- Click to safely remove the disk. When the USB disk is ejected 8. Safely Remove Disk: successfully, the USB status shows 'No device '.

### 2.3.6.5 DLNA

DLNA (Digital Living Network Alliance) lets you share audio, image and video. Your WiFi Router lets DLNA-supported devices access multimedia files from the USB disk connected to your WiFi Router. This page shows information about the DLNA Server and enable or disable it. If you want to set more configurations, please go to Advanced > Servers > DLNA.

Basic Advanced	Wizard	
		Services > DLNA
Network	>	
Router	>	TOSHIBA_TransMemory
Parental Control	>	
Services	~	DLNA
USB Printer Sharii	ng	Enable DLNA Media Server
FTP Server		Media Server Name
Samba		
WebDAV		
DLNA		

Steps to set DLNA:

- 1. From the navigation panel, go to Basic > Services > DLNA.
- device will be displayed here.
- 3. Enable DLNA Media Server: Switch DLNA media server on or off.
- 4. Media Server Name:

5. Safely Remove Disk:

The DLNA server's name, which will be displayed by the media player such as VLC or Windows Media Player. Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.

		Safely Remove	Disk	G HELP
On				
DLNA server on	RAC2V1K			

2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your

### 2.3.6.6 AFP

An AFP server is a kind of network file sharing server based on AFP protocol implementation, mainly used for file sharing between Linux and MAC systems. This page shows information about the AFP server and enable or disable it. If you want to set more configurations, please go to Advanced > Servers > AFP.

Basic	Advanced	Wizard			
			Services > AFP		
Netw	vork	>			
Route	er	>	Generic_UDISK		Safely Remove Disk
Parer	ntal Control	>	Kingston_DataTraveler_3_0	)	Safely Remove Disk
Servi	ces	×			
US	B Printer Sharing	1	AFP		
FTF	Server		Enable Share	On	
Sar	nba				
We	bDAV		AFP Access Path	afp://192.168.1.1	
DLI	NA				

### Steps to set AFP:

- 1. From the navigation panel, go to Basic > Services > AFP.
- 2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your device will be displayed here.
- 3. Enable Share: Click On/Off to enable/disable AFP service.
- 4. Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.

### 2.3.6.7 NFS

Network File System Server is used to share the USB disk with clients via network. Clients can mount the remote disk to a local directory for a faster speed than using a Samba server. This page shows information about the NFS Server and enable or disable it. If you want to set more configurations, please go to Advanced > Servers > NFS.

Basic Advanced	Wizard	
		Services > NFS
Network	>	
Router	>	Generic_UDISK
Parental Control	>	Kingston_DataTraveler_3_
Services	<b>~</b>	
USB Printer Sharing	1	NFS
FTP Server		Enable NFS
Samba		Enable Ni 5
WebDAV		
DLNA		
AFP		
NFS		

### Steps to set NFS:

- 1. From the navigation panel, go to Basic > Services > NFS.
- 2. Connect an external USB hard disk drive or USB flash drive to the WiFi Router, then device's name will be displayed here.
- 3. Enable NFS: USB storage via the NFS service.
- 4. Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected

_0			ly Remove Disk ly Remove Disk	G HELP
	On			

Enable or disable NFS service. When disabled, users can't access the

successfully, the USB status shows 'No device '.

### 2.3.7 System

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

Basic Advanced	Wizard						
		System					
Network	>						
Router	>	Change the Router Login Password					
Parental Control	>	Username	admin		( HELP		
Services	>	New Password					
System	>	Retype New Password		Show Password			
		Miscellaneous	America (Denous				
		Time Zone	America/Denver	0			
		Auto Logout	5	Minutes (Disable: 0)			
		NTP Server (Maxir	num:6)				
		NTP Ser	ver	Add/Delete			
				0			
		us.pool.nt	p.org	0			
		north-america.p	ool.ntp.org	0			
		time.nist.	gov	0			
		pool.ntp.	org	0			
			Apply				
Steps to set th 1. From the na 2. Username:		m settings: on panel, go to Basic > Sys Name used to sign ir					

- 3. New Password: New sign in password for WiFi Router.
- 4. Retype New Password: Retype new sign in password for WiFi Router.
- The time zone used by default. 5. Time Zone:

6. Auto Logout: Auto sign out after a specified period of time.

7. NTP Server: DNS of a NTP (Network Time Protocol) server.

8. Click Apply.

## 2.4 Advanced Setup

### 2.4.1 Network

### 2.4.1.1 WAN Settings

## 2.4.1.1.1 Internet Settings

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

asic Advanced	Wizard	
		Network > WAN > Internet
Network	×	
WAN		Internet DDNS UPnP
LAN		
Wireless		Basic
IPv6		Dasic
Parental Control		WAN Connection Type
Multicast		MTU
Routing		
Services Config	>	WAN DNS Sett
Security	>	Connect to DNS Server
QoS	>	DNS 1
Admin	>	DNS 2
ools	>	
itatus	>	Account Setting
		Authentication
		Username
		Password
		Special Require
		Host Name
		MAC Address
		DHCP Query Frequency

Port Trigg	ering	Port Forwarding	DMZ	NAT Pass Through	
					( HELP
	DHC	P	0		
	1280		~		
	1280				
ings					
	Yes	O No			
	10.7.4				
	61.13	9.2.69			
gs					
0	• • •	• • • • • • • •			
	<ul><li>No</li></ul>	ne 🔿 802.1x ME	)5		
ement					
ement					
				MAC Clone	
	Aar	active Made			
	Agre	essive Mode		\$	
		4-1-			
		Apply			

Steps to configure WAN connection settings:

- 1. From the navigation panel, go to Advanced > Network > WAN > Internet.
- 2. WAN Connection Type: Choose the Internet Service Provider type. There are 5 options: DHCP, PPPoE, Static, PPTP and L2TP. If you are unsure which type to select, please consult your ISP.
- 3. MTU: Maximum Transmission Unit value, which defines the maximum length of a packet. 4. Connect to DNS Server: Lets WiFi Router get IP address from the DNS Server
  - automatically. DNS Server is a host on the Internet that translates Internet names to numeric IP addresses.
- 5. Get WAN IP Automatically: Select Yes to get WAN IP automatically and No to enter IP manually below. 6. IP Address: If your WAN connection requires a static IP address, key in the
- IP address in this field. 7. Subnet Mask: If your WAN connection requires a static IP address, key in the subnet mask in this field.
- 8. Default Gateway: If your WAN connection requires a static IP address, type in the gateway IP address in this field.
- 9. DNS 1 & DNS 2: Either of them indicates an IP address of a DNS server.
- 10. Authentication: Use 802.1x MD5 authentication or not (IEEE 802.1x is an IEEE Standard for port-based Network Access Control).

Username for 802.1x MD5 authentication.

Password for 802.1x MD5 authentication.

PPTP Encryption method. Select Auto for automatic Microsoft

- 11. Username:
- 12. Password:
- 13. PPTP Options:
  - Point-to-Point Encryption (MPPE) and select No Encryption to disable MPPE. Select MPPE 40 for 40-bit MPPE with PPTP
    - Server and select MPPE 128 for 128-bit MPPE with PPTP Server.
- 14. Access Concentrator Name: Specifies the Access Concentrator to connect to. If unset, pppd uses the first discovered one.
- 15. Additional Pppd Options: Additional command line arguments to pass to the pppd daemon.
- 16. Host Name: This field lets you provide a host name for your WiFi Router. It is usually provided by ISP.
- 17. MAC Address: MAC address identifies a device in the network. ISPs monitor the MAC addresses of devices that connect to their services, and would disallow Internet connection for new MAC addresses.
  - To fix this issue, you can do either of the following:
  - Contact your ISP and request to update the MAC address associated with your ISP subscription.
  - · Clone or change the MAC address of the new device to match the MAC address of the original device.

19. Enable Default Route:

20.VPN Server:

21. Click Apply.

18. DHCP Query Frequency: Some ISP blocks MAC addresses if the device makes DHCP gueries too often. To prevent this, change the DHCP Query Frequency. In the default Aggressive mode, if your WiFi 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 your WiFi Router does not get a response from the ISP, it makes a second query after 120 seconds and makes two more attempts. Whether to create a default route over the tunnel. IP address or DNS for VPN server.

### 2.4.1.1.2 DDNS

DDNS(Dynamic DNS)makes administrator can get access to WiFi Router even though it's working within a local network.

Basic	Advanced	Wizard						
			Network > WAN > DDNS					
Netwo	rk	×						
WAN			Internet DDNS UPnP	Port Triggering	Port Forwarding	DMZ	NAT Pass Through	
LAN								( HELP
Wirel	ess		D					
IPv6			Basic					
Paren	tal Control		Enable the DDNS Client	Yes	O No			
Multi	cast		Server	WWW	dyndns.com	\$	Vendor Website	
Routi	ng		Host Name	Enter	the name.			
Service	es Config	>	Username or E-mail Addres	SS				
Securit	ty	>	Password or DDNS Key					
QoS		>						
Admin		>			Apply			

Steps to set up DDNS:

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

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

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

### 2.4.1.1.3 UPnP

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

Basic	Advanced	Wizard							
			Network > WAN > UPnP						
Netw	vork	×							
WA	AN		Internet DDNS UPnP Port	Triggering	Port For	warding	DMZ	NAT Pass Through	
LA	N								( HELP
Wi	reless		Desta						
IPv	6		Basic						
Par	rental Control		Enable UPnP	Yes	O No				
Mu	ulticast		Advertisement Period	30		Seconds			
Ro	uting		Advertisement Time To Live	2		hops			
Servi	ices Config	>							
Secu	rity	>			Apply				

### Steps to set up UPnP:

- 1. From the navigation panel, go to Advanced > Network > WAN > UPnP.
- 2. Enable UPnP:
- 3. Advertisement Period:

- 4. Advertisement Time To Live: Number of hops that an advertisement will be transmitted.
- 5. Click Apply.

- Yes means enable UPnP and No means disable it.
- WiFi Router will broadcast its UPnP information to all devices every advertisement-period seconds.

### 2.4.1.1.4 Port Triggering

Port triggering mechanism forwards the packets from the Incoming Port to the local client when the local client makes an outgoing connection through a predetermined port/port range (Triggering Port).

Basic <u>Advanced</u>	Wizard	
		Network > WAN > Port Triggering
Network	×	
WAN		Internet DDNS UPnP Port Triggering Port Forwarding DMZ NAT Pass Through
LAN		
Wireless		Basic
IPv6		DASIC
Parental Control		Enable Port Triggering O Yes O No
Multicast		Well-Known Applications Please Select 0
Routing		
Services Config	>	Port Triggering List (Maximum: 32)
Security	>	Description Trigger Port Local IP Protocol Incoming Port Operation Operation
QoS	>	C TCP C TCP C
Admin	>	Apply

Steps to set up Port Triggering:

- 1. From the navigation panel, go to Advanced > Network > WAN > Port Triggering.
- 2. Enable Port Triggering: Check to enable or disable Port Triggering.
- 3. Well-Known Applications: Select popular games and web services to add to the Port Triggering List.
- 4. Description: A brief description for application.
- 5. Triggering Port: When there is incoming data from LAN-side application to this port, the Port Triggering mechanism will be activated.

Defines the range of port. After Port triggering mechanism has

been activated, the data from port within this range will be

forwarded to the corresponding port of the application which

- 6. Local IP: Local host's IP address. Select the type of protocol that the application will use.
- 7. Protocol:
- 8. Incoming Port:
- 9. Operation:

10. Click Apply.

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

has activated Port triggering mechanism.

Add, Edit or Delete operation for this item.

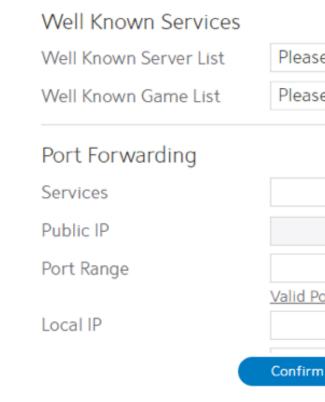
### 2.4.1.1.5 Port Forwarding

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

Basic	Advanced	Wizard				
			Network > W	/AN > Por	t Forwa	rdi
Netv	vork	~				
W	AN		Internet	DDNS	UPnP	P
LA	N					
W	reless		Port F	orwa	ardin	q
IPv	6			_		
Par	rental Control		Servio	es	Public	: IP
Mu	ulticast					

### Steps to set up Port Forwarding:

- 1.
- 2. Click the Add button to add the port forwarding rules.



ding							
Port Triggering	Port Forwarding	DMZ	NAT	Pass Th	rough	_	
						0 H	ELP
g List (Max	ximum: 128)				A	dd	
IP/Port	Local ID /Dort	Proto	col	Status	Oneret	tion	
IP/POIL	Local IP/Port	Proto	COI	Status	Operat	tion	
	Apply						

From the navigation panel, go to Advanced> Network> WAN>Port Forwarding.

		<b>^</b>
ase Select	$\hat{}$	
ase Select	$\odot$	
	0	1
l Port Range		
	0	
		*

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

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

8. Local IP: The client's LAN IP address.

- 9. Local Port: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
- 10. Protocol: The required protocol. Refer to the documentation for the service that you are hosting.
- The status of this rule, on or off. 11. Status:
- 12. Operation: Edit or Delete operation for this rule.
- 13. Click Apply

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

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

Differences between port triggering and port forwarding:

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

## 2.4.1.1.6 DMZ

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

CAUTION: Opening all of the client's ports to outside attacks. Please be aware

Basic	Advanced	Wizard		
			Network > WAN > DMZ	
Netv	vork	~		
W	AN		Internet DDNS UPnP	
LA	N			
Wi	reless		Pasia	
IPv	6		Basic	
Par	rental Control		Enable IPv4 DMZ	
Mu	ulticast		IP Address of Exposed Stati	C
Ro	uting		Enable IPv6 DMZ	
Serv	ices Config	>	IPv6 Address of Exposed St	а
Secu	rity	>	IPv6 prefix for DMZ setting	
QoS		>		
Adm	in	>		

Steps to set up DMZ:

- 1. From the navigation panel, go to Advanced > Network > WAN > DMZ.
- 2. Enable IPv4 DMZ:
- - address.
- 4. Enable IPv6 DMZ:

				vulnerable to in using DMZ	
Port Triç	ggering	Port Forwarding	DMZ	NAT Pass Through	( HELP
on	Yes	O No			
ation	Yes	O No			
	No pre	fix for ipv6 DMZ set	ting!		

Check to enable or disable DMZ.

3. IP Address of Exposed Station: LAN IP address of a client who can provide DMZ service. This makes the device with this IP address expose to Internet. Make sure that the server client has a static IP

Check to enable or disable IPv6 DMZ.

5. IPv6 Address of Exposed Station: The client's LAN IPv6 address that will provide the DMZ service and be exposed on the Internet.

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

### 2.4.1.1.7 NAT Pass Through

Router to the network server.

		Network > W		T Pass T	brough					
		Network > W	AN ZINA	I Fd55 I	mougn					
Network	~									
WAN		Internet	DDNS	UPnP	Port Triggerin	g Por	t Forwarding	DMZ	NAT Pass Through	_
LAN										(0 H
Wireless		Decie								
IPv6		Basic								
Parental Control		PPTP Pass	through		En	able		;		
Multicast		L2TP Pass	through		En	able		;		
Routing		IPSec Pass	through		En	able		(		
Services Config	>	SSL Passth	rough		En	able		:		
Security	>	RTSP Pass	through		En	able		:		
QoS	>	H.323 Pas	sthrough		En	able		;		
Admin	>	SIP Passth	rough		En	able		;		
		NORM Pas	sthroug	h	En	able		;		
Tools	>	Enable PPI	PoE Relay	/	Di	able		(		
Status	>									

Steps to set up NAT Pass Through:

- Through.
- 2. PPTP Passthrough: Enable or disable. Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. 3. L2TP Passthrough: Enable or disable. In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private

- 4. IPSec Passthrough: Enable or disable. Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
- communications security over a computer network. 6. RTSP Passthrough: Enable or disable. The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

### NAT Pass Through lets a Virtual Private Network (VPN) connection pass through the WiFi

1. To configure NAT Pass Through settings, go to Advanced > Network > WAN > NAT Pass

- networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself.
- 5. SSL Passthrough: Secure Sockets Layer(SSL) is cryptographic protocols that provide

- 7. H.323 Passthrough: Enable or disable. H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network.
- 8. SIP Passthrough: Enable or disable. The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging all over Internet Protocol (IP) networks.
- 9. NORM Passthrough: Enable or disable. NACK-Oriented Reliable Multicast (NORM) Transport Protocol, which is able to provide end-to-end reliable transport of bulk data objects or streams over generic IP multicast routing and forwarding services.
- 10. Enable PPPoE Relay: PPPoE relay lets devices in LAN establish an individual PPPoE connection that passes through NAT.
- 11. When done, click Apply.

### 2.4.1.2 LAN Settings

### 2.4.1.2.1 LAN

The LAN IP module lets administrator modi

Basic	Advanced	Wizard	
			Network > LAN > LAN IP
Netw	vork	×	
WA	AN .		LAN IP DHCP Server
LA	N		
Wi	reless		D
IPv	6		Basic
Par	ental Control		IP Address
Mu	lticast		Subnet Mask
Roi	uting		
Servi	ces Config	>	

Steps to modify the LAN IP settings:

- 1. From the navigation panel, go to Advanced > Network > LAN > LAN IP.
- addresses.
- 4. Click Apply.

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

fy LAN-	-side IP ad	dress of	the rout	ter.	
					( HELP
	192.168.1.1				
	255.255.255.	D			
	Apply				

2. IP Address: The LAN IP address of WiFi Router. The default value is 192.168.1.1. In IPbased networks, data packets are sent to the network devices' specific IP

3. Subnet Mask: The LAN subnet mask of WiFi Router. Its default value is 255.255.255.0

### 2.4.1.2.2 DHCP Server

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

Basic	Advanced	Wizard					addro
			Network > LAN > DHCP Server				eithe
Net	work	×				<ol> <li>Default Gateway:</li> <li>8. DNS Server:</li> </ol>	IP ad IP ad
v	VAN		LAN IP DHCP Server			8. DNS Server.	into a
L	AN				G HELP		as a l
v	Vireless					9. WINS Server:	Winc
15	Pv6		Basic				each
P	arental Control		Enable DHCP Server	🖲 Yes 🔵 No			Addr
N	fulticast		Domain Name	lan1		10. Enable Manual:	Assig
R	outing		IP Pool Starting Address	192.168.1.2		11. MAC: 12. IP:	MAC IP ad
Ser	vices Config	>	IP Pool Ending Address	192.168.1.254		13. Add/Delete:	Add/
	-		-			14. Click Apply.	,
Sec	urity	>	Lease Time	604800			
Qo	S	>	Default Gateway	192.168.1.1			
Adr	nin	>					
Тоо	lc	>	DNS and WINS S	erver		NOTES:	
			DNS Server	192.168.1.1		<ul> <li>We recommend the</li> </ul>	at administra
Sta	tus	>		192.108.1.1		can be any numbe	
			WINS Server			An IP Pool Starting	9 Address sho
			Static IP Assignm	ent within DHCP IP Pool	(Maximum:		
			64)				
			Enable Manual	O Yes			
				Apply			

Steps to configure the DHCP server:

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

49

Domain Name for clients who request IP Address from DHCP Server. This field only contains alphanumeric characters and

4. IP Pool Starting Address: Starting address that can be allocated to LAN-side devices. 5. IP Pool Ending Address: Ending address that can be allocated to LAN-side devices. Defines the time that LAN-side devices can use the assigned IP ess. When the lease time expires, the network client will er send renew or rebind message to a DHCP server. Idress of the gateway for LAN.

Idress of a DNS server. DNS Server is used to resolve a DNS a numerical IP Address. By default, the WiFi Router will act DNS server.

lows Internet Naming Service manages interactions of PC with the Internet. If you use a WINS server, enter the IP ress of server here.

an fixed IP address for clients.

address of LAN-side device.

Idress within DHCP IP Pool for LAN-side device.

/Delete static IP.

dash symbols.

3. Domain Name:

6. Lease Time:

ator use an IP address format of 192.168.1.xxx (where xxx) and 254) when specifying an IP address range. ould not be greater than the IP Pool Ending Address.

### 2.4.1.3 Wireless Settings

### 2.4.1.3.1 Basic

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

Basic	Advanced	Wizard			
			Network > Wireless > <b>Basic</b>		
Netv	work	~			
W	AN		Basic WPS ACL Radio Advanced	1	
LA	AN .				G HEL
W	/ireless		Basic		
IP	v6		Dasic		
Pa	rental Control		Frequency	2.4GHz 0	
M	ulticast		SSID Enable	💿 Yes 🔵 No	
Ro	outing		WiFi Network Name	MySpectrumWiFi8d-2G	
Serv	vices Config	>	Hide SSID	🔿 Yes 💿 No	
Secu	urity	>	Security Setting	WPA2 Personal 0	
QoS	)	>	WPA Encryption	AES 0	
Adm	nin	>	WiFi Password	reasonanchor876	
			Protected Management Frames	Disable 0	
Tool	S	>	Max Clients	128	
Stat	us	>	Password Rotation Interval	3600	
				Apply	

- 8. WiFi Password:
- 9. Protected Management Frames: Protected some ty disasso
  10. Max Clients: The main the enclosed some ty disasso
  11. Password Rotation Interval: This fiel a WPA to indice
  12. Click Apply. Please i

Steps to set up the basic wireless settings:

- 1. From the navigation panel, go to Advanced > Network > Wireless > Basic.
- 2. Frequency: Select the frequency band to configure.
- 3. SSID Enable: Switch the SSID on/off (enable/disable).
- 4. WiFi Network Name: A name whose length is less than 32 characters is used to identify a wireless network. WiFi devices automatically detect all networks within its communication range.
- 5. Hide SSID: If [Yes] is selected, network name (SSID) does not show in site surveys by wireless mobile clients and they can only connect to WiFi Router by manually enteringnetwork name (SSID).
- 6. Security Setting: This field enables authentication methods for wireless clients.
- 7. WPA Encryption: Enable WPA Encryption to encrypt data.

Requires a password of 8-63 characters (letters,

numbers or a combination) or 8 - 64 hex digits to start the encryption process.

Protected Management Frames is a feature to protect some types of management frames like deauthorization, disassociation and action frames.

The maximum number of clients allowed.

This field specifies the interval (in seconds) after which a WPA group password is changed. Enter [0] (zero) to indicate that a periodic key-change is not required. Please input the value between 600 to 86400 (seconds).

### 2.4.1.3.2 WPS

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

Basic <u>Advanced</u>	Wizard			
		Network > Wireless > WPS		
Network	×			
WAN		Basic WPS ACL Radio	Advanced	
LAN				( HELP
Wireless		Note: ACL will only take	effect when WPS is disabled.	
IPv6		Basic		
Parental Control		DASIC		
Multicast		Frequency	2.4GHz 0	
Routing		Enable WPS	On	
Services Config	>	Connection Status	WPS-ENROLLEE-SEEN	
Security	>	Configured	Yes	
QoS	>	AP PIN Code	62312387	
		WPS Method	Push Button O Client PIN Code	
Admin	>	PIN Code		
Tools	>			
Status	>		Start	

### 2.4.1.3.3 ACL

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

_			
Basic	Advanced	Wizard	
			Network > Wireless > ACL
Netw	vork	~	
W/	AN		Basic WPS ACL Radio A
LA	N		
W	reless		🚹 Note: ACL will only take e
IPv	6		Desta
Par	rental Control		Basic
Mu	ilticast		Frequency
Roi	uting		WiFi Network Name
Servi	ices Config	>	Enable MAC Filter
Secu	rity	>	MAC Filter Mode
QoS		>	MAC Filter List
Adm	in	>	MACTILEI LISU
Tools		>	MAC
TOOLS	>		
Statu	IS	>	

Steps to set up the ACL:

1.	From the navigation	panel, go to Advance
2.	Frequency:	In the frequency fiel
		use for the ACL sett
3.	WiFi Network Name:	A name whose lengt
		wireless network.
4.	Enable MAC Filter:	Enable MAC filter or
5.	MAC Filter Mode:	Select Accept to allo
		the AP/ Router, sele
		from associating to
6.	MAC Filter List:	Enter the MAC addre
		either limit specific I
		Router, or specifical
		with the AP/Router.
7	When done click An	nly

7. When done, click Apply.

dvanced				G HELP
ffect when	WPS is disabled.			
	2.4GHz	0		
	MySpectrumWiFi67-2G			
	Yes O No			
	Accept	0		
(Maxir	num: 64)			
Filter List			Add / Delete	
	\$		Θ	
	Apply			

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

ld, select the frequency band that you want to tings.

yth is less than 32 characters is used to identify a

r disable.

low devices in the MAC filter list to associate to ect Reject to prevent devices in the MAC filter list the AP /Router.

ress of the wireless device. MAC filtering lets users MAC addresses from associating with the AP/ Ily indicates which MAC addresses can associate

### 2.4.1.3.4 Radio

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

Basic	Advanced	Wizard			
			Network > Wireless > Radio		
Netw	vork	×			
WA	AN		Basic WPS ACL Radio Advance	ed	
LAI	N				G
Wi	reless		Basic		
IPv	6		Dasic		
	rental Control		Frequency	2.4GHz 0	
	lticast				
	uting		Schedule		
Servi	ices Config	>	Enable Wireless Scheduler	🖲 Yes 🔵 No	
Secu	rity	>	Date to Enable (Weekdays)	Mon Tue Wed Thu Fri	
QoS		>	Time of Day To Enable	00 : 00 ~ 23 : 59 All Day	
Adm	in	>	Date to Enable (Weekend)	Sat Sun	
Tools		>	Time of Day To Enable	00 : 00 ~ 23 : 59 All Day	
Statu		>			
			Radio Setting		
			Enable Radio	Yes O No	
			Wireless Mode	b/g/n 0	
				b/g Protection	
			Channel Bandwidth	20/40 MHz 0	
			Control Channel	Auto 0	
			Extension Channel	Auto 0	
			Enable TX Bursting	Enable 0	
			Tx Power Adjustment	100% 0	
			OBSS RSSI	35	
			RTS Threshold	2347	
			Fragmentation Threshold	2346	
			Beacon Interval	100	
			HT AMPDU Factor	65535 0	
			VHT AMPDU Factor	1048575 0	
			DCS Enable	Disable 0	
			Radio Resource Managment	Enable 0	

Steps to set Radio:

- 1.
- 2. Frequency: 3. Enable Wireless Scheduler: Switch wireless schedule on or not. 4. Date to Enable (Weekdays): Select weekdays to enable Wi-Fi.
- 5. Time of Day To Enable:
- 7. Time of Day To Enable: 8. Enable Radio:
- 9. Wireless Mode:
- 10. Channel Bandwidth:
- 11. Control Channel:
- 12. Extension Channel:
- 13. Enable TX Bursting:
- 14. Tx Power Adjustment:

From the navigation panel, go to Advanced > Network > Wireless > Radio. Selecting the frequency band that the WiFi Router is running. Set weekday time to enable Wi-Fi. 6. Date to Enable (Weekend): Select weekend days to enable Wi-Fi. Set weekend time to enable WiFi. Select [Yes] to enable wireless radio (wireless network). Select [No] to disable wireless radio (wireless network). Select a Wireless Mode of your 802.11n interface. Sets manual channel bandwidth. The radio channel for wireless connection operation. Extension (Secondary) channel is above/below the control (Primary) channel. TX Bursting improves transmission speed between WiFi Router and 802.11g devices. Set the capability for transmission power. The maximum value is 100%. You can save power and increase security if you don't require full wireless range.

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

15.	OBSS RSSI:	Configure OB
16.	RTS Threshold:	configured va Select a lower improve wirel network with devices.
17.	Fragmentation Threshold:	Set the fragm fragment size
18.	Beacon Interval:	Beacon Interv beacon and the millisecond, of improve trans or for roaming
19.	HT AMPDU Factor:	Enables or dis interface. Red but no aggreg disabled.

Apply

BSS RSSI threshold. If OBSS RSSI is greater than alue, then only move to 20 Mhz.

er value for RTS (Request to Send) Threshold to less communication in a busy or noisy wireless high network traffic and numerous wireless

nentation threshold, which is the maximum e.

val means the period of time between one the next one. The default value is 100 (the unit is or 1/1000 second). Lower the Beacon Interval to smission performance in unstable environment ng clients, but it will be power consuming. isables Tx AMPDU aggregation for the entire eceiving aggregate frames will still be performed, gate frames will be transmitted if this is

20.	VHT AMPDU Factor:	Set VHT capability field, Maximum A-MPDU length
		exponent.Value range is 0 to 7. Maximum A-MPDU length
		exponent indicates the maximum length of A-MPDU that
		the station can receive.
21.	DCS Enable:	Enable or disable DCS function which is a feature to
		detect and avoid CW interference.
22	Dadia Dasaurea Managamant	Enables or disables 802 11/

- 22. Radio Resource Management: Enables or disables 802.11k
- 23. When done, click Apply.

### 2.4.1.3.5 Advanced

The Professional module provides advanced configuration options.

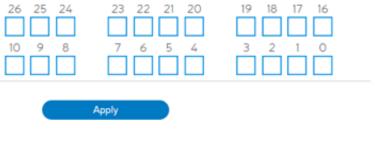
Basic	Advanced	Wizard	
			Network > Wireless > Advanced
Netw	/ork	~	
WA	AN		Basic WPS ACL Radio A
LAI	N		
Wi	reless		CCID Catting
IPv	6		SSID Setting
Par	ental Control		Frequency
Mu	lticast		WiFi Network Name
Rou	uting		TX STBC
Servi	ces Config	>	RX STBC
Secu	rity	>	Set AP Isolated
QoS		>	Multicast Rate (Mbps)
Adm	in	>	Short Guard Interval
-		>	DTIM Interval
Tools		/	WMM
Statu	IS	>	WMM APSD
			Turbo QAM
			Universal Beamforming
			Disable Specific

31	30	29	28	27
15	14	13	12	11
	_			_

NOTE: We recommend that administrators use the default settings.

I	
l	
2.4GHz	0
MySpectrumWiFi67-2G	
Enable	0
Enable	0
🔿 Yes 💿 No	
Auto	0
Enable	0
3	
Enable	0
	0
Enable	

### c MCS Data Rates



In this module, administrator can configure the followings:

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

2.	Frequency:	Select the frequency band to configure professional settings.				
3.	WiFi Network Name:	A name whose length is less than 32 characters is used to identify a wireless network.				
4.	TX STBC:	Enables or disables the Space Time Coding Block (STBC) feature, as described in 802.11n specification, in transmitting (TX) direction.				
5.	RX STBC:	Enables or disables the Space Time Coding Block (STBC)feature, as described in 802.11n specification, in receiving(RX) direction.				
6.	Set AP Isolated:	Prevent wireless devices from communicating with each other via WiFi Router. This feature is useful if many guests frequently join or leave your network. Select [Yes] to enable this feature or select [No] to disable.				
7.	Multicast Rate (Mbps):	Setting transmission rate for multicast.				
8.	Short Guard Interval:	Defines the length of time that the WiFi Router spends for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select Enable for a busy wireless network with high network				
9.	DTIM Interval:	traffic. DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is				
10.	WMM:	three milliseconds. Enables or disables WMM capabilities in the driver. The WMM capabilities perform special processing for multimedia stream data including voice and video data.				
11.	WMM APSD:	Enable WMM APSD (WiFi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select Disable to switch off WMM APSD.				
12.	Turbo QAM:	256-QAM (MCS 8/9) support. Wireless Mode must be set to auto.				
13.	Universal Beamforming:	For legacy wireless network adapters which do not support beamforming, the WiFi Router estimates the channel and determines the steering direction to improve the downlink speed. (Also known as Implicit Beamforming.)				
14.	. Disable Specific MCS Data Rates: Disabling specific MCS data rates per SSID.					

15. Click Apply.

### 2.4.1.4 IPv6

widely available, contact your ISP to make sure whether IPv6 service is provided.

Basic Advanced	Wizard	
		Network > IPv6
Network	~	
WAN		Basic
LAN		
Wireless		Connection Type
IPv6		
Parental Control		IPv6 WAN Settir
Multicast		WAN IPv6 MTU
Routing		User Class Option
Services Config	>	Auto Configuration
Security	>	
QoS	>	IPv6 LAN Settin
Admin	>	Enable LAN
Tools	>	Simultaneous
Status	>	LAN IPv6 Address
		LAN Prefix Length
		LAN IPv6 Prefix
		Enable Pool Setting For Lan H
		DHCP Pool Start
		DHCP Pool End
		LAN IPv6 MTU
		IPv6 DNS Setting

Port Ranges Val

MapT function is enable, but

# The module is used to set some basic functions related to IPv6. For IPv6 service is not yet

					0	HELP
	Native		\$			
			-			
ng						
ng						
	1280					
	charter_m	ap				
	O Enable	Disable				
a						
ıg						
	Enable	O Disable				
	💿 Enable	O Disable				
	64					
Host	O Enable	Disable				
				- 1		
				1000		
	15.00			1000		
	1500					
g						
matic	🖲 Yes 🛛 N	0				
id for	Port Fo	rwarding				
	nge for port					
bore re	inge sor port	evenuevenų:				
				h.		

Apply

Steps to set up IPv6:

- 1. From the navigation panel, go to Advanced > Network > IPv6.
- Select IPv6 connection type to configure Disable, 2. Connection Type: Native and Static IPv6. Set the WAN interface's ipv6 address. 3. WAN IPv6 Address: WAN Prefix Length: Set the WAN interface's ipv6 prefix length. 4. 5. WAN IPv6 Gateway: Set the WAN interface's ipv6 gateway Set the WAN interface's IPv6 MTU 6. WAN IPv6 MTU: (Maximum Transmission Unit). The user class option (15) of ORO that DHCPv6 7. User Class Option: clients send to the DHCPv6 server by solicit message.
- 8. Auto Configuration:

The WAN interface's address assign type (SLAAC). Enable: WAN interface can get ipv6 address by SLAAC. Disable: WAN interface gets the ipv6 address only by stateful.

9. Enable LAN: Enable/Disable WiFi Router allocating IPv6 addresses for LAN-side devices. 10. Simultaneous: The mode which hosts connected to the LAN interface can get IPv6 addresses. When enabled, hosts get IPv6 address by simultaneous Stateless and Stateful (requires address between DHCP pool start and end values). When disabled, hosts do not get IPv6 addresses simultaneously, and a mode must be selected instead (SLAAC + RDNSS, SLAAC+Stateless DHCPv6, Stateful DHCPv6). 11. LAN IPv6 Address: Set LAN interface's IPv6 address. 12. LAN Prefix Length: Set LAN interface's IPv6 prefix length. 13. LAN IPv6 Prefix: Set LAN interface's prefix. 14. Enable Pool Setting For Lan Host: Enable to set DHCP pool start and end values for client IPv6 address assign range, it's disable by default. 15. DHCP Pool Start: DHCPv6 address setting address pool start. 16. DHCP Pool End: DHCPv6 address setting address pool end. 17. PD-Valid Lifetime: Prefix delegation for valid lifetime. 18. PD-Preferred Lifetime: Prefix delegation for preferred lifetime. 19. LAN IPv6 MTU: Set MTU for LAN-side devices. 20. Connect to DNS Server Automatically: Choose to get the DNS from manually from uplink. 21. IPv6 DNS Server 1: IPv6 address for DNS server.

61

22. IPv6 DNS Server 2:

23. IPv6 DNS Server 3:

24. Port Ranges Valid for Port Forwarding: The "port ranges" are set by Map-T mode, and the port setting for port forwarding must be in these ranges.

25. Click Apply.

IPv6 address for DNS server.

IPv6 address for DNS server.

### 2.4.1.5 Parental Control

Refer to 2.3.5 Parental Control for relevant setting descriptions.

### 2.4.1.6 Multicast

Enable multicast. The sender and receiver achieve a point to multipoint connection.

Basic	Advanced	Wizard				
			Network > Multicast			
Netw	vork	×				
WA	AN		Multicast			
LAI	N			Dis 11	^	G
Wi	reless		IPv4 Multicast Route	Disable	0	
IPv	6		IPv6 Multicast Route	Disable	0	
Par	rental Control		Enable IGMP/MLD Snooping	🔿 Yes 💿 No		
Mu	ilticast					
Rou	uting			Apply		

Steps to set up Multicast:

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

	* IGMP Proxy:	IGMP Proxy enables hosts in a unidirectional link routing (UDLR) environment that are not directly connected to a downstream WiFi Router to join a multicast group sourced from an upstream network.
	* PIM:	PIM-Source-specific multicast (SSM) is used in IPv4/IPv6 and is a method of delivering multicast packets in which the only packets that are delivered to a receiver are those originating from a specific source address requested by the receiver. By limiting the source, SSM reduces demands on the network and improves security.
3.	IPv6 Multicast Route: * MLD Proxy:	Select an IPv6 Multicast Route. The MLD proxy is used in IPv6 environments. This feature enables a device to learn proxy group membership information, and forward multicast packets based upon that information. If a device is acting as RP for route proxy entries, MLD membership reports for these entries can be generated on user specified proxy interface.

- 5. When done, click Apply.

4. Enable IGMP/MLD Snooping: Check [Yes] to enable snooping and Check [No] to disable snooping. IGMP/MLD snooping is the process of listening to Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD) network traffic. The feature lets a network switch listen in on the IGMP/MLD conversation between hosts and WiFi Routers.

# 2.4.1.7 Routing

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

asic <u>Advanced</u>	Wizard					
		Network > Routing				
Network	~					
WAN		Basic				
LAN		Enable 1:1 NAT		Ne		0
Wireless		Enable LINAT	🔾 Yes 💿	140		
IPv6		1:1 NAT List (I	Maximum <sup>,</sup> 13)			
Parental Control						
Multicast		Name	Public IP	Local IP	On/Off	Operation
Routing			0		On 🗘	0

Steps to set up Routing:

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

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

## 2.4.2 Services Config

### 2.4.2.1 USB Printer sharing

Refer to 2.3.6.1 USB Printer sharing for relevant setting descriptions.

### 2.4.2.2 FTP

FTP Server enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet.

Basic	Advanced	Wizard	
			Services Config > FTP Server
Netw	/ork	>	
Servi	ces Config	~	SanDisk_Extreme
US	B Printer Sharing	1	Kingston_DataTraveler_3_
FTF	P Server		
Sar	nba		FTP
We	bDAV		Enable FTP
DL	NA		
AFI	P		Maximum number of Connec
NE	S		Enable Outside Access
Secu	rity	>	Outside Access
QoS		>	
Adm	in	>	
Table			Device and Folder
Tools		>	⊟ SanDisk_Extreme
Statu	IS	>	UNTITLED
			test
			a music
			mov
			🖿 file
			pictures-1000
			☐ Kingston_DataTraveler_3_0
			@ DINO

To set up FTP Server:

- 1. From the navigation panel, go to Advanced > Services > FTP.
- device will be displayed here.

			_
		Safely Remove D	isk 🕜 HELP
_0		Safely Remove D	isk
	On		
ections	20		
	Yes  No		
	8021		
	Apply		
0	User and Permission	00	51
	Anonymous Login	Off	
	User List	R/W R No	
	💄 admin	0 0 0	
	👤 test	0 0     0	
		Save Permission	

2. Connect an external USB hard disk drive or USB flash drive to the WiFi Router, and your

3. Click On/Off to enable/disable Internet access to FTP service.

To create a new account:

- 1. Add new account.
- 2. In the Account and Password fields, key in the name and password of your network client. Retype the password to confirm. Click Add to add the account to the list.

#### To add a folder:

- 1. Add new folder.
- 2. Enter a folder name. The folder that you created will be added to the folder list.

To set up permissions on the folder for FTP server:

- 1. From the list of folders, choose one of the shared folders and select the type of access permission that you want to assign for specific users:
  - R/W: Select this option to assign read/write access.
  - R: Select this option to assign read-only access.
  - No: Select this option if you do not want to share a specific file folder.
- 2. Click Save Permission to apply the changes.

Refer to the following descriptions:

- Maximum number of Connections: The maximum number of concurrent connections for the Network Neighborhood or FTP Server.
- Enable Outside Access: Select On/Off to enable/disable to access FTP server by wide area network.
- Outside Access: The numbers of external service ports (default value: 8021).
- Anonymous Login: Enable/disable anonymous access to the FTP server.
- Safely Remove Disk: Click to safely remove disk. When the USB disk is ejected successfully, the USB status shows "No device".
- Click Save Permission.

### 2.4.2.3 Samba

Samba Share lets you set up the accounts and permissions for the Samba service.

asic	Advanced	Wizard		
			Se	rvices Config > Samba
Netwo	ork	>		
	es Config Printer Sharing	*		SanDisk_Extreme
	Server			Kingston_DataTraveler_3_
Sam				Samba
DLN	DAV A		I	Enable Share
AFP			I	Device Name
NFS			1	Work Group
Securi	ity	>		
QoS		>		Design and Solder
Admir	n	>		Device and Folder
Tools		>		UNTITLED
Status	;	>		🖿 test
				mov
				file
				⊟ Kingston_DataTraveler_3_0
				BING

To set up Samba:

- 1. From the navigation panel, go to Advanced > Services > Samba.
- device will be displayed here.
- 3. Click On/Off to enable/disable Internet access to Samba service.

To create a new account:

- 1. Add new account.
- Retype the password to confirm. Click Add to add the account to the list.

			Safely R	emove	Disk	🔇 HEL
_0			Safely R	emove	Disk	
	On					
	RAC2V	1K				
	Workgr	000				
	Workgi	oop				
	Ar	pply				
	0	User and Permission	n		00	
		Guest Login			Off	
		User List	R/W	R	No	
		💄 admin	0	0	۲	
	music	🚨 test	0	0	0	
			Save Peri	mission		
0						

2. Connect an external USB hard disk drive or USB flash drive to the WiFi Router, and your

2. In the Account and Password fields, key in the name and password of your network client.

To add a folder:

- 1. Add new folder.
- 2. Enter a folder name. The folder that you created will be added to the folder list.

To set up permissions on the folder for Samba server:

- 1. From the list of folders, choose one of the shared folders and add the share name, and choose the type of access permission that you want to assign for specific users:
  - R/W: Select this option to assign read/write access.
  - R: Select this option to assign read-only access.
  - No: Select this option if you do not want to share a specific file folder.
- 2. Click Save Permission to apply the changes

Refer to the following descriptions:

- Device Name: Enter a name for your device and you can use this name in your web browser's URL field to quickly access the device as a Network Place service.
- Work Group: Group name of the cascade in Network Neighborhood. Note: The standard input characters include letters (A-Z, a-z), digits (0-9). The hyphen (-) and under line (\_) characters may also be used, but the hyphen (-) can't be as the first character. Guest Login: By enabling [Guest Login], any user in your local network can access ٠
- your network place (Samba) without authentication.
- Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.
- Click Save Permission.

### 2.4.2.4 WebDAV

The client can write operation in WebDAV directory with appropriate permissions.

sic Advanced	Wizard	
		Services Config > WebDAV
letwork	>	
ervices Config	~	SanDisk_Extreme
USB Printer Sharing		Kingston_DataTraveler_3_
FTP Server		
Samba		WebDAV
WebDAV		Enable WebDAV
DLNA		
AFP		Enable Outside Access
NFS		Outside Access HTTP
ecurity	>	Outside Access HTTPS
QoS	>	
dmin	>	
		Device and Folder
ools	>	SanDisk_Extreme
itatus	>	UNTITLED
		🖿 test
		🖿 music
		mov
		🖿 file
		⊨ pictures-1000
		☐ Kingston_DataTraveler_3_0
		ili birto

To set up WebDAV:

- 1. From the navigation panel, go to Advanced > Services > WebDAV.
- device will be displayed here.
- 3. Click On/Off to enable/disable Internet access via WebDAV.

To create a new account:

- 1. Add new account.
- Retype the password to confirm. Click Add to add the account to the list.

_0					afely Remove afely Remove		( HELP
	On						
	Yes	O No					
	8080						
	8443						
	Ар	_					
	0		and Permi	ssion		00	
		R/W ම	R	Anon	vmous Logi User List		
	music				👤 test	$\checkmark$	
				Saw	Permission		
D							

2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your

2. In the Account and Password fields, key in the name and password of your network client.

To add a folder:

- 1. Add new folder.
- 2. Enter a folder name. The folder that you created will be added to the folder list.

To set up permissions on the folder for WebDAV server:

- 1. From the list of folders, choose one of the shared folders and add the share name, then choose the type of access permission that you want to assign for specific users:
  - R/W: Select this option to assign read/write access.
  - R: Select this option to assign read-only access.
- 2. Click Save Permission to apply the changes.

Refer to the following for the descriptions of the fields:

- Enable Outside Access: Select On/Off to enable/ disable access to WebDAV server by WAN (wide area network).
- Outside Access: The port number of external service ports via HTTP (default value: 8080).
- Outside Access HTTPS: The port number of external service ports via HTTPS (default value: 8443).
- Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.
- Click Save Permission.

### 2.4.2.5 DLNA

your WiFi Router.

Basic	Advanced	Wizard	
			Services Config > DLNA
Network		>	
Services Config		~	TOSHIBA_TransMemory
US	B Printer Sharing	g	
FT	P Server		DLNA
Sa	mba		Enable DLNA Media Server
WebDAV			Media Server Name
DLNA			
AF	P		Media Server Path Setting
NF	S		
Secu	rity	>	
QoS		>	
Admin		>	
Tools		>	
Status		>	

To set up DLNA:

- 1. From the navigation panel, go to Advanced > Services > DLNA.
- 2. Enable DLNA Media Server: Switch DLNA media on or off.
- 3. Media Server Name: The DLNA server's name, which will be displayed by the media player, such as VLC or windows media player.

		There are tw
		share all of t
		Server Path
		When Manu
		information
5.	Manual Media Server Path:	Set the folde
		shared by th

6. Media Server Directory:

### DLNA (Digital Living Network Alliance) lets you share audio, image and video. Your WiFi Router lets DLNA-supported devices access multimedia files from the USB disk connected to

	Safely Remove Disk
On	
DLNA server on RAC2V1K	
All Disks Shared	
🔿 Manual Media Server Path	
Apply	

4. Media Server Path Setting: The methods of setting the folders' path which will be shared. vo methods to be chose, "All Disks Shared" means the mounted disks' all media; "Manual Media " means set the folders to be shared manually,

ual is selected you must enter additional

in " Manual Media Server Path".

lers to be shared and the media type that will be shared by the DLNA server.

The folders that will be shared by the DLNA.

- 7. Shared Content Type: The media type that will be shared by the DLNA server: audio, image, video.
- 8. Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.
- 9. Click Apply.

### 2.4.2.6 AFP

An AFP server is a kind of network file sharing server based on AFP protocol implementation, mainly used for file sharing between Linux and MAC systems.

Basic	Advanced	Wizard	
			Services Config > AFP
Netw	vork	>	
Servi	ces Config	~	SanDisk_Extreme
US	B Printer Sharing	9	Kingston_DataTraveler_3
FTF	Server		
Sar	nba		AFP
We	bDAV		Enable Share
DLI	NA		Enable Share
AF	P		
NE	S		Device and Folder
Secu	rity	>	⊒ SanDisk_Extreme
QoS		>	🖿 test
Adm	in	>	🖿 music
Aum		-	i mov
Tools	÷	>	🖿 file
Statu	IS	>	⊨ pictures-1000 GataTraveler_3_
			BING

To set up AFP:

- 1. From the navigation panel, go to Advanced > Services > AFP.
- device will be displayed here.
- 3. Click the On/Off to enable/disable Internet access via AFP.

To create a new account:

- 1. Add new account.
- 2. In the Account and Password fields, key in the name and password of your network client. Retype the password to confirm. Click Add to add the account to the list.

To add a folder:

- 1. Add new folder.
- 2. Enter a folder name. The folder that you created will be added to the folder list.

			Safely R	emove	Disk		
_0			Safely R	emove		I HEU	P
	On						
	On						
	0/	User and Permission			00		
		Guest Login			Off		
		User List	R/W	R	No		
	music	💄 admin	0	0	۲		
	music	👤 test	۲	0	0		
			Save Perr	nissior			
0							

2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your

To set up permissions on the folder for AFP server:

- 1. From the list of folders, choose one of the shared folder and add the share name, and choose the type of access permission that you want to assign for specific users:
  - RW: Select this option to assign read/write access. •
  - R: Select this option to assign read-only access.
  - No: Select this option if you do not want to share a specific file folder.
- 2. Click Save Permission to apply the changes.

Refer to the following for the descriptions of the fields:

- Guest Login: By enabling [Guest Login], any user in your local network can access your network place (AFP) without authentication.
- Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.
- Click Save Permission. •

### 2.4.2.7 NFS

Network File System Server is used to share the USB disk with clients via network. Clients can mount the remote disk to a local directory for a faster speed than using a Samba server.

Basic	Advanced	Wizard	
			Services Config > NFS
Netw	ork	>	
Servi	ces Config	~	SanDisk_Extreme
USB Printer Sharing		3	Kingston_DataTraveler_3_
FTP	Server		
San	nba		NFS
We	bDAV		5
DLM	A		Enable NFS
AFF	, ,		🖴 SanDisk_Extreme
NFS	5		UNTITLED
Secur	rity	>	BING
QoS		>	

To setup NFS:

- 1. From the navigation panel, go to Advanced > Services > NFS.
- device will be displayed here.
- storage via the NFS service.
- 4. Clients: "\*" and means all IPs. For example,
  - with "read and write" permission.
  - 192.168.1.2,ro;192.168.1.3,rw

		Safely Remove Disk	A 11710
_0		Safely Remove Disk	( HELP
	On		
	Clients: 192.168.1.46,rw		
0	172.100.1.40,1W		
	Saus Description		
	Save Permission		

2. Connect an external USB hard disk drive or USB flash drive to your WiFi Router, and your

3. Enable NFS: Enable or disable NFS service. When disabled, users can't access the USB

"Clients" are users who can access the shared partition specified. You can input the proper information into the input field to allow the clients to access the specified shared partition. The proper permission format is "IP address, Read and write permission" and if you want to set more than one clients and with different permission, you can input the information separated by ";". For read and write permissions, "ro" means "read only" permission and the "rw" means " read and write" permission. The IP address can be replaced by

```
1) Let the clients with the IP address 192.168.1.2 access the partition
2) Let two clients access the shared partition. The client with IP
    address 192.168.1.2 has "read only" permission, and the client with IP
    address 192.168.1.3 has "read and write" permission. >
```

- 3) Let clients access the destination shared partition with the "read only" permission. > \*,ro
- 5. Safely Remove Disk: Click to safely remove the disk. When the USB disk is ejected successfully, the USB status shows 'No device '.

### 2.4.3 Security

### 2.4.3.1 VPN

remote network using a public network such as the Internet.

### 2.4.3.1.1 PPTP VPN Server

The VPN server lets administrator get access to home network anytime, anywhere.

Basic	Advanced	Wizard				
			Security > VPN > PPTP VPN S	Server		
Netv	vork	>				
Serv	ices Config	>	PPTP VPN Server Oper	VPN Server VPN Client		G HEL
Secu	irity	~				C nee
VF	PN		Basic Config			
IP۱	/4 Firewall		Enable VPN Server	On		
IP۱	v6 Firewall		VPN Details	General	0	
QoS		>				
Adm	in	>	Username and	Password (Ma	ximum: 16)	
Tool	s	>	Connection Status	Username	Password	Add / Delete
State	us	>				G
				Apply		
	E: Boforo a	otting	up a VPN connection	a you need the IP	addross or dor	main name of the
	L. Delote S	etting	up a VPN connectior	i, you need the IP		

VPN server you are trying to access.

Steps to set up access to PPTP VPN server:

- 1. From the navigation panel, go to Advanced > Security > VPN > PPTP VPN Server.
  - Enable VPN Server:

• VPN Details:

- settings.
- - button.

# VPN (Virtual Private Network) provides a secure communication to a remote computer or

Enable or disable PPTP VPN Server. The details of PPTP VPN Server. Select General or Advanced

• Username and Password: The user information of PPTP VPN Server. Input the user name and password for the VPN server and click the

Broadcast Support	● Yes ○ No
	When Network Place is enabled, this must be enabled.
Authorization Mode	Auto 0
MPPE Encryption	MPPE-128
	MPPE-40
	✓ No Encryption
Connect to DNS Server Automatic	● Yes O No
Connect to WINS Server Automati	● Yes O No
MRU	1482
MTU	1482
Client IP Address	192.168.0.2 ~ 192.168.0. 11 (Maximum:10)

Router.

Select Authorization Mode.

### Broadcast Support:

- Authorization Mode:
- MPPE Encryption: •
- Connect to DNS Server Automatically:
- Connect to WINS Server Automatically:
- MRU/MTU: .

Select MPPE Encryption type.
DNS of PPTP clients.
WINS of PPTP clients.
The Maximum Receive Unit (MRU) or 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 MTU or MRU values sure the
change from the known problem with your PPTP
sessions correctly. Incorrect MTU or MRU values
cause traffic through the PPTP VPN to fail.
The IP address range of PPTP clients.

Turns on broadcast relay to clients from the WiFi

### Client IP Address:

Click Apply. •

### 2.4.3.1.2 OpenVPN Server

### The VPN server lets administrator get access to home network anytime, anywhere.

Basic	Advanced	Wizard	
			Security > VPN > OpenVPN Ser
Netv	work	>	
Serv	ices Config	>	PPTP VPN Server OpenVI
Secu	irity	~	Update succeeded!
VF	PN		
IP	/4 Firewall		Basic Config
IP	v6 Firewall		Enable VPN Server
QoS		>	VPN Details
Adm	nin	>	
Tool	s	>	Username and F
State	us	>	Connection Status

Steps to set OpenVPN Server:

- 1. From the navigation panel, go to Advanced > Security > VPN > OpenVPN Server. • Enable VPN Server: Enable or disable OpenVPN server function.
- - VPN Details: Enter the details of your VPN server. Select General or Advanced settings.
  - name and password for the VPN server and click the button.
- 2. Advanced VPN server settings:

rver						
/PN Server	VPN Clie	ent				
						( HELP
	On					
	General	_	<u>^</u>			
	General		÷			
Passw	ord (N	laximum	: 16)			
Userna	me	Passw	ord	Add ,	/ Delete	
					0	
					·	
	Appl	y				

• Username and Password: The user information of OpenVPN server. Input the user

## Advanced Settings

Interface Type	TUN 0
Protocol	UDP 0
Server Port	1194
Firewall	Auto 0
Authorization Mode	TLS 0
	Content Modification of Keys & Certification.
Username / Password Auth. Only	O Yes 💿 No
Extra HMAC Authorization	Disable 0
VPN Subnet / Subnet Mask	10.8.0.0
	255.255.255.0
Poll Interval	O Minutes
Push LAN to Clients	O Yes 💿 No
All traffic through VPN	🔾 Yes 💿 No
Respond to DNS	🔾 Yes 💿 No
Encryption Cipher	Default 0
Compression	Disable 0
TLS Renegotiation Time	O Seconds
Manage Client-Specific Options	O Yes

•	Interface Type:

- Protocol:
- Server Port:
- Firewall: .
- Authorization Mode:

Disable	0	
10.8.0.0		
255.255.255.0		
0	Minutes	
🔾 Yes 🛛 💿 No		
🔿 Yes 🛛 💿 No		
🔾 Yes 🛛 No		
Default	0	
Disable	0	
0	Seconds	
🔿 Yes 🛛 💿 No		
"TUN" will create an Ethernet tunn		nnel, "TAP" will create

- certificate. . Extra HMAC Authorization: • VPN Subnet / Subnet Mask: Poll Interval: Push LAN to Clients: • All traffic through VPN: • Respond to DNS: • Encryption Cipher: • Compression: **TLS Renegotiation Time:** Manage Client-Specific Options: •
  - Click Apply. •

TCP or UDP server.

on.

The TCP/UDP port which OpenVPN server will listen

Firewall configuration for VPN server. Auto will create

create basic firewall configurations and Custom will not

complete firewall configurations, External only will

create any firewall configurations.

Select Authorization Mode.

Username / Password Auth. Only: Yes requires only username and password for authentication. No also requires authentication

> If enabled, a tls auth key will be used on the server. Every client must also have the key.

VPN subnet and subnet mask settings.

The interval time for crontab of VPN server starting. Push routes to the client to allow it to reach other private subnets behind the server.

If enabled, this directive will configure all clients to redirect their default network gateway through the VPN, causing all IP traffic such as web browsing and DNS lookups to go through the VPN.

Push DNS to clients.

Select a cryptographic method. This configure item must be copied to the client configure file as well. Enable compression on the VPN link. If this function is enable here, in the client configure administrator also should enable it.

After a period of time, authentication is required again. To assign specific IP addresses to specific clients or if a connecting client has a private subnet behind it that should also have VPN access, enable this option.

### 2.4.3.1.3 VPN Client

View the VPN server list and add profiles. There are three types of VPN servers: PPTP, L2TP and Open VPN.

Basic	Advanced	Wizard						
			Security > VPN > VPN Client	t				
Netw	vork	>						
Servi	ces Config	>	PPTP VPN Server Ope	nVPN Server	PN Client			G
Secu		~	VPN Server Li	st (Maximu	ım: 8)			
IPv	4 Firewall		Connection Status	Description	VPN Type	Edit	Delete	Connection
IPve	6 Firewall				Add Profile			

- 5. Enable Default Route: Check [Yes] to use default route acquiring from VPN Server. Check [No] to use general default route.
- Enter a description for reference. Description: 6. 7. VPN Server: VPN Server IP address or URL.
  - Username:
- 8. 9. Password:
- 10. PPTP Options:
- VPN authentication password.
- 11. When done, click Confirm.

Steps to setup a VPN Client:

- 1. From the navigation panel, go to Advanced > Security > VPN > VPN Client.
- 2. VPN Sever list is displayed. Click Add Profile to set up VPN Client.

V/PN	Client
VFIN	Client

VPN Type	PPTP 0	
Enable Default Route	🔿 Yes 💿 No	
Description		
VPN Server		
Username		
Password		
PPTP Options	Auto $\Diamond$	

Confirm

83

- 3. VPN Server List: Current VPN Services which have been configured.
- 4. VPN Type: Type of VPN Server access such as PPTP, L2TP and OpenVPN.

VPN authentication username.

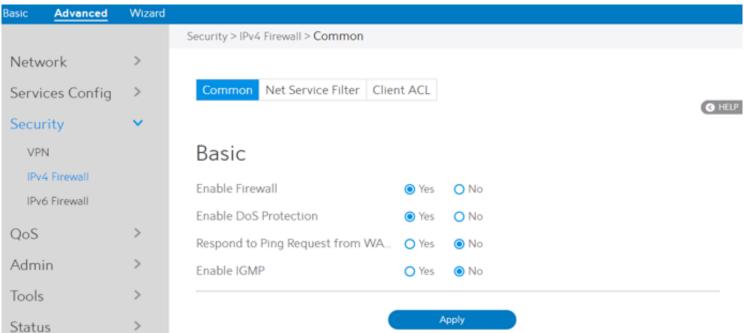
PPTP Encryption method. Select Auto for automatic Microsoft Point-to-Point Encryption (MPPE) and select No Encryption to disable MPPE. Select MPPE 40 for 40-bit MPPE with PPTP Server and select MPPE 128 for 128-bit MPPE with PPTP Server.

### 2.4.3.2 IPv4 Firewall

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

### NOTE: Firewall is enable by default.

### 2.4.3.2.1 Common



Steps to set up basic Firewall settings:

- From the navigation panel, go to Advanced > Security > IPv4 Firewall > Common. 1.
- Enable Firewall: Disabling the firewall will deactivate all related 2. functions. Enable DoS Protection: A "denial-of-service" attack is an explicit attempt 3. to deny legitimate users from using a service or computer resource. Enabling this feature can protect the WiFi Router from DoS attack but it would increase the WiFi Router's workload. Respond to Ping Request from WAN: This feature lets WiFi Router make a response to 4. ping request from WAN. Enable IGMP: Check [Yes] to allow IGMP packages to be 5. transferred to the WiFi Router. Check No to denv IGMP packages.
- Click Apply. 6.

## 2.4.3.2.2 Net Service Filter

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

Basic	Advanced	Wizard	
			Security > IPv4 Firewall > Net Ser
Netv	vork	>	
Serv	ices Config	>	Common Net Service Filte
Secu	irity	~	
VP	'N		Basic
IPv	4 Firewall		Enable Net Service Filter
IPv	6 Firewall		
QoS		>	Filter Table List
Adm	-	>	Filtered ICMP packet types
Aam	lin		
Tools	5	>	Network Service
Statu	JS	>	Source IP Port Ran

Steps to set Net Service Filter:

- 1. From the navigation panel, go to Advanced> Security> IPv4 Firewall> Net Service Filter. Enable Net Service Filter: Enable or disable this module.
- 2.
- 3. Filter Table List:

specified service.

- that will be filtered. For example, if you would like to filter Echo (type 8) and Echo Reply (type 0) ICMP packets, you need to enter a string with numbers separated by blank, such
- 4. Filtered ICMP packet types: This field defines a list of LAN to WAN ICMP packets type
- - as [0 8].
- 5. Source IP: For source or destination IP address, you can: (a) enter a specific IP address such as "192.168.122.1";
  - or "192.168.\*.\*";
  - (c) enter all IP addresses as "\*.\*.\*".

ervice F	Filter			
ter Cl	lient ACL ○ Yes ● No			C HELP
	White List		0	
es F	ilter Table	(Maximu	m: 32)	
ange	Destination IP	Port Range	Protocol	Add / Delete
			TCP 0	Φ
	Apply			

There are two kinds of filter list: White List, Black List. White List can make WiFi Router serve the specified service defined in the list, Black List make WiFi Router deny serving the

(b) enter IP addresses within one subnet or within the same IP pool such as "192.168.123.\*"

6. Port Range:

For source or destination port range, you can either:

- a) enter a specific port, such as "95";
- b) enter ports within a range such as "103:315", ">100", or "<65535".
- 7. Destination IP: For source or destination IP address, you can:
  - a) enter a specific IP address such as "192.168.122.1";
  - b) enter IP addresses within one subnet or within the same IP pool such as "192.168.123.\*" or "192.168.\*.\*"
  - c) enter all IP addresses as "\*.\*.\*".
- 8. Port Range:
  - For source or destination port range, you can either:
  - a) enter a specific port, such as "95";
  - b) enter ports within a range, such as "103:315", ">100", or "<65535".
- 9. Protocol: The protocol of service used to transport the packages. (UDP, TCP)
- 10. Add/Delete: Click or to add/delete the profile.
- 11. When done, click Apply.

## 2.4.3.2.3 Client ACL

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

asic Advanced	Wizard		
		Security > IPv4 Firewall > Client ACL	
Network	>		
Services Config	>	Common Net Service Filter Client ACL	
Security	~		O H
VPN		Basic	
IPv4 Firewall		Enable Client ACL O Yes 💿 No	
IPv6 Firewall			
QoS	>	Client ACL List (Maximum: 16)	
Admin	>		
Tools	>	Client	Add/Delete
	ŕ	0	Θ
Status	>		
		Apply	

Steps to set up Client ACL:

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

### 2.4.3.3 IPv6 Firewall

### 2.4.3.3.1 Common

Basic Advance	ed Wizard		
		Security > IPv6 Firewall > Common	
Network	>		
Services Conf	fig >	Common Allow Services	(G H
Security	~		
VPN		Basic	
IPv4 Firewall		Enable Firewall       Yes       No	
IPv6 Firewall			
QoS	>	Respond to Ping Request from WA 🔿 Yes 💿 No	
905		Enable MLD O Yes O No	
Admin	>		
Tools	>	Apply	

Steps to set up common IPv6 Firewall:

1. From the navigation panel, go to Advanced > Security >IPv6 Firewall > Common. 2. Enable Firewall: Enable or disable the IPv6 firewall. When disabled, all IPv6 packages can input WiFi Router, output WiFi Router and forward without any limitation. 3. Respond to Ping Request from WAN: This feature lets WiFi Router make a response to ping request from WAN. 4. Enable MLD: Check [Yes] to allow MLD packages to be

transferred to the WiFi Router.

Check [No] to deny MLD packages.

5. Click Apply.

### 2.4.3.3.1 Allow Services

WAN-side to LAN-side.

Basic	Advanced	Wizard		
			Security > IPv6 Fire	wall > Allow S
Netv	vork	>		
Servi	ices Config	>	Common All	ow Services
Secu	rity	~		
VP	'N		Basic	
IPv	4 Firewall		Enable Allow Se	rvices
IPv	6 Firewall		Allowed Well-K	
QoS		>	Allowed Well-Ki	lown server
Adm	in	>	Allowed	Service
Tools	5	>	Service Name	Remote I
Statu	IS	>		
			Allowed	ICMPv6
			ICMPv6	Message typ
			destination-u	nreachable

Steps to set up IPv6 Firewall:

- 1. From the navigation panel, go to Advanced > Security > IPv6 Firewall > Allow Services.
- 2. Enable Allow Services:

  - be allowed.
- - ftp, samba.

- 4. Service Name:
- 5. Remote IP/Prefix:
- 6. Local IP/Prefix:
- 7. Port Range:

- - 3021).

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

Services					
I				Ø	HELP
List	O Yes ● No	0			
2103	116436 361666	Ŷ			
Rule	s (Maximum: 32)				
IP/Prefix	Local IP/Prefix	Port Range	Protocol	Add / Delete	
			TCP 0	0	
5 Rule	s (Maximum: 16)				
pe	Local Host		Add /	Delete	
¢			•	•	
	Apply				

Enable or disable the IPv6 Allow Services feature. When

Allow Services is enabled, the Allowed Service Rules will

3. Allowed Well-Known Server List: List of well-known servers to be allowed. For example:

The name of the service which will add IPv6 firewall rule. IPv6 address or Prefix of a remote server.

IPv6 address or Prefix of a LAN-side client.

Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024,

- Protocol: The protocol the service uses to transport the packages e.g. (UDP, TCP). 8.
- ICMPv6 Message Type: Make WiFi Router process the defined types of ICMPv6 packet 9.
- from specified host. 10. Local Host: IPv6 address of the host.
- 11. Add/Delete: Click 💿 or 🔵 to add/delete the profile.
- 12. When done, click Apply.

### 2.4.4 QoS

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

### 2.4.4.1 Airtime Fairness

The ATF(Airtime Fairness, ATF) module supports mixing rates of WiFi devices to achieve better performance in busy/intense environments.

Basic <u>Advanced</u>	Wizard			
		QoS > Airtime Fairness		
Network	>			
Services Config	>	General		G HELP
Security	>	Enable ATF	Yes O No	
QoS	×	Frequency	2.4GHz 0	
Airtime Fairness		ATF Mode	fair-queue 🗘	
Common				
Queue		WiFi Network I	Name Percentage of Air Time (%)	
Classification		✓ MySpectrumWiFi	100	
Admin	>	MAC	C 🕲	
Tools	>		Apply	

### Steps to set ATF:

- 1. From the navigation panel, go to Advanced > QoS > Airtime Fairness.
- 2. Enable ATF: 3. Frequency:
- 4. ATF Mode:

Airtime Fairness implements 2 scheduling algorithms: strict-queue and fair-queue algorithm, which are mutually exclusive. Strict-queue algorithm follows strict airtime allocation as configured by the user and does not try and utilize any unused bandwidth. Fair-queue algorithm guarantees the configured airtime in congested environments and it also utilizes any unused bandwidth.

Enable or disable. ATF require primarily focuses on scheduling fairness for transmission of traffic from Access Point (AP), and efficient WiFi bandwidth utilization.

In the frequency field, select the frequency band that you want to use for the ATF settings.

5. WiFi Network Name: Set the network name (SSID) which will be controlled by ATF.

- Percentage of Air Time: Set the percentage of SSID which will be used for ATF control. 6.
- 7. MAC: Select client by MAC address and set the percentage which will
  - be used for ATF control.
- 8. Click Apply.

### 2.4.4.2 Common

Set up queue and down queue type, decided in the queue page we can operate the type of gueue, and set uplink and downlink limit, limit our uplink and downlink transmission rate.

Basic	Advanced	Wizard	
			QoS > Common
Netv	vork	>	
Serv	ices Config	>	Basic
Secu	rity	>	QoS Enable
QoS		~	
Air	rtime Fairness		Speed Limitatio
Co	mmon		WAN Uploading Speed
Qu	ieue		
Cla	assification		LAN Downloading Speed
Adm	in	>	от.
Tools	5	>	Queue Type
Statu	JS	>	WAN Interface Queue Type
			LAN Interface Queue Type

Steps to set it:

- 1. From the navigation panel, go to Advanced > QoS > Common.
- 2. QoS Enable:
- 3. WAN Uploading Speed:
- 4. LAN Downloading Speed: The downstream limit of the subnet LAN.
- - Priority / Weighted Round Robin / Weighted Fair Queuing), For Subnet LAN.

7. Click Apply.

		_
	🔿 Yes 💿 No	G HELP
n		
		Mbps
		Mbps
	Strict Priority	0
	Strict Priority	¢
	Apply	
	Арріу	

- Set the switch of CPE QoS function through Web page. The speed of the uplink data limit.
- 5. WAN Interface Queue Type: Upstream Qos queue type, should to be set (Strict Priority / Weighted Round Robin / Weighted Fair Queuing).
- 6. LAN Interface Queue Type: Downstream Qos queue type should to be set (Strict

### 2.4.4.3 Queue

Create an upstream queue and a downstream queue to classify traffic of different types into the upstream or downstream queue. Up queue and down queue type based on common page selection. In the queue page on the queue. Add, delete, modify.

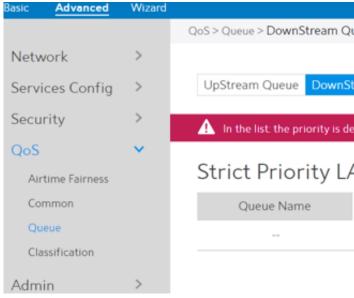
## 2.4.4.3.1 UpStream Queue

Basic	Advanced	Wizard						
			QoS > Queue > UpStream Queu	e				
Netw	vork	>						
Servi	ices Config	>	UpStream Queue DownSt	ream Qu	eue			( HELP
Secu	rity	>	🚹 In the list: the priority is de	scending f	rom top to bo	ttom, and	the top has the highest priority.	
QoS		×						
Air	time Fairness		Strict Priority W	AN C	)ueue (	Maxir	mum: 8)	
Co	mmon		Queue Name		Enable		Operation	
Qu	eue			Yes		0	0	
Cla	ssification							
Adm	in	>			Apply			

Steps to set queue:

- 1. From the navigation panel, go to Advanced > QoS > Queue > UpStream Queue.
- 2. Enable: Enables or disables this queue.
- Weight of this queue in case of Weighted Round Robin or Weighted Fair 3. Weight: Queuing, but only used for queues of equal precedence.
- 4. Operation: Add, Edit or Delete operation for this item.
- 5. Click Apply.

### 2.4.4.3.2 DownStream Queue



### Steps to set queue:

- From the navigation panel, go to Advanced > QoS > Queue > DownStream Queue. 1. 2. Enable: Enables or disables this queue.
- Weight of this queue in case of Weighted Round Robin or Weighted Fair 3. Weight: Queuing, but only used for queues of equal precedence.
- Operation: Add, Edit or Delete operation for this item. 4.
- Click Apply. 5.

)u	eue				
		_			
ŝti	ream Queue	2			
		-			G HELP
les	scending fror	n top to botto	m, an	d the top has the highest priority.	
Α	N Que	eue (Ma	xin	num: 8)	
				,	
	E	nable		Operation	
	Yes		^	0	
	165		Ŷ	•	
		Apply			
		Арріу			

## 2.4.4.4 Classification

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

Classification Display page:

Display classification table (Simple information).

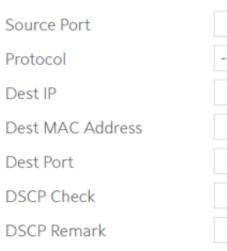
### Wizard Advanced asic QoS > Classification Network 5 Classification (Maximum:64) Services Config > Name Queue Interface Enable Security Edit/Delete QoS ~ Apply Airtime Fairness Common Queue Classification

Steps to set up Classification:

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

### Classification

Enable	Yes	0
Base On	Custom	0
Name		
Queue Interface	WAN	0
There is no any queue added on th	e WAN Interface.	
Queue Name		
Class Interface	LAN	0
Source IP		
Source MAC Address		



7. 8.	Enable: Base On:	Disable or enable It is a fast classifi
9.	Name:	SSID, APP). Define this classi
10.	Queue Interface:	Select the existin
11.	Queue Name:	Only display. Indi
		selected by the u
12.	Class Interface:	This specifies the
13.	Source IP:	Source IP addres
		used for classifica
14.	Source MAC Address:	Source MAC Add
		not used for class
15.	Source Port:	Source port num
16.	Protocol:	Protocol
17.	Dest IP:	Destination IP ad
		not used for class
18.	Dest MAC Address:	Destination MAC
		is not used for cla
19.	Dest Port:	Destination port
20.	DSCP Check:	DSCP number (0
21.	DSCP Remark:	Remark new DSC
22.	When done, click App	ly.

:	>
	Ŧ

### Confirm

e this classification function.

ication, (can be based on Client, Custom, Server,

ification alias name.

ng queue (upstream or downstream).

licates the index number of the queue type user.

e ingress interface associated with the entry.

ss. An empty string indicates this criterion is not ation.

dress. An empty string indicates this criterion is sification.

nber

ddress, an empty string indicates this criterion is sification.

C Address. An empty string indicates this criterion lassification

number.

0~63), base on it filter.

CP number.

### 2.4.5.1 System

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

5.	Remote Log Server:	IP address
		be sent in a
6.	Time Zone:	Default tim
7.	Auto Logout:	Auto sign o
8.	Enable WAN Down Notification:	When ther
		notification
9.	NTP Server:	WiFi Route
		server in o

10. Click Apply.

Basic	Advanced	Wizard				
			Admin > System			
Netw	vork	>				
Servi	ices Config	>	Change the Router	Login Password		G HELP
Secu	rity	>	Username	admin		
QoS		>	New Password			
Adm	in	~	Retype New Password		Show password	
	stem nfiguration g		Miscellaneous Remote Log Server			
Ret	boot		-	Anna in 10		
Tools		>	Time Zone	America/Denver	0	
			Auto Logout	5	Minutes(Disable:0)	
Statu	IS	>	Enable WAN Down Notification	Yes ONo		
			NTP Server (Maximu	m: 6)		
			NTP Serve	r	Add/Delete	
					0	
			us.pool.ntp.o	rg	•	
			north-america.poo	I.ntp.org	•	
			time.nist.go	v	•	
			pool.ntp.org	3	۰	
				Apply		

99

Steps to set System:

- 1. From the navigation panel, go to Advanced > Admin > System.
- 2. Username: WiFi Router's sign in name.
- 3. New Password: New password.
- 4. Retype New Password: Retype new password.

- ss of a syslog server to which log messages will n addition to the local destination.
- time-zone is America/Denver.
- n out after a specified time.
- ere is no Internet access, redirect to local ion.
- uter can access a NTP (Network Time Protocol) order to synchronize the time automatically.

### 2.4.5.2 Configuration

Basic	Advanced	Wizard					
			Admin > Configuration				
Netw	ork	>					
Servio	ces Config	>	Configuration				G HELP
Secur	ity	>	Save to File	Save			<b>U</b> Hedr
QoS		>	Reset to Default	Reset to Default			
Admi	n	~	Restore from File		Q	Upload	
Syst	tem						
Con	figuration						

Steps to Save to File, Reset to Default and Restore from File WiFi Router's configuration:

- 1. From the navigation panel, go to Advanced > Admin > Configuration.
- 2. Click Save, and then the browser will automatically download WiFi Router's setting files.
- 3. Click Reset to Default, this will this resets all settings to factory default settings.
- 4. Click 💿 to select setting file, the click Upload button, this will make the WiFi Router to be set.

### 2.4.5.3 Log

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

Basic	Advanced	Wizard	
			Admin > Log
Netw	vork	>	
Sorvi	ices Config	>	System Time
			Up Time
Secu	rity	>	/tmp/mf_info.txt, what = Serial
QoS		>	Fri Feb 17 00:44:32 2017 daemon Fri Feb 17 00:44:32 2017 daemon
Adm	in	~	<pre>Fri Feb 17 00:44:32 2017 daemon /tmp/mf_info.txt, what = Manufe</pre>
Svs	tem		Fri Feb 17 00:44:32 2017 daemon Fri Feb 17 00:44:32 2017 daemon
	nfiguration		/tmp/fe80::213:3bff:fe12:2b69_c Fri Feb 17 00:44:32 2017 daemor
Loc	, in the second		<pre>/tmp/mf_info.txt, what = Serial Fri Feb 17 00:44:32 2017 daemon</pre>
Ret	boot		Fri Feb 17 00:44:32 2017 daemor Fri Feb 17 00:44:32 2017 daemor
			/tmp/mf_info.txt, what = Hardwa Fri Feb 17 00:44:32 2017 daemon
Tools	5	>	<pre>Fri Feb 17 00:44:32 2017 daemon /tmp/mf_info.txt, what = Manufe </pre>
Statu	IS	>	Fri Feb 17 00:44:32 2017 daemor Fri Feb 17 00:44:32 2017 daemor
			Fri Feb 17 00:44:32 2017 daemor /tmp/mf_info.txtodhcp6c[4631]:
			Fri Feb 17 00:45:00 2017 cron.: Fri Feb 17 00:46:00 2017 cron.:
			Fri Feb 17 00:47:00 2017 cron.:

Steps to set System log:

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

Fri Feb 17 0 : 47 : 09 2017

OD 02H 38M 54S

```
HELP
```

alNumber on.notice netifd: wan6 (4631): ] on.notice netifd: wan6 (4631): on.notice metifd: wan6 (4631): method = 1 , where = facturer on.notice metifd: wan6 (4631): Askey Computer Corp. on.notice netifd: wan6 (4631): filename: options on.notice netifd: wan6 (4631): method = 1 , where = alNumber on.notice netifd: wan6 (4631): ] on.notice netifd: wan6 (4631): on.notice netifd: wan6 (4631): method = 1 , where = WareVersion on.notice netifd: wan6 (4631): V1.0 REV:5 on.notice netifd: wan6 (4631): method = 1 , where = facturerOUI on.notice netifd: wan6 (4631): B4EEB4 on.notice odhop6c[4631]: Got a valid reply after 267984ms on.notice netifd: wan6 (4631): method = 1 , where = Got a valid reply after 267984ms .info crond[2266]: USER root pid 11483 cmd /sbin/wifi\_log .info crond[2266]: USER root pid 11558 cmd /sbin/wifi log .info crond[2266]: USER root pid 11674 cmd /sbin/wifi\_log

Clear

Refresh Save

### 2.4.5.4 Reboot

Click the Reboot button, the WiFi Router will restart.

Basic	Advanced	Wizard	
			Admin > Reboot
Net	work	>	
Serv	ices Config	>	Basic
Secu	urity	>	Reboot
QoS		>	
Adm	nin	~	
Sy	stem		
Co	onfiguration		
Lo	g		
Re	boot		

### 2.4.6 Tools

## 2.4.6.1 Diagnostic Tools

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

Basic Advanced	Wizard	
		Tools > Diagnostic Tools
Network	>	
Services Config	>	Diagnostic To
Security	>	Method
QoS	>	Target
Admin	>	Count
Tools	~	
Diagnostic Tools Wake on LAN Status	>	<pre>PING www.wikipedia.org (198 64 bytes from 198.35.26.96: 64 bytes from 198.35.26.96: 64 bytes from 198.35.26.96: 64 bytes from 198.35.26.96:  www.wikipedia.org ping 5 packets transmitted, 4 pa round-trip min/avg/max = 19</pre>

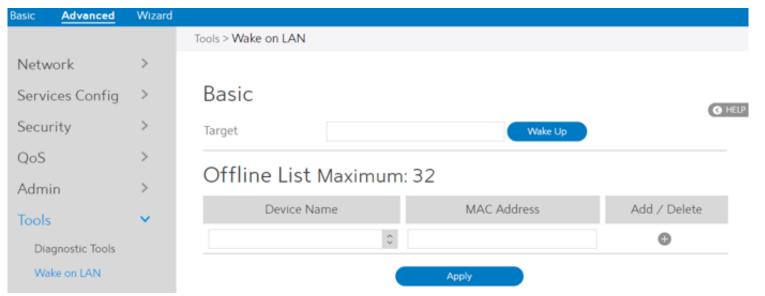
Steps to use Diagnostic Tools:

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

S			
			( HELP
	Ping	0	
	Wikipedia	0	
	5		
	Diagnose		
3.26.96): 56	data bytes ime=193.385 ms		
	ime=195.101 ms		
	ime=192.473 ms		
eq=4 ttl=51 t	ime=194.157 ms		
tistics			
ts received,	20% packet loss 95.101 ms		

### 2.4.6.2 Wake on LAN

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



### Steps to set Wake on LAN:

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

### 2.4.7 Status

## 2.4.7.1 System Information

System Information displays basic System, WAN, LAN and USB information. From the navigation panel, go to Advanced > Status > System Information.

asic	Advanced	Wizard			
			Status > System Information		
Netw	vork	>			
Servi	ices Config	>	System Informati	on	G
Secu	rity	>	Up Time	0D 02H 42M 02S	<b>U</b>
QoS		>	Date Time	2017-02-17 0:50:17	
Adm	in	>	FW Version	1.0.4	
Tools		>	HW Version	V1.0 REV:5	
Statu		•	WAN Information	ı	
	stem Informatio	n	Connection Status	Connected	
	ICP Lease		Connection Type	DHCP	
Rou	uting Table		Connect IP	10.8.4.227	
Por	rt Forwarding		Connection Time	0D 02H 40M 15S	
Cor	nnection List				
IPv	6 Information		LAN Information		
Sno	ooping Table				
Cu	rrent Users		IP (Subnet Mask)	192.168.1.1(255.255.255.0)	
-	cked Users		DHCP Server On/Off	ON	

### USB Information

Model Name Total Space Available Space

Kingston_DataTraveler_3_0
28.9G
23.3G

### 2.4.7.2 Wireless

Wireless shows status information for wireless clients. From the navigation panel, go to Advanced > Status > Wireless.

Basic	Advanced	Wizard		
			Status > Wireless > 2.4GHz Clients	
Netv	vork	>		
Serv	ices Config	>	2.4GHz Clients 5GHz Clients	G HELP
Secu	rity	>		<b>G</b> hear
QoS		>	Wireless Log	
Adm	in	>	<pre>interrace i: ath1 IEEE 802.11ng ESSID:'MySpectrumNiFi' Mode:Master Frequency:2.437 GHz Access Point: B4:EE:B4:E9:B0:1C Bit Rate:800 Mb/s Tx-Power:29 dBm</pre>	
Tools	5	>	RTS thr:off Fragment thr:off	
Statu	IS	~	Encryption key:6429-5AC7-0FFF-93CF-5834-5BD7-EAD7-8C52 [2] Security mode:open Power Management:off Link Quality=94/94 Signal level=-97 dBm Noise level=-95 dBm	
Sys	stem Information	n	Rx invalid nwid:1416 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:0 Invalid misc:0 Missed beacon:0	
w	reless			
DH	ICP Lease		Stations List No station connected	

## 2.4.7.3 DHCP Lease

Show DHCP Lease status information, including MAC, IP and Hostname information. From the navigation panel, go to Advanced > Status > DHCP Lease.

Basic	Advanced	Wizard				
			Status > DHCP Lease			
Netw	ork	>				
Servio	ces Config	>	DHCP Leases			( HELP
Secur	rity	>	MAC	IP	Hostname	
QoS		>	<			>
Admi	n	>				
Tools		>				
Statu	s	~				
Syst	tem Information	1				
Win	eless					
DHO	CP Lease					

## 2.4.7.4 Routing Table

Show IPv4 and IPv6 routing table and status information. From the navigation panel, go to Advanced > Status > Routing Table.

Basic	Advanced	Wizard									
			Status > Routing T	able							
Netv	vork	>									
	101K										
Serv	ices Config	>	Routing	Table							
Secu	irity	>	Kernel IP rout: Destination	ing table Gateway	Genmask	Flags	Metric	Ref	Use Iface		4
	-		0.0.0.0	10.8.4.1	0.0.0.0	UG	0	0	0 eth0		
QoS		>	10.8.4.0	0.0.0.0	255.255.255.0	υ	0	0	0 eth0		
			10.8.4.1	0.0.0.0	255.255.255.255	UH	0	0	0 eth0		
Adm	in	>	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0 br-lan		
Tools	s	>	Kernel IPv6 rou	ting table							
			Destination			t Hop				Flag	9
Stati	10	~	::/0			0::213	:3bff:f	(e12:2b	69	UG U	
Statt	12		2001:db8:5555: 2001:db8:5555:		11		:3bff:f	a12.2b	60	UG	
~			2001:db8:ffff:				:3bff:f			UGDJ	
Sy	stem Information	ר	2001:4860:ffff				:3bff:f			UGD	
140	ireless		fe80::/64							U	
**	il eless		fe80::/64		11					υ	
DF	ICP Lease		fe80::/64							υ	
21			fe80::/64							υ	
Ro	uting Table		fe80::/64							U	
			::/0			0::213	:3bff:f	e12:2b	69	UGDJ	A
Po	rt Forwarding		::1/128		11					υ	
			2001:db8:5555:	5555::f6f/128						U	
Co	nnection List		fe80::/128		11					0	
			fe80::/128 fe80::/128							0	
IPv	6 Information		fe80::/128							U	
6	engine Table		fe80::/128							0	
Sh	ooping Table		fe80::3862:4bf:	:fe85:899f/128						Ŭ	
C	rrent Users		fe80::3862:4bf							Ŭ	-
Cu	itent osers		•							•	Ē

### 2.4.7.5 Port Forwarding

This module is used to show the WiFi Router's port forwarding rules information, which contains both Port Forwarding module's rules and UPnP module's rules. From the navigation panel, go to Advanced > Status > Port Forwarding.

Basic	Advanced	Wizard				
			Status > DHCP Lease			
Netw	ork	>				
Servi	ces Config	>	DHCP Leases			O HELP
Secur	rity	>	MAC	IP	Hostname	Call
QoS		>	<			>
Admi	n	>	_			
Tools		>				
Statu	s	×				

### 2.4.7.6 Connection List

Show active connections status information. From the navigation panel, go to Advanced > Status > Connection List.

Wizard					
	Status > Connect	ion List			
>					
>	Active C	onnecti	ons		GH
>	Network	Protocol	Status	Source	Destination
>	ipv4	tcp	TIME_WAIT	192.168.1.77:52242	192.168.1.1:80
>	ipv4	tcp	TIME_WAIT	192.168.1.77:52244	42.236.37.92:80
>	ipv4	tcp	TIME_WAIT	192.168.1.77:52232	192.168.1.1:80
~	ipv4	tcp	TIME_WAIT	192.168.1.77:52235	192.168.1.1:80
n	ipv4	tcp	ESTABLISHED	192.168.1.77:50836	10.7.246.80:28992
	ipv4	tcp	ESTABLISHED	192.168.1.77:50733	10.7.246.80:28992
	ipv4	tcp	ESTABLISHED	192.168.1.77:50772	10.7.246.80:29166
	ipv4	tcp	TIME_WAIT	192.168.1.77:52204	222.92.95.8:443
	ipv4	tcp	TIME_WAIT	192.168.1.77:52246	192.168.1.1:80
	> > > > >	Status > Connect > Active C > Network > ipv4 > ipv4 > ipv4 • ipv4 • ipv4 • ipv4 • ipv4 • ipv4 • ipv4 • ipv4 • ipv4	Status > Connection List         Active Connection         Network       Protocol         Ipv4       tcp         Ipv4       tcp	Status > Connection List         Active Connections         Network       Protocol       Status         Ipv4       tcp       TIME_WAIT         Ipv4       tcp       ESTABLISHED         Ipv4       tcp       ESTABLISHED         Ipv4       tcp       TIME_WAIT         Ipv4       tcp       ESTABLISHED         Ipv4       tcp       ESTABLISHED         Ipv4       tcp       TIME_WAIT	Network         Protocol         Status           Network         Protocol         Status         Source           Ipv4         tcp         TIME_WAIT         192.168.177:52242           Ipv4         tcp         TIME_WAIT         192.168.177:52242           Ipv4         tcp         TIME_WAIT         192.168.177:52242           Ipv4         tcp         TIME_WAIT         192.168.177:52242           Ipv4         tcp         TIME_WAIT         192.168.177:52232           Ipv4         tcp         Status         Ipv2.168.177:52235           Ipv4         tcp         ESTABLISHED         192.168.177:50336           Ipv4         tcp         ESTABLISHED         192.168.177:50733           Ipv4         tcp         ESTABLISHED         192.168.177:50733           Ipv4         tcp         TIME_WAIT         192.168.177:50733

## 2.4.7.7 IPv6 Information

Display details on WAN and LAN IPv6 information. From the navigation panel, go to Advanced > Status > IPv6 Information.

Basic	Advanced	Wizard	
			Status > IPv6 Information
Netwo	ork	>	
Service	es Config	>	IPv6 Network Ir
Securi	ty	>	IPv6 Connection Type: Native-S WAN IPv6 Address: 2001:db8:ac
QoS		>	WAN IFv6 Gateway: fe80::7co LAN IFv6 Address: 2001:db8:33 LAN IFv6 Link-Local Address:
Admin		>	DHCP-PD: Enabled LAN IPv6 Prefix: 2001:db8:333
Tools		>	DNS Address: 2000::ff 2000::f
Status		~	IPv6 LAN Devices List
Syste	m Informatio	n	Hostname MAC Addr
Wire	less		

## 2.4.7.8 Snooping Table

Displays snooping table for client joins/leaves for both wired and wireless client streams. From the navigation panel, go to Advanced > Status > Snooping Table.

Basic <u>Advanced</u>	Wizard	
		Status > Snooping Table
Network	>	
Services Config	>	Snooping Table
Security	>	
QoS	>	NUM GROUP FDB PORT AGE
Admin	>	Bridge Snooping Hash Table IPv6
Tools	>	NUM GROUP PDB PORT AGE
Status	~	
System Information		

nformation	( HELP
Simultaneous 003:5555::808 0d:8800:b0a9:70c6	Griede
333:5555:b04:4ff:fea0:8dec/64 fe80::b004:04ff:fea0:8dec	
33:5555::/64 5e 2000::1 2001::1	
ress IPvő Address	

### 2.4.7.9 Current Users

Display current users who are permitted to get access to Internet through the router. From the navigation panel, go to Advanced > Status > Current Users.

Basic	Advanced	Wizard				
			Status > Current User:	5		
Netv	vork	>				
Serv	ices Config	>	Current Us	ers		(O HEL
Secu	irity	>	Name	IP	MAC	Interface
QoS		>				
Adm	iin	>				
Tool	s	>				
State	JS	•				
Sy	stem Information	n				
W	ireless					
Dł	ICP Lease					
Ro	uting Table					
Po	rt Forwarding					
Co	nnection List					
IPv	6 Information					
Sn	ooping Table					
Cu	rrent Users					

## 2.4.7.10 Blocked Users

Display blocked users who are not permitted to get access to Internet through the router. From the navigation panel, go to Advanced > Status > Blocked Users.

Basic <u>Advanced</u>	Wizard	
		Status > Blocked Users
Network	>	
Services Config	>	Blocked Users
Security	>	MAC
QoS	>	
Admin	>	
Tools	>	
Status	<b>~</b>	
System Information	1	
Wireless		
DHCP Lease		
Routing Table		
Port Forwarding		
Connection List		
IPv6 Information		
Snooping Table		
Current Users		
Blocked Users		

Blocked By

**O HELF** 

# **3 FCC Statement**

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

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

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

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

This device is restricted for indoor use.

### IMPORTANT NOTE:

FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 21 cm between the radiator & your body.