User Manual

Super Hybrid 4G/LTE VDSL
Gigabyte Modem Router with VoIP
and 4G Failover
C5912TR-V2

V1.0.0

Preface

Please read this user guide before you use C5912TR-V2. We trust you will not regret choosing us.

Conventions

The typographical elements in this document are defined as below.

Item or Mark	Presentation	For Example
Cascading menus	**>**	**Advanced Setup > WAN**
UI button	Bold	Click **Logout** on the upper right corner of the web UI also can log out.

Contents

Chapter 1

Introduction

This Chapter describes the product general introduction.

It contains the following sections:

1.1 Product Description

C5912TR-V2, which features an integrated port that supports all 4G and DSL standards, including VDSL, ADSL2+, ADSL2 and ADSL, supports an access rate of 300Mbps, and dual band Wi-Fi speeds up to 1167Mbps, including 300Mbps on the 2.4GHz band and 867Mbps on the 5GHz band, 4 GE ports in a single device. With two external 5dBi antennas, beamforming technology and MU-MIMO Technology, C5912TR-V2 provides wide range of wireless signal coverage.

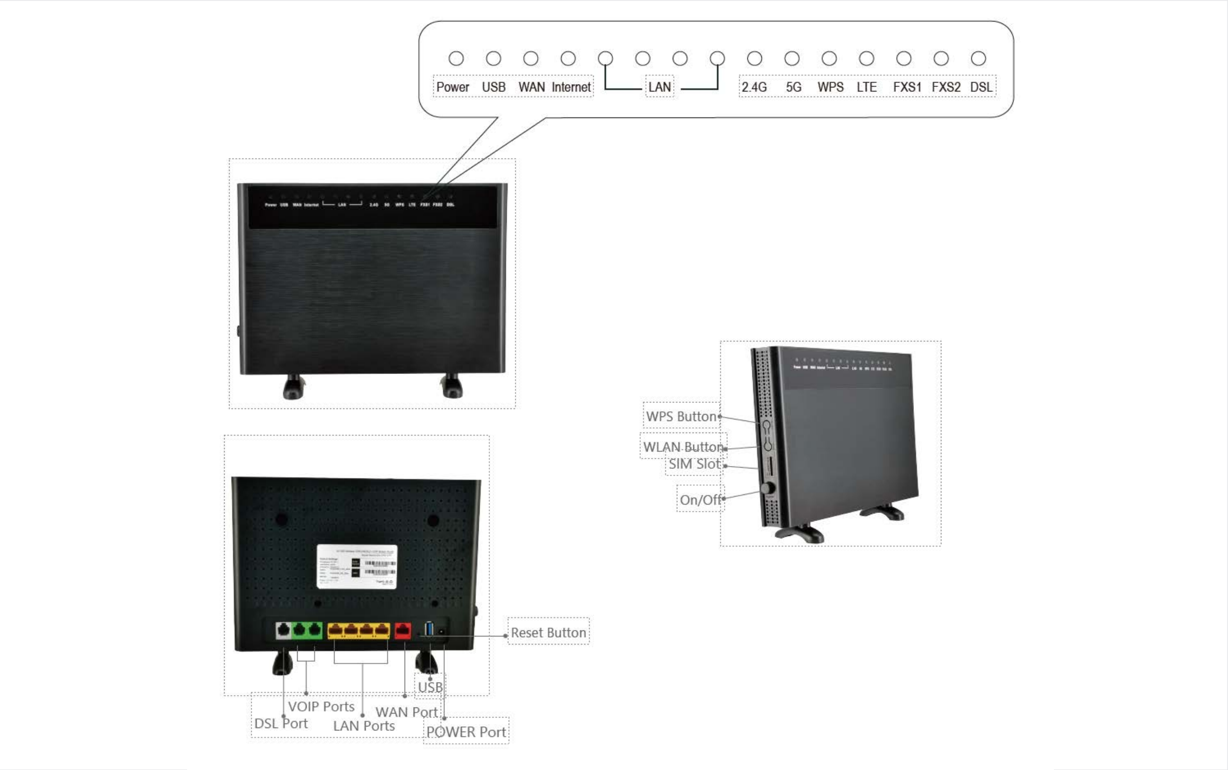
1.2 Features

- High speed： Delivering both 867Mbps at 5GHz and 300Mbps at 2.4 GHz concurrently.
- All-in-one device combines a VDSL/ADSL2+/ADSL2/ADSL, wired router, wireless router and switch.
- Ethernet and VDSL uplinks: Access the internet via DSL port or WAN port (RJ45 Port).
- Hybrid Internet Access: Support VDSL2 17a & 30a, 4G LTE Plus (including 700MHz), and Ethernet WAN internet connections.
- One-press WPS encures quick and secure wireless devices.
- 4 Full Gigabit Ethernet Ports: Gigabit wired speed for ultrafast data transfer.
- Supports IPTV feature.
- Varies Backup Connectivity: Provide 4G VDSL/ADSL and Ethernet WAN connection types by fiber or cable.
- Superior Wireless Coverage: 2*5 dBi high-performance external antennas boost Wi-Fi throughout your house to enjoy ultimate fun. MU-MIMO and Beamforming technology for simultaneous, lag-free streaming and good gaming experiences.
- Advanced Features: IPv6, DDNS, virtual server, DMZ, IP filter, MAC filter, UPnP, and so on.

1.3 Appearance

This section introduces the front panel, the rear panel and body label.

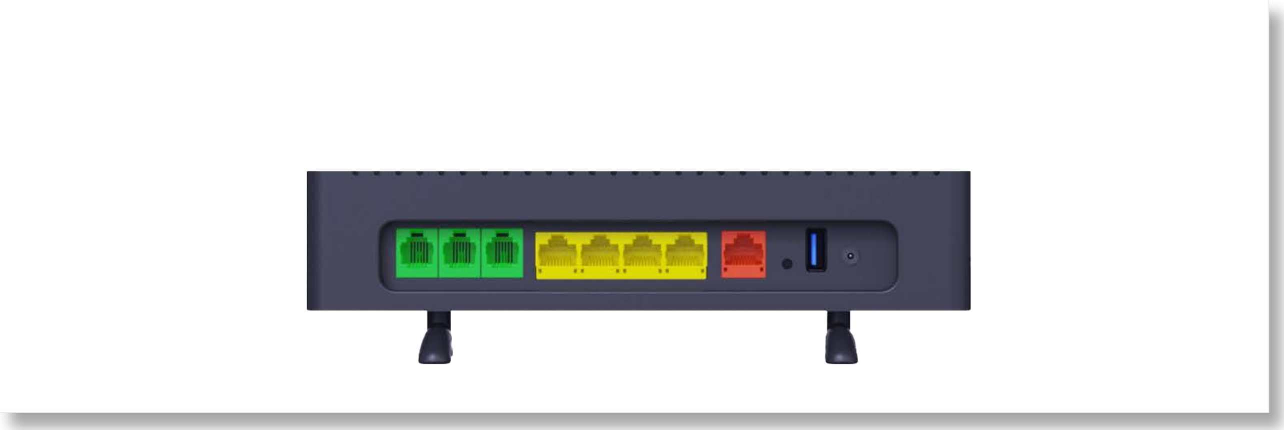
1.3.1 The Front Panel



Indicators	Status	Description
Power	On	The router is powered on.
	Off	The router is not powered on. Please check adapter is connected correctly.
Internet	On	Internet connection is available.
	Blinking	Datas are being transmitted or received through the internet.
	Off	No internet connection or the modem router is operating in Bridge mode.
DSL	On	DSL synchronization is completed.
	Blinking	DSL synchronization is in progress.
	Off	DSL synchronization is failed.

FXS1-2	On	VoIP synchronization is completed.
	Blinking	VoIP synchronization is in progress.
	Off	VoIP is not synchronized.
WAN	On	The WAN port is properly connected.
	Blinking	Datas are being transmitted or received through the WAN port.
	Off	The WAN port is not connected.
LAN1-4	On	The corresponding LAN port is properly connected.
	Blinking	Datas are being transmitted or received through the corresponding port.
	Off	The corresponding port is not connected.
USB	On	USB connection is established.
	Blinking	Datas are being transmitted or received through the USB device.
	Off	No USB device is detected, or the USB device is ejected safely.
2.4G&5G	On	The 2.4GHz/5GHz wireless band is enabled.
	Blinking	Datas are being transmitted or received through 2.4GHz/5GHz band.
	Off	The 2.4GHz/5GHz wireless band is disabled.
LTE	Green	4G internet service is available
	Red	No Service or Dail up fail
	Off	SIM Card not Detected
WPS	On	When the wireless terminal is successfully connected through the WPS function, the WPS light will stay on for about 2 minutes.
	Blinking	It is establishing WPS connection
	Off	WPS connection is finished or disable.

1.3.2 The Rear Panel

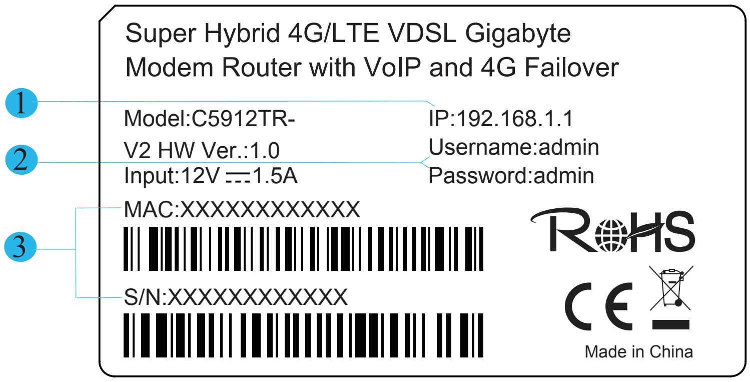


The following parts are located on the rear panel.

Buttons/Ports	Description
ON/OFF	This button is used to turn on/off the modem router.
POWER Port	Used to connect to the power adapter included with the package.
POTS	RJ11 port. For connecting your phone devices.
WAN Port	For connecting to a modem, or an Ethernet jack.
LAN Port	For connecting your wired devices to the modem router.
DSL	RJ11 port. Used to connect to a phone jack for internet access.
USB	USBV2.0 port. Used to connect to a USB device.
Reset	Hold down this button for about 6 seconds to restore factory settings.
WLAN	This button is used to enable or disable both 2.4 GHz and 5 GHz WiFi networks.
WPS	Press this button for about 3 seconds and then release it to perform the WPS negotiation process. Within 2 minutes after pressing the button, enable the wireless device’s WPS feature to establish WPS connection.

1.3.3 Body Label

You can find login IP, WiFi password, login IP address and other related information on the bottom of your C5912TR-V2.



Super Hybrid 4G/LTE VDSL Gigabyte
Modem Router with VoIP and 4G Failover

Model:C5912TR-
V2 HW Ver.:1.0
Input:12V ⎓1.5A

IP:192.168.1.1
Username:admin
Password:admin

MAC:XXXXXXXXXXXX

S/N:XXXXXXXXXXXX

Made in China

1. It specifies the login IP address. You can use this IP address to access the web management page of the C5912TR-V2.

2. It specifies the default Username and Password of loging in the web management of the C5912TR-V2.

3. It specifies the serial number and MAC address of the C5912TR-V2.

Chapter 2

Hardware Connection

This Chapter describes about hardware connection.

It contains the following sections:

2.1 Safety Precautions

Read all of these instructions and save this user guide for later use before use it. Follow all warnings and instructions on the product.

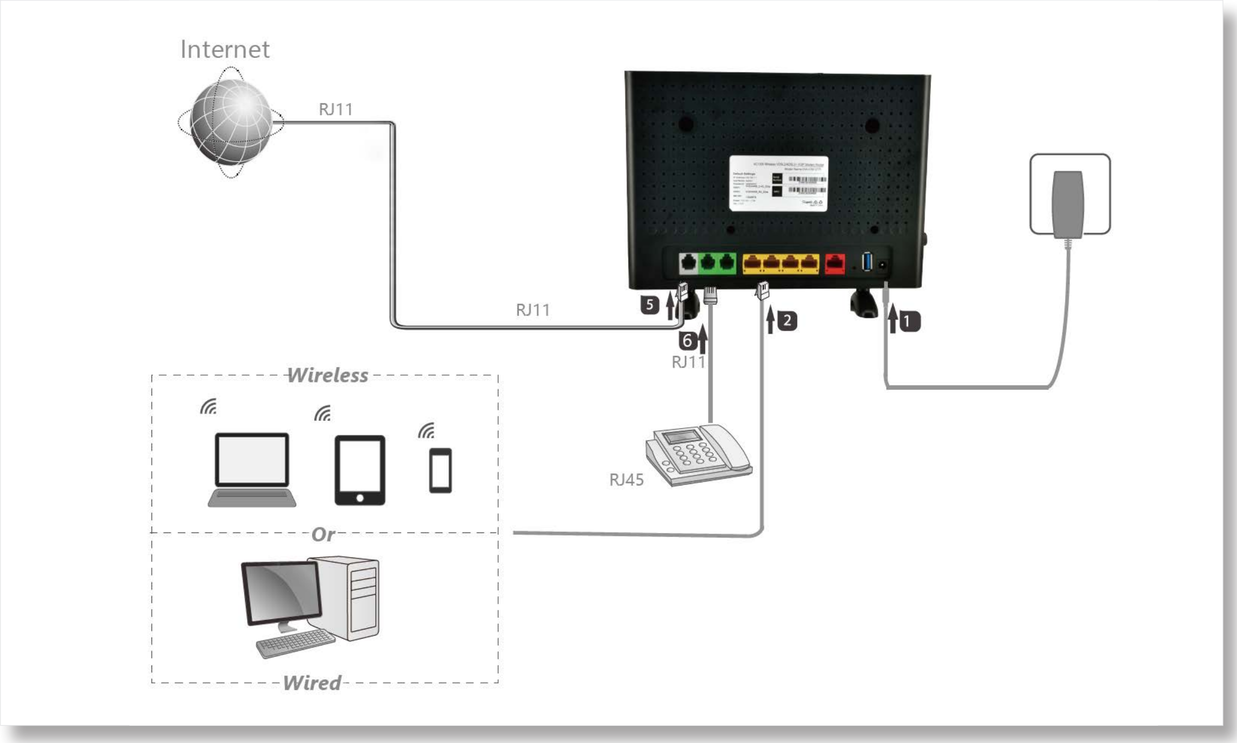
- Relative humidity: 10%~90%
- Storage temperature: -40°C to 70°C
- Operation temperature: 0~40°C
- Do not place heavy objects on the unit.
- Use only the power cord supplied with the unit. In the event that another power cord is used, one that is different than the one provided by the supplier, make sure that it is certified by the local and applicable national standards.
- Overloaded AC outlets, extension cords, frayed power cords, and broken plugs are extremely dangerous. They may, and can, result in an electrical shock or fire hazard. Call an authorized service technician for any replacements.
- Hands must be dry when plugging the power cord into an AC outlet to prevent electrical shock. Do not damage the power cord by disassembling, bending, pulling or exposing it to heat as it may cause a fire or electrical shock.
- Make sure to completely insert the power plug into an AC outlet. Insecure connections can cause a fire.
- Ensure that the power source is grounded correctly.
- Unplug the power if cleaning is needed. The unit may be wiped with a dry or slightly damp cloth when the power is off.

2.2 Connecting the C5912TR-V2 to the Internet

The modem router supports phone cable connection and Ethernet cable connection. Select a connection type to follow according to your internet service.

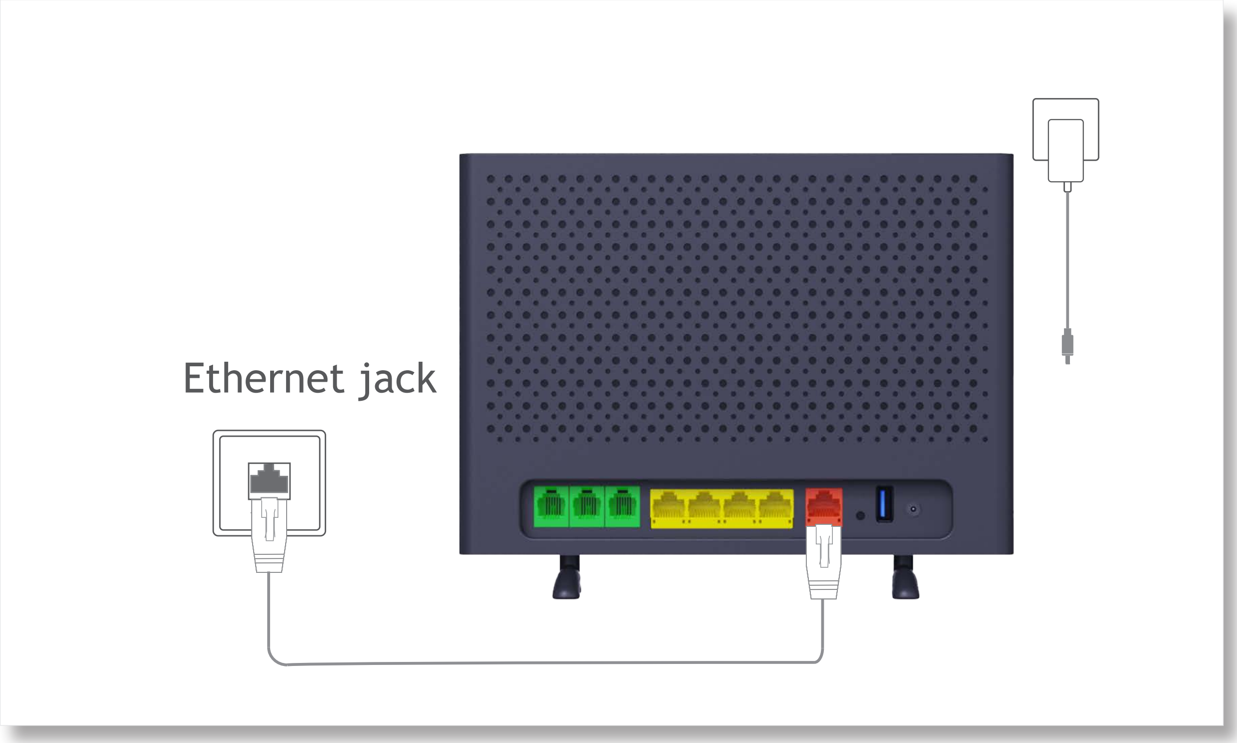
2.2.1 Phone Cable Connection

If you access the internet with a phone cable, connect the modem router as follows:



2.2.2 Ethernet Cable Connection

If you access the internet with an Etherent cable, connect the modem router as follows:



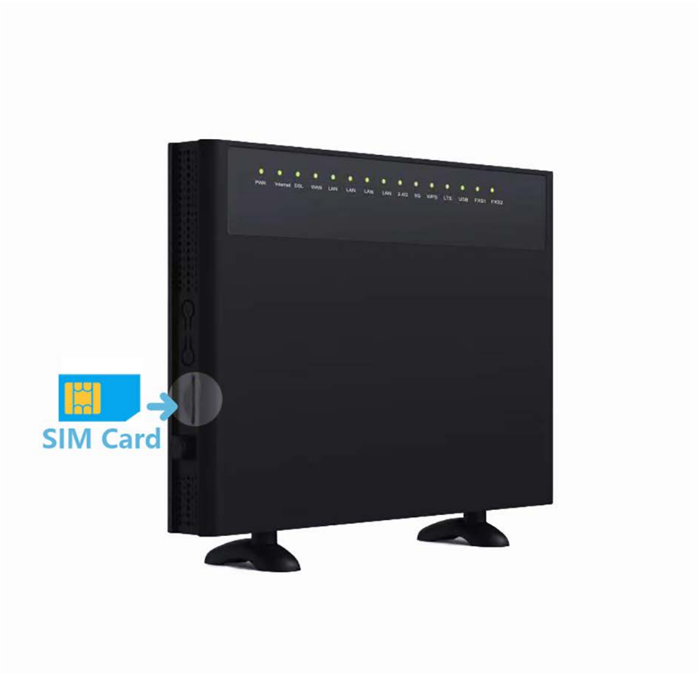
Step 1 Connect WAN port of the modem ruter to the internet.

Step 2 Use the included power adapter to connect the modem router to a power supply.

Step 3 Turn the modem router on.

2.3 4G Connection

Please input the **Standard Size** SIM Card before the device power on, or you need to turn the device off and on the make sure the New SIM service is detected by the modem



If the LTE Light stay on Red, please help to double check your SIM service provider on the SIM APN Value, you may need to change the APN Value to the correct/specify one.
For changing the APN Value:
On the User interface: 192.168.1.1 -> Basic Setup -> WAN Service -> 4G USB -> Click on the Modify Icon.

On the 4G Setting, add the APN Value on the APN Box show as the image above.

Chapter 3

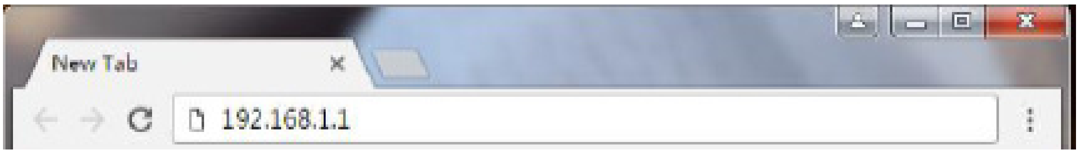
Internet Connection

This Chapter describes about internet connection through web UI.

It contains the following sections:

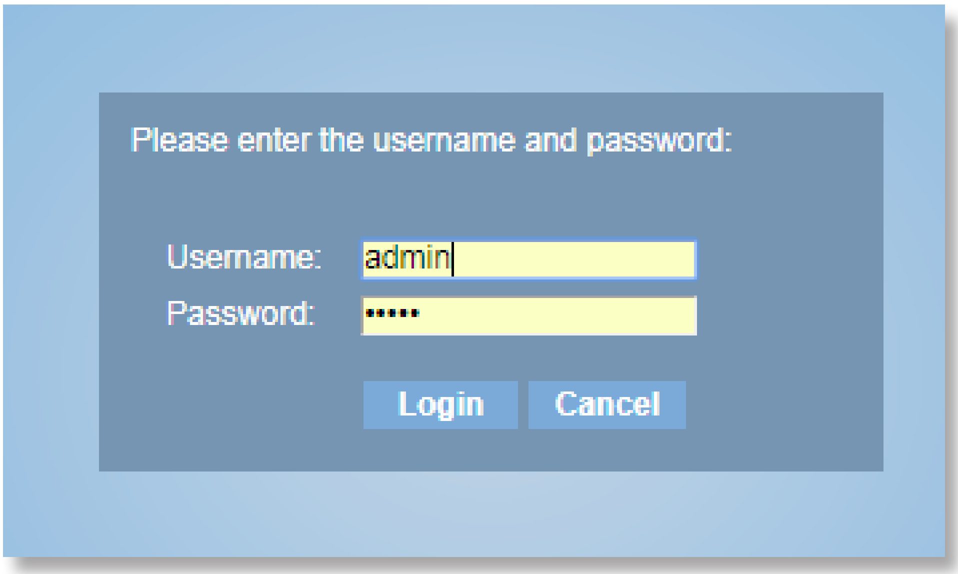
3.1 Login

Step 1 Start a web brower on the client connected to the modem router, then visit **192.168.1.1.**



192.168.1.1

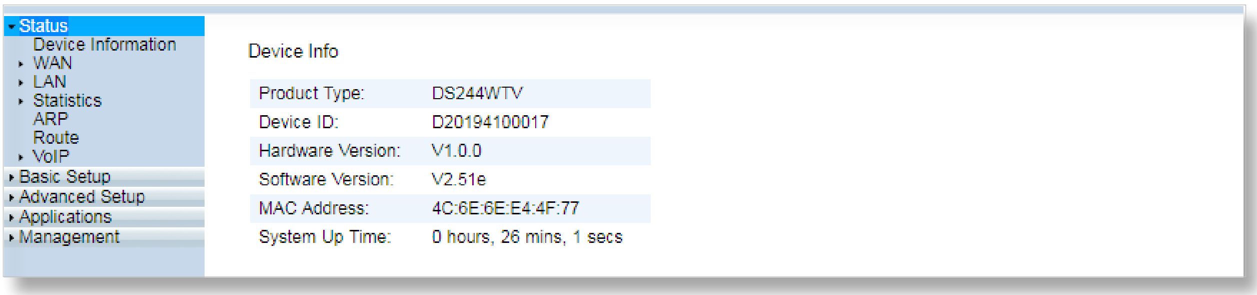
Step 2 Enter the default login user name and password (both are **admin**), and click **Login**.


Please enter the username and password:

Username: admin

Password: •••••

To prevent an unauthorized user from changing the settings of the modem router, you'd better change the default login user name and password.



Device Info

Product Type:	DS244WTV
Device ID:	D20194100017
Hardware Version:	V1.0.0
Software Version:	V2.51e
MAC Address:	4C:6E:6E:E4:4F:77
System Up Time:	0 hours, 26 mins, 1 secs

3.2 Logout

Click **Logout** on the upper right corner of the web UI also can log out.

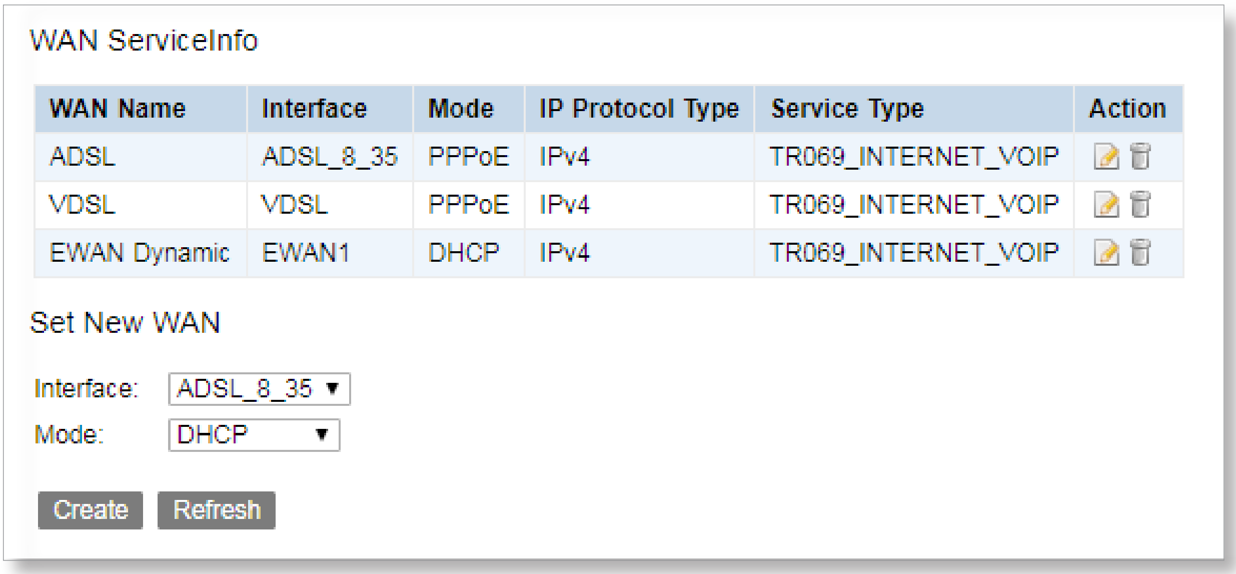
3.3 Internet Status

The **Home** page allows you to view the network status of the router, WiFi information, Online device and other status information.

3.4 Basic Setup

WAN Interface

There are three WAN Service has been created: ADSL, VDSL and EWAN Dynamic. According to your atual situation, choose your connection mode to edit the settings. (Take PPPoE connection mode for VDSL as an example in the following illustrations.) Enter the MTU, user name, password or other related information provided by your ISP. And the click **Apply**.



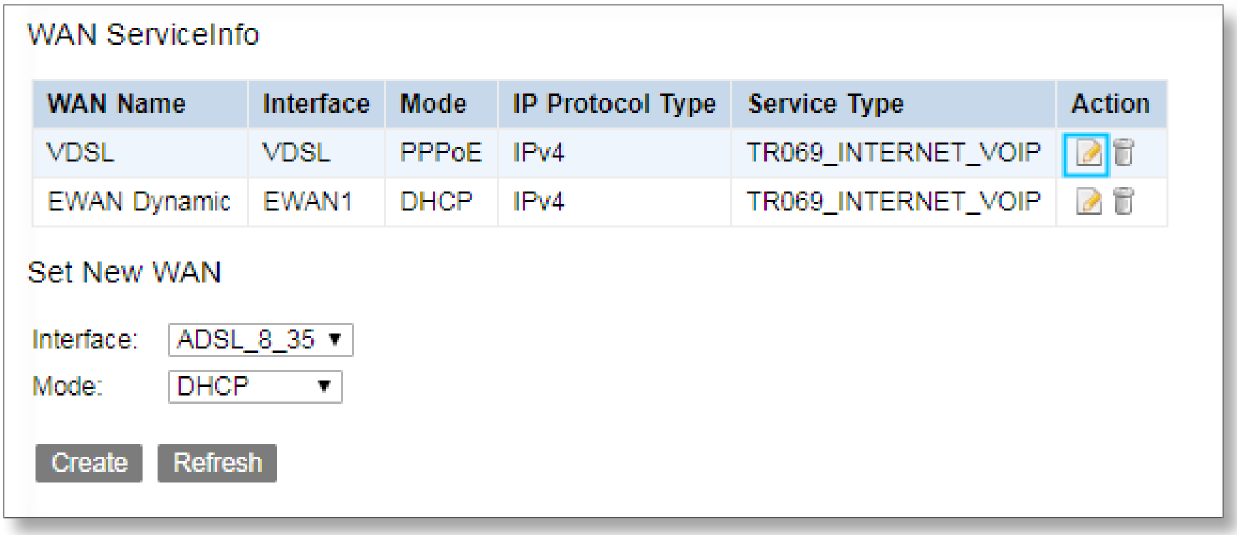
WAN ServiceInfo

WAN Name	Interface	Mode	IP Protocol Type	Service Type	Action
ADSL	ADSL_8_35	PPPoE	IPv4	TR069_INTERNET_VOIP	✎ 🗑
VDSL	VDSL	PPPoE	IPv4	TR069_INTERNET_VOIP	✎ 🗑
EWAN Dynamic	EWAN1	DHCP	IPv4	TR069_INTERNET_VOIP	✎ 🗑

Set New WAN

Interface: ADSL_8_35 ▼

Mode: DHCP ▼



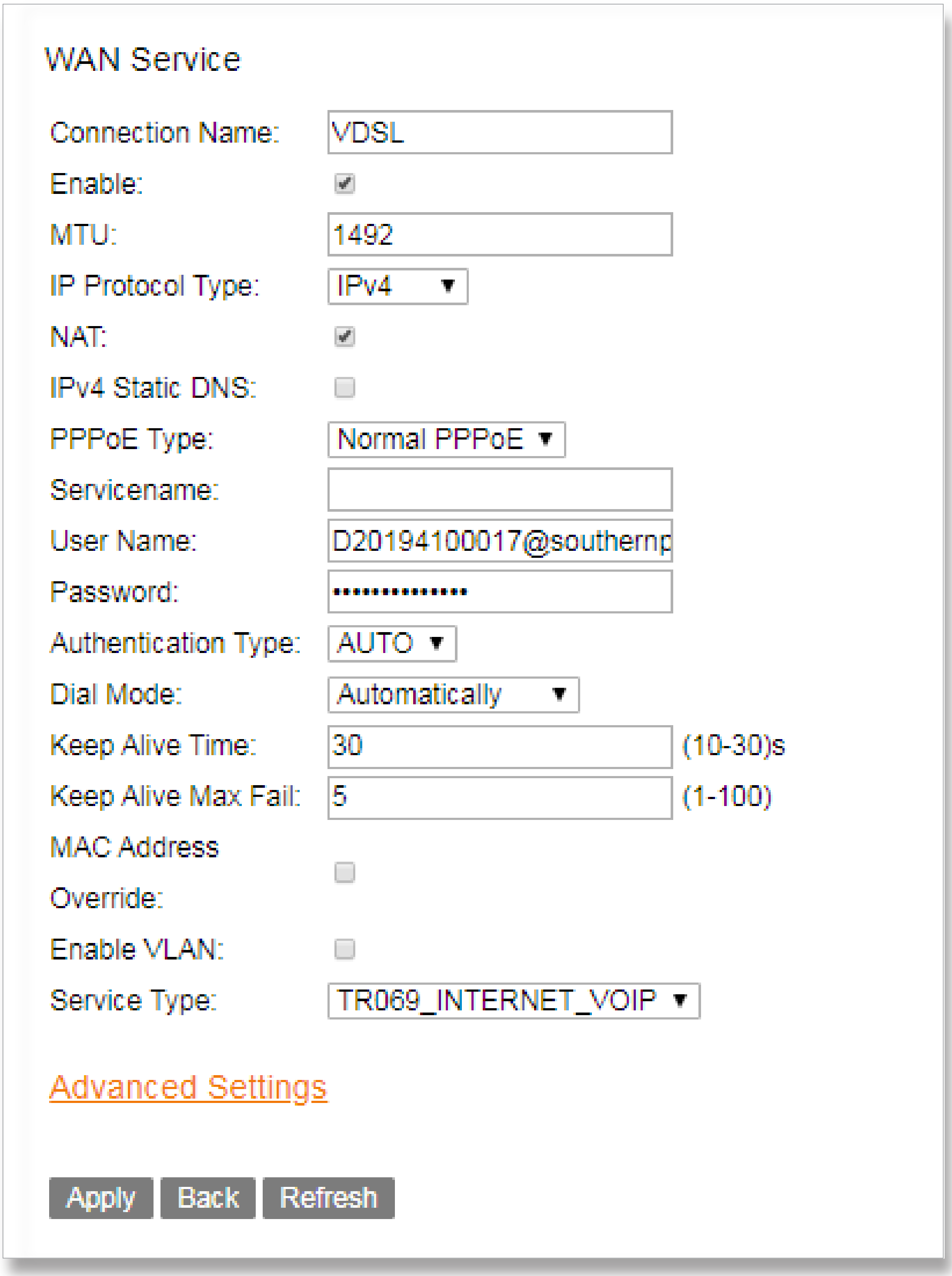
WAN ServiceInfo

WAN Name	Interface	Mode	IP Protocol Type	Service Type	Action
VDSL	VDSL	PPPoE	IPv4	TR069_INTERNET_VOIP	✎ 🗑
EWAN Dynamic	EWAN1	DHCP	IPv4	TR069_INTERNET_VOIP	✎ 🗑

Set New WAN

Interface: ADSL_8_35 ▼

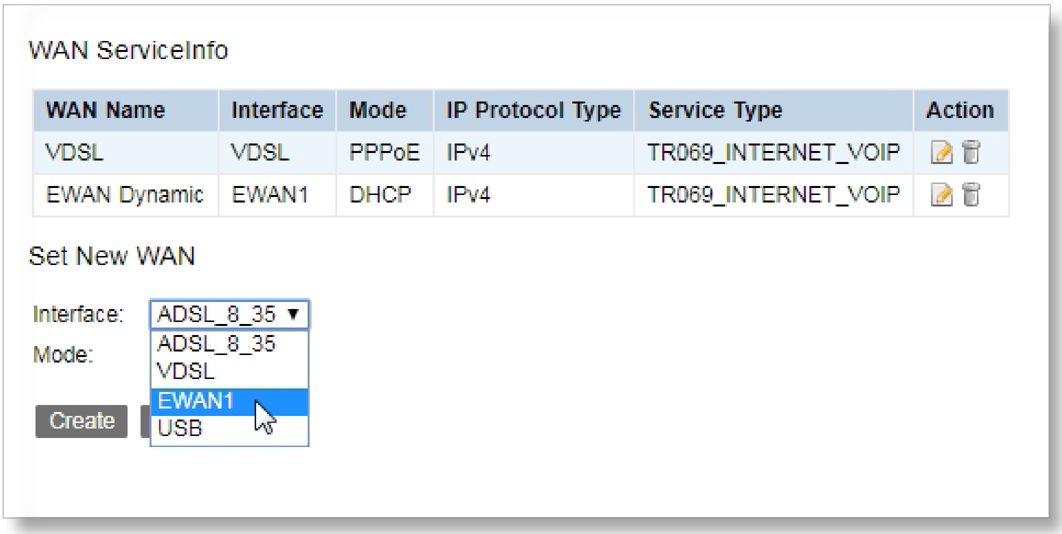
Mode: DHCP ▼



WAN Service

Connection Name:	VDSL	
Enable:	☑	
MTU:	1492	
IP Protocol Type:	IPv4 ▼	
NAT:	☑	
IPv4 Static DNS:	□	
PPPoE Type:	Normal PPPoE ▼	
Servicename:		
User Name:	D20194100017@southernp	
Password:	•••••••••••••••	
Authentication Type:	AUTO ▼	
Dial Mode:	Automatically ▼	
Keep Alive Time:	30	(10-30)s
Keep Alive Max Fail:	5	(1-100)
MAC Address Override:	□	
Enable VLAN:	□	
Service Type:	TR069_INTERNET_VOIP ▼	

Note: If your connection mode is not in one of these three, you can create a new one by choosing your actual interface and mode, then click **Create**. (Take PPPoE connection mode for EWAN1 as an example in the following illustrations.) Enter the MTU, user name, password or other related information provided by your ISP. And then click **Apply**.



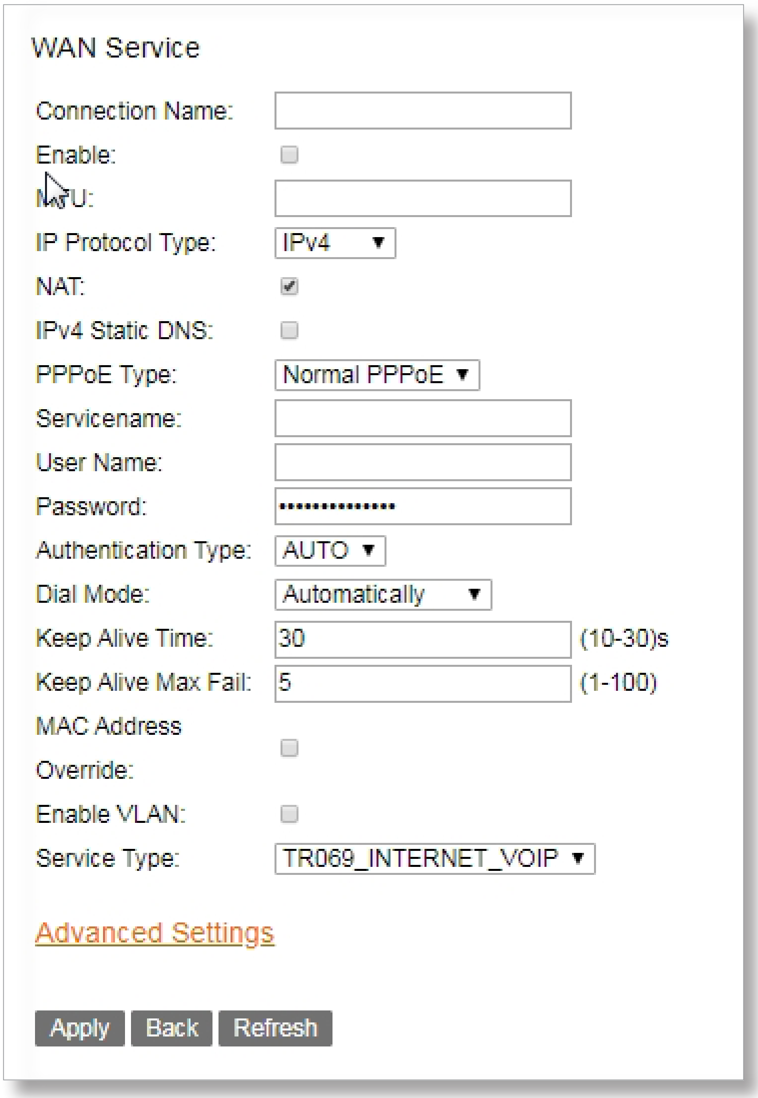
WAN ServiceInfo

WAN Name	Interface	Mode	IP Protocol Type	Service Type	Action
VDSL	VDSL	PPPoE	IPv4	TR069_INTERNET_VOIP	
EWAN Dynamic	EWAN1	DHCP	IPv4	TR069_INTERNET_VOIP	

Set New WAN

Interface: ADSL_8_35 ▾

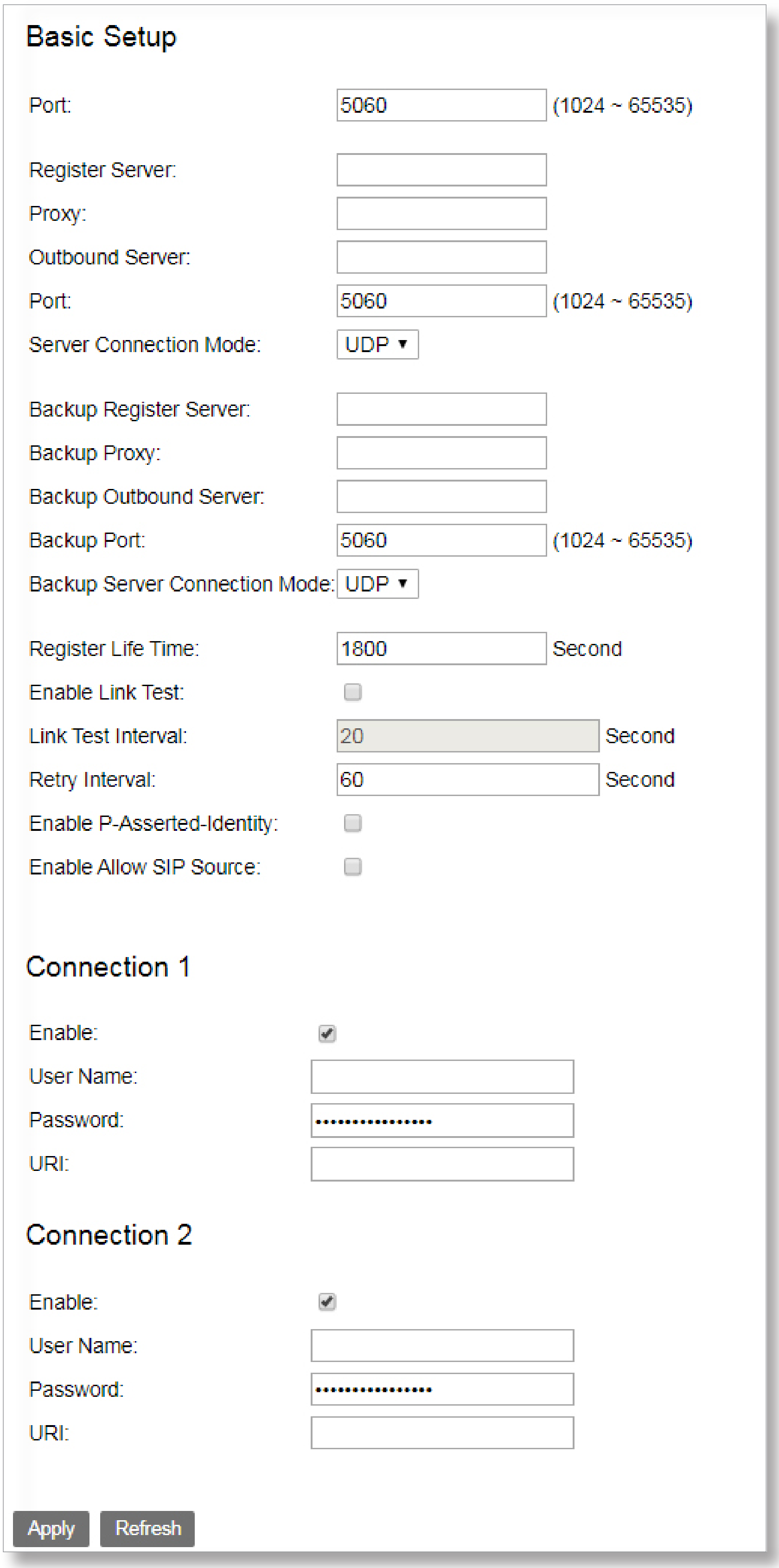
Mode:



WAN Service

Connection Name:	
Enable:	□
MTU:	
IP Protocol Type:	IPv4 ▾
NAT:	☑
IPv4 Static DNS:	□
PPPoE Type:	Normal PPPoE ▾
Servicename:	
User Name:	
Password:	•••••••••••••••
Authentication Type:	AUTO ▾
Dial Mode:	Automatically ▾
Keep Alive Time:	30 (10-30)s
Keep Alive Max Fail:	5 (1-100)
MAC Address Override:	□
Enable VLAN:	□
Service Type:	TR069_INTERNET_VOIP ▾

Enabling VoIP feature if necessary, go to the **Application** > **VoIP** > **Basic Setup** page. Enter the Register Server, Proxy, and other information provided by ISP.



Basic Setup

Port:	5060	(1024 ~ 65535)
Register Server:		
Proxy:		
Outbound Server:		
Port:	5060	(1024 ~ 65535)
Server Connection Mode:	UDP ▾	
Backup Register Server:		
Backup Proxy:		
Backup Outbound Server:		
Backup Port:	5060	(1024 ~ 65535)
Backup Server Connection Mode:	UDP ▾	
Register Life Time:	1800	Second
Enable Link Test:	□	
Link Test Interval:	20	Second
Retry Interval:	60	Second
Enable P-Asserted-Identity:	□	
Enable Allow SIP Source:	□	

Connection 1

Enable:	☑
User Name:	
Password:	•••••••••••••••••
URI:	

Connection 2

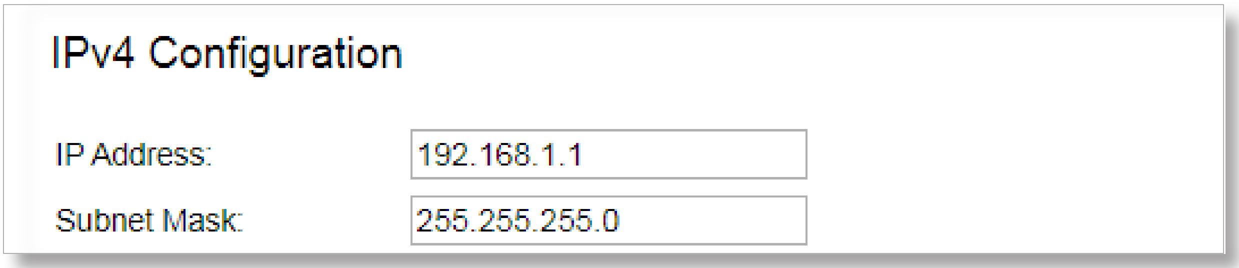
Enable:	☑
User Name:	
Password:	•••••••••••••••••
URI:	

3.5 LAN

Here you can configure the LAN settings. Choose **Basic Setup > LAN** to enter the configuration page. It allows you to modify the LAN IP of the modem router, configure the DHCP server settings, and DNS server settings.

3.5.1 IPv4 Configuration

Primary LAN IP Address



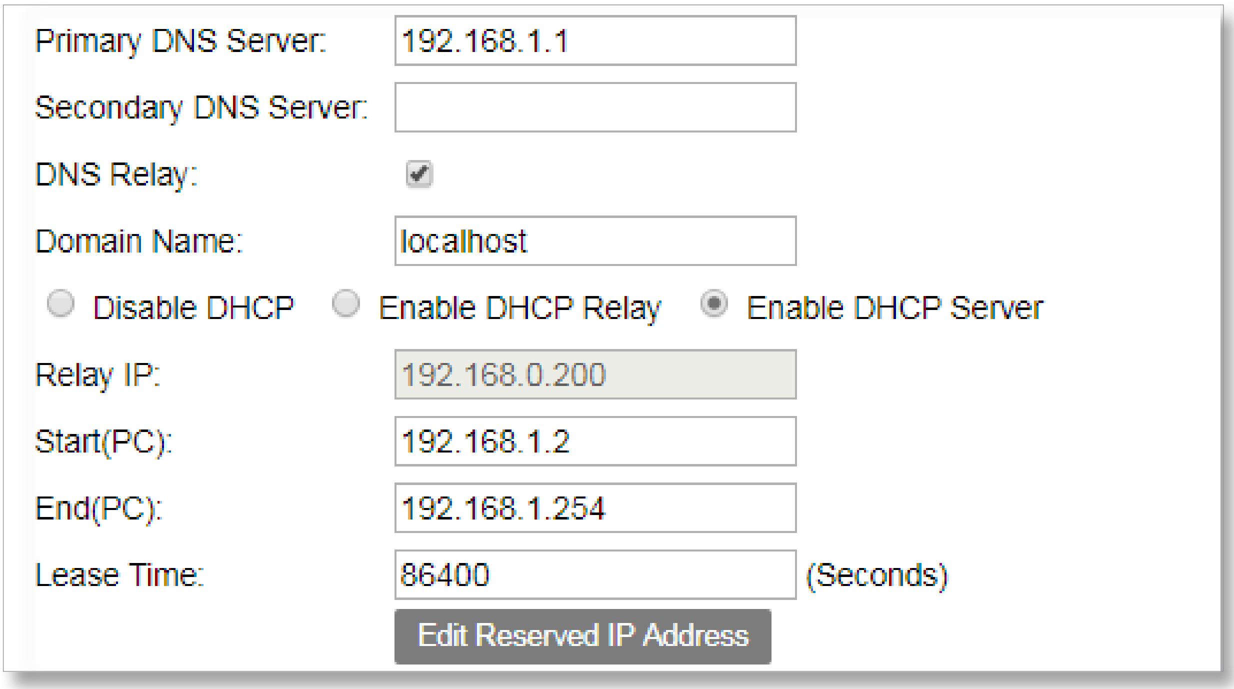
IPv4 Configuration

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0

Parameter	Description
IP Address	It specifies the LAN IP address of the modem router, that is, the login address of the web UI of the modem router.
Subnet Mask	The LAN subnet mask of the LAN port. It specifies the network segment of the LAN IP address.

Note: After the LAN IP address is changed, the computers in LAN need release their IP addresses and obtain them again to ensure gateway of the computers is the new LAN IP address.

DHCP Server



Primary DNS Server:	192.168.1.1
Secondary DNS Server:	
DNS Relay:	☑
Domain Name:	localhost

○ Disable DHCP ○ Enable DHCP Relay ● Enable DHCP Server

Relay IP:	192.168.0.200
Start(PC):	192.168.1.2
End(PC):	192.168.1.254
Lease Time:	86400 (Seconds)

Parameter	Description
Primary DNS server	It specifies the primary DNS IP addresses assigned to connected devices.
Secondary DNS server	It specifies the secondary DNS IP addresses assigned to connected devices.
Disable DHCP	If this option is selected, the DHCP server of this modem router is disabled. In this case, this modem router does not assign IP addresses and related parameters to its clients.
Enable DHCP Relay	If this option is selected, the modem router works as a DHCP relay. The DHCP requests from local computers will forward to the DHCP server runs on WAN side.
Enable DHCP Server	It indicates that the modem router can assign IP addresses to connected devices. **Start IP Address:** It specifies the start IP address of the IP address pool of the DHCP server. **End IP Address:** It specifies the end IP address of the IP address pool of the DHCP server.
Leased Time (seconds)	It specifies the validity period of one IP address assigned to a device by the modem router.

DHCP Reservation

Generally, IP addresses assigned by the modem router to devices are changeable. Some functions require static device IP addresses, such as DMZ Host and virtual server. In this case you can use the DHCP reservation function to bind IP addresses with the devices involved in the functions.

To bind an IP address to a specified device

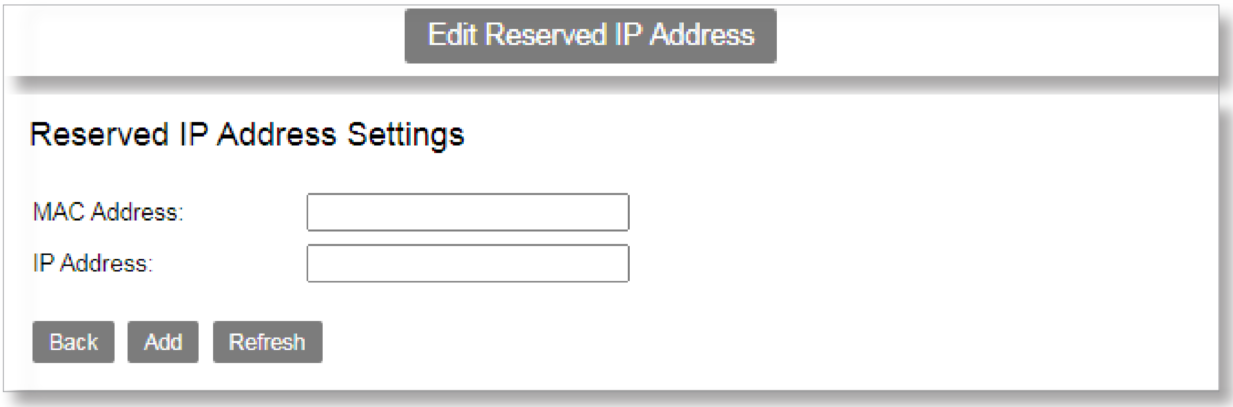
Step 1 Go to **Basic Setup > LAN > IPv4 Configuration** page.

Step 2 Click **Edit Reserved IP Address**.

Step 3 Enter the MAC address of the specified device in the **MAC Address** box.

Step 4 Enter an IP address included in the DHCP pool of the device. Assume that the IP address of the device is 192.168.1.1. You can enter 192.168.1.X (X ranges from 2 to 253).

Step 5 Click **Apply**.

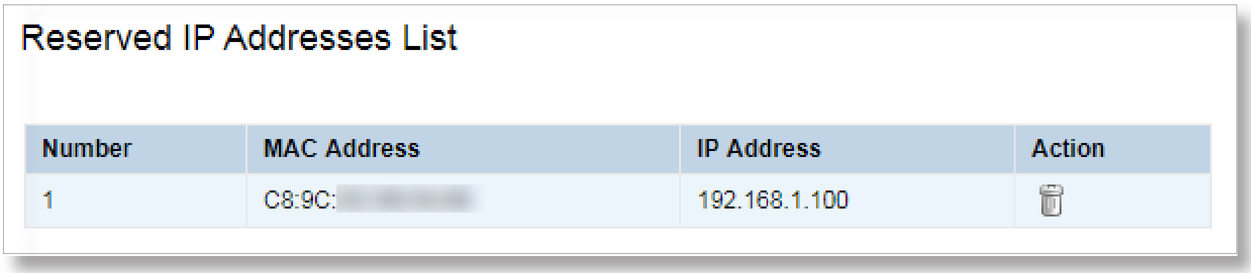


Reserved IP Address Settings

MAC Address:

IP Address:

The added entry displays in the following table.



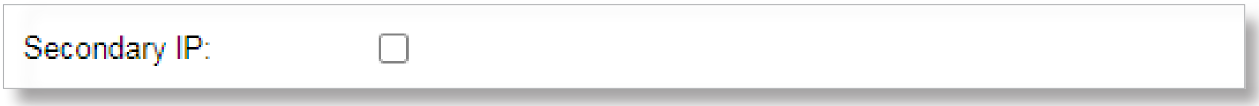
Reserved IP Addresses List

Number	MAC Address	IP Address	Action
1	C8:9C:[redacted]	192.168.1.100	🗑

Note: The IP address specified in the table will be always assigned to the device with the specified MAC address in the table after the rule takes effect.

Secondary LAN IP Address

By default, there is only one LAN IP address for the modem router, and you can access the web UI of the modem router by this IP address. And the modem router allows you to set up a second LAN IP address for the modem router.



Secondary IP: ☐

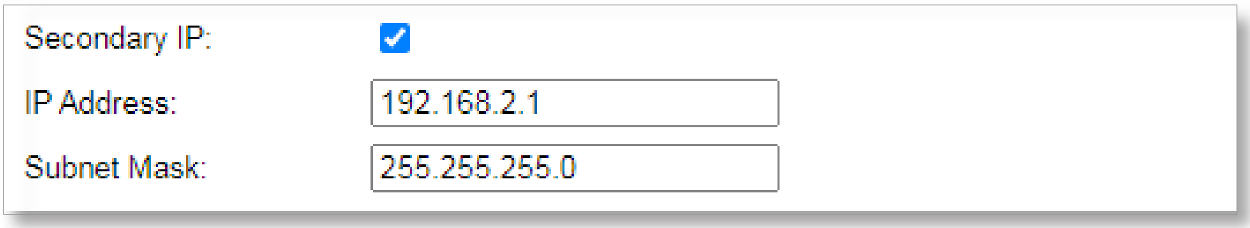
To Set up a second LAN IP address

Step 1 Check the **Secondary IP** option.

Step 2 Specify an IP address that belongs to a different network segment of the first IP address, such as 192.168.2.1.

Step 3 Specify a subnet mask that fits the network segment, such as 255.255.255.0.

Step 4 Click **Apply**.



Secondary IP: ☑

IP Address: 192.168.2.1

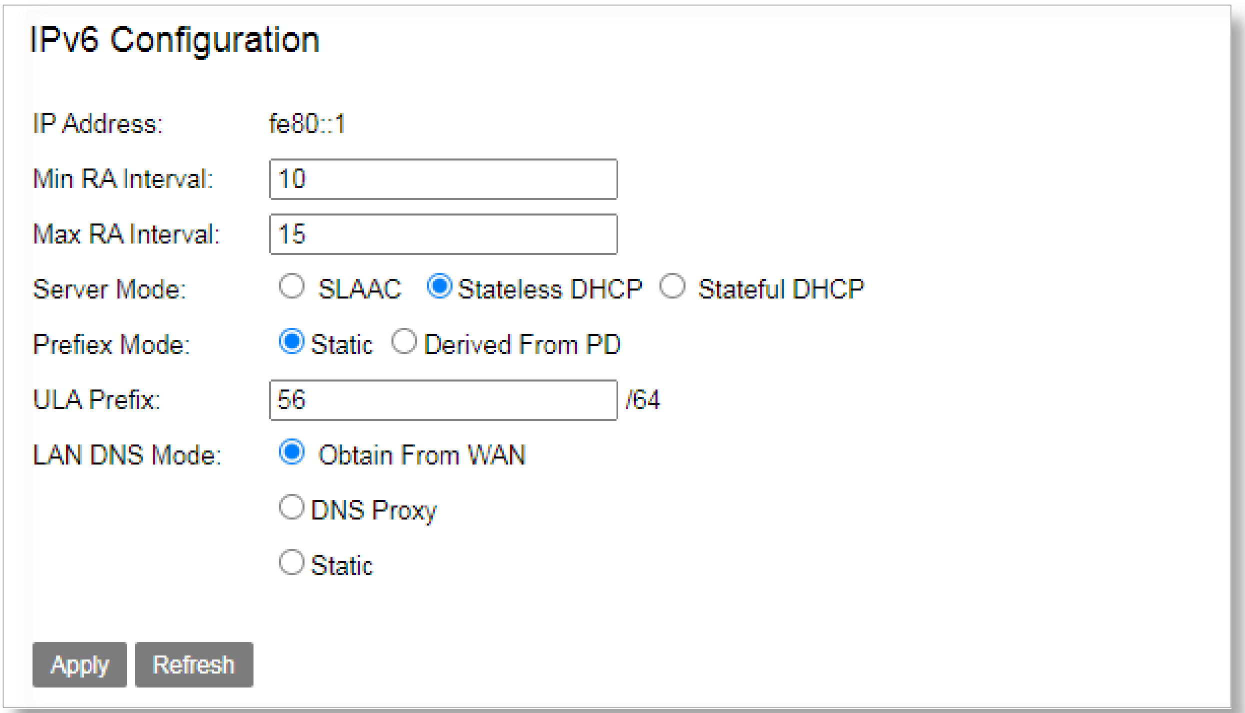
Subnet Mask: 255.255.255.0

Tip: The second LAN IP address can also be used to log in to the web UI of the modem router.

3.5.2 IPv6 Configuration

The Modem router supports two IPv6 address configuration types: SLAAC, Stateless and Stateful. Select one to follow as required.

Stateless Address Configuration



IPv6 Configuration

IP Address: fe80::1

Min RA Interval: 10

Max RA Interval: 15

Server Mode: ○ SLAAC ● Stateless DHCP ○ Stateful DHCP

Prefix Mode: ● Static ○ Derived From PD

ULA Prefix: 56 /64

LAN DNS Mode: ● Obtain From WAN

○ DNS Proxy

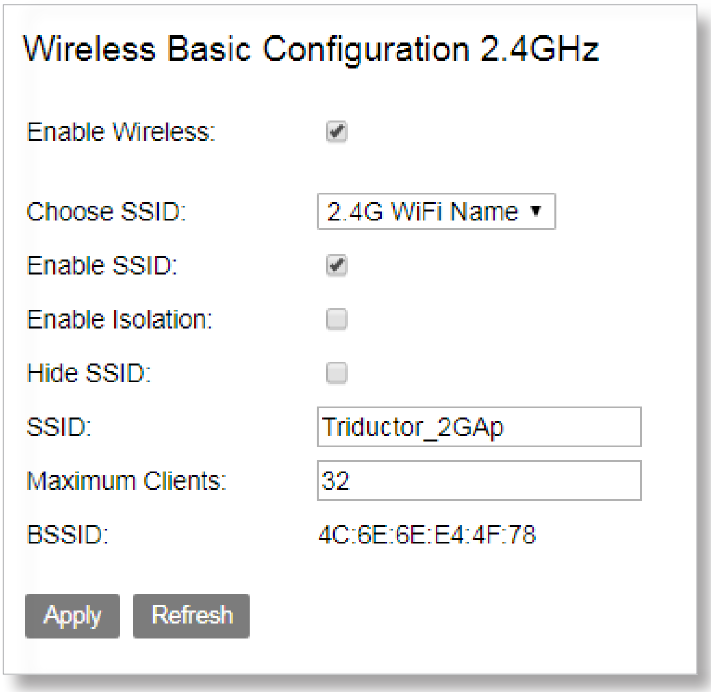
○ Static

Parameter	Description
SLAAC	Stateless address autoconfiguration.
Stateless	The computers in LAN only obtain prefix and DNS information from the modem router. The interface ID is generated based on its MAC address automatically.
Stateful	Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Select this option and configure the start/end interface ID and lease time. The modem router will automatically assign IPv6 addresses to IPv6 clients.
Prefix Mode	**Static:** If this option is selected, you need to manually configure the prefix. **Derived From PD:** If this option is selected, the prefix can be automatically generated from PD.
URL Prefix	The ULA prefix can be generated by the modem router, or be set up manually.
LAN DNS Mode	Select one to follow according to your actual needs

3.6 Wireless

Basic Configuration 2.4GHz

The wireless feature is enabled by default. The default SSID for 2.4 GHz wireless network is Triductor_2GAp, and for 5 GHz wireless network is Triductor_5GAp. By default, there is a preset WiFi password 12345678 at the WPA Preshare key box in Security Setting page for both 2.4 GHz and 5 GHz wireless networks.



Wireless Basic Configuration 2.4GHz

Enable Wireless: ☑

Choose SSID: 2.4G WiFi Name ▾

Enable SSID: ☑

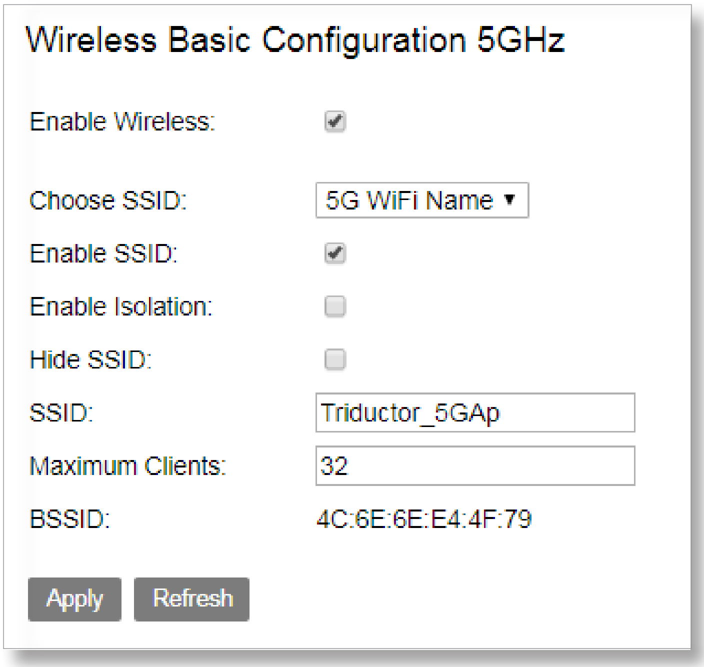
Enable Isolation: □

Hide SSID: □

SSID: Triductor_2GAp

Maximum Clients: 32

BSSID: 4C:6E:6E:E4:4F:78



Wireless Basic Configuration 5GHz

Enable Wireless: ☑

Choose SSID: 5G WiFi Name ▾

Enable SSID: ☑

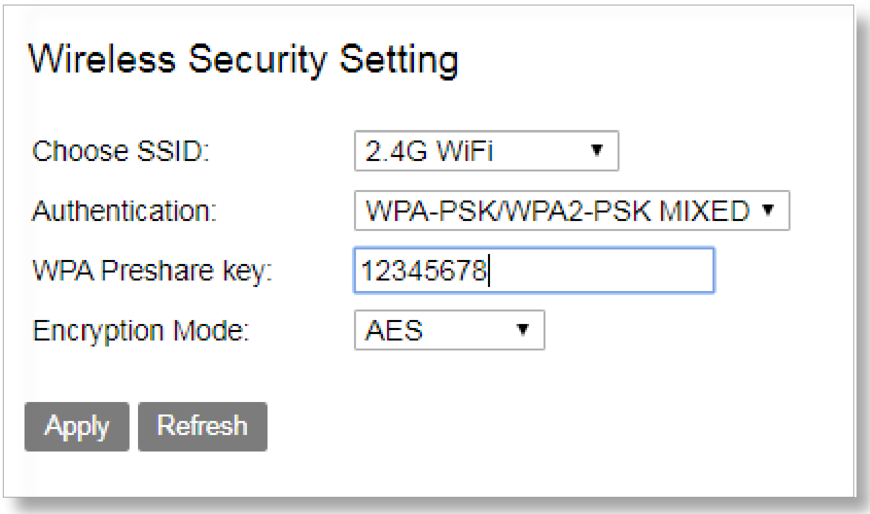
Enable Isolation: □

Hide SSID: □

SSID: Triductor_5GAp

Maximum Clients: 32

BSSID: 4C:6E:6E:E4:4F:79



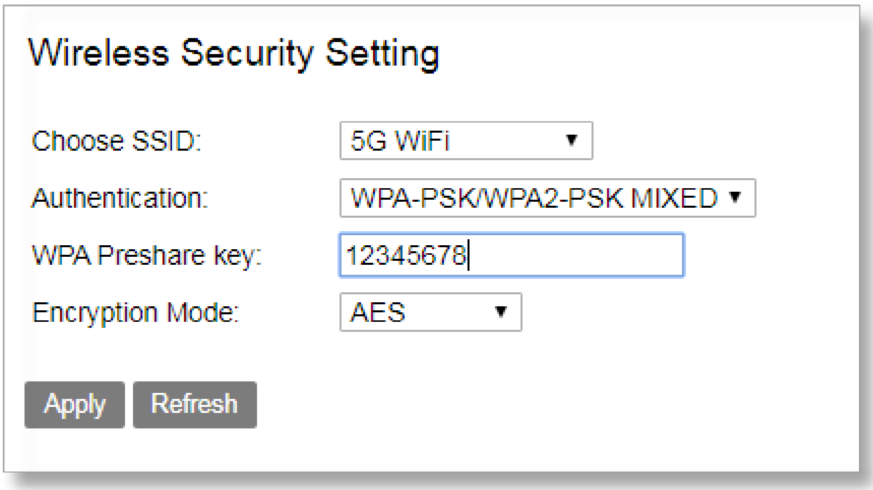
Wireless Security Setting

Choose SSID: 2.4G WiFi

Authentication: WPA-PSK/WPA2-PSK MIXED

WPA Preshare key: 12345678

Encryption Mode: AES



Wireless Security Setting

Choose SSID: 5G WiFi

Authentication: WPA-PSK/WPA2-PSK MIXED

WPA Preshare key: 12345678

Encryption Mode: AES

To customize a WiFi name and password:

Step 1 Enter the **Basic Setup > Wireless > Basic Configuration 2.4GHz/Basic Configuration 5GHz / Security Setting** page.

Step 2 **SSID:** Enter new Wifi name at SSID box for 2.4GHz / 5GHz wireless networks.

Step 3 **WPA Preshare Key:** Enter new WiFi passwords for 2.4GHz / 5GHz wireless networks.

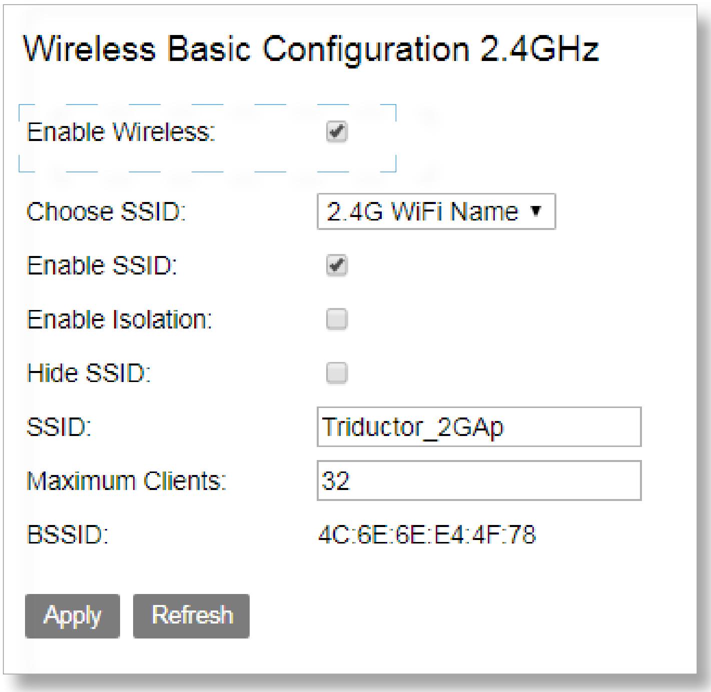
Step 4 Click **Apply**.

To disable wireless function:

Step 1 Enter the **Basic Setup > Wireless > Basic Configuration 2.4GHz/Basic Configuration 5GHz** page.

Step 2 Deselet the Wireless Enable option for 2.4GHz / 5GHz wireless networks.

Step 3 Click **Apply**.



Wireless Basic Configuration 2.4GHz

Enable Wireless: ☑

Choose SSID: 2.4G WiFi Name ▾

Enable SSID: ☑

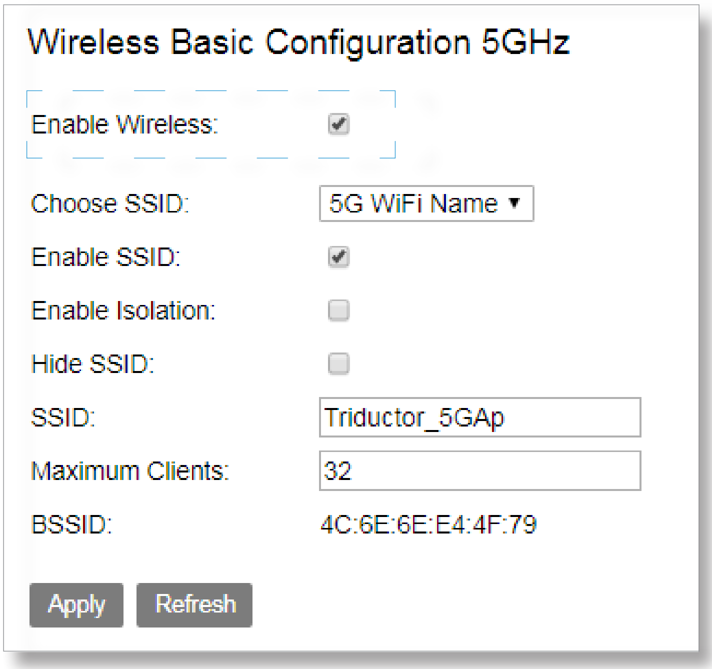
Enable Isolation: ☐

Hide SSID: ☐

SSID: Triductor_2GAp

Maximum Clients: 32

BSSID: 4C:6E:6E:E4:4F:78



Wireless Basic Configuration 5GHz

Enable Wireless: ☑

Choose SSID: 5G WiFi Name ▾

Enable SSID: ☑

Enable Isolation: ☐

Hide SSID: ☐

SSID: Triductor_5GAp

Maximum Clients: 32

BSSID: 4C:6E:6E:E4:4F:79

When the wireless function is disabled, wireless devices cannot connect to the modem router wirelessly.

Chapter 4

Advanced Setup

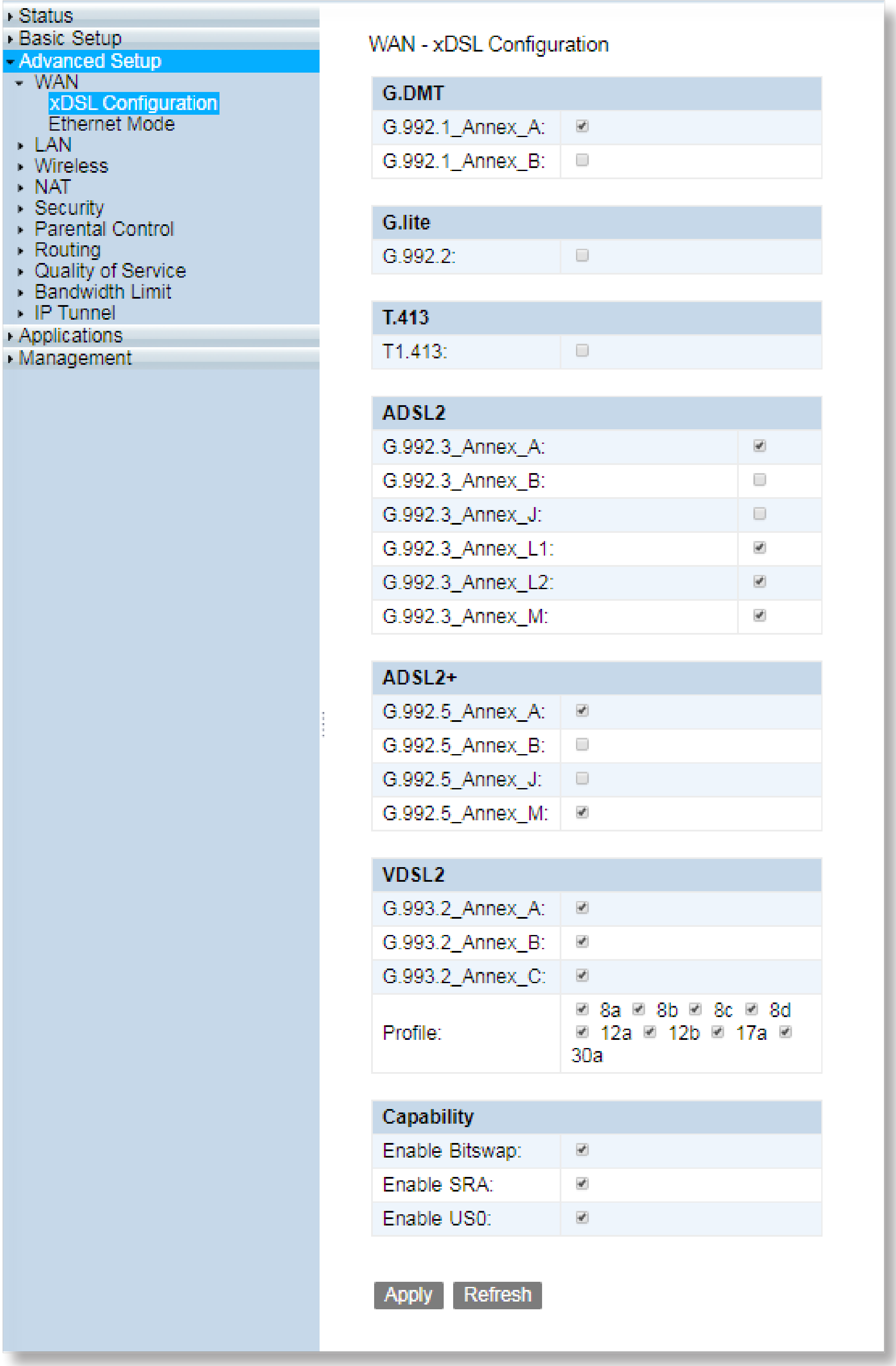
This Chapter describes about advanced setup of web UI.

It contains the following sections:

4.1 WAN

4.1.1 xDSL Configuration

Go to **Advanced Setup** > **WAN** > **xDSL Configuration** page. This page is to configurate for different standards and rate models. It is recommended that you keep the default parameters.



WAN - xDSL Configuration

G.DMT	
G.992.1_Annex_A:	☑
G.992.1_Annex_B:	□

G.lite	
G.992.2:	□

T.413	
T1.413:	□

ADSL2	
G.992.3_Annex_A:	☑
G.992.3_Annex_B:	□
G.992.3_Annex_J:	□
G.992.3_Annex_L1:	☑
G.992.3_Annex_L2:	☑
G.992.3_Annex_M:	☑

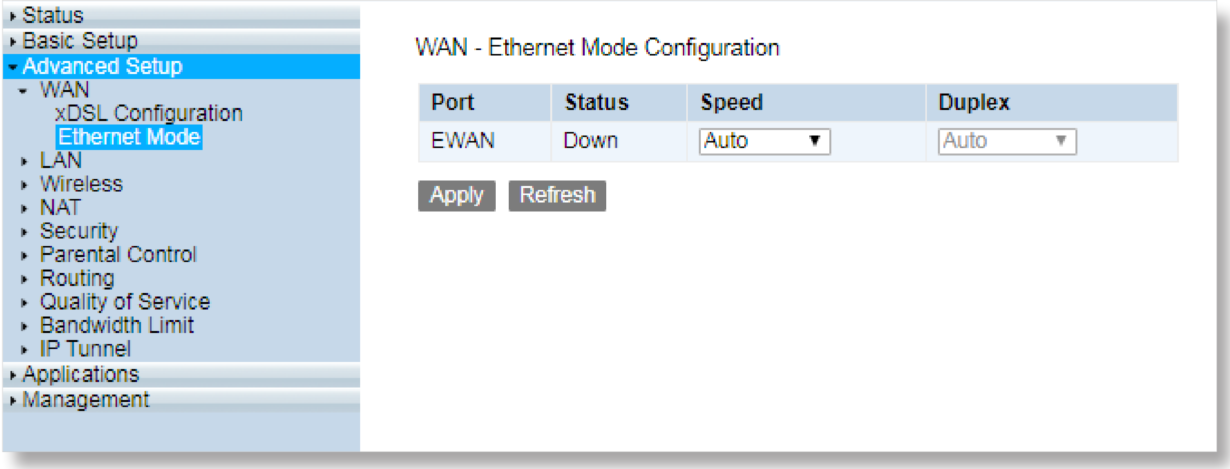
ADSL2+	
G.992.5_Annex_A:	☑
G.992.5_Annex_B:	□
G.992.5_Annex_J:	□
G.992.5_Annex_M:	☑

VDSL2	
G.993.2_Annex_A:	☑
G.993.2_Annex_B:	☑
G.993.2_Annex_C:	☑
Profile:	☑ 8a ☑ 8b ☑ 8c ☑ 8d ☑ 12a ☑ 12b ☑ 17a ☑ 30a

Capability	
Enable Bitswap:	☑
Enable SRA:	☑
Enable US0:	☑

4.1.2 Ethernet Mode

Go to **Advanced Setup** > **WAN** > **Ethernet Mode** page. This page is to configurate for different standards and rate models. It is recommended that you keep the default parameters.

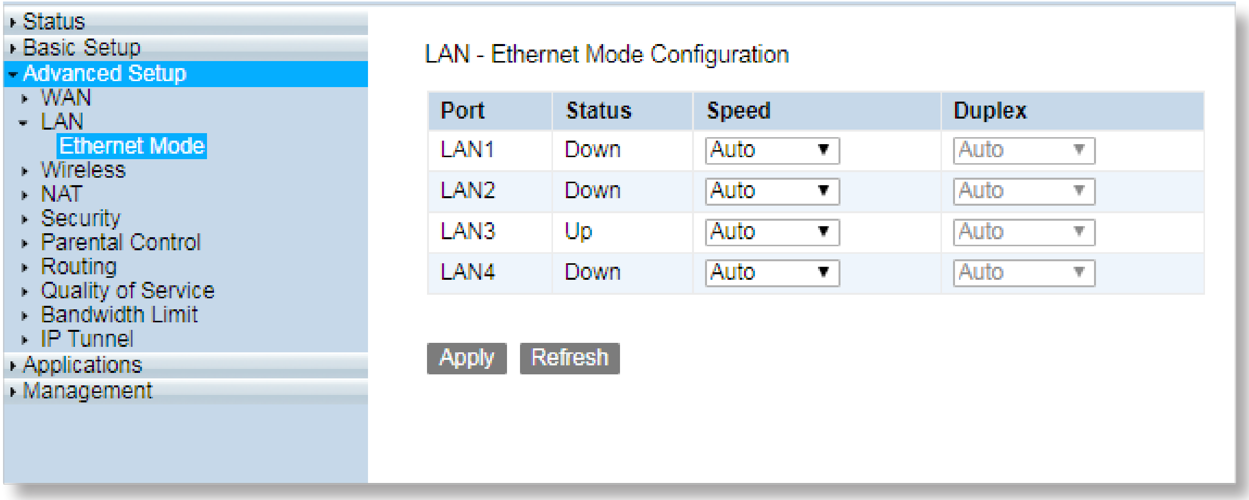


WAN - Ethernet Mode Configuration

Port	Status	Speed	Duplex
EWAN	Down	Auto ▼	Auto ▼

4.2 LAN

Go to **Advanced Setup** > **LAN** > **Ethernet Mode** page. This page is to configurate speed and corresponding duplex for LAN. It is recommended that you keep the default parameters.



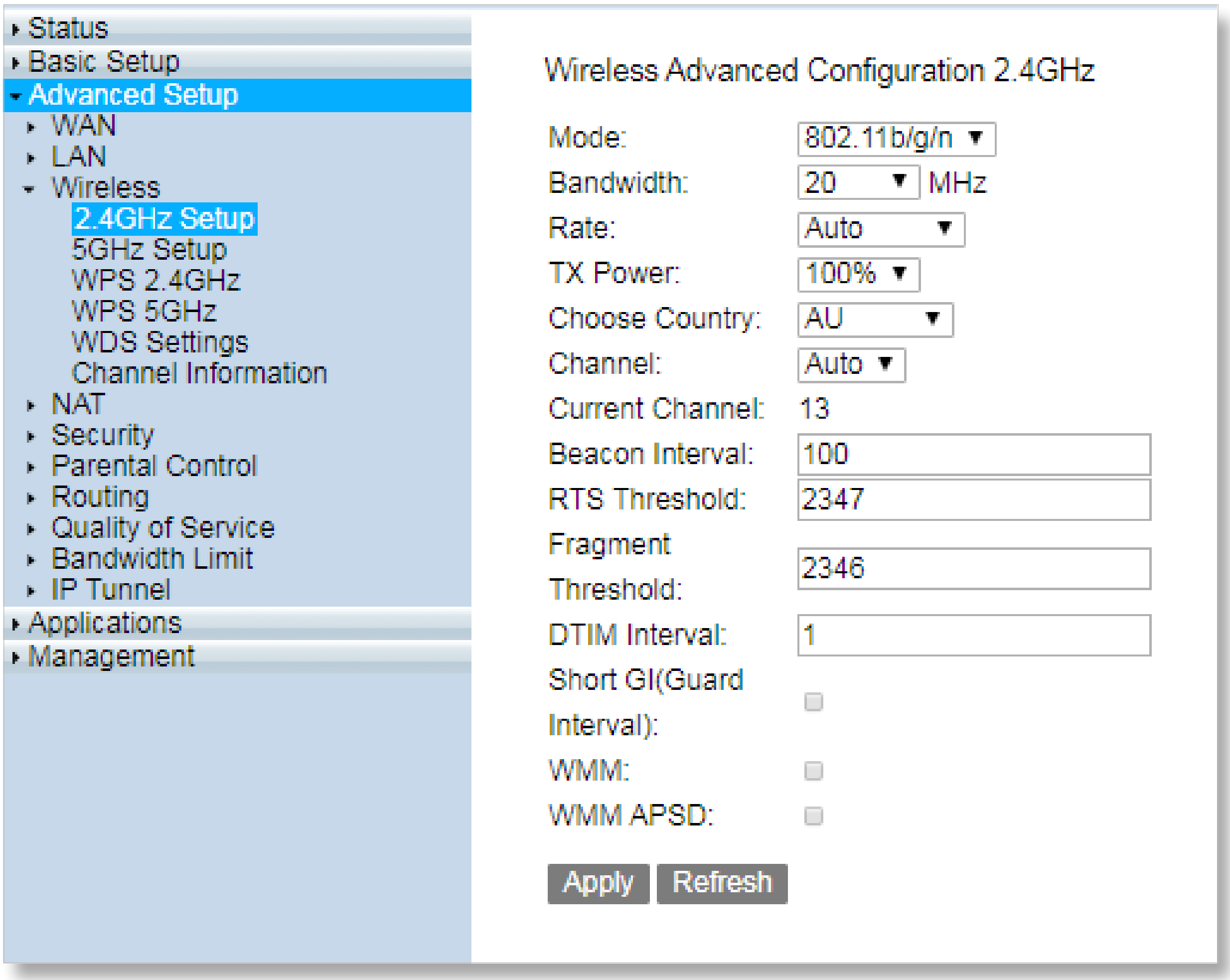
LAN - Ethernet Mode Configuration

Port	Status	Speed	Duplex
LAN1	Down	Auto	Auto
LAN2	Down	Auto	Auto
LAN3	Up	Auto	Auto
LAN4	Down	Auto	Auto

4.3 Wireless

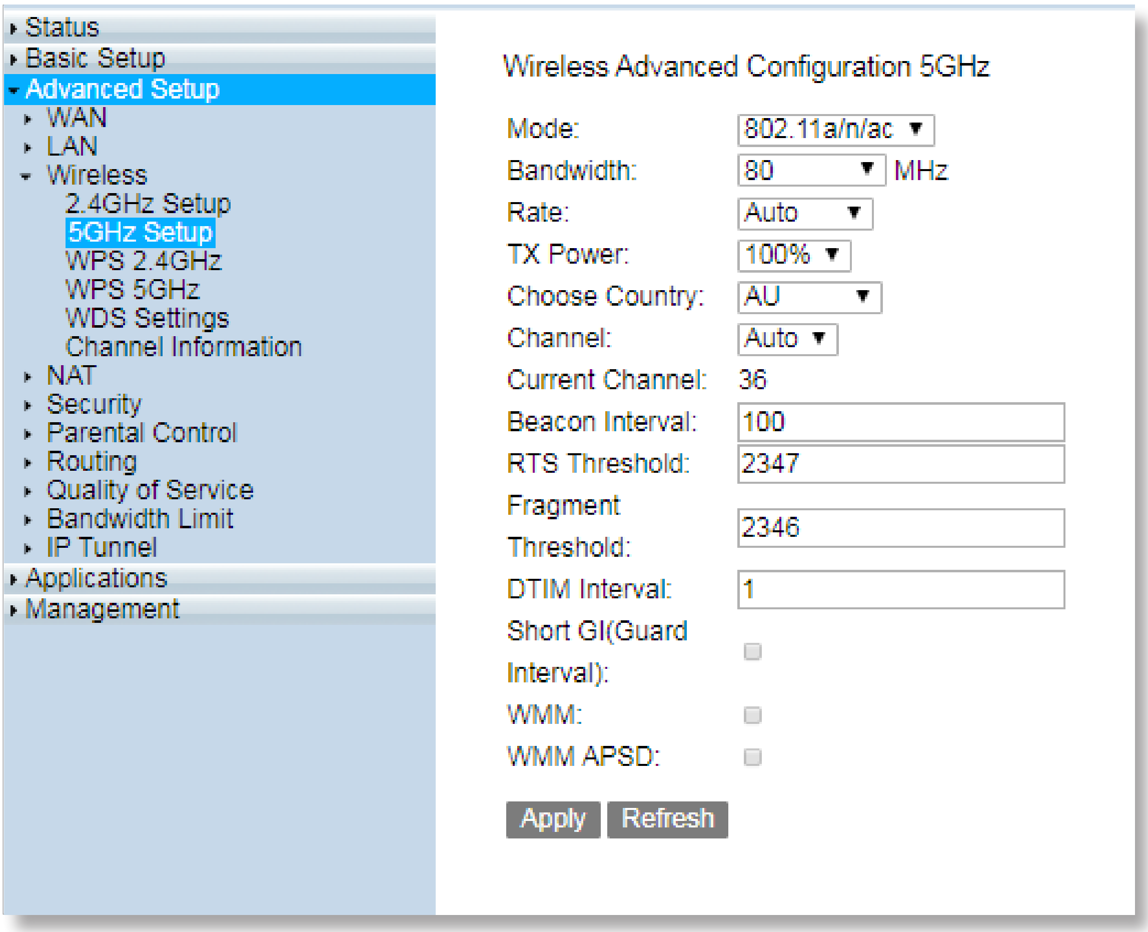
4.3.1 2.4GHz /5 GHz Setup

Go to **Advanced Setup** > **Wireless** > **2.4GHz/5GHz Setup** page. This page is to configurate for 2.4GHz Setup. It is recommended that you keep the default parameters.



Wireless Advanced Configuration 2.4GHz

Mode:	802.11b/g/n
Bandwidth:	20 MHz
Rate:	Auto
TX Power:	100%
Choose Country:	AU
Channel:	Auto
Current Channel:	13
Beacon Interval:	100
RTS Threshold:	2347
Fragment Threshold:	2346
DTIM Interval:	1
Short GI(Guard Interval):	☐
WMM:	☐
WMM APSD:	☐

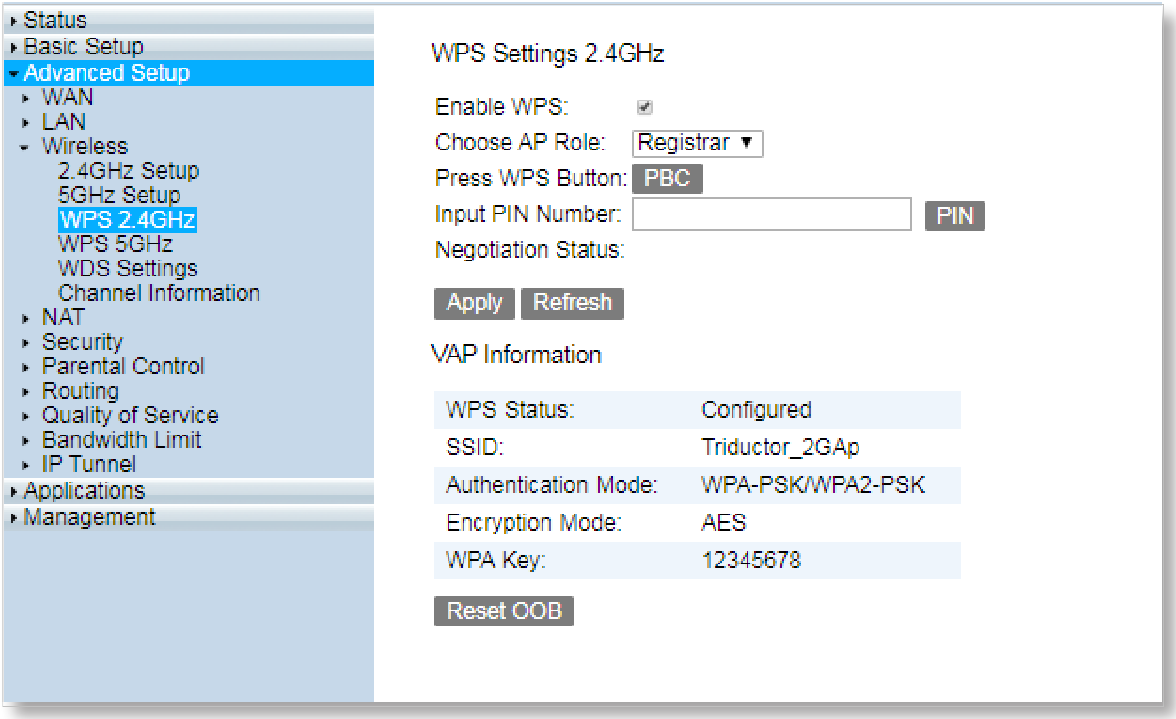


Wireless Advanced Configuration 5GHz

Mode:	802.11a/n/ac ▼
Bandwidth:	80 ▼ MHz
Rate:	Auto ▼
TX Power:	100% ▼
Choose Country:	AU ▼
Channel:	Auto ▼
Current Channel:	36
Beacon Interval:	100
RTS Threshold:	2347
Fragment Threshold:	2346
DTIM Interval:	1
Short GI(Guard Interval):	□
WMM:	□
WMM APSD:	□

4.3.2 WPS 2.4GHz/5GHz

Go to **Advanced Setup** > **Wireless** > **WPS 2.4GHz/5GHz** page. This page is to configurate for WPS 2.4GHz/5GHz. It is recommended that you keep the default parameters.



WPS Settings 2.4GHz

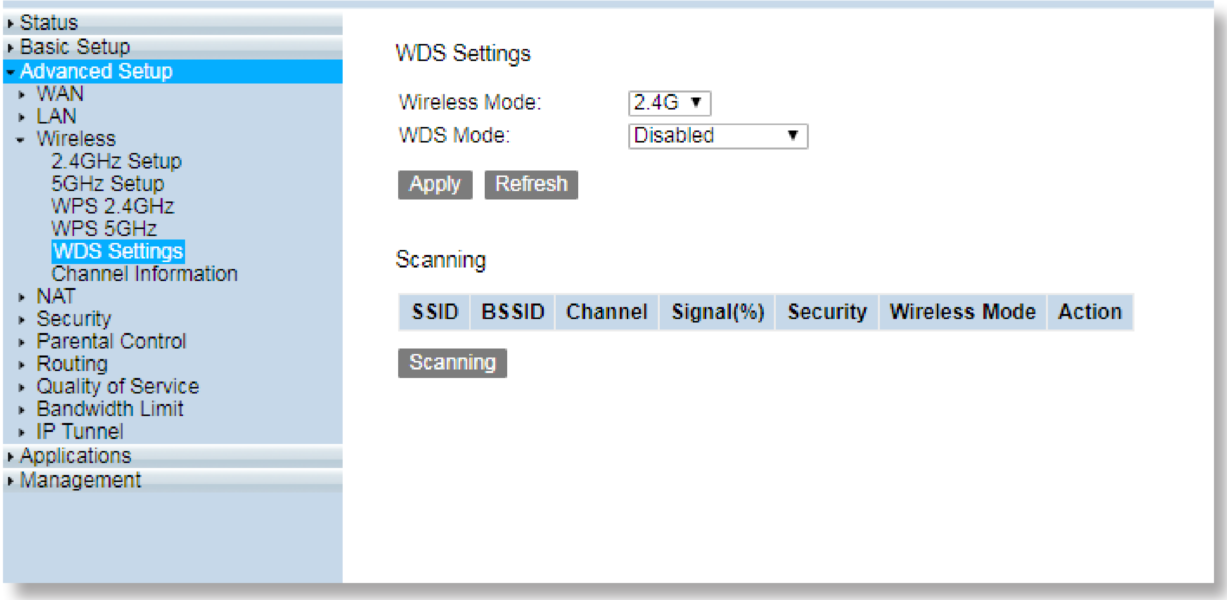
Enable WPS:	☑
Choose AP Role:	Registrar ▼
Press WPS Button:	PBC
Input PIN Number:	
Negotiation Status:	

VAP Information

WPS Status:	Configured
SSID:	Triductor_2GAp
Authentication Mode:	WPA-PSK/WPA2-PSK
Encryption Mode:	AES
WPA Key:	12345678

4.3.3 WDS Setting

Go to **Advanced Setup** > **Wireless** > **WDS Settings** page. This page is to configurate for WDS settings. It is recommended that you keep the default parameters.



WDS Settings

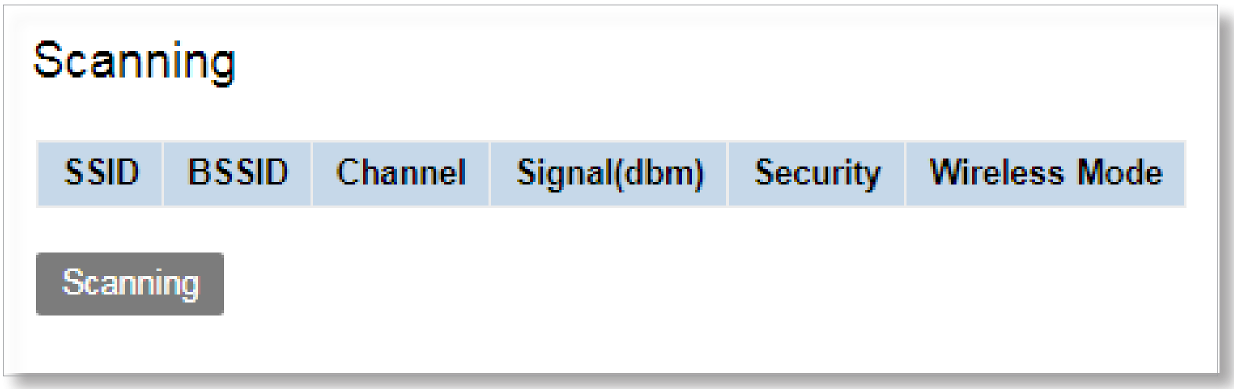
Wireless Mode: 2.4G

WDS Mode: Disabled

Scanning

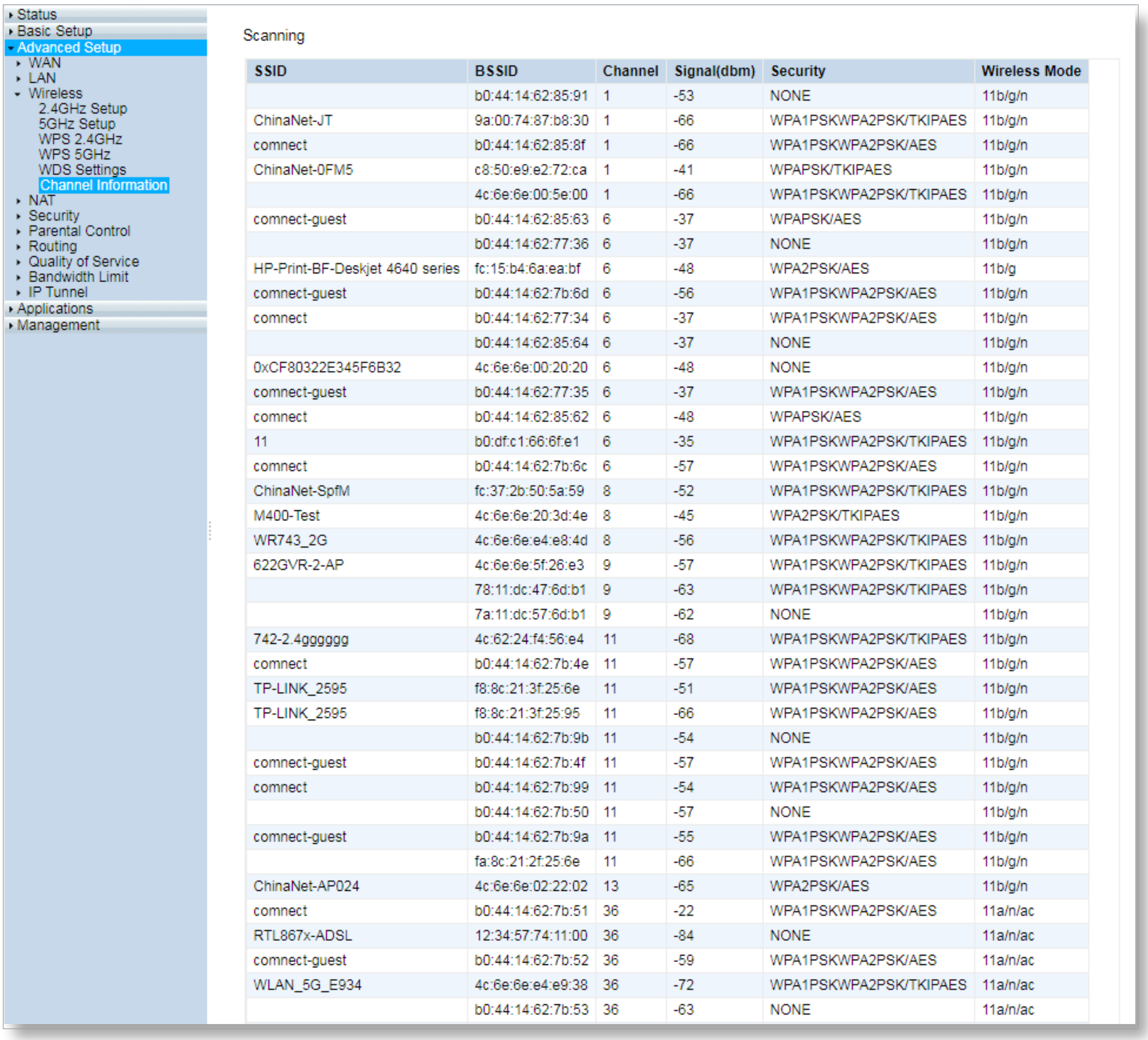
SSID	BSSID	Channel	Signal(%)	Security	Wireless Mode	Action

4.3.4 Channel Information



Scanning

SSID	BSSID	Channel	Signal(dbm)	Security	Wireless Mode



Scanning

SSID	BSSID	Channel	Signal(dbm)	Security	Wireless Mode
	b0:44:14:62:85:91	1	-53	NONE	11b/g/n
ChinaNet-JT	9a:00:74:87:b8:30	1	-66	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
comnect	b0:44:14:62:85:8f	1	-66	WPA1PSKWPA2PSK/AES	11b/g/n
ChinaNet-0FM5	c8:50:e9:e2:72:ca	1	-41	WPAPSK/TKIPAES	11b/g/n
	4c:6e:6e:00:5e:00	1	-66	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
comnect-guest	b0:44:14:62:85:63	6	-37	WPAPSK/AES	11b/g/n
	b0:44:14:62:77:36	6	-37	NONE	11b/g/n
HP-Print-BF-Deskjet 4640 series	fc:15:b4:6a:ea:bf	6	-48	WPA2PSK/AES	11b/g
comnect-guest	b0:44:14:62:7b:6d	6	-56	WPA1PSKWPA2PSK/AES	11b/g/n
comnect	b0:44:14:62:77:34	6	-37	WPA1PSKWPA2PSK/AES	11b/g/n
	b0:44:14:62:85:64	6	-37	NONE	11b/g/n
0xCF80322E345F6B32	4c:6e:6e:00:20:20	6	-48	NONE	11b/g/n
comnect-guest	b0:44:14:62:77:35	6	-37	WPA1PSKWPA2PSK/AES	11b/g/n
comnect	b0:44:14:62:85:62	6	-48	WPAPSK/AES	11b/g/n
11	b0:df:c1:66:6f:e1	6	-35	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
comnect	b0:44:14:62:7b:6c	6	-57	WPA1PSKWPA2PSK/AES	11b/g/n
ChinaNet-SpfM	fc:37:2b:50:5a:59	8	-52	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
M400-Test	4c:6e:6e:20:3d:4e	8	-45	WPA2PSK/TKIPAES	11b/g/n
WR743_2G	4c:6e:6e:e4:e8:4d	8	-56	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
622GVR-2-AP	4c:6e:6e:5f:26:e3	9	-57	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
	78:11:dc:47:6d:b1	9	-63	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
	7a:11:dc:57:6d:b1	9	-62	NONE	11b/g/n
742-2.4gggggg	4c:62:24:f4:56:e4	11	-68	WPA1PSKWPA2PSK/TKIPAES	11b/g/n
comnect	b0:44:14:62:7b:4e	11	-57	WPA1PSKWPA2PSK/AES	11b/g/n
TP-LINK_2595	f8:8c:21:3f:25:6e	11	-51	WPA1PSKWPA2PSK/AES	11b/g/n
TP-LINK_2595	f8:8c:21:3f:25:95	11	-66	WPA1PSKWPA2PSK/AES	11b/g/n
	b0:44:14:62:7b:9b	11	-54	NONE	11b/g/n
comnect-guest	b0:44:14:62:7b:4f	11	-57	WPA1PSKWPA2PSK/AES	11b/g/n
comnect	b0:44:14:62:7b:99	11	-54	WPA1PSKWPA2PSK/AES	11b/g/n
	b0:44:14:62:7b:50	11	-57	NONE	11b/g/n
comnect-guest	b0:44:14:62:7b:9a	11	-55	WPA1PSKWPA2PSK/AES	11b/g/n
	fa:8c:21:2f:25:6e	11	-66	WPA1PSKWPA2PSK/AES	11b/g/n
ChinaNet-AP024	4c:6e:6e:02:22:02	13	-65	WPA2PSK/AES	11b/g/n
comnect	b0:44:14:62:7b:51	36	-22	WPA1PSKWPA2PSK/AES	11a/n/ac
RTL867x-ADSL	12:34:57:74:11:00	36	-84	NONE	11a/n/ac
comnect-guest	b0:44:14:62:7b:52	36	-59	WPA1PSKWPA2PSK/AES	11a/n/ac
WLAN_5G_E934	4c:6e:6e:e4:e9:38	36	-72	WPA1PSKWPA2PSK/TKIPAES	11a/n/ac
	b0:44:14:62:7b:53	36	-63	NONE	11a/n/ac

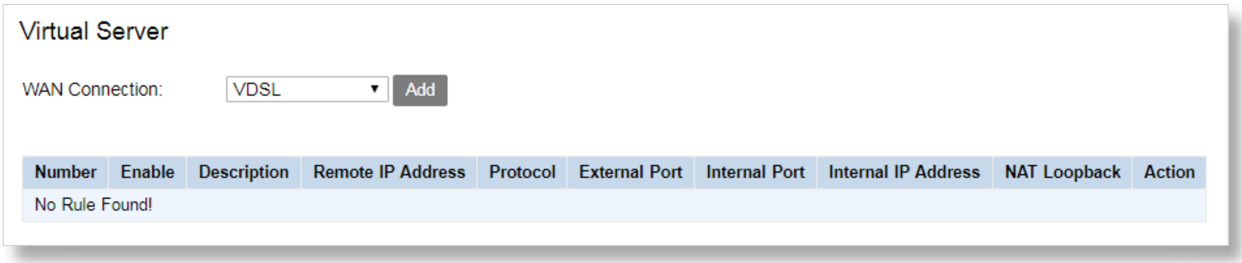
4.4 NAT

4.4.1 Virtual Server

If computer are connected to the modem router to form a LAN and access the internet through the modem router, internet users cannot access the hosts on the LAN. Therefore, the servers, such as web servers, email servers, and FTP servers, onthe LAN are inaccessible to internet users.

To enable internet users to access a LAN server, enable the virtual server function of the modem router, and map one service port of the virtual server to the IP address of the LAN server. This enables the modem router to forward the requests arriving at the port from the internet to the LAN server.

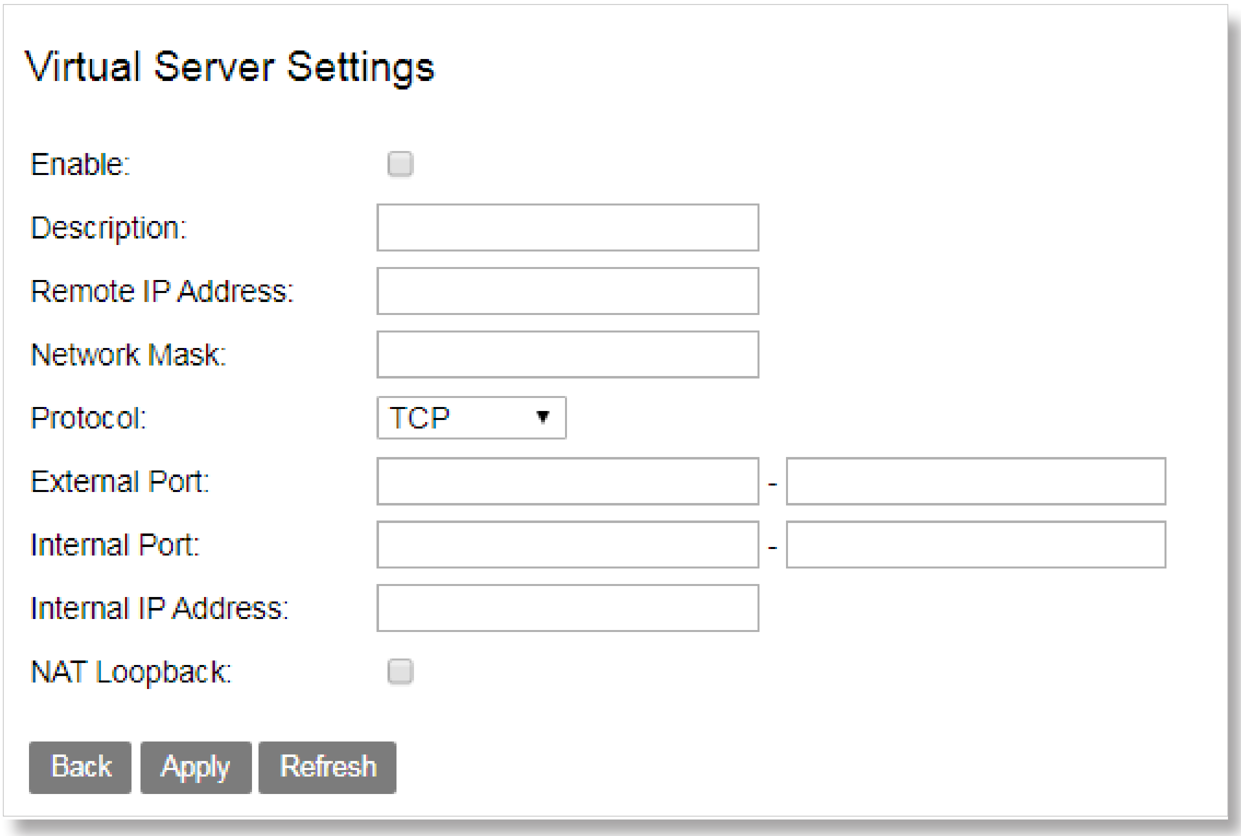
Choose **Advanced Setup > NAT > Virtual Server** to enter the configuration page.



Virtual Server

WAN Connection: VDSL ▼ Add

Number	Enable	Description	Remote IP Address	Protocol	External Port	Internal Port	Internal IP Address	NAT Loopback	Action
No Rule Found!									



Virtual Server Settings

Enable:	□
Description:	
Remote IP Address:	
Network Mask:	
Protocol:	TCP ▼
External Port:	-
Internal Port:	-
Internal IP Address:	
NAT Loopback:	□

Parameter	Description
Enable	It specifies whether to enable the Virtual Server Settings function.
Description	Allows you to customize a service
Remote IP Address	Enter the destination IP address.
Network Mask	Enter your network mask.
Protocol	Select a protocol from the Protocol drop-down list. If you are unsure, select **TCP/UDP**.
External Port	These are the start number and end number for the public ports at the internet interface.
Internal Port	These are the start number and end number for the public ports on the LAN of the modem router.
Internal IP Address	Enter the IP address of your local computer that provides the service.

To configure a virtual server

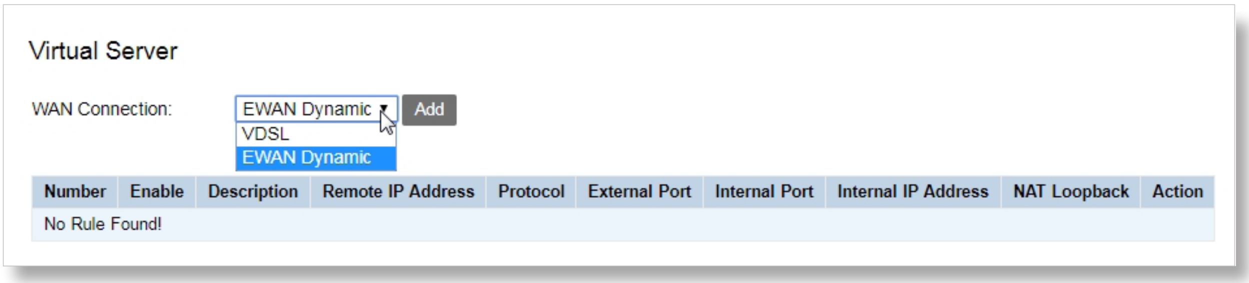
For example, you have to set up an FTP server on your LAN:

An FTP server(using the default port number of 21) at the IP address of 192.168.1.100

And want your friends to access the FTP server on default port over the internet. To access you FTP server from the internet, a remote user has to know the internet IP address or domain name of the modem router. In this example, assume that the WAN IP address of your router is 183.37.227.201.

To configure the router to make your local FTP server accessible over the internet:

Step 1 Go to **Advanced Setup > NAT > Virtual Server** page, and select a WAN Connection from the drop-down box, then click **Add**.



Virtual Server

WAN Connection: EWAN Dynamic

Number	Enable	Description	Remote IP Address	Protocol	External Port	Internal Port	Internal IP Address	NAT Loopback	Action
No Rule Found!									

Step 2 Check the **Enable** box.

Step 3 Customize a name for service in **Description** field.

Step 4 Select a protocol from the **Protocol** drop-down list. If you are unsure about which protocol is required, select **TCP/UDP**.

Step 5 Manually set the port number (21) used by this service in the External Port (Start to End), Internal Port (Start to End).

Step 6 In the **Internal IP Address** field, enter the IP address of your local computer that offers this service, which is 192.168.1.100 in this example.

Step 7 Click the **Apply/Save**.

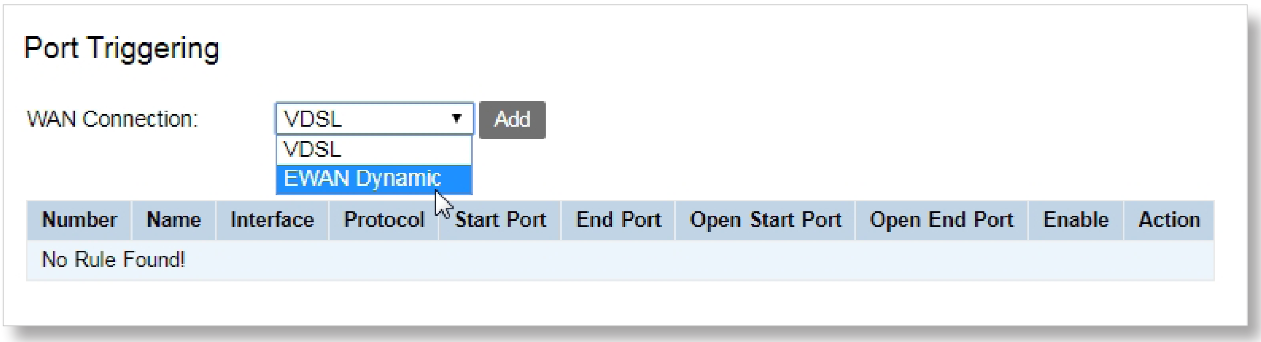
Note: As the WAN ip address changes dynamically, to ensure the stability of this function, it is recommended to use this function together with DDNS function to allow internet users to access the service through domain names.

4.4.2 Port Triggering

Some applications, such as games, video conferencing, and remote access, require that specific ports in the router's firewall be opened for access by the applications. Port triggering opens an incoming port when the user's computer is using a specified outgoing port for specific traffic. This allows computers behind a NAT-enabled router on a local network to provide services. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or range of ports.

Choose **Advanced Setup > NAT > Port triggering** to enter the configuration page.

Select a WAN Connection from the drop-down box, then click **Add** to configure the function.

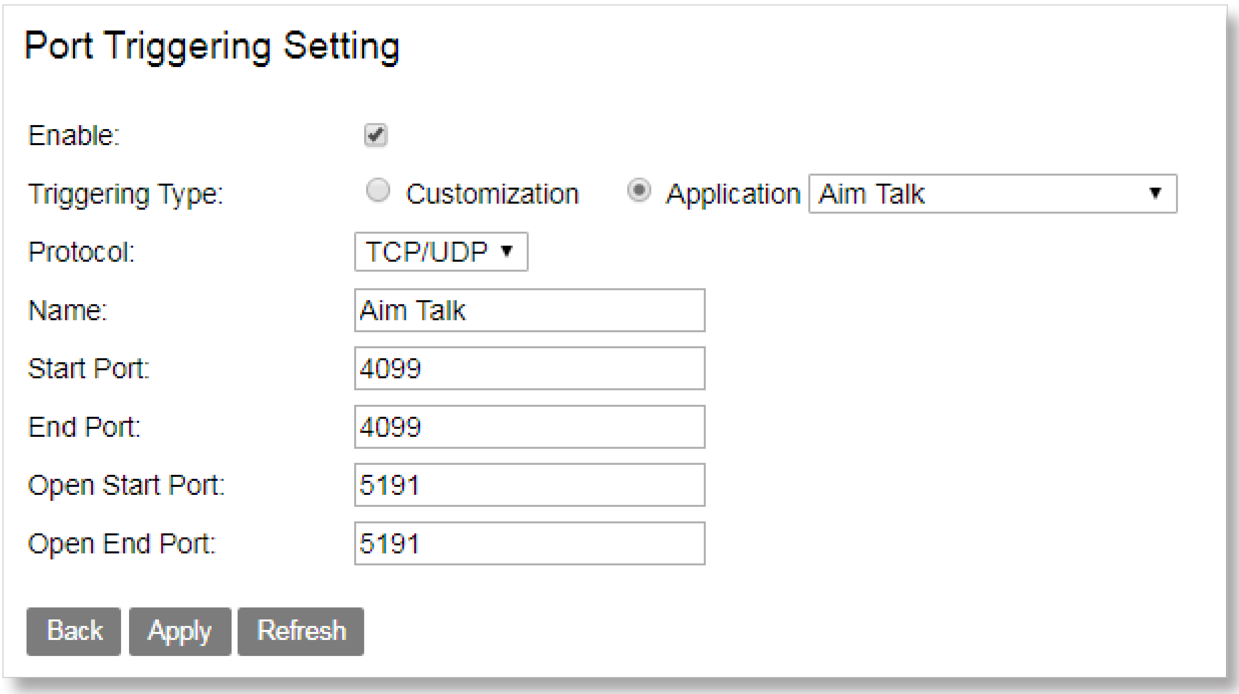


Port Triggering

WAN Connection: VDSL ▾ Add

Number	Name	Interface	Protocol	Start Port	End Port	Open Start Port	Open End Port	Enable	Action
No Rule Found!									

Parameter	Description
Enable	It specifies whether to enable the Port Triggering Settings function.
Triggering Type	**Customization:** Allows you to customize a service. **Application:** Allows you to select an existing service from the drop-down list.
Protocol	Select a protocol from the Protocol drop-down list. If you are unsure, select **TCP/UDP**.
Start/End Port	The port range for an application to initiate connections.
Open Start Port / Open End Port	These are the starting number and ending number for the ports that are automatically opened by the built-in firewall when connections initiated by an application are establishhed.



Port Triggering Setting

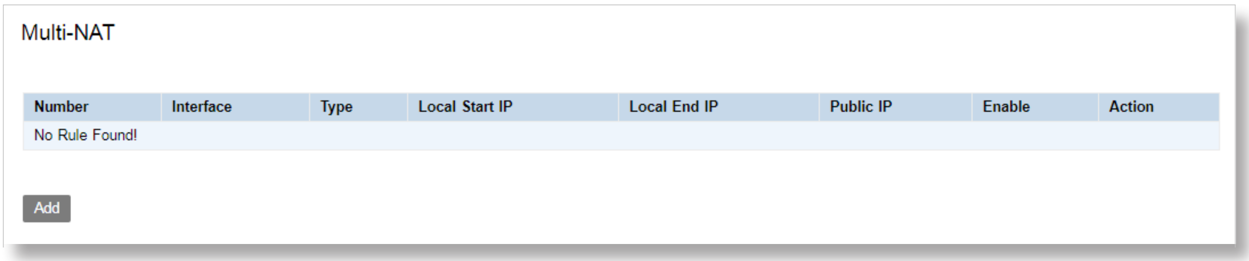
Enable:	☑
Triggering Type:	○ Customization ● Application Aim Talk ▼
Protocol:	TCP/UDP ▼
Name:	Aim Talk
Start Port:	4099
End Port:	4099
Open Start Port:	5191
Open End Port:	5191

4.4.3 Multi-NAT

Multi-NAT is a network function whereby one network address is rewritten (translated) to another address: Network Address Translation is frequently used to allow multiple network nodes (computers or inter-networked devices) to share a single public (or local network) IP address.

Multi-NAT can work in one-toone or many-to-one mode.

Choose **Advanced Setup > NAT > Multi-NAT** to enter the configuration page.

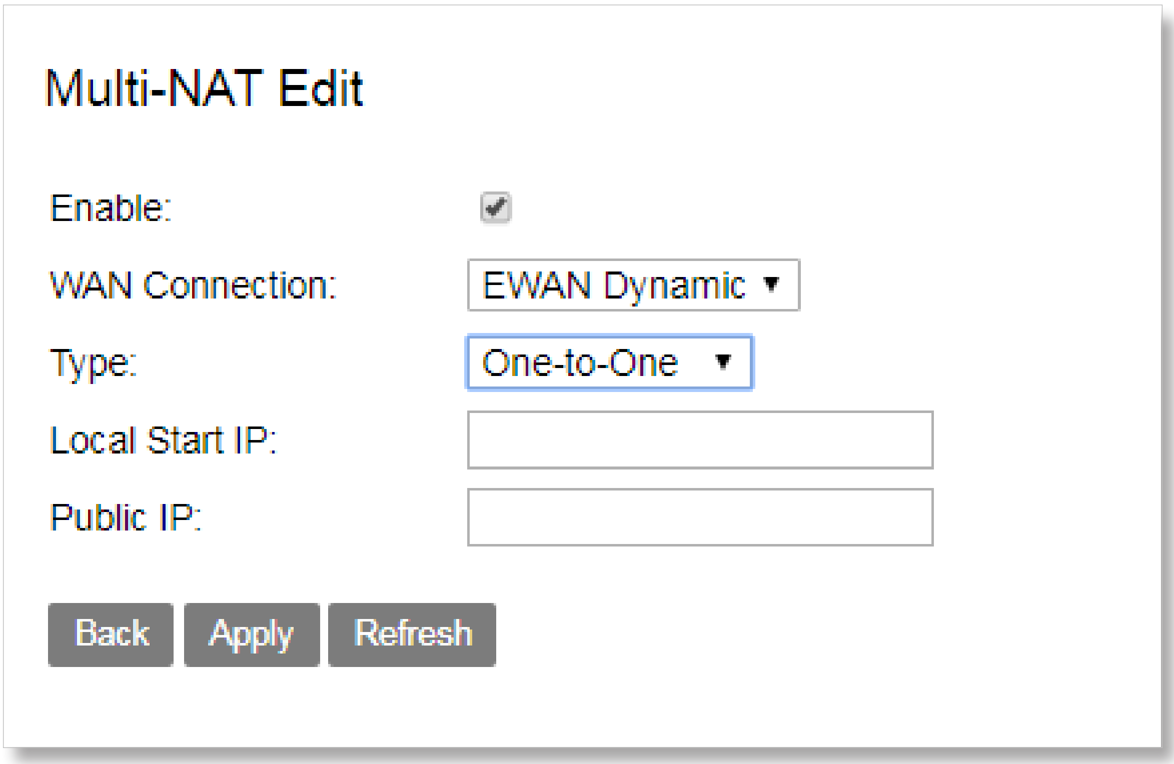


Multi-NAT

Number	Interface	Type	Local Start IP	Local End IP	Public IP	Enable	Action
No Rule Found!							

Click **Add** to configure the function.

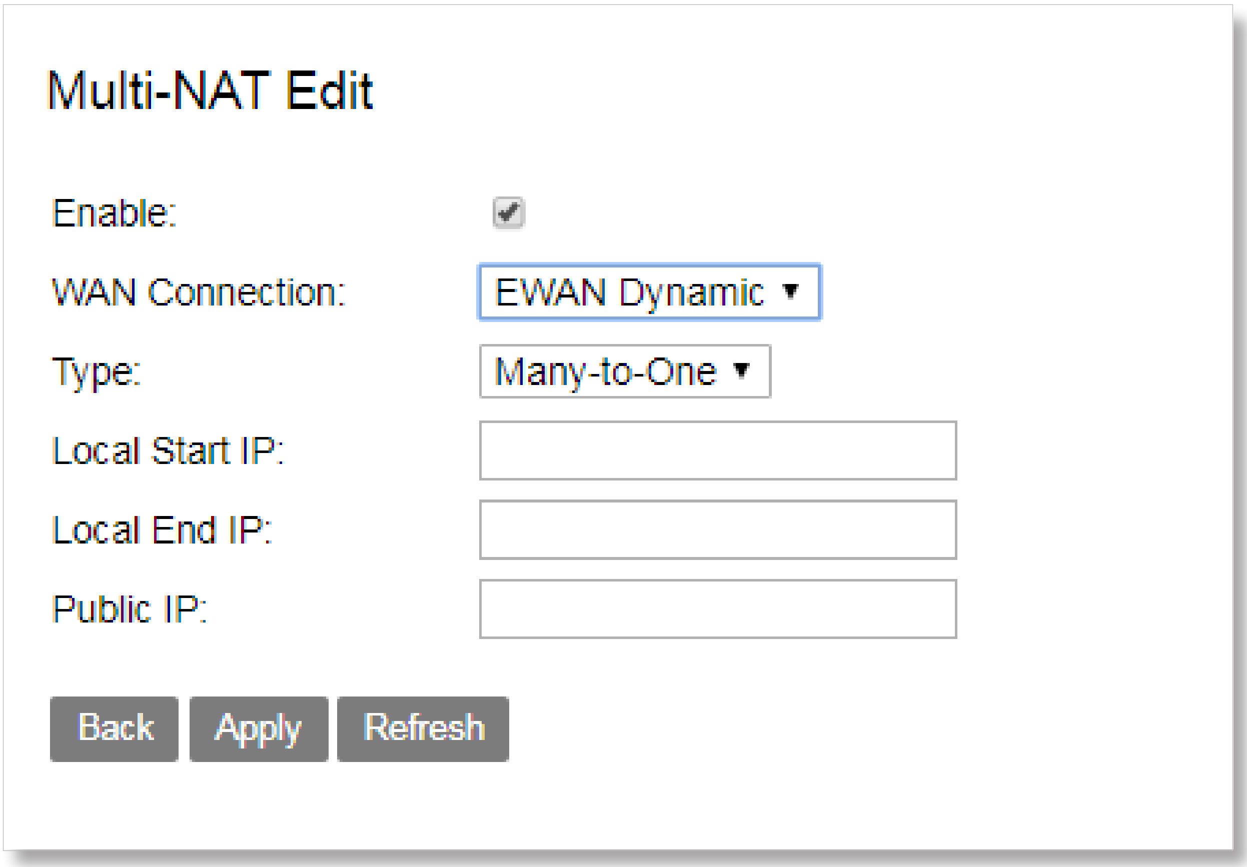
One-to-One



Multi-NAT Edit

Enable:	☑
WAN Connection:	EWAN Dynamic ▼
Type:	One-to-One ▼
Local Start IP:	
Public IP:	

Many-to-One



Multi-NAT Edit

Enable:	☑
WAN Connection:	EWAN Dynamic ▼
Type:	Many-to-One ▼
Local Start IP:	
Local End IP:	
Public IP:	

Parameter	Description
Enable	It specifies whether to enable the Multi-NAT function.
WAN Connection	Allows you to select a WAN Connection from the drop-down box, then click **Add**.
Type	**One-to-One:** Set a route from a local IP address to a public IP address. **Many-to-One:** Set a route from many local IP address to a public IP address.
Local IP	It specifies a local IP address.
Public IP	It specifies a public IP address.

To Configure the Multi-NAT function

Step 1 Go to **Advanced Setup > NAT > Multi-NAT** page, and click **Add**.

Step 2 Select a WAN Connection from the drop-down list.

Step 3 Select a type. If you only need to set a route for a local IP address, select **One-to-One**; If you need to set multiple routes for a local network, select **Many-to-One**.

Step 4 If you select **One-to-One**, specfy a local IP address. If you select **Many-to-One**, specfy the **Local Start IP** and **Local End IP**.

Step 5 Set **Public IP** to a public IP address.

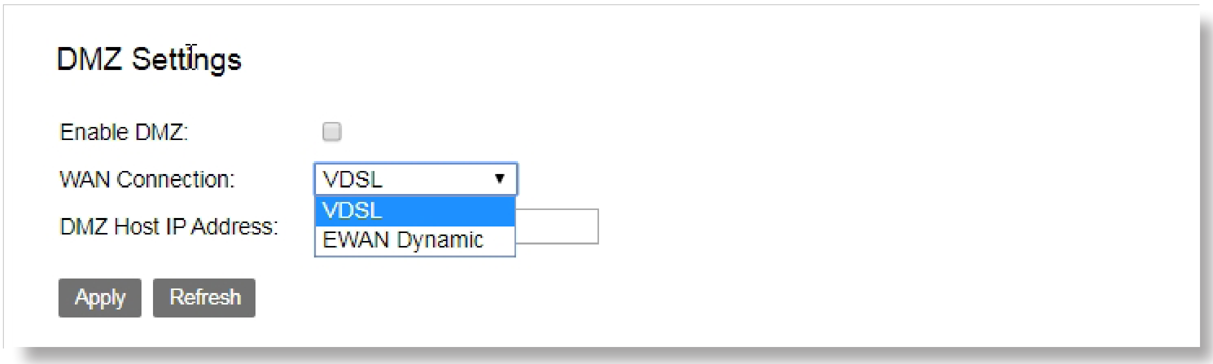
Step 6 Click **Apply**.

Note: *The local IP and Public IP you set should be static IP address.*

4.4.4 DMZ Host

The default DMZ (De-Militarized Zone) host feature is helpful when you are using some online games and video conferencing applications that are not compatible with NAT (Network Address Translation).

Choose **Advanced Setup > NAT > DMZ Host** to enter the configuration page.



DMZ Settings

Enable DMZ: □

WAN Connection: VDSL ▾

DMZ Host IP Address:

Parameter	Description
Enable DMZ	It specifies whether to enable the DMZ function when check the box.
WAN Connection	Allows you to select a WAN Connection from the drop-down box, then click **Add**.
DMZ Host IP Address	DMZ Host IP Address: The IP Address of the device for which the firewall of the modem router is disabled. Ensure that the IP address is a static IP address. The DMZ host should be connected to a LAN port of the modem router.

Note:

1. A DMZ host is not protected by the firewall of the router. A hacker may leverage the DMZ host to attack your LAN. Therefore, enable the DMZ function only when necessary.

2. Manually set the IP address of the LAN computer that functions as a DMZ host, to prevent IP address changes, which lead to DMZ function failures.

3. Security software, antivirus software, and the built-in OS firewall of the computer may cause DMZ function failures. Disable them when using the DMZ function. If the DMZ function is not required, it is recommended that you disable it and enable your firewall, security, and antivirus software.

To Configure the DMZ Host function

Step 1 Go to **Advanced Setup > NAT > DMZ Host** page.

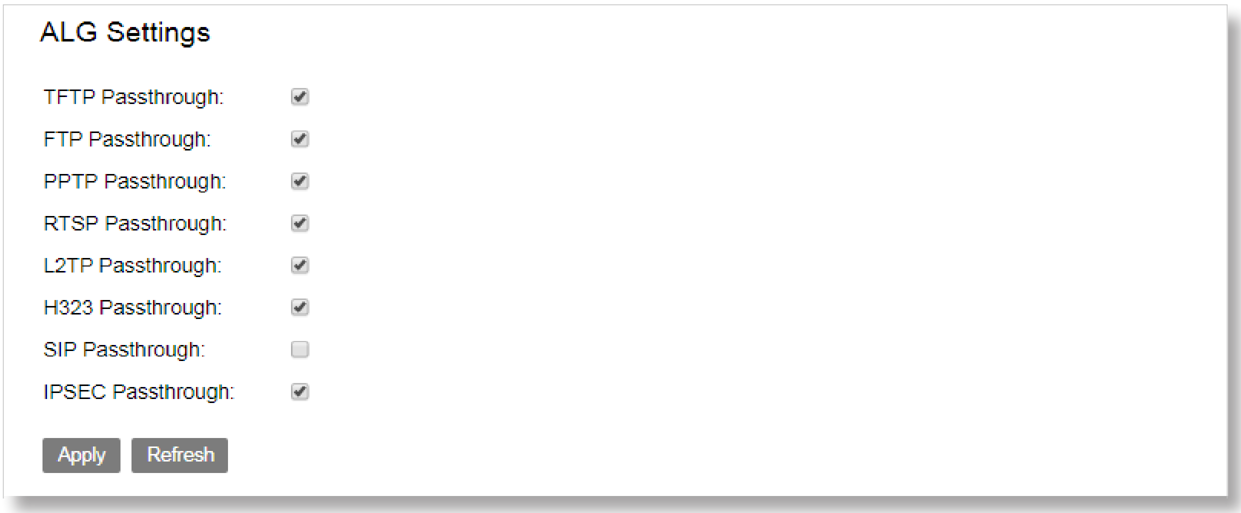
Step 2 Check the **Enable DMZ** box, then select a WAN Connection from the drop-down list.

Step 3 Set DMZ Host IP Address to the IP address of the DMZ host.

Step 4 Click **Apply**.

4.4.5 ALG

ALG allows you to enable SIP, FTP, TFTP, H323, RTSP functions, and VPN pass through as required.



ALG Settings

TFTP Passthrough: ☑

FTP Passthrough: ☑

PPTP Passthrough: ☑

RTSP Passthrough: ☑

L2TP Passthrough: ☑

H323 Passthrough: ☑

SIP Passthrough: □

IPSEC Passthrough: ☑

Parameter	Description
TFTP	The users on LAN can share resources on the TFTP server on WAN only when it is selected.
FTP	The users on LAN can share resources on the FTP server on WAN only when it is selected.
PPTP	If you select PPTP protocol when you create a VPN connection on your computer, it takes effect only when this checkbox is selected.
RTSP	The user on LAN can view video on demand when it is selected.
L2TP/IPSEC	If you select L2TP or IPSEC protocol when you create a VPN connection on your computer, it takes effect only when this checkbox is selected.
H323	The IP phone and network conference function can be used on the computers connected to the modem router only when it is selected.
SIP	The IP phone function can be used on the computers conneted to the modem router when it is selected.

4.5 Security

4.5.1 IP Filtering

This function can forbid the LAN devices to access the internet or allow WAN devices to visit the LAN devices.

LAN to WAN

By default, all outgoing traffic from LAN is allowed, but some IP traffic can be blocked or allowed by setting up filtering rules for whitelist or blacklist. Outgoing IP filtering function allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition.

To configure the outgoing IP filtering function

Step 1 Go to **Advanced Setup > Security > IP Filtering** page.

Step 2 Check the **Firewall Enable** box, and select Whitelist or Blacklist, then click **Add** at the LAN WAN field.

Step 3 Select your IP protocol which can be IPv4 or IPv6 and your WAN connection.

Step 4 **Description:** Customize a descriptive filtering name.

Step 5 Check the **Enable** box.

Step 6 Select a protocol for the filter rule.

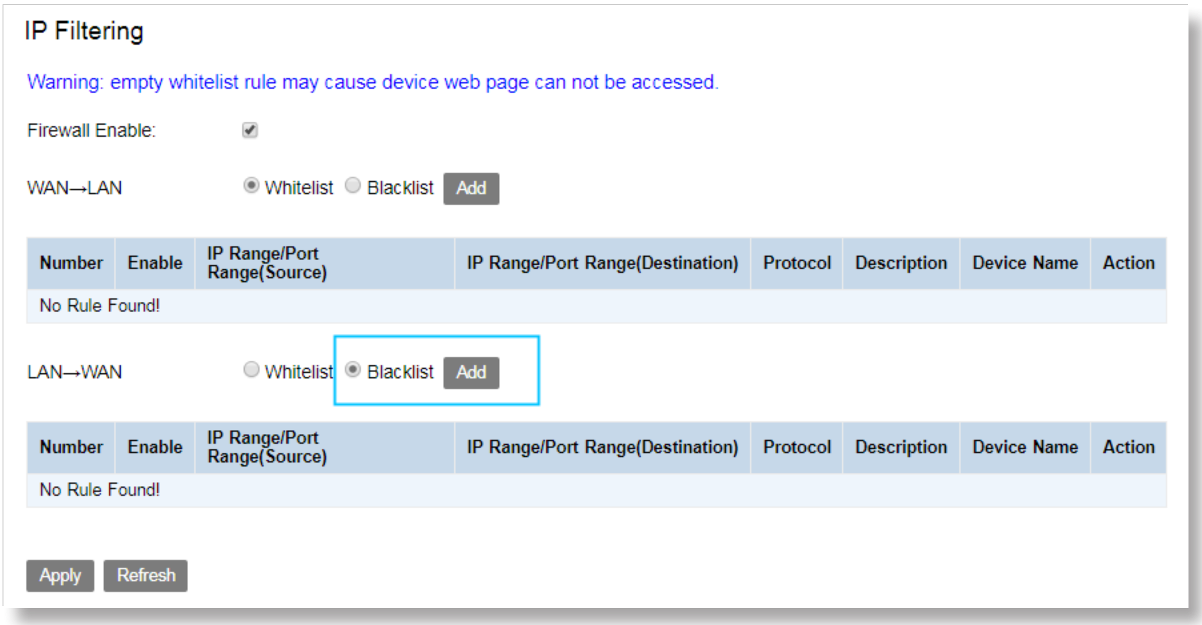
Step 7 **Source IP:** Enter the LAN IP address to be filtered.

Step 8 **Source Port:** Enter a port number or a port range used by LAN computers to access the internet. If you are not sure, leave it blank.

Step 9 **Destination IP:** Enter the external network IP address to be accessed by specified LAN computers.

Step 10 Destination Port: Enter a port number or a port range that the internet service you restrict uses.

Step 11 Click **Apply**.



IP Filtering

Warning: empty whitelist rule may cause device web page can not be accessed.

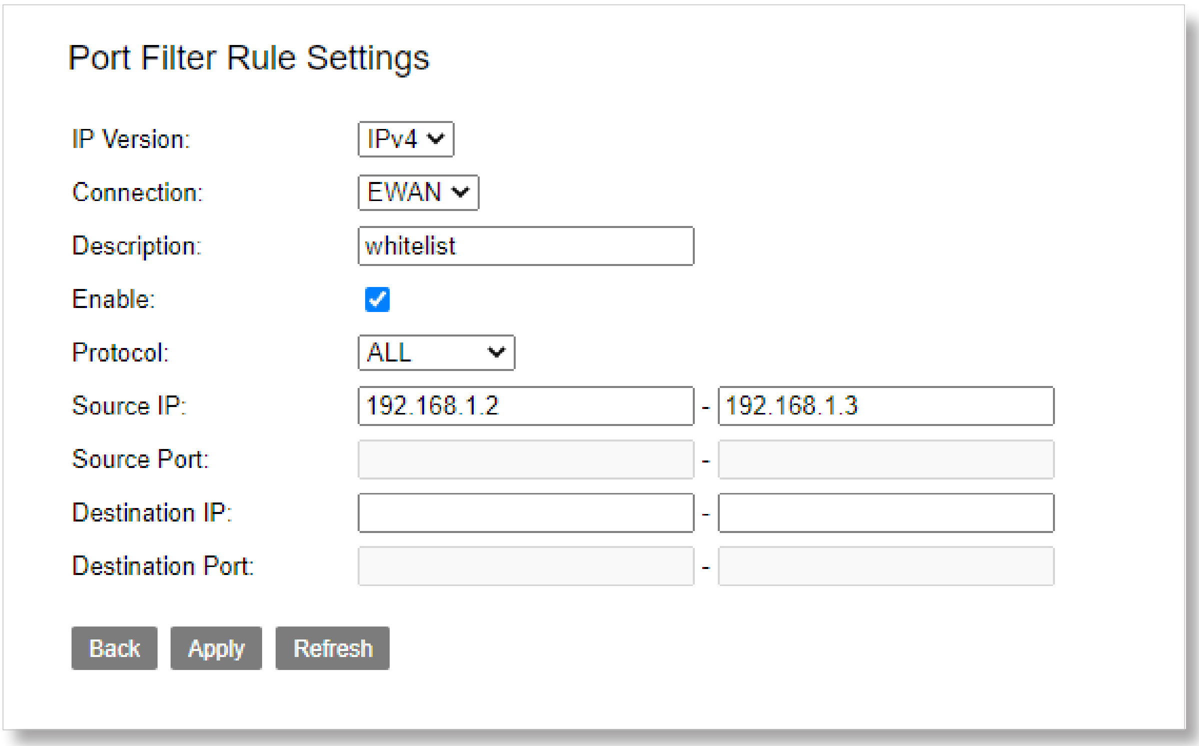
Firewall Enable: ☑

WAN→LAN ● Whitelist ○ Blacklist Add

Number	Enable	IP Range/Port Range(Source)	IP Range/Port Range(Destination)	Protocol	Description	Device Name	Action
No Rule Found!							

LAN→WAN ○ Whitelist ● Blacklist Add

Number	Enable	IP Range/Port Range(Source)	IP Range/Port Range(Destination)	Protocol	Description	Device Name	Action
No Rule Found!							



Port Filter Rule Settings

IP Version:	IPv4	
Connection:	EWAN	
Description:	whitelist	
Enable:	☑	
Protocol:	ALL	
Source IP:	192.168.1.2	192.168.1.3
Source Port:		
Destination IP:		
Destination Port:		

WAN to LAN

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be accepted by setting up filtering rules. The Incoming IP Filtering function allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition.

To configure the ingoing IP filtering function

Step 1 Go to **Advanced Setup > Security > IP Filtering** page.

Step 2 Check the **Firewall Enable** box, and select Whitelist or Blacklist, then click **Add** at the WAN to LAN field.

Step 3 Select your IP protocol which can be IPv4 or IPv6 and your WAN connection.

Step 4 **Description:** Customize a descriptive filtering name.

Step 5 Check the **Enable** box.

Step 6 Select a protocol for the filter rule.

Step 7 **Source IP:** Enter the internal IP address to be filtered.

Step 8 **Source Port:** Enter a port number or a port range used by computers from external network to access your internal network.

Step 9 **Destination IP:** Enter the internal network IP address to be accessed by specified computers from external network..

Step 10 **Destination Port:** Enter the port used by the internet service to be restricted.

Step 11 Click **Apply**.

4.5.2 MAC Filtering

There are two policies of the function:

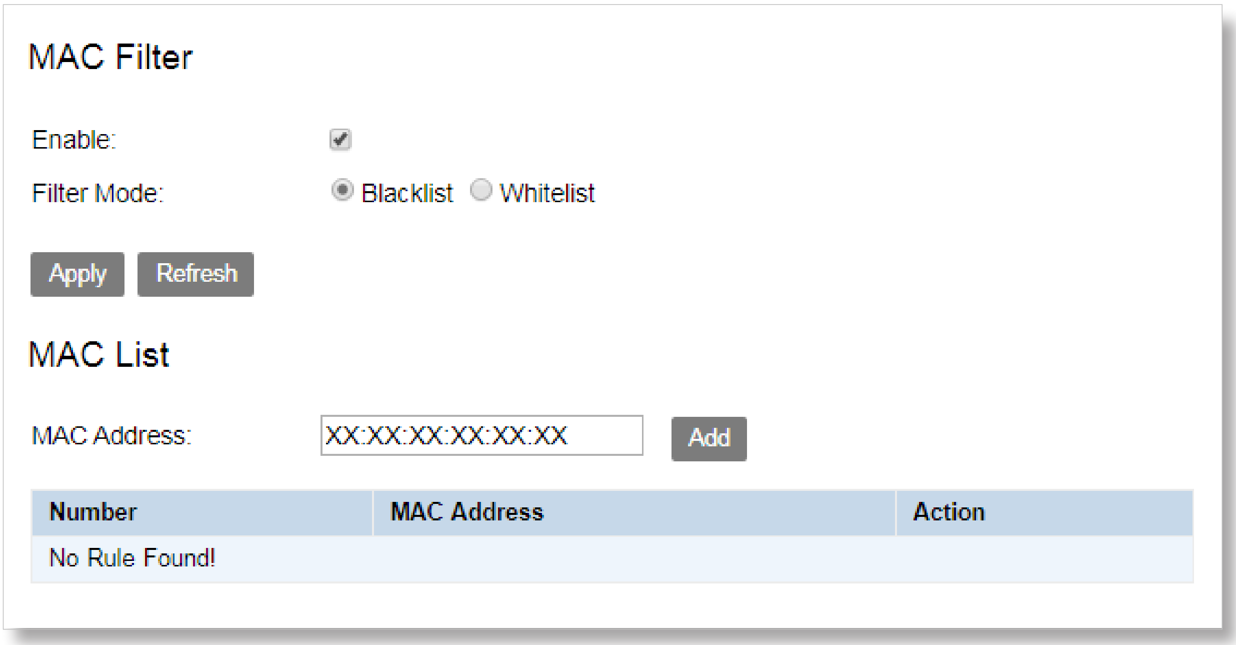
Whitelist indicates that all MAC address those matching the rules you specify will be allowed to access the internet.

To add a frame Whitelist or Blacklist rule

Step 1 Go to **Advanced Setup > Security > MAC Filtering** page.

Step 2 Check the **Enable** box, select a Filter Mode which can be Blacklist or Whitelist.

Step 3 Enter the MAC Address to which you want to apply the MAC filtering rule, and then click **Add** and **Apply**.



MAC Filter

Enable: ☑

Filter Mode: ● Blacklist ○ Whitelist

MAC List

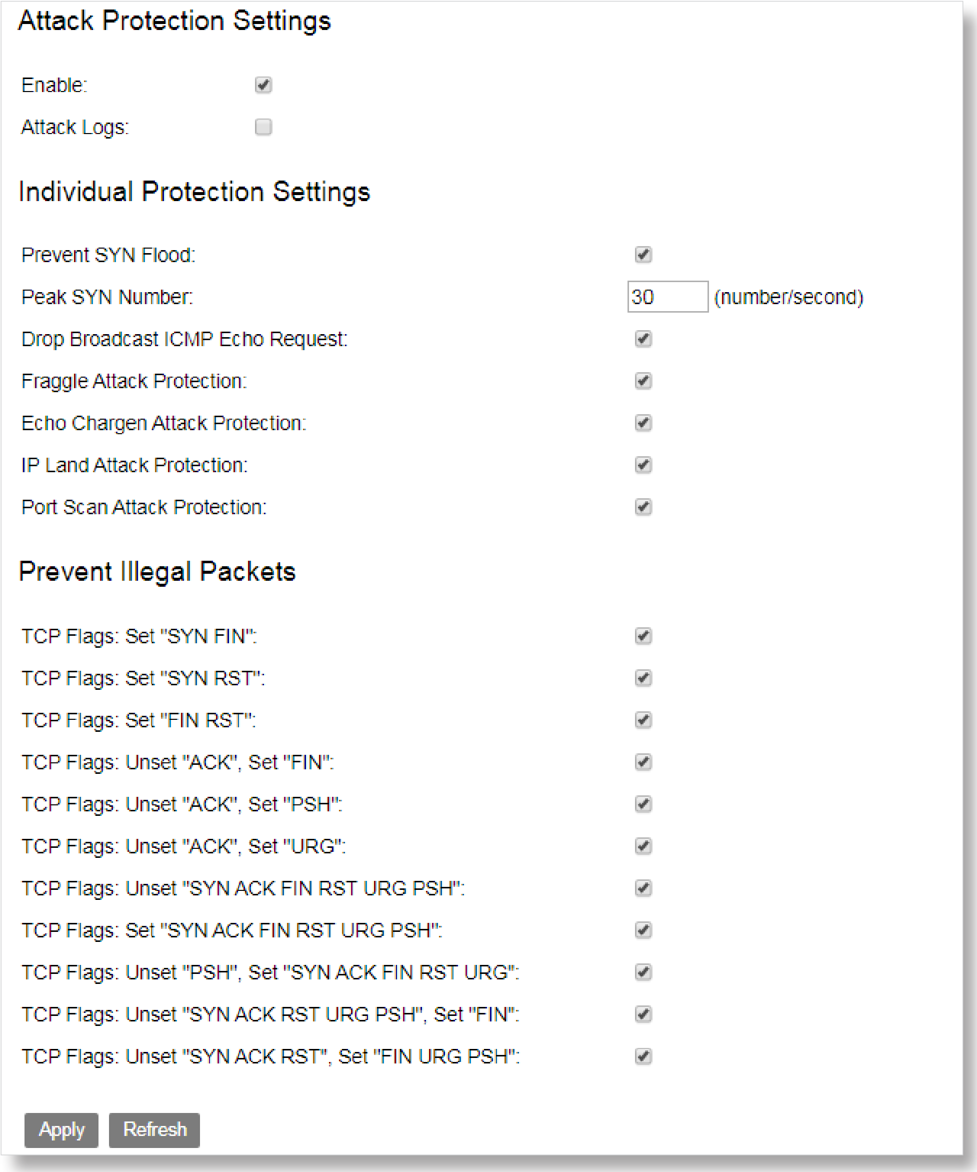
MAC Address: XX:XX:XX:XX:XX:XX

Number	MAC Address	Action
No Rule Found!		

4.5.3 DoS Protection

This function is used to protect the modem router against some attacks, helping ensure network security. By default, the DoS Protection is enabled. It is recommended that you retain the default settings.

Go to **Advanced Setup > Security > DoS Protection** page.



Attack Protection Settings

Enable:	☑
Attack Logs:	□

Individual Protection Settings

Prevent SYN Flood:	☑
Peak SYN Number:	30 (number/second)
Drop Broadcast ICMP Echo Request:	☑
Fraggle Attack Protection:	☑
Echo Chargen Attack Protection:	☑
IP Land Attack Protection:	☑
Port Scan Attack Protection:	☑

Prevent Illegal Packets

TCP Flags: Set "SYN FIN":	☑
TCP Flags: Set "SYN RST":	☑
TCP Flags: Set "FIN RST":	☑
TCP Flags: Unset "ACK", Set "FIN":	☑
TCP Flags: Unset "ACK", Set "PSH":	☑
TCP Flags: Unset "ACK", Set "URG":	☑
TCP Flags: Unset "SYN ACK FIN RST URG PSH":	☑
TCP Flags: Set "SYN ACK FIN RST URG PSH":	☑
TCP Flags: Unset "PSH", Set "SYN ACK FIN RST URG":	☑
TCP Flags: Unset "SYN ACK RST URG PSH", Set "FIN":	☑
TCP Flags: Unset "SYN ACK RST", Set "FIN URG PSH":	☑

4.6 Parental Control

This function enables you to control internet connectivity availability and content accessibility for devices connected to the router.

4.6.1 MAC Control

This page adds time of day restriction by MAC, to a special LAN device connected to the Router. Only LAN host with the input MAC will be controlled, and takes no effects to the other MAC.

Adding a time restriction rule for blocking

Step 1 Go to **Advanced Setup > Parental Control > MAC Control** page.

Step 2 Check the **Enable Time Restriction** box and click **Add**.

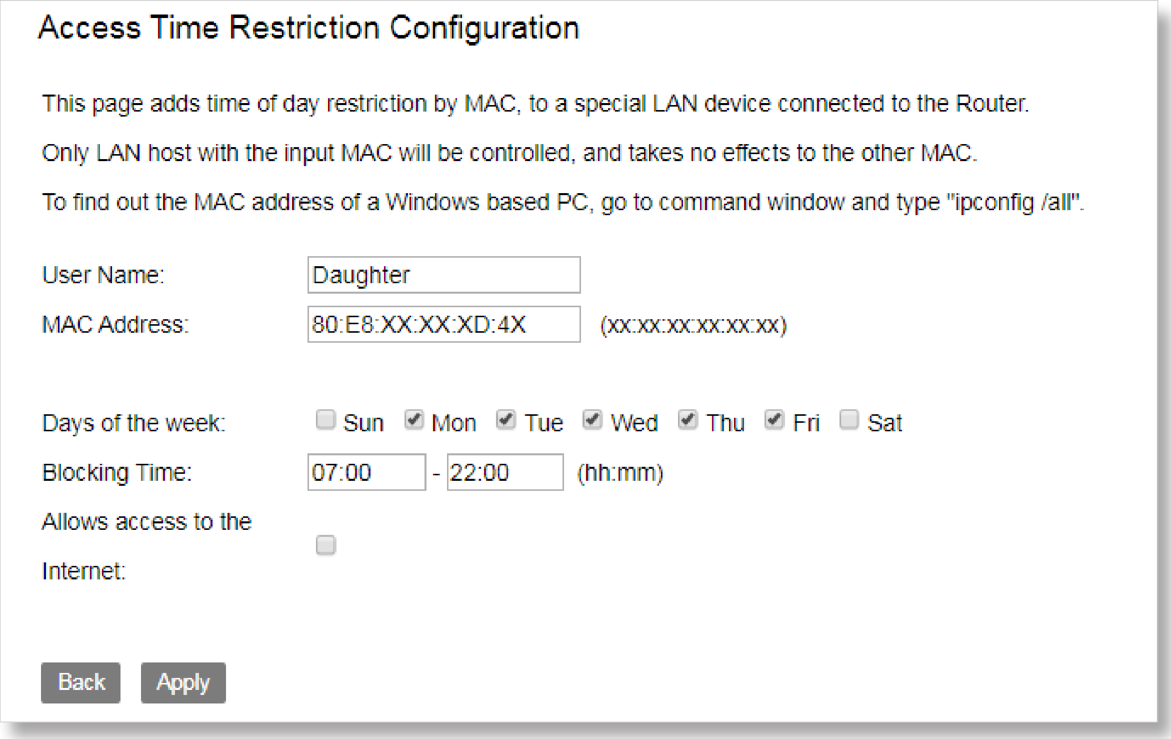
Step 3 **User Name:** Enter a user name for this rule.

Step 4 **MAC Address:** Enter the MAC address of a computer to which the rule is applied.

Step 5 **Days of the week:** Select the days of week during which the rule takes effect.

Step 6 **Blocking Time (hh:mm):** Enter the time period of day restriction for the rule. Within this specified period of the day, this LAN device cannot access the internet. For example, if you set Blocking Time as 07:00 to 22:00, the device to which this rule is applied cannot access the internet during 07:00~22:00.

Step 7 Click **Apply**.



Access Time Restriction Configuration

This page adds time of day restriction by MAC, to a special LAN device connected to the Router.

Only LAN host with the input MAC will be controlled, and takes no effects to the other MAC.

To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name: Daughter

MAC Address: 80:E8:XX:XX:XD:4X (xx:xx:xx:xx:xx:xx)

Days of the week: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Blocking Time: 07:00 - 22:00 (hh:mm)

Allows access to the Internet: □

Adding a time restriction rule for accessing the internet

Step 1 Go to **Advanced Setup > Parental Control > MAC Control** page.

Step 2 Check the **Enable Time Restriction** box and click **Add**.

Step 3 **User Name:** Enter a user name for this rule.

Step 4 **MAC Address:** Enter the MAC address of a computer to which the rule is applied.

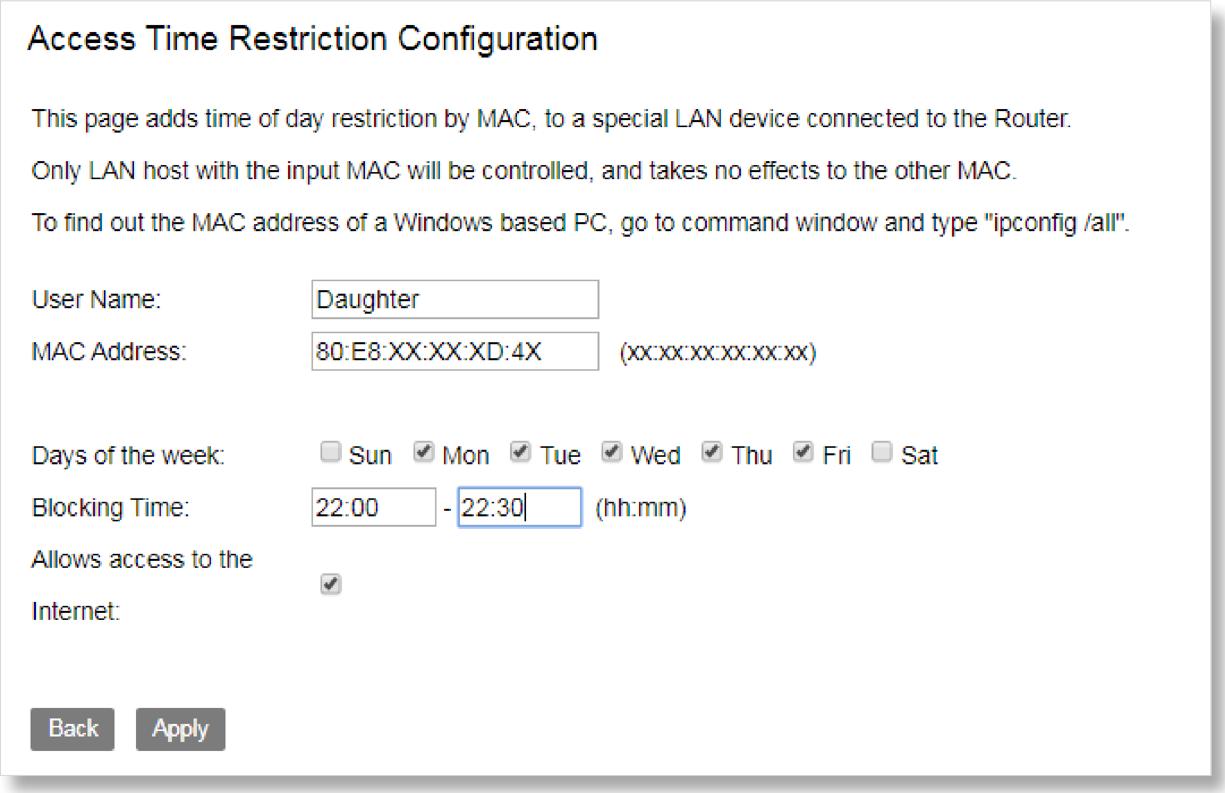
Step 5 **Days of the week:** Select the days of week during which the rule takes effect.

Step 6 **Blocking Time (hh:mm):** Enter the time period of day restriction for the rule. Within this specified period of the day, this LAN device can access the internet.

Step 7 Check the **Allows access to the internet** box.

Step 8 Click **Apply**.

For example as follow, if you set Time as 22:00 to 22:30, the device to which this rule is applied can access the internet during 22:00~22:30 On Monday, Tuesday, Wednesday, Thursday and Friday.



Access Time Restriction Configuration

This page adds time of day restriction by MAC, to a special LAN device connected to the Router.

Only LAN host with the input MAC will be controlled, and takes no effects to the other MAC.

To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name: Daughter

MAC Address: 80:E8:XX:XX:XD:4X (xx:xx:xx:xx:xx:xx)

Days of the week: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Blocking Time: 22:00 - 22:30 (hh:mm)

Allows access to the Internet: ☑

4.6.2 Url & IP Control

This page adds time of day restriction to access some URL for a special LAN device connected to the Router. There are two policies:

Blacklist: can not access the specify URL.

Whitelist: can access the specify URL.

Adding a time restriction rule for accessing the specify URL

Step 1 Go to **Advanced Setup > Parental Control > Url & IP Control** page.

Step 2 Check the **Enable, select Blacklist or Whitelist**, click **Add**.

Step 3 **Description:** Customize a descriptive filtering name.

Step 4 **LAN PC IP:** Enter the IP address of a computer to which the rule is applied.

Step 5 **URL Key:** Enter the URL Key which you want to restrict.

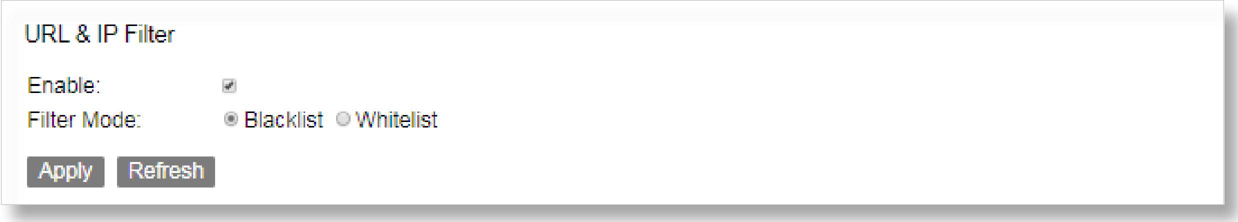
Step 5 **Days of the week:** Select the days of week during which the rule takes effect.

Step 6 **Blocking Time (hh:mm):** Enter the time period of day restriction for the rule.

Step 8 Click **Apply**.

Step 9 Click **Back** then click **Apply**.

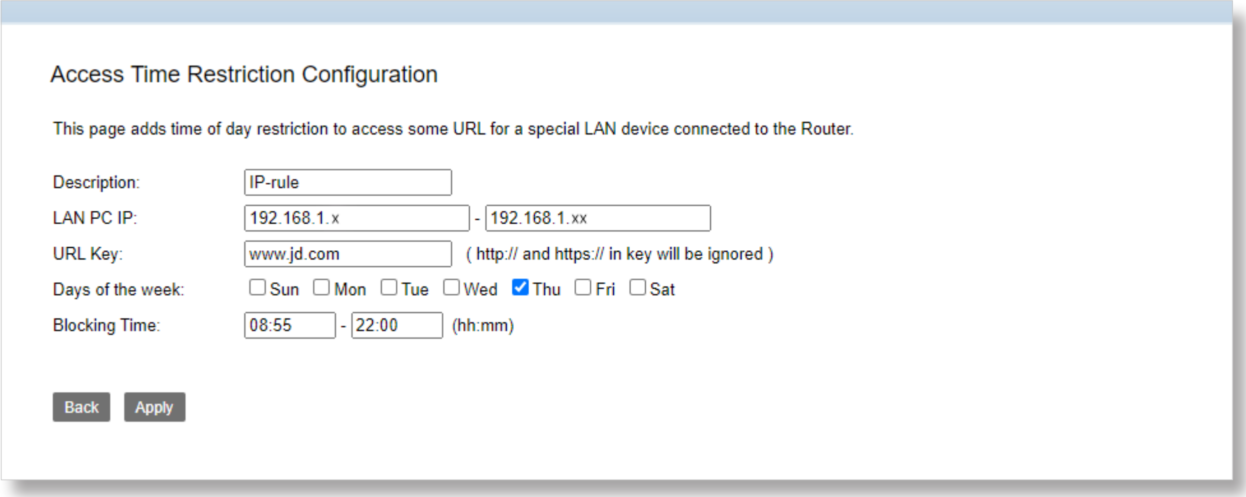
For example as follow, If you select Blacklist and set the Blocking Time as 22:00 to 22:30, the device to which this rule is applied can not access https://www.jd.com/ during 08:55~22:00 On Thursday.



URL & IP Filter

Enable: ☑

Filter Mode: ● Blacklist ○ Whitelist



Access Time Restriction Configuration

This page adds time of day restriction to access some URL for a special LAN device connected to the Router.

Description: IP-rule

LAN PC IP: 192.168.1.x - 192.168.1.xx

URL Key: www.jd.com (http:// and https:// in key will be ignored)

Days of the week: □ Sun □ Mon □ Tue □ Wed ☑ Thu □ Fri □ Sat

Blocking Time: 08:55 - 22:00 (hh:mm)

4.7 Routing

The Routing part includes static route and dynamic route.

4.7.1 Static Route

Static Route is used to select the best route for delivering data from a source address to a destination address. A static route is a manually configured route, which is simple, efficient, and reliable. Appropriate static routes help reduce the number of route selection problems and reduce route selection load, increasing the packet forwarding speed.

Adding a static route

Step 1 Go to **Advanced Setup > Routing > Static Route** page.

Step 2 Click **Add**.

Step 3 Select your connection mode and check the **Enable** box.

Step 4 **Destination Subnet:** Set an IP address of a specified host or a specified network.

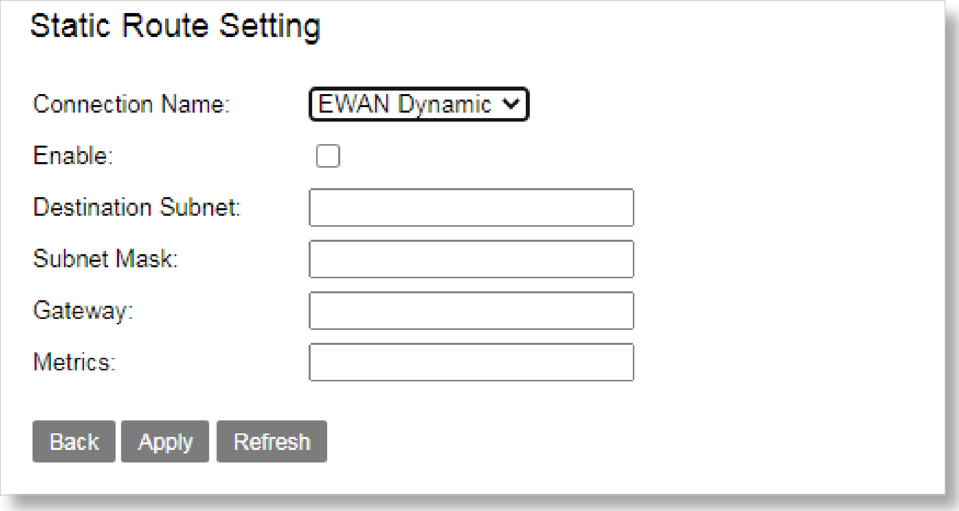
For example, if you want to set the Destination IP address/prefix length to a specified host, assume that the IP address of the host is 1.2.3.4, you can set it to 1.2.3.4/32. If you want to set the Destination IP address/prefix length to all hosts in a specified network, assume that the network is 2.2.3.3/255.255.0.0, you can set it to 2.2.0.0/16 which represents all hosts whose IP address start with 2.2.

Step 5 **Subnet Mask:** Enter your subnet mask.

Step 6 **Gateway:** set the gateway IP address to the IP address of the next-hop router.

Step 7 **Metrics:** Set a metric value for the static route. A smaller number indicates a higher priority.

Step 8 Click **Apply**.



Static Route Setting

Connection Name: EWAN Dynamic

Enable: □

Destination Subnet:

Subnet Mask:

Gateway:

Metrics:

4.7.2 Dynamic Route

Dynamic routing means that the router can automatically establish its own routing table and adjust it according to the change of the actual situation.

Adding a dynamic route

Step 1 Go to **Advanced Setup > Routing > Dynamic Route** page.

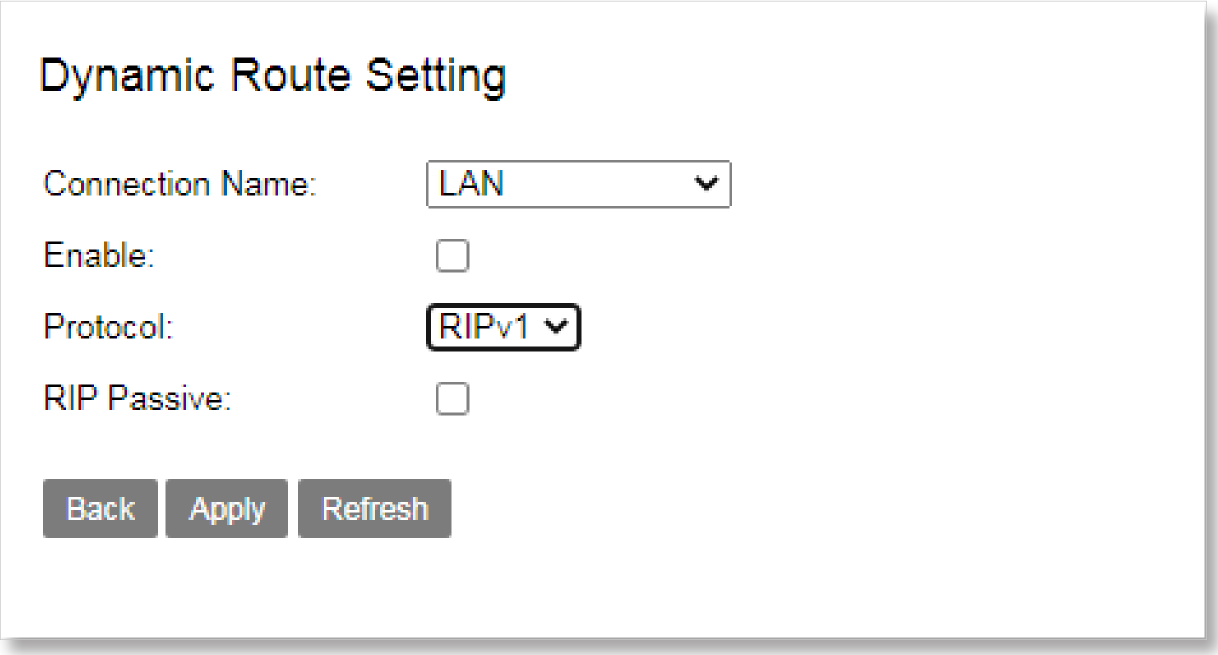
Step 2 Click **Add**.

Step 3 Select your connection mode and check the **Enable** box.

Step 4 Select the protocol.

Step 5 Check the RIP Passive box.

Step 6 Click **Apply**.



Dynamic Route Setting

Connection Name: LAN

Enable: □

Protocol: RIPv1

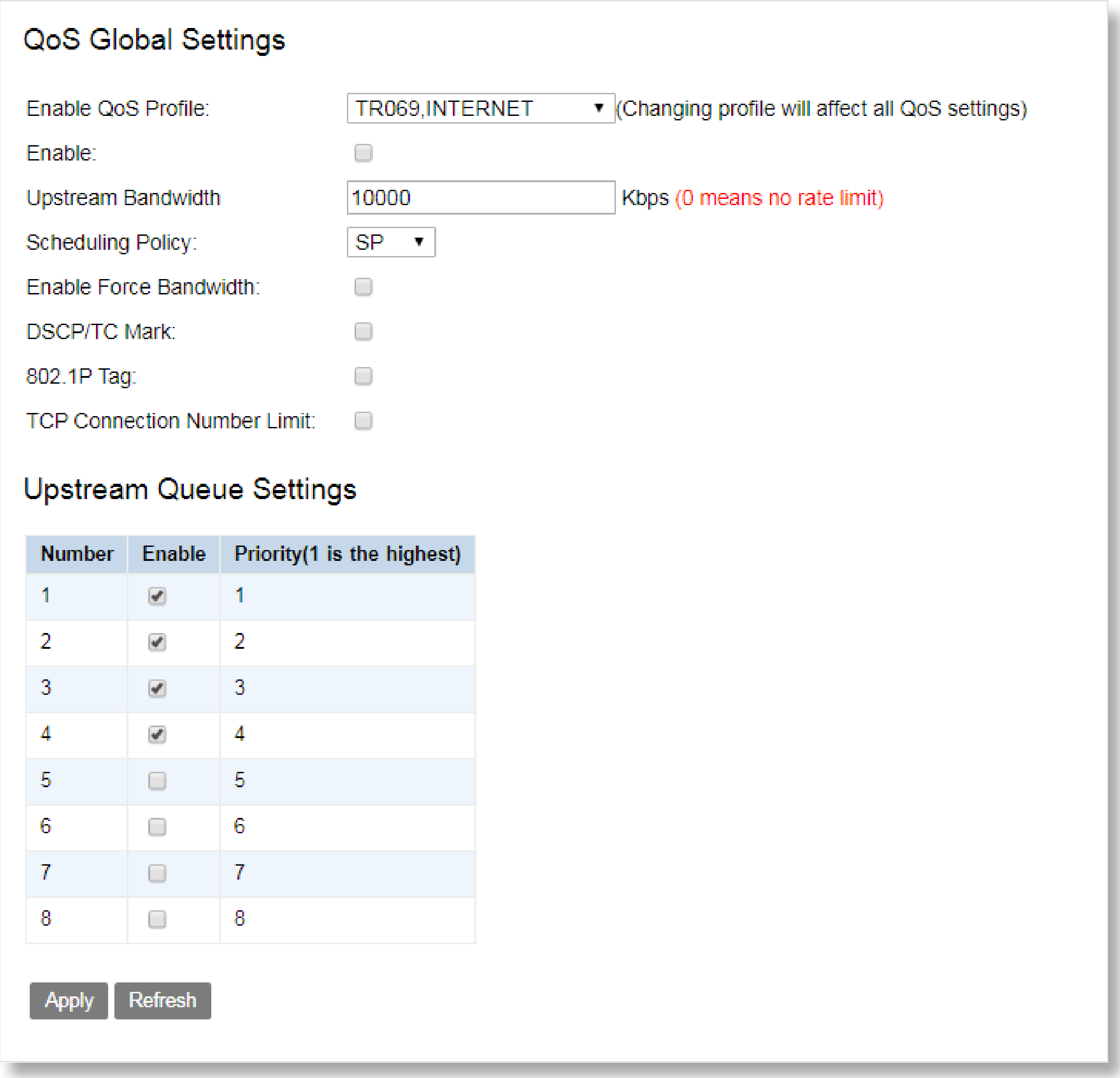
RIP Passive: □

4.8 Quality of Service

QoS makes priority for better performance when needed. By attaching special identification marks or headers to incoming packets, QoS determines queue of packets based on priority. It is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This function provides better service of selected network traffic over various technologies.

4.8.1 QoS Queue

This page is used to configure the QoS policy and Queue. Choose the QoS Profile which you want to applied and set a value as the top Uptream Bandwidth limit. select SP of policy, the lower numbers imply greater precedence.



QoS Global Settings

Enable QoS Profile:	TR069,INTERNET ▾ (Changing profile will affect all QoS settings)
Enable:	□
Upstream Bandwidth	10000 Kbps (0 means no rate limit)
Scheduling Policy:	SP ▾
Enable Force Bandwidth:	□
DSCP/TC Mark:	□
802.1P Tag:	□
TCP Connection Number Limit:	□

Upstream Queue Settings

Number	Enable	Priority(1 is the highest)
1	☑	1
2	☑	2
3	☑	3
4	☑	4
5	□	5
6	□	6
7	□	7
8	□	8

4.8.2 QoS Classification

To add a QoS classification rule:

Step 1 Go to **Advanced Setup > Quality of Service > Classification** page.

Step 2 Click **Add traffic Type**.

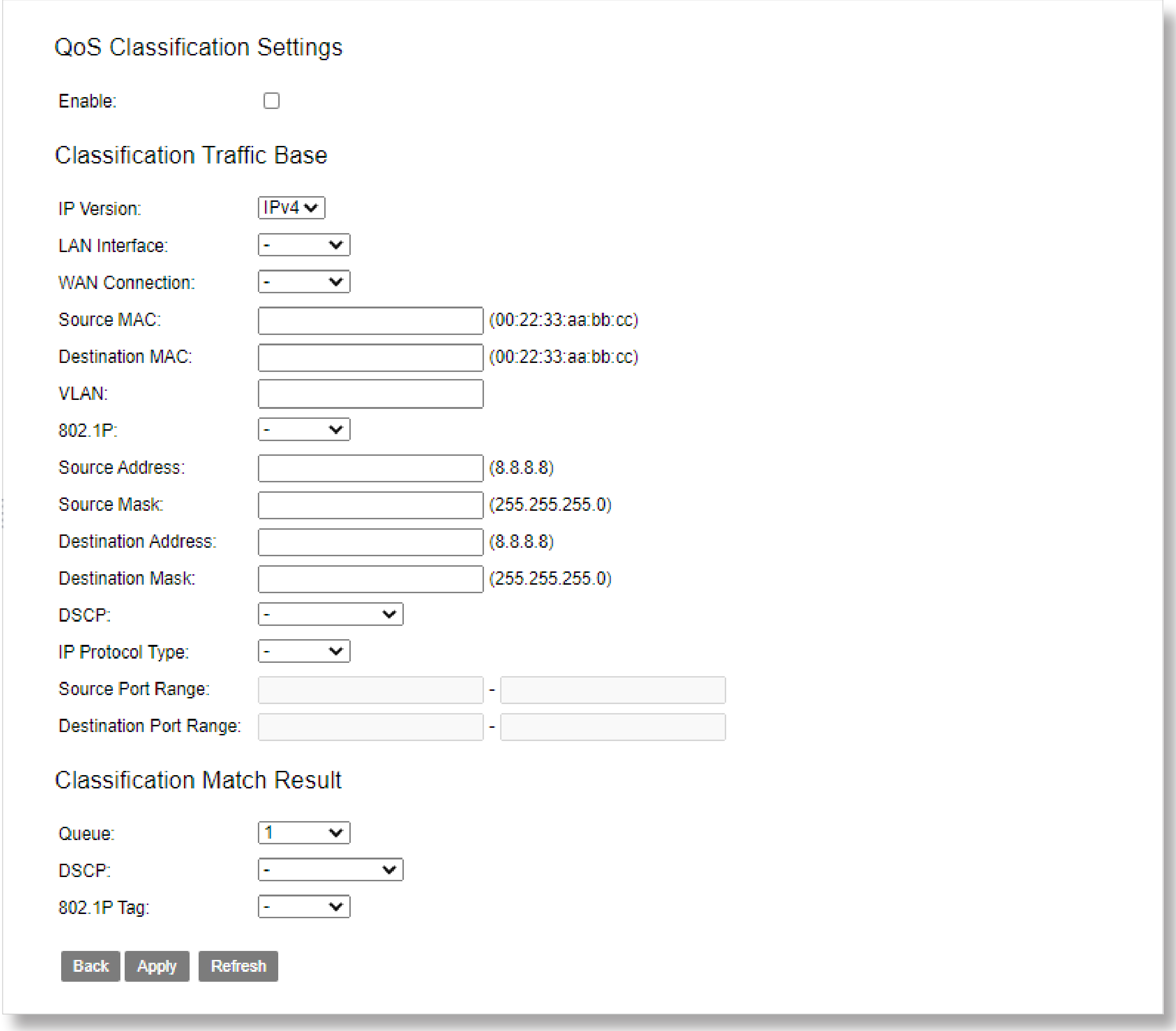
1. Check the **Enable** box.
2. Select a Service Name.
3. Select the Queue, DSCP, 802.1P Tag according to your actual demands.

Note: The lower Queue numbers imply greater precedence.
The higher DSCP numbers imply greater precedence.
The lower 802.1P Tag numbers imply greater precedence.

4. Click **Apply**.

Step 3 Click **Add Flow**.

1. Check the **Enable** box.
2. Select the WAN Connection, 802.1P, IP Protocol Type, Destination Port Range, Queue, DSCP, 802.1P Tag according to your actual demands.
3. Click **Apply**.



QoS Classification Settings

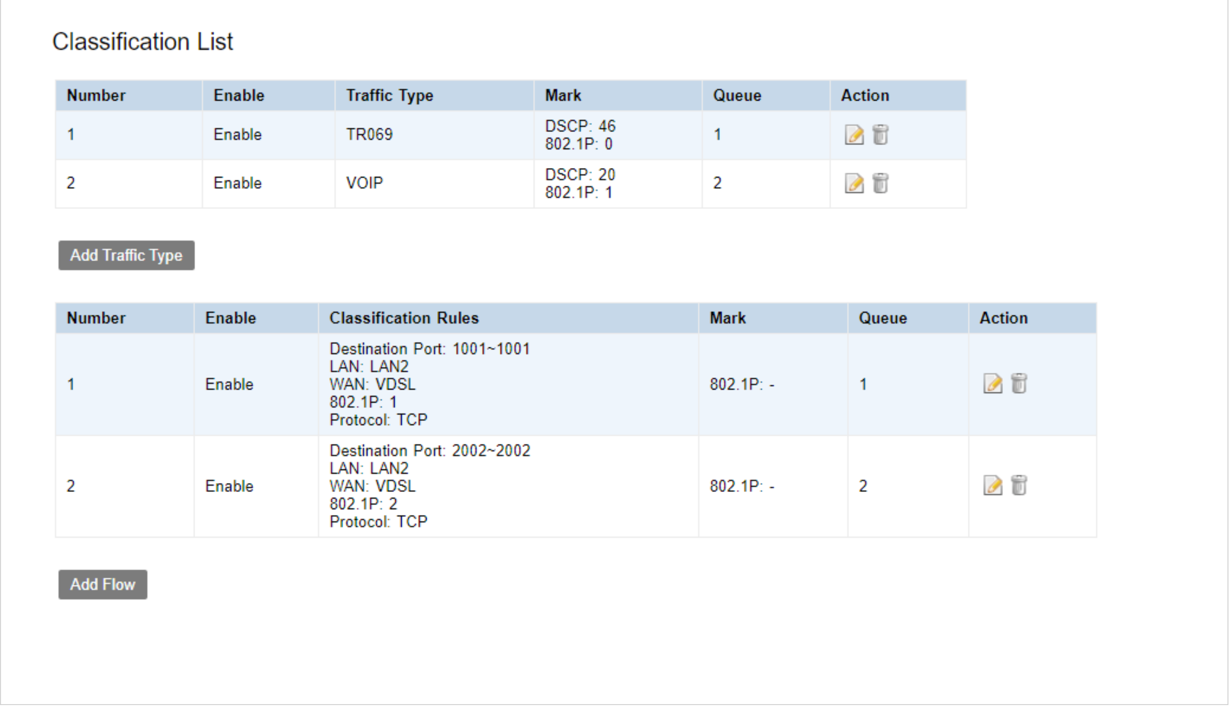
Enable: □

Classification Traffic Base

IP Version:	IPv4
LAN Interface:	-
WAN Connection:	-
Source MAC:	(00:22:33:aa:bb:cc)
Destination MAC:	(00:22:33:aa:bb:cc)
VLAN:	
802.1P:	-
Source Address:	(8.8.8.8)
Source Mask:	(255.255.255.0)
Destination Address:	(8.8.8.8)
Destination Mask:	(255.255.255.0)
DSCP:	-
IP Protocol Type:	-
Source Port Range:	-
Destination Port Range:	-

Classification Match Result

Queue:	1
DSCP:	-
802.1P Tag:	-



Classification List

Number	Enable	Traffic Type	Mark	Queue	Action
1	Enable	TR069	DSCP: 46 802.1P: 0	1	
2	Enable	VOIP	DSCP: 20 802.1P: 1	2	

Number	Enable	Classification Rules	Mark	Queue	Action
1	Enable	Destination Port: 1001~1001 LAN: LAN2 WAN: VDSL 802.1P: 1 Protocol: TCP	802.1P: -	1	
2	Enable	Destination Port: 2002~2002 LAN: LAN2 WAN: VDSL 802.1P: 2 Protocol: TCP	802.1P: -	2	

4.9 Bandwidth Limit

4.9.1 Port Bandwidth Limit

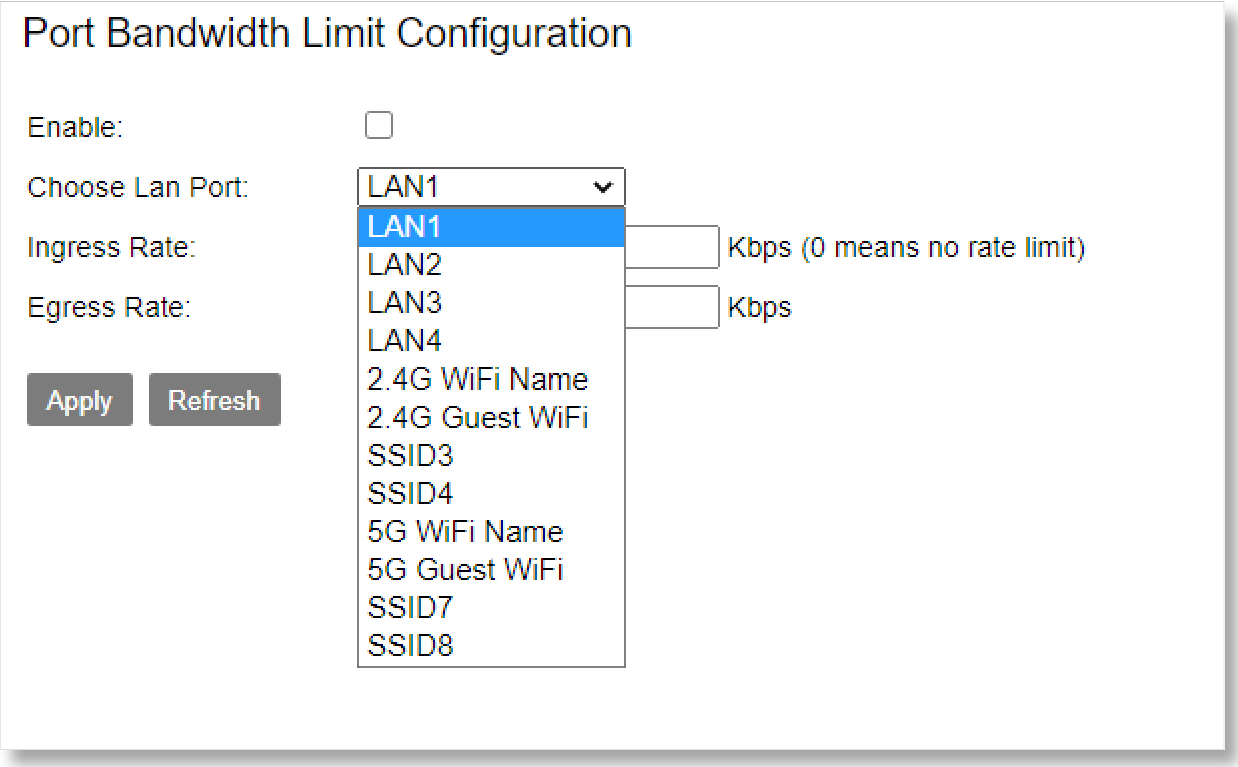
If you want to allocate bandwidth according to your demands, configure the bandwidth control function to meet the requirement.

To configure the port bandwidth limit：

Step 1 Go to **Advanced Setup > Bandwidth Limit > Port Bandwidth Limit** page and check the **Enable** box.

Step 2 Target LAN Port to be controlled, and enter the Top Ingress rate and Top Egress Rate for it.

Step 3 Click **Apply**.



Port Bandwidth Limit Configuration

Enable: □

Choose Lan Port: LAN1

Ingress Rate: Kbps (0 means no rate limit)

Egress Rate: Kbps

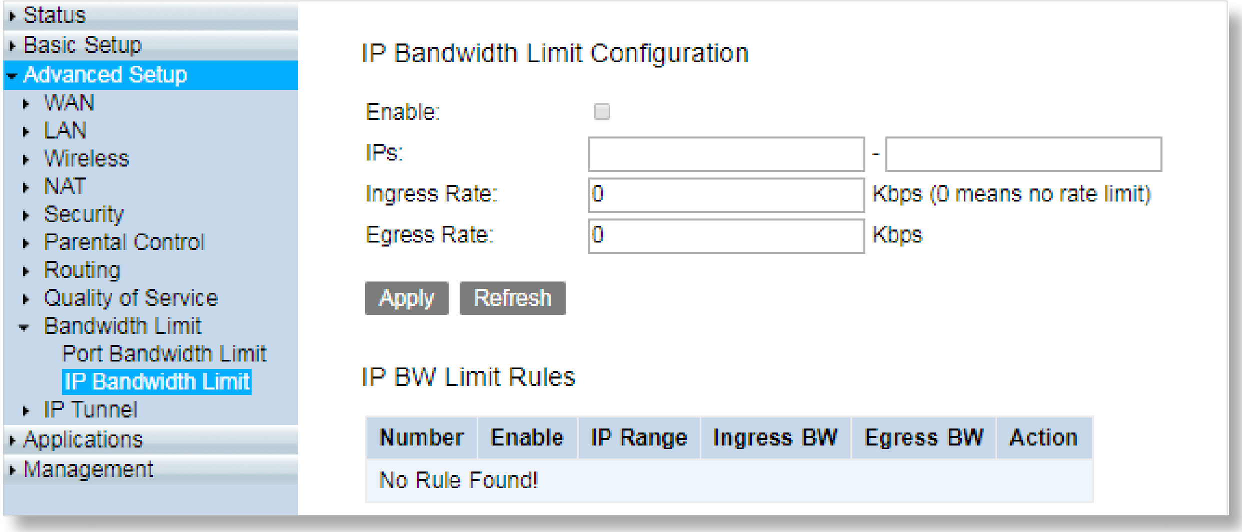
4.9.2 IP Bandwidth Limit

To configure the IP bandwidth limit：

Step 1 Go to **Advanced Setup > Bandwidth Limit > IP Bandwidth Limit** page and check the **Enable** box.

Step 2 Target IPs to be controlled, and enter the Top Ingress rate and Top Egress Rate.

Step 3 Click **Apply**.



IP Bandwidth Limit Configuration

Enable: □

IPs: [ ] - [ ]

Ingress Rate: 0 Kbps (0 means no rate limit)

Egress Rate: 0 Kbps

IP BW Limit Rules

Number	Enable	IP Range	Ingress BW	Egress BW	Action
No Rule Found!					

4.10 IP Tunnel

An IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulating one IP packet in another IP packet. To encapsulate an IP packet in another IP packet, an outer header is added with source IP, the entry point of the tunnel and the destination point, the exit point of the tunnel. While doing this, the inner packet is unmodified.

4.10.1 IPv4inIPv6

IPv4inIPv6 is an Internet interoperation mechanism allowing Internet Protocol version 4 (IPv4) to be used in an IPv6 only network. 4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels.

To configure the IPv4inIPv6 tunnel：

Step 1 Go to **Advanced Setup > IP Tunnel > IPv4inIPv6** page.

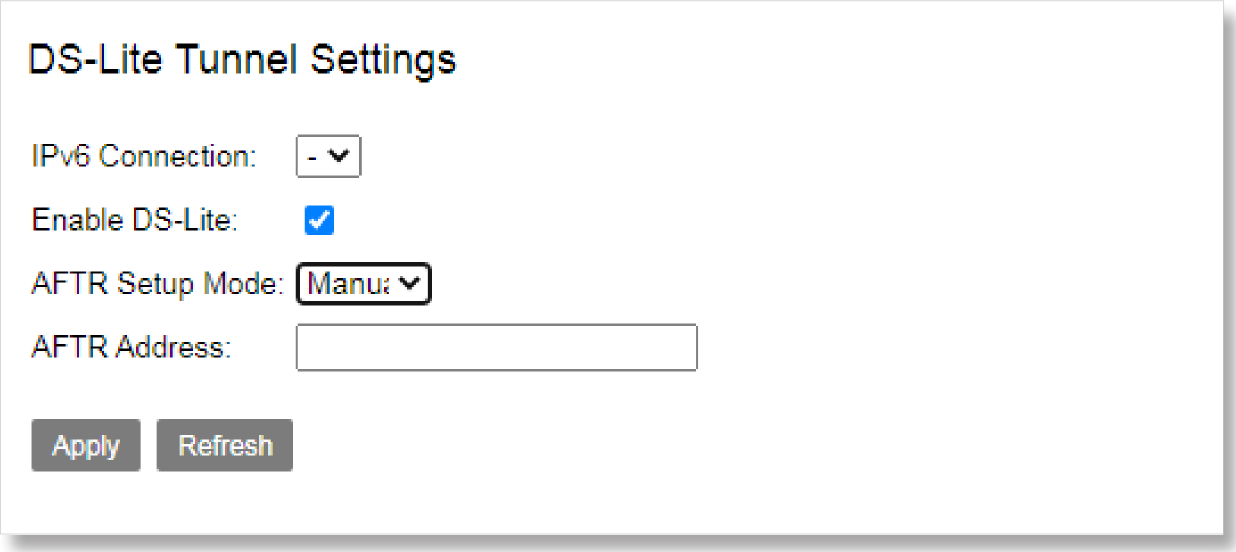
Step 2 Check **Enable DS-Lite** box.

Step 3 Select a mode of obtaining AFTR IPv6 address.

Manual: Manually set an AFTR IPv6 address.
Automatic: The modem router obtains the AFTR name through DHCPv6 option, and translates the AFTR name to specific IPv6 IP address through DNS. If you select Automatic, skip step 4.

Step 4 **AFTR:** Set the IPv6 AFTR address.

Step 5 Click **Apply**.



DS-Lite Tunnel Settings

IPv6 Connection: -

Enable DS-Lite: ☑

AFTR Setup Mode: Manu:

AFTR Address:

4.10.2 IPv6inIPv4

IPv6inIPv4 is an internet transition mechanism for migrating from Internet Protocol version 4 (IPv4) to IPv6. IPv6inIPv4 uses tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.

To configure the IPv6inIPv4 tunnel:

Step 1 Go to **Advanced Setup > IP Tunnel > IPv6inIPv4** page.

Step 2 Check **Enable** box.

Step 3 **Tunnel Name:** Specify a name for the tunnel you set up.

Step 4 **Mechanism:** Set the 6in4 tunnel implement mechanism. The modem router only supports 6RD.

Step 5 **Associated WAN Interface:** Select an associated WAN interface for the 6in4 tunnel. The WAN interface is required to use IPv4 protocol only.

Step 6 Select a type of obtaining border relay address.

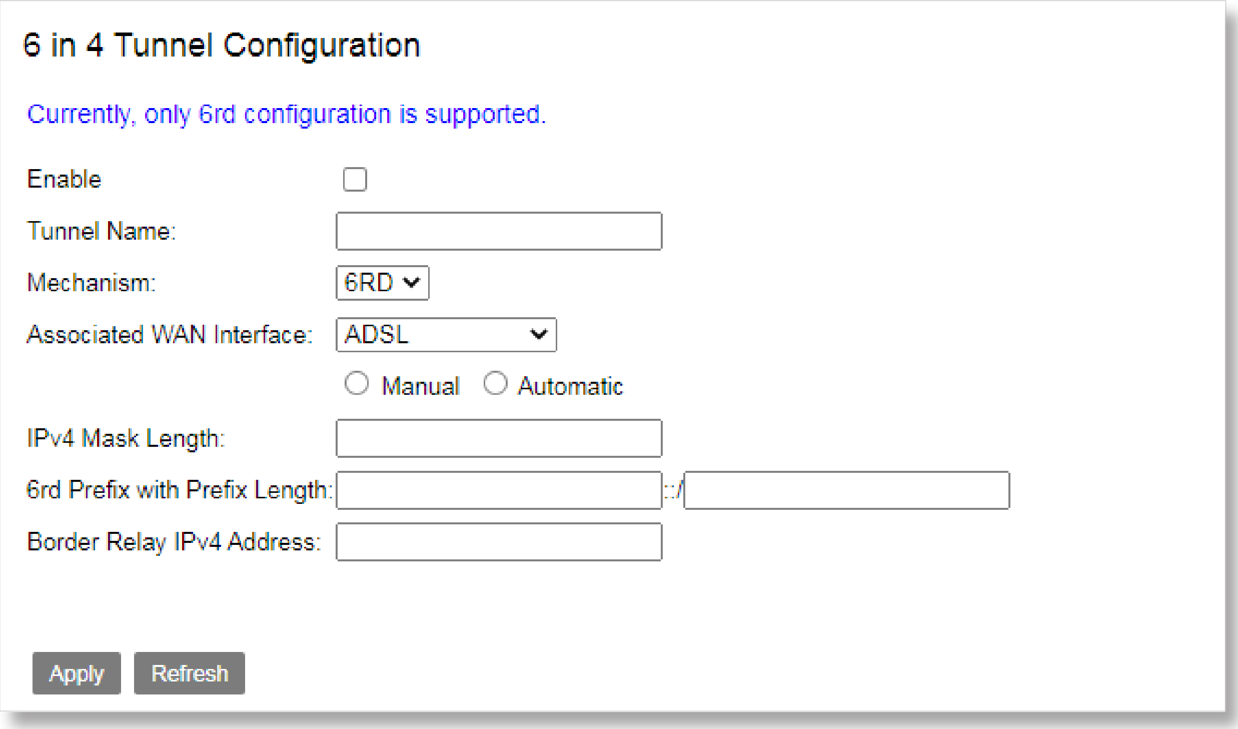
Manual: Manually set a 6RD-BR address.
Automatic: Automatically obtain a 6RD-BR address from BR. If you select Automatic, skip step 7 to 9.

Step 7 **IPv4 Mask Length:** Enter the IPv4 mask length.

Step 8 6rd Prefix with Prefix Length: Enter the 6RD prefix with prefix length.

Step 9 Border Relay IPv4 Address: Enter the border relay IPv4 address of WAN interface.

Step 10 Click **Apply**.



6 in 4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Enable □

Tunnel Name:

Mechanism: 6RD

Associated WAN Interface: ADSL

○ Manual ○ Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length: ::/

Border Relay IPv4 Address:

4.10.3 GRE Tunnel

GRE is a method of establishing direct point-to-point connections over a network with the aim of simplifying connections between individual networks.

To configure the GRE tunnel：

Step 1 Go to **Advanced Setup > IP Tunnel > GRE Tunnel** page.

Step 2 Select your connection name.

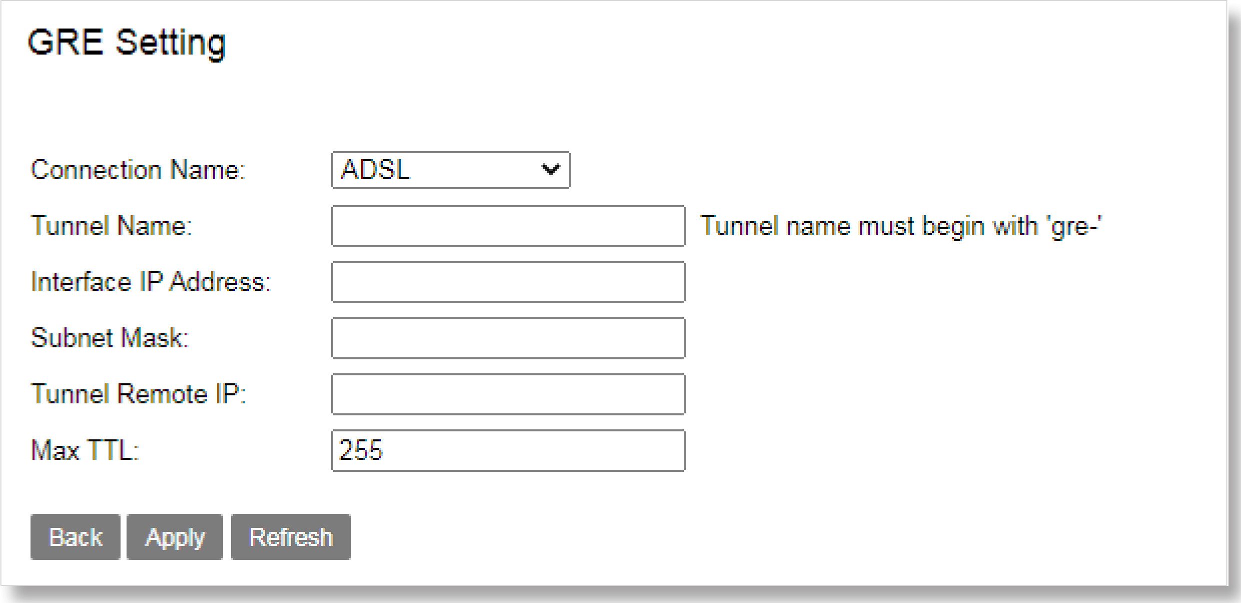
Step 3 **Tunnel Name:** Specify a name for the tunnel you set up.

Step 4 Enter the IP Address which interface you want to created.

Step 5 Set **Subnet Mask**.

Step 6 **Tunnel Remote IP:** Specify the destination IP address for the Tunnel interface.

Step 7 Click **Apply**.



GRE Setting

Connection Name: ADSL

Tunnel Name: Tunnel name must begin with 'gre-'

Interface IP Address:

Subnet Mask:

Tunnel Remote IP:

Max TTL: 255

Chapter 5

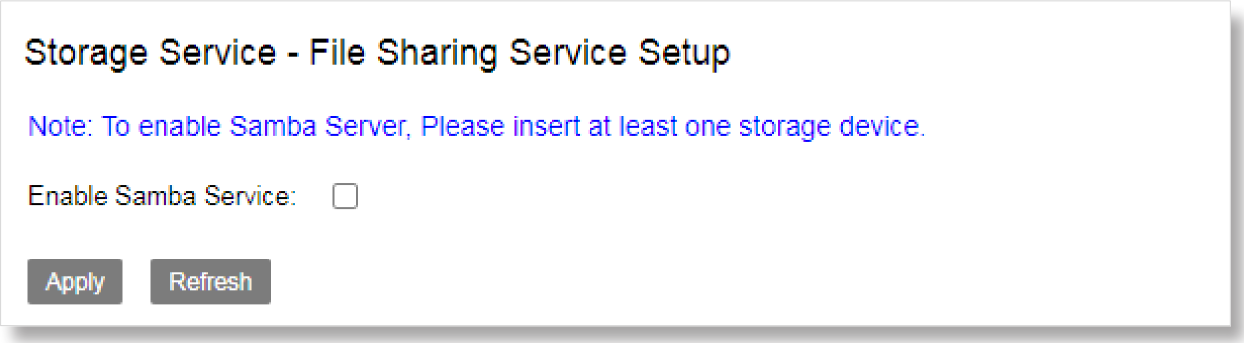
Applications

This Chapter describes about application of web UI.

It contains the following sections:

5.1 Storage Service

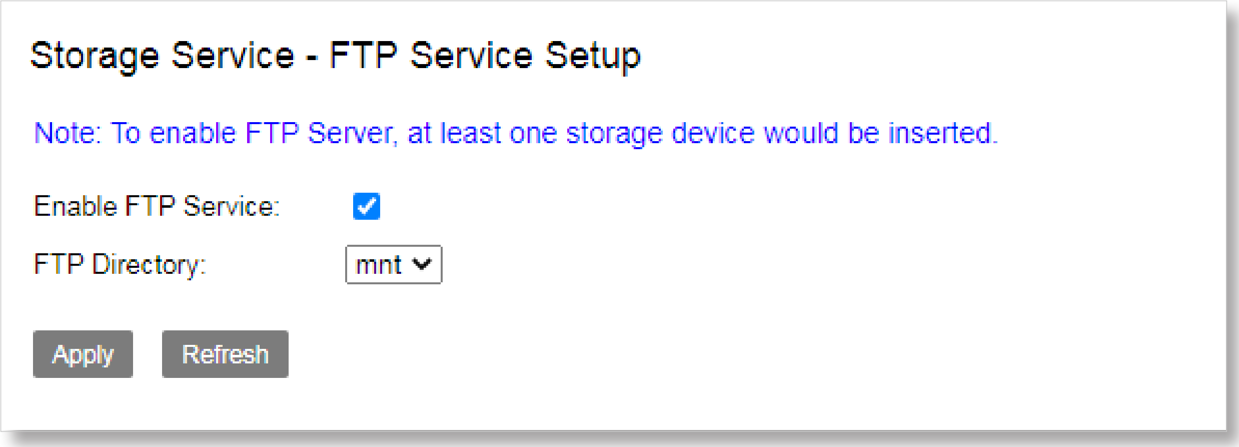
The modem router can automatically recognize a USB storage device connected to the USB port of the modem router. The device can be accessed over the LAN through Samba, FTP or TFTP.



Storage Service - File Sharing Service Setup

Note: To enable Samba Server, Please insert at least one storage device.

Enable Samba Service: □

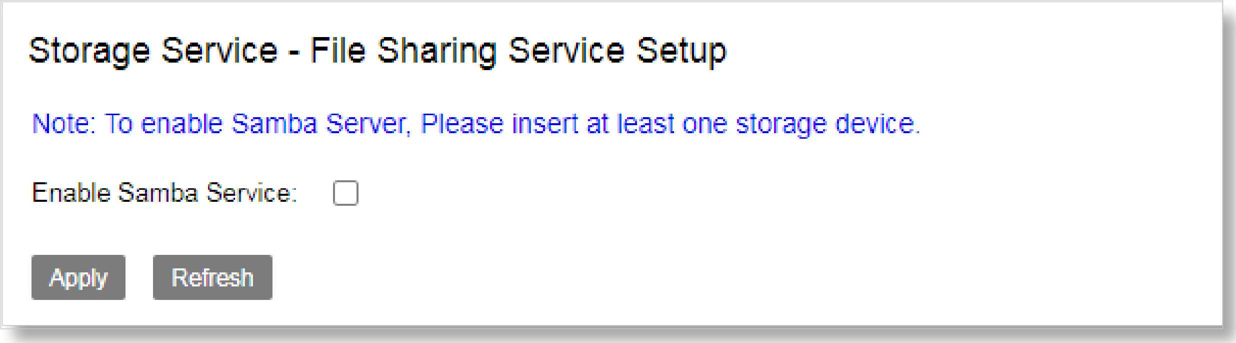


Storage Service - FTP Service Setup

Note: To enable FTP Server, at least one storage device would be inserted.

Enable FTP Service: ☑

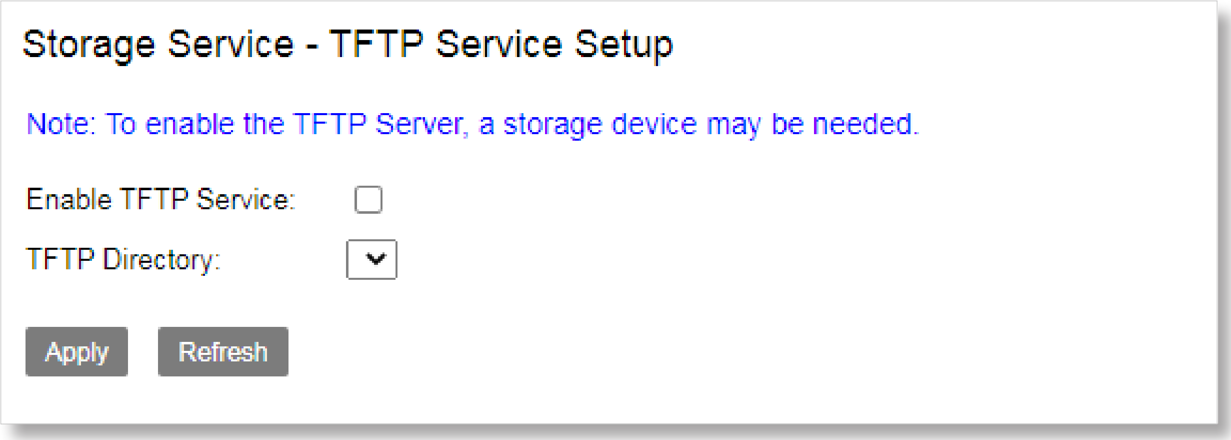
FTP Directory: mnt



Storage Service - File Sharing Service Setup

Note: To enable Samba Server, Please insert at least one storage device.

Enable Samba Service: □



Storage Service - TFTP Service Setup

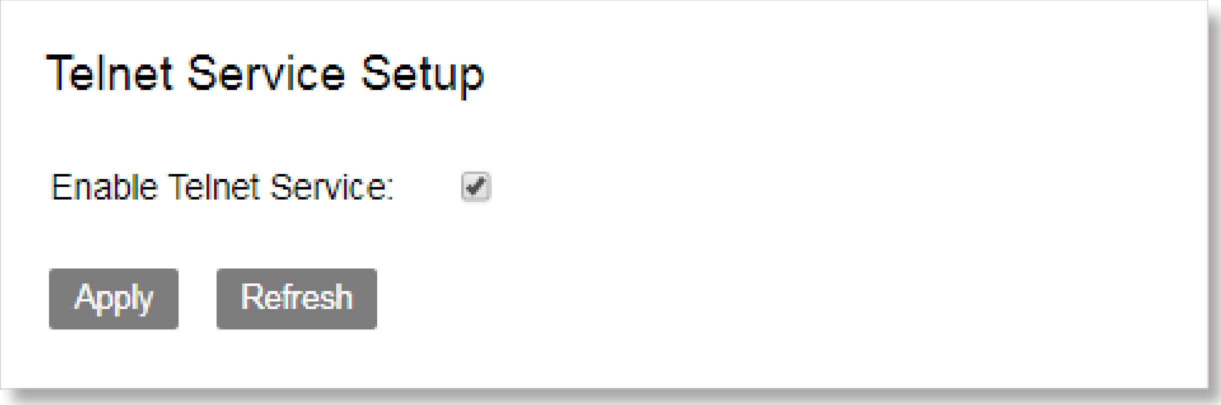
Note: To enable the TFTP Server, a storage device may be needed.

Enable TFTP Service: □

TFTP Directory:

5.2 Telnet Service

Telnet protocol is a member of TCP/IP protocol family, is the Internet remote login service standard protocol and the main way. It provides users with the ability to perform remote host work on their local computer. Use the Telnet program on the end user's computer to connect to the server. An end user can type commands into a Telnet program that are run on the server as if they were typed directly on the server's console.You can control the server locally. To start a Telnet session, you must enter a user name and password to log on to the server.Telnet is a common method for remote control of Web servers.

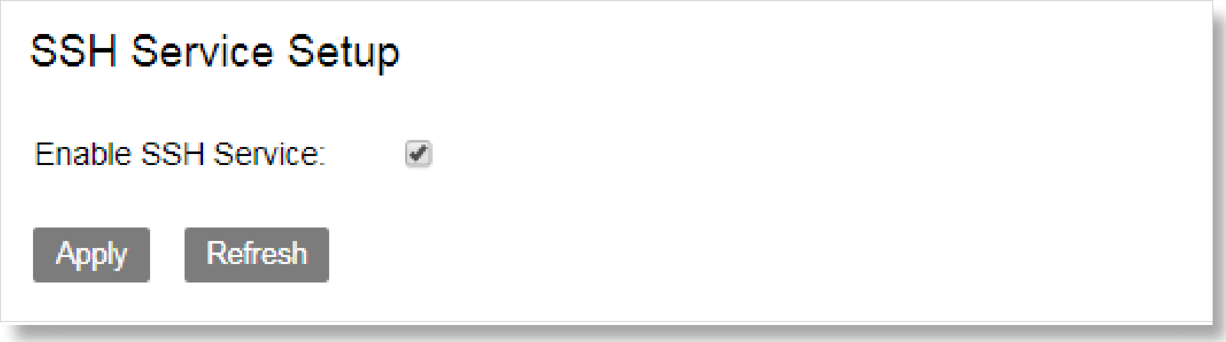


Telnet Service Setup

Enable Telnet Service: ☑

5.3 SSH Service

SSH is a security protocol based on the application layer. SSH is a relatively reliable protocol designed to provide security for remote login sessions and other network services. Using SSH protocol can effectively prevent information leakage in the process of remote management. SSH was originally a program on UNIX systems and has since expanded rapidly to other operating platforms. SSH, when used correctly, can fill holes in your network.The SSH client is available on a variety of platforms.

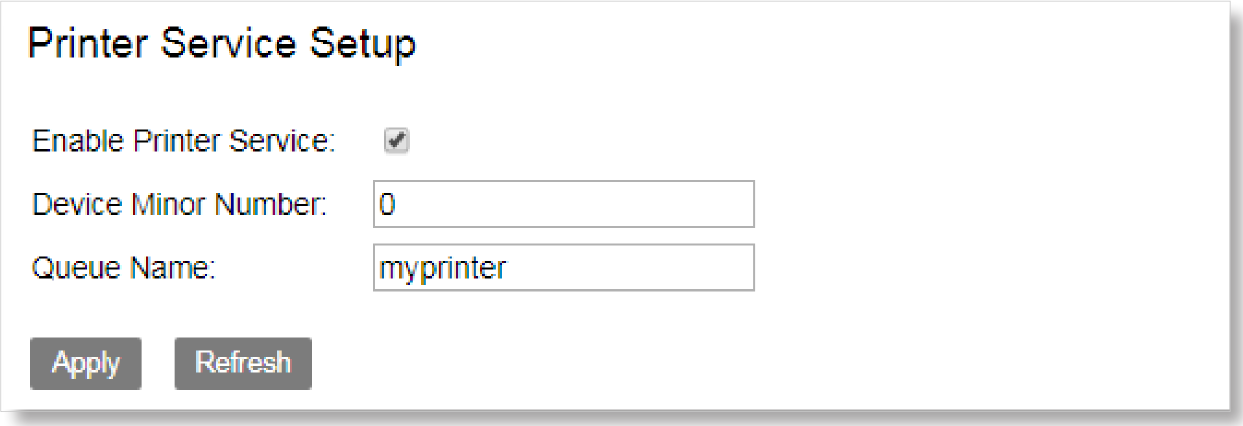


SSH Service Setup

Enable SSH Service: ☑

5.4 Printer Share

This function allows you to share with printer.



Printer Service Setup

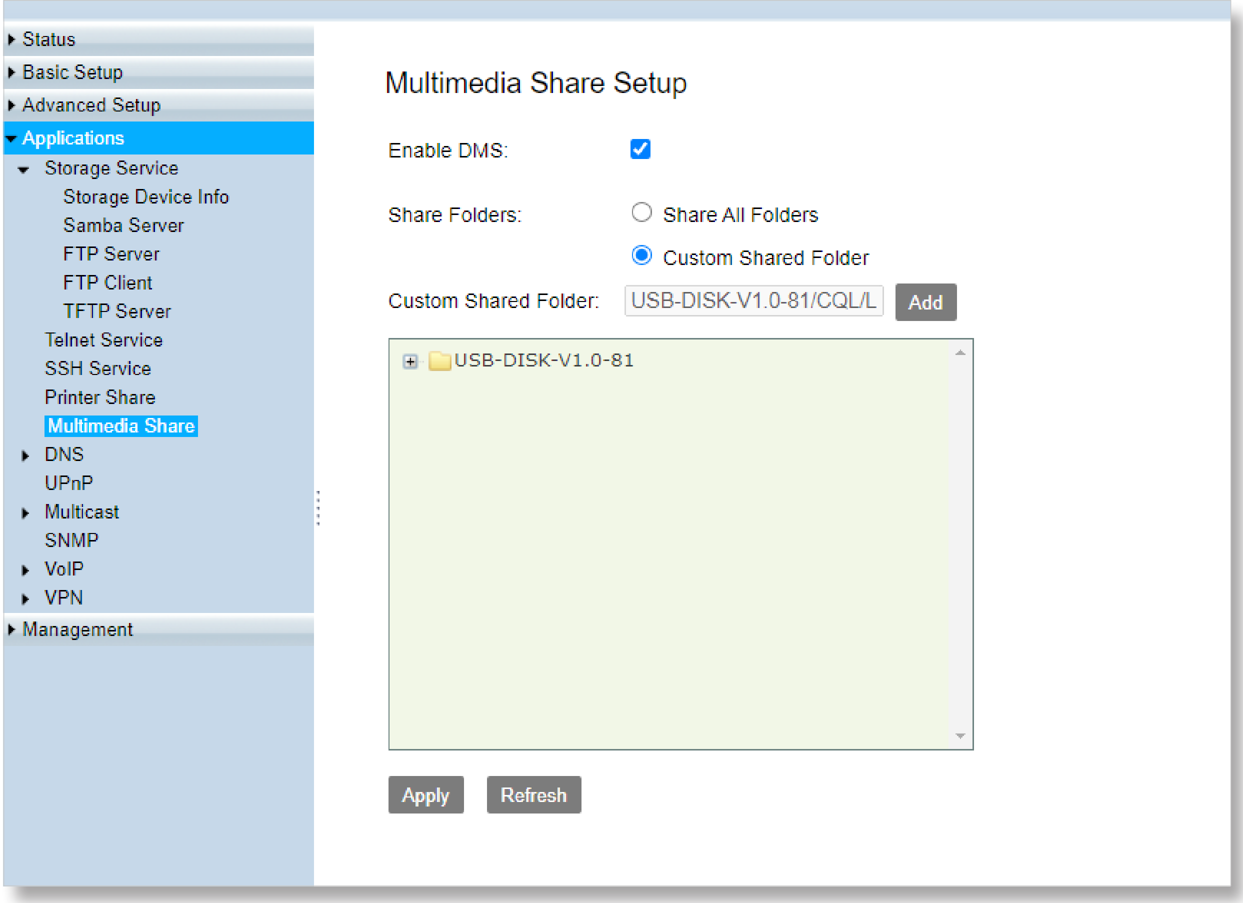
Enable Printer Service: ☑

Device Minor Number: 0

Queue Name: myprinter

5.5 Multimedia Share

This function allows you to share with multimedia.



Multimedia Share Setup

Enable DMS: ☑

Share Folders: ○ Share All Folders ● Custom Shared Folder

Custom Shared Folder: USB-DISK-V1.0-81/CQL/L

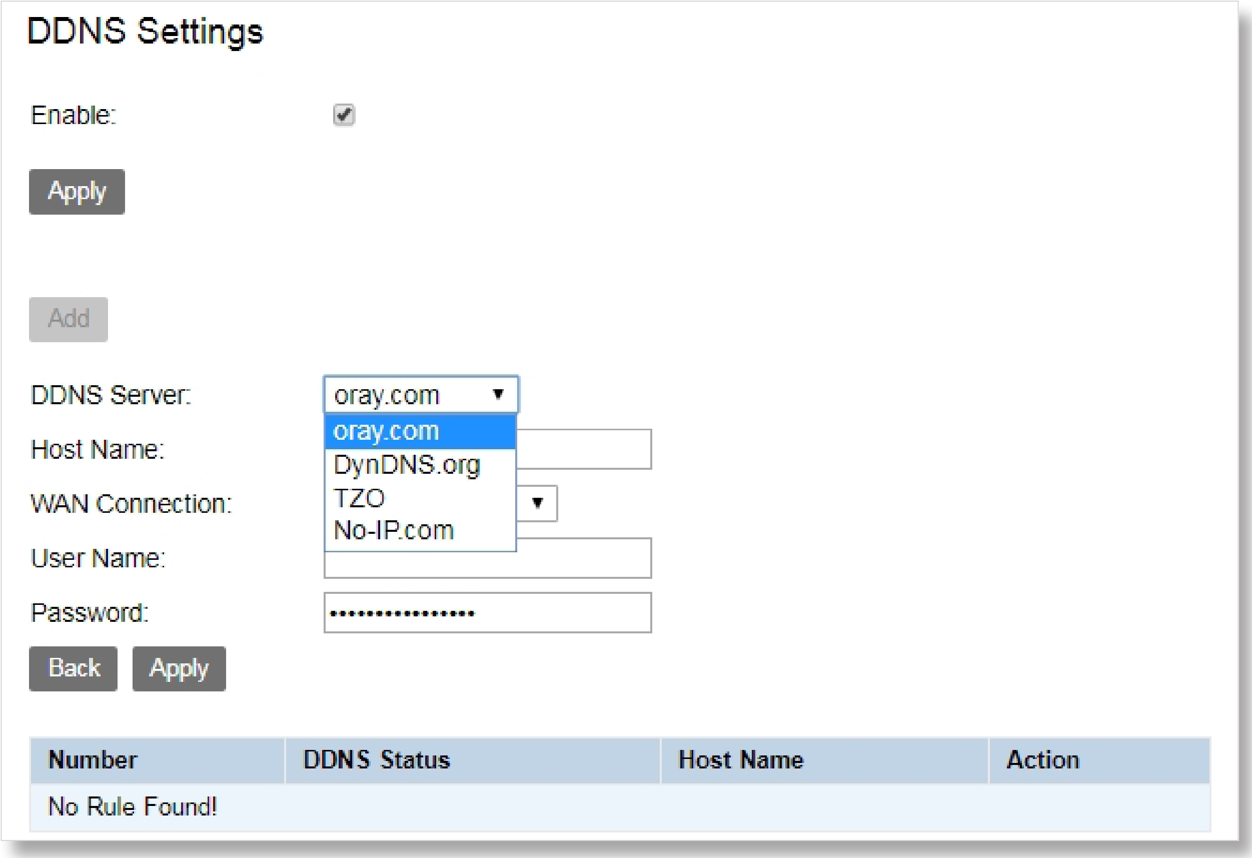
5.6 DNS

Dynamic DNS

DDNS maps the WAN IP address (changeable public IP address) of the router to a domain name for dynamic domain name resolution. This ensures proper operation of functions that involve the WAN IP address of the modem router, such as the remote management and virtual server functions.

To access the configuration page, log in to the web UI of the router, and choose **Applications > DNS > Dynamic DNS**.

This function is disabled by default. When it is enabled, the page is shown as below.



DDNS Settings

Enable: ☑

DDNS Server: oray.com ▾

Host Name:

WAN Connection:

User Name:

Password: ••••••••••••••••

Number	DDNS Status	Host Name	Action
No Rule Found!			

Parameter	Description
Enable	It specifies whether to enable the DDNS function.
DDNS Server	It specifies a DDNS provider that can map changeable IP addresses to one static domain name. The modem router supports the oray.com, DynDNS.org, TZO and no-ip.com DDNS providers.
Host Name	It specifies the domain name you applied on the website of your service provider. It is only required when dyn.com is chosen as the service provider.
Username	It specifies the user name and password registered on a DDNS service provider's website for logging in to the DDNS service.
Password	

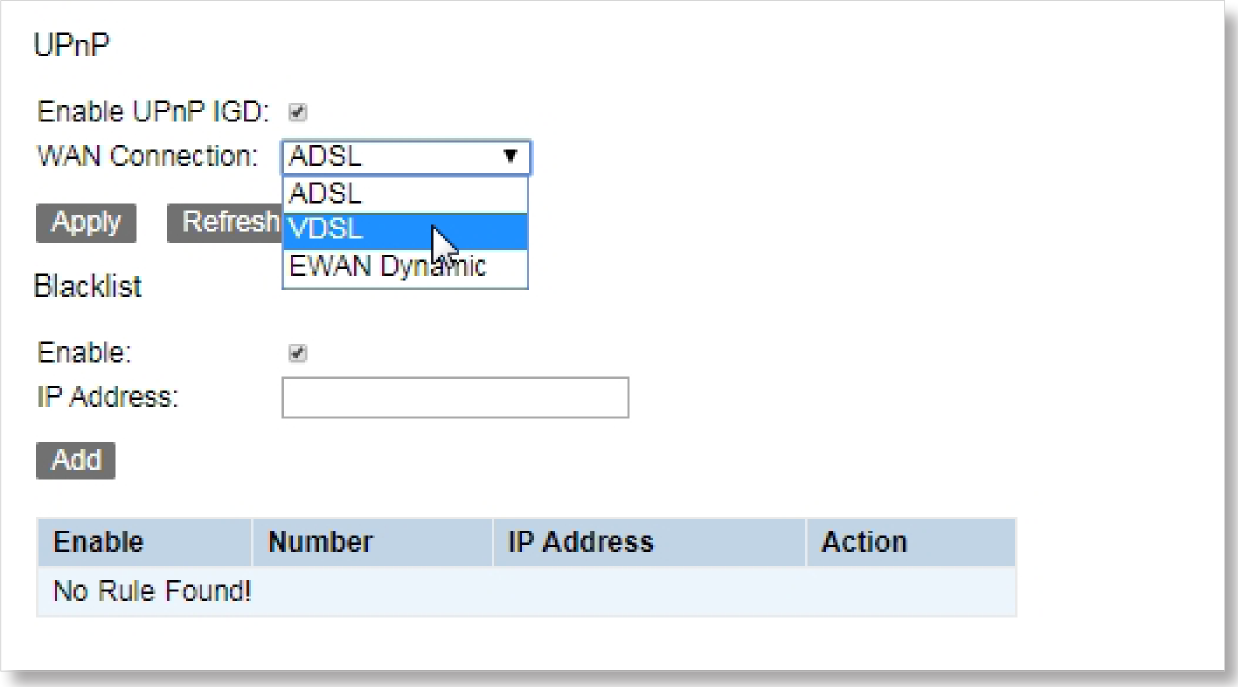
5.7 UPnP

After the UPnP function is enabled, it can automatically enable ports for UPnP-supported programs, such as P2P and gaming software, in the internal network to improve your network experience.

To access the configuration page, log in to the web UI of the router, and choose **Applications > UPnP**.

This function is disabled by default. When it is enabled, the page is shown as below.

And you can specify a IP Address into the blacklist.



UPnP

Enable UPnP IGD: ☑

WAN Connection: ADSL

Blacklist

Enable: ☑

IP Address:

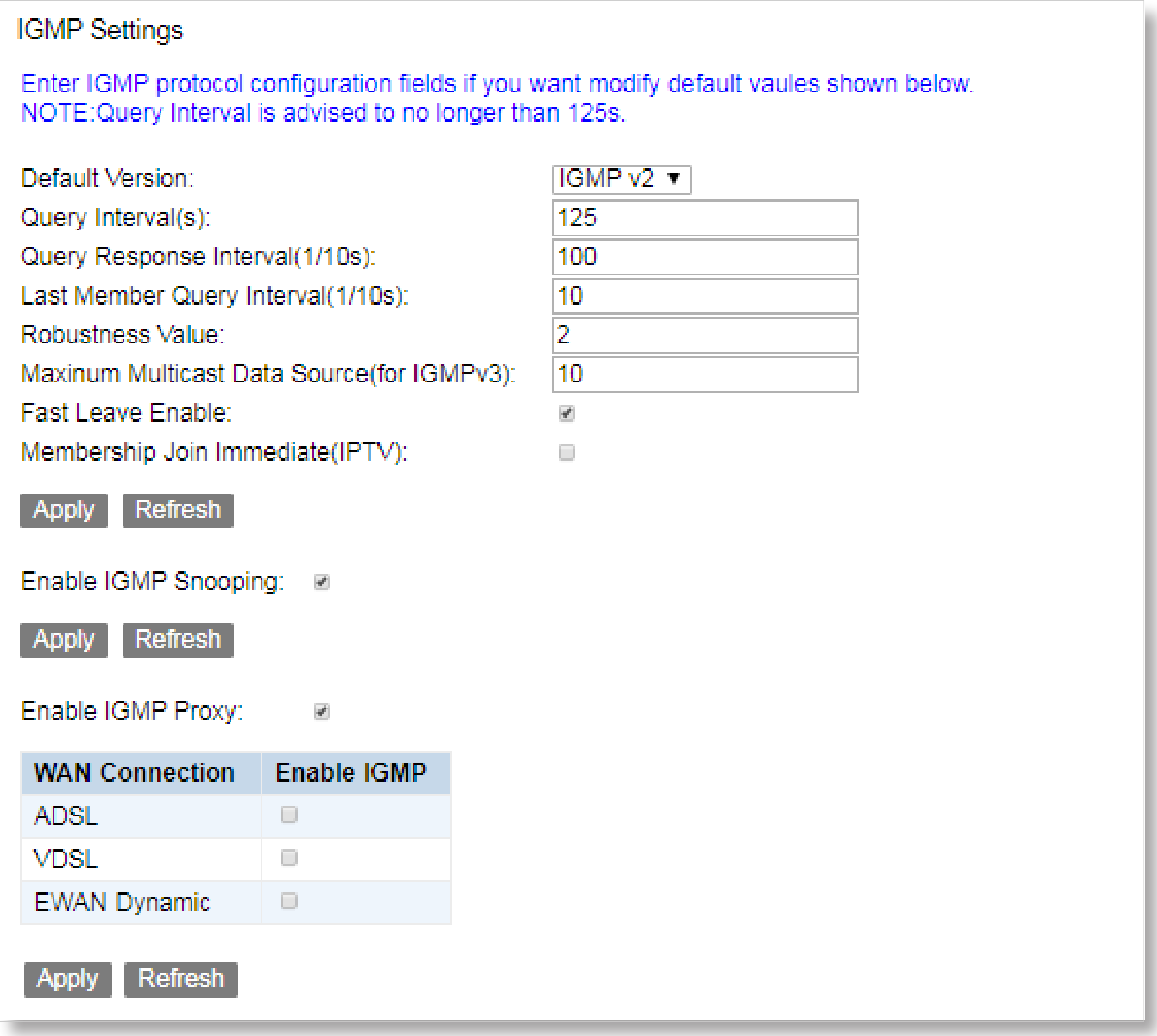
Enable	Number	IP Address	Action
No Rule Found!			

5.8 Multicast

5.8.1 IGMP

To access the configuration page, log in to the web UI of the router, and choose **Applications > Multicast > IGMP**.

Enter IGMP protocol configuration fields if you want modify default vaules shown below.



IGMP Settings

Enter IGMP protocol configuration fields if you want modify default vaules shown below.
NOTE:Query Interval is advised to no longer than 125s.

Default Version:	IGMP v2 ▼
Query Interval(s):	125
Query Response Interval(1/10s):	100
Last Member Query Interval(1/10s):	10
Robustness Value:	2
Maxinum Multicast Data Source(for IGMPv3):	10
Fast Leave Enable:	☑
Membership Join Immediate(IPTV):	□

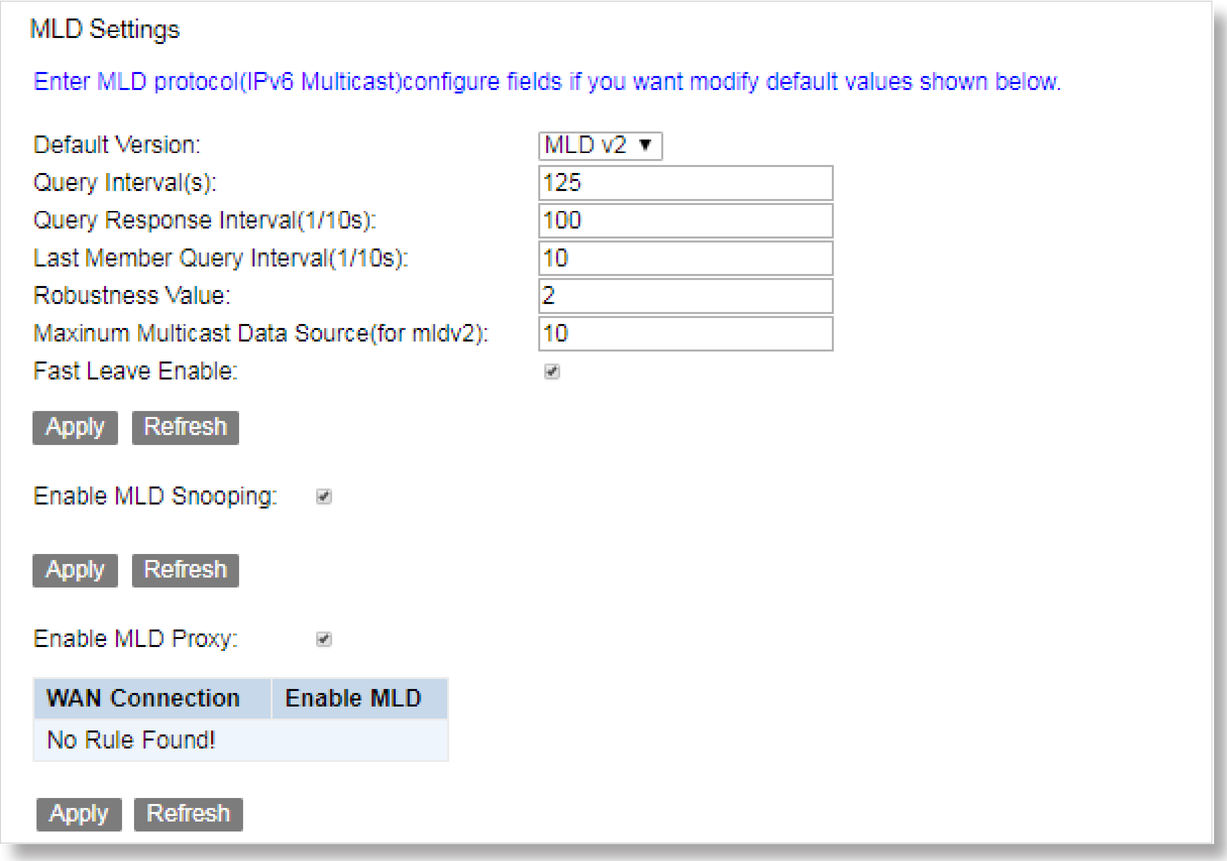
Enable IGMP Snooping: ☑

Enable IGMP Proxy: ☑

WAN Connection	Enable IGMP
ADSL	□
VDSL	□
EWAN Dynamic	□

5.8.2 MLD

To access the configuration page, log in to the web UI of the router, and choose **Applications > Multicast > MLD**.



MLD Settings

Enter MLD protocol(IPv6 Multicast)configure fields if you want modify default values shown below.

Default Version:	MLD v2 ▼
Query Interval(s):	125
Query Response Interval(1/10s):	100
Last Member Query Interval(1/10s):	10
Robustness Value:	2
Maxinum Multicast Data Source(for mldv2):	10
Fast Leave Enable:	☑

Enable MLD Snooping: ☑

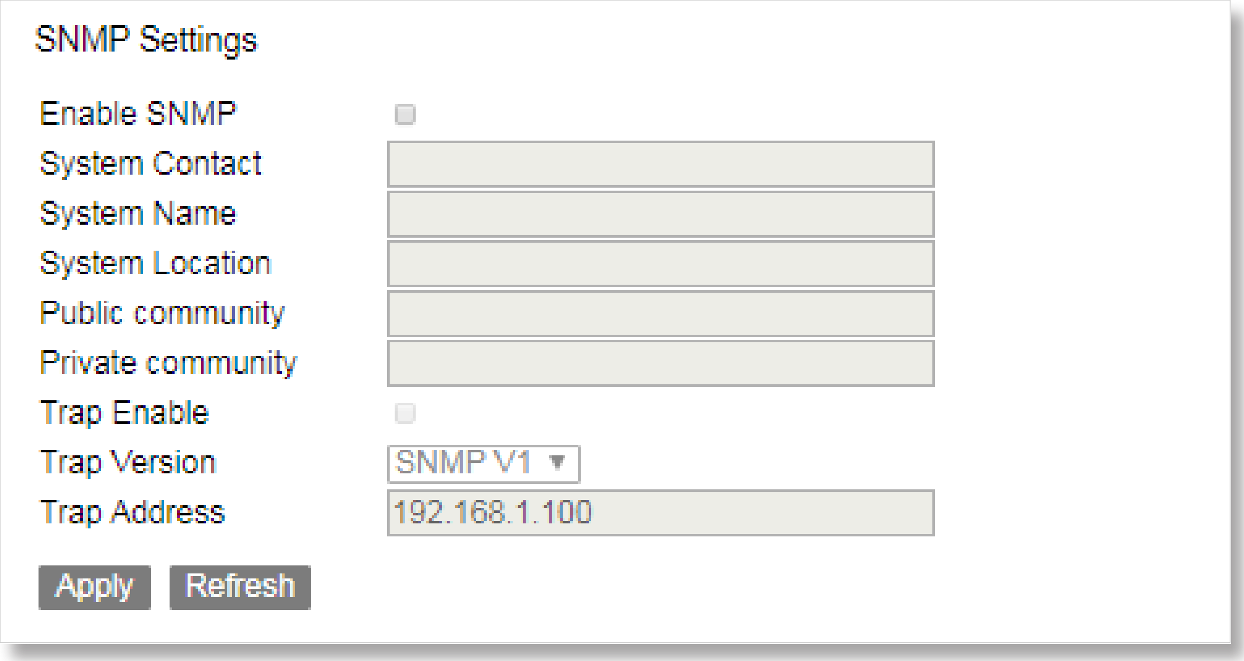
Enable MLD Proxy: ☑

WAN Connection	Enable MLD
No Rule Found!	

5.9 SNMP

The Simple Network Management Protocol (SNMP) is the most widely used network management protocol in TCP/IP networks. SNMP enables you to remotely manage all your network devices compliant with this protocol, such as monitoring the network status, changing network device settings, and receive network event alarms.

Go to **Applications > SNMP** to enter the configuration page.


SNMP Settings

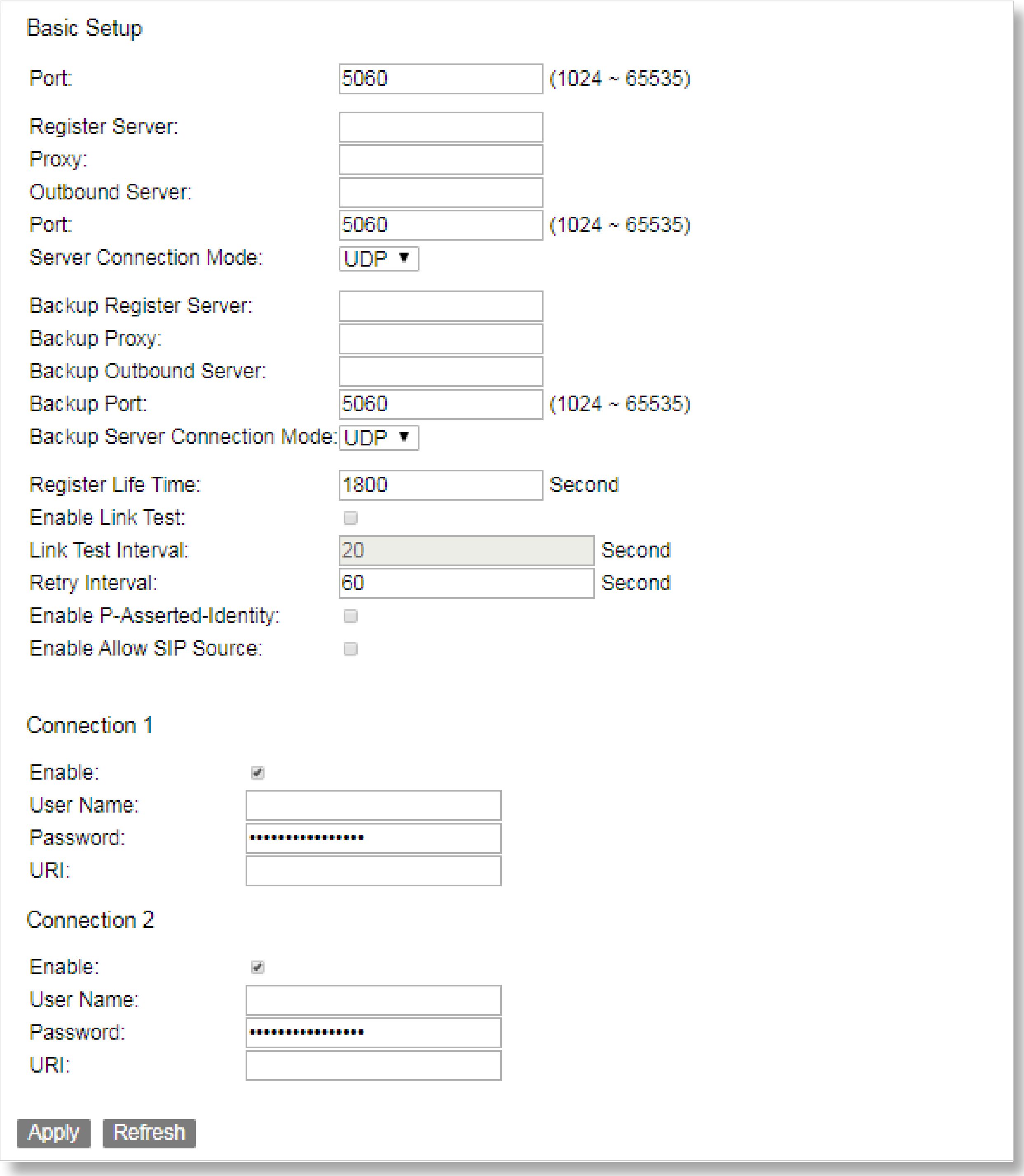
Enable SNMP	□
System Contact	
System Name	
System Location	
Public community	
Private community	
Trap Enable	□
Trap Version	SNMP V1 ▼
Trap Address	192.168.1.100

Parameter	Description
Enable SNMP	It specifies whether to enable the SNMP function of the modem router. By default, it is disabled.
System Contact	It specifies the contact information of the modem router.
System Name	It specifies the device name of the modem router.
System Location	It specifies the location where the modem router is used.
Public community	It specifies the read password shared between SNMP managers and this SNMP agent. The default password is public.
Priate community	It specifies the set password shared between SNMP managers and this SNMP agent. The default password is private.
Trap Address	It specifies the IP address of the server or terminal where alarm information is sent to.

5.10 VoIP

5.10.1 Basic Setup

Go to the **Applications > VoIP > Basic Setup** to access the configuration page.



Basic Setup

Port:	5060	(1024 ~ 65535)
Register Server:		
Proxy:		
Outbound Server:		
Port:	5060	(1024 ~ 65535)
Server Connection Mode:	UDP ▼	
Backup Register Server:		
Backup Proxy:		
Backup Outbound Server:		
Backup Port:	5060	(1024 ~ 65535)
Backup Server Connection Mode:	UDP ▼	
Register Life Time:	1800	Second
Enable Link Test:	□	
Link Test Interval:	20	Second
Retry Interval:	60	Second
Enable P-Asserted-Identity:	□	
Enable Allow SIP Source:	□	

Connection 1

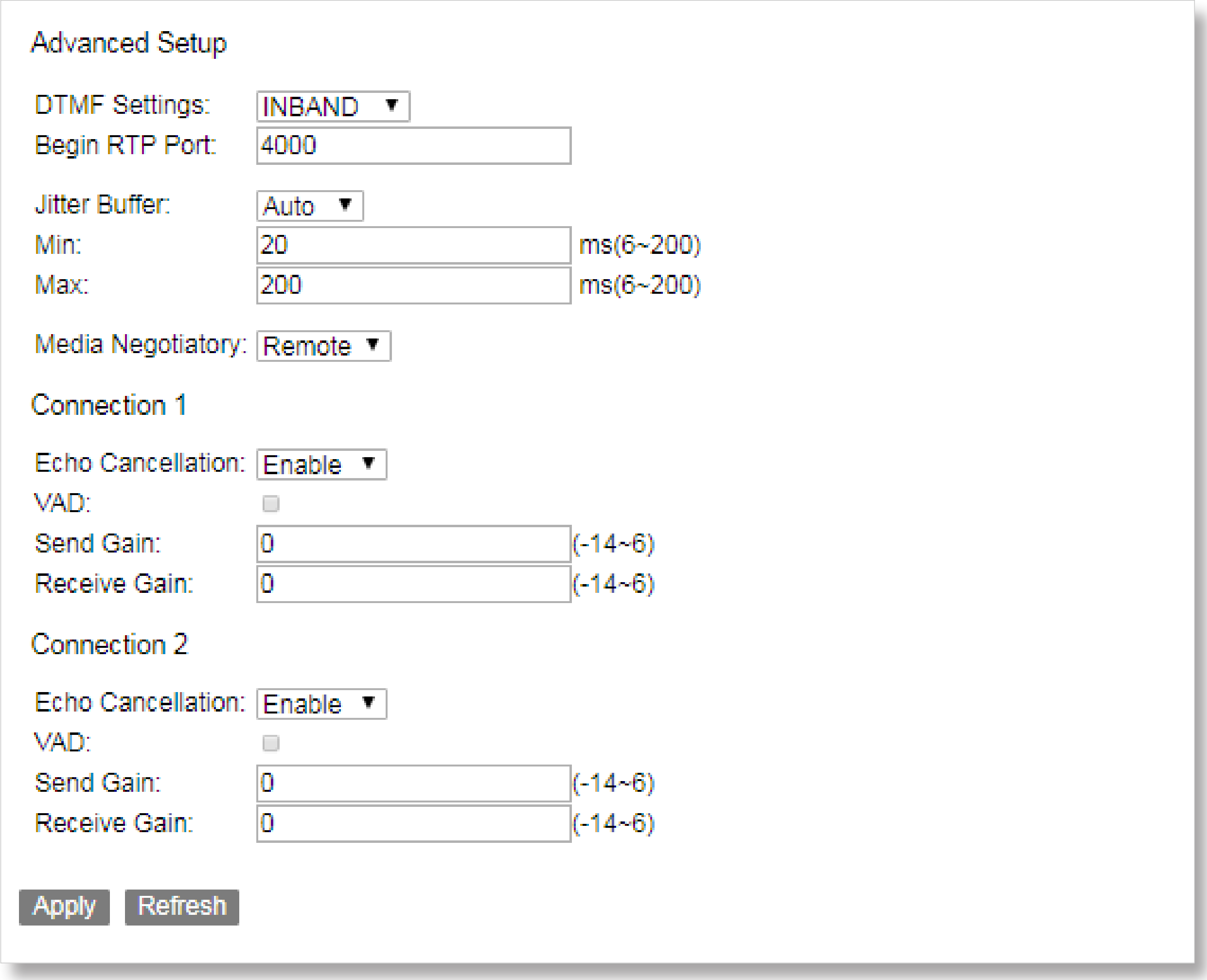
Enable:	☑
User Name:	
Password:	••••••••••••••••
URI:	

Connection 2

Enable:	☑
User Name:	
Password:	••••••••••••••••
URI:	

5.10.2 Advanced Setup

Go to the **Applications > VoIP > Advanced Setup** to access the configuration page.



Advanced Setup

DTMF Settings:	INBAND ▼	
Begin RTP Port:	4000	
Jitter Buffer:	Auto ▼	
Min:	20	ms(6~200)
Max:	200	ms(6~200)
Media Negotiatory:	Remote ▼	

Connection 1

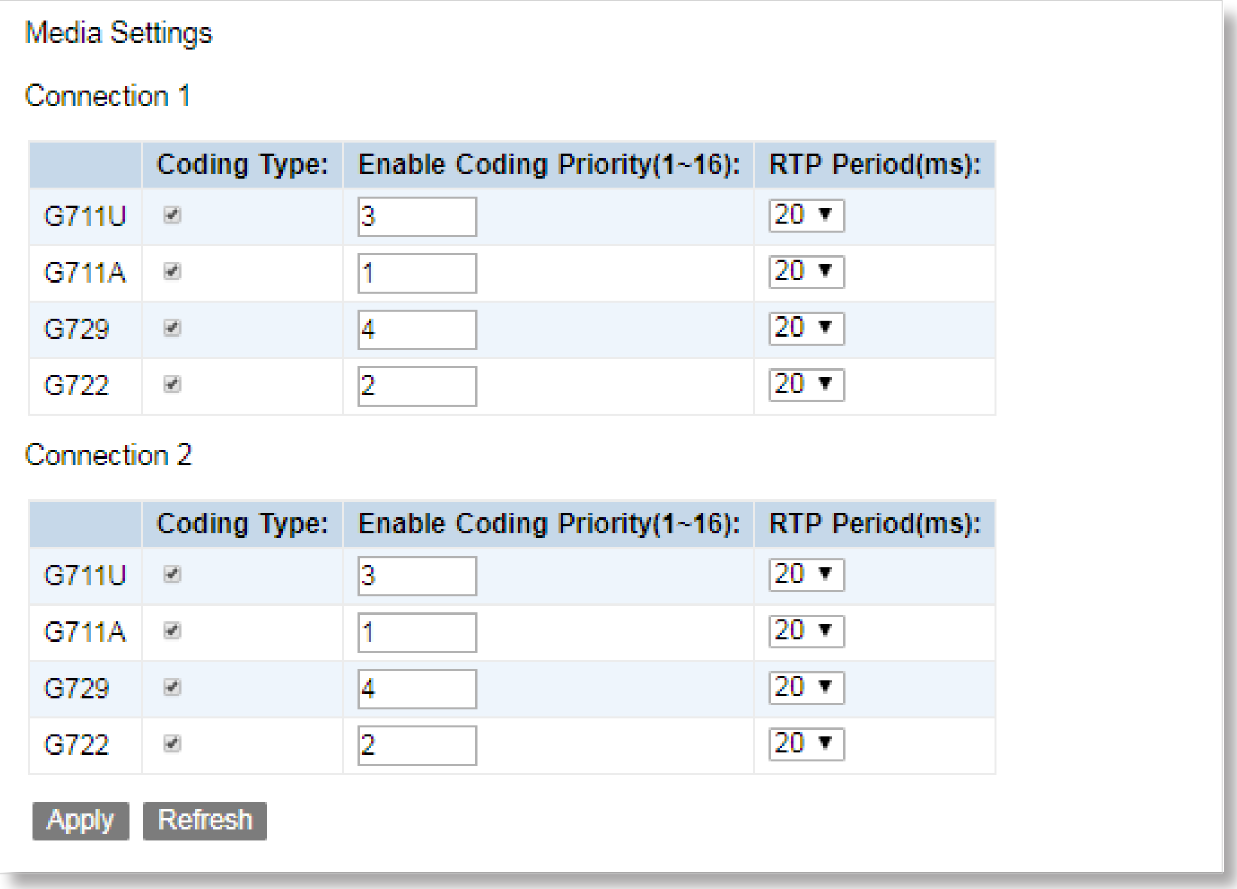
Echo Cancellation:	Enable ▼	
VAD:	□	
Send Gain:	0	(-14~6)
Receive Gain:	0	(-14~6)

Connection 2

Echo Cancellation:	Enable ▼	
VAD:	□	
Send Gain:	0	(-14~6)
Receive Gain:	0	(-14~6)

5.10.3 Media Settings

To access the configuration page, log in to the web UI of the router, and choose **Applications > VoIP > Advanced Setup**.



Media Settings

Connection 1

	Coding Type:	Enable Coding Priority(1~16):	RTP Period(ms):
G711U	☑	3	20 ▼
G711A	☑	1	20 ▼
G729	☑	4	20 ▼
G722	☑	2	20 ▼

Connection 2

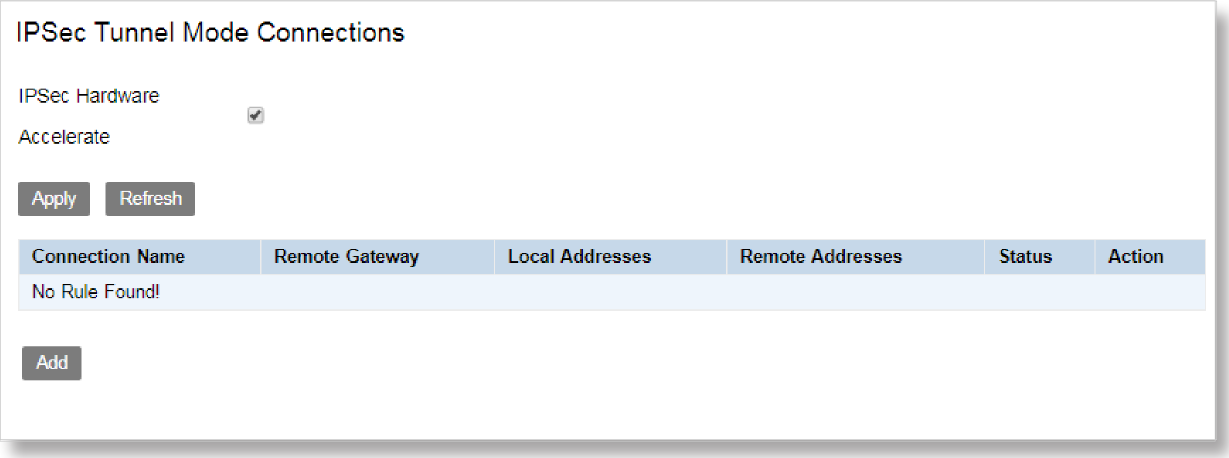
	Coding Type:	Enable Coding Priority(1~16):	RTP Period(ms):
G711U	☑	3	20 ▼
G711A	☑	1	20 ▼
G729	☑	4	20 ▼
G722	☑	2	20 ▼

5.11 VPN

IPSec

Internet Protocol Security (IPSec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks.

Choose **Applications > VPN > IPSec** page.

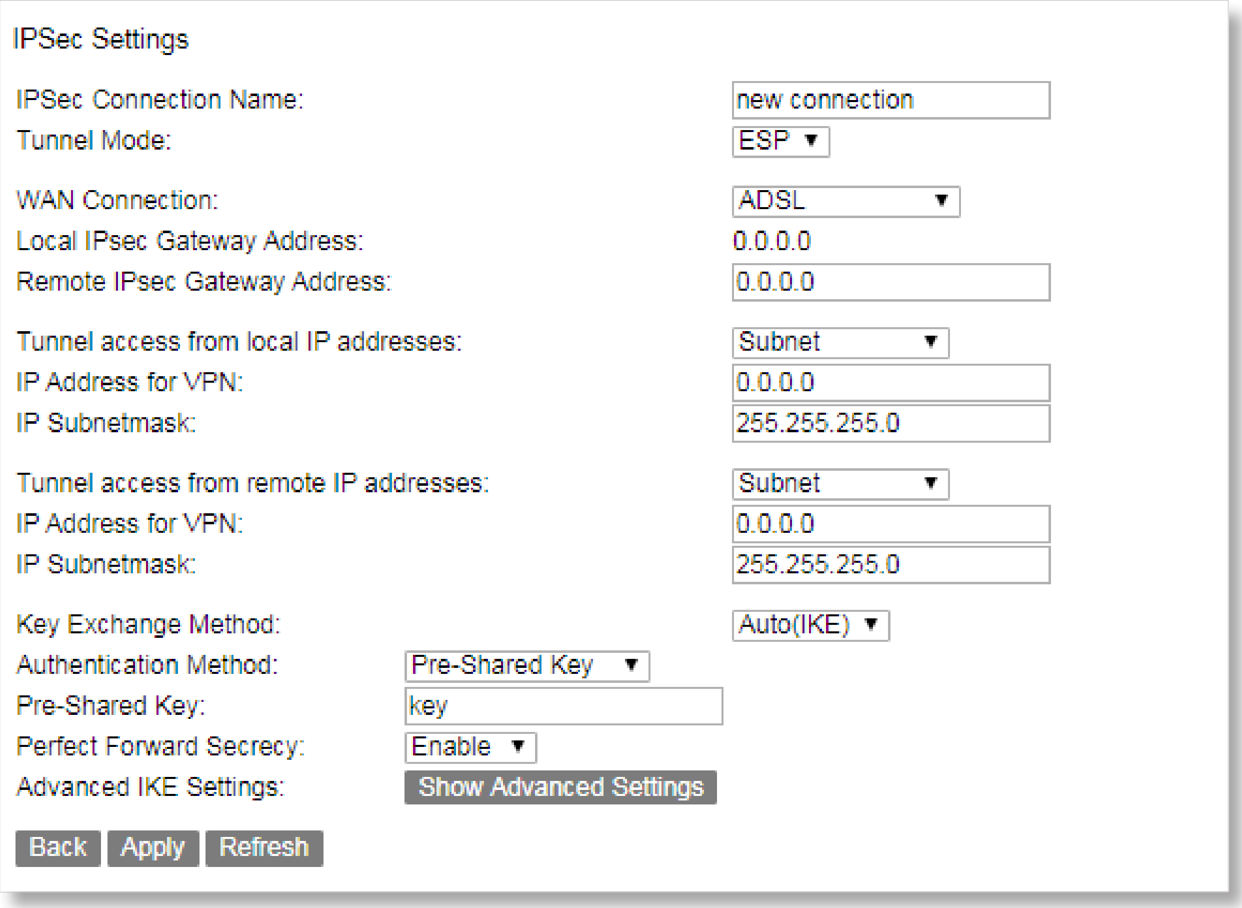


IPSec Tunnel Mode Connections

IPSec Hardware Accelerate ☑

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Status	Action
No Rule Found!					

Click **Add** to create a new connection.



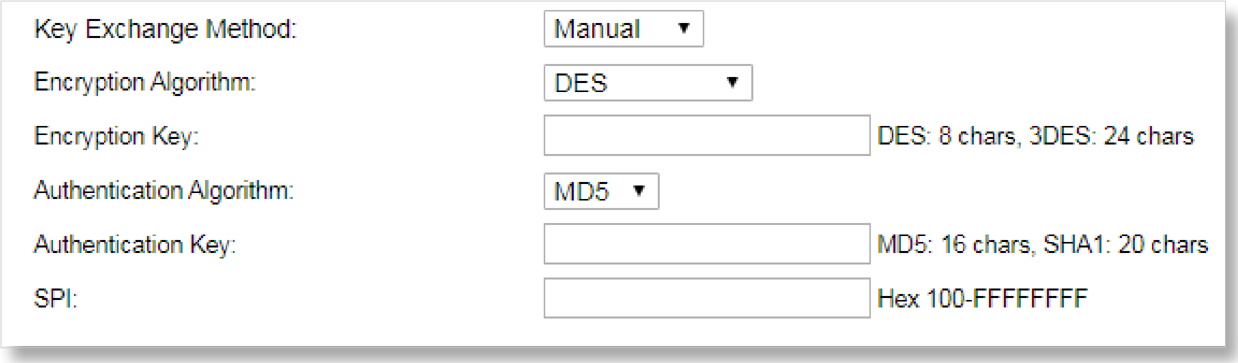
IPSec Settings

IPSec Connection Name:	new connection
Tunnel Mode:	ESP ▾
WAN Connection:	ADSL ▾
Local IPsec Gateway Address:	0.0.0.0
Remote IPsec Gateway Address:	0.0.0.0
Tunnel access from local IP addresses:	Subnet ▾
IP Address for VPN:	0.0.0.0
IP Subnetmask:	255.255.255.0
Tunnel access from remote IP addresses:	Subnet ▾
IP Address for VPN:	0.0.0.0
IP Subnetmask:	255.255.255.0
Key Exchange Method:	Auto(IKE) ▾
Authentication Method:	Pre-Shared Key ▾
Pre-Shared Key:	key
Perfect Forward Secrecy:	Enable ▾
Advanced IKE Settings:	Show Advanced Settings

Parameter	Description
IPSec Connection Name	It specifies a name for the IPSec connection.
Tunnel Mode	It specifies tunnel protocol the rule uses. ESP: It specifies Encapsulating Security Payload. This protocol is used to test data integrity and encryption. Even the encrypted packet is intercepted, the third party also cannot obtain correct message. AH: It specifies Authentication Header. This protocol is used to test data integrity. If a packet is tampered during transmission, the receiver discards the packet when it performs data integrity test.
Local Gateway Interface	Select a WAN service for the rule.
Remote IPSec Gateway Address	It specifies the WAN IP address or domain name of the peer device enabled IPSec function.
Tunnel access from local IP addresses	Subnet: When Subnet is selected, you can specify any network address on LAN and the corresponding subnet mask.
IP Address for VPN	It specifies the IP address of a local host.
Mask or Prefix Length	It specifies the subnet mask of the LAN you specified in IP Address for VPN.
Tunnel access from remote IP addresses	**Subnet:** When Subnet is selected, you can specify all hosts on the peer network. **Single Address:** When Single Address is selected, you can only specify one host on the peer network.
IP Address for VPN	It specifies IP address of a host on peer network.
Mask or Prefix Length	It specifies LAN IP network segment of the peer router.
Key Exchange Method	It specifies the key negotiation method. **Auto(IKE):** When Auto(IKE) is selected, the negotiation process is divided into two stages: **Stage 1:** Both communication sides exchange verification algorithm, encryption algorithm and so on security protocols, and establish an ISAKMP (Internet Security Association and Key Management Protocol) SA (Security Association) which is used to exchange more information in stage 2. **Stage 2:** Both communication sides take ISAKMP SA as IPSec security protocol parameters, and create IPSec SA which is used to secure data transmission. Manual: Refer to Key Exchange Method-Manual.

Key Exchange Method-Manual

When **Manual** is selected, the following parameters appear.

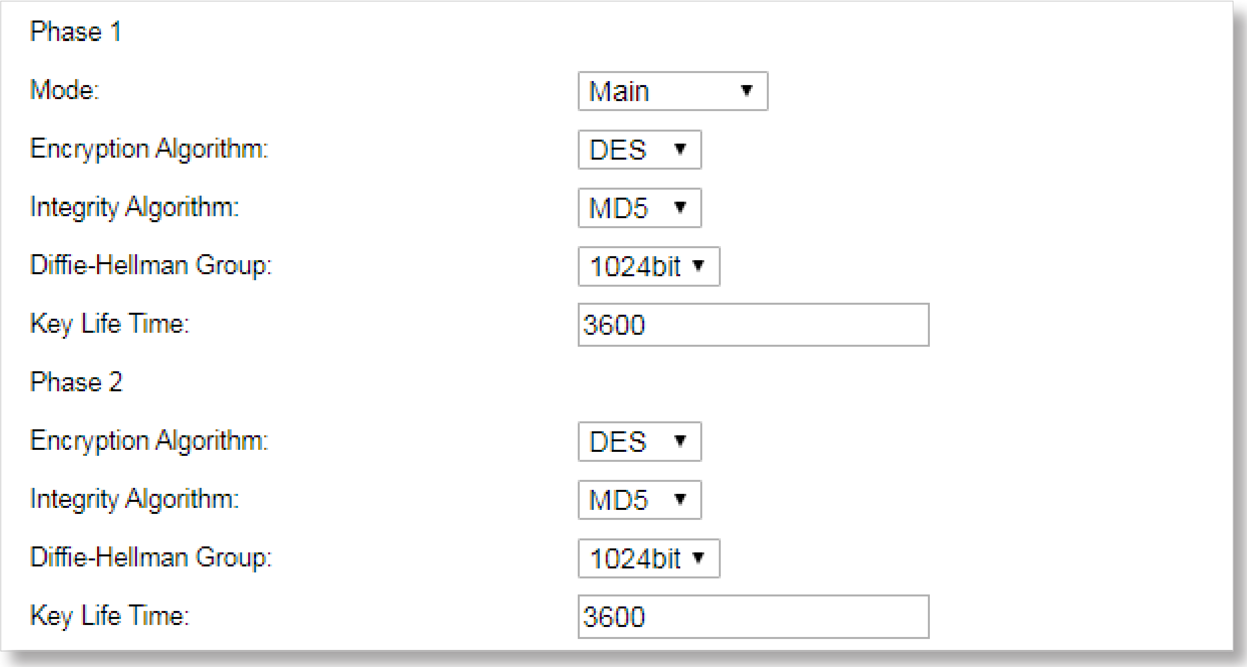


Key Exchange Method:	Manual ▼	
Encryption Algorithm:	DES ▼	
Encryption Key:		DES: 8 chars, 3DES: 24 chars
Authentication Algorithm:	MD5 ▼	
Authentication Key:		MD5: 16 chars, SHA1: 20 chars
SPI:		Hex 100-FFFFFFFF

Parameter	Description
Encryption Algorithm	When the Tunnel Mode is set to ESP, you can configure ESP encryption algorithm. The modem router supports the following encryption algorithm: DES: It specifies Data Encryption Standard. 3DES: It specifies Triple DES. AES(aes-cbc): It specifies Advanced Encryption Standard
Encryption Key	It specifies an encryption key. Both communication sides should set it to the same one.
Authenticatio Algorithm	When the Tunnel Mode is set to AH, you can configure AH authentication algorithm. The modem router supports the following authentication algorithm: MD5: It specifies Message Digest Algorithm. The system generates a 128 bit message digest for a message. SHA1: It specifies Secure Hash Algorithm. The system generates a 128 bit message digest for a message.
Authentication Key	It specifies an authentication key. Both communication sides should set it to the same one.
SPI	It specifies Security Parameter Index. It is an identification tag added to the header while using IPsec for tunneling the IP traffic. This tag helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use.

Advanced IKE Settings

When the Show Advanced Settings button is clicked, the following parameters appear.



Phase 1

Mode: Main

Encryption Algorithm: DES

Integrity Algorithm: MD5

Diffie-Hellman Group: 1024bit

Key Life Time: 3600

Phase 2

Encryption Algorithm: DES

Integrity Algorithm: MD5

Diffie-Hellman Group: 1024bit

Key Life Time: 3600

Parameter	Description
Mode	The mode should be set to the same one as that of the peer device. Main: This mode provides identity protection, and is applicable to high requirement situation for identity protection. Aggressive: This mode does not provide identity protection, and is applicable to not high requirement situation for identity protection.
Encryption Algorithm	DES: It specifies Data Encryption Standard. 3DES: It specifies Triple DES. AES: It specifies Advanced Encryption Standard. AES - 128/192/256 indicates that the key length is 128/192/256 bit.
Integrity Algorithm	MD5: It specifies Message Digest Algorithm. The system generates a 128 bit message digest for a message. SHA1: It specifies Secure Hash Algorithm. The system generates a 128 bit message digest for a message.
Diffie-Hellman Group	It specifies the group information of Diffie-Hellman algorithm. It is used to generate session key encrypted IKE tunnel.
Key Life Time	It specifies the life time of IPSec SA.

Configuring the IPSec function as below

Step 1 Go to **Application > VPN > IPSec** page. And click **Add**.

Step 2 Enter an IPSec connection name, which is IPSec_1 in this example.

Step 3 Select a local gateway interface, which is **EWAN Dynamic** in this example.

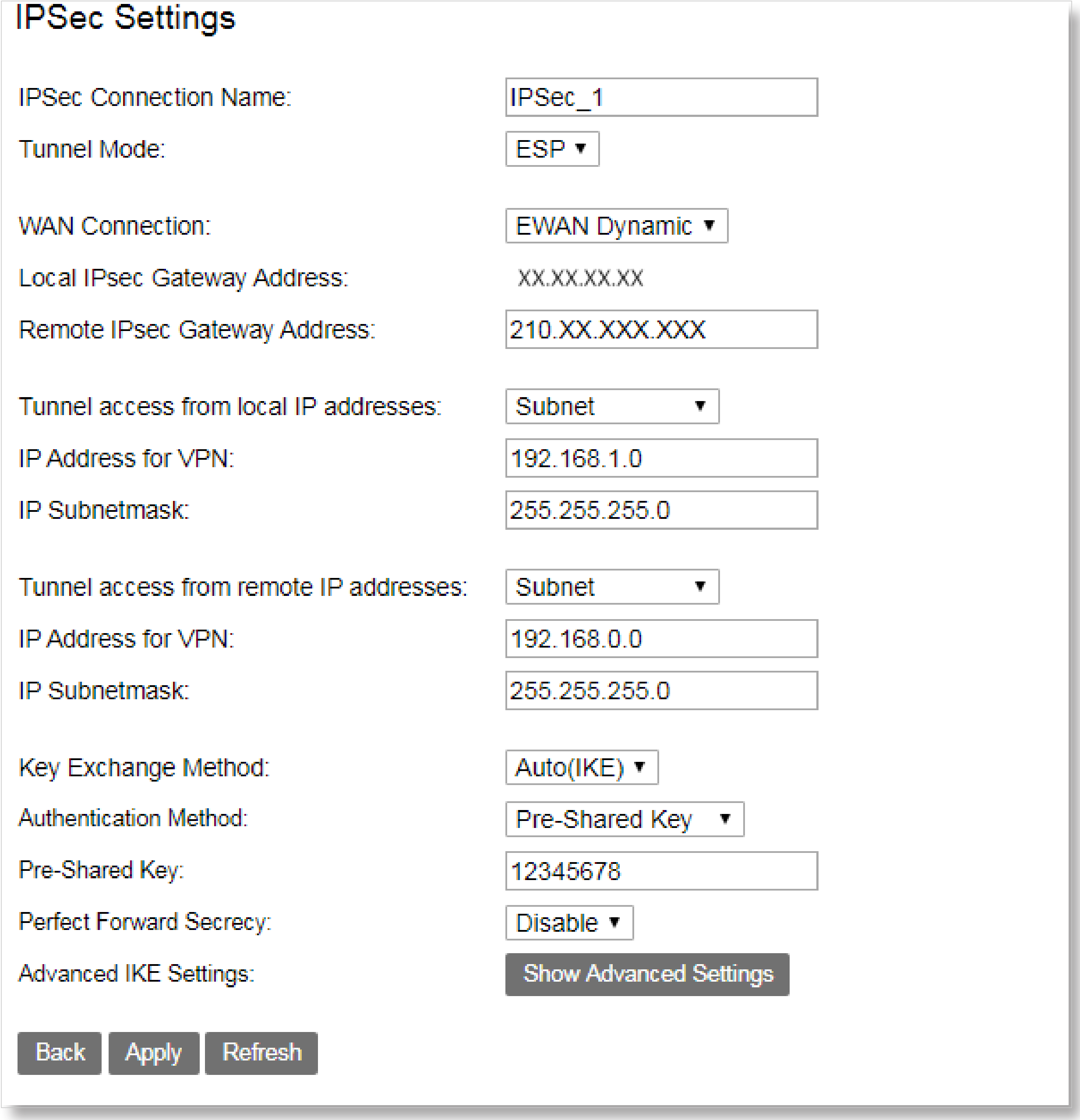
Step 4 Enter a remote IPSec gateway address, which is 210.XX.XXX.XXX in this example.

Step 5 Set Tunnel access from local IP address to Subnet.

Step 6 Set Tunnel access from remote IP address to Subnet, and set a local network segment of the peer router which is 192.168.0.0 and 255.255.255.0 in this example.

Step 7 Enter a Pre-Shared key which is 12345678 in this example. And leave other parameters unchanged.

Step 8 Click **Apply**.



IPSec Settings

IPSec Connection Name:	IPSec_1
Tunnel Mode:	ESP ▼
WAN Connection:	EWAN Dynamic ▼
Local IPsec Gateway Address:	XX.XX.XX.XX
Remote IPsec Gateway Address:	210.XX.XXX.XXX
Tunnel access from local IP addresses:	Subnet ▼
IP Address for VPN:	192.168.1.0
IP Subnetmask:	255.255.255.0
Tunnel access from remote IP addresses:	Subnet ▼
IP Address for VPN:	192.168.0.0
IP Subnetmask:	255.255.255.0
Key Exchange Method:	Auto(IKE) ▼
Authentication Method:	Pre-Shared Key ▼
Pre-Shared Key:	12345678
Perfect Forward Secrecy:	Disable ▼
Advanced IKE Settings:	Show Advanced Settings

Chapter 6

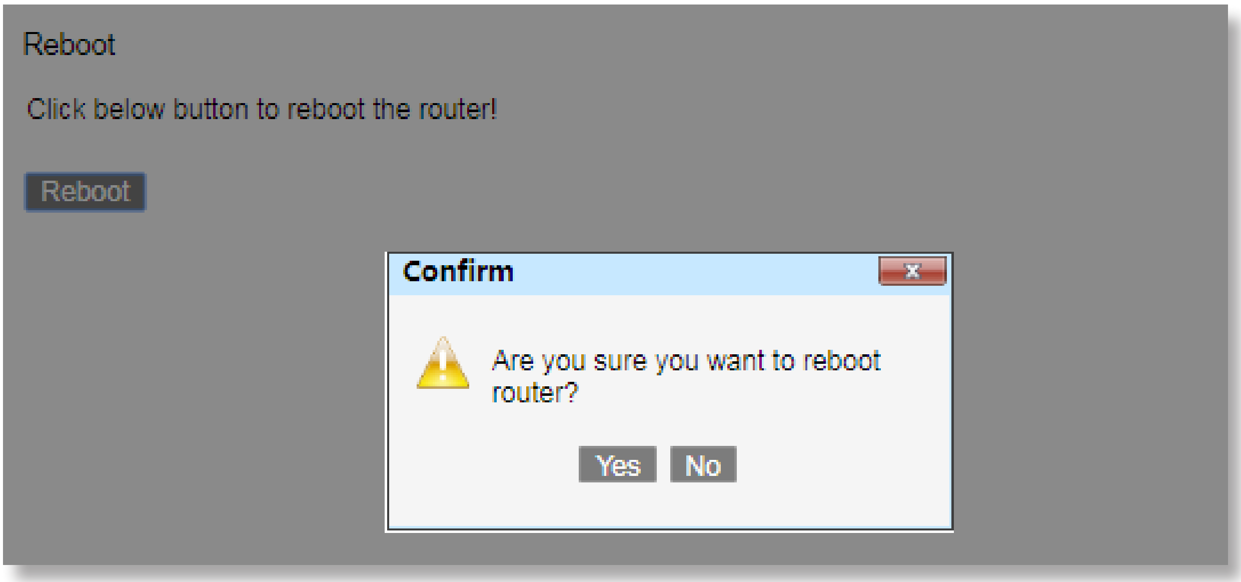
Management

This Chapter describes about management of web UI.
It contains the following sections:

6.1 Reboot

This function allows you to manually reboot the device on the web UI.

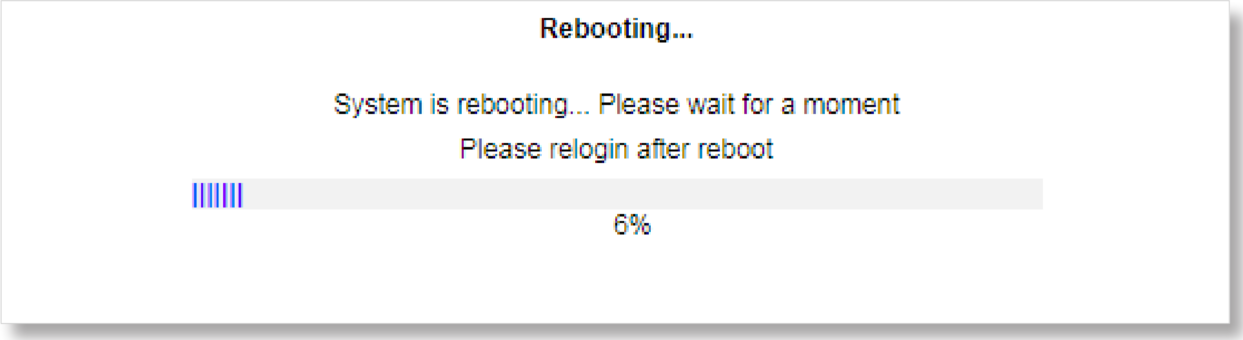
Step 1 Go to **Management > Reboot** page.
Step 2 Click **Reboot**.
Step 3 Click **Yes**. And then wait for the modem router to restart.



Reboot

Click below button to reboot the router!

Are you sure you want to reboot router?



Rebooting...

System is rebooting... Please wait for a moment

Please relogin after reboot

6%

6.2 Settings

Here you can back up the current settings, restore earlier settings, and restore the factory settings of the device.

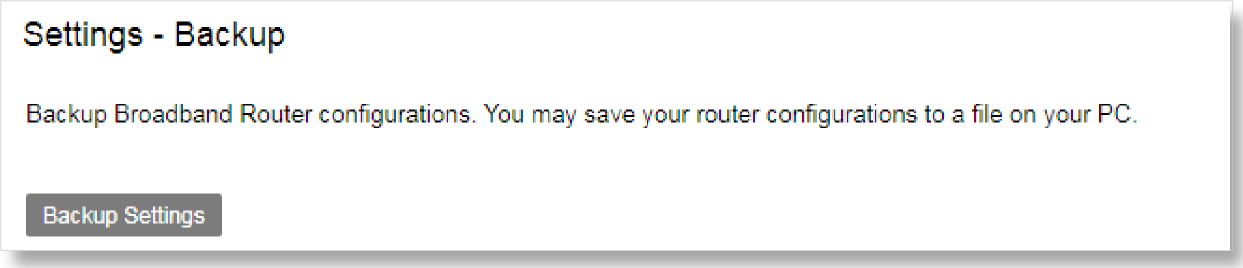
6.2.1 Backup

This function allows you to save a copy of your device’s configurations to your computer. Once you have configured the device, you can save these settings to a configuration file on your local computer. The configuration file can later be imported to your device in case the device is reset.

To Back up the settings

Step 1 Choose **Management > Settings > Backup** page.

Step 2 Click **Backup Settings**.

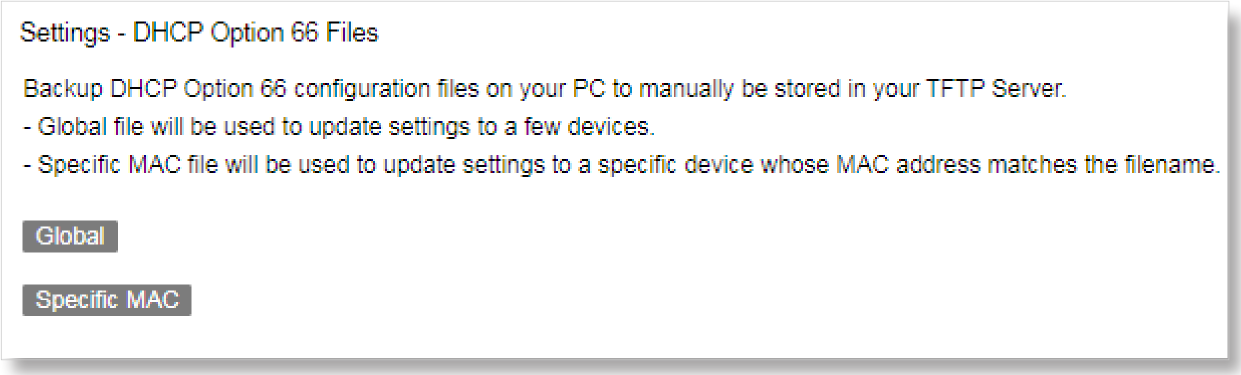


Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

6.2.2 DHCP Option 66 files

Choose **Management > Settings > DHCP Option 66 Files** page.
Backup DHCP Option 66 configuration files on your PC to manually be stored in your TFTP Server.
- Global file will be used to update settings to a few devices.
- Specific MAC file will be used to update settings to a specific device whose MAC address matches the filename.



Settings - DHCP Option 66 Files

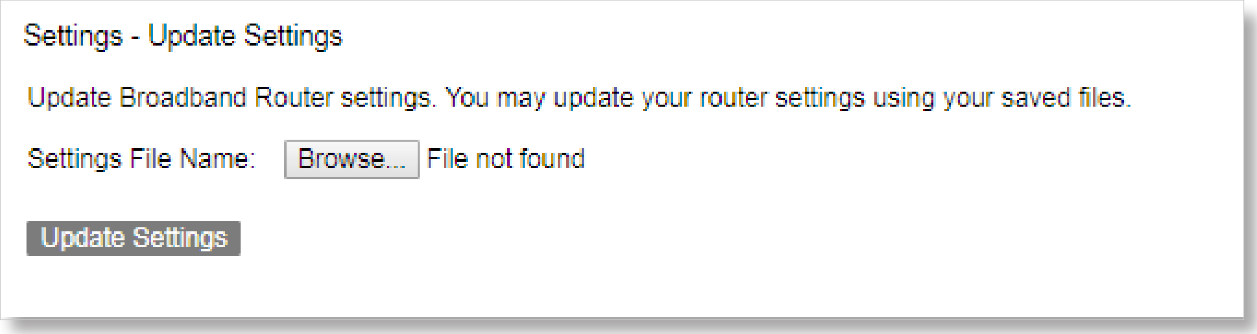
Backup DHCP Option 66 configuration files on your PC to manually be stored in your TFTP Server.
- Global file will be used to update settings to a few devices.
- Specific MAC file will be used to update settings to a specific device whose MAC address matches the filename.

6.2.3 Update

Here you may update your router settings using your saved files.

Choose **Management > Settings > Update** page, and click **Browse** to find out the saved files.

Then click **Update Settings**.



Settings - Update Settings

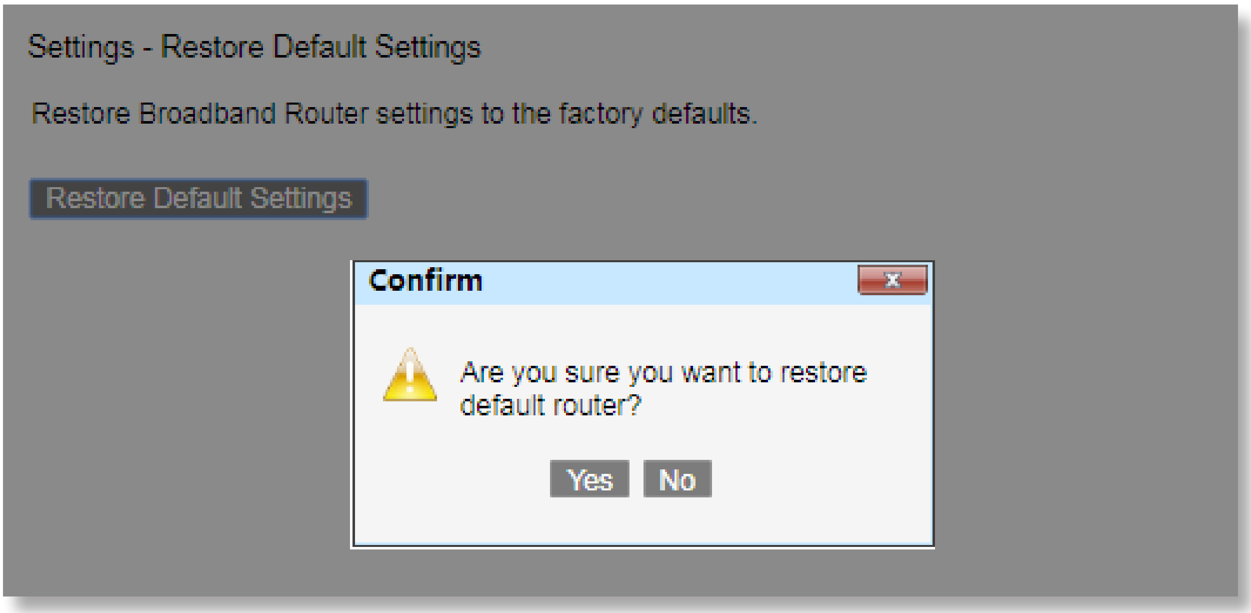
Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name: File not found

6.2.4 Restore Default

Here you may restore your router settings to the factory defaults.

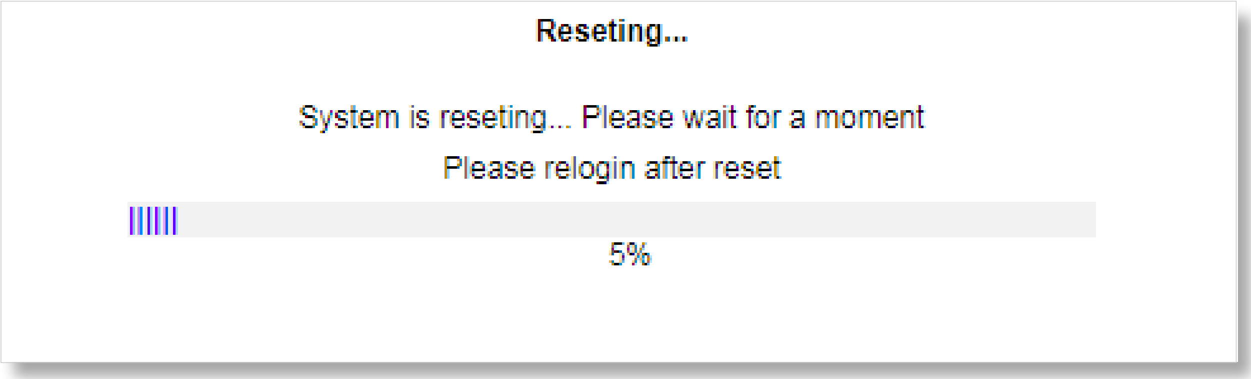
Choose **Management > Settings > Restore Default** page, and click **Restore Default Settings.**



Settings - Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Are you sure you want to restore default router?



Reseting...

System is reseting... Please wait for a moment

Please relogin after reset

5%

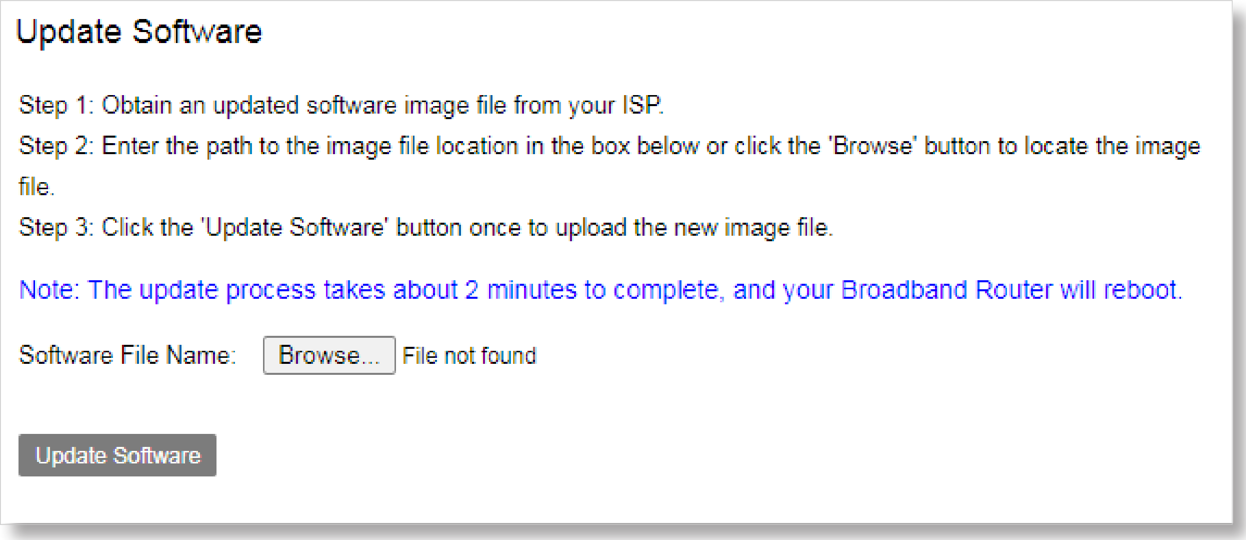
6.2.5 Update Software

Here you may update your router software.

Choose **Management > Settings > Update Software** page, and click **Browse** to locate the updated software files.

Then click **Update Settings**.

Note: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.



Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.

Step 3: Click the 'Update Software' button once to upload the new image file.

Note: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Software File Name: Browse... File not found

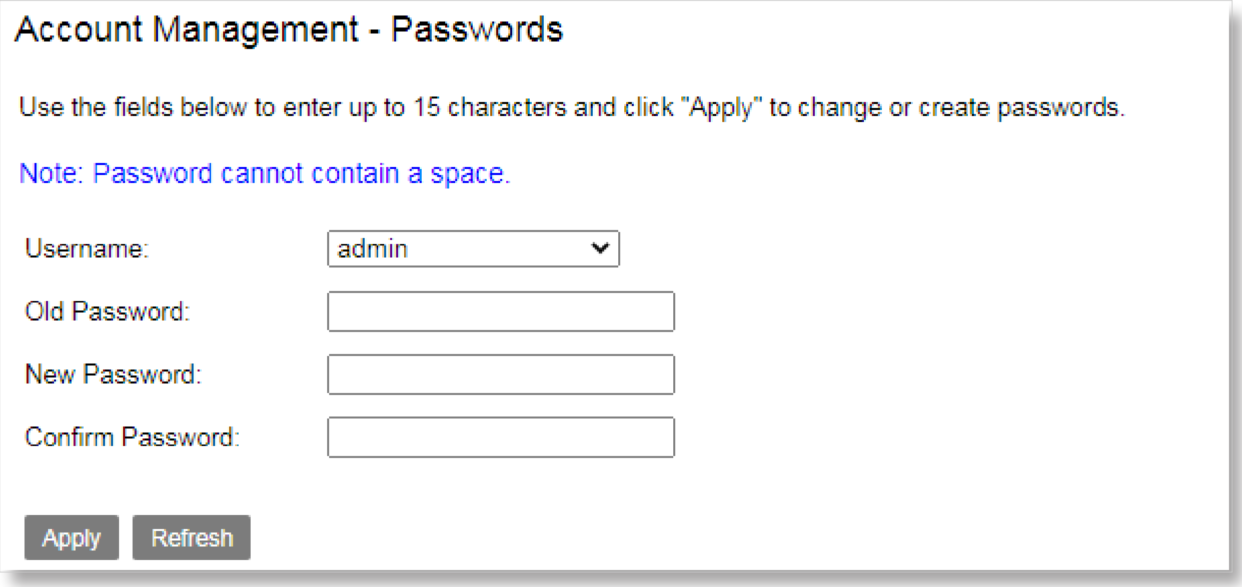
6.3 Account Management

Here you may change the loging password.

Choose **Management > Account Management > Passwords** page.

Enter the old password and set a new password.

Then click **Apply**.



Account Management - Passwords

Use the fields below to enter up to 15 characters and click "Apply" to change or create passwords.

Note: Password cannot contain a space.

Username:	admin
Old Password:	
New Password:	
Confirm Password:	

6.4 Logs

This function allows you to configure, view, and export system logs, which helps you understand the operating conditions of the device.

6.4.1 Log level

Here you may configure system logs.

Step 1 Choose **Management > Log > Log level** page.

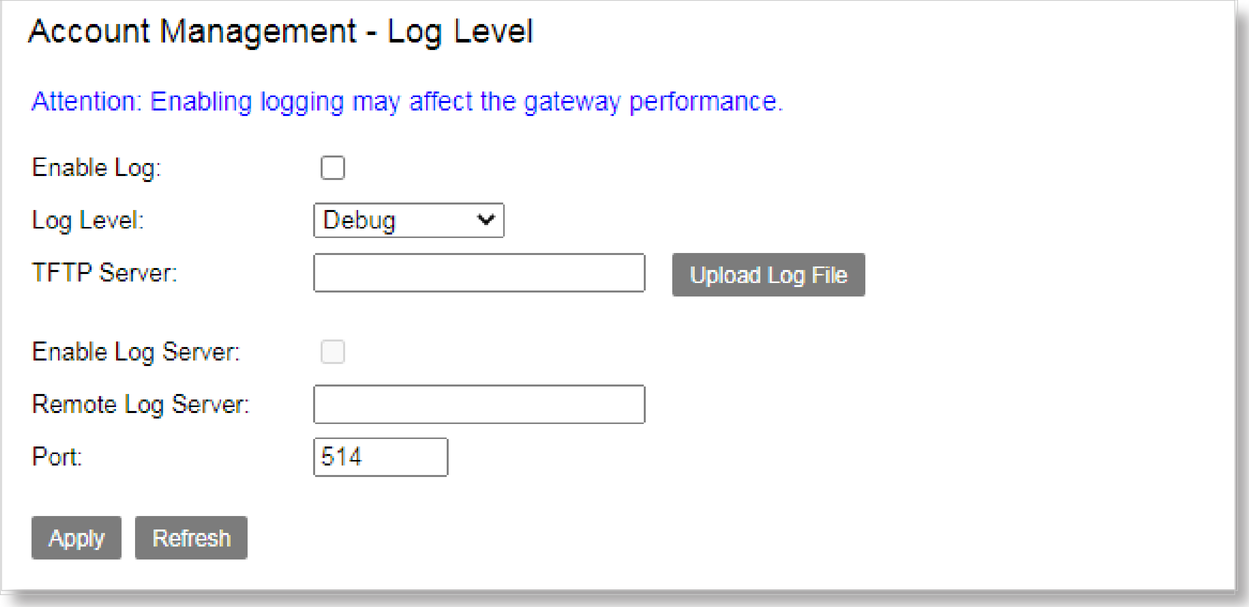
Step 2 Check the **Enable Log** box.

Step 3 Select a log level from the Log Level drop-down list box. All the system events at or above the selected level are logged.

Step 4 **Enable Log Server** option.

Step 5 Set **Remote Log Server** and the specified **Port**.

Step 6 Click **Apply**.



Account Management - Log Level

Attention: Enabling logging may affect the gateway performance.

Enable Log: □

Log Level: Debug

TFTP Server:

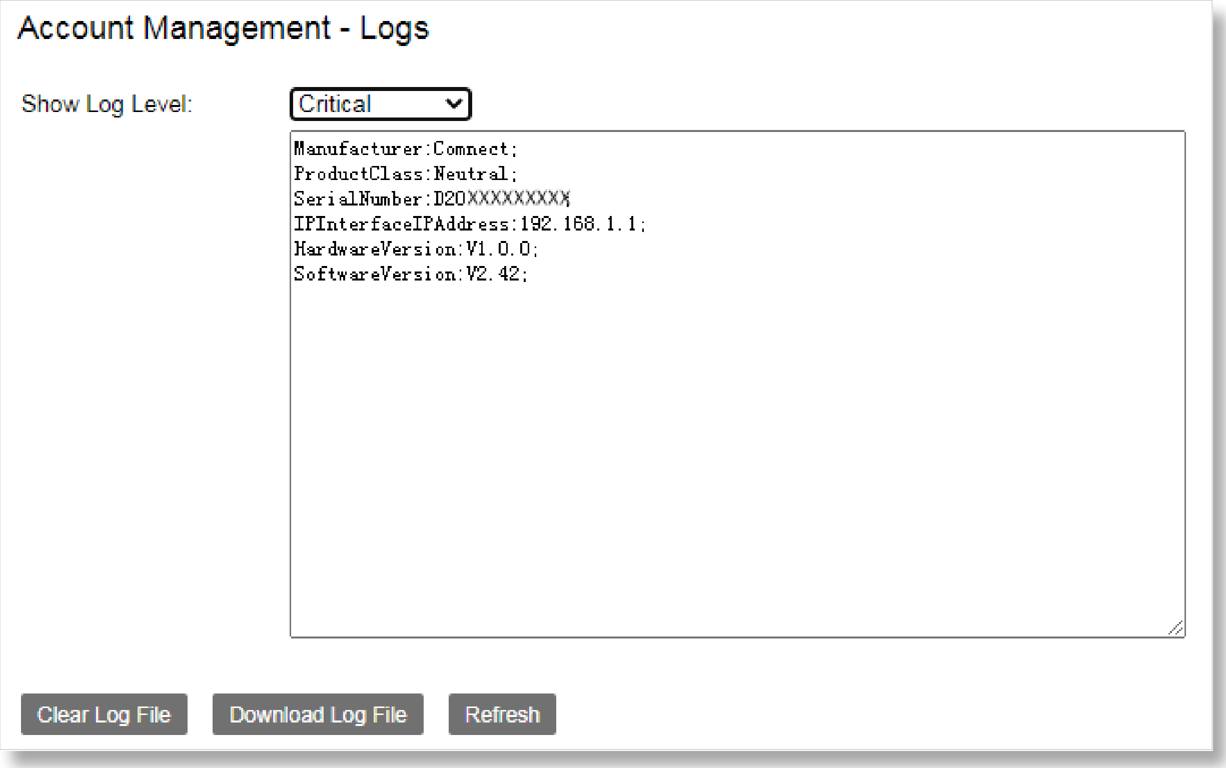
Enable Log Server: □

Remote Log Server:

Port: 514

6.4.2 Logs

Here you may clear or download log file.



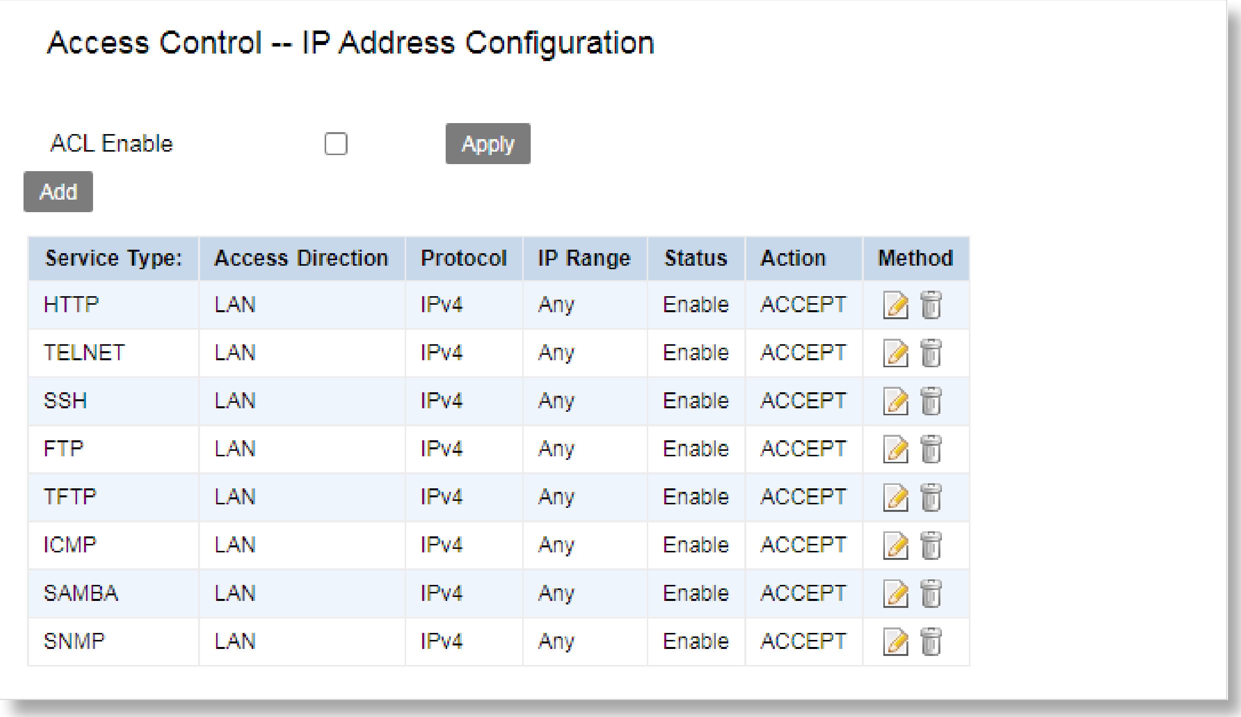
Account Management - Logs

Show Log Level: Critical

```
Manufacturer:Connect;
ProductClass:Neutral;
SerialNumber:D20XXXXXXXXX
IPInterfaceIPAddress:192.168.1.1;
HardwareVersion:V1.0.0;
SoftwareVersion:V2.42;
```

6.5 Service Control

This function allows you to use the HTTP, TELNET, SSH, FTP, TFTP, ICMP, SAMBA and SNMP to manage the modem router from LAN or WAN side.
Choose **Management > Service Control** to enter the configuration page.



Access Control -- IP Address Configuration

ACL Enable □

Service Type:	Access Direction	Protocol	IP Range	Status	Action	Method
HTTP	LAN	IPv4	Any	Enable	ACCEPT	
TELNET	LAN	IPv4	Any	Enable	ACCEPT	
SSH	LAN	IPv4	Any	Enable	ACCEPT	
FTP	LAN	IPv4	Any	Enable	ACCEPT	
TFTP	LAN	IPv4	Any	Enable	ACCEPT	
ICMP	LAN	IPv4	Any	Enable	ACCEPT	
SAMBA	LAN	IPv4	Any	Enable	ACCEPT	
SNMP	LAN	IPv4	Any	Enable	ACCEPT	

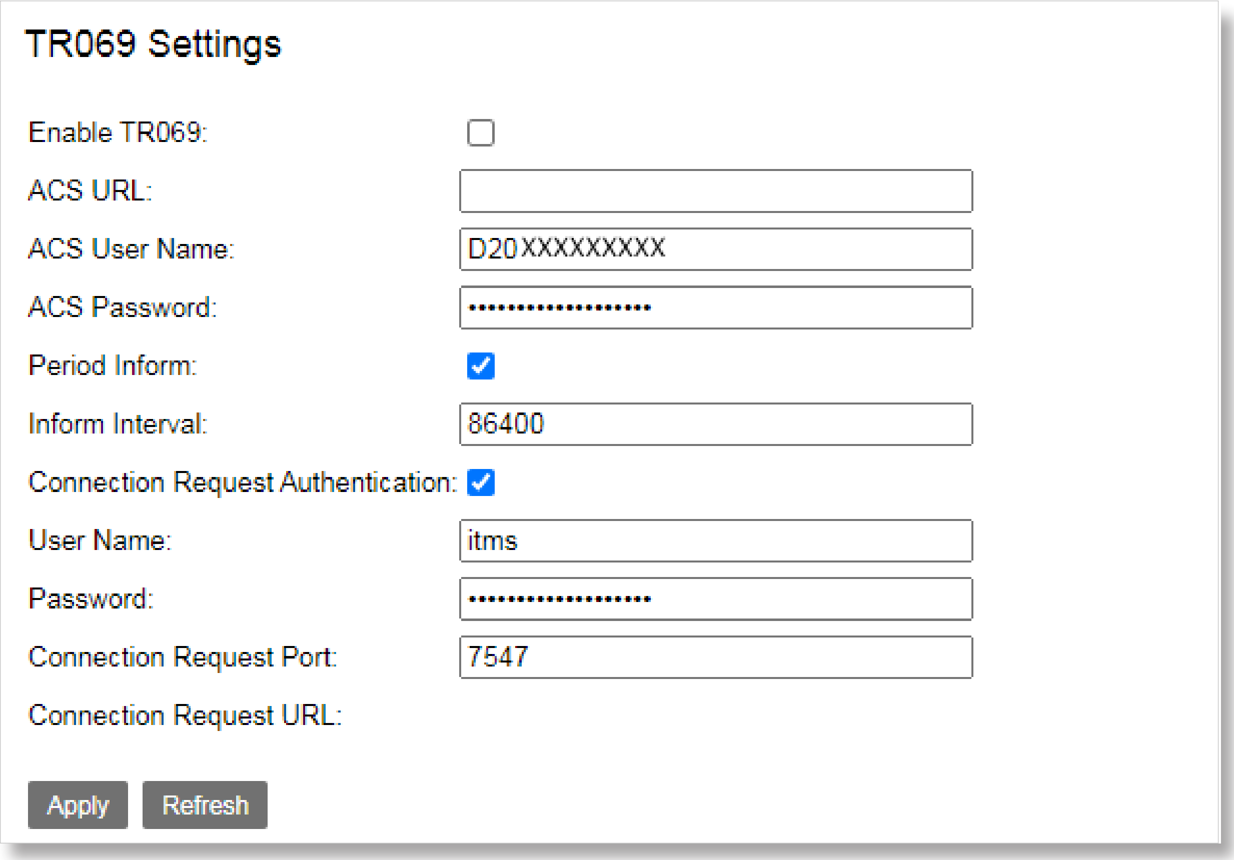
Parameter	Description
HTTP	After it is enabled, users can manage the modem router using HTTP protocol through the browser from the corresponding sides (LAN or WAN). This method is acceptable for most users.
TELNET	After it is enabled, users can use TELNET to establish a connection with the device, and visit the command-line interface of the device from the corresponding sides (LAN or WAN).
SSH	After it is enabled, users can manage the modem router through the Secure Shell connection (SSH).
FTP	After it is enabled, the modem router servers as a server and users can use FTP protocol to check, upload, or download files of the device from the corresponding sides (LAN or WAN).
TFTP	After it is enabled, the devise servers as a server and users can use TFTP protocol to check, upload, or download files of the device from the corresponding sides (LAN or WAN).
IGMP	After it is enabled, it allows users to ping the modem router from the corresponding sides (LAN or WAN) for connectivity diagnosis.

SNMP	After it is enabled, the SNMP management software can establish a connection with the device, and check some parameters of the device through MIB nodes from the corresponding sides (LAN or WAN).

6.6 CWMP

The WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to the modem router from the internet. This function allows you to manage the modem router remotely.

Choose **Management > CWMP** to enter the configuration page.



TR069 Settings

Enable TR069:	□
ACS URL:	
ACS User Name:	D20XXXXXXXXX
ACS Password:	•••••••••••••••••••
Period Inform:	☑
Inform Interval:	86400
Connection Request Authentication:	☑
User Name:	itms
Password:	•••••••••••••••••••
Connection Request Port:	7547
Connection Request URL:	

Parameter	Description
ACS URL	It specifies the domain name of the ACS
ACS User Name	It specifies the user name used to authenticate the CPE when the CPE connects to the ACS using the TR-069 protocol.
ACS Password	It specifies the password used to authenticate the CPE when the CPE connects to the ACS using the TR-069 protocol.
Inform Interval	It specifies the interval at which the CPE uses the inform method to send messages to the ACS.
Connection Request Authentication	It specifies whether to authenticate the connection request sent by the ACS.
User Name	It specifies the user name used to authenticate the ACS when it sends the connection request to the CPE.
Password	It specifies the password used to authenticate the ACS when it sends the connection request to the CPE.
Connection Request URL	It specifies the domain name used by the ACS when it sends the connection request to the CPE. After the WAN port used by the TR-069 client is selected, this domain name will be generated automatically.

To configure the TR069 settings

Step 1 Go to **Management > CWMP** page.

Step 2 Check **Enable TR069** box.

Step 3 Set ACS User Name to the user name of the ACS .

Step 4 Set ACS Password to the password of the ACS.

Step 5 Check the **Period Inform** box.

Step 6 Set Inform Interval to the interval at which inform packets are sent.

Step 7 Select **Connection Request Authentication** if connection request authentication is required. If it is selected, perform the following steps:

1. Set **User Name** to the user name for connection request authentication.
2. Set **Password** to the password for connection request authentication.
3. The **Connection Request URL** will be automatically generated after the WAN interface used by the TR-069 client is selected.

Step 8 Click **Apply**.

6.7 Internet Time

This function allows you to synchronize the time of the device with the internet time.

To synchronize the system time with the internet

Step 1 Go to **Management > Internet Time** page.

Step 2 Check **Time Service Enable** box.

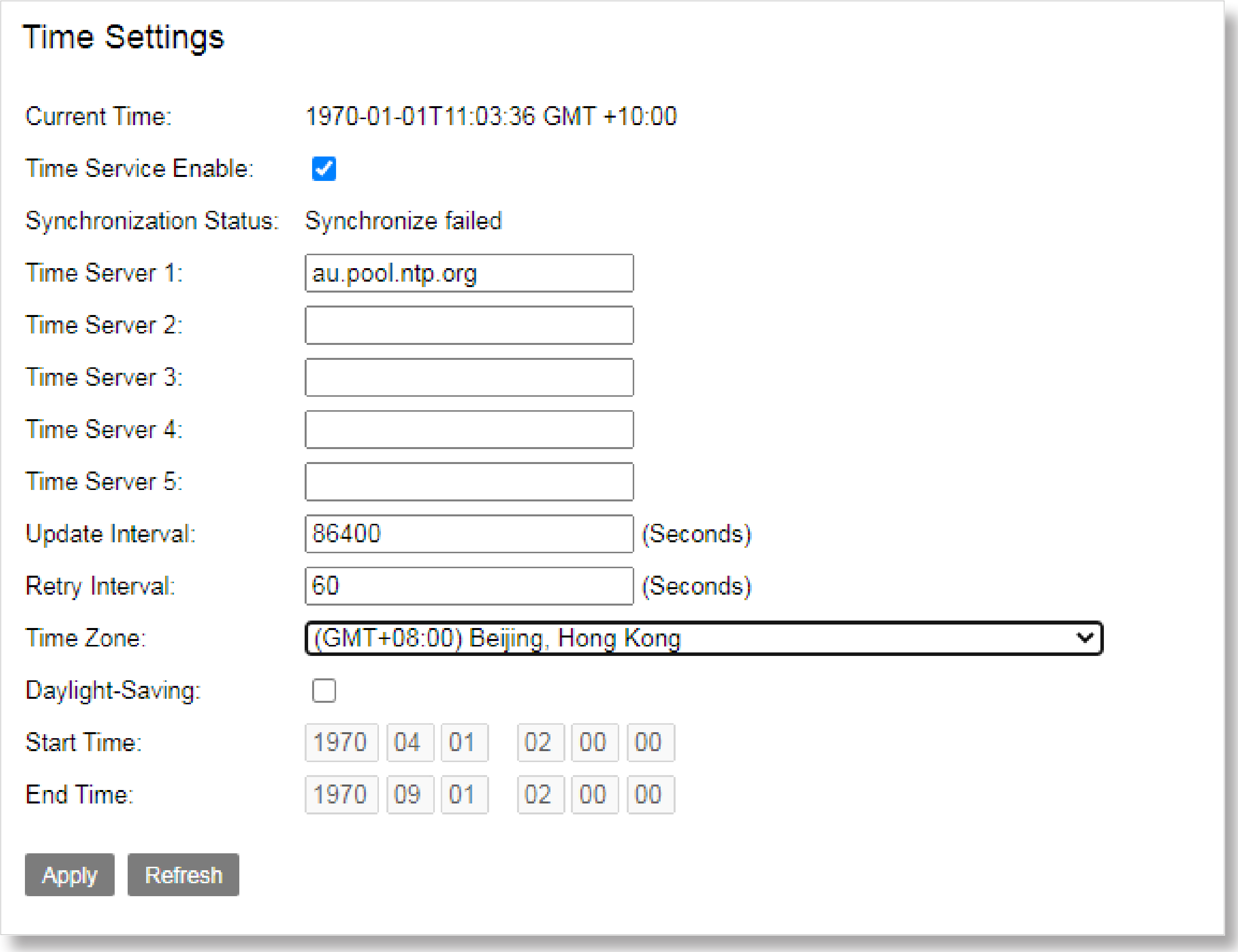
Step 3 Set First/Second/Third/Fourth/Fifth NTP time server to the first/second/third/fourth/fifth time server with which the device time is synchronized.

Step 4 Select your time zone from the **Time Zone** drop-down list box.

Step 5 If your country or region has daylight saving time, select the **Daylight-Saving** option, and

set the **Start Time** and **End Time**.

Step 6 Click **Apply**.



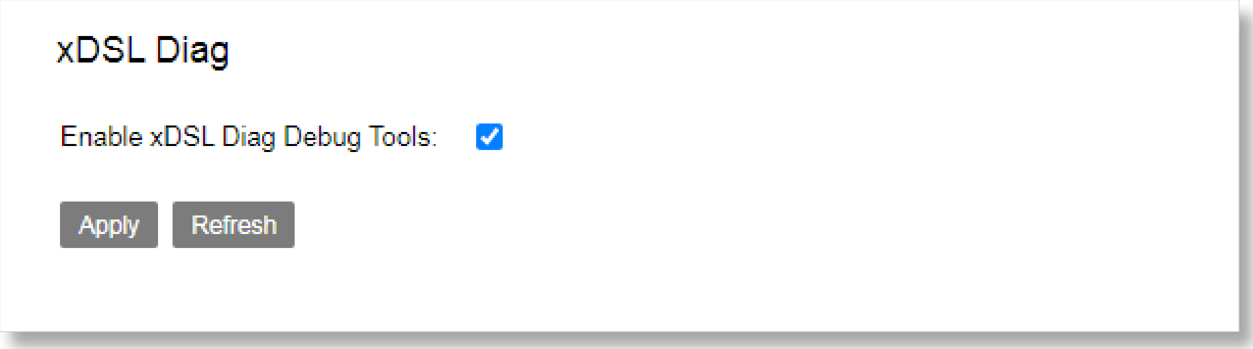
Time Settings

Current Time:	1970-01-01T11:03:36 GMT +10:00
Time Service Enable:	☑
Synchronization Status:	Synchronize failed
Time Server 1:	au.pool.ntp.org
Time Server 2:	
Time Server 3:	
Time Server 4:	
Time Server 5:	
Update Interval:	86400 (Seconds)
Retry Interval:	60 (Seconds)
Time Zone:	(GMT+08:00) Beijing, Hong Kong
Daylight-Saving:	□
Start Time:	1970 04 01 02 00 00
End Time:	1970 09 01 02 00 00

6.8 xDSL Diag

This function allows you to debug this router. By default, it is disabled.

Go to **Management > xDSL Diag** page, check the box to enable this function when needed.



xDSL Diag

Enable xDSL Diag Debug Tools: ☑

6.9 Tools

6.9.1 Ping Route

Ping test can help test whether a host or the internet is reachable.

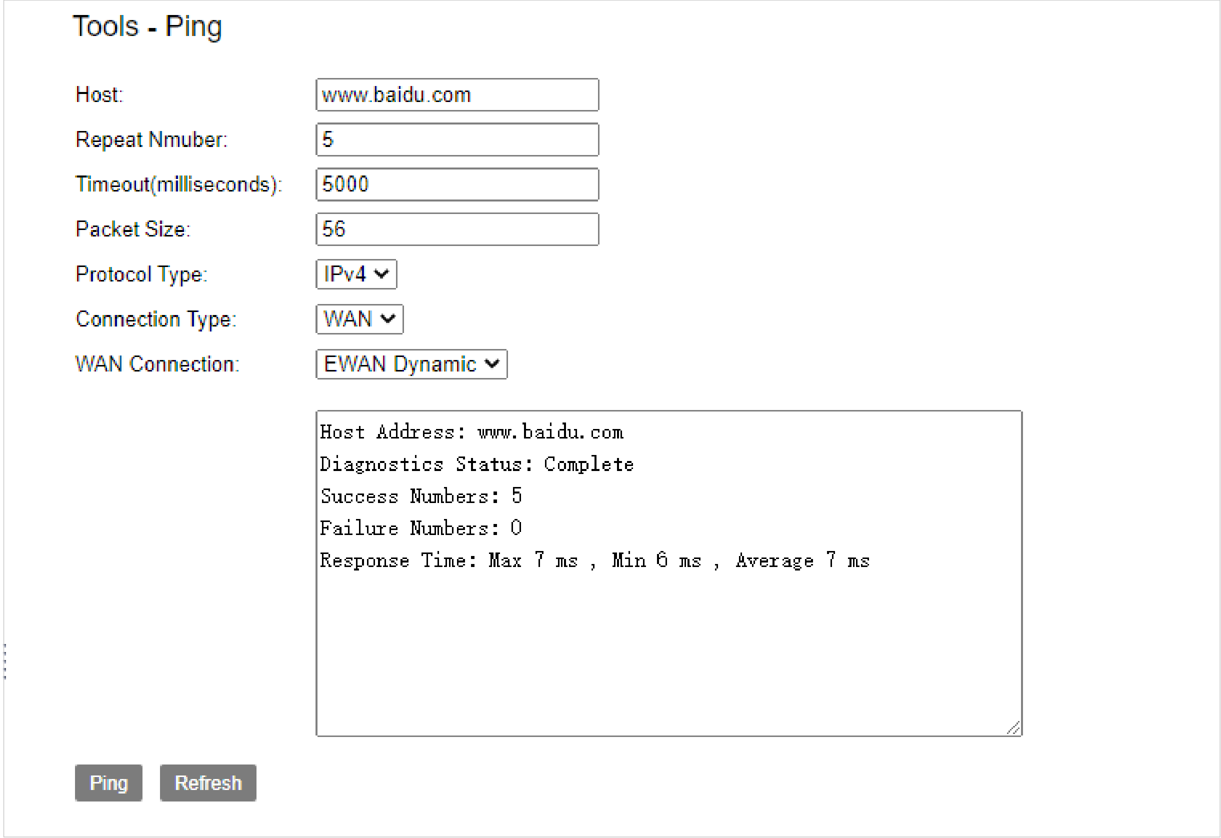
To perform the ping test:

Step 1 Go to **Management > Tools > Ping Route** page.

Step 2 Enter the IP address or domain name of the host in the **Host** field.

Step 3 Click **Ping**.

Note: If you get a similar screenshot shown as below, it indicates that the host is reachable from the modem router.



Tools - Ping

Host:	www.baidu.com
Repeat Nmuber:	5
Timeout(milliseconds):	5000
Packet Size:	56
Protocol Type:	IPv4
Connection Type:	WAN
WAN Connection:	EWAN Dynamic

```
Host Address: www.baidu.com
Diagnostics Status: Complete
Success Numbers: 5
Failure Numbers: 0
Response Time: Max 7 ms , Min 6 ms , Average 7 ms
```

6.9.2 Trace Route

Trace Route helps you check the specific routes to a host.

To perform the trace Route:

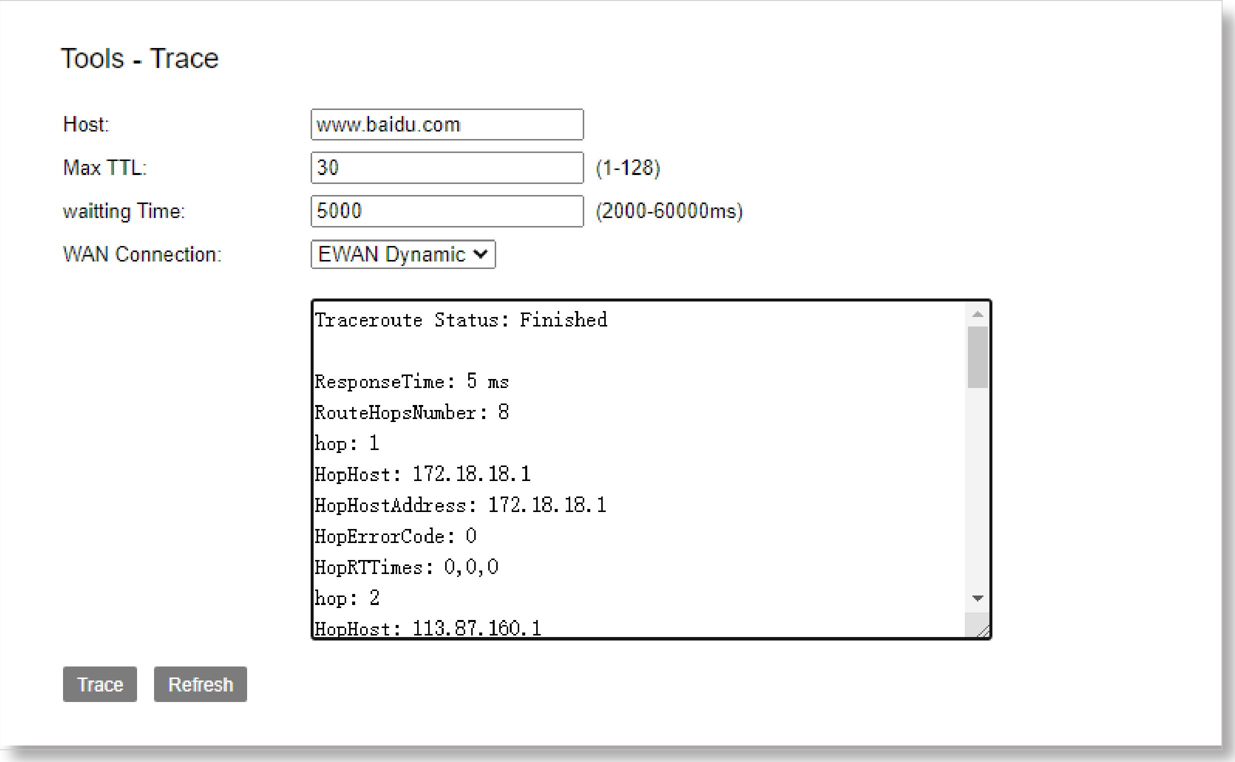
Step 1 Go to **Management > Tools > Trace Route** page.

Step 2 Enter the IP address or domain name of the host in the **Host** field.

Step 3 Choose your **WAN Connection**.

Step 4 Click **Trace**.

Note: Then you can check the result. The following route information is as a example.



Tools - Trace

Host: www.baidu.com

Max TTL: 30 (1-128)

waitting Time: 5000 (2000-60000ms)

WAN Connection: EWAN Dynamic

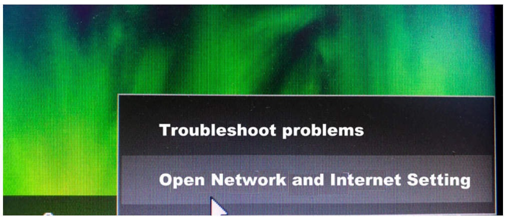
```
Traceroute Status: Finished

ResponseTime: 5 ms
RouteHopsNumber: 8
hop: 1
HopHost: 172.18.18.1
HopHostAddress: 172.18.18.1
HopErrorCode: 0
HopRTTimes: 0,0,0
hop: 2
HopHost: 113.87.160.1
```

FAQ

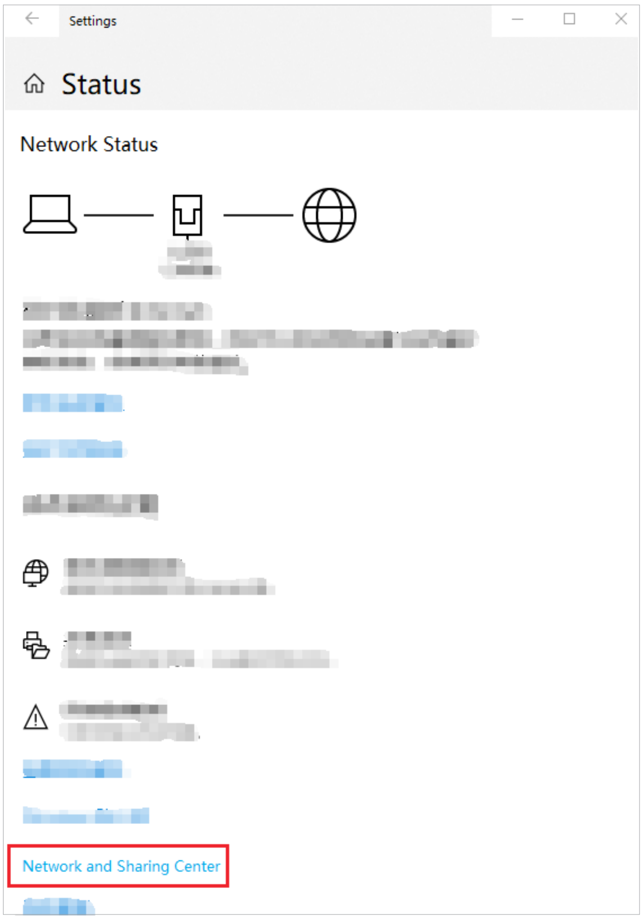
Q1: How to set up the TCP/IP Protocol in Obtain an IP address automatically mode on your computer?

A1: A computer installed with a wired network adapter is used as an example here to describe the steps in Win 10 and in similar steps for the other systems.

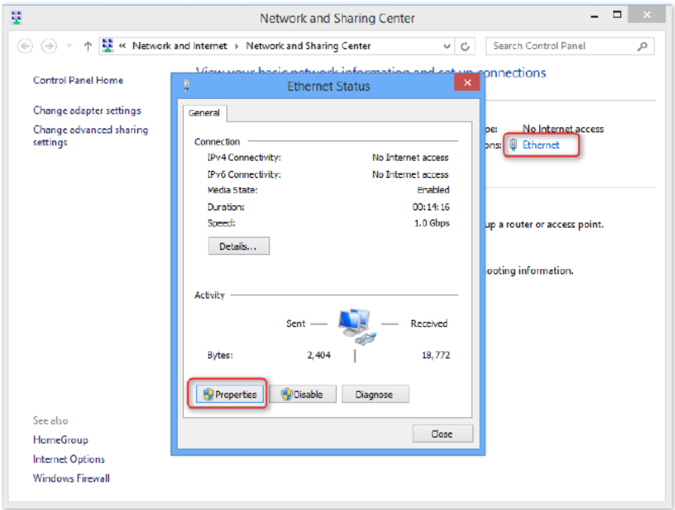
Step 1. Right-click 🖳 in the lower-right corner of the desktop and choose **Open Network and Internet Setting**.



Step 2. Click **Network and Sharing Center**.



Step 3. Click **Ethernet and Properties**.



Connection

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 00:14:16

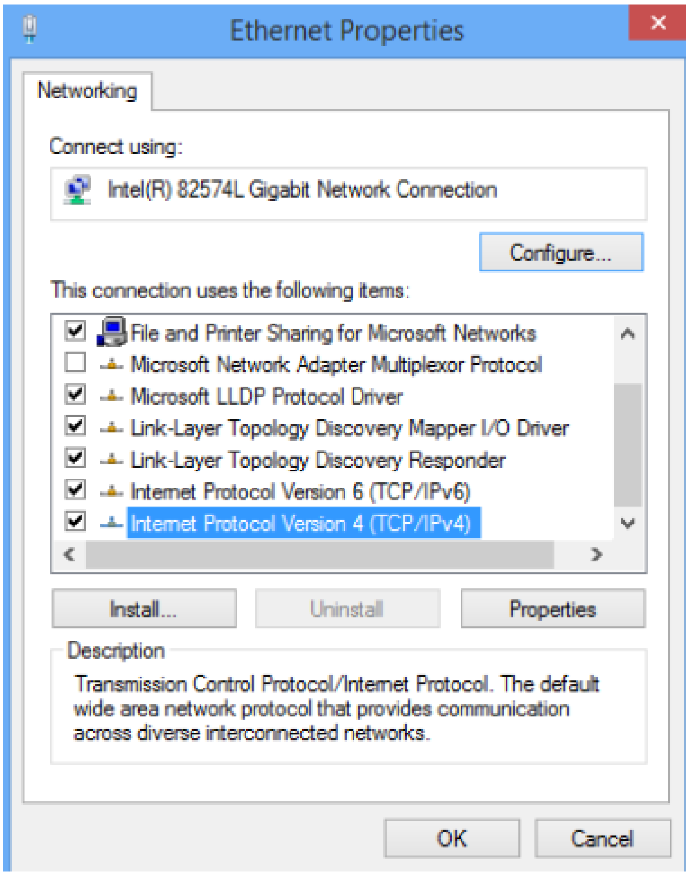
Speed: 1.0 Gbps

Activity

Sent — Received

Bytes: 2,404 | 18,772

Step 4. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Connect using:

Intel(R) 82574L Gigabit Network Connection

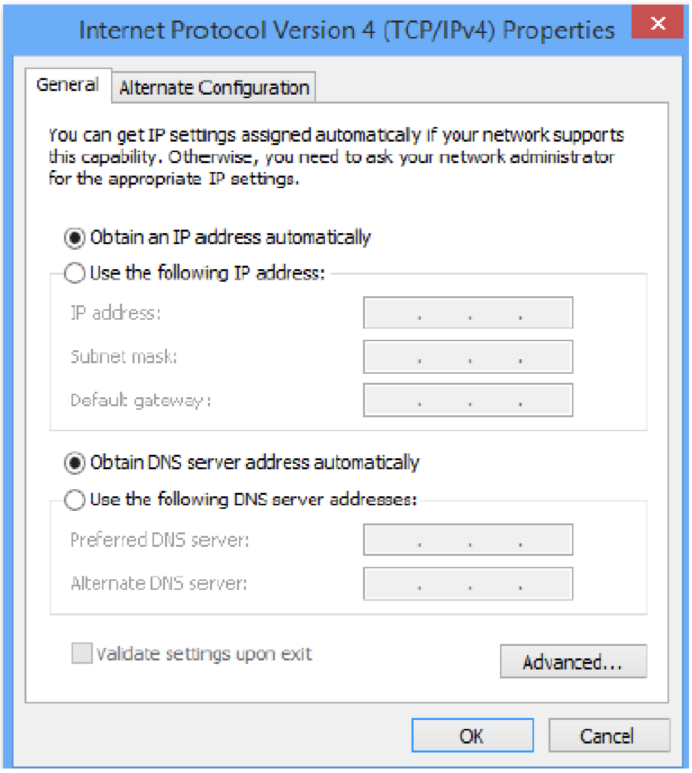
This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 5. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**, and click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Step 6. You'll go back to the **Enternet Properties** box, please click **OK**.

Q2: If I can't access the web UI of the router after entering 192.168.1.1, what should I do?

A2: Please try the following methods to log in again.

A2-1： Make sure the connection of DSL and LAN port(s) is correct.

Ensure that your Ethernet cable with internet connectivity is plugged into the DSL port of the router rather than a LAN port.

Ensure that your wireless device is connected to the LAN port(s) of the router.

A2-2: Make sure you enter the correct IP address(192.168.1.1) to log in.

A2-3: Make sure the IP address of your computer is configured as Obtain an IP address automatically and Obtain DNS server address automatically.

A2-4: Use another web browser to log in again.

A2-5: Reset the router to factory default settings and try again.

Q3: How to reset the router to factory default settings?

A3: Powered on your modem router, long-press the RST button for about 6 seconds by a needle. The router is reset successfully when all the LED indicators blink.

Q4: If I forget the login password of the router, what should I do?

A4: The default username and password of the web management page are admin (in the bottom of the router). If you have changed the username and password before this, please reset the router to restore to factory settings and log in the router’s web UI.

Q5: If An IP address conflict message appears after a computer which is connected to the router starts, what should I do?

A5: Please try checking the following items.

A5-1: Ensure that there is no other DHCP server in your LAN or the other DHCP server is disabled.

A5-2: Make sure the IP address of your router is not used by another device in your LAN. The default IP address of the router is 192.168.1.1.

A5-3: Ensure that the static IP address assigned to the computer in your LAN is not used by other devices.

Disclaimer

All ascreenshoots, pictures and product specifications herein are for references only. Comnect reserves the right to make alteration to the products without obligation to notify any person or organization of the revisions or changes, due to the improvement of internal design,operational function, and/or reliability. Comnect does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

© Copyright 2020

IN NO EVENT WILL THE VENDOR BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION; EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, THE VENDOR SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING,OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

The specifications in this user guide are subject to change without notice.