PLANET
Networking & Communication

User's Manual

300Mbps 802.11n Wireless Internet Fiber Router

► FRT-415N

www.PLANET.com.tw

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Federal Communication Commission Interference Statement

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

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Plug the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance, for example, use only shielded interface cables when connecting to computer or peripheral devices. Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remarks
Bulgaria	None	General authorization required for outdoor use and public service.
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012.
Italy	None	If used outside of own premises, general authorization is required.
Luxembourg	None	General authorization required for network and service supply (not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund.
Russian Federation	None	Only for indoor applications

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste; WEEE should be collected separately.

Revision

User’s Manual of 802.11n Wireless Internet Fiber Router

Model: FRT-415N

Rev: 1.0 (November, 2015)

Part No. EM-FRT-415N (**2081-B53080-000**)

Table of Contents

Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET FRT-415N. Before installing the router, please verify the contents inside the package box.

FRT-415N Unit

Quick Installation Guide

Power Adapter

12V DC, 1A output

100~240V AC input

Ethernet Cable

If there is any item missing or damaged, please contact the seller immediately.

1.2 Product Description

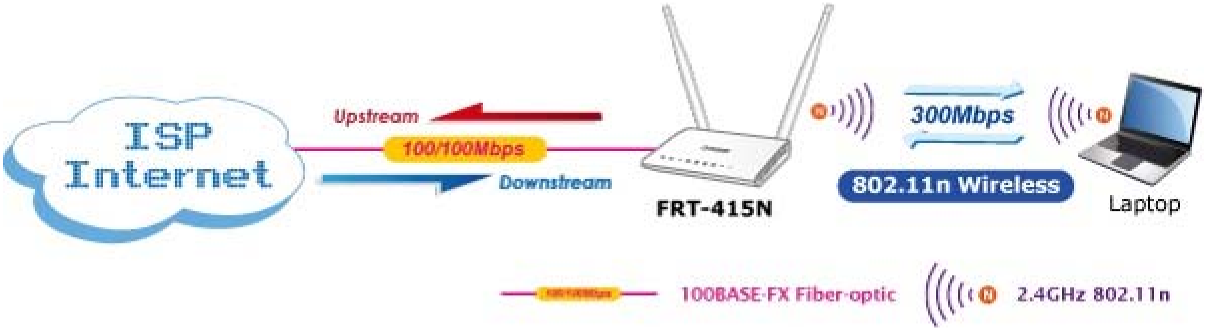
Delivering Highly-demanding Service Connectivity for ISP/Triple Play Devices

With built-in 100BASE-FX fiber interface, the FRT-415N supports different optic types for WAN and the distance can be up to 15~60 km through the fiber connection. The FRT-415N is an ideal solution for FTTH (Fiber-to-the-home) applications in the IPv6 environment. It can handle multiple high-throughput services such as **IPTV**, **on-line gaming**, **VoIP** and **Internet** access, and keep the bandwidth usage smoothly. The FRT-415N also incorporates a 4-port 10/100BASE-TX switching hub, which makes it easy to create or extend your LAN, and prevents DOS attacks.

Fiber Router Total Solution
100/100Mbps
Fiber Router
ISP
Video
Data
Voice
100BASE-FX
Fiber Optic
Video Phone
100/100Mbps
FRT-415N
IPTV (HD)
Online Gaming

High-speed 802.11n Wireless

With built-in IEEE 802.11b/g and 802.11n wireless network capability, the FRT-415N allows any computer and wireless-enabled network device to connect to it without additional cabling. 802.11n wireless capability brings users the highest speed of wireless experience ever; the data transmission rate can be as high as **300Mbps.** The radio coverage is also doubled to offer high-speed wireless connection even in widely spacious offices or houses.



Secure Wireless Access Control

To secure wireless communication, the FRT-415N supports up-to-date encryptions including WEP, WPA-PSK and WPA2-PSK. Moreover, the FRT-415N supports WPS configuration with PBC/PIN type for users to easily connect to a secure wireless network.

WPS (Wi-Fi Protected Setup)
Quick & Easy Wireless Connection
STEP 1
WPS
Click
STEP 2
Press
STEP 3
Connected

Providing Superior Function

The FRT-415N provides user-friendly management interface to be managed easily through standard web browsers. For networking management features, the FRT-415N not only provides basic router functions such as DHCP server, virtual server, DMZ, QoS and UPnP, but also provides full firewall functions including Network Address Translation (NAT), IP/Port/MAC filtering and content filtering. Furthermore, the FRT-415N serves as an Internet firewall to protect your network from being accessed by unauthorized users.

1.3 Product Features

- Internet Access Features

  - **Shared Internet Access:** All users on the LAN can access the Internet through the FRT-415N using only one single external IP address. The local (invalid) IP addresses are hidden from external sources. This process is called NAT (Network Address Translation).

  - **IEEE 802.3u 100BASE-FX standard:** The FRT-415N provides long-distance connection based on optical fiber transceiver which supports **FTTH** and **IPTV** applications.

  - **Multiple WAN Connections:** Upon the Internet (WAN port) connection, the FRT-415N supports dynamic IP address (IP address is allocated upon connection), fixed IP address, PPPoE and bridge. SFP or RJ45 can be selected to be the default WAN interface.

- Advanced Internet Functions

  - **Virtual Servers:** This feature allows Internet users to access Internet servers on your LAN. The setup is quick and easy.

  - **Firewall:** The FRT-415N supports simple firewall with NAT technology.

  - **Universal Plug and Play (UPnP):** UPnP allows automatic discovery and configuration of the broadband router. UPnP is supported by Windows XP, or later.

- **User Friendly Interface:** The FRT-415N can be managed and controlled through Web UI.
- **DMZ Support:** The FRT-415N can translate public IP addresses into private IP address to allow unlimited 2-way communication with the servers or individual users on the Internet. It provides the most flexibility to run programs smoothly for programs that might be restricted in NAT environment.
- **RIP1/2 Routing:** It supports RIPv1/2 routing protocol for routing capability.
- **IPv6 Support:** The FRT-415N supports IPv6 for new services and higher security.

➢ LAN Features

- **4-port Switch:** The FRT-415N incorporates a 4-port 10/100BASE-TX switching hub, making it easy to create or extend your LAN.
- **DHCP Server Support: D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The FRT-415N can act as a DHCP Server for devices on your local LAN.

➢ Wireless Features

- **Supports IEEE 802.11b, g and n Wireless Stations:** The 802.11n standard provides backward compatibility with the 802.11b and 802.11g standard, so 802.11b, 802.11g, and 802.11n can be used simultaneously. IEEE 802.11n wireless technology is capable of having a data rate of up to 300Mbps.
- **Two External Antennas with MIMO Technology:** The FRT-415N provides farther coverage, less dead spaces and higher throughput with 2T2R MIMO technology.
- **WPS Push Button Control:** The FRT-415N supports WPS (Wi-Fi Protected Setup) for users to easily connect to wireless network without configuring the security.
- **WEP Support:** WEP (Wired Equivalent Privacy) is included. Key sizes of 64 bit and 128 bit are supported.
- **WPA-PSK Support:** WPA-PSK_TKIP and WAP-PSK_AES encryption are supported.
- **Wireless MAC Access Control:** The Wireless Access Control feature can check the MAC address (hardware address) of wireless stations to ensure that only trusted wireless stations can access your LAN.

1.4 Product Specifications

Model		FRT-415N
Product Description		300Mbps 802.11n Wireless Internet Fiber Router
Hardware Specifications		
Interface	LAN	4 x 10/100BASE-TX, auto-negotiation, auto MDI/MDI-X RJ45 port
	WAN	1 x 100BASE-FX SFP slot
	Wireless	2x 5dBi fixed antenna
Optic Interface	Connector	SFP (Small form-factor Pluggable)
	Mode	Vary on module
	Distance	Vary on module
LED Indicators		PWR, WAN, Internet, LAN1-4, WLAN, WPS, Security
Button		1 x Reset button 1 x WPS button 1 x Power button
Material		Plastic
Dimensions (W x D x H)		132 x 93 x 25 mm
Power		12V DC, 0.5A
Router Features		
Internet Connection Type		Shares data and Internet access for users, supporting the following internet accesses: ■ PPPoE ■ Dynamic IP ■ Static IP ■ Bridge
Max. Session		45659
Fiber-optic Cable		■ 50/125µm or 62.5/125µm multi-mode fiber cable, up to 2km. ■ 9/125µm single-mode cable, providing long distance of 15/20/35/50km or longer (vary on SFP module)
Routing Protocol		Static routing RIPv1/2
Security		Built-in NAT firewall MAC/IP/Port filtering Content filtering SPI firewall

Protocol/Feature	WPS DMZ and virtual server 802.1D QoS DHCP server/relay IGMP snooping IGMP proxy and MLD proxy UPnP and DDNS
System Management	Web-based (HTTP) configuration SNTP time synchronization System log supports remote log Password protection for system management TR-069
Wireless Interface Specifications	
Wireless Standard	IEEE 802.11b, g and n
Frequency Band	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Modulation Type	DBPSK, DQPSK, CCK and OFDM (BPSK/QPSK/16-QAM/ 64-QAM)
Data Transmission Rates	**802.11n (40MHz)**: 270/243/216/162/108/81/54/27Mbps 135/121.5/108/81/54/40.5/27/13.5Mbps (dynamic)
	802.11n (20MHz): 130/117/104/78/52/39/26/13Mbps 65/58.5/52/39/26/19.5/13/6.5Mbps (dynamic)
	802.11g: 54/48/36/24/18/12/9/6Mbps (dynamic)
	802.11b: 11/5.5/2/1Mbps (dynamic)
Channel	Maximum 13 Channels, depending on regulatory authorities
Antenna Connector	2 x 5dBi fixed antenna
Wireless Data Encryption	64-/128-bit WEP, WPA-PSK, WPA2-PSK, 802.1x encryption, and WPS PBC
Environment Specifications	
Temperature/Humidity	Operating: 0~40 degrees C, 10%~ 90% (non-condensing), Storage: -10~70 degrees C, 0~95% (non-condensing)
Certification	CE

Standards Conformance	
Standard	Fiber Interface Complaint with IEEE802.3/802.3u 10/100 BASE-TX, 100BASE-FX standard UP band support (25KHz to 276KHz) Packet Transfer Mode Ethernet in the first mile(PTM-EFM)

Chapter 2. Hardware Installation

This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

2.1 Hardware Description

2.1.1 Front Panel of FRT-415N

The front panel provides a simple interface monitoring of the router. Figure 2-1 shows the front panel of the FRT-415N.

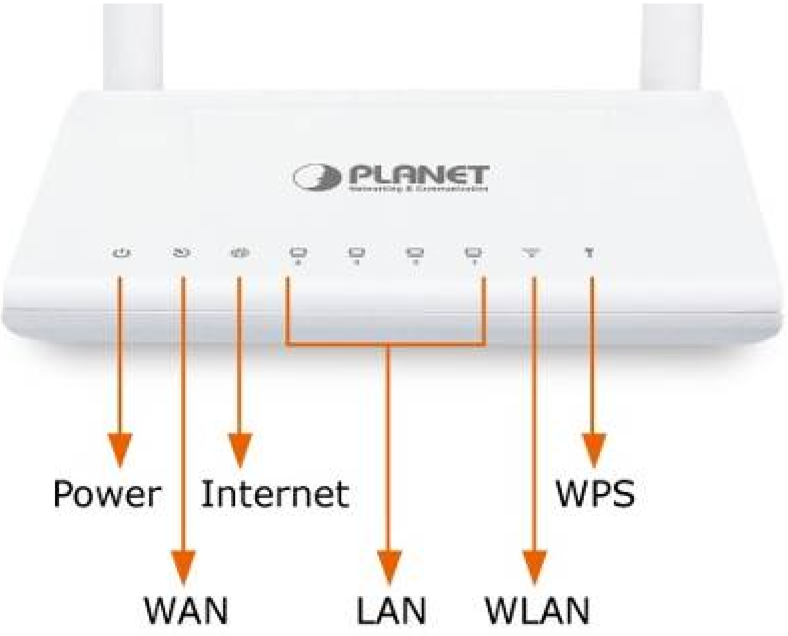


Figure 2-1 FRT-415N Front Panel

2.1.2 LED Indications of FRT-415N

The LEDs on the top panel indicate the instant status of system power, WAN data activity and port links, and help monitor and troubleshoot when needed. Figure 2-1 and Table 2-1 show the LED indications of the FRT-415N.

Front Panel LED Definition

LED	State	Description
Power	On	When the router is powered on, and in ready state.
	Off	When the router is powered off.
WAN	Flashing	Router is trying to establish a WAN connection to device.
	On	The WAN is connected successfully.
Internet	Flashing	Router is trying to establish an Internet connection to device.
	On	The Internet is connected successfully.
LAN1-4	Flashing	Data is being transmitted or received via the corresponding LAN port.
	On	The port is up.
WLAN	On	WLAN radio is on.
	Flashing	Data is being transmitted through WLAN.
	Off	WLAN radio is off.
WPS	On	WPS client registration is successful.
	Flashing	Press the button over 6 seconds and WPS client registration window is going to open.
	Off	WPS is not available, or WPS is not enabled or initialized.

Table 2-1 The LED indication of FRT-415N

2.1.3 Rear Panel of FRT-415N

The rear panel provides the physical connectors connected to the power adapter and any other network device. Figure 2-2 shows the rear panel of the FRT-415N.

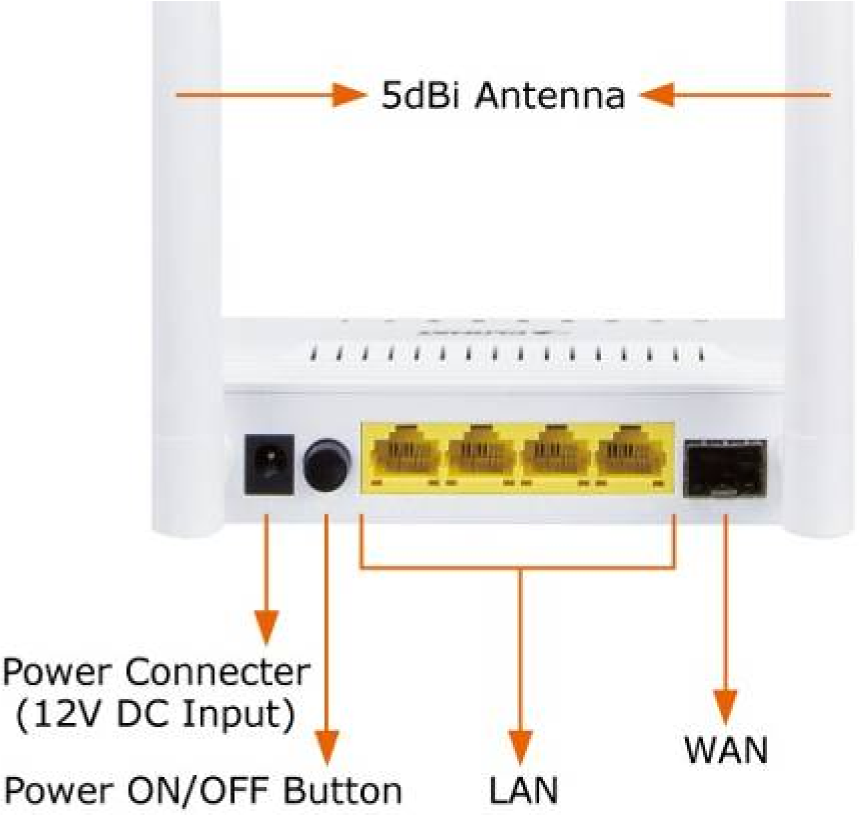


Figure 2-2 FRT-415N Rear Panel

Rear Panel Port and Button Definition

Connector	Description
Power	Power connector with 12V DC, 0.5 A
Power Button	Power on/off button
LAN (1-4)	Router is successfully connected to a device through the corresponding port (1, 2, 3, or 4). If the LED light of LNK/ACT is flashing, the router is actively sending or receiving data over that port.
WAN	The SFP connector allows data communication between the router and the fiber network through an optical fiber cable

2.2 Cabling

- **100BASE-TX and 100BASE-FX**

The 10/100Mbps RJ45 ports come with auto-negotiation capability. Users only need to plug in working network device into one of the 10/100Mbps RJ45 ports. The FRT-415N will automatically run in 10Mbps or 100Mbps after the negotiation with the connected device. The FRT-415N has one 100BASE-FX SFP interface (optional multi-mode/single-mode 100BASE-FX SFP module).

- **Cabling**

Each 10/100BASE-TX port uses RJ45 sockets for connection to unshielded twisted-pair cable (UTP).

Port Type	Cable Type	Connector
10BASE-T	Cat 3, 4, 5, 2-pair	RJ45
100BASE-TX	Cat 5, 5e, 6 UTP, 2-pair	RJ45

Any Ethernet devices like hubs or PCs can connect to the fiber router by using straight-through wires. The 10/100Mbps RJ45 ports which support auto MDI/MDI-X can be used on straight-through or crossover cable.

2.2.1 Installing the SFP Transceiver

This section describes how to insert an SFP transceiver into an SFP slot. The SFP transceiver is hot-pluggable and hot-swappable. You can plug in and out the transceiver to/from any SFP port without having to power down the fiber router as Figure 2-12 appears.

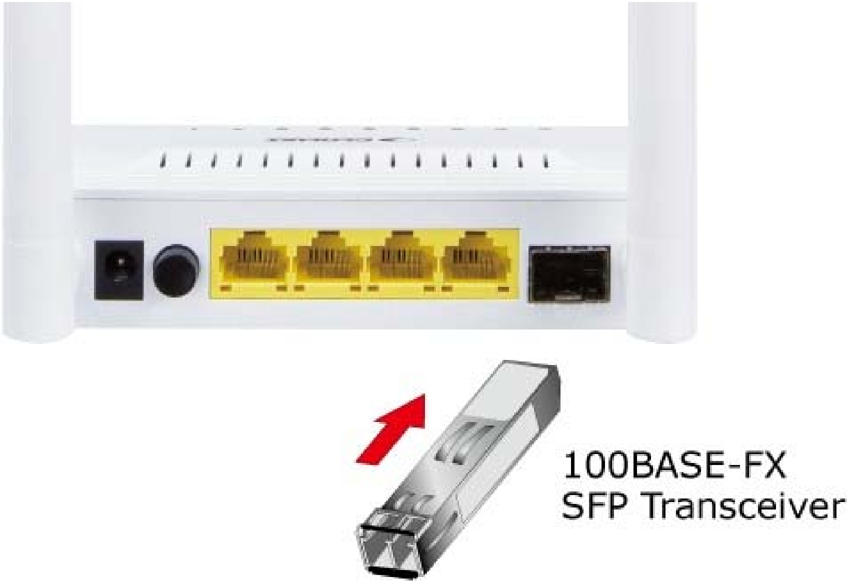


Figure 2-3 Plug in the SFP transceiver

Before connecting the other switches, workstation or media converter,

1. Make sure both sides of the SFP transceiver are with the same media type or WDM pair; for example, 100BASE-FX to 100BASE-FX and 100BASE-BX20-U to 100BASE-BX20-D.
2. Check whether the fiber-optic cable type matches the SFP transceiver model.
   - To connect to **MFB-FX** SFP transceiver, use the **multi-mode** fiber cable, with one side being the male duplex LC connector type.
   - To connect to **MFB-F20/F40/F60/FA20/FB20** SFP transceiver, use the **single-mode** fiber cable, with one side being the male duplex LC connector type.

Connecting the fiber cable

1. Attach the duplex LC connector on the network cable to the SFP transceiver.
2. Connect the other end of the cable to a device – switches with SFP installed, fiber NIC on a workstation or a media converter.
3. Check the LNK/ACT LED of the SFP slot of the switch/converter. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. It functions with some fiber-NICs or media converters; setting the Link mode to “100 Force” is needed.

2.2.2 Removing the Module

1. Please make sure there is no network activity by console or check with the network administrator. You can access the management interface of the fiber router to disable the port in advance.
2. Remove the Fiber Optic Cable gently.
3. Turn the handle of the MFB module/mini GBIC SFP module to horizontal.
4. Pull out the module gently through the handle.

Note

Never pull out the module without pulling the lever or the push bolts on the module. Directly pulling out the module with force could damage the module and SFP module slot of the device.

Chapter 3. Connecting to the Router

3.1 System Requirements

- Broadband Internet Access Service (FTTH connection)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- PC of subscribers running Windows XP, Windows Vista/Win 7, MAC OS 9 or later, Linux, UNIX or other platform compatible with **TCP/IP** protocols
- The above PC is installed with Web browser

Note

1. The Router in the following instructions is named as PLANET FRT-415N.

2. It is recommended to use Internet Explore 8.0 or above to access the Router.

3.2 Installing the Router

Please connect the device to your computer as follows:

- Locate the FRT-415N in an optimum place and adjust the antenna for the best coverage. Figure 3-1 shows the antenna connection diagram.

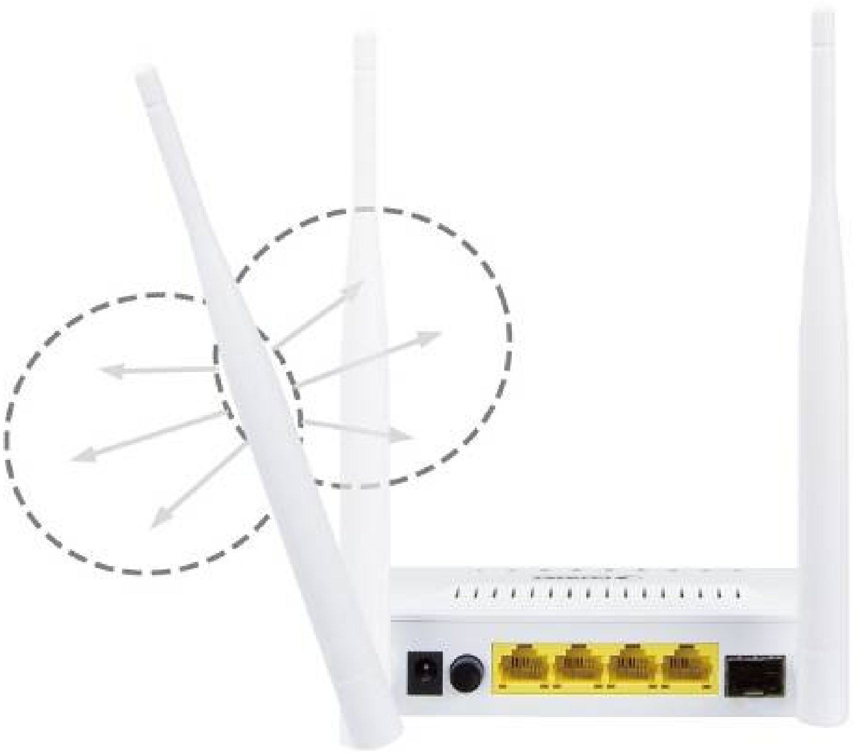


Figure 3-1 FRT-415N Antenna Adjustment Diagram

- Connect your fiber wire to the "**WAN**" port via SFP fiber wire.Figure3-2 shows the WAN port connection diagram

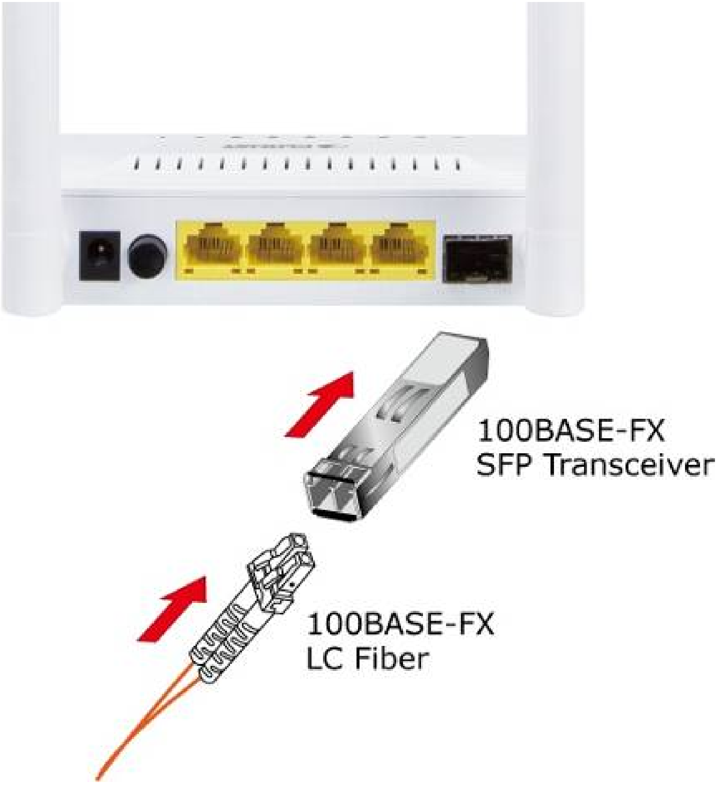


Figure 3-2 FRT-415N WAN Port Connection Diagram

- Use Ethernet cable to connect to the "**LAN**" port of the modem and the "**LAN**" port of your computer.
- Connect Power Adapter to the FRT-415N. Figure3-3 shows the power adapter connection diagram.

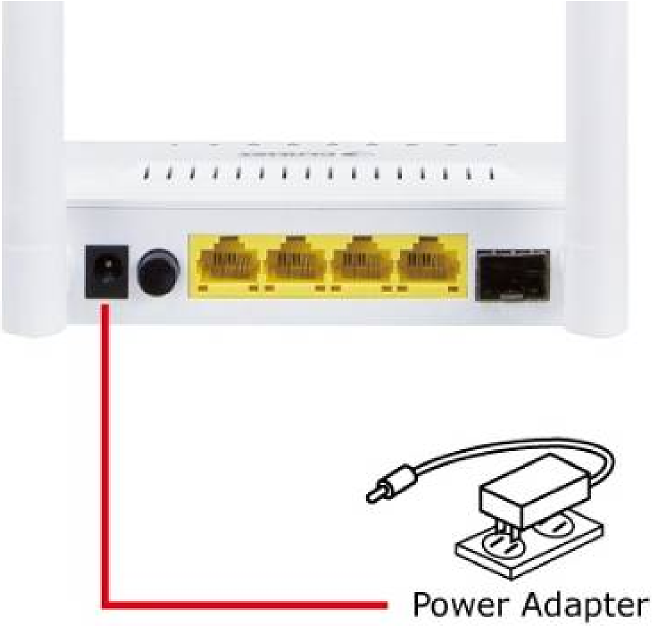


Figure 3-3 FRT-415N Power Adapter Connection Diagram

- Follow Figure 3-4 to connect the network devices.

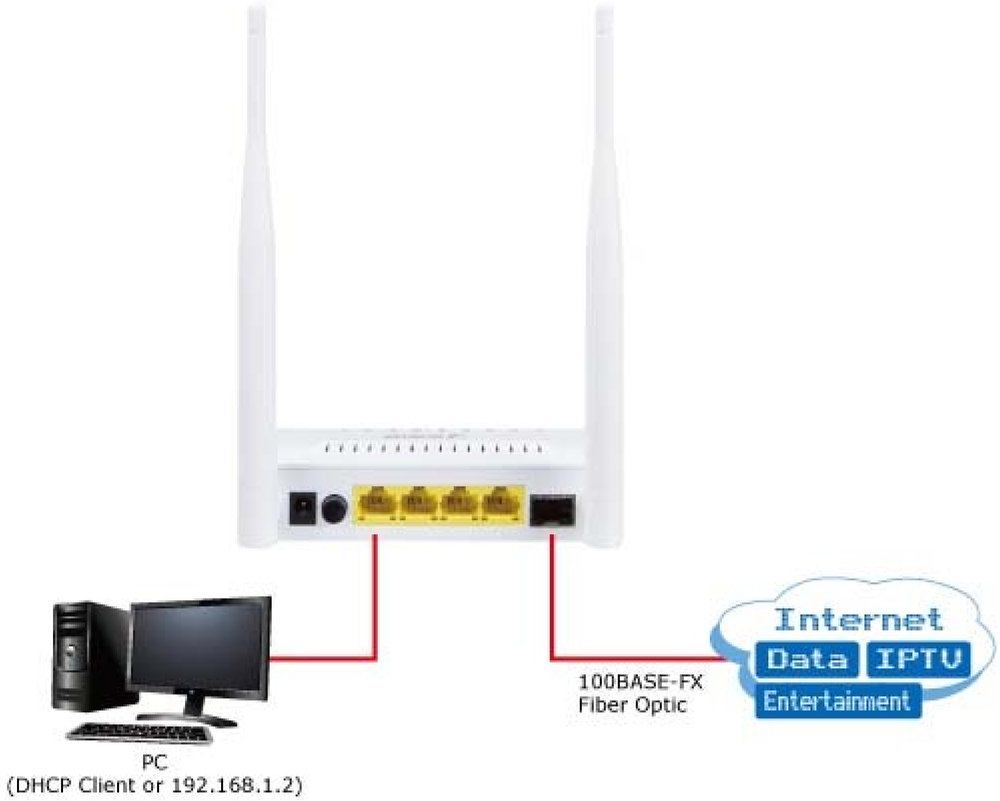


Figure 3-4 FRT-415N Connection Diagram

Chapter 4. Installation Guide

4.1 Configuring the Network Properties

Configuring PC in Windows 7

1. Go to **Start, Control Panel, Network and Internet, and Network and Sharing Center**. Click **Change adapter settings** on the left banner.
2. Double-click **Local Area Connection**.

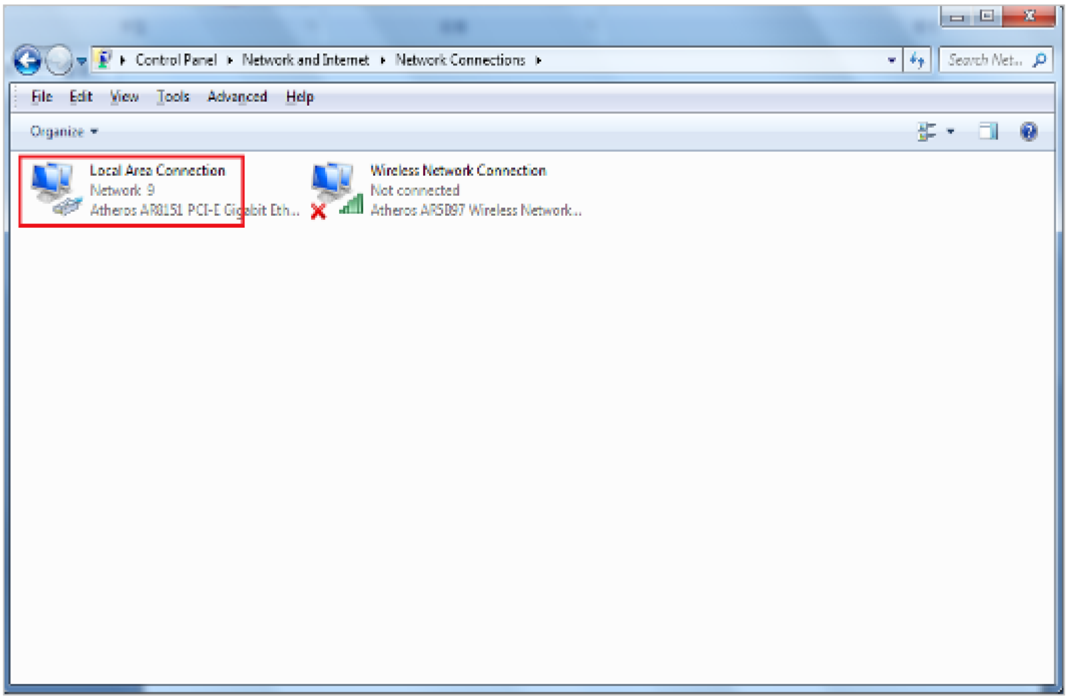

Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Net...
File Edit View Tools Advanced Help
Organize ▾
Local Area Connection
Network 9
Atheros AR8151 PCI-E Gigabit Eth...
Wireless Network Connection
Not connected
Atheros AR5B97 Wireless Network...

Figure 4-1 Select Local Area Connection

3. In the **Local Area Connection Status** window, click **Properties**.

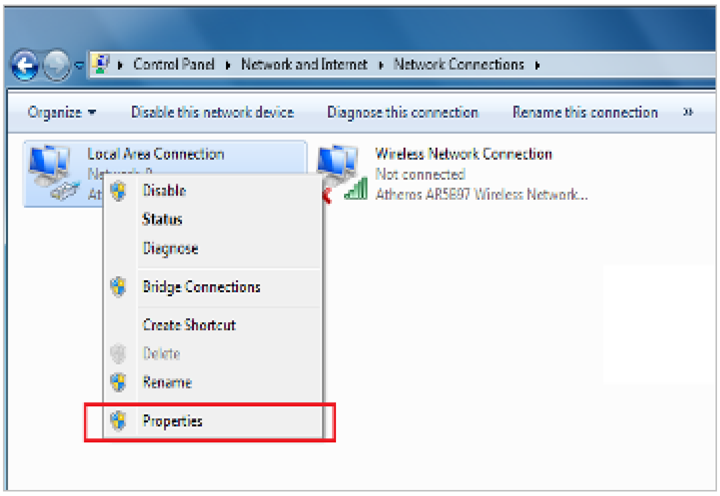
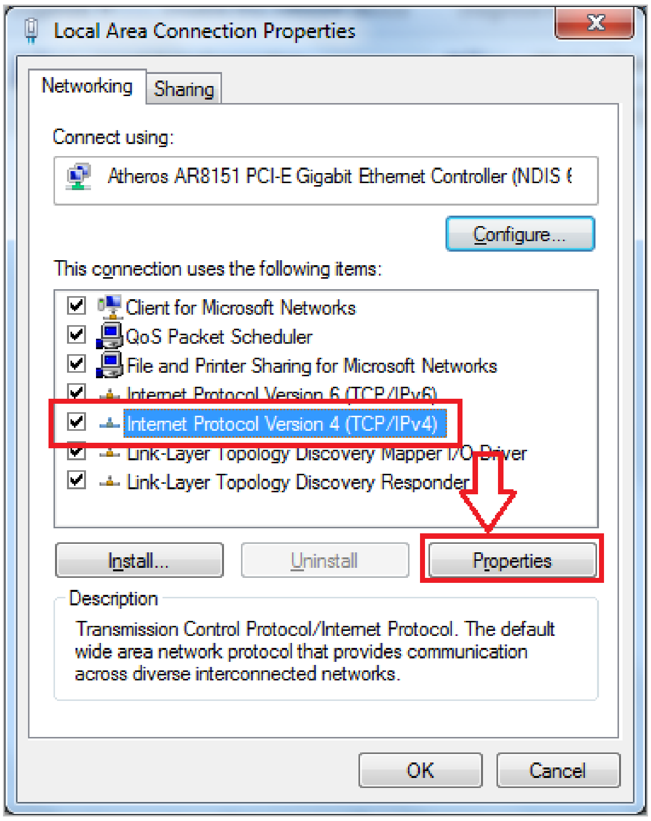


Figure 4-2 Network Connection Properties

4. Select **Internet Protocol Version 4 (TCP/IPv4)** and **click Properties**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

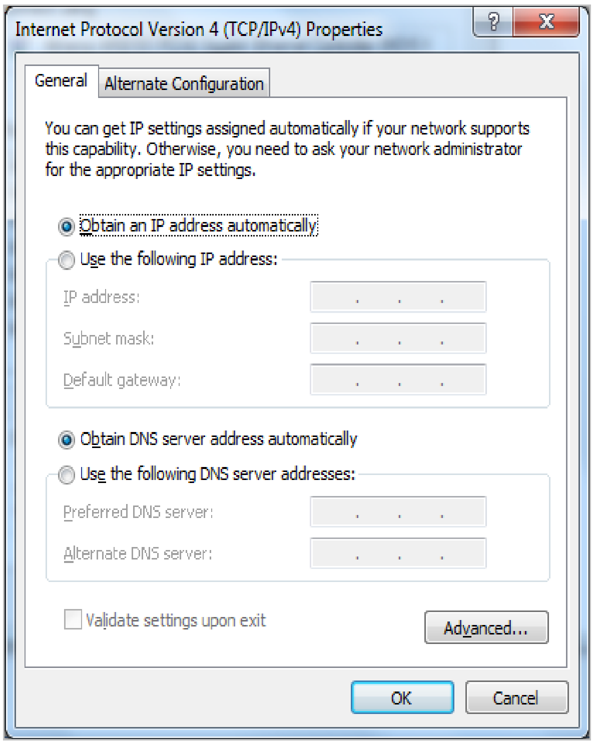
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Figure 4-3 TCP/IP Setting

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** button.

6. Click **OK** to finish the configuration.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

Advanced...

OK | Cancel

Figure 4-4 Obtain an IP address automatically

Configuring PC in Windows XP

1. Go to **Start and Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**

2. Double-click **Local Area Connection**.

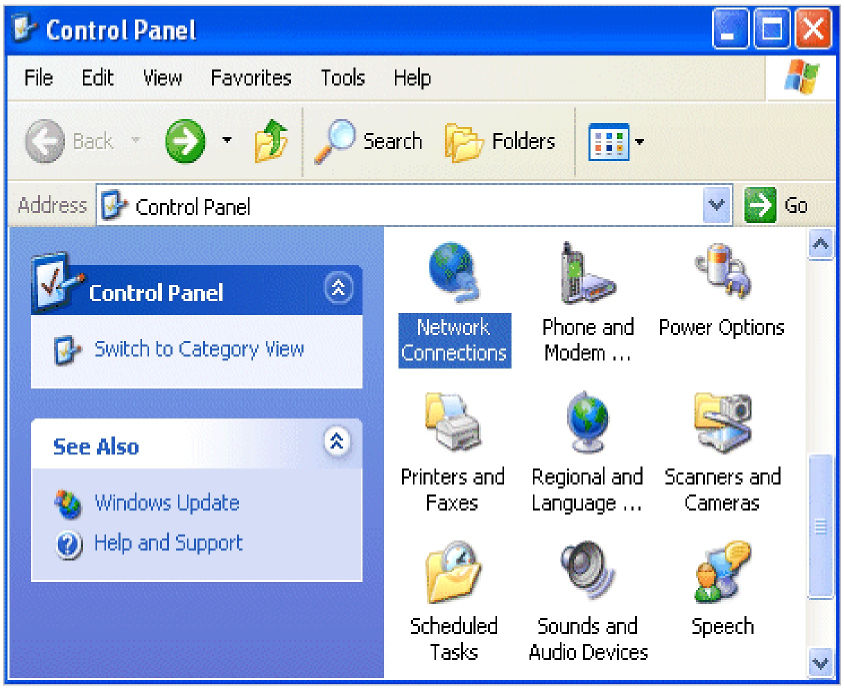
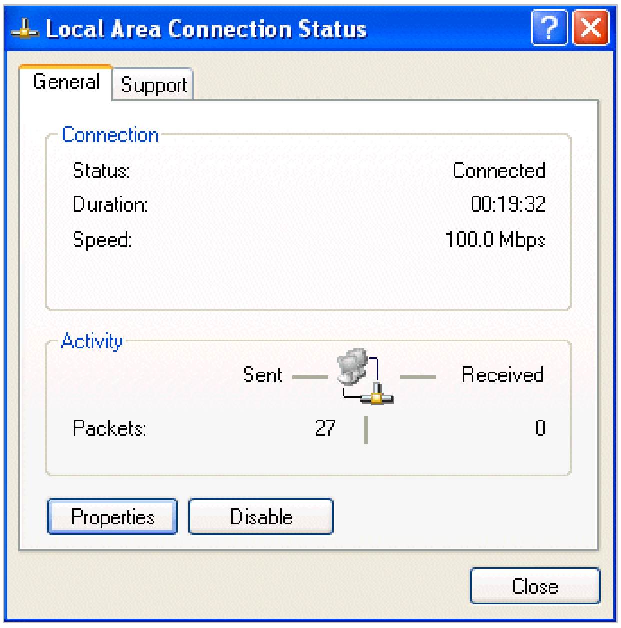


Figure 4-5 Select Network Connections

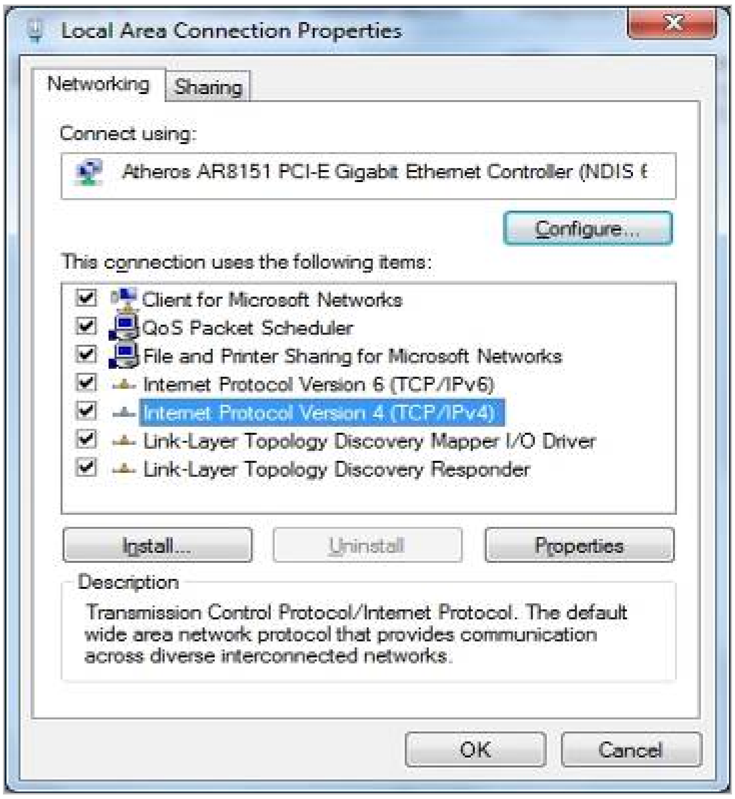
3. In the **Local Area Connection Status** window, click **Properties**.



Status: Connected
Duration: 00:19:32
Speed: 100.0 Mbps
Packets: 27 0

Figure 4-6

4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



Local Area Connection Properties

Networking | Sharing

Connect using:

Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

Description

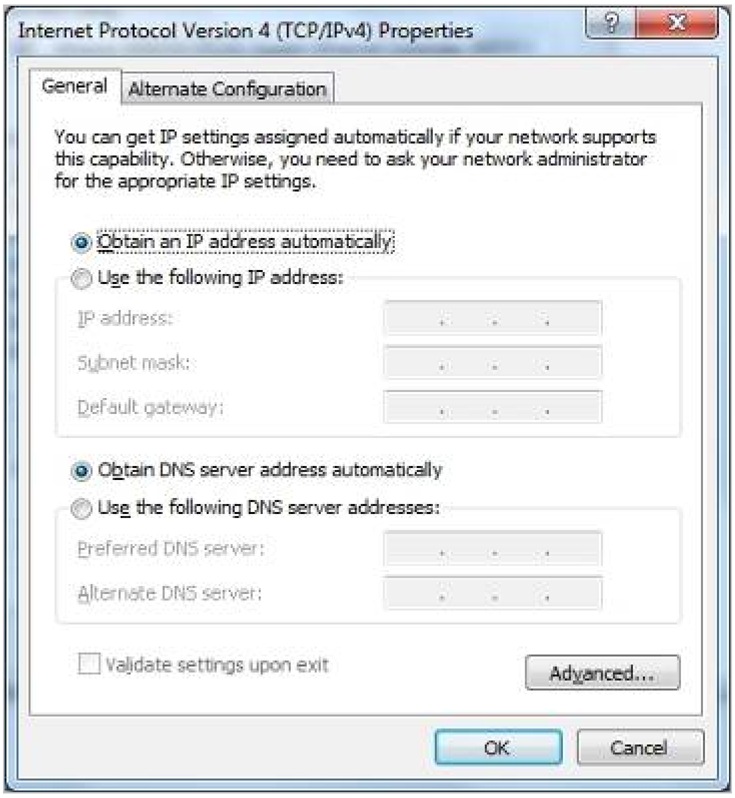
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Figure 4-7 TCP/IP Setting

5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** button.

6. Click **OK** to finish the configuration.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

Advanced...

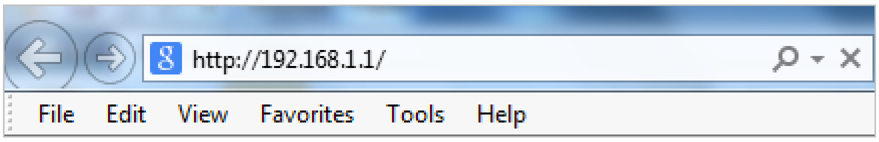
OK | Cancel

Figure 4-8 Obtain an IP address automatically

4.2 Configuring with Web Browser

It would be better to change the administrator password to safeguard the security of your network. To configure the router, open your browser, type **"http: //192.168.1.1"** into the address bar and click **"Go"** to get to the login page.

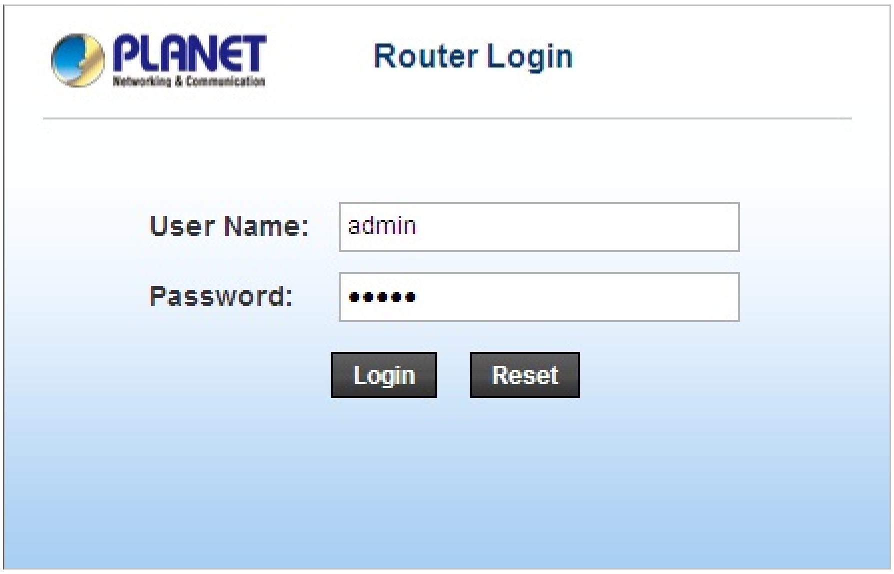
Save this address in your Favorites for future reference.



http://192.168.1.1/

Figure 4-9 Login the Router

At the User Name and Password prompt, type your proper user name and password to login. The default user name and password are both **"admin**. You can change these later if you wish. Click **"OK".**



Router Login

User Name: admin

Password: •••••

Figure 4-10 Login Window

If the user name and password are correct, you will log in to Fiber Router successfully and see the status page. Now you can configure the Fiber Router for your needs.

Chapter 5. System Settings

Determining your Connection Settings

Before you configure the router, you need to know the connection information supplied by your Internet service provider.

Connecting the Fiber Router to your Network

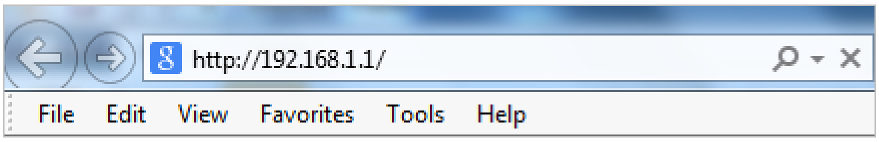
Unlike a simple hub or switch, the setting up of the Fiber Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP addresses the Router chooses to assign them.

Generally there are several different operation modes for your applications. And you can know which mode is necessary for your system from ISP. These WAN modes are PPPoE, Bridge and IPoE.

Configuring with Web Browser

It is advisable to change the administrator password to safeguard the security of your network. To configure the router, open your browser, type **"http: //192.168.1.1"** into the address bar and click **"Go"** to get to the login page.

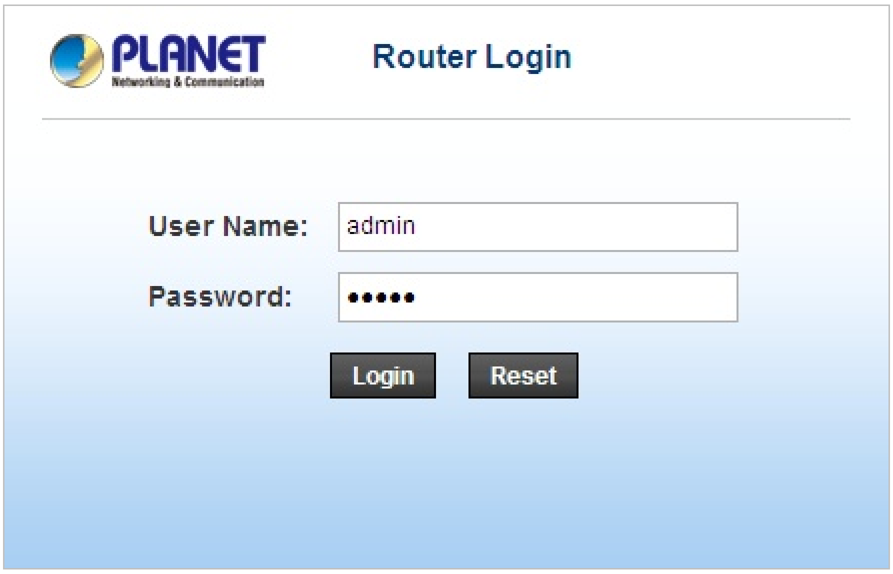
Save this address in your Favorites for future reference.



http://192.168.1.1/

Figure 5-1 Login the Router

At the User Name prompt, type **"admin"**, and the Password prompt, type **"admin"**. You can change these later if you wish. Click **"OK"** to log in to the router and you can start to configure it now.



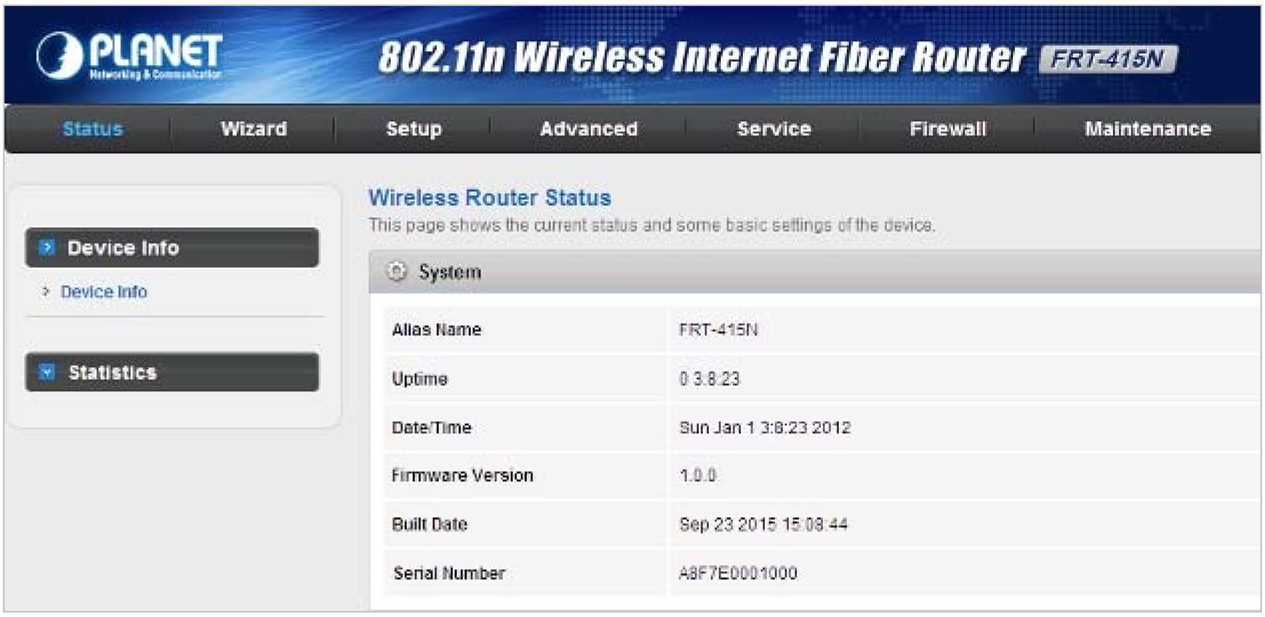
Router Login

User Name: admin

Password: •••••

Figure 5-2 Login Window

After logging in, the page shown in the following figure appears. You can check, configure and modify all the settings.



Wireless Router Status

This page shows the current status and some basic settings of the device.

System

Alias Name	FRT-415N
Uptime	0 3:8:23
Date/Time	Sun Jan 1 3:8:23 2012
Firmware Version	1.0.0
Built Date	Sep 23 2015 15:08:44
Serial Number	A8F7E0001000

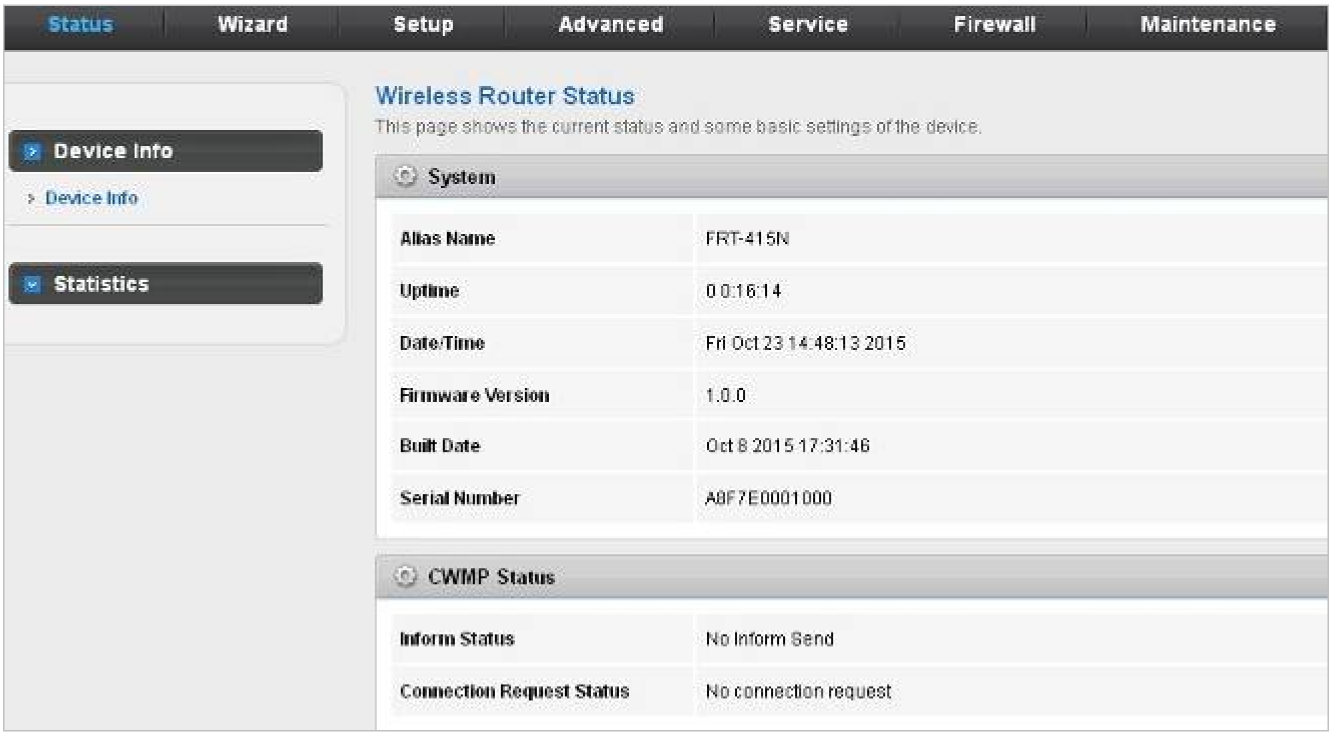
Figure 5-3 Status

5.1 Status

In the navigation bar, choose **Status**. On the **Status** page that is displayed contains: **Device Info** and **Statistics**.

5.1.1 Device Information

Choose Status > Device Info and the page displayed shows the current status and some basic settings of the router, such as software version, CWMP status, LAN configuration, DNS status and WAN interfaces.



Wireless Router Status

This page shows the current status and some basic settings of the device.

System

Alias Name	FRT-415N
Uptime	0 0:16:14
Date/Time	Fri Oct 23 14:48:13 2015
Firmware Version	1.0.0
Built Date	Oct 8 2015 17:31:46
Serial Number	A8F7E0001000

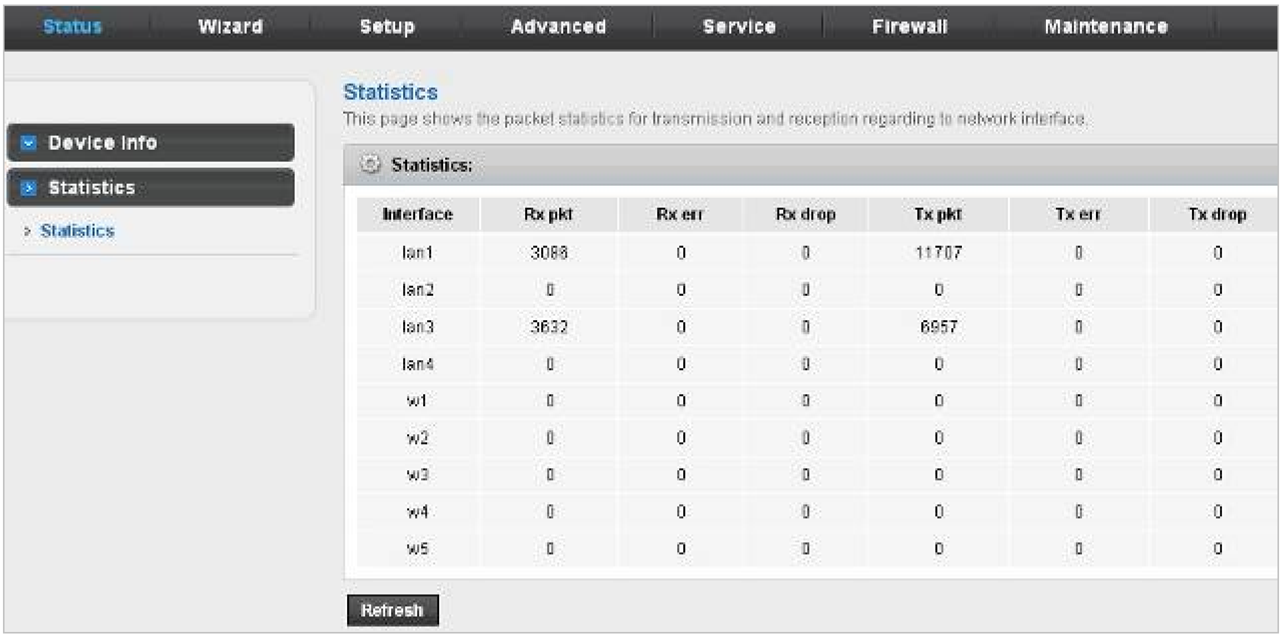
CWMP Status

Inform Status	No Inform Send
Connection Request Status	No connection request

Figure 5-4 Device Info

5.1.2 Statistics

Choose **Status** > **Statistics.** Click **Statistics** in the left pane and the page shown in the following figure appears. On this page, you can view the statistics of each network port.



Statistics

This page shows the packet statistics for transmission and reception regarding to network interface.

Statistics:

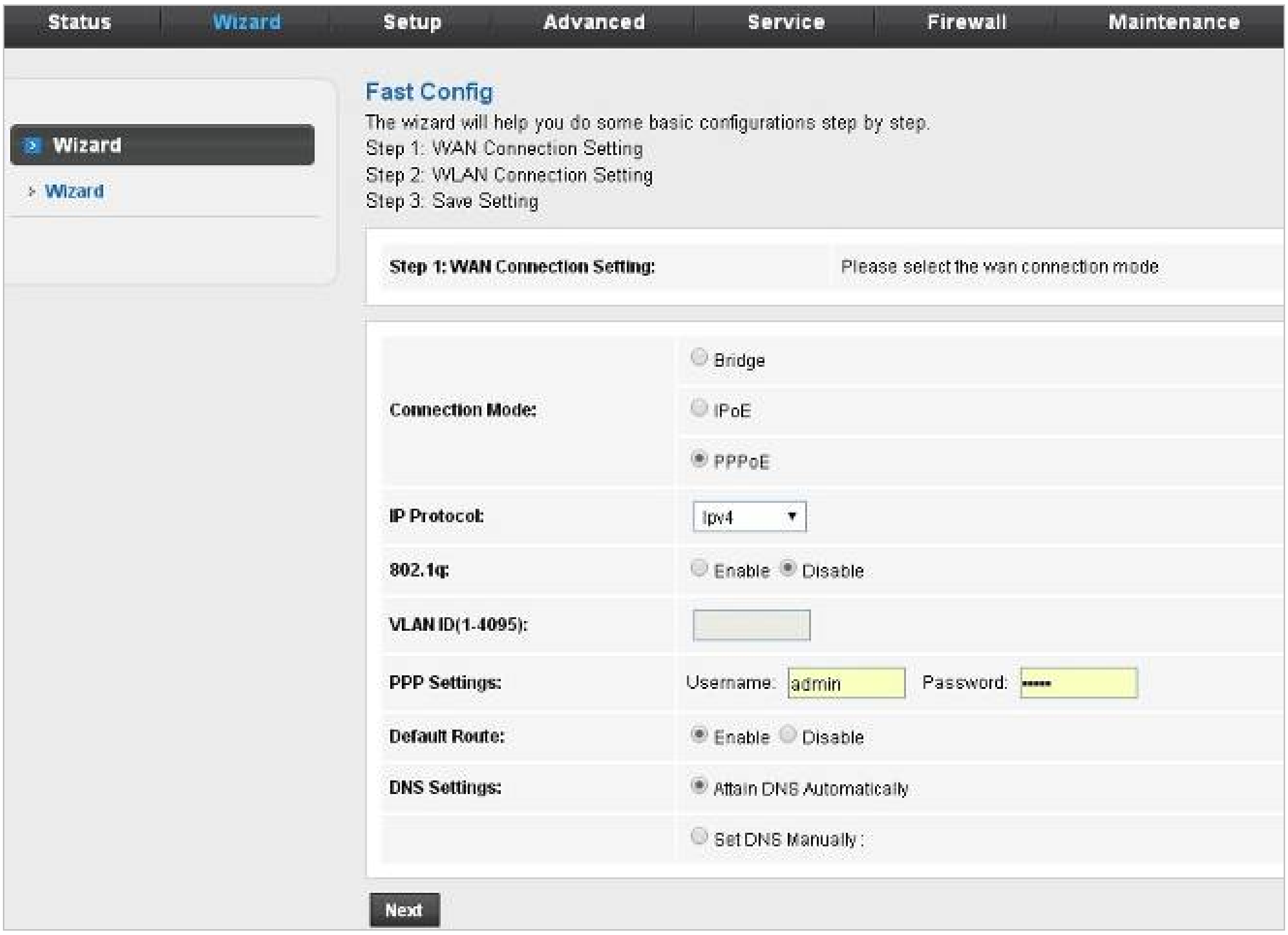
Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
lan1	3088	0	0	11707	0	0
lan2	0	0	0	0	0	0
lan3	3632	0	0	6957	0	0
lan4	0	0	0	0	0	0
w1	0	0	0	0	0	0
w2	0	0	0	0	0	0
w3	0	0	0	0	0	0
w4	0	0	0	0	0	0
w5	0	0	0	0	0	0

Figure 5-5 Statistics

5.2 Wizard

When subscribing to a broadband service, you should be aware of the method by which you are connected to the Internet. Your physical WAN device can be either Ethernet or fiber port. The technical information about the properties of your Internet connection is provided by your Internet Service Provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol that you use to communicate on the Internet.

In the navigation bar, choose **Wizard**. The page shown in the following figure appears. The **Wizard** page guides fast and accurate configuration of the Internet connection and other important parameters. The following sections describe these various configuration parameters. Whether you configure these parameters or use the default ones, click **NEXT** to enable your Internet connection.



Fast Config

The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

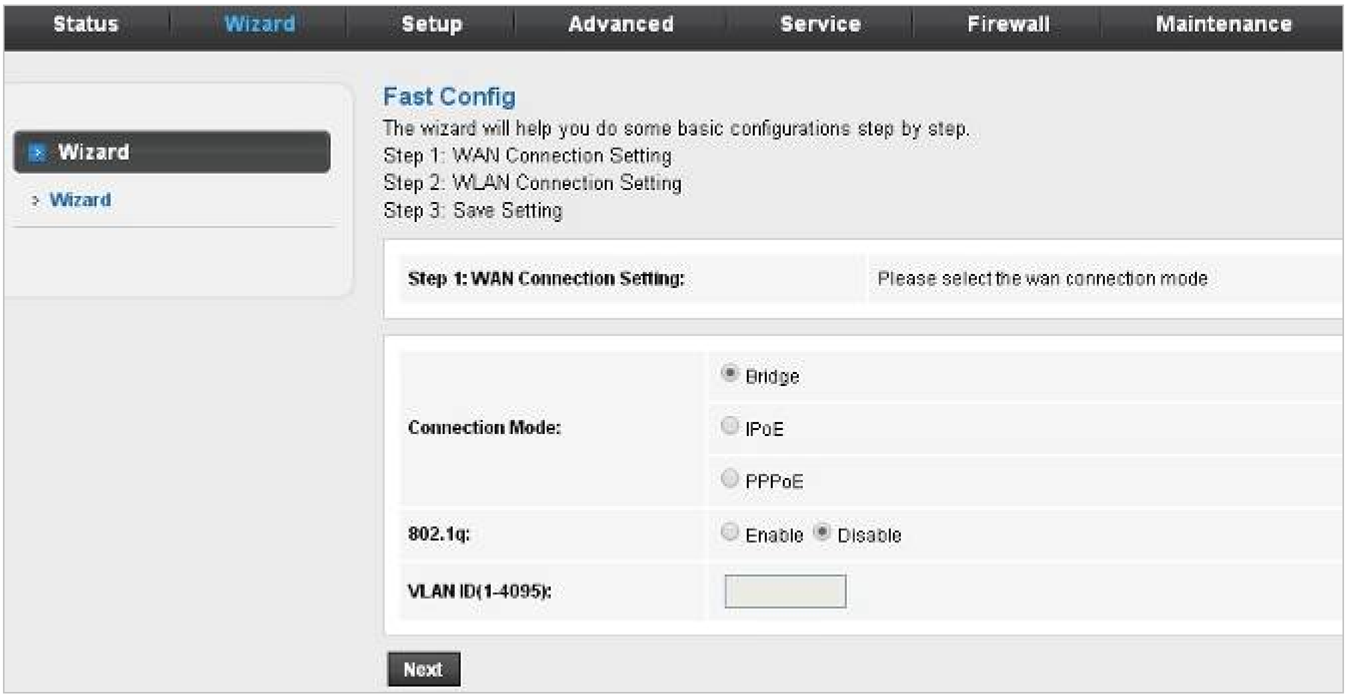
Step 1: WAN Connection Setting:	Please select the wan connection mode

Connection Mode:	○ Bridge ○ IPoE ● PPPoE
IP Protocol:	Ipv4 ▾
802.1q:	○ Enable ● Disable
VLAN ID(1-4095):	
PPP Settings:	Username: admin Password: •••••
Default Route:	● Enable ○ Disable
DNS Settings:	● Attain DNS Automatically ○ Set DNS Manually :

Figure 5-6 Wizard

There are three WAN connection types: **Bridge, IPoE and PPP over Ethernet (PPPoE)**. The following describes them respectively.

5.2.1 Bridge



Fast Config

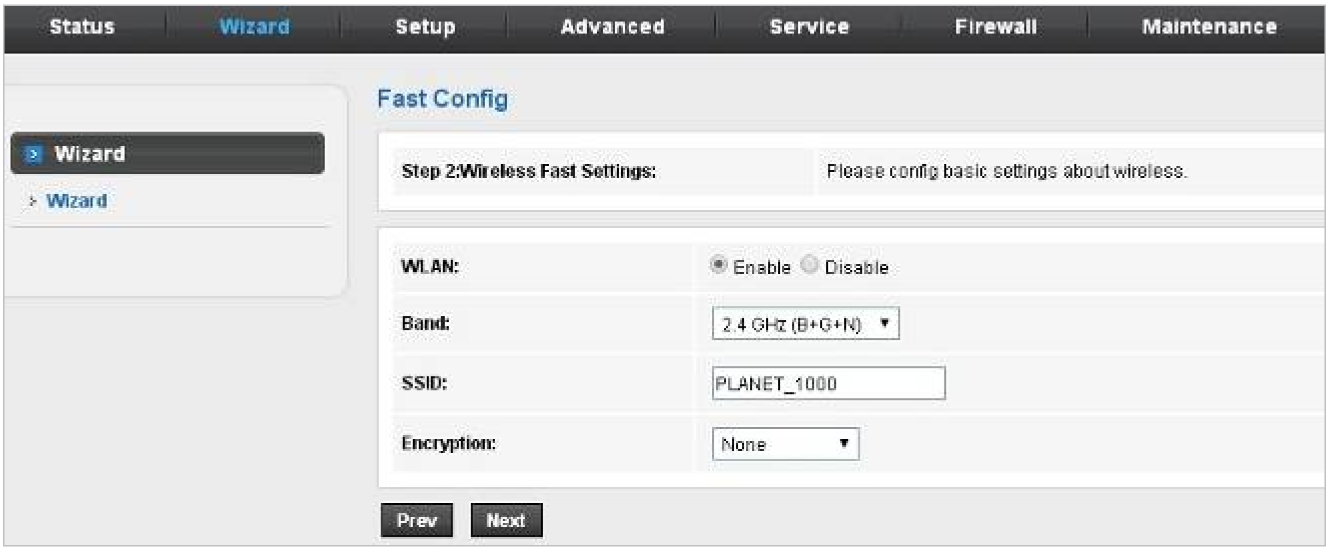
The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting:	Please select the wan connection mode

Connection Mode:	● Bridge ○ IPoE ○ PPPoE
802.1q:	○ Enable ● Disable
VLAN ID(1-4095):	

Figure 5-7 Wizard Bridge

After setting, click **Next** and the page as shown in the following figure appears.



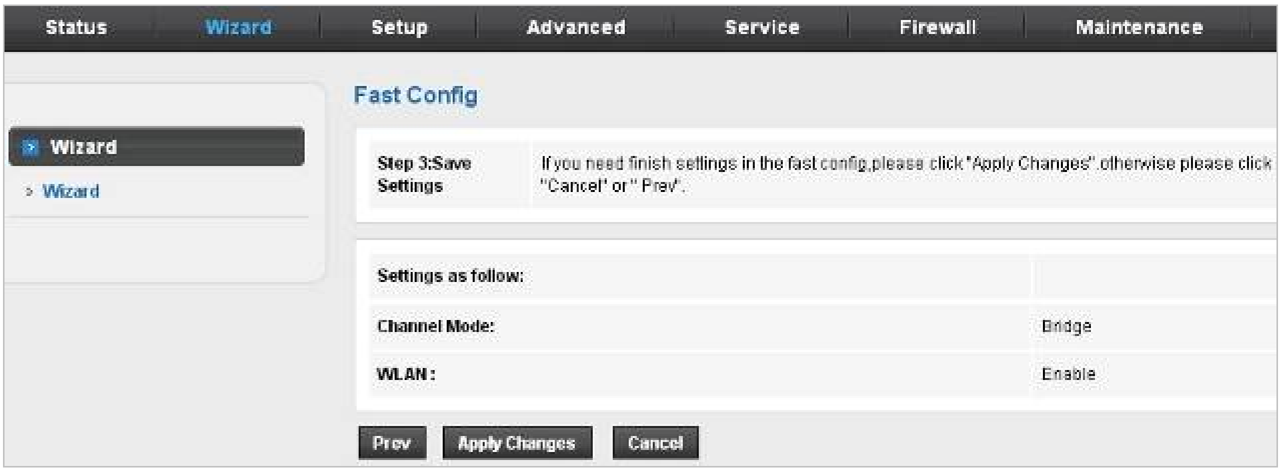
Fast Config

Step 2:Wireless Fast Settings:	Please config basic settings about wireless.

WLAN:	● Enable ○ Disable
Band:	2.4 GHz (B+G+N) ▼
SSID:	PLANET_1000
Encryption:	None ▼

Figure 5-8 Wizard Bridge WLAN

And click **Apply changes** to save the configuration.



Fast Config

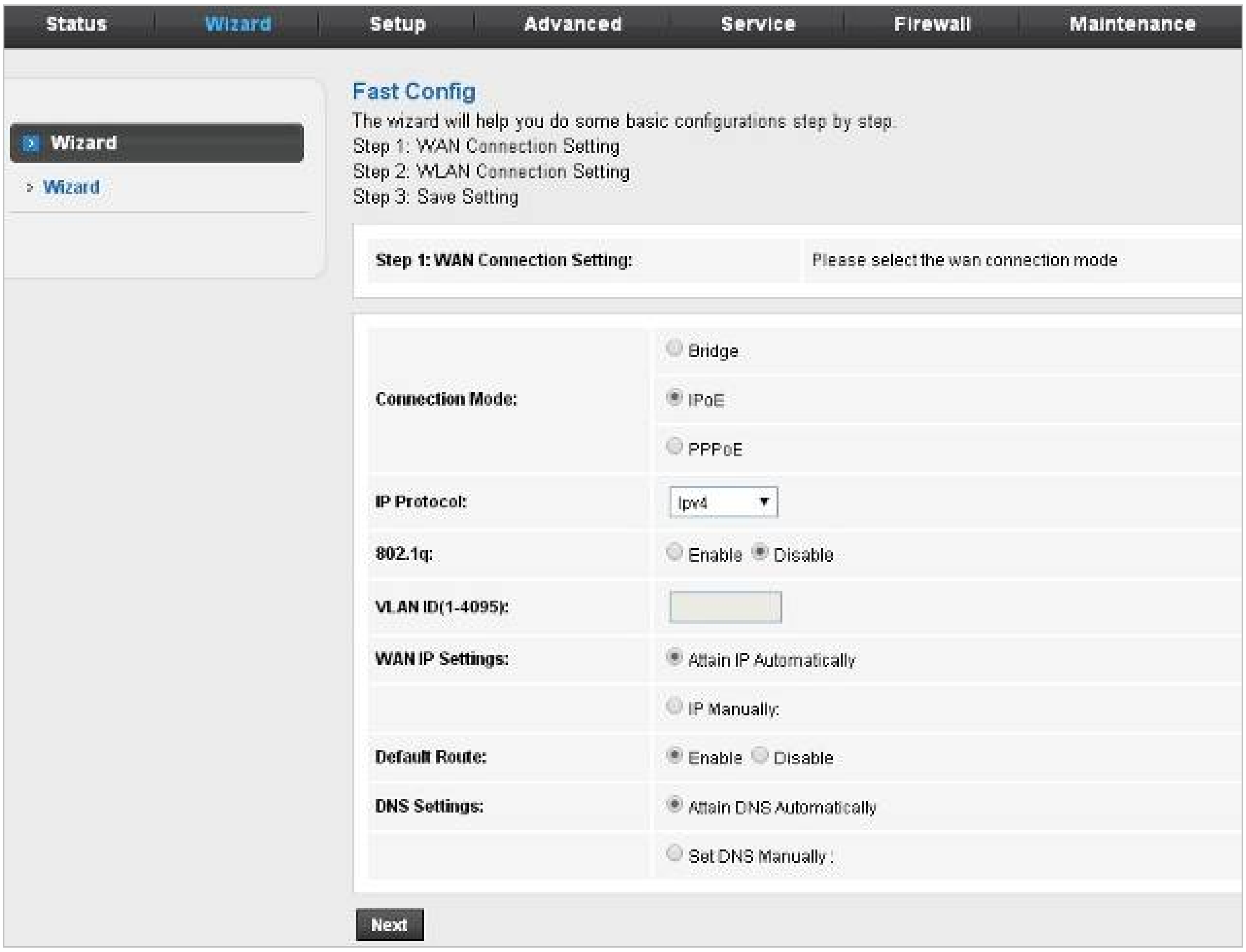
Step 3:Save Settings	If you need finish settings in the fast config,please click "Apply Changes",otherwise please click "Cancel" or " Prev".

Settings as follow:	
Channel Mode:	Bridge
WLAN :	Enable

Prev | Apply Changes | Cancel

Figure 5-9 Wizard Bridge Save

5.2.2 IPoE



Fast Config

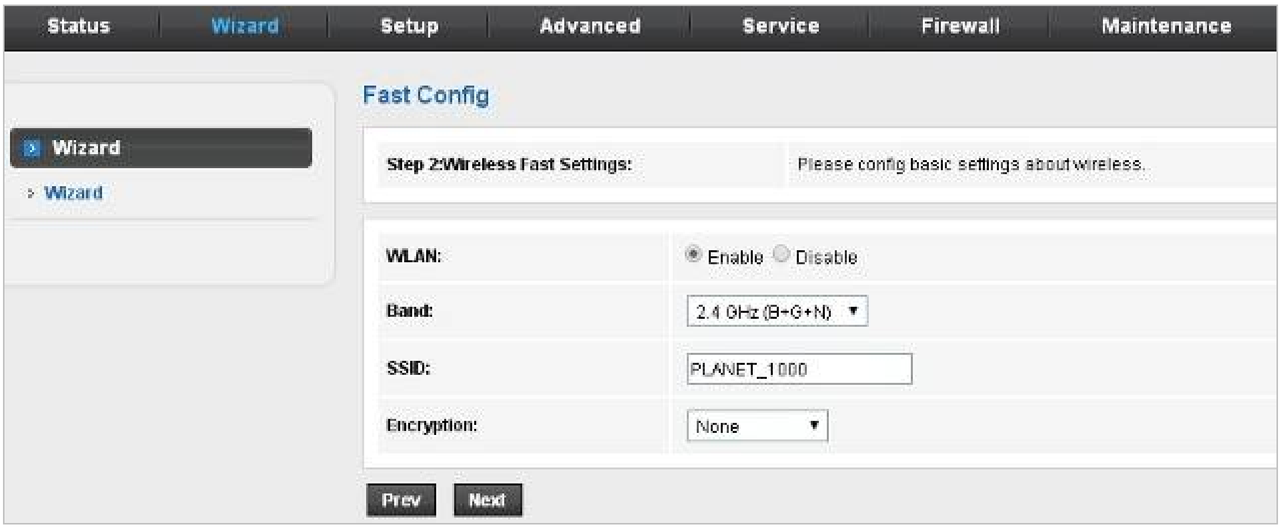
The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting:	Please select the wan connection mode

Connection Mode:	○ Bridge ● IPoE ○ PPPoE
IP Protocol:	Ipv4 ▼
802.1q:	○ Enable ● Disable
VLAN ID(1-4095):	
WAN IP Settings:	● Attain IP Automatically
	○ IP Manually:
Default Route:	● Enable ○ Disable
DNS Settings:	● Attain DNS Automatically
	○ Set DNS Manually :

Next

Figure 5-10 Wizard IPoE



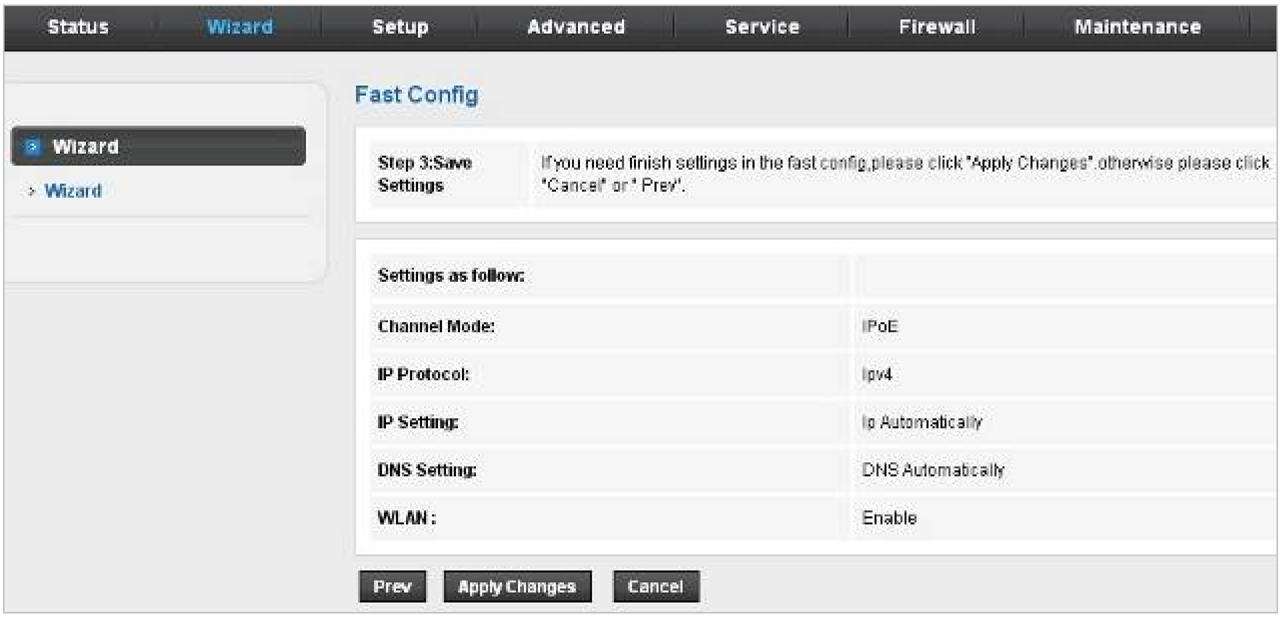
Fast Config

Step 2:Wireless Fast Settings: Please config basic settings about wireless.

WLAN:	● Enable ○ Disable
Band:	2.4 GHz (B+G+N)
SSID:	PLANET_1000
Encryption:	None

Figure 5-11 Wizard IPoE WLAN

And click **Apply changes** to save the configuration.



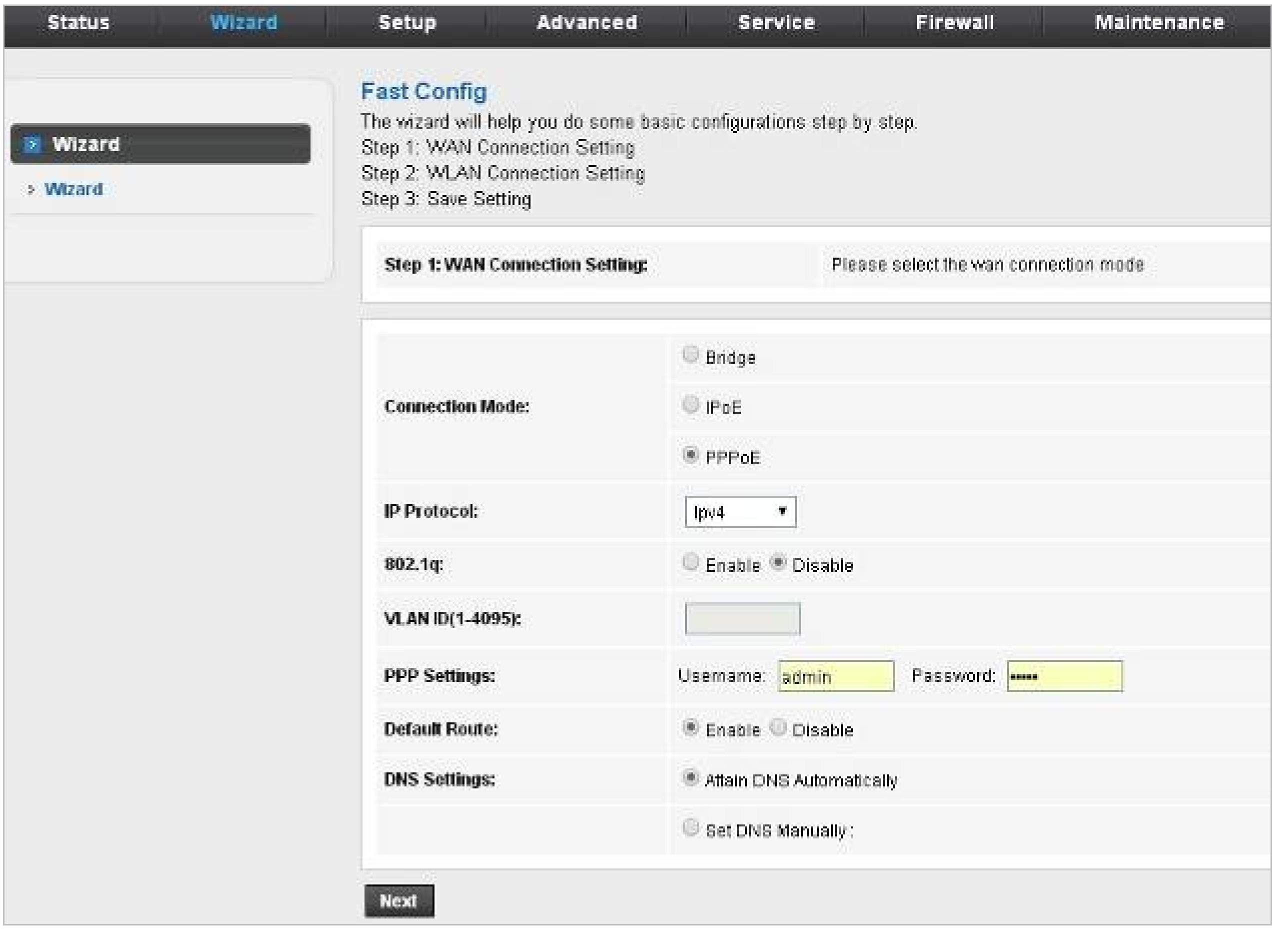
Fast Config

Step 3:Save Settings: If you need finish settings in the fast config,please click "Apply Changes",otherwise please click "Cancel" or " Prev".

Settings as follow:	
Channel Mode:	IPoE
IP Protocol:	Ipv4
IP Setting:	Ip Automatically
DNS Setting:	DNS Automatically
WLAN :	Enable

Figure 5-12 Wizard IPoE Save

5.2.3 PPPoE



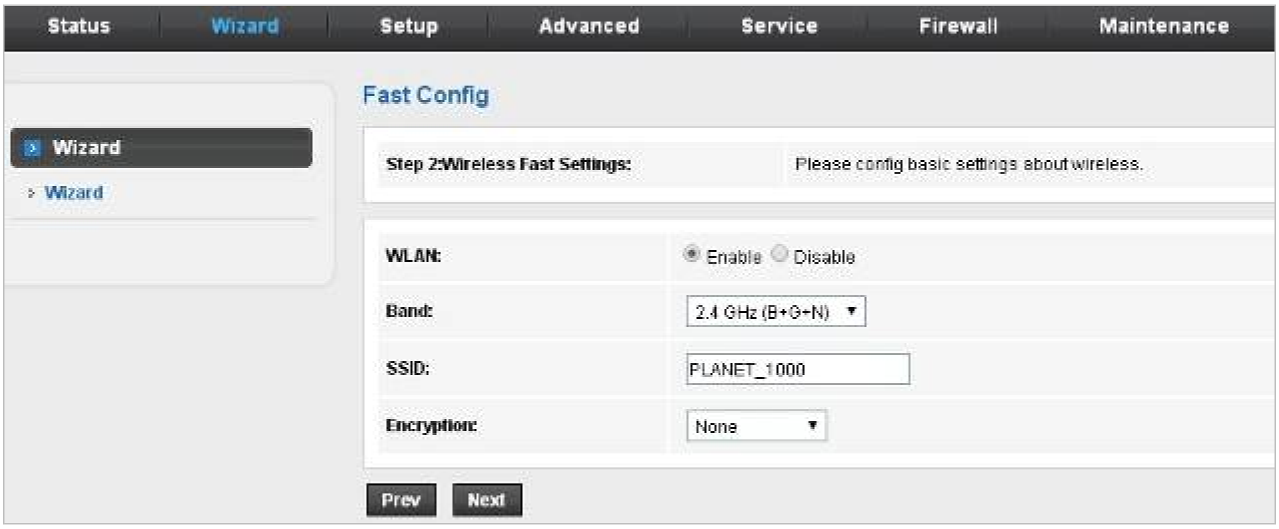
Fast Config

The wizard will help you do some basic configurations step by step.
Step 1: WAN Connection Setting
Step 2: WLAN Connection Setting
Step 3: Save Setting

Step 1: WAN Connection Setting:	Please select the wan connection mode

Connection Mode:	○ Bridge
	○ IPoE
	● PPPoE
IP Protocol:	Ipv4
802.1q:	○ Enable ● Disable
VLAN ID(1-4095):	
PPP Settings:	Username: admin Password: •••••
Default Route:	● Enable ○ Disable
DNS Settings:	● Attain DNS Automatically
	○ Set DNS Manually :

Figure 5-13 Wizard PPPoE

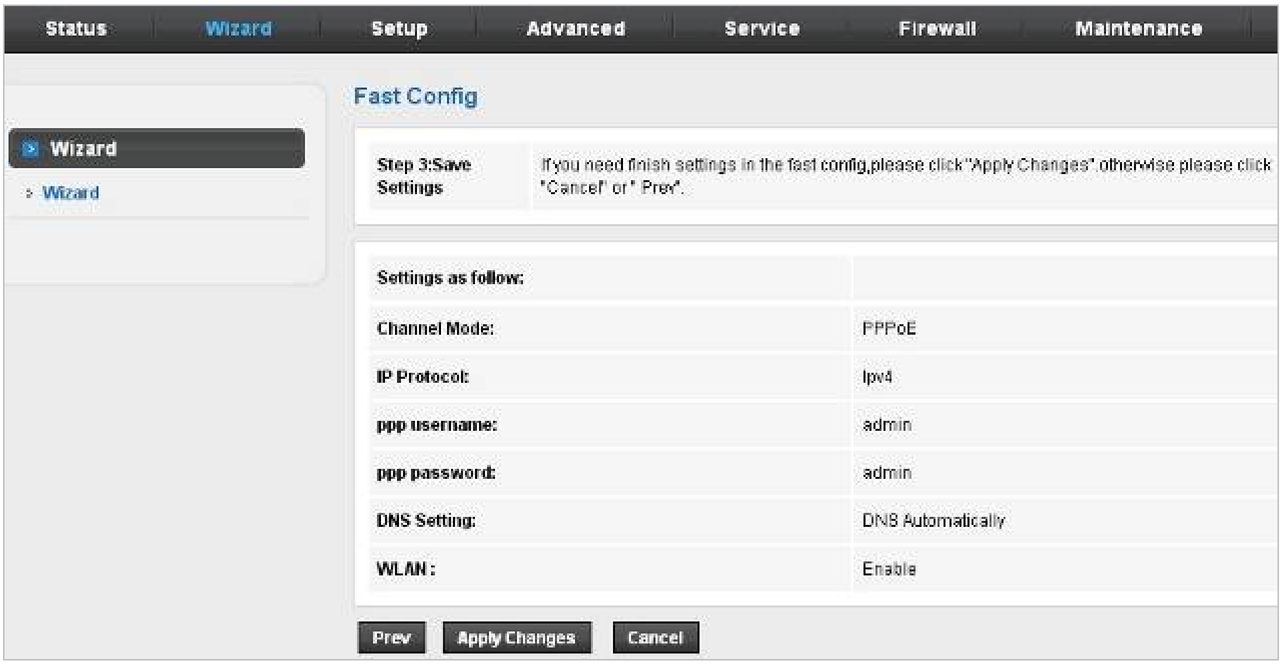


Fast Config

Step 2:Wireless Fast Settings:	Please config basic settings about wireless.

WLAN:	● Enable ○ Disable
Band:	2.4 GHz (B+G+N)
SSID:	PLANET_1000
Encryption:	None

Figure 5-14 Wizard PPPoE WLAN



Fast Config

Step 3:Save Settings	If you need finish settings in the fast config,please click "Apply Changes",otherwise please click "Cancel" or " Prev".

Settings as follow:	
Channel Mode:	PPPoE
IP Protocol:	Ipv4
ppp username:	admin
ppp password:	admin
DNS Setting:	DNS Automatically
WLAN :	Enable

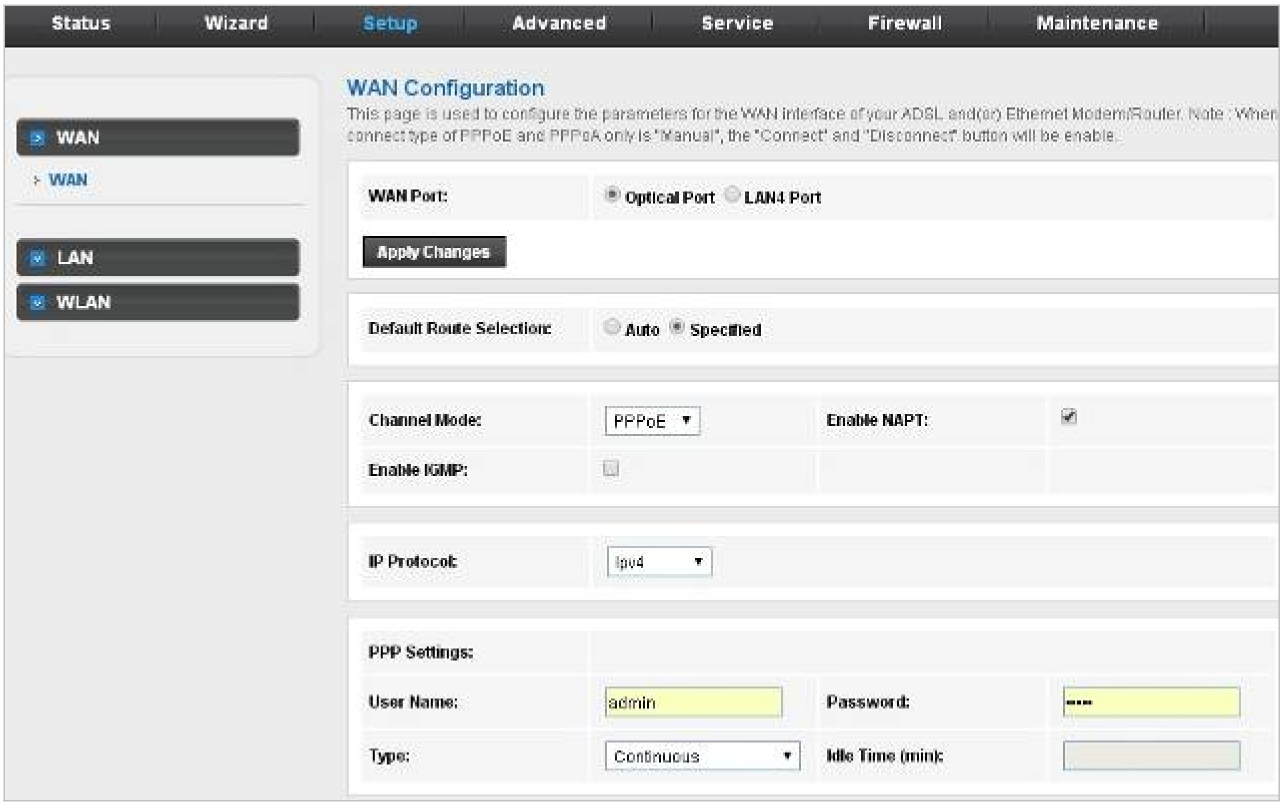
Figure 5-15 Wizard PPPoE Save

5.3 Setup

In the navigation bar, click Setup. The Setup page that is displayed contains WAN, LAN and WLAN.

5.3.1 WAN

Choose **Setup** > **WAN** and the page is displayed below.



WAN Configuration

This page is used to configure the parameters for the WAN interface of your ADSL and(or) Ethernet Modem/Router. Note : When connect type of PPPoE and PPPoA only is "Manual", the "Connect" and "Disconnect" button will be enable.

WAN Port: ● Optical Port ○ LAN4 Port

Default Route Selection: ○ Auto ● Specified

Channel Mode: PPPoE
Enable NAPT: ☑
Enable IGMP: □

IP Protocol: Ipv4

PPP Settings:
User Name: admin
Password: ----
Type: Continuous
Idle Time (min):

Figure 5-16 WAN

The following table describes the parameters:

Field	Description
WAN Port	You can select **Optical Port** or **LAN4 Port** as default WAN port.
Default Route Selection	You can select **Auto** or **Specified**.
Channel Mode	You can choose **PPPoE**, **Bridge** or **IPoE**.
Enable NAPT	Select it to enable Network Address Port Translation (NAPT) function. If you do not select it and you want to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, it is enabled.
Enable IGMP	You can enable or disable Internet Group Management Protocol (IGMP) function.

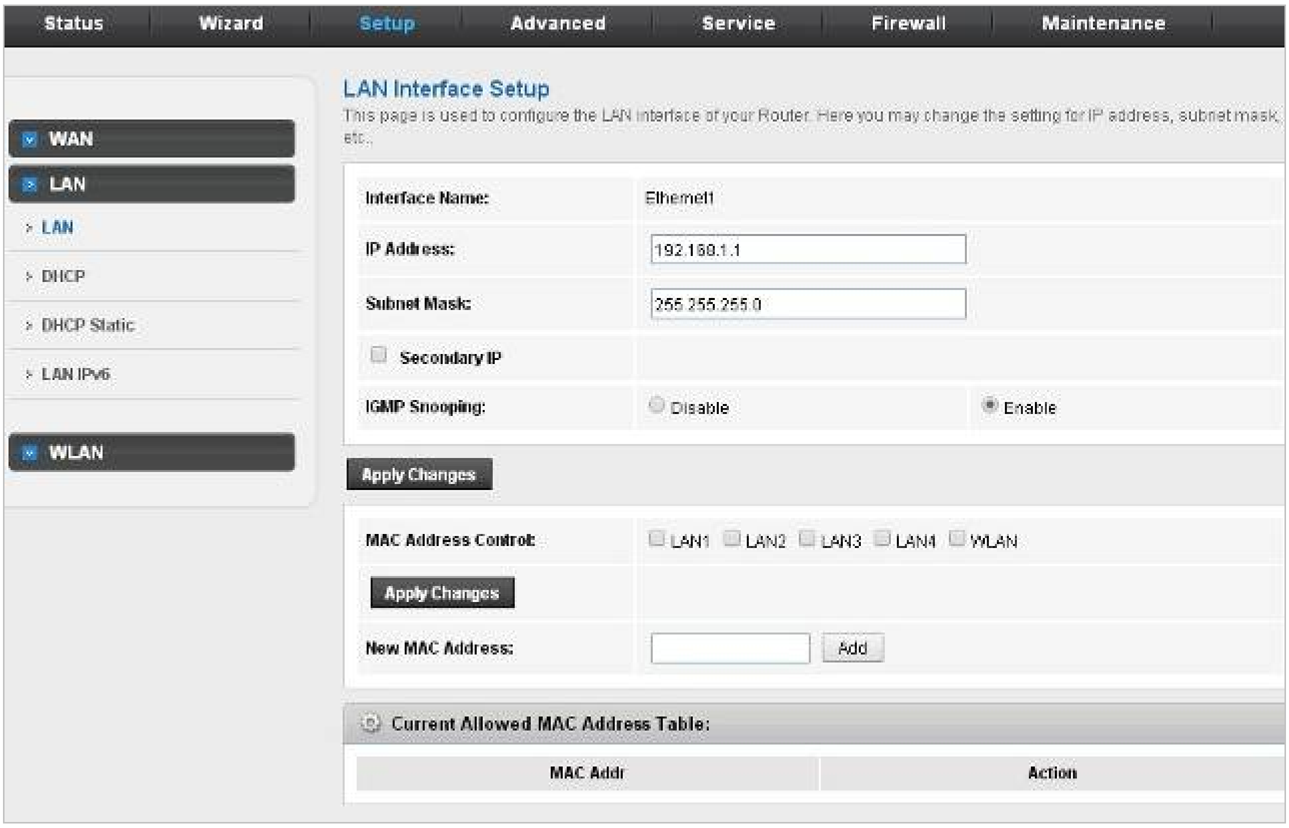
IP Protocol	You can select **IPv4**, **IPv4/IPv6** or **IPv6**.
PPP Settings	
User Name	Enter the correct user name for PPP dial-up, which is provided by your ISP.
Password	Enter the correct password for PPP dial-up, which is provided by your ISP.
Type	You can choose **Continuous**, **Connect on Demand**, or **Manual**.
Idle Time (min)	To set the type to Connect on Demand, you need to enter the idle timeout time. Within the preset minutes, if the router does not detect the flow of the user continuously, the router automatically disconnects the PPPoE connection.
WAN IP Settings	
Type	You can choose **Fixed IP** or **DHCP**. ● To select Fixed IP, you should enter the local IP address, remote IP address and subnet mask. ● To select DHCP, the router is a DHCP client and the WAN IP address is assigned by the remote DHCP server.
Local IP Address	Enter the IP address of WAN interface provided by your ISP.
Remote IP Address	Enter the default gateway of WAN interface provided by your ISP.
Netmask	Enter the subnet mask of the local IP address.
Default Route	Select **Disable**, **Enable** or **Auto**. The default setting is **Enable**.
Unnumbered	Select this checkbox to enable IP unnumbered function.
WAN Interfaces Table	This table shows the existing WAN settings. The maximum item of this table is eight.

5.3.2 LAN

Choose Setup > **LAN**. The **LAN** page that is displayed contains **LAN, DHCP, DHCP Static and LAN IPv6**.

5.3.2.1 LAN

Click **LAN** in the left pane and the page shown in the following figure appears. On this page, you can change IP address of the router. The default IP address is **192.168.1.1**, which is the private IP address of the router.



LAN Interface Setup

This page is used to configure the LAN interface of your Router. Here you may change the setting for IP address, subnet mask, etc..

Interface Name: Ethernet1

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

□ Secondary IP

IGMP Snooping: ○ Disable ● Enable

MAC Address Control: □ LAN1 □ LAN2 □ LAN3 □ LAN4 □ WLAN

New MAC Address:

Current Allowed MAC Address Table:

MAC Addr	Action

Figure 5-17 LAN

The following table describes the parameters:

Field	Description
IP Address	The IP address of your LAN hosts is used to identify the device's LAN port.
Subnet Mask	Enter the subnet mask of LAN interface.
Secondary IP	Select it to enable/disable a secondary LAN IP address. The two LAN IP addresses must be in the different network.
IGMP Snooping	**Enable** or **Disable** the IGMP snooping function for the multiple bridged LAN ports.
MAC Address Control	It is the access control based on MAC address. Select LAN1, LAN2, LAN3, LAN4, WLAN and the host whose MAC address listed in the Currently Allowed MAC Address Table can access the device. Then

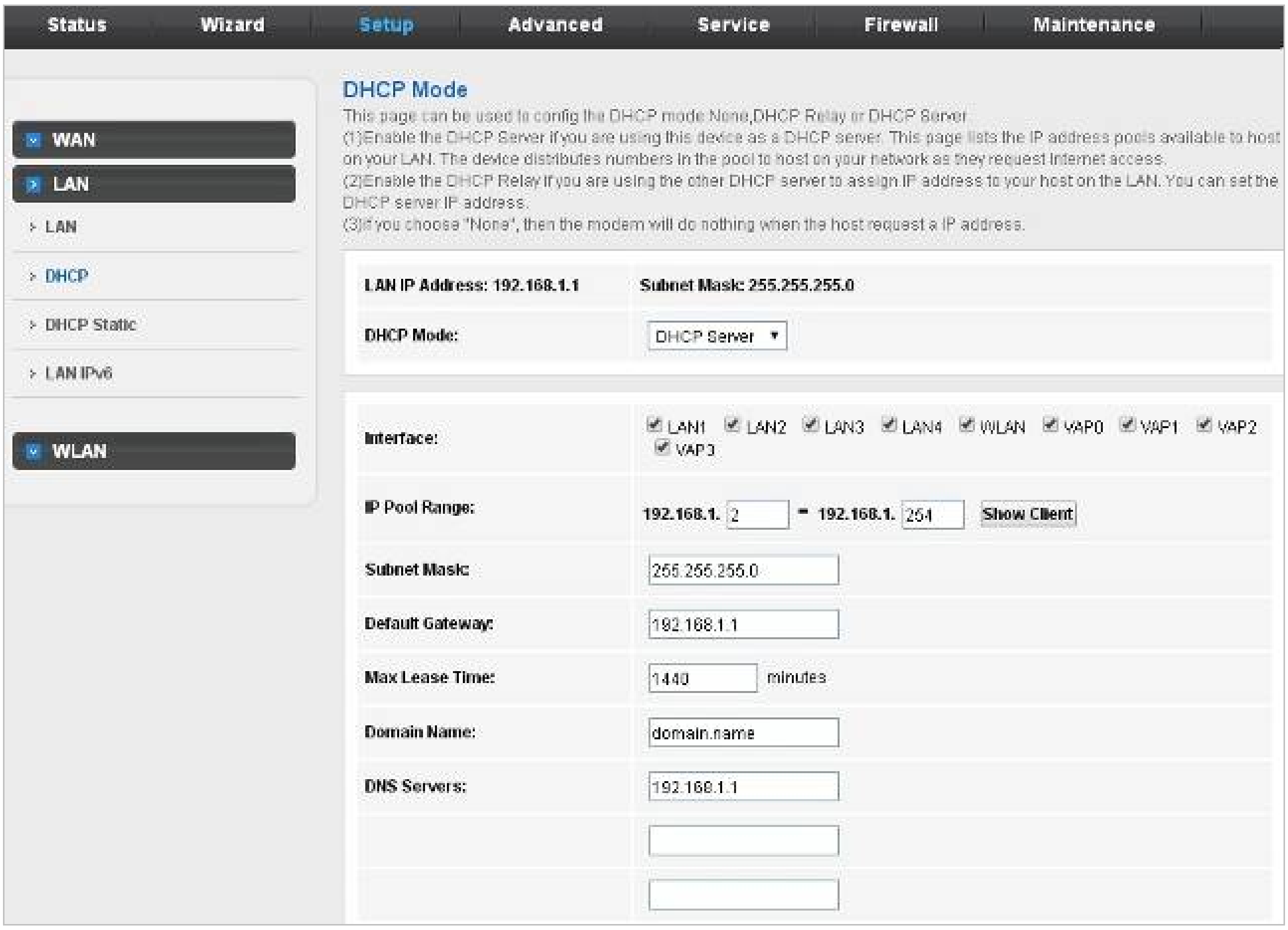
	click “**Apply Changes**” to save the new settings.
New MAC Address	Enter MAC address and then click **Add** to add a new MAC address.

5.3.2.2 DHCP

Dynamic Host Configuration Protocol (DHCP) allows the individual PC to obtain the TCP/IP configuration from the centralized DHCP server. You can configure this router as a DHCP server or disable it. The DHCP server can assign IP address, IP default gateway, and DNS server to DHCP clients. This router can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from an actual real DHCP server to clients. You can enable or disable DHCP server.

- **DHCP Server**

Click **DHCP** in the left pane and the page shown in the following figure appears.



DHCP Mode

This page can be used to config the DHCP mode None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to host on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address.
(3)If you choose "None", then the modem will do nothing when the host request a IP address.

LAN IP Address: 192.168.1.1   Subnet Mask: 255.255.255.0

DHCP Mode: DHCP Server

Interface: ☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN ☑ VAP0 ☑ VAP1 ☑ VAP2 ☑ VAP3

IP Pool Range: 192.168.1. 2 - 192.168.1. 254

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Max Lease Time: 1440 minutes

Domain Name: domain.name

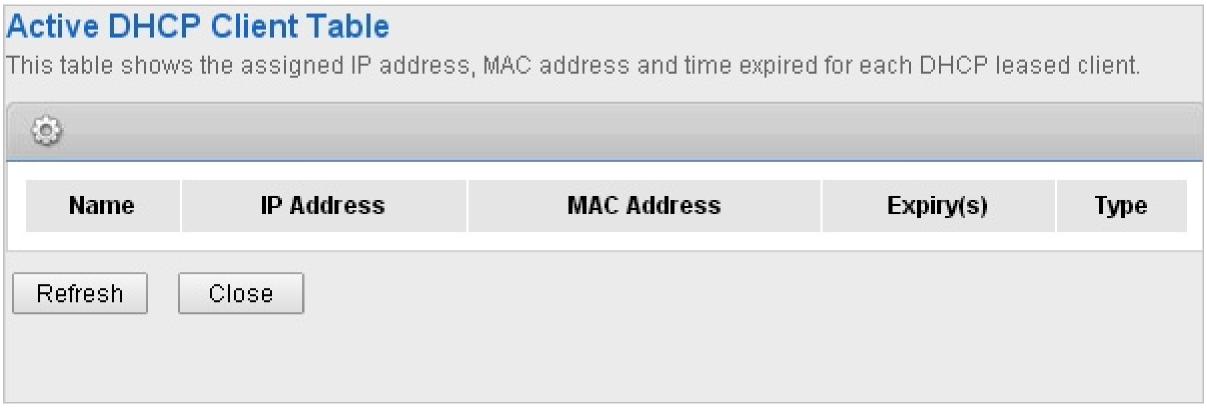
DNS Servers: 192.168.1.1

Figure 5-18 DHCP

The following table describes the parameters:

Field	Description
DHCP Mode	You can choose **None**, **DHCP Relay** or **DHCP Server**. If set to DHCP Server, the router can assign IP addresses, IP default gateway and DNS Servers to the host in Windows XP, Windows 7 and other operating systems that support the DHCP client.
Interface	By default, all ports are selected; click it to unselect and those ports cannot function with the IP address.
IP Pool Range	Specify the lowest and highest addresses in the pool. It specifies the first IP address in the IP address pool. The router assigns IP address based on the IP pool range to the host.
Show Client	Click it and the **Active DHCP Client Table** appears. It shows IP addresses assigned to clients.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the default gateway of the IP address pool.
Max. Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the device using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 1440 minutes (1 day).
Domain Name	Domain Name is the most recognized system for assigning addresses to Internet web servers.
DNS Servers	You can configure the DNS server IP addresses for DNS Relay.

Click **Show Client** on the **DHCP Mode** page and the page shown in the following figure appears. You can view the IP address assigned to each DHCP client.



Active DHCP Client Table

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.

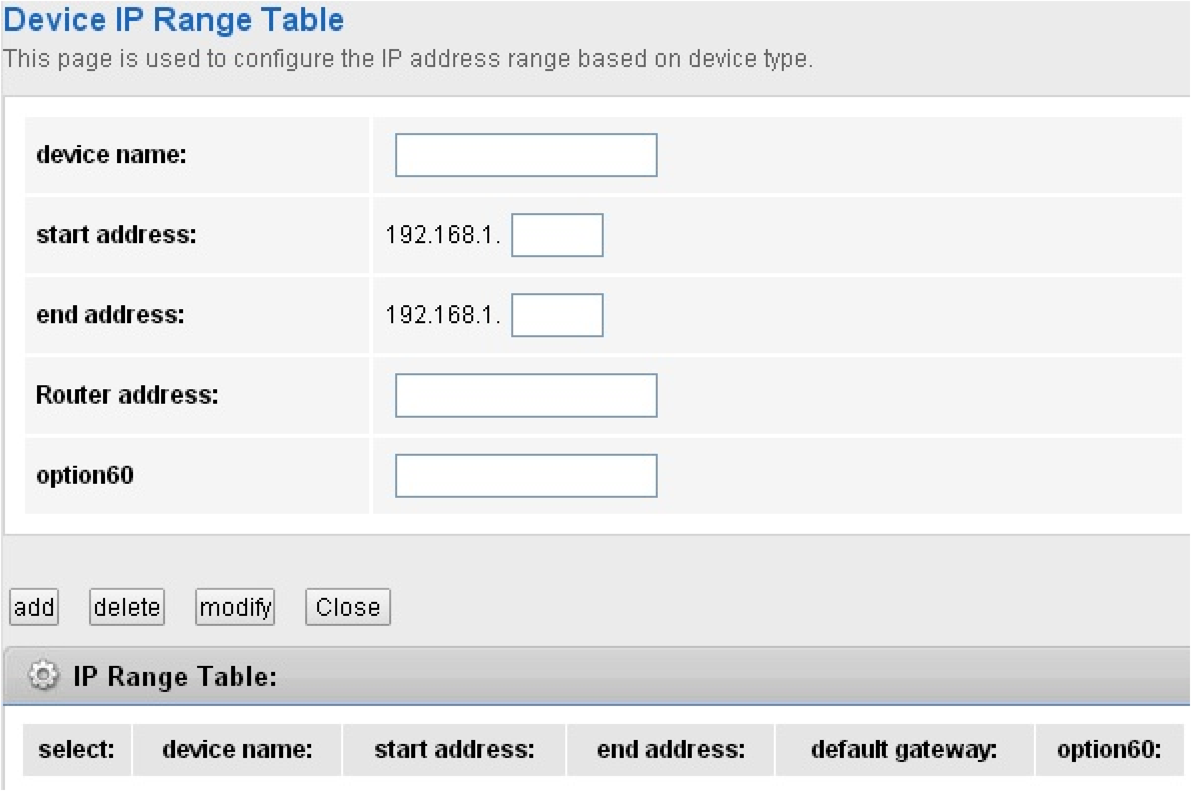
Name	IP Address	MAC Address	Expiry(s)	Type

Figure 5-19 DHCP Table

The following table describes the parameters:

Field	Description
IP Address	It displays the IP address assigned to the DHCP client from the router.
MAC Address	It displays the MAC address of the DHCP client. Each Ethernet device has a unique MAC address. The MAC address is assigned at the factory and it consists of six pairs of hexadecimal character, for example, A8-F7-E0-00-11-22.
Expiry	It displays the lease time. The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.
Refresh	Click it to refresh this page.
Close	Click it to close this page.

Click **Set Vendor Class IP Range** on the **DHCP Mode** page and the page as shown in the following figure appears. On this page, you can configure the IP address range based on the device type.



Device IP Range Table

This page is used to configure the IP address range based on device type.

device name:	
start address:	192.168.1.
end address:	192.168.1.
Router address:	
option60	

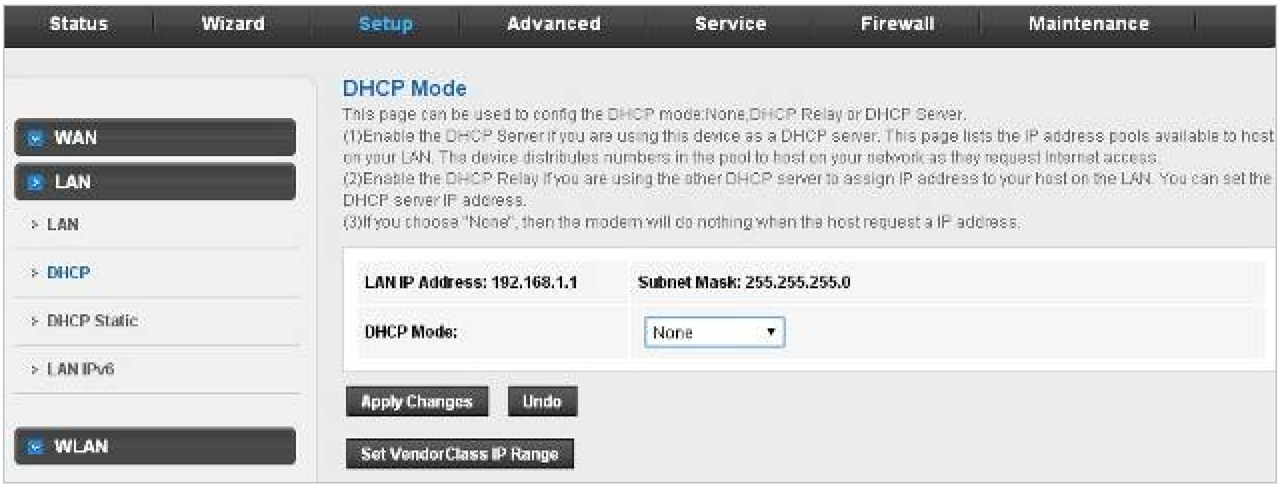
IP Range Table:

select:	device name:	start address:	end address:	default gateway:	option60:

Figure 5-20 Device IP Range Table

- **None**

In the **DHCP Mode** field, choose **None** and the page shown in the following figure appears.



DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to host on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address.
(3)If you choose "None", then the modem will do nothing when the host request a IP address.

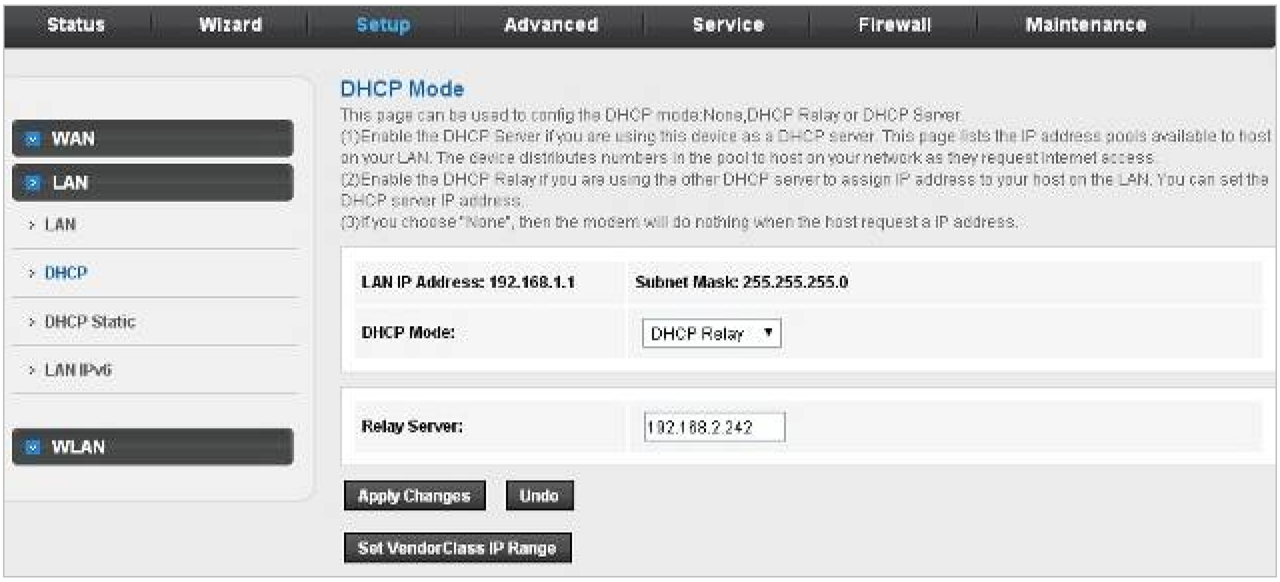
LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP Mode: None

Figure 5-21 DHCP None

■ DHCP Relay

In the **DHCP Mode** field, choose **DHCP Relay** and the page shown in the following figure appears.



DHCP Mode

This page can be used to config the DHCP mode:None,DHCP Relay or DHCP Server.
(1)Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to host on your LAN. The device distributes numbers in the pool to host on your network as they request Internet access.
(2)Enable the DHCP Relay if you are using the other DHCP server to assign IP address to your host on the LAN. You can set the DHCP server IP address.
(3)If you choose "None", then the modem will do nothing when the host request a IP address.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

DHCP Mode: DHCP Relay

Relay Server: 192.168.2.242

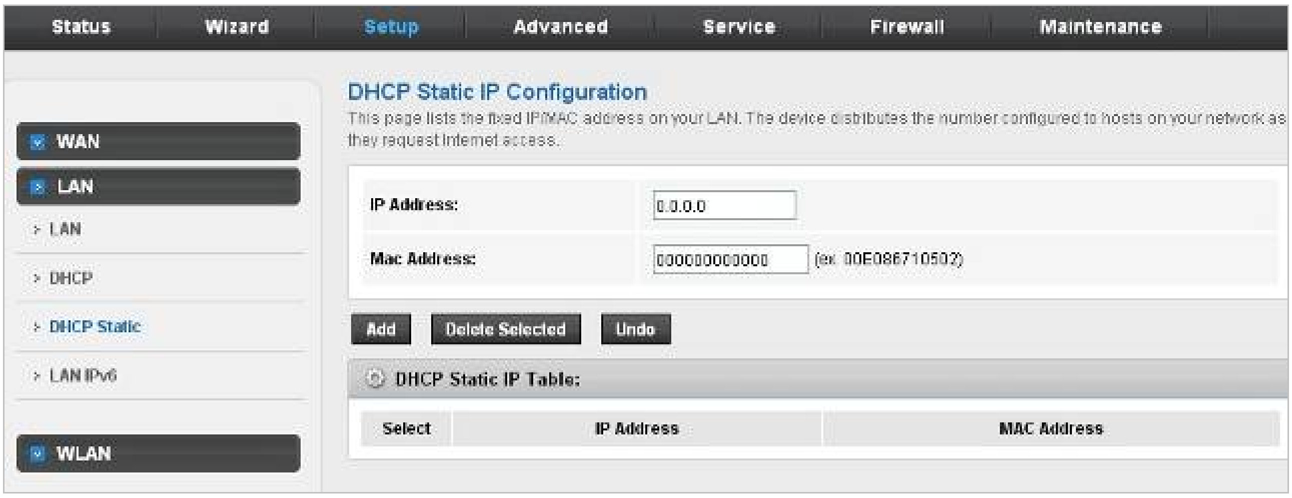
Figure 5-22 DHCP Relay

The following table describes the parameters:

Field	Description
DHCP Mode	If set to **DHCP Relay**, the router acts as a surrogate DHCP Server and relays the DHCP requests and responses between the remote server and the client.
Relay Server	Enter the DHCP server address provided by your ISP.
Apply Changes	Click it to save the settings on this page.
Undo	Click it to refresh this page.

5.3.2.3 DHCP Static

Click **DHCP Static** in the left pane and the page shown in the following figure appears. You can assign the IP addresses on the LAN to the specific individual PCs based on their MAC address.



DHCP Static IP Configuration

This page lists the fixed IP/MAC address on your LAN. The device distributes the number configured to hosts on your network as they request Internet access.

IP Address: 0.0.0.0

Mac Address: 000000000000 (ex. 00E086710502)

DHCP Static IP Table:

Select	IP Address	MAC Address

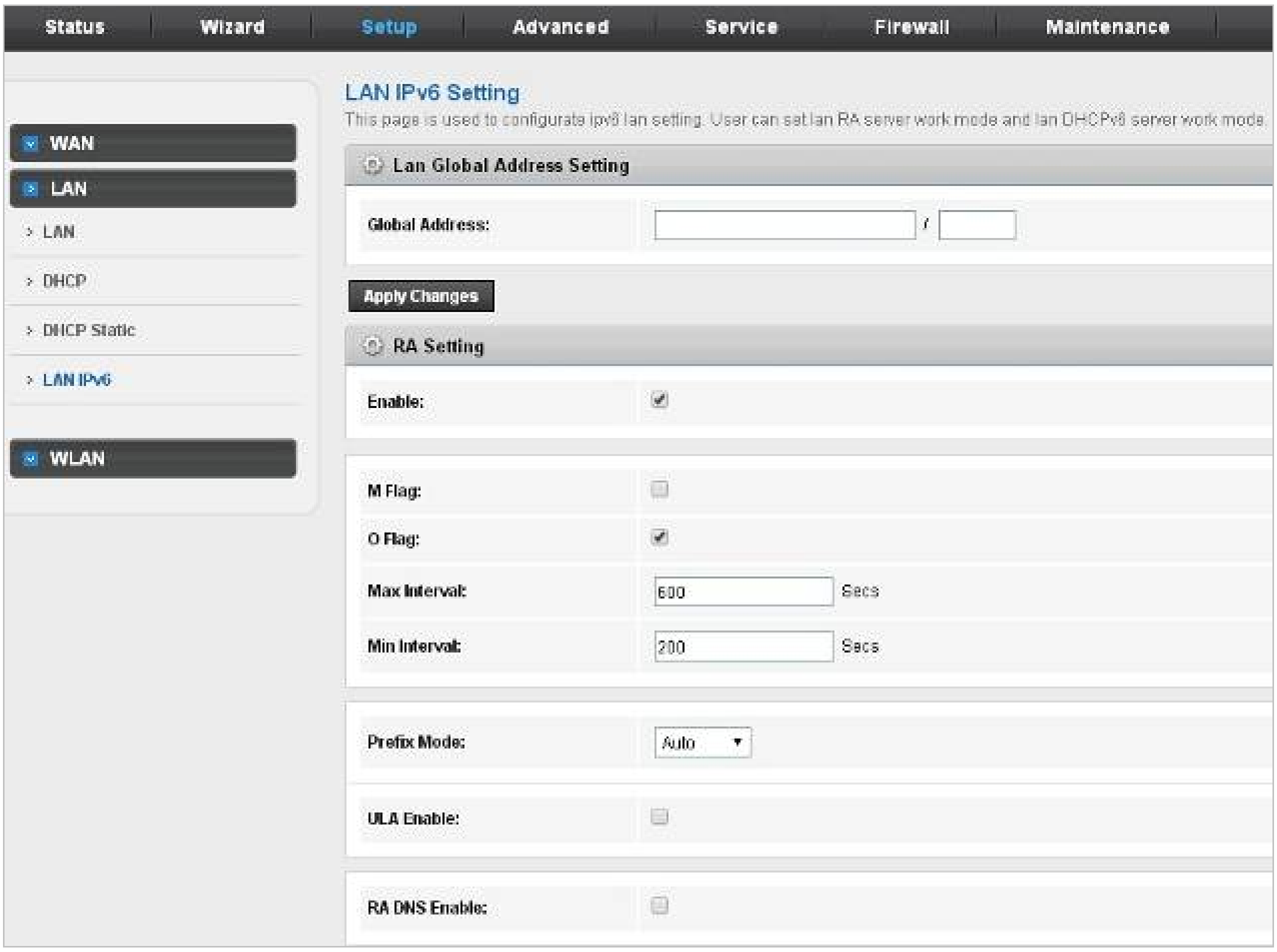
Figure 5-23 DHCP Static

The following table describes the parameters:

Field	Description
IP Address	Enter the specified IP address in the IP pool range, which is assigned to the host.
MAC Address	Enter the MAC address of a host on the LAN.
Add	After entering the IP address and MAC address, click it. A row will be added in the **DHCP Static IP Table**.
Delete Selected	Select a row in the **DHCP Static IP Table**; then click it and this row is deleted.
Undo	Click it to refresh this page.
DHCP Static IP Table	It shows the assigned IP address based on the MAC address.

5.3.2.4 LAN IPv6

On this page, you can configure the LAN IPv6. Choose **Setup** > **LAN** > **LAN IPv6**. The **IPv6 LAN setting** page as shown in the following figure appears.



LAN IPv6 Setting

This page is used to configurate ipv6 lan setting. User can set lan RA server work mode and lan DHCPv6 server work mode.

Lan Global Address Setting

Global Address: /

RA Setting

Enable: ☑

M Flag: □

O Flag: ☑

Max Interval: 600 Secs

Min Interval: 200 Secs

Prefix Mode: Auto

ULA Enable: □

RA DNS Enable: □

Figure 5-24 LAN IPv6

The following table describes the parameters:

LAN Global Address Setting

Field	Description
Global Address	Specify the LAN global IPv6 address; may be assigned by ISP.

RA Setting

Field	Description
Enable	Enable or disable the Router Advertisement feature.
M Flag	Enable or disable the “Managed address configuration” flag in RA packet.
O Flag	Enable or disable the “other configuration” flag in RA packet.
Max Interval	Maximum sending time interval.
Min Interval	Minimum sending time interval.
Prefix Mode	Specify the RA feature prefix mode

	Auto: The RA prefix will use WAN DHCP-pd prefix **Manual:** User will specify the **Prefix Address**, **Length**, **Preferred Time** and **Valid Time**.
ULA	Unique Local Address. Enable/Disable the feature to access.
RA DNS Enable	Enable/Disable the feature to access.

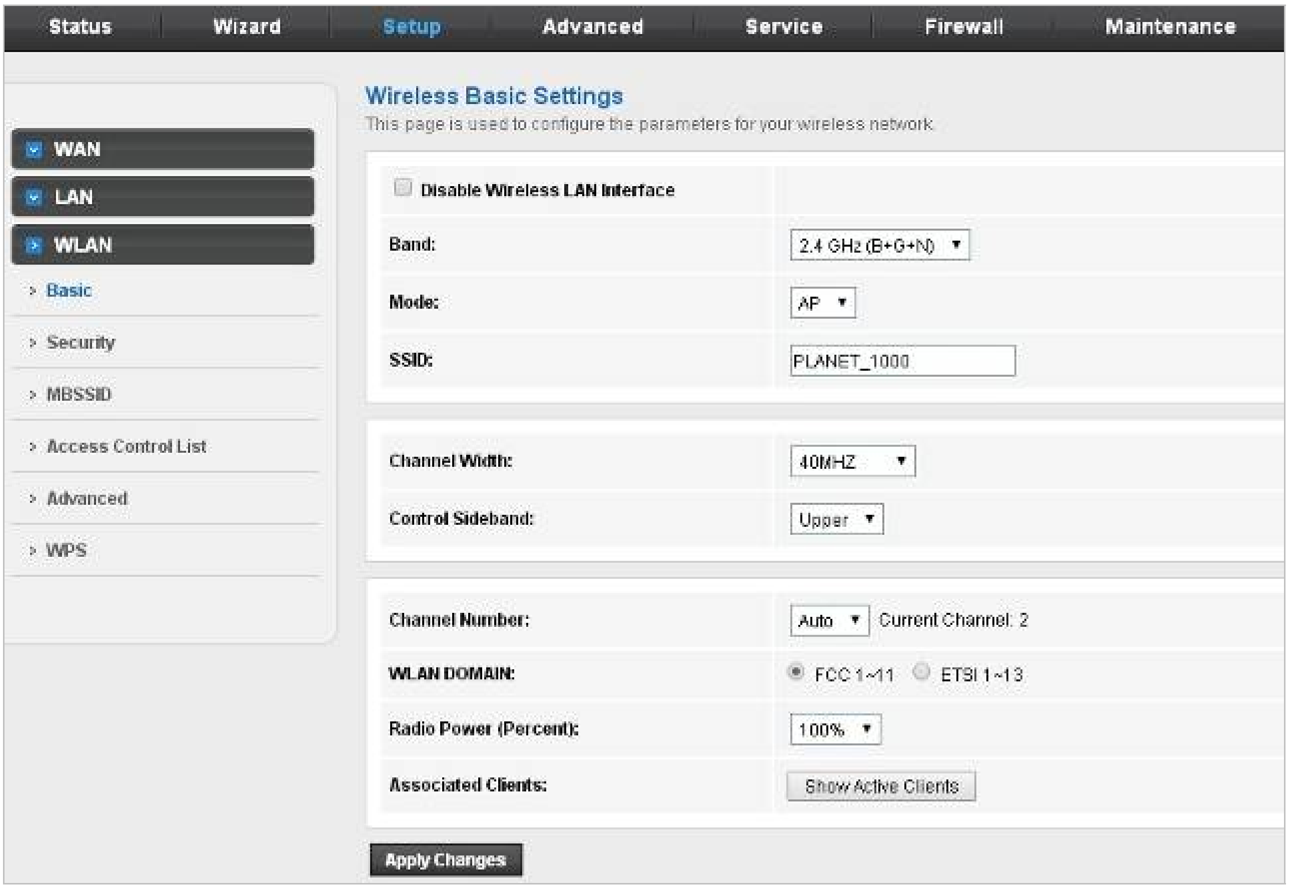
DHCPv6 Setting

Field	Description
DHCPv6 Mode	Select the Mode to **None**, **Manual Mode** or **Auto Mode**.
IPv6 Address Suffix Pool	Enter the IPv6 address.
IPv6 DNS Mode	Select the Mode to **Auto** or **Manual**.

5.3.3 WLAN

5.3.3.1 Basic

This page contains all the wireless basic settings. Most users will be able to configure the wireless portion and get it working properly using the setting on this screen.



Wireless Basic Settings

This page is used to configure the parameters for your wireless network.

□ Disable Wireless LAN Interface	
Band:	2.4 GHz (B+G+N)
Mode:	AP
SSID:	PLANET_1000
Channel Width:	40MHZ
Control Sideband:	Upper
Channel Number:	Auto Current Channel: 2
WLAN DOMAIN:	● FCC 1~11 ○ ETSI 1~13
Radio Power (Percent):	100%
Associated Clients:	Show Active Clients

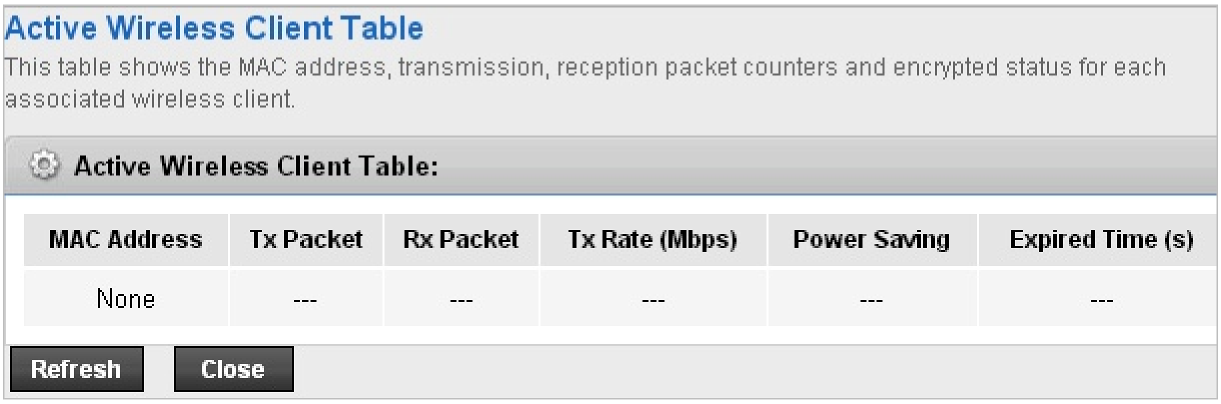
Figure 5-25 WLAN

The following table describes the parameters:

Field	Description
Disable Wireless LAN Interface	Enable/Disable the wireless function for FRT-415N.
Band	Select the appropriate band from the list provided to correspond with your network setting.
Mode	Select AP Mode.
SSID	The Service Set Identifier (SSID) or network name. It is case sensitive and must not exceed 32 characters, which may be any keyboard character. The mobile wireless stations will select the same SSID to be able to communicate with your fiber router.
Channel Width	Select channel width to **20MHz**, **40MHz** or **20/40MHz**.

Control Sideband	Select **Upper** or **Lower** sideband.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. You will assign a different channel for each AP to avoid signal interference.
WLAN Domain	Select **FCC 1~11** or **ETSI 1~13**.
Radio Power (Percent)	100%, 80%, 50%, 25%, 10%.
Associated Clients	Click it to see the clients currently associated with FRT-415N.

Click **Show Active Client** and the page shown in the following figure appears. You can view the information of the clients connected to the fiber router.



Active Wireless Client Table

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client.

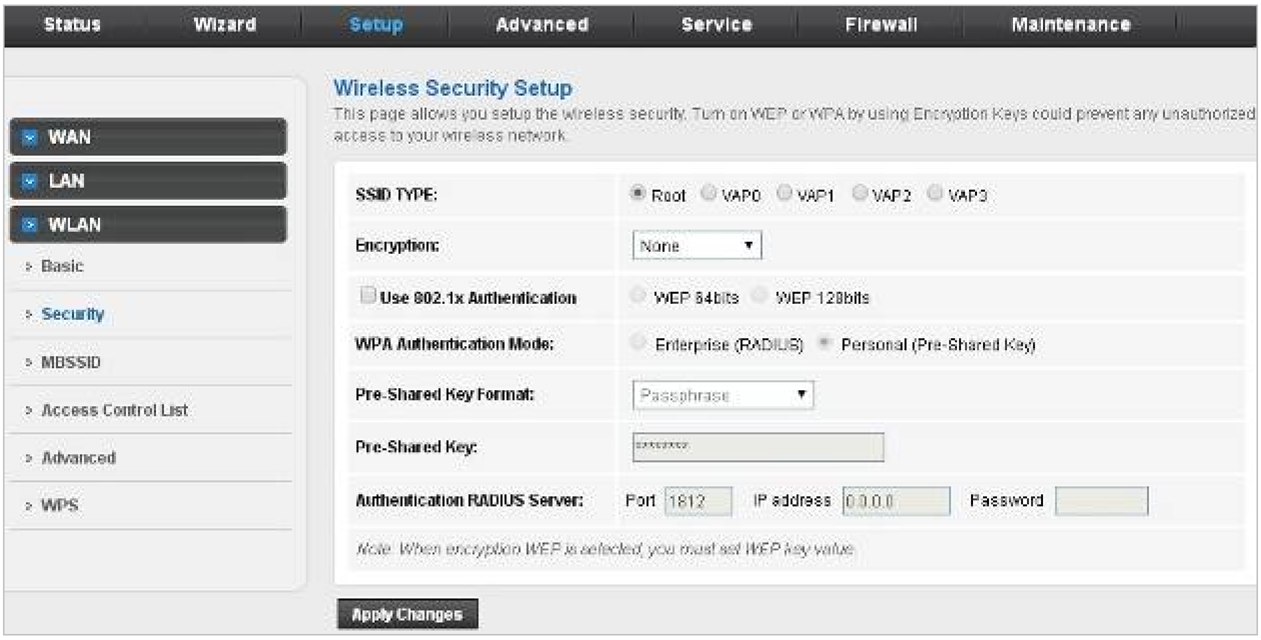
Active Wireless Client Table:

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Figure 5-26 Active Wireless Client Table

5.3.3.2 Security

This screen allows you to set up the wireless security. Turn on WEP or WPA by using encryption keys that could prevent any unauthorized access to your WLAN.



Wireless Security Setup

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID TYPE:	● Root ○ VAP0 ○ VAP1 ○ VAP2 ○ VAP3
Encryption:	None
□ Use 802.1x Authentication	○ WEP 64bits ○ WEP 128bits
WPA Authentication Mode:	○ Enterprise (RADIUS) ● Personal (Pre-Shared Key)
Pre-Shared Key Format:	Passphrase
Pre-Shared Key:	********
Authentication RADIUS Server:	Port 1812 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

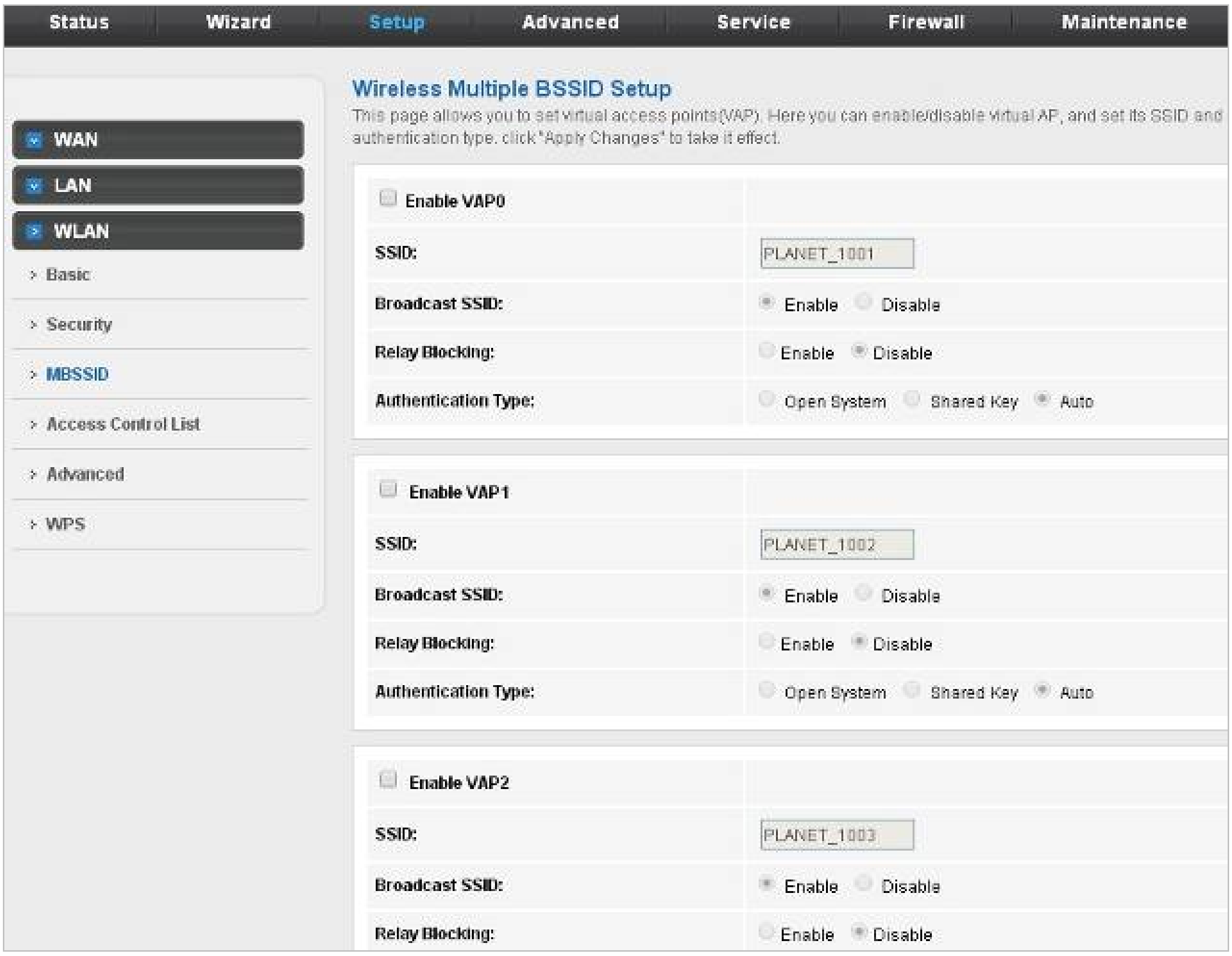
Figure 5-27 Wireless Security

The following table describes the parameters:

Field	Description
SSID Type	Select the SSID Type.
Encryption	There are 4 types of security to be selected. To secure your WLAN, it's strongly recommended to enable this feature. **WEP:** Make sure that all wireless devices on your network are using the same encryption level and key. **WPA/WPA2 (TKIP):** WPA/WPA2 uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers. **WPA/WPA2 (AES):** WPA/WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilizes a symmetric 128-bit block data encryption. **WPA2 Mixed:** The AP supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.
Use 802.1x Authentication	Check it to enable 802.1x authentications. This option is selected only when the "Encryption" is chosen to either None or WEP. If the "Encryption" is WEP, you need to further select the WEP key length to be either WEP 64 character or WEP 128 character.
WPA Authentication Mode	There are 2 types of authentication mode for WPA. **Enterprise (RADIUS):** WPA RADIUS uses an external RADIUS server to perform user authentication. To use WPA RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. **Personal (Pre-Shared Key):** Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively.
Pre-Shared Key Format	**Passphrase:** Select this to enter the Pre-Shared Key secret as user-friendly textual secret. **Hex (64 characters):** Select this to enter the Pre-Shared Key secret as hexadecimal secret.
Pre-Shared Key	Specify the shared secret used by this Pre-Shared Key. If the "Pre-Shared Key Format" is specified as PassPhrase, then it indicates a passphrase of 8 to 64 character long or 64-hexadecimal number.
Authentication RADIUS Server	If the WPA-RADIUS is selected in "WPA Authentication Mode", the port (default is 1812), IP address and password of external RADIUS server are specified here.

5.3.3.3 MBSSID

This screen allows you to do the wireless multiple SSIDs setup.



Wireless Multiple BSSID Setup

This page allows you to set virtual access points(VAP). Here you can enable/disable virtual AP, and set its SSID and authentication type. click "Apply Changes" to take it effect.

□ Enable VAP0	
SSID:	PLANET_1001
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

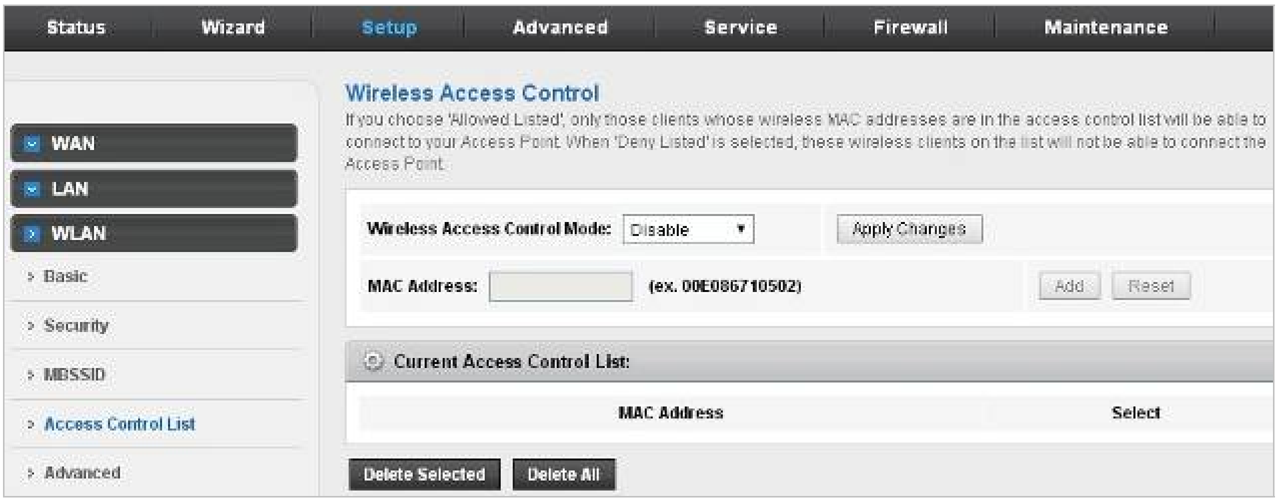
□ Enable VAP1	
SSID:	PLANET_1002
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable
Authentication Type:	○ Open System ○ Shared Key ● Auto

□ Enable VAP2	
SSID:	PLANET_1003
Broadcast SSID:	● Enable ○ Disable
Relay Blocking:	○ Enable ● Disable

Figure 5-28 Wireless MBSSID

5.3.3.4 Access Control List

This page allows administrator to have access control by entering MAC address of client stations. When this function is enabled, MAC address can be added to access control list and only those clients whose wireless MAC address are in the access control list will be able to connect to your FRT-415N.



Wireless Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode: Disable ▾ Apply Changes

MAC Address: (ex. 00E086710502) Add Reset

Current Access Control List:

MAC Address	Select

Delete Selected Delete All

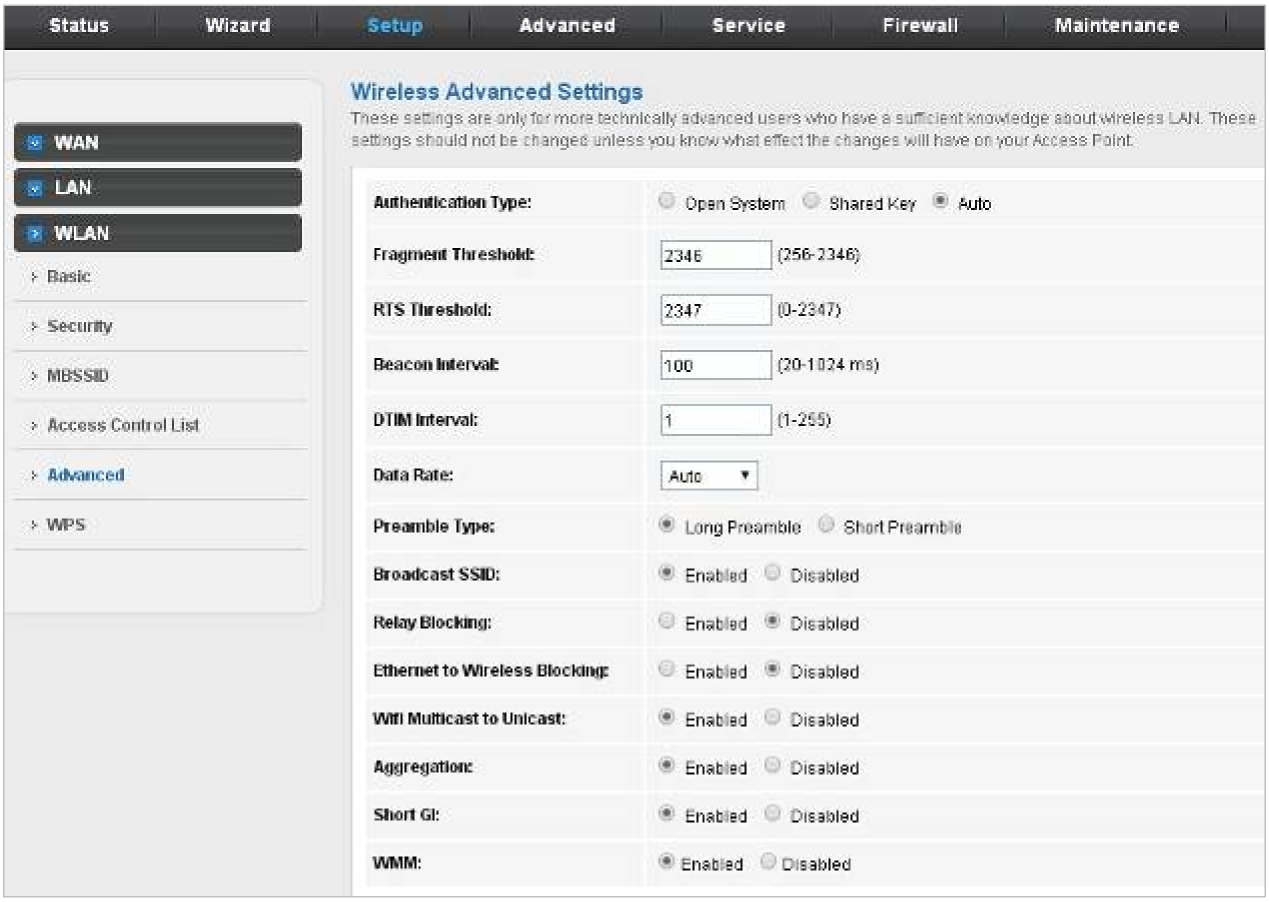
Figure 5-29 Wireless Access Control

The following table describes the parameters:

Field	Description
Wireless Access Control Mode	The Selections are: **Disable:** Disable the wireless ACL feature. **Allow Listed:** When this option is selected, no wireless clients except those whose MAC addresses are in the current access control list will be able to connect (to this device). **Deny Listed:** When this option is selected, all wireless clients except those whose MAC addresses are in the current access control list will not be able to connect (to this device).
MAC Address	Enter client MAC address.
Apply Changes	Click Apply Changes to add new settings; then it restarts.
Add	Click to add MAC address to the Current Access Control List.
Reset	Clear the settings.
Delete Selected	Select the rows to be deleted from Current Access Control List.
Delete All	Flush the list.

5.3.3.5 Advanced

This page allows advanced users who have sufficient knowledge of wireless LAN. These settings will not be changed unless you know exactly what will happen for the changes you made on your fiber router.



Wireless Advanced Settings

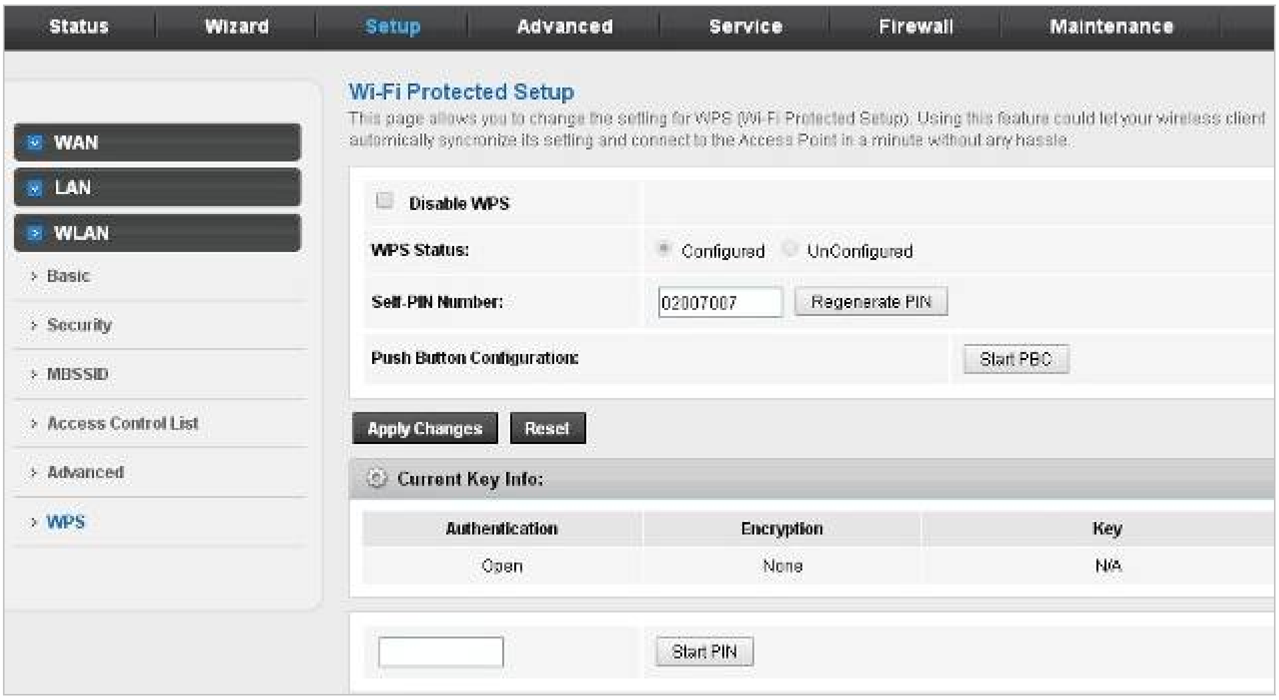
These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

Authentication Type:	○ Open System ○ Shared Key ● Auto
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1024 ms)
DTIM Interval:	1 (1-255)
Data Rate:	Auto
Preamble Type:	● Long Preamble ○ Short Preamble
Broadcast SSID:	● Enabled ○ Disabled
Relay Blocking:	○ Enabled ● Disabled
Ethernet to Wireless Blocking:	○ Enabled ● Disabled
Wifi Multicast to Unicast:	● Enabled ○ Disabled
Aggregation:	● Enabled ○ Disabled
Short GI:	● Enabled ○ Disabled
WMM:	● Enabled ○ Disabled

Figure 5-30 Wireless Advanced

5.3.3.6 WPS

Wi-Fi Protected Setup (WPS) is a push-button or pin to simplify a secure network set-up.



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automically syncronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status: ● Configured ○ UnConfigured

Self-PIN Number: 02007007

Push Button Configuration:

Current Key Info:

Authentication	Encryption	Key
Open	None	N/A

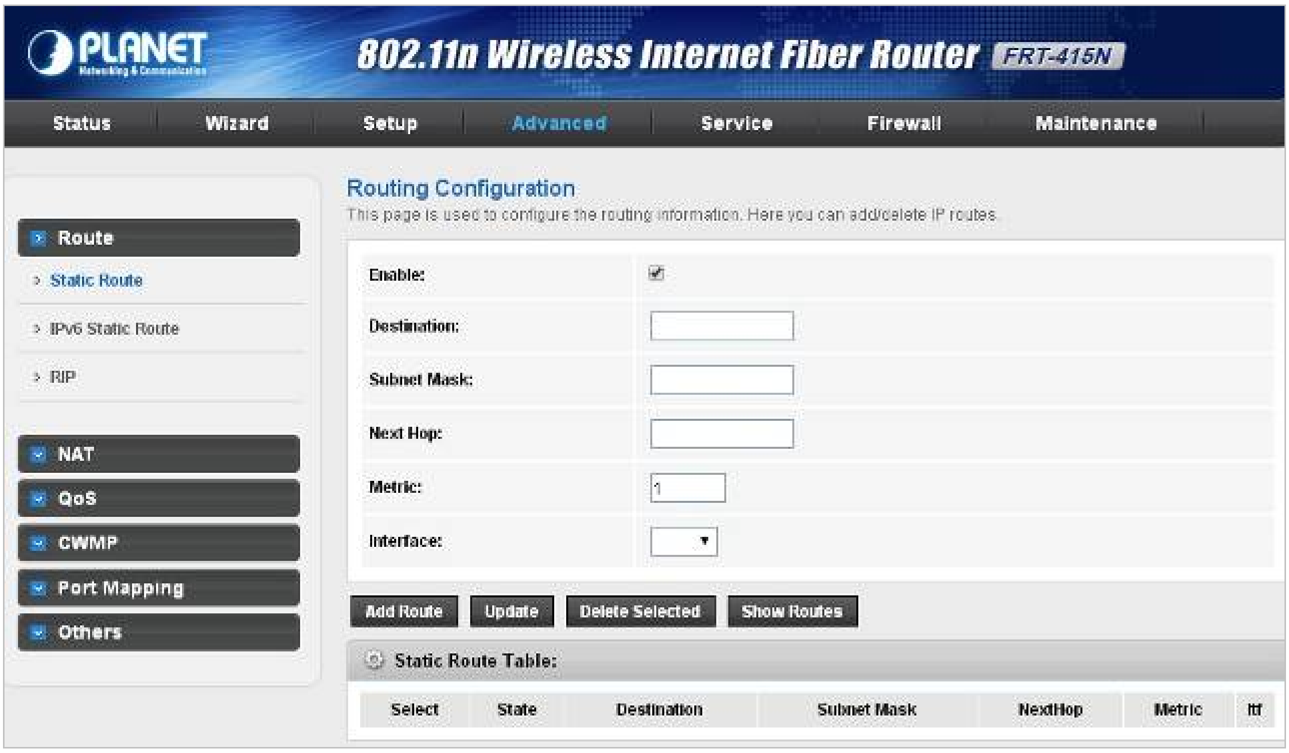
Figure 5-31 WPS

The following table describes the parameters:

Field	Description
Disable WPS	**Enable** or **Disable** the WPS function.
Self-Pin Number	Click Regenerate Pin to reset automatically to obtain an 8-digit number.
Push Button Configuration	Click the **Start PBC** button to connect from Wi-Fi dongle to device automatically.
Start Pin	Enter the Pin number to connect from device to Wi-Fi dongle.

5.4 Advanced

In the navigation bar, click **Advanced**. On the **Advanced** page that is displayed contains **Route**, **NAT**, **QoS**, **CWMP** (**TR-069**), **Port Mappings** and **Others**.



Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	1
Interface:	▼

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

Figure 5-32 Advanced

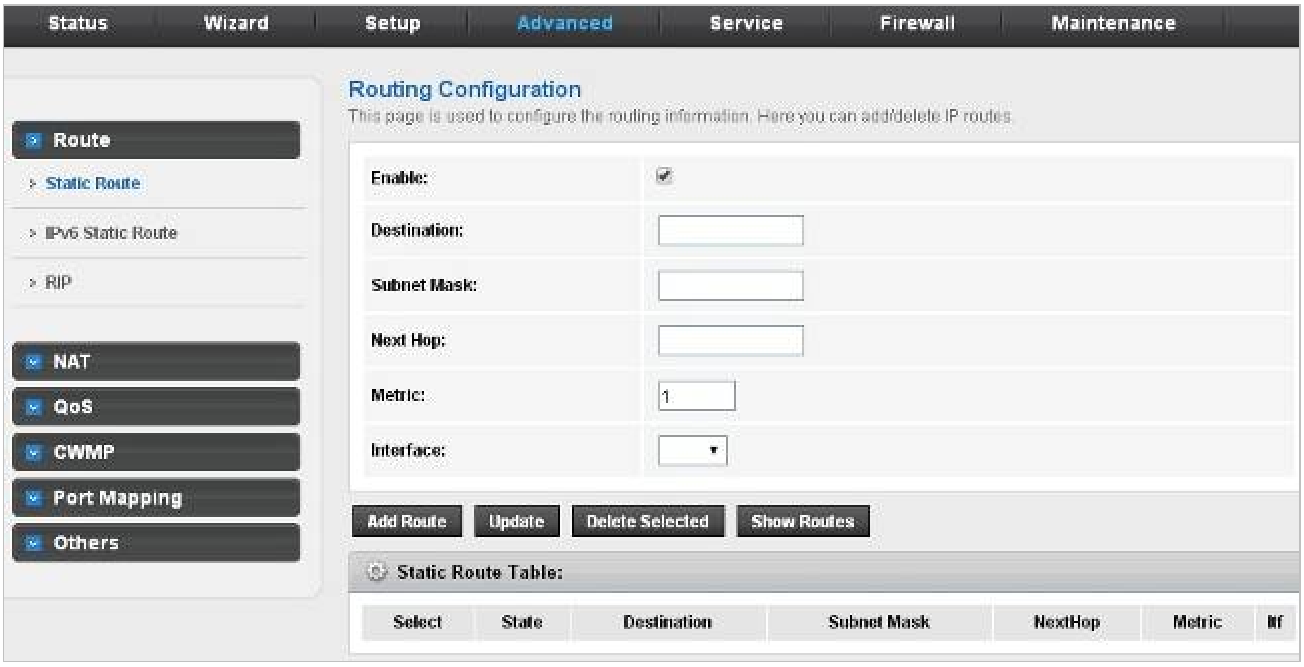
5.4.1 Route

The Routing page enables you to define specific route for your Internet and network data. Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the fiber router provide the most appropriate path for all your Internet traffic.

- On your LAN hosts, a default gateway directs all Internet traffic to the LAN port(s) on the fiber router. Your LAN hosts know their default gateway either because you assigned it to them when you modified your TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet.
- On the fiber router itself, a default gateway is defined to direct all outbound Internet traffic to a route at your ISP. The default gateway is assigned either automatically by your ISP whenever the device negotiates an Internet access, or manually by user to set up through the configuration. You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.

5.4.1.1 Static Route

Click **Static Route** in the left pane and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



Routing Configuration

This page is used to configure the routing information. Here you can add/delete IP routes.

Enable:	☑
Destination:	
Subnet Mask:	
Next Hop:	
Metric:	1
Interface:	▾

Static Route Table:

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf

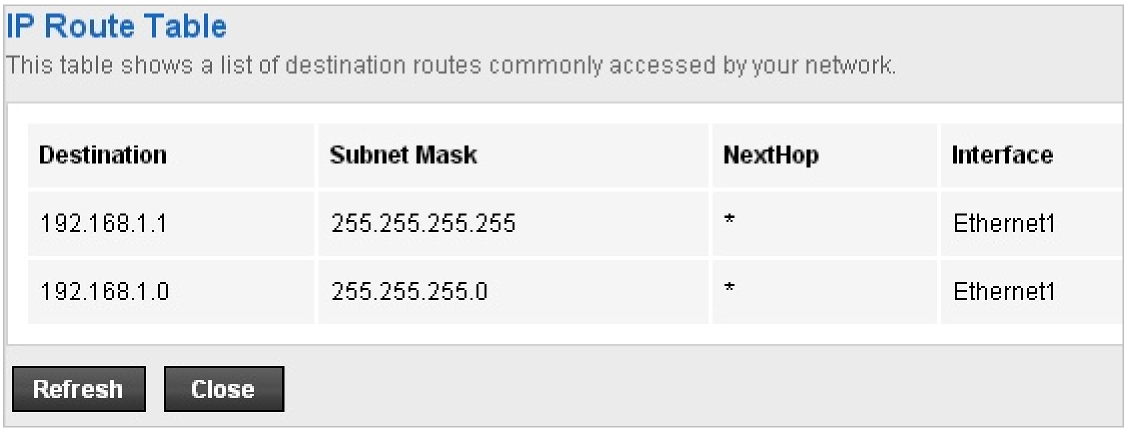
Figure 5-33 Static Route

The following table describes the parameters:

Field	Description
Enable	Click it to enable/disable the selected route or route to be added.
Destination	The network IP address of the subnet. The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Subnet Mask	The network mask of the destination subnet.
Next Hop	The IP address of the next hop through which traffic will flow towards the destination subnet.
Metric	Defines the number of hops between network nodes that data packets travel.
Interface	The WAN interface to which a static routing subnet is to be applied.
Add Route	Add a user-defined destination route.
Update	Update the selected destination route on the Static Route Table.

Delete Selected	Delete a selected destination route on the Static Route Table.

Click **Show Routes** and the page shown in the following figure appears. You can view the information of the clients connected to the fiber router.



IP Route Table

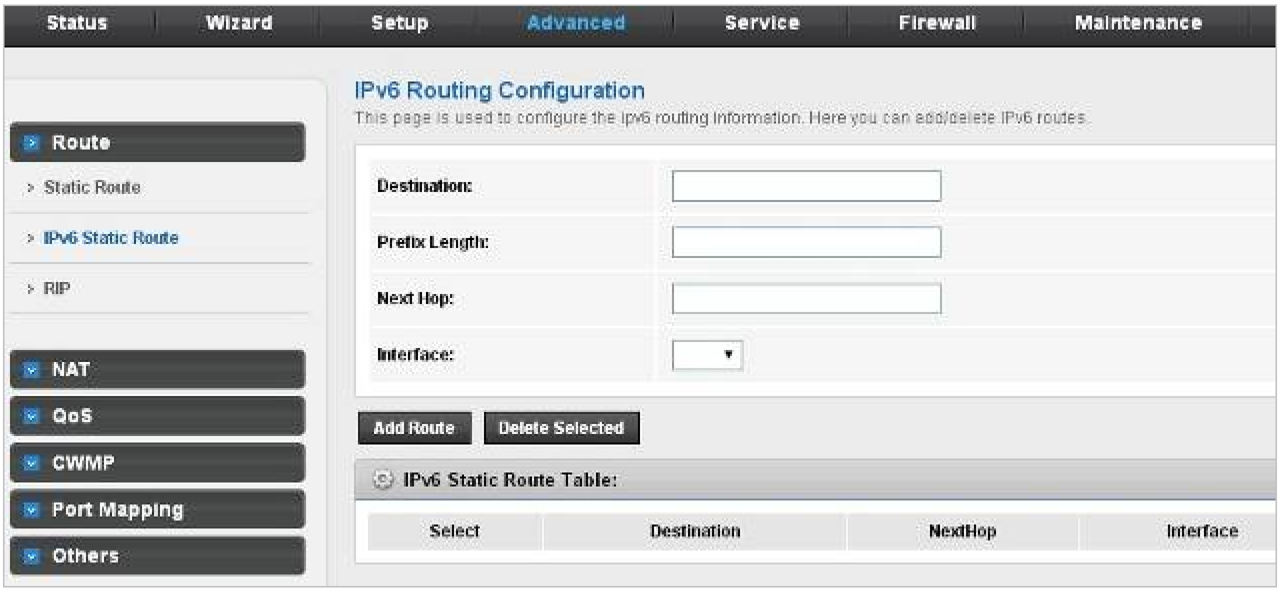
This table shows a list of destination routes commonly accessed by your network.

Destination	Subnet Mask	NextHop	Interface
192.168.1.1	255.255.255.255	*	Ethernet1
192.168.1.0	255.255.255.0	*	Ethernet1

Figure 5-34 IP Route Table

5.4.1.2 IPv6 Static Route

Click **IPv6 Static Route** in the left pane and the page shown in the following figure appears. This page is used to configure the routing information. You can add or delete IP routes.



IPv6 Routing Configuration

This page is used to configure the ipv6 routing information. Here you can add/delete IPv6 routes.

Destination:

Prefix Length:

Next Hop:

Interface:

IPv6 Static Route Table:

Select	Destination	NextHop	Interface

Figure 5-35 IPv6 Static Route

The following table describes the parameters:

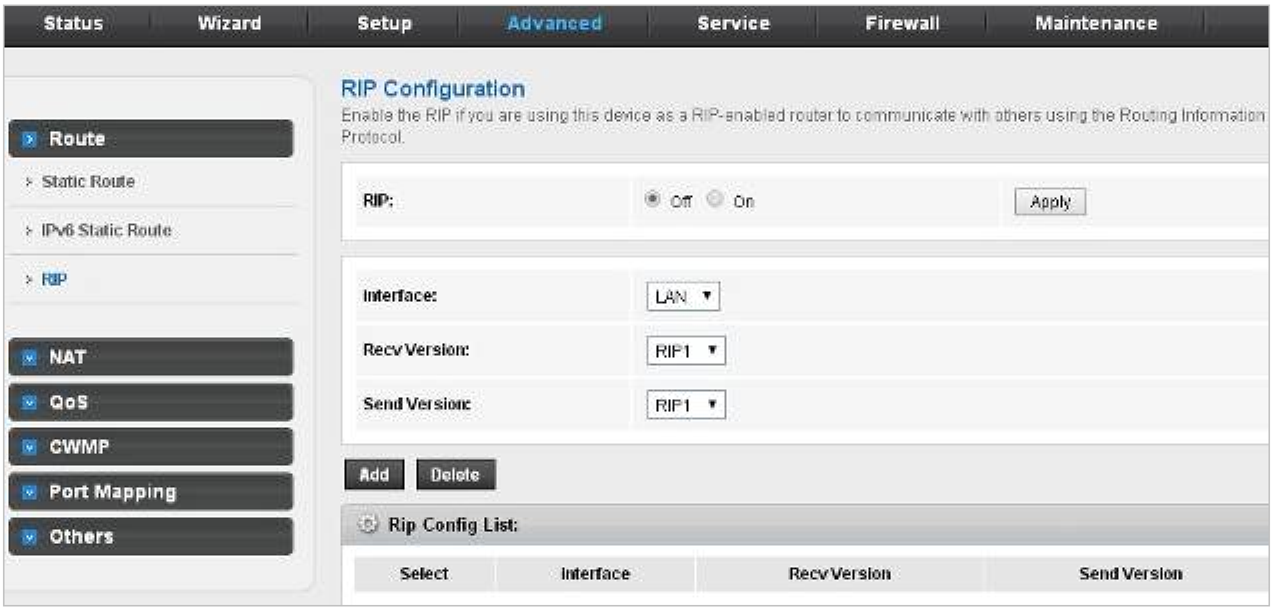
Field	Description
Destination	Enter the IPv6 address of the destination device.

Prefix Length	Enter the prefix length of the IPV6 address.
Next Hop	Enter the IPv6 address of the next hop in the IPv6 route to the destination address.
Interface	The interface for the specified route.
Add Route	Click it to add the new static route to the IPv6 Static Route Table.
Delete the Selected	Select a row in the IPv6 Static Route Table and click it to delete the row.

5.4.1.3 RIP

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the fiber. Most small home or office networks do not need to use RIP; they have only one router, such as the Fiber Router, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway. You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled PC (other than the Fiber Router). The Fiber Router and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the fiber to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should both be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.



RIP Configuration

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.

RIP: ● Off ○ On

Interface: LAN

Recv Version: RIP1

Send Version: RIP1

Rip Config List:

Select	Interface	Recv Version	Send Version

Figure 5-36 RIP

The following table describes the parameters:

Field	Description
RIP	You can select **Off** or **On**.
Apply	Click it to save the settings on this page.
Interface	Choose the router interface that uses RIP.
Recv Version	Choose the interface version that receives RIP messages. You can choose **RIP1**, **RIP2**, or **Both**. ● Choose **RIP1** to indicate the router receives RIP v1 messages. ● Choose **RIP2** to indicate the router receives RIP v2 messages. ● Choose **Both** to indicate the router receives RIP v1 and RIP v2 messages.
Send Version	The working mode for sending RIP messages. You can choose **RIP1** or **RIP2**. ● Choose **RIP1** to indicate the router broadcasts RIP1 messages only. ● Choose **RIP2** to indicate the router multicasts RIP2 messages only.
Add	Click it to add the RIP interface to the **Rip Config List**.
Delete	Select a row in the **Rip Config List** and click it to delete the row.

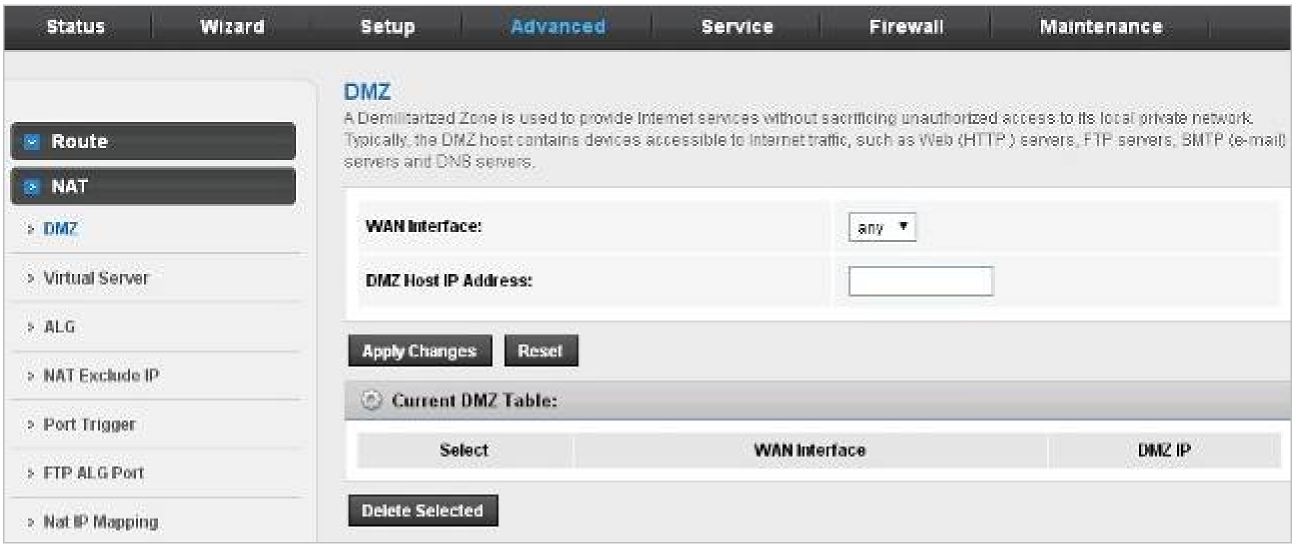
5.4.2 NAT

Choose **Advanced** > **NAT** and the page shown in the following figure appears. The page displayed contains **DMZ**, **Virtual Server**, **ALG**, **NAT Exclude IP**, **Port Trigger**, **FTP ALG Port**, and **NAT IP Mapping**.

5.4.2.1 DMZ

Demilitarized Zone (DMZ) is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

Click **DMZ** in the left pane and the page shown in the following figure appears. The following describes how to configure manual DMZ. Enter an IP address of the DMZ host. Click **Apply Changes** to save the settings on this page temporarily.



DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

WAN Interface: any

DMZ Host IP Address:

Current DMZ Table:

Select	WAN Interface	DMZ IP

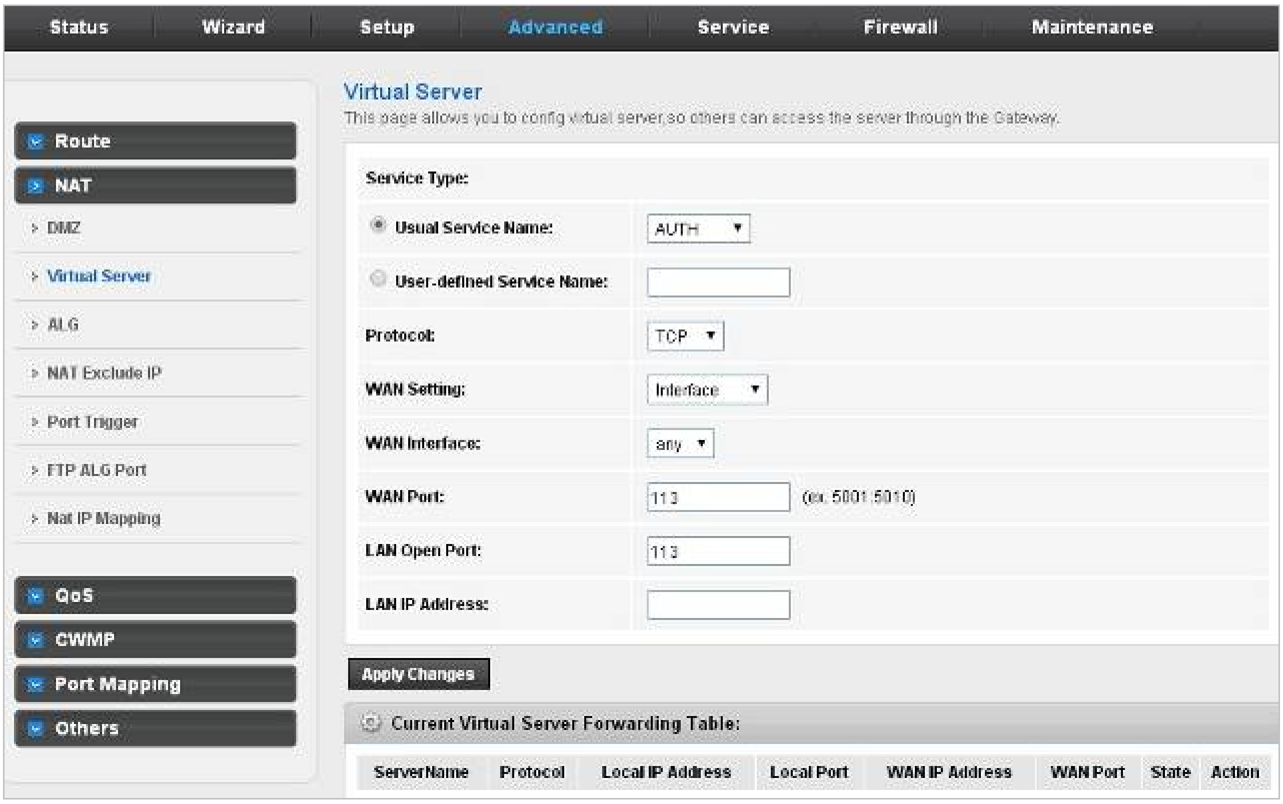
Figure 5-37 DMZ

The following table describes the parameters:

Field	Description
WAN Interface	Choose a WAN Interface.
DMZ Host IP Address	Enter an IP address of the DMZ host.
Current DMZ Table	A list of the previously configured DMZ information.
Apply Changes	Click Apply Changes to add new settings.
Reset	Clear the settings.
Delete the Selected	Select the number of rows from the Current DMZ Table to be deleted.

5.4.2.2 Virtual Server

Internet users would not be able to access a server on your LAN because of native NAT protection.The "virtual server" feature solves these problems and allows internet users to connect to your servers.



Virtual Server

This page allows you to config virtual server,so others can access the server through the Gateway.

Service Type:	
● Usual Service Name:	AUTH
○ User-defined Service Name:	
Protocol:	TCP
WAN Setting:	Interface
WAN Interface:	any
WAN Port:	113 (ex. 5001:5010)
LAN Open Port:	113
LAN IP Address:	

Current Virtual Server Forwarding Table:

ServerName	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action

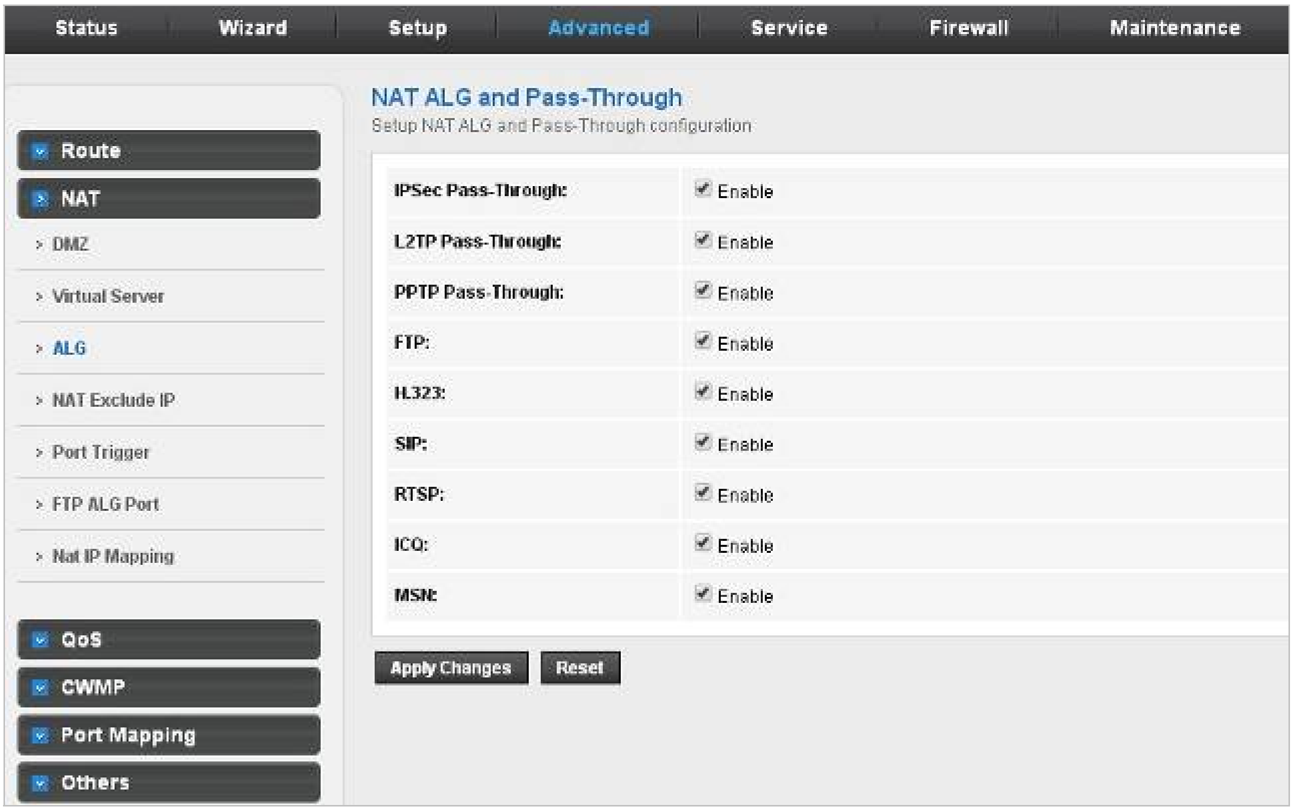
Figure 5-38 Virtual Server

The following table describes the parameters:

Field	Description
Service Type	You can select the common service type, for example, **AUTH**, **DNS** or **FTP**. You can also define a service name. ● If you select **Usual Service Name**, the corresponding parameter has the default settings. ● If you select **User-defined Service Name**, you need to enter the corresponding parameters.
Protocol	Choose the transport layer protocol that the service type uses. You can choose **TCP** or **UDP**.
WAN Setting	You can choose **Interface** or **IP Address**.
WAN Interface	Choose the WAN interface that will apply virtual server.
WAN Port	Choose the access port on the WAN.
LAN Open Port	Enter the port number of the specified service type.
LAN IP Address	Enter the IP address of the virtual server. It is in the same network segment with LAN IP address of the router.

5.4.2.3 ALG

An application layer gateway (ALG) is a feature that enables the gateway to parse application layer payloads and take decisions on them. ALG is typically employed to support applications that use the application layer payload to communicate the dynamic Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports on which the applications open data connections. Such applications include the File Transfer Protocol (FTP) and various IP telephony protocols.



NAT ALG and Pass-Through

Setup NAT ALG and Pass-Through configuration

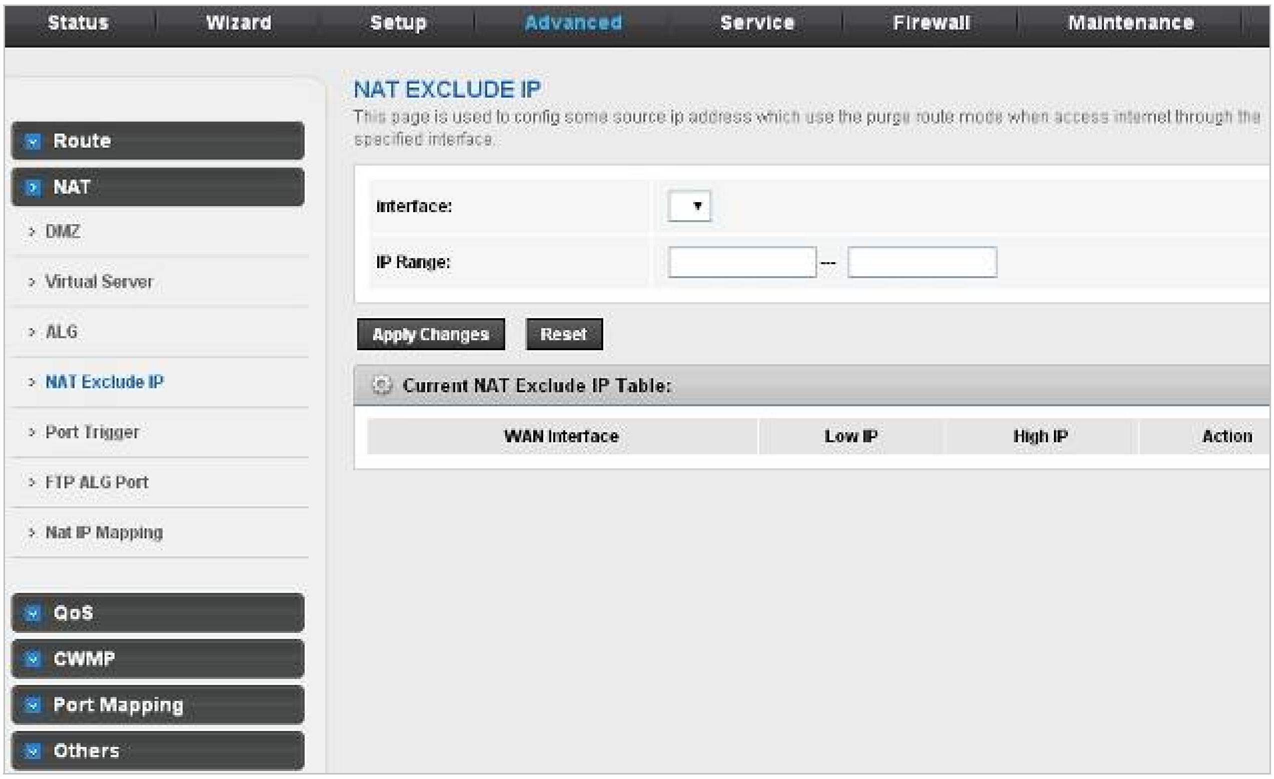
IPSec Pass-Through:	☑ Enable
L2TP Pass-Through:	☑ Enable
PPTP Pass-Through:	☑ Enable
FTP:	☑ Enable
H.323:	☑ Enable
SIP:	☑ Enable
RTSP:	☑ Enable
ICQ:	☑ Enable
MSN:	☑ Enable

Figure 5-39 ALG

5.4.2.4 NAT Exclude IP

NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection. Network Address Translation (NAT) is the method by which the Router shares the single IP address assigned by your ISP with the other computers on your network. This function should only be used if your ISP assigns you multiple IP addresses or you need NAT disabled for an advanced system configuration.

If you have a single IP address and you turn NAT off, the computers on your network will not be able to access the Internet. Other problems may also occur. Turning off NAT will disable your firewall functions.



NAT EXCLUDE IP

This page is used to config some source ip address which use the purge route mode when access internet through the specified interface.

Interface: ▾

IP Range: --

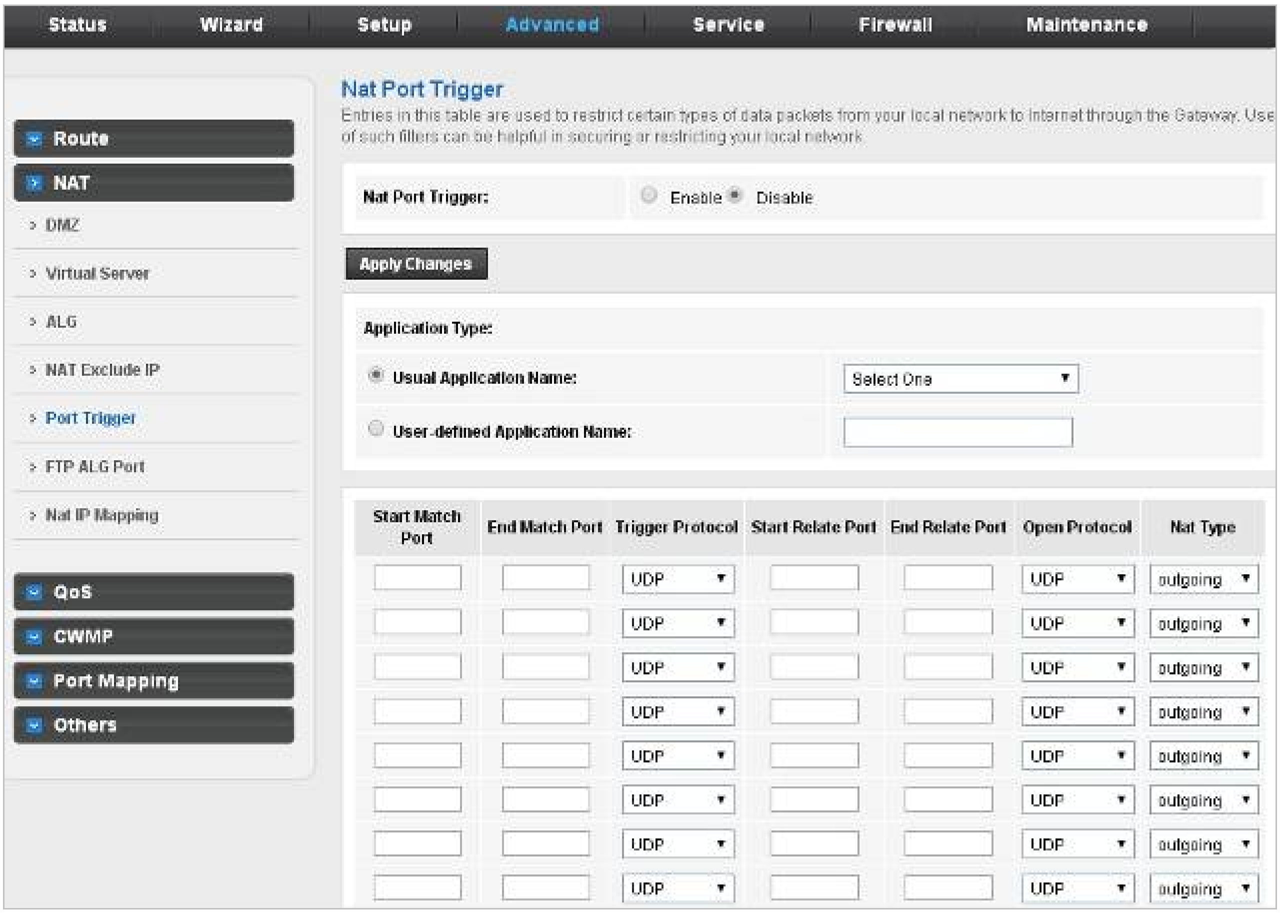
Current NAT Exclude IP Table:

WAN Interface	Low IP	High IP	Action

Figure 5-40 NAT Exclude IP

5.4.2.5 Port Trigger

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT Router. Port Trigger is used for some of these applications that can work with an NAT Router.



Nat Port Trigger

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network

Nat Port Trigger: ○ Enable ● Disable

Application Type:

● Usual Application Name: Select One

○ User-defined Application Name:

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing
		UDP			UDP	outgoing

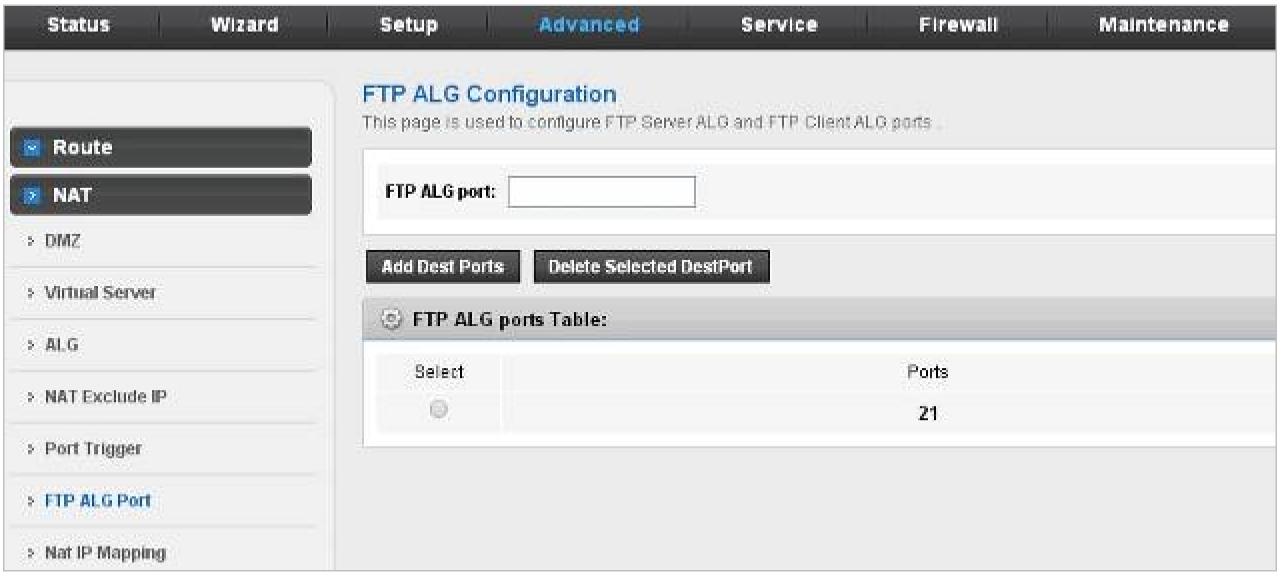
Figure 5-41 Port Trigger

Click the **Usual Application Name** drop-down menu to choose the application you want to set up for port triggering. When you have chosen an application the default Trigger settings will populate the table below.

If the application you want to set up isn’t listed, click the **User-defined Application Name** button and type in a name for the trigger in the Custom application field. Configure the **Start Match Port**, **End Match Port**, **Trigger Protocol**, **Start Relate Port**, **End Relate Port**, **Open Protocol** and **Nat Type** settings for the port trigger you want to configure. When it is finished, click the **Apply changes** button.

5.4.2.6 FTP ALG Port

FTP uses two communication channels, one for control commands and one for the actual files being transferred. When an FTP session is opened, the FTP client establishes a TCP connection (the control channel) to (usually) port 21 on the FTP server. What happens after this point depends on the mode of FTP being used.



FTP ALG Configuration

This page is used to configure FTP Server ALG and FTP Client ALG ports .

FTP ALG port:

FTP ALG ports Table:

Select	Ports
○	21

Figure 5-42 FTP ALG Port

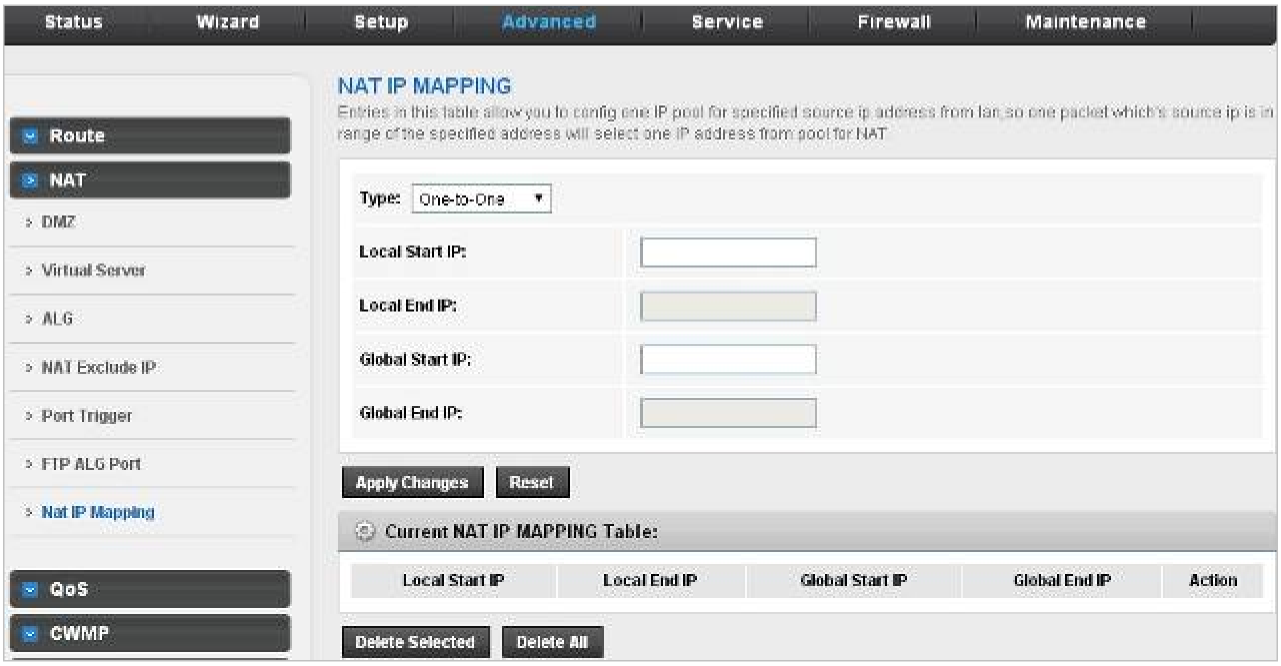
The following table describes the parameters:

Field	Description
FTP ALG port	Set an FTP ALG port.
Add Dest Ports	Add a port configuration.
Delete Selected Dest Port	Delete a selected port configuration from the list.

5.4.2.7 NAT IP Mapping

NAT is short for Network Address Translation. The Network Address Translation Settings window allows you to share one WAN IP address for multiple computers on your LAN. Click **NAT IP Mapping** in the left pane and the page shown in the following figure appears.

Entries in this table allow you to configure one IP pool for specified source IP address from LAN, so one packet whose source IP is in range of the specified address will select one IP address from the pool for NAT.



NAT IP MAPPING

Entries in this table allow you to config one IP pool for specified source ip adderss from lan,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT

Type: One-to-One ▼

Local Start IP:

Local End IP:

Global Start IP:

Global End IP:

Current NAT IP MAPPING Table:

Local Start IP	Local End IP	Global Start IP	Global End IP	Action

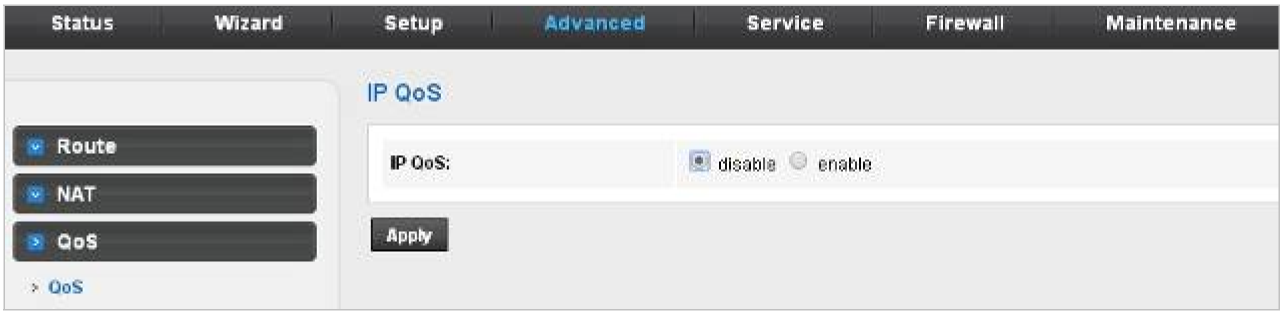
Figure 5-43 NAT IP Mapping

The following table describes the parameters:

Field	Description
Type	There are four types: **One-to-One**, **Many-to-One**, **Many-to-Many** and **One-to-Many**.
Local Start & End IP	Enter the local IP Address you plan to map to. Local Start IP is the starting local IP address and Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255
Global Start & End IP	Enter the Globe IP Address you want to do NAT. Global Start IP is the starting global IP address and Global End IP is the ending global IP address. If you have a dynamic IP, enter 0.0.0.0 as the global Start IP.
NAT IP Mapping Table	This displays the information about the Mapping addresses.

5.4.3 QoS

TheFRT-415N provides a control mechanism that can provide a different priority to different users or data flows. The QoS is enforced by the QoS rules in the QoS table. A QoS rule contains two configuration blocks: Traffic Classification and Action. The Traffic Classification enables you to classify packets on the basis of various fields in the packet and perhaps the physical ingress port. The Action enables you to assign the strict priority level and mark some fields in the packet that matches the Traffic Classification rule. You can configure any or all fields as needed in these two QoS blocks for a QoS rule.



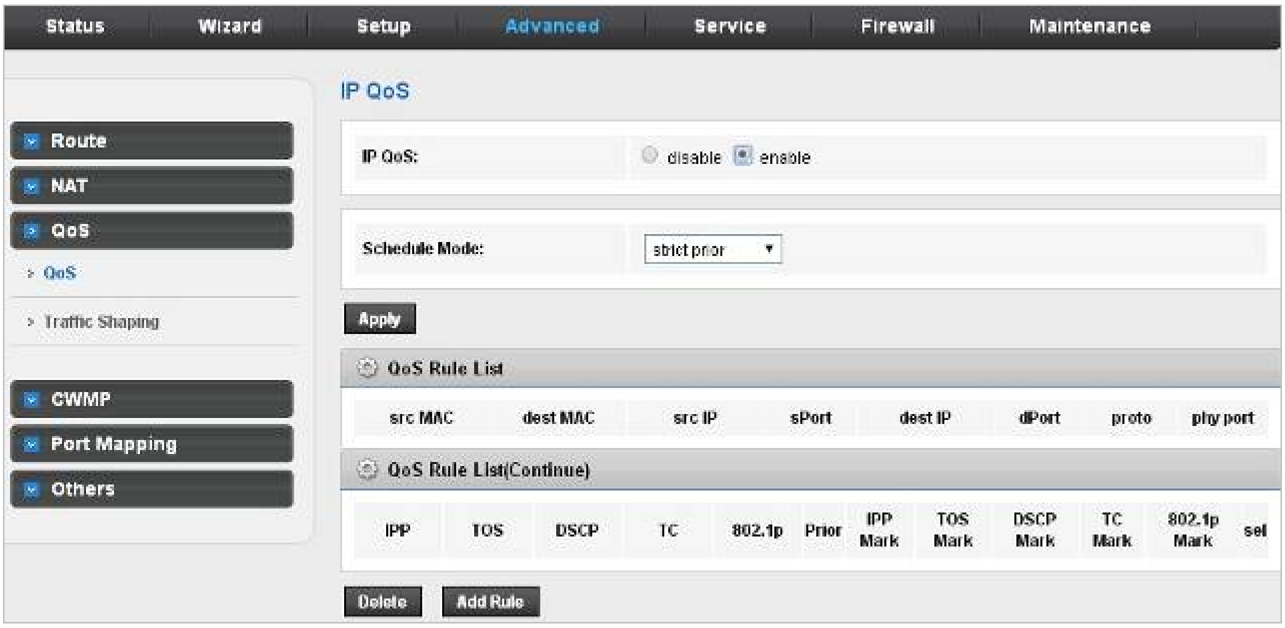
IP QoS

IP QoS: ● disable ○ enable

Apply

Figure 5-44 QoS Disable

Enable QoS and click **Apply** to enable IP QoS function. Click **add rule** to add a new IP QoS rule.



IP QoS

IP QoS: ○ disable ● enable

Schedule Mode: strict prior

Apply

QoS Rule List

src MAC	dest MAC	src IP	sPort	dest IP	dPort	proto	phy port

QoS Rule List(Continue)

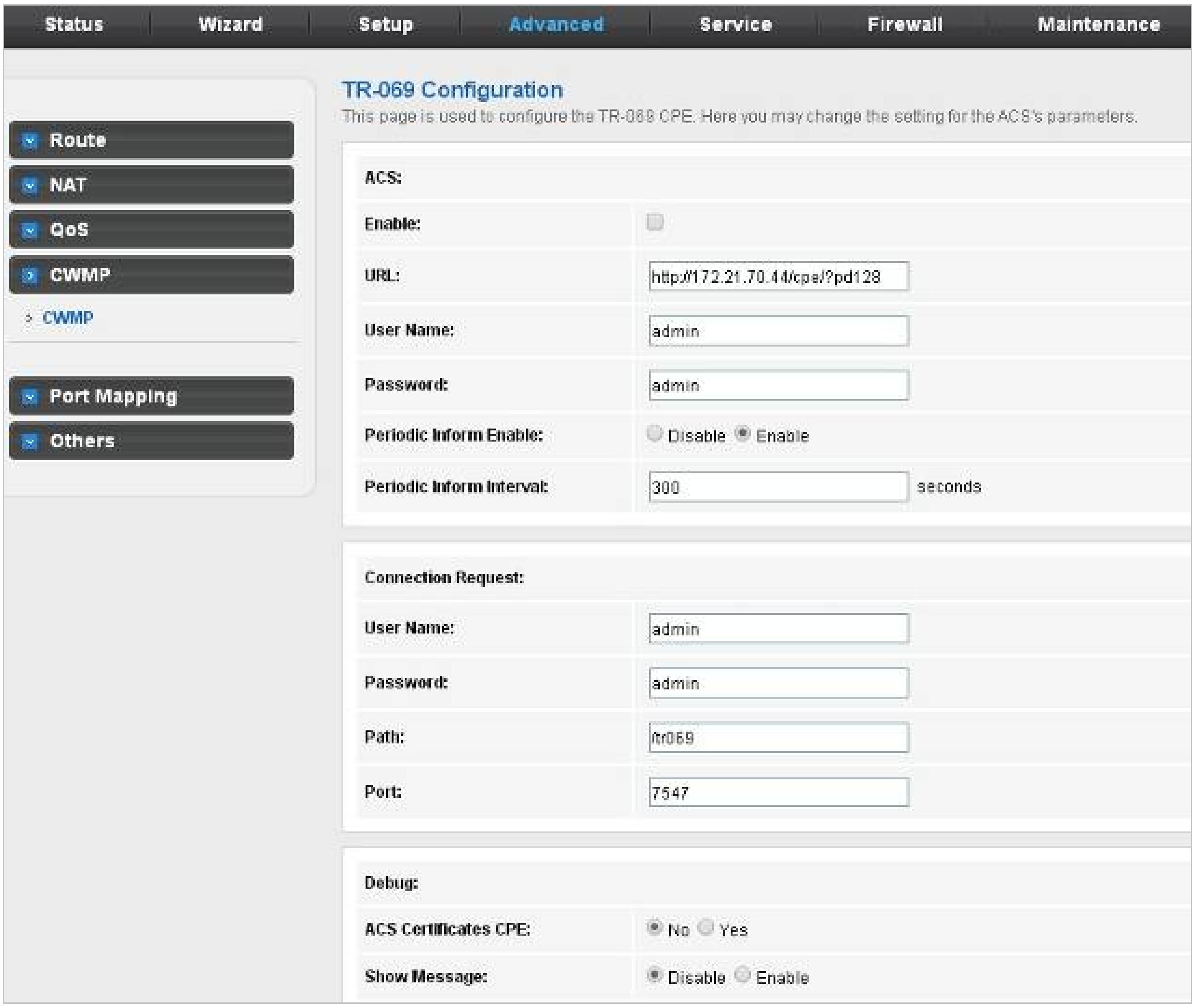
IPP	TOS	DSCP	TC	802.1p	Prior	IPP Mark	TOS Mark	DSCP Mark	TC Mark	802.1p Mark	sel

Delete　Add Rule

Figure 5-45 QoS Enable

5.4.4 CWMP (TR-069)

Choose **Advanced** > **CWMP** and the page shown in the following page appears. On this page, you can configure the TR-069 CPE.



TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

ACS:	
Enable:	□
URL:	http://172.21.70.44/cpe/?pd128
User Name:	admin
Password:	admin
Periodic Inform Enable:	○ Disable ● Enable
Periodic Inform Interval:	300 seconds
Connection Request:	
User Name:	admin
Password:	admin
Path:	/tr069
Port:	7547
Debug:	
ACS Certificates CPE:	● No ○ Yes
Show Message:	● Disable ○ Enable

Figure 5-46 CWMP

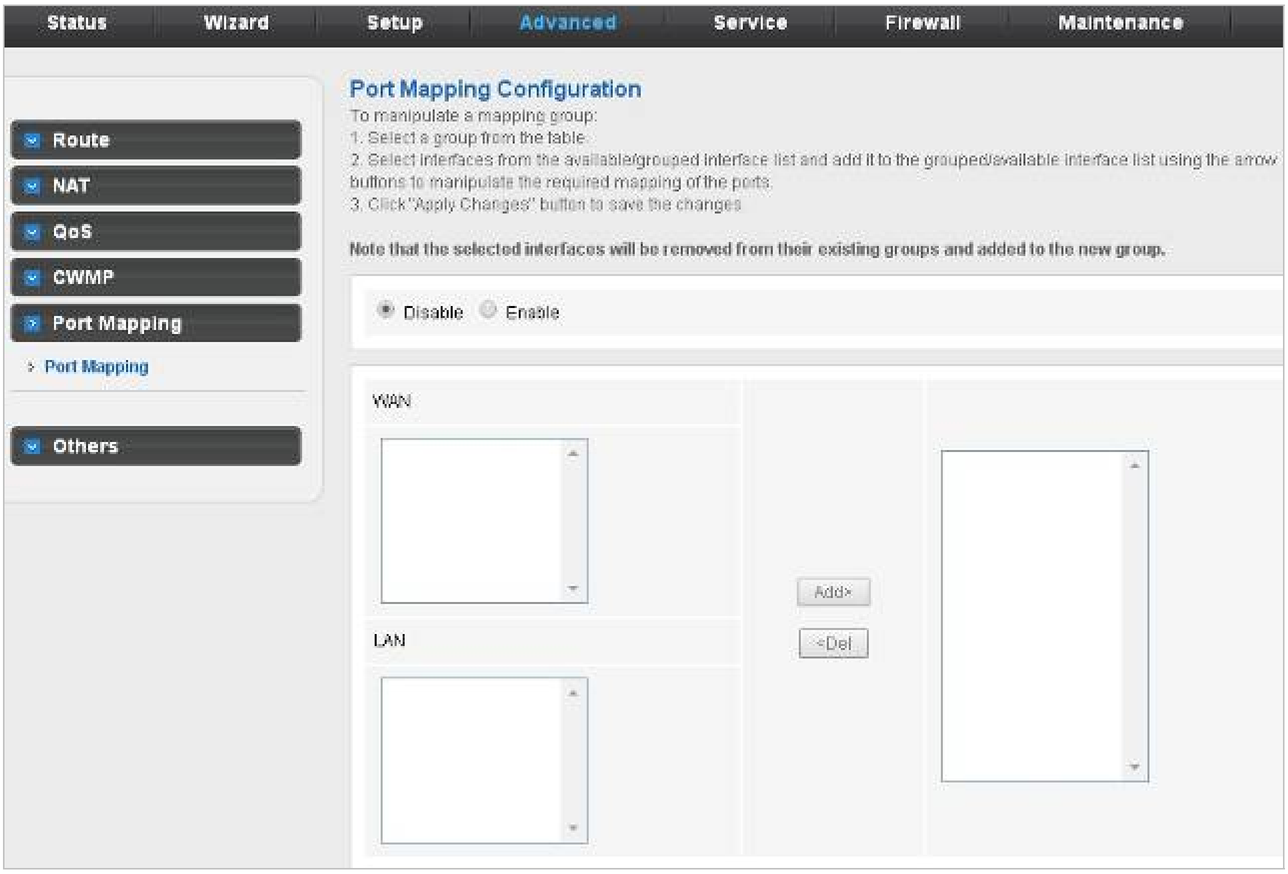
The following table describes the parameters:

Field	Description
ACS	
Enable	Enable/Disable the function to access.
URL	The URL of the auto-configuration server to connect to.
User Name	The user name for logging in to the ACS.
Password	The password for logging in to the ACS.

Periodic Inform Enable	Select **Enable** to periodically connect to the ACS to check whether the configuration updates.
Periodic Inform Interval	Specify the amount of time between connections to ACS.
Connection Request	
User Name	The connection username provided by TR-069 service.
Password	The connection password provided by TR-069 service.
Debug	
Show Message	Select **Enable** to display ACS SOAP messages on the serial console.
CPE sends GetRPC	Select **Enable** to enable the router to contact the ACS to obtain configuration updates.
Skip MReboot	Specify whether to send an MReboot event code in the inform message.
Delay	Specify whether to start the TR-069 program after a short delay.
Auto-Execution	Specify whether to automatically start the TR-069 after the router is powered on.

5.4.5 Port Mapping

The FRT-415N provides multiple interface groups. Up to five interface groups are supported including one default group. The LAN and WAN interfaces could be included. Traffic coming from one interface of a group can only be flowed to the interfaces in the same interface group. Thus, the FRT-415N can isolate traffic from group to group for some applications. By default, all the interfaces (LAN and WAN) belong to the default group, and the other four groups are all empty. It is possible to assign any interface to any group but only one group.



Port Mapping Configuration

To manipulate a mapping group:
1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note that the selected interfaces will be removed from their existing groups and added to the new group.

● Disable ○ Enable

Figure 5-47 Port Mapping

The following table describes the parameters:

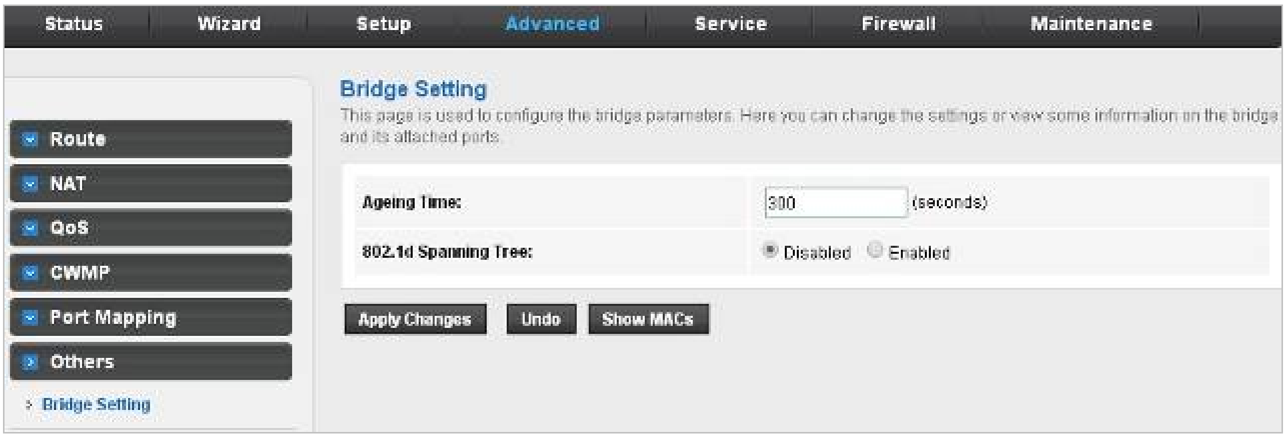
Field	Description
Enabled/Disabled	Click the **radio** button to enable/disable the interface group feature. If disabled, all interfaces belong to the default group.
Interface groups	To manipulate a mapping group: 1. Select a group from the table. 2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.

5.4.6 Others

Choose **Advance** > **Others** and the page shown in the following figure appears. The page displayed contains **Bridge Setting**, **Client Limit**, **Tunnel**, Telnet and **Others**.

5.4.6.1 Bridge Setting

Choose **Advance** > **Others** > **Bridge Setting** and the page shown in the following figure appears. This page is used to configure the bridge parameters. You can change the settings or view some information on the bridge and its attached ports.



Bridge Setting

This page is used to configure the bridge parameters. Here you can change the settings or view some information on the bridge and its attached ports.

Ageing Time: 300 (seconds)

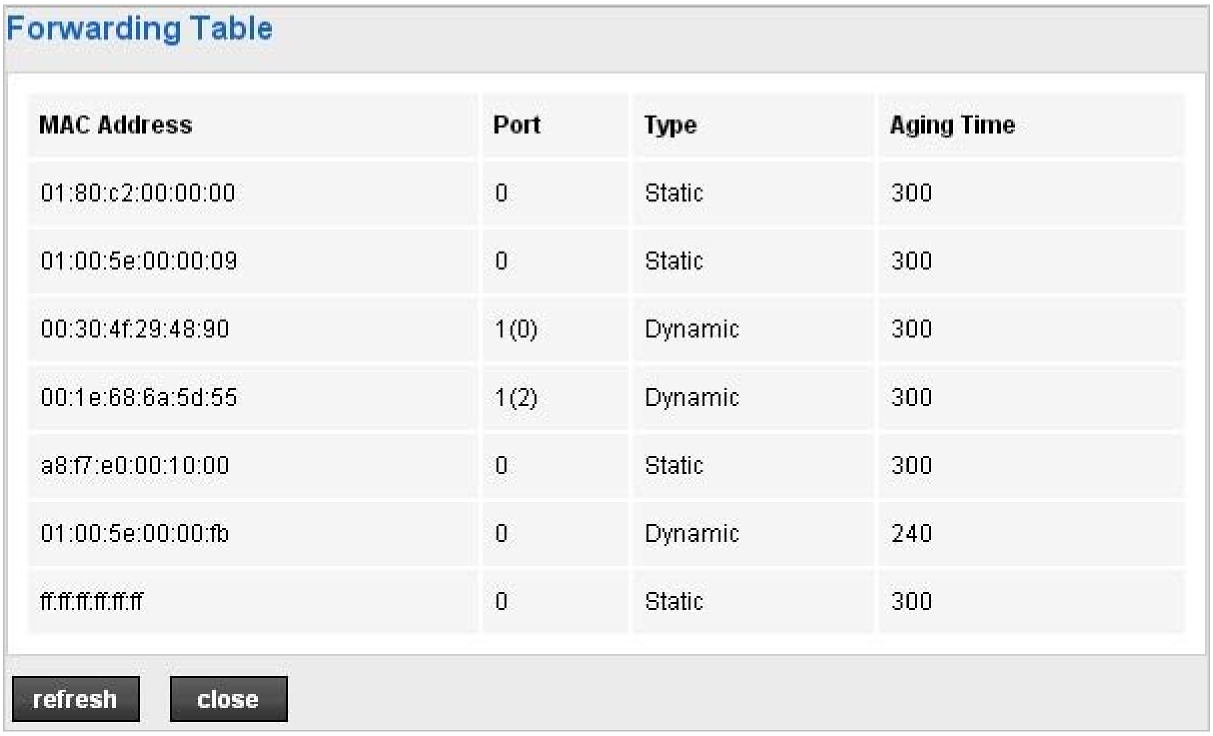
802.1d Spanning Tree: ● Disabled ○ Enabled

Figure 5-48 Bridge Setting

The following table describes the parameters:

Field	Description
Aging Time	If the host is idle for 300 seconds (default value), its entry is deleted from the bridge table.
802.1d Spanning Tree	You can select **Disable** or **Enable**. Select **Enable** to provide path redundancy while preventing undesirable loops in your network.
Show MACs	Click it to show a list of the learned MAC addresses for the bridge.

Click **Show MACs** and the page shown in the following figure appears. This table shows a list of learned MAC addresses for this bridge.



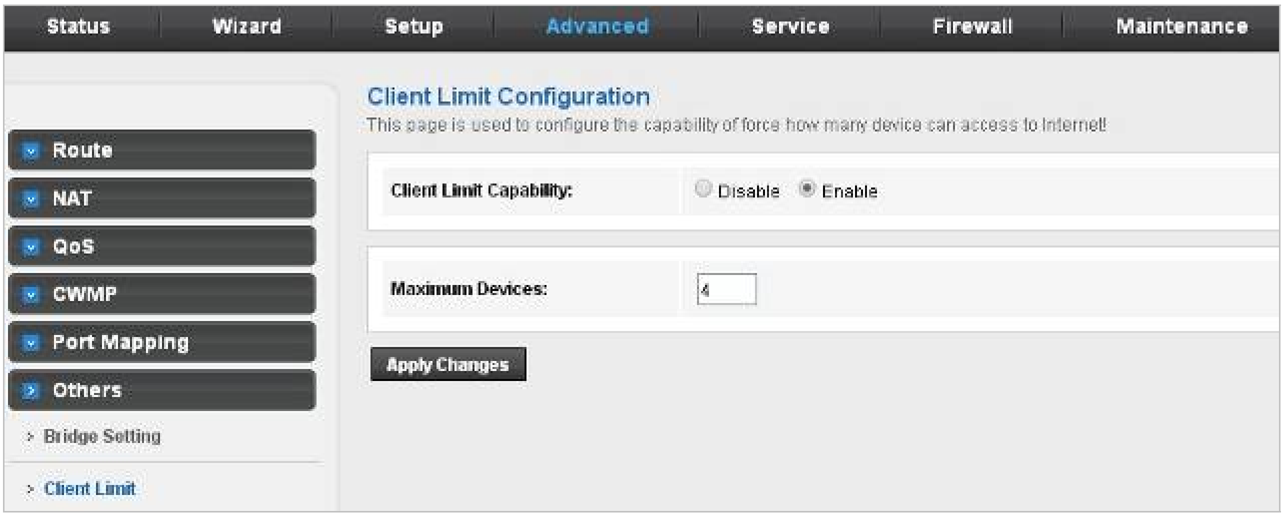
Forwarding Table

MAC Address	Port	Type	Aging Time
01:80:c2:00:00:00	0	Static	300
01:00:5e:00:00:09	0	Static	300
00:30:4f:29:48:90	1(0)	Dynamic	300
00:1e:68:6a:5d:55	1(2)	Dynamic	300
a8:f7:e0:00:10:00	0	Static	300
01:00:5e:00:00:fb	0	Dynamic	240
ff:ff:ff:ff:ff:ff	0	Static	300

Figure 5-49 Forwarding Table

5.4.6.2 Client Limit

Choose **Advance** > **Others** > **Client Limit** and the page shown in the following figure appears. This page is used to configure the capability of forcing how many devices can access the Internet.



Client Limit Configuration

This page is used to configure the capability of force how many device can access to Internet!

Client Limit Capability: ○ Disable ● Enable

Maximum Devices: 4

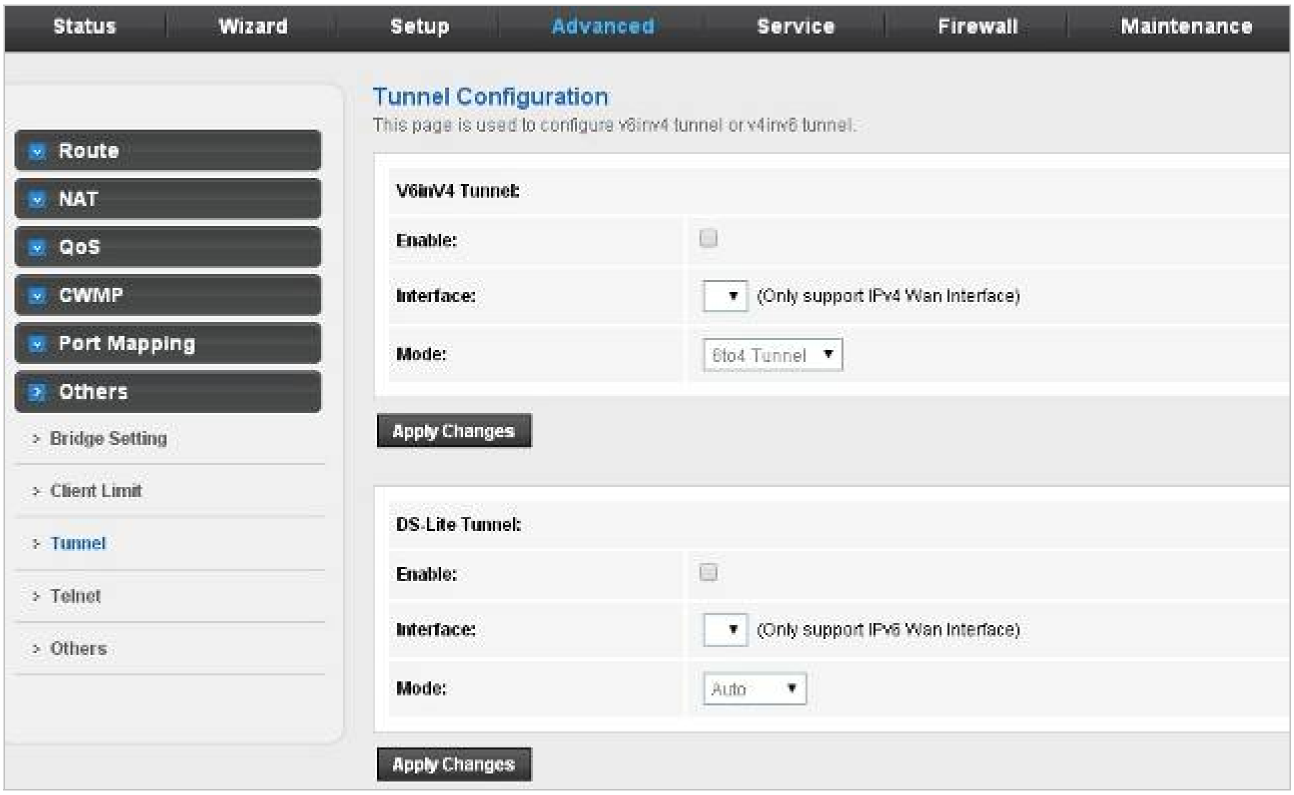
Figure 5-50 Client Limit

The following table describes the parameters:

Field	Description
Client Limit Capability	Enable/Disable the function to access If enabled, maximum devices would be 32; default is 4.

5.4.6.3 Tunnel

Choose **Advanced** > **Others** > **Tunnel** and the page shown in the following figure appears. This page is used to configure the IPv6 with LAN to transfer to IPv4.



Tunnel Configuration

This page is used to configure v6inv4 tunnel or v4inv6 tunnel.

V6inV4 Tunnel:

Enable: □

Interface: ▾ (Only support IPv4 Wan Interface)

Mode: 6to4 Tunnel ▾

DS-Lite Tunnel:

Enable: □

Interface: ▾ (Only support IPv6 Wan Interface)

Mode: Auto ▾

Figure 5-51 Tunnel

The following table describes the parameters:

V6inV4 Tunnel

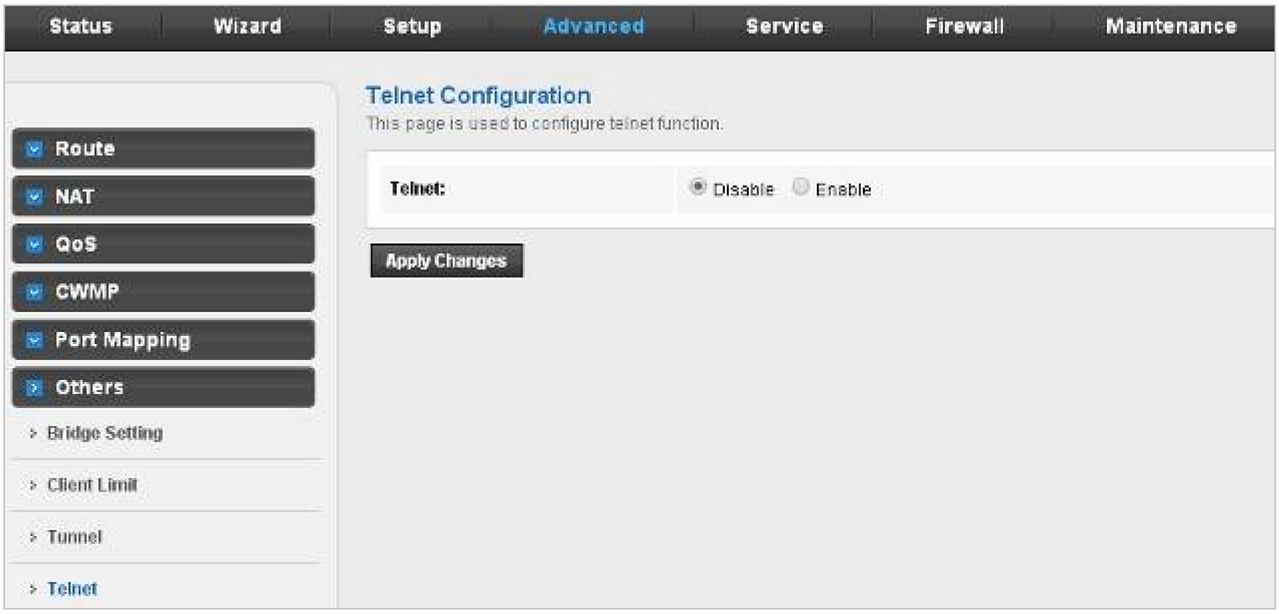
Field	Description
Enable	Enable or Disable the V6inV4 Tunnel.
Interface Name	Select the current WAN interface used as tunnel interface.
Mode	6to4 Tunnel or 6rd Tunnel.

DS-Lite Tunnel

Field	Description
Enable	Enable or disable the DS-Lite tunnel.
Interface	Select the current WAN interface used as tunnel interface.
Mode	Auto or manual.

5.4.6.4 Telnet

Choose **Advanced > Others > Telnet** in the left pane and the page shown in the following figure appears. You can enable or disable the Telnet function on this page.



Telnet Configuration

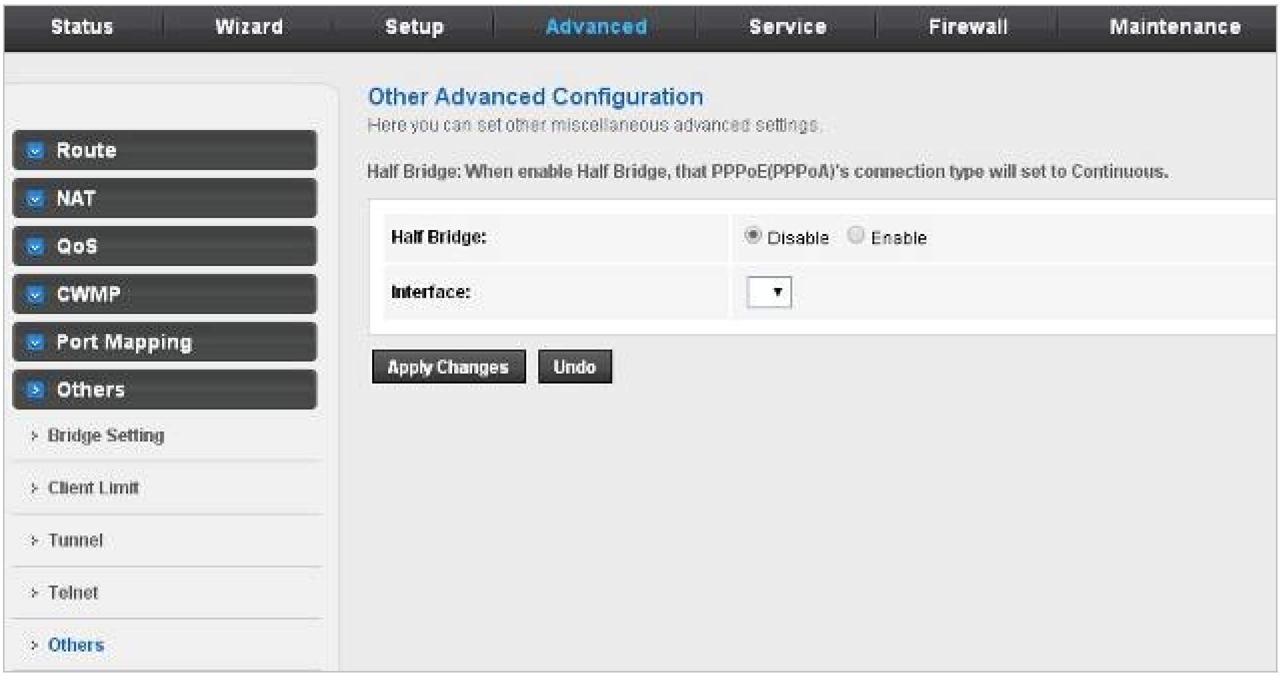
This page is used to configure telnet function.

Telnet: ● Disable ○ Enable

Figure 5-52 Telnet

5.4.6.5 Others

Choose **Advanced > Others > Others** in the left pane and the page shown in the following figure appears. You can enable half bridge so that the PPPoE or PPPoA connection will set to Continuous.



Other Advanced Configuration

Here you can set other miscellaneous advanced settings.

Half Bridge: When enable Half Bridge, that PPPoE(PPPoA)'s connection type will set to Continuous.

Half Bridge: ● Disable ○ Enable

Interface:

Figure 5-53 Others

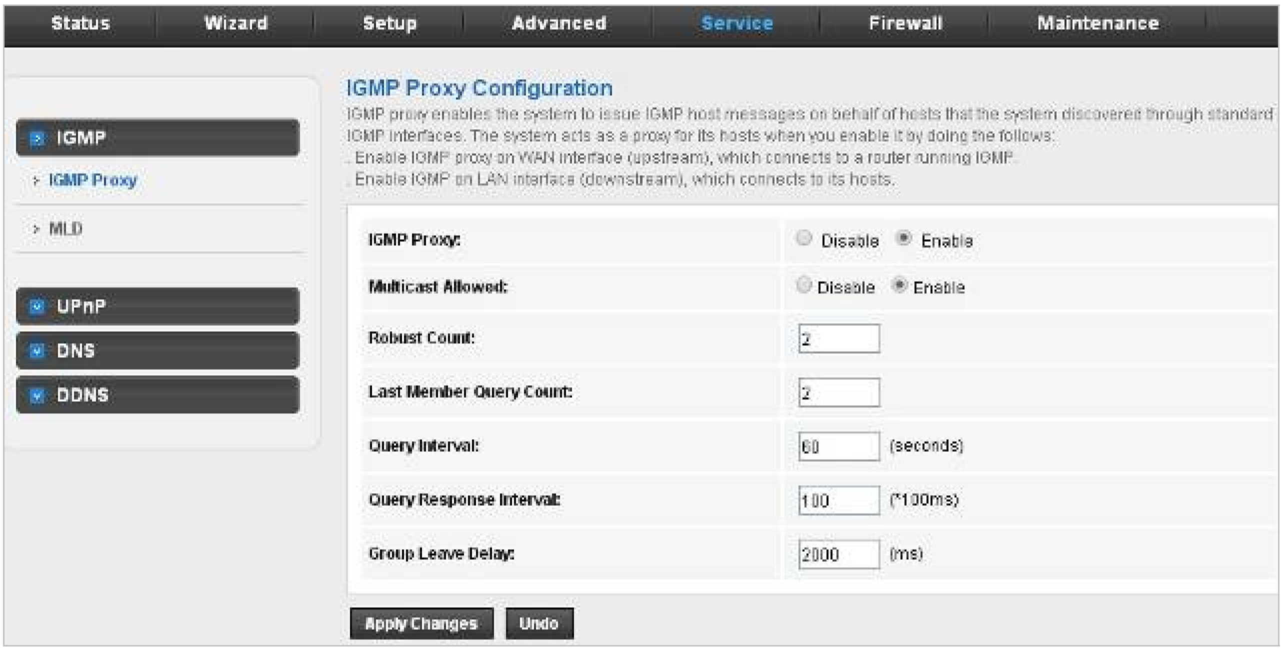
5.5 Service

In the navigation bar, click **Service**. On the **Service** page that is displayed contains **IGMP**, **UPnP**, **DNS** and **DDNS**.

5.5.1 IGMP

5.5.1.1 IGMP Proxy

Choose **Service** > **IGMP** and the page shown in the following figure appears. IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts after you enable it.



IGMP Proxy Configuration

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by doing the follows:

. Enable IGMP proxy on WAN interface (upstream), which connects to a router running IGMP.

. Enable IGMP on LAN interface (downstream), which connects to its hosts.

IGMP Proxy:	○ Disable ● Enable
Multicast Allowed:	○ Disable ● Enable
Robust Count:	2
Last Member Query Count:	2
Query Interval:	60 (seconds)
Query Response Interval:	100 (*100ms)
Group Leave Delay:	2000 (ms)

Figure 5-54 IGMP Proxy

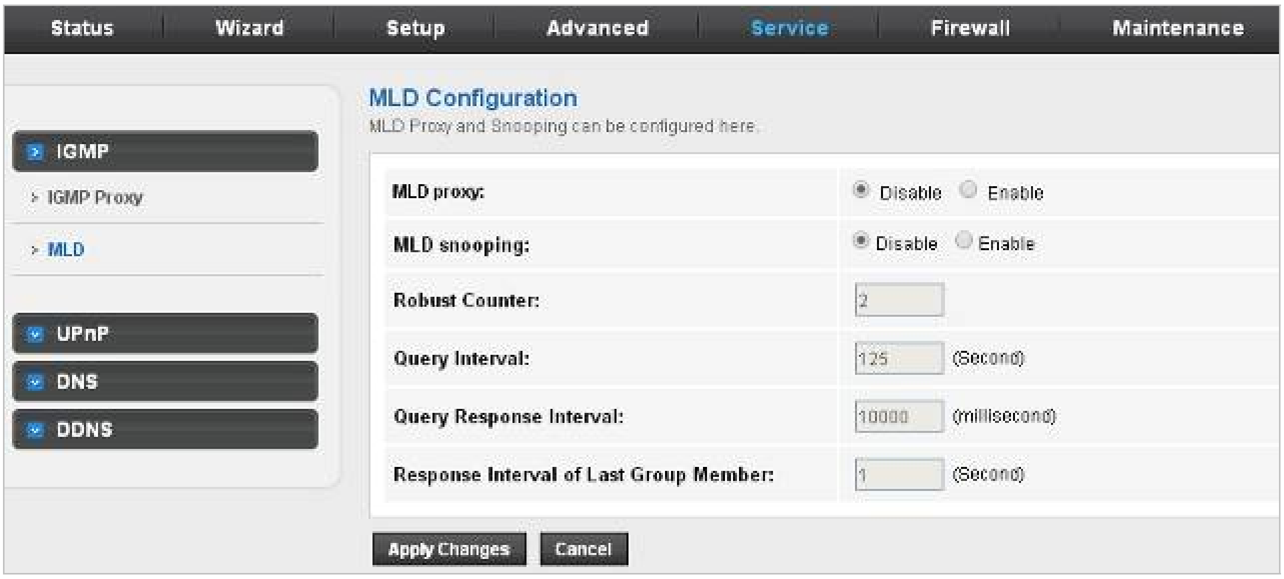
The following table describes the parameters:

Field	Description
IGMP Proxy	The Internet Group Management Protocol. Enable/Disable the function to access.
Multicast Allowed	Enable/Disable the function to access.
Robust Count	Robust factor of the IGMP Proxy Counter.
Last Member Query Count	The last-member query interval is the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You can configure this interval to change the amount of time it takes a routing device to detect the loss of the last member of a group.

Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Group Leave Delay	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

5.5.1.2 MLD

MLD means Multicast Listener Discovery -- its component of the IPv6. MLD is used by IPv6 routers for discovering multicast listeners on a directly-attached link, much like IGMP being used in IPv4.



MLD Configuration

MLD Proxy and Snooping can be configured here.

MLD proxy: ● Disable ○ Enable

MLD snooping: ● Disable ○ Enable

Robust Counter: 2

Query Interval: 125 (Second)

Query Response Interval: 10000 (millisecond)

Response Interval of Last Group Member: 1 (Second)

Figure 5-55 MLD

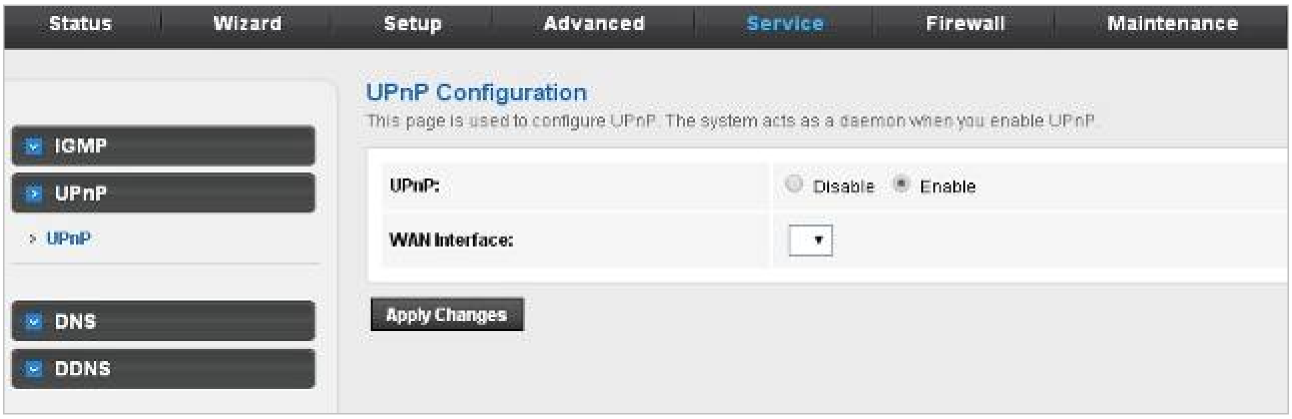
The following table describes the parameters:

Field	Description
MLD Proxy	MLD Proxy can be used to support IPv6 multicast data. Enable/Disable the function to access.
MLD Snooping	Snooping is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC

	addresses and forwards IPv6 multicast data based on these mappings. Multicast Listener Discovery Snooping (MLD). Enable/Disable the function to access.
Robust Counter	Robust factor of the MLD Counter.
Query Interval	The amount of time between IGMP General Query messages sent by the router (if the router is a querier on this subnet).
Query Response Interval	The maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Response Interval of Last Group Member	The amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

5.5.2 UPnP

Choose **Service** > **UPnP** and the page shown in the following figure appears. This page is used to configure UPnP. The system acts as a daemon after you enable it.



UPnP Configuration

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

UPnP: ○ Disable ● Enable

WAN Interface:

Figure 5-56 UPnP

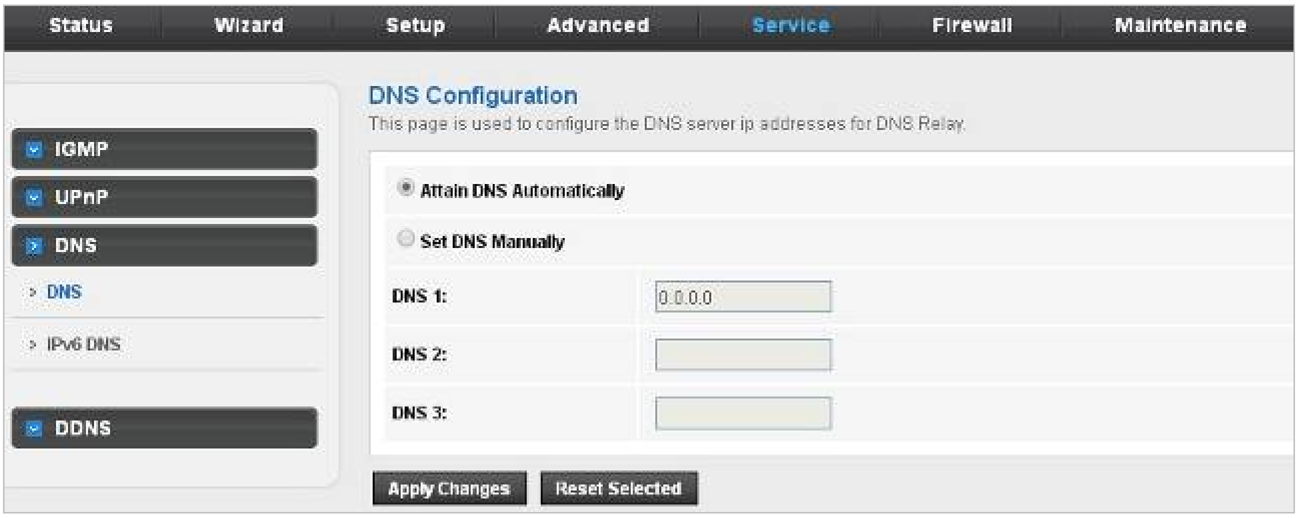
5.5.3 DNS

Domain Name System (DNS) is an Internet service that translates the domain name into IP address. Because the domain name is alphabetic, it is easier to remember. The Internet, however, is based on IP addresses. Every time you use a domain name, DNS translates the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4. The DNS has its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Choose **Service** > **DNS**. The **DNS** page that is displayed contains **DNS** and **IPv6 DNS**.

5.5.3.1 DNS

Click **DNS** in the left pane and the page shown in the following figure appears.



DNS Configuration

This page is used to configure the DNS server ip addresses for DNS Relay.

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: 0.0.0.0

DNS 2:

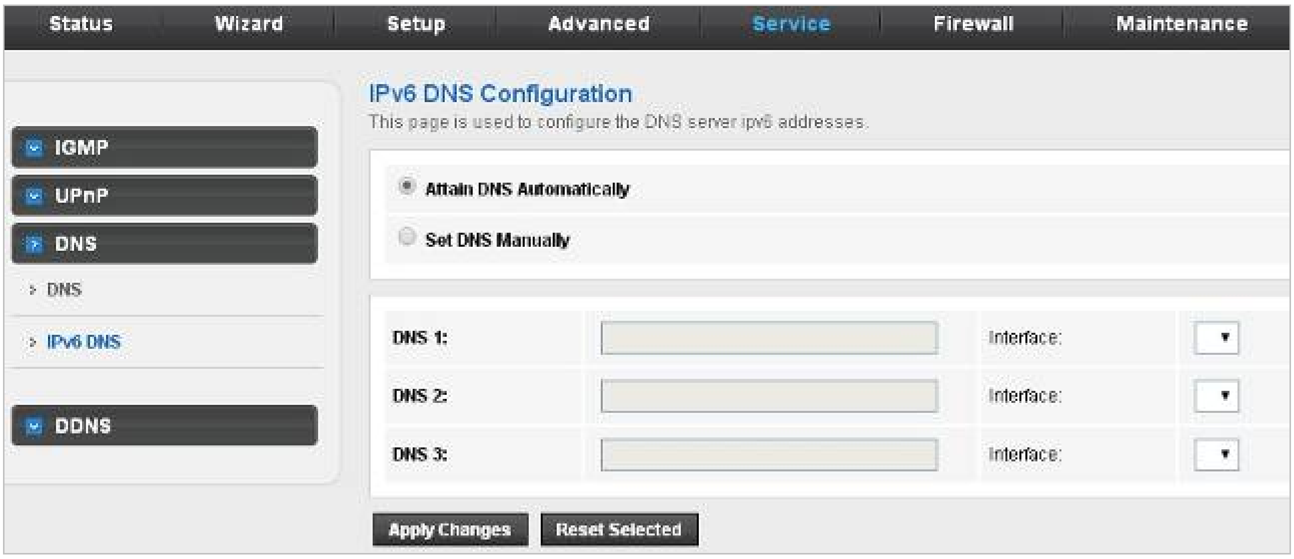
DNS 3:

Figure 5-57 DNS

The following table describes the parameters:

Field	Description
Attain DNS Automatically	Select it, and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it to enter the IP addresses of the DNS 1, DNS 2, DNS 3, servers manually.

5.5.3.2 IPv6 DNS



IPv6 DNS Configuration

This page is used to configure the DNS server ipv6 addresses.

● Attain DNS Automatically

○ Set DNS Manually

DNS 1: Interface: ▼

DNS 2: Interface: ▼

DNS 3: Interface: ▼

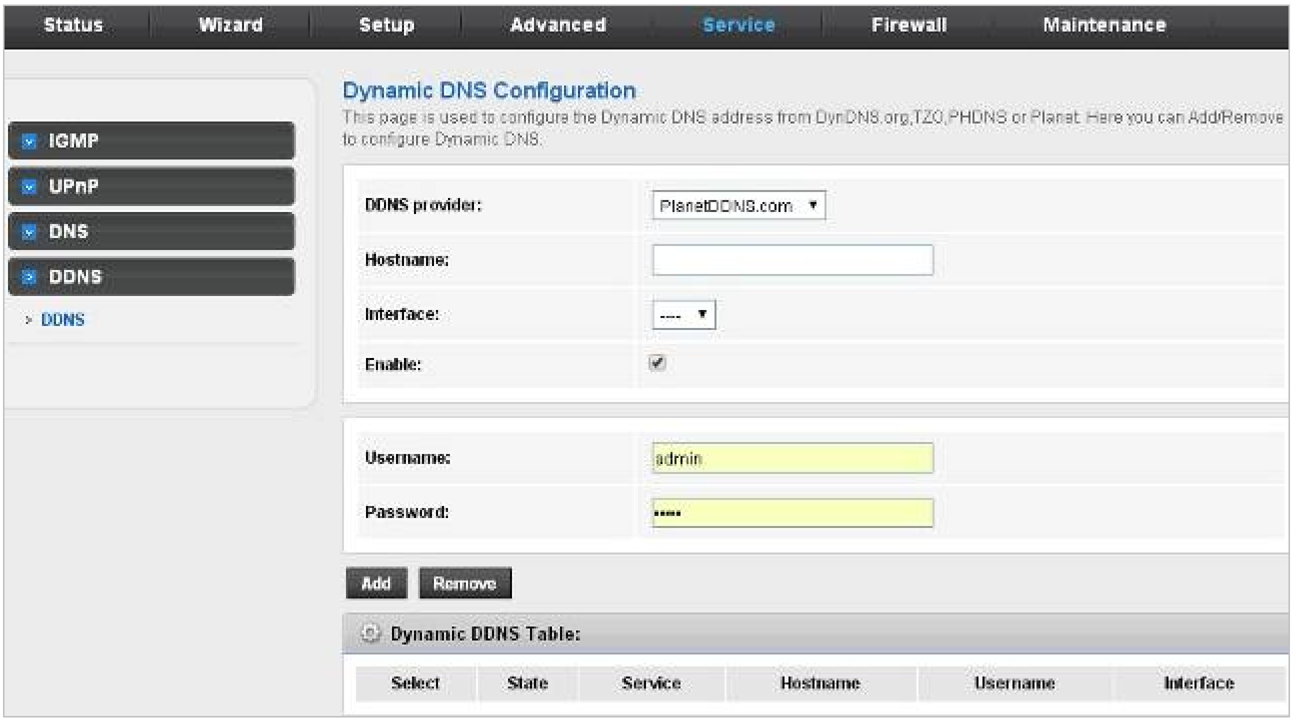
Figure 5-58 IPv6 DNS

The following table describes the parameters:

Field	Description
Attain DNS Automatically	Select it and the router accepts the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the connection establishment.
Set DNS Manually	Select it and enter the IP addresses of the primary and secondary DNS server.

5.5.4 DDNS

Click **DDNS** in the left pane and the page shown in the following figure appears. This page is used to configure the dynamic DNS address from DynDNS.org, TZO, PHDNS, NO-IP or PlanetDDNS. You can add or remove to configure dynamic DNS. The Planet DDNS is free for customers



Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org,TZO,PHDNS or Planet. Here you can Add/Remove to configure Dynamic DNS.

DDNS provider: PlanetDDNS.com

Hostname:

Interface: ----

Enable: ☑

Username: admin

Password: •••••

Dynamic DDNS Table:

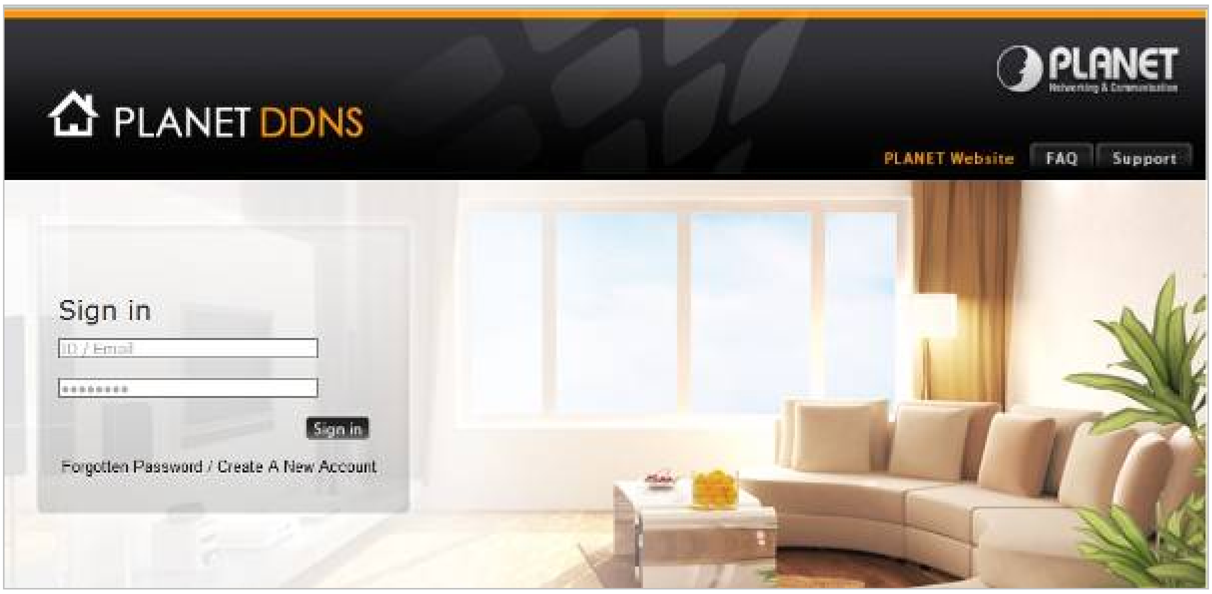
Select	State	Service	Hostname	Username	Interface

Figure 5-59 DDNS

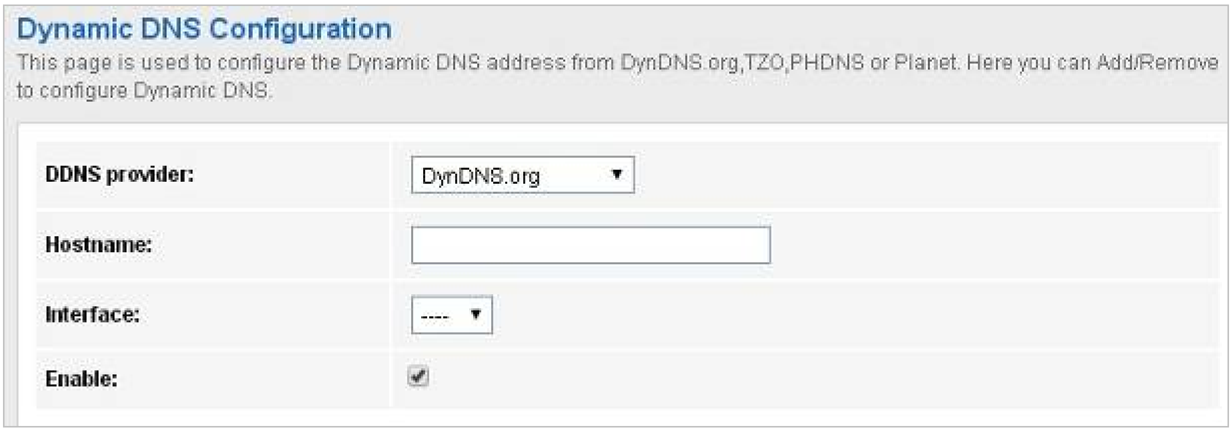
The following table describes the parameters:

Field	Description
DDNS provider	Choose the DDNS provider name. You can choose DynDNS.org, TZO, PHDNS, NO-IP or Planet.
Host Name	The DDNS identifier.
Interface	The WAN interface of the fiber router.
Enable	Enable or disable DDNS function.
Username	The name provided by DDNS provider.
Password	The password provided by DDNS provider.

First of all, please go to http://www.planetddns.com to register a Planet DDNS account, and refer to the FAQ (http://www.planetddns.com/index.php/faq) for how to register a free account.


PLANET DDNS
PLANET Networking & Communication
PLANET Website
FAQ
Support
Sign in
ID / Email
••••••••
Sign in
Forgotten Password / Create A New Account

To select **Service > DDNS**

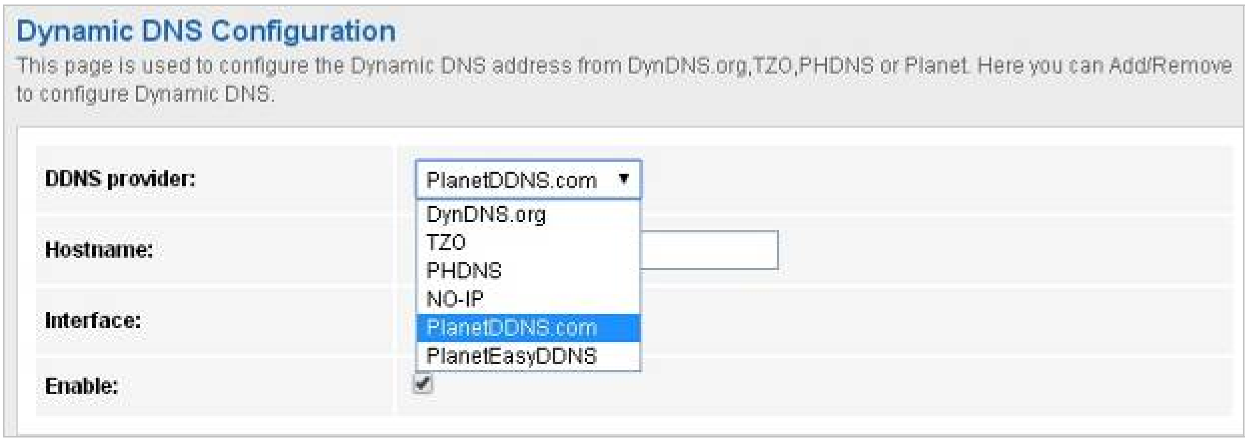


Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org,TZO,PHDNS or Planet. Here you can Add/Remove to configure Dynamic DNS.

DDNS provider:	DynDNS.org ▼
Hostname:	
Interface:	---- ▼
Enable:	☑

Step 1. Select **Planet DDNS**



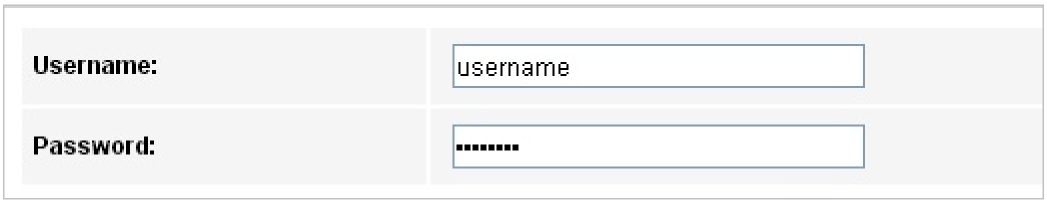
Dynamic DNS Configuration

This page is used to configure the Dynamic DNS address from DynDNS.org,TZO,PHDNS or Planet. Here you can Add/Remove to configure Dynamic DNS.

DDNS provider:	PlanetDDNS.com ▼
Hostname:	
Interface:	
Enable:	☑

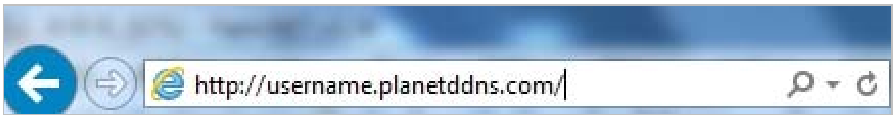
Step 2. Type the User Name for your DDNS account.

Step 3. Type the Password for your DDNS account.



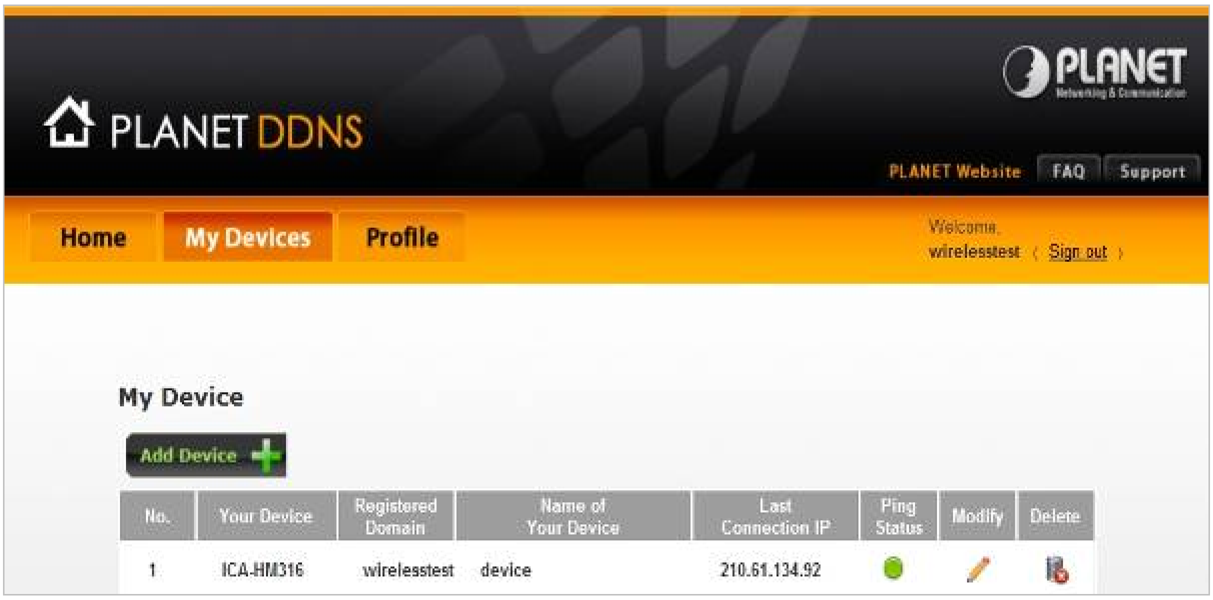
Username:	username
Password:	•••••••••

Apply the settings and ensure you have connected the WAN port to the Internet. In a remote device, enter the Domain Name to the internet browser’s address bar.



http://username.planetddns.com/

You can go to My Devices page of Planet DDNS website to check if the “Last Connection IP” is displayed. This indicates your DDNS service is working properly.



My Device

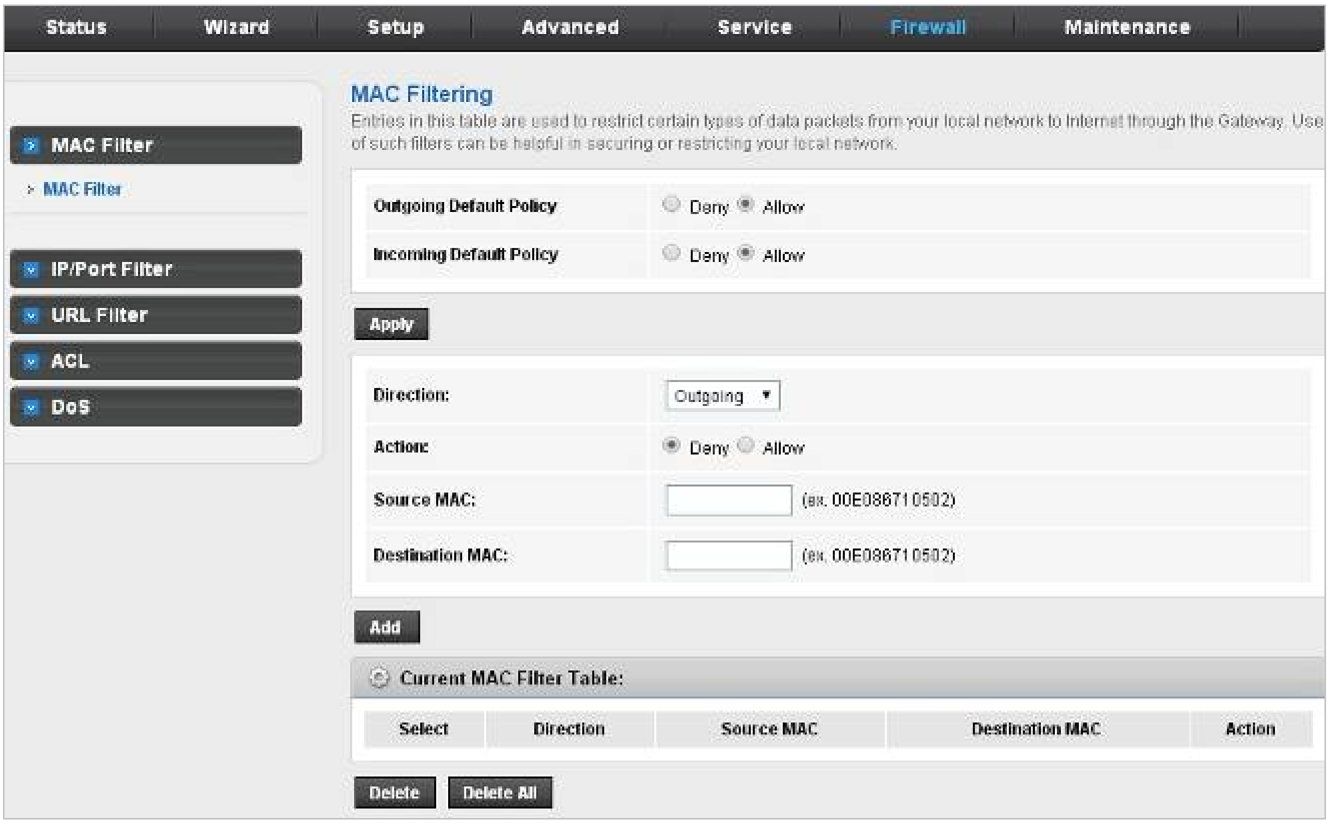
No.	Your Device	Registered Domain	Name of Your Device	Last Connection IP	Ping Status	Modify	Delete
1	ICA-HM316	wirelesstest	device	210.61.134.92	●	✎	🗑

5.6 Firewall

Choose Service > **Firewall** and the Firewall page that is displayed contains **MAC Filter**, **IP/Port Filter**, **URL Filter**, **ACL, DoS** and **Parent Control**.

5.6.1 MAC Filter

Click **MAC Filter** in the left pane and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets from your local network to Internet through the gateway. These filters are helpful in securing or restricting your local network.



MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy ○ Deny ● Allow

Incoming Default Policy ○ Deny ● Allow

Direction: Outgoing

Action: ● Deny ○ Allow

Source MAC: (ex. 00E086710502)

Destination MAC: (ex. 00E086710502)

Current MAC Filter Table:

Select	Direction	Source MAC	Destination MAC	Action

Figure 5-60 MAC Filter

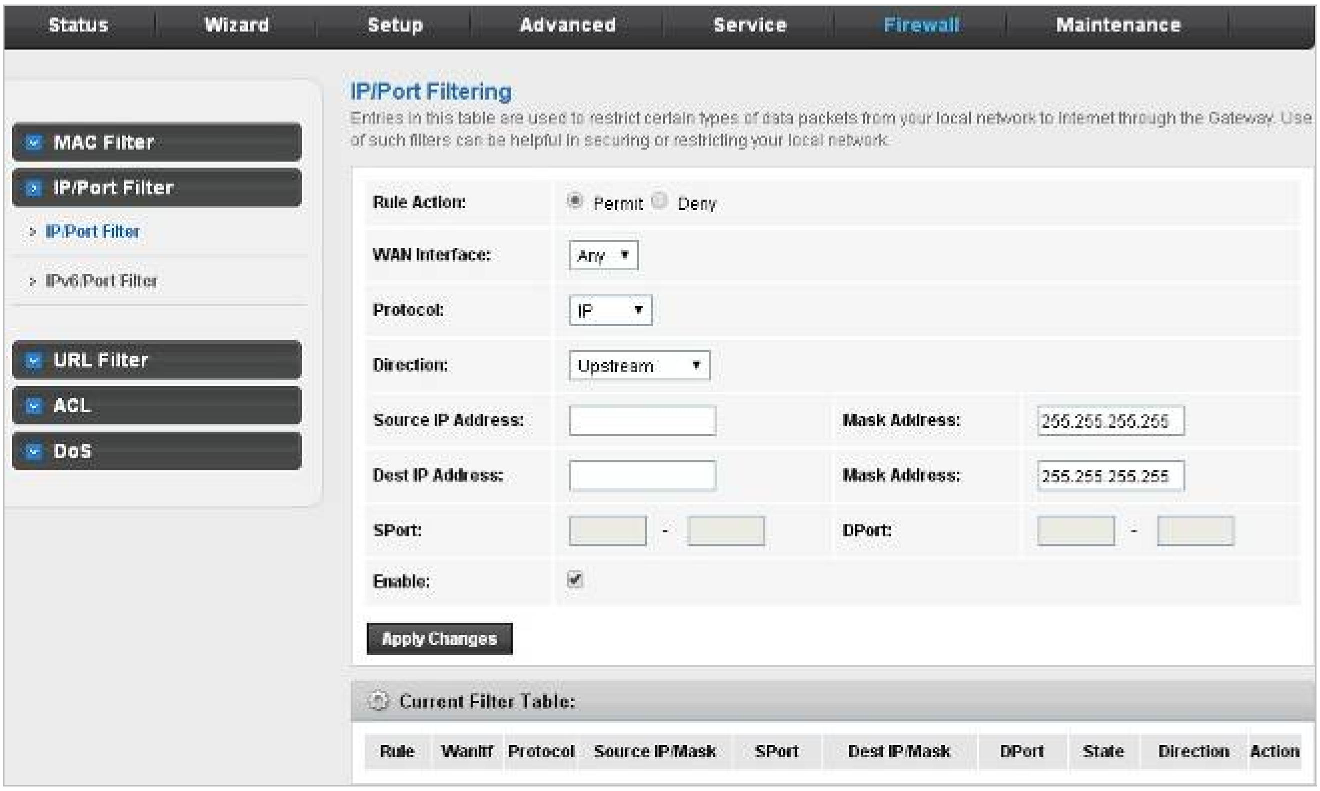
The following table describes the parameters:

Field	Description
Outgoing Default Policy	Specify the default action on the LAN to WAN bridging/forwarding path.
Incoming Default Policy	Specify the default action on the WAN to LAN bridging/forwarding path.
Direction	Traffic **Outgoing**/**Incoming** direction.
Action	Deny or allow traffic when matching this rule.
Source MAC	The source MAC address must be xxxxxxxxxxxx format.
Destination MAC	The destination MAC address must be xxxxxxxxxxxx format.

5.6.2 IP/Port Filter

5.6.2.1 IP/Port Filter

Click **IP/Port Filter** in the left pane and the page shown in the following figure appears. Entries in the table are used to restrict certain types of data packets through the gateway. These filters are helpful in securing or restricting your local network.



IP/Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Rule Action: ● Permit ○ Deny

WAN Interface: Any

Protocol: IP

Direction: Upstream

Source IP Address: Mask Address: 255.255.255.255

Dest IP Address: Mask Address: 255.255.255.255

SPort: - DPort: -

Enable: ☑

Current Filter Table:

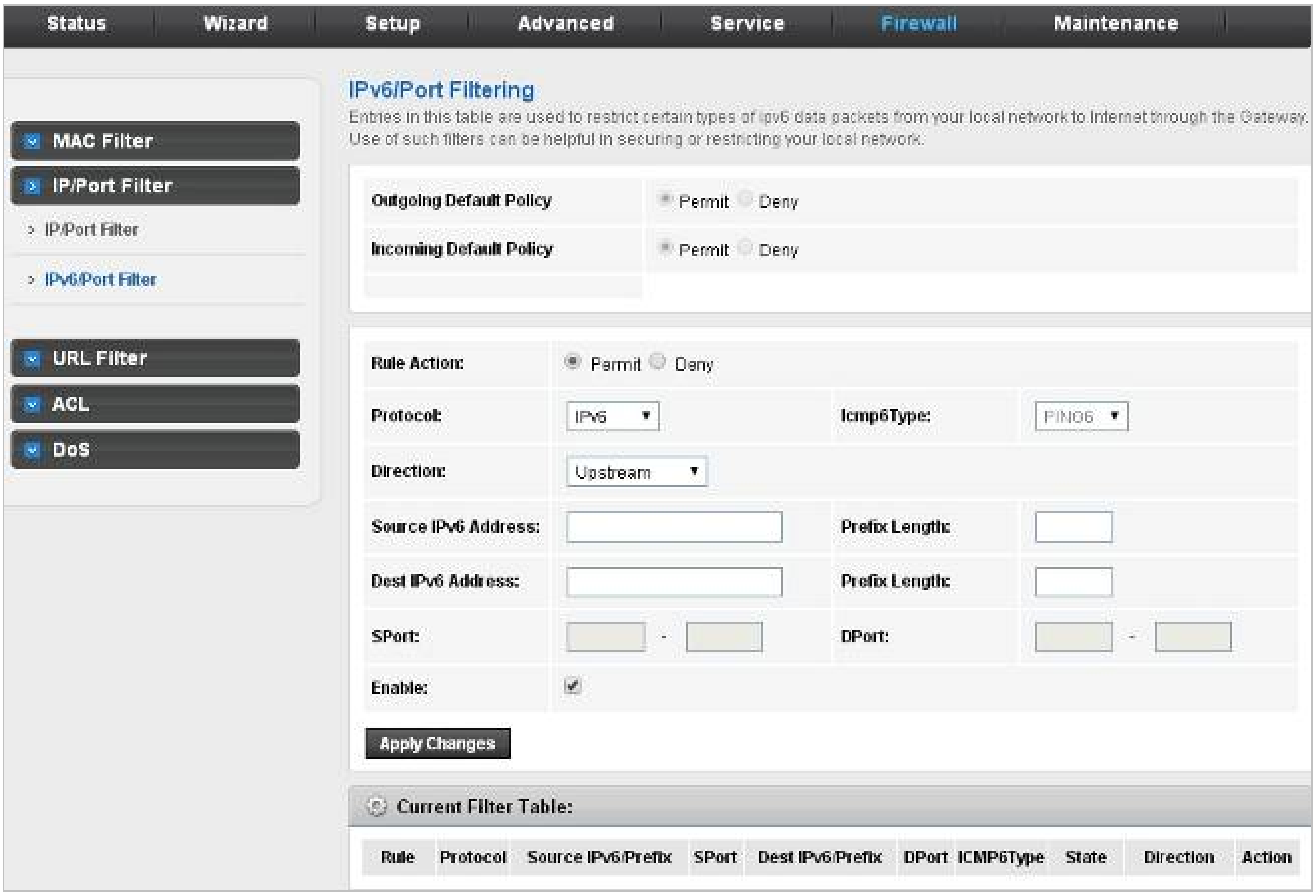
Rule	WanItf	Protocol	Source IP/Mask	SPort	Dest IP/Mask	DPort	State	Direction	Action

Figure 5-61 IP/Port Filter

The following table describes the parameters:

Field	Description
Rule Action	Permit or deny traffic when matching this rule.
WAN Interface	Select the WAN interface of the fiber router.
Protocol	There are 4 options available: **IP**, **ICMP**, **TCP**, and **UDP**.
Direction	Traffic forwarding direction.
Source IP Address	The source IP address assigned to the traffic on which filtering is applied.
Mask Address	Subnet-mask of the source IP.
S Port	Starting and ending source port numbers.
Dest IP Address	The destination IP address assigned to the traffic on which filtering is applied.
Mask Address	Subnet-mask of the destination IP.
D Port	Starting and ending destination port numbers.
Enable	Enable/Disable the function to access.

5.6.2.2 IPv6/Port Filter



IPv6/Port Filtering

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Outgoing Default Policy	● Permit ○ Deny
Incoming Default Policy	● Permit ○ Deny

Rule Action:	● Permit ○ Deny		
Protocol:	IPV6 ▾	Icmp6Type:	PING6 ▾
Direction:	Upstream ▾		
Source IPv6 Address:		Prefix Length:	
Dest IPv6 Address:		Prefix Length:	
SPort:	-	DPort:	-
Enable:	☑		

Current Filter Table:

Rule	Protocol	Source IPv6/Prefix	SPort	Dest IPv6/Prefix	DPort	ICMP6Type	State	Direction	Action

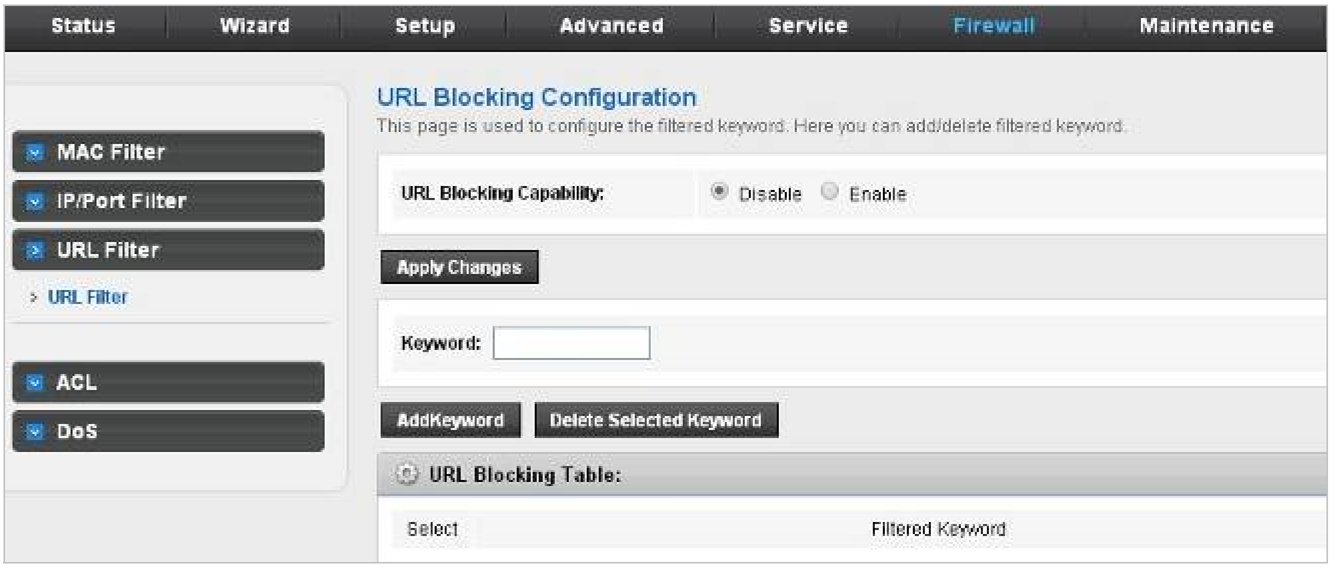
Figure 5-62 IPv6/Port Filter

The following table describes the parameters:

Field	Description
Rule Action	Permit or deny traffic when matching this rule.
Protocol	There are 4 options available: **IPv6**, **ICMP6**, **TCP**, and **UDP**.
ICMP6 Type	Select the PING6 type.
Direction	Traffic forwarding direction.
Source IPv6 Address	The source IP address assigned to the traffic on which filtering is applied.
Prefix Length	Subnet-mask of the source IP.
S Port	Starting and ending source port numbers.
Dest IPv6 Address	The destination IP address assigned to the traffic on which filtering is applied.
Prefix Length	Subnet-mask of the destination IP.
D Port	Starting and ending destination port numbers.
Enable	Enable/Disable the function to access.

5.6.3 URL Filter

Click **URL Filter** in the left pane and the page shown in the following figure appears. This page is used to block a fully qualified domain name, such as tw.yahoo.com and filtered keyword (yahoo). You can add or delete fully qualified domain name and filtered keyword.



URL Blocking Configuration

This page is used to configure the filtered keyword. Here you can add/delete filtered keyword.

URL Blocking Capability: ● Disable ○ Enable

Keyword:

URL Blocking Table:

Select	Filtered Keyword

Figure 5-63 URL Filter

The following table describes the parameters:

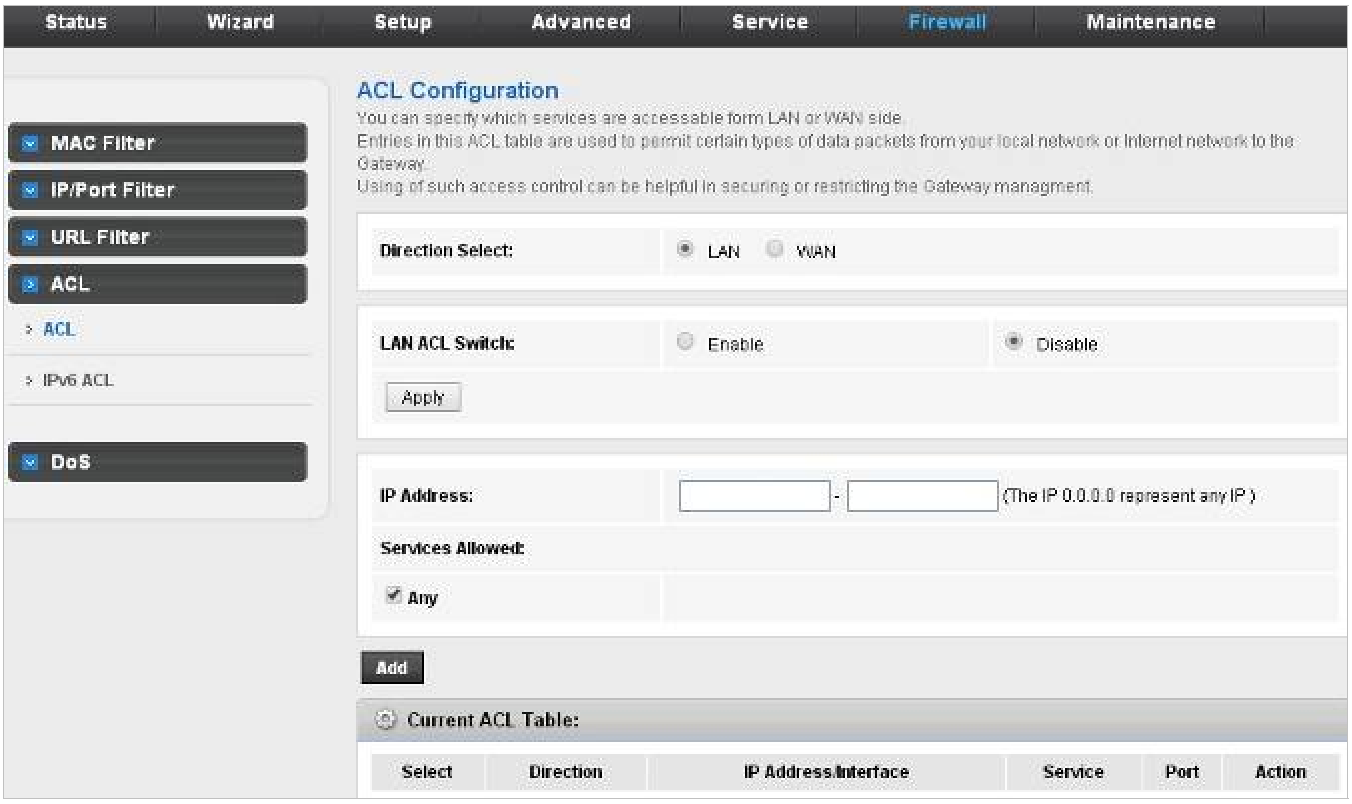
Field	Description
URL Blocking Capability	You can choose **Disable** or **Enable**. ● Select **Disable** to disable URL blocking and keyword filtering function. ● Select **Enable** to block access to the URLs and keywords specified in the **URL Blocking Table**.
Keyword	Enter the keyword to block.
Add Keyword	Click it to add a URL/keyword to the **URL Blocking Table**.
Delete Selected Keyword	Select a row in the **URL Blocking Table** and click it to delete the row.
URL Blocking Table	A list of the URLs to which access is blocked.

5.6.4 ACL

5.6.4.1 ACL

Choose **Service** > **ACL** and the page shown in the following figure appears. On this page, you can permit the data packets from LAN or WAN to access the router. You can configure the IP address for Access Control List (ACL). If ACL is enabled, only the effective IP address in the ACL can access the router.

Note	If you select **Enable** in ACL capability, ensure that your host IP address is in ACL list before it takes effect.



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ● LAN ○ WAN

LAN ACL Switch: ○ Enable ● Disable

Apply

IP Address: [ ] - [ ] (The IP 0.0.0.0 represent any IP)

Services Allowed:

☑ Any

Add

Current ACL Table:

Select	Direction	IP Address/Interface	Service	Port	Action

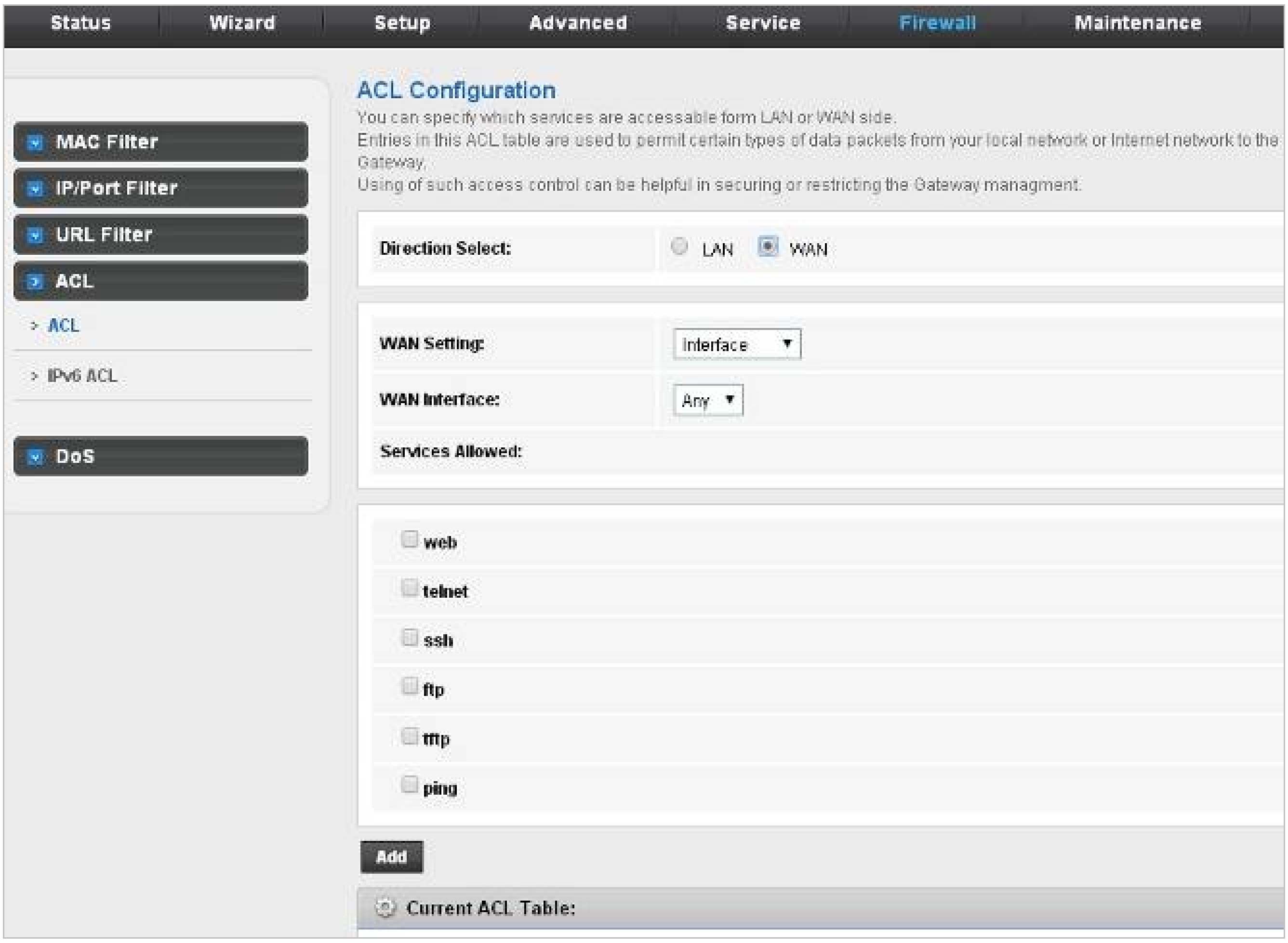
Figure 5-64 ACL

The following table describes the parameters:

Field	Description
Direction Select	Select the router interface. You can select **LAN** or **WAN**. In this example, **LAN** is selected.
LAN ACL Switch	Select it to enable or disable ACL function.
IP Address	Enter the IP address of the specified interface. Only the IP address that is in the same network segment with the IP address of the specified interface can access the router.

Services Allowed	You can choose the following services from LAN: **Web**, **Telnet**, **SSH**, **FTP**, **TFTP**, **SNMP**, or **PING**. You can also choose all the services.
Add	After setting the parameters, click it to add an entry to the **Current ACL Table**.

If **WAN** is selected in the field of **Direction Select**, the page is shown in the following figure.



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ○ LAN ● WAN

WAN Setting: Interface

WAN Interface: Any

Services Allowed:

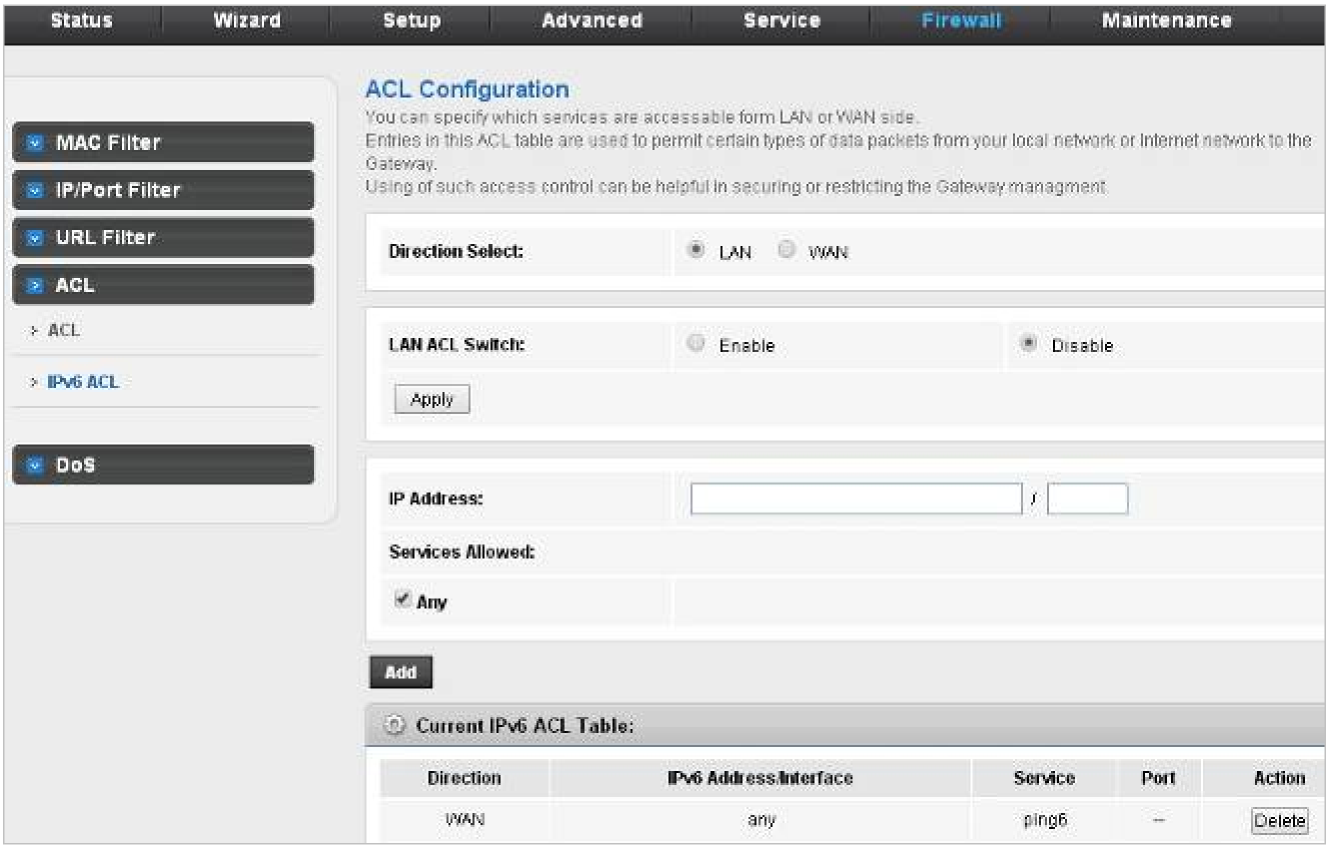
□ web
□ telnet
□ ssh
□ ftp
□ tftp
□ ping

Current ACL Table:

Figure 5-65 ACL WAN

5.6.4.2 IPv6 ACL

Choose **Service** > **IPv6 ACL** and the page shown in the following figure appears.



ACL Configuration

You can specify which services are accessable form LAN or WAN side.
Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.
Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ● LAN ○ WAN

LAN ACL Switch: ○ Enable ● Disable

Apply

IP Address: /

Services Allowed:

☑ Any

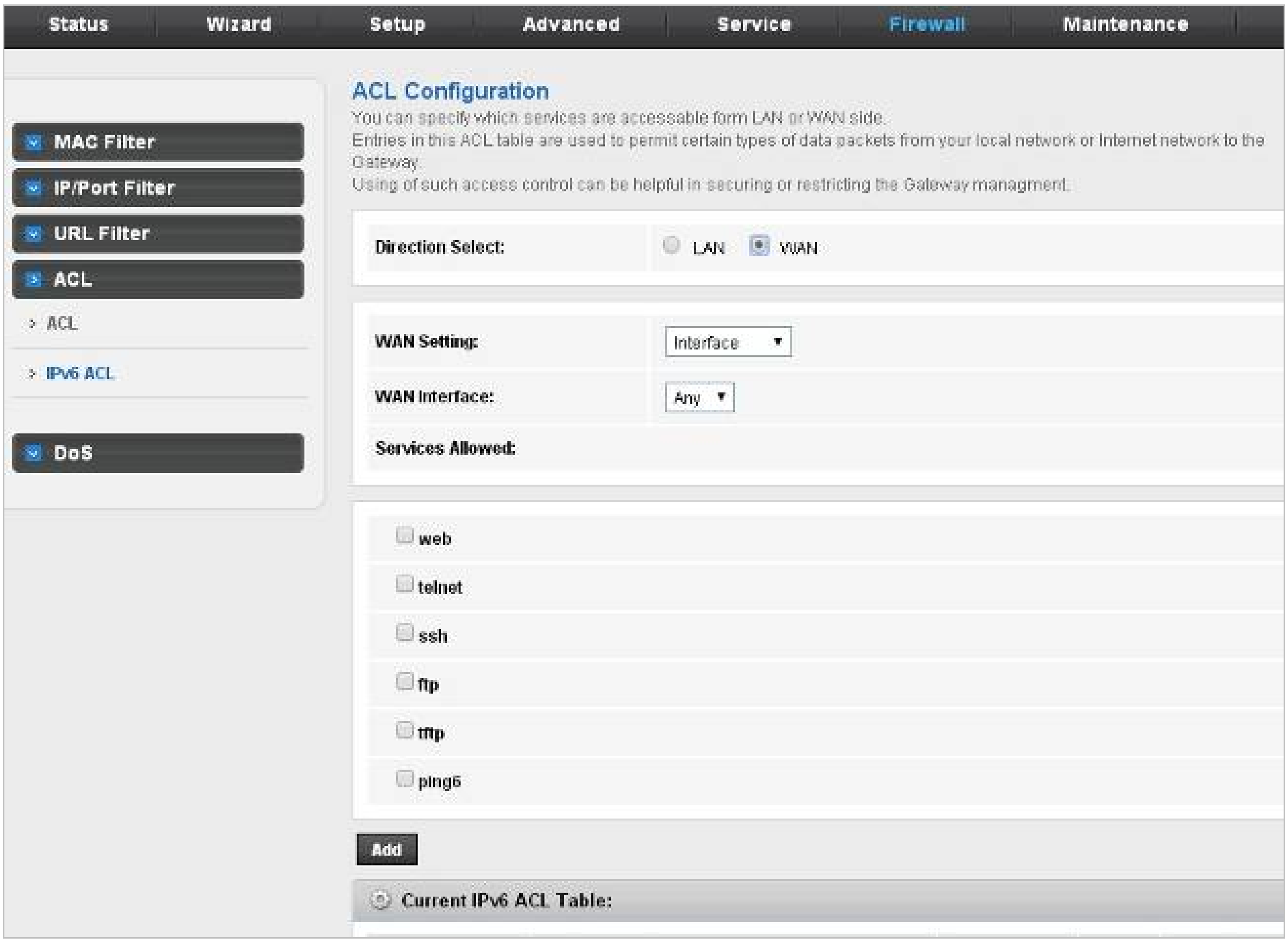
Add

Current IPv6 ACL Table:

Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	Delete

Figure 5-66 IPv6 ACL

If **WAN** is selected in the field of **Direction Select**, the page is shown in the following figure.



ACL Configuration

You can specify which services are accessable form LAN or WAN side.

Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway.

Using of such access control can be helpful in securing or restricting the Gateway managment.

Direction Select: ○ LAN ● WAN

WAN Setting: Interface

WAN Interface: Any

Services Allowed:

□ web

□ telnet

□ ssh

□ ftp

□ tftp

□ ping6

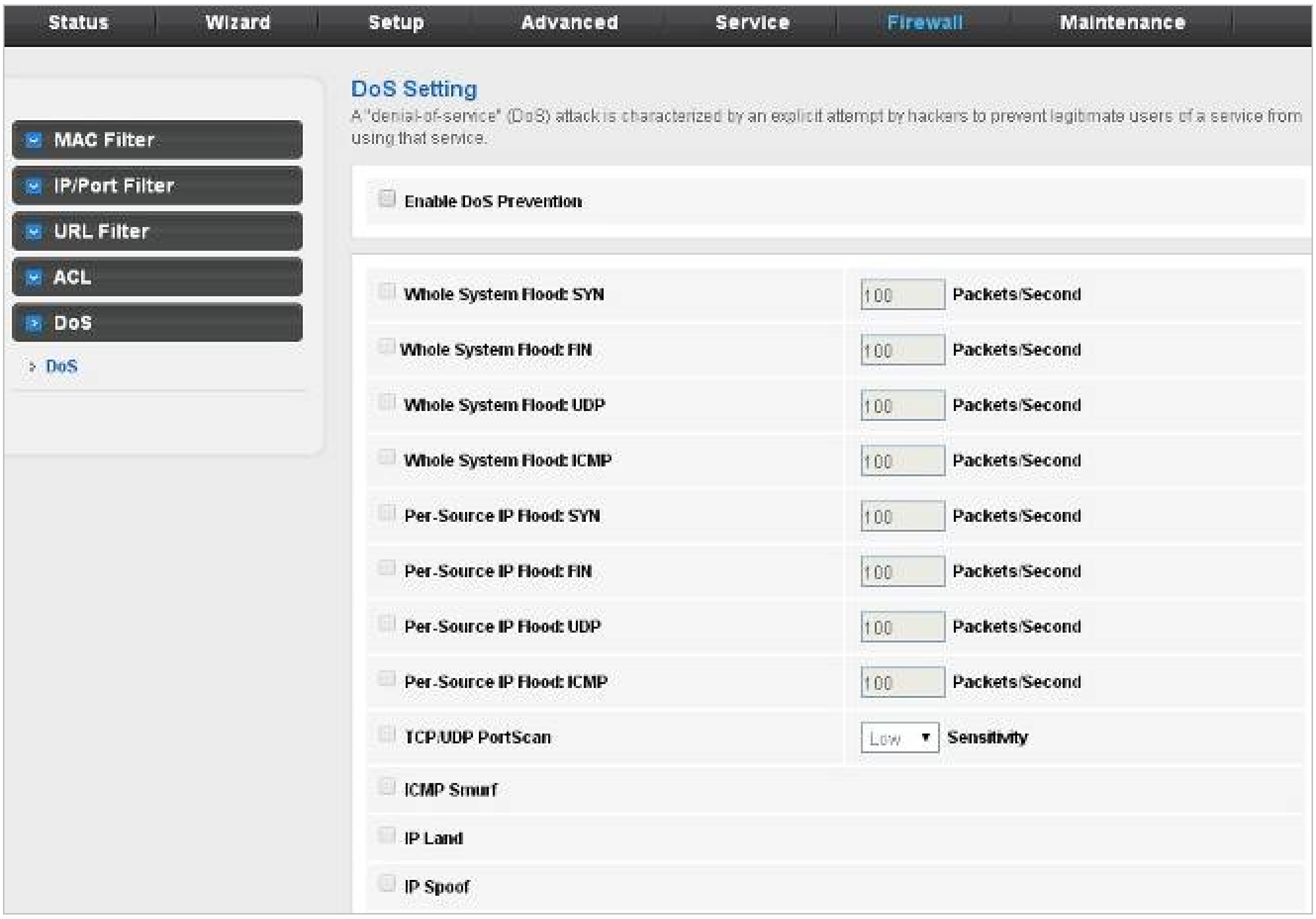
Add

Current IPv6 ACL Table:

Figure 5-67 IPv6 ACL WAN

5.6.5 DoS

Denial-of-Service Attack (DoS attack) is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.



DoS Setting

A "denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☐ Enable DoS Prevention

☐ Whole System Flood: SYN 100 Packets/Second
☐ Whole System Flood: FIN 100 Packets/Second
☐ Whole System Flood: UDP 100 Packets/Second
☐ Whole System Flood: ICMP 100 Packets/Second
☐ Per-Source IP Flood: SYN 100 Packets/Second
☐ Per-Source IP Flood: FIN 100 Packets/Second
☐ Per-Source IP Flood: UDP 100 Packets/Second
☐ Per-Source IP Flood: ICMP 100 Packets/Second
☐ TCP/UDP PortScan Low ▾ Sensitivity
☐ ICMP Smurf
☐ IP Land
☐ IP Spoof

Figure 5-68 DoS

The following table describes the parameters:

Field	Description
Enable DoS Prevention	Enable denial-of-service feature to access.
Enable Source IP Blocking	Enable the function to block IP Source and set the time in seconds.

5.7 Maintenance

In the navigation bar, click Maintenance. The Maintenance page displayed contains **Update**, **Password**, **Reboot**, **Time**, **Log** and **Diagnostics**.

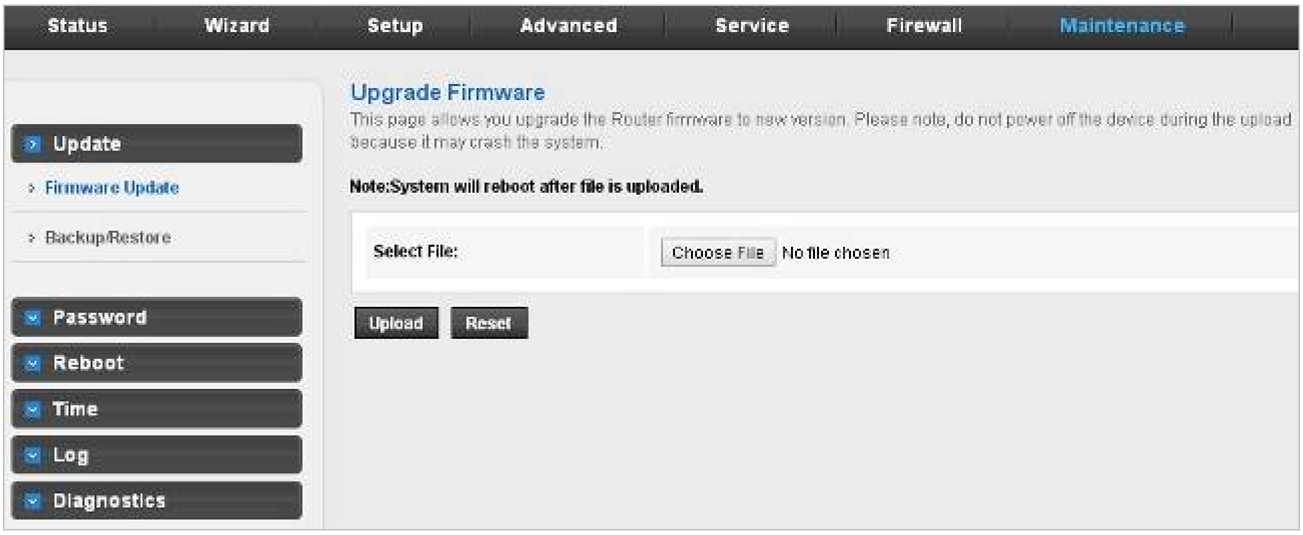
5.7.1 Update

Choose **Maintenance** > **Update**. The **Update** page displayed contains **Upgrade Firmware** and **Backup/Restore**.

Caution	Do not turn off the router or press the Reset button while the procedure is in progress.

5.7.1.1 Firmware Update

Click **Firmware** Update in the left pane and the page shown in the following figure appears. On this page, you can upgrade the firmware of the router.



Upgrade Firmware

This page allows you upgrade the Router firmware to new version. Please note, do not power off the device during the upload because it may crash the system.

Note:System will reboot after file is uploaded.

Select File: Choose File No file chosen

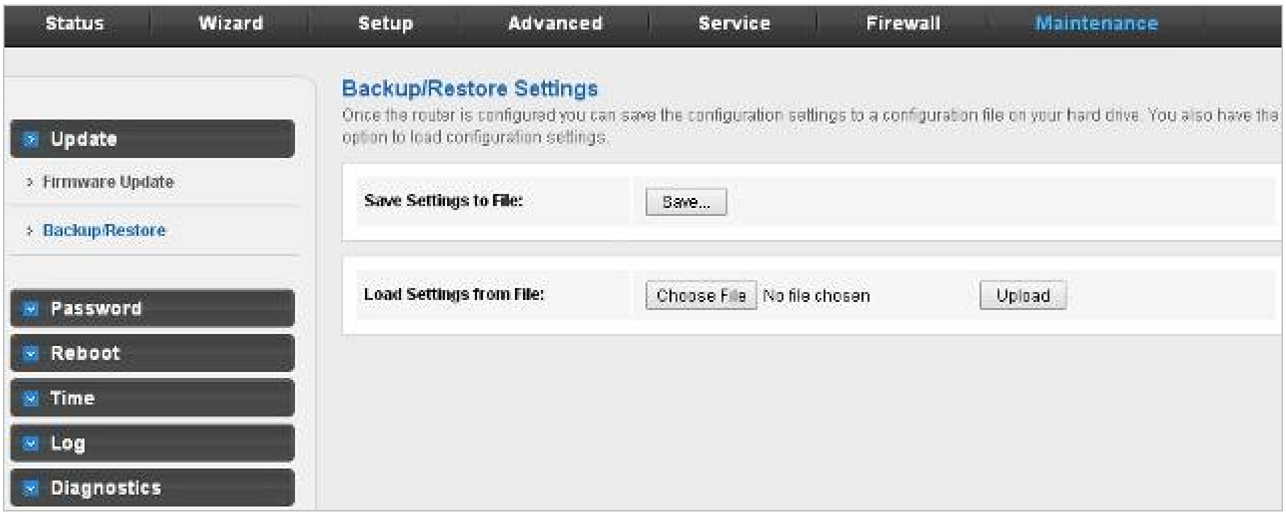
Figure 5-69 Firmware Update

The following table describes the parameters:

Field	Description
Select File	Click **Browse** or **Choose File** to select the firmware file.
Upload	After selecting the firmware file, click **Upload** to start upgrading the firmware file.
Reset	Click it to start selecting the firmware file.

5.7.1.2 Backup/Restore

Click **Backup/Restore** in the left pane and the page shown in the following figure appears. You can back up the current settings to a file and restore the settings from the file that was saved previously.



Backup/Restore Settings

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings.

Save Settings to File:

Load Settings from File: No file chosen

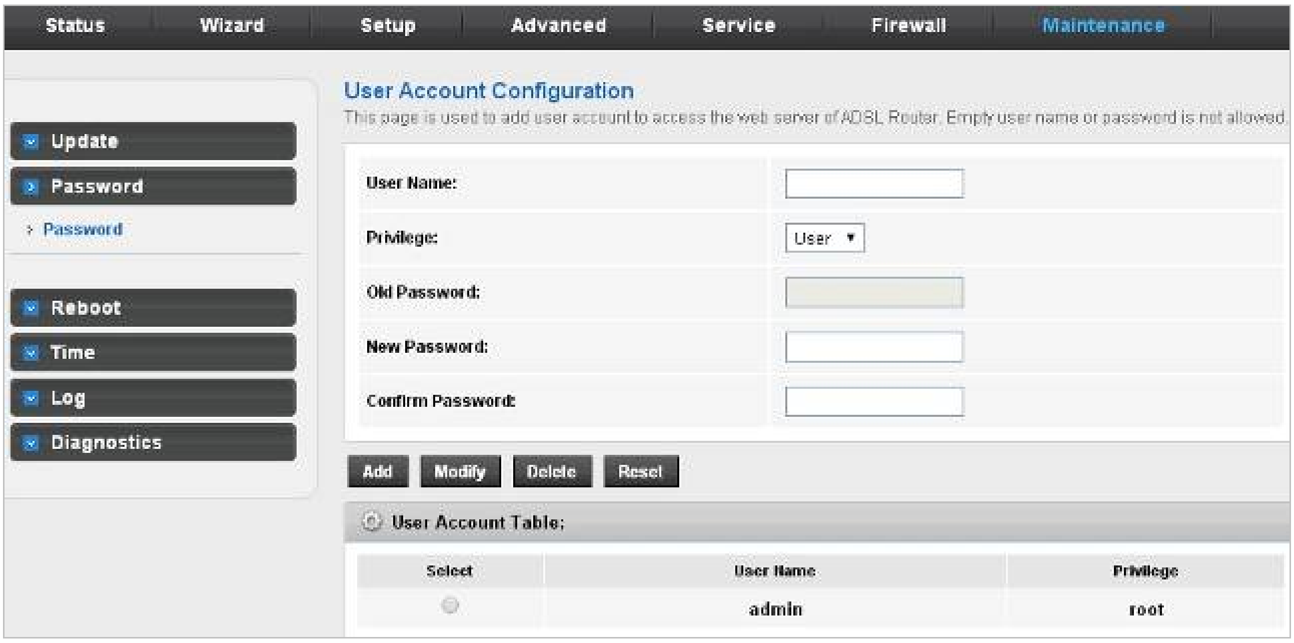
Figure 5-70 Backup/Restore

The following table describes the parameters:

Field	Description
Save Settings to File	Click it and select the path. Then you can save the configuration file of the router.
Load Settings from File	Click **Browse** or **Choose File** to select the configuration file.
Upload	After selecting the configuration file of the router, click **Upload** to start uploading the configuration file of the router.

5.7.2 Password

Choose **Maintenance** > **Password** and the page shown in the following figure appears. By default, the user name and password of the administrator are **admin** and **admin** respectively. The user name and password of the common user are **user** and **user** respectively.



User Account Configuration

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

User Name:	
Privilege:	User
Old Password:	
New Password:	
Confirm Password:	

User Account Table:

Select	User Name	Privilege
○	admin	root

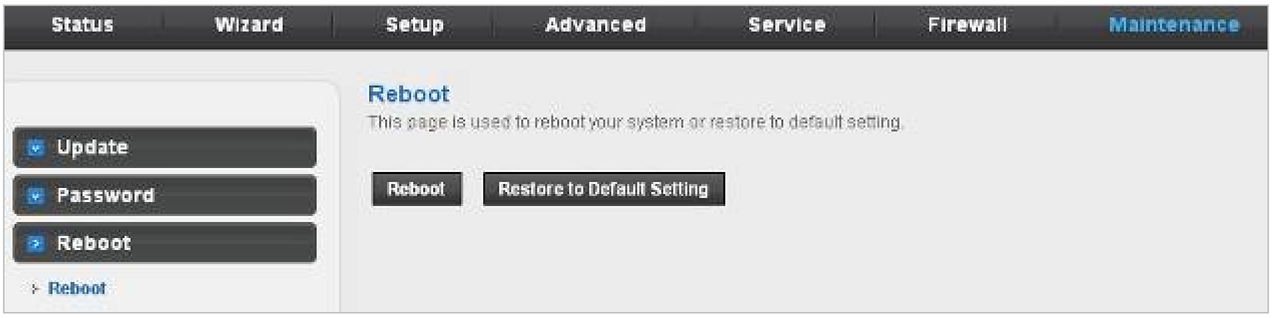
Figure 5-71 Password

The following table describes the parameters:

Field	Description
User Name	Choose the user name for accessing the router. You can choose **admin** or **user**.
Privilege	Choose the privilege for the account.
Old Password	Enter the old password
New Password	Enter your new password to which you want to change.
Confirmed Password	For confirmation, enter the new password again.

5.7.3 Reboot

Choose **Maintenance** > **Reboot** and the page shown in the following figure appears. You can set the router reset to the default settings or set the router to commit the current settings.



Reboot

This page is used to reboot your system or restore to default setting.

Figure 5-72 Reboot

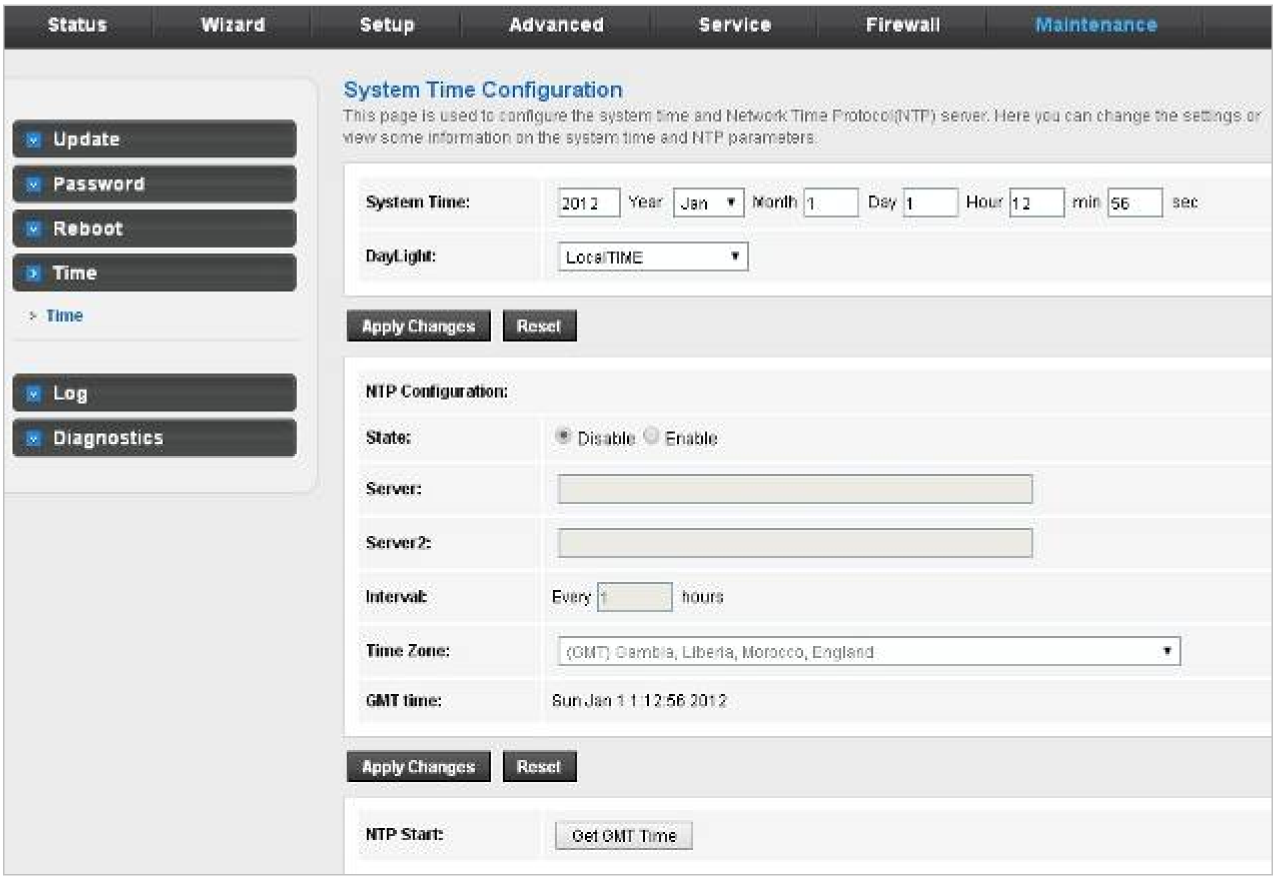
The following table describes the parameters:

Field	Description
Reboot	It takes around 30 seconds to reboot the device and then again log in User Name and Password.
Restore to Default Setting	It helps to change to default settings. It takes around 30 seconds to restart the device and then again log in User Name and Password.

Note	Do not turn off the FRT-415N or press the reset button while this procedure is in progress.

5.7.4 Time

Choose **Maintenance** > **Time** and the page shown in the following figure appears. You can configure the system time manually or get the system time from the time server.



System Time Configuration

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

System Time:	2012 Year Jan Month 1 Day 1 Hour 12 min 56 sec
DayLight:	LocalTIME

NTP Configuration:	
State:	● Disable ○ Enable
Server:	
Server2:	
Interval:	Every 1 hours
Time Zone:	(GMT) Gambia, Liberia, Morocco, England
GMT time:	Sun Jan 1 1:12:56 2012

NTP Start: Get GMT Time

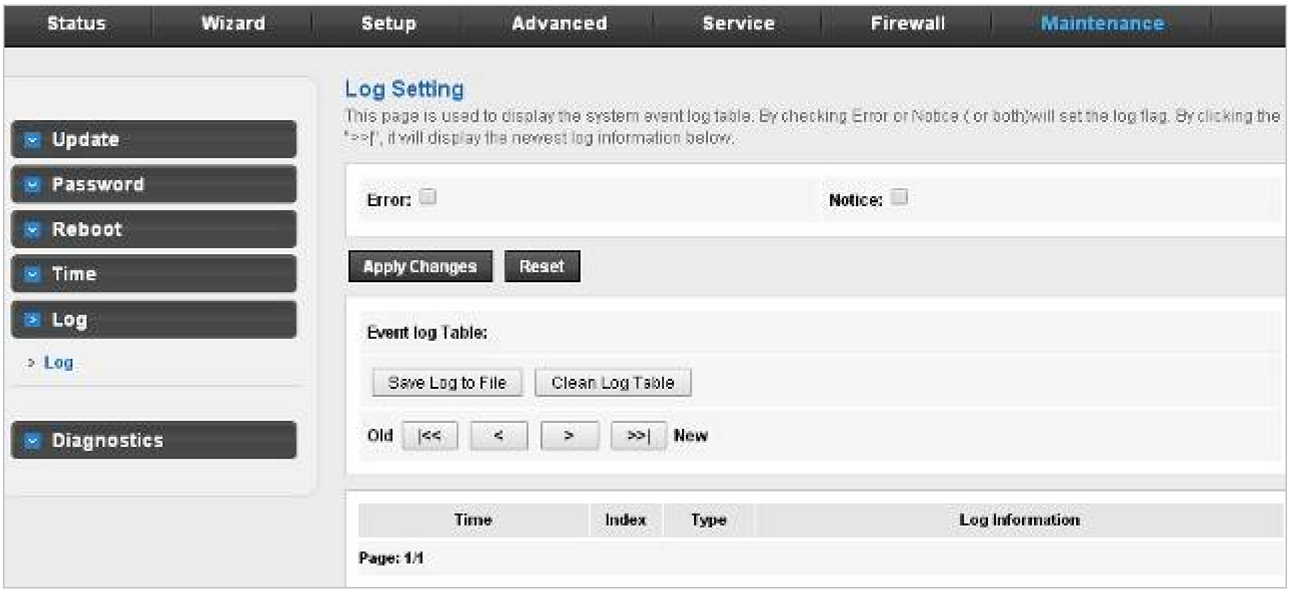
Figure 5-73 Time

The following table describes the parameters:

Field	Description
System Time	Configure the system time manually.
Day Light	Daylight Saving Time.
State	Enable the option to update the system clock automatically. Disable the option to update the system clock manually.
Server	Configure the primary NTP server manually.
Server2	Configure the secondary NTP server manually.
Interval	NTP updating time interval.
Time Zone	Choose the time zone of your country from the drop-down list.
GMT Time	Greenwich Mean time.

5.7.5 Log

Choose **Maintenance** > **Log** and the page shown in the following figure appears. On this page, you can enable or disable system log function and view the system log.



Log Setting

This page is used to display the system event log table. By checking Error or Notice (or both)will set the log flag. By clicking the ">>|", it will display the newest log information below.

Error: □ Notice: □

Event log Table:

Time	Index	Type	Log Information

Page: 1/1

Figure 5-74 Log

The following table describes the parameters:

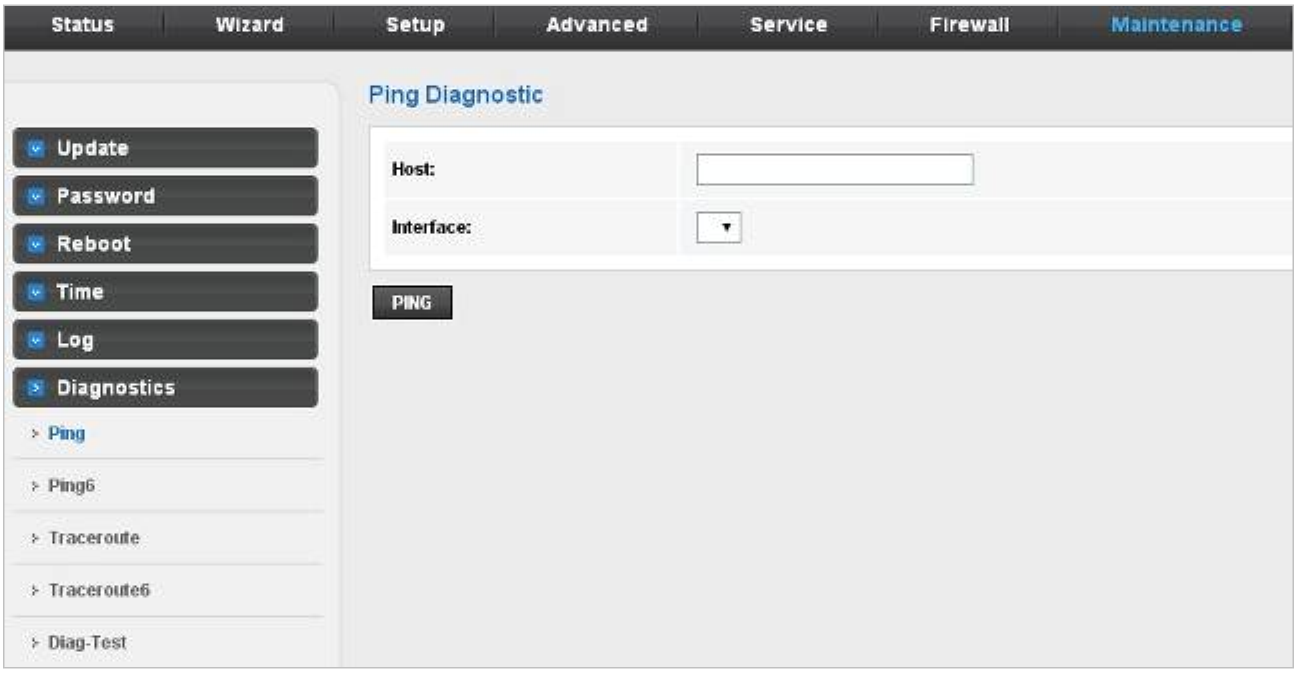
Field	Description
Error	Enable/Disable the function to display the Error.
Notice	Enable/Disable the function to notify the Error.

5.7.6 Diagnostic

In the navigation bar, click **Diagnostic**. The **Diagnostic** page displayed contains **Ping**, **Ping6**, **Traceroute**, **Traceroute6**, and **Diag-Test**.

5.7.6.1 Ping

Choose **Diagnostic** > **Ping** and the page shown in the following figure appears.



Ping Diagnostic

Host:

Interface:

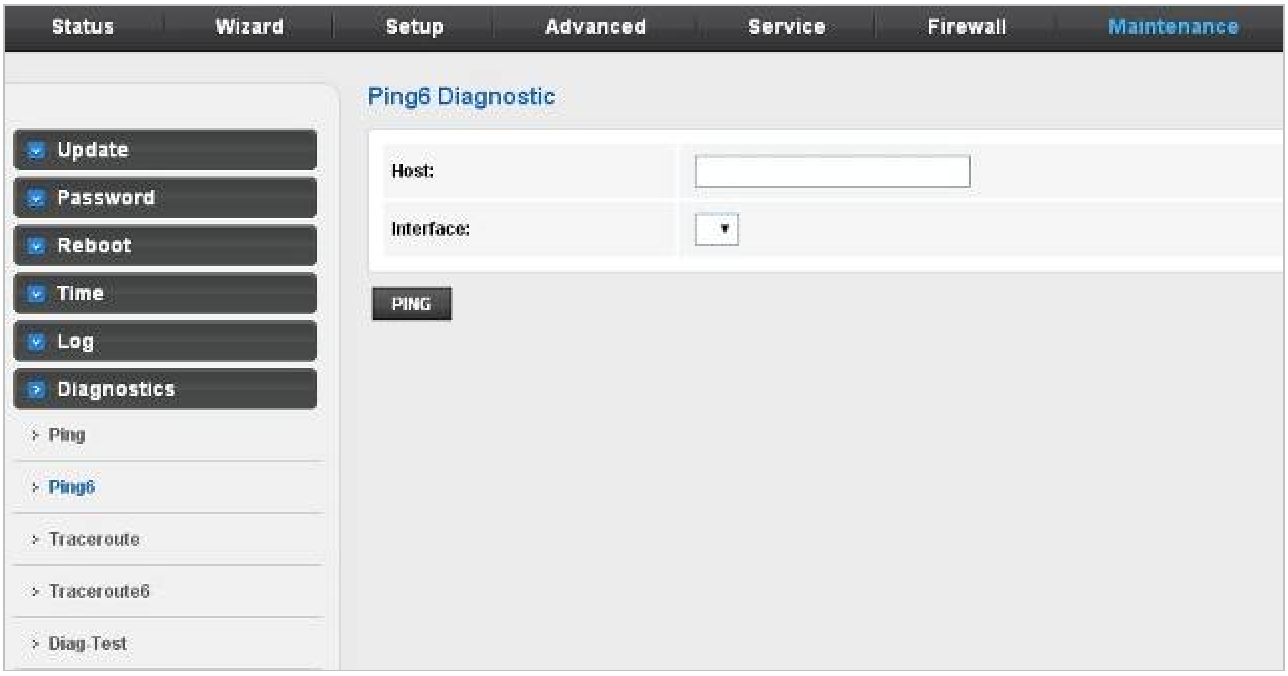
Figure 5-75 Ping

The following table describes the parameters:

Field	Description
Host Address	Enter IP address you want to ping.
Interface	Choose a WAN interface.

5.7.6.2 Ping6

Choose **Diagnostic** > **Ping6** and the page shown in the following figure appears.



Ping6 Diagnostic

Host:

Interface:

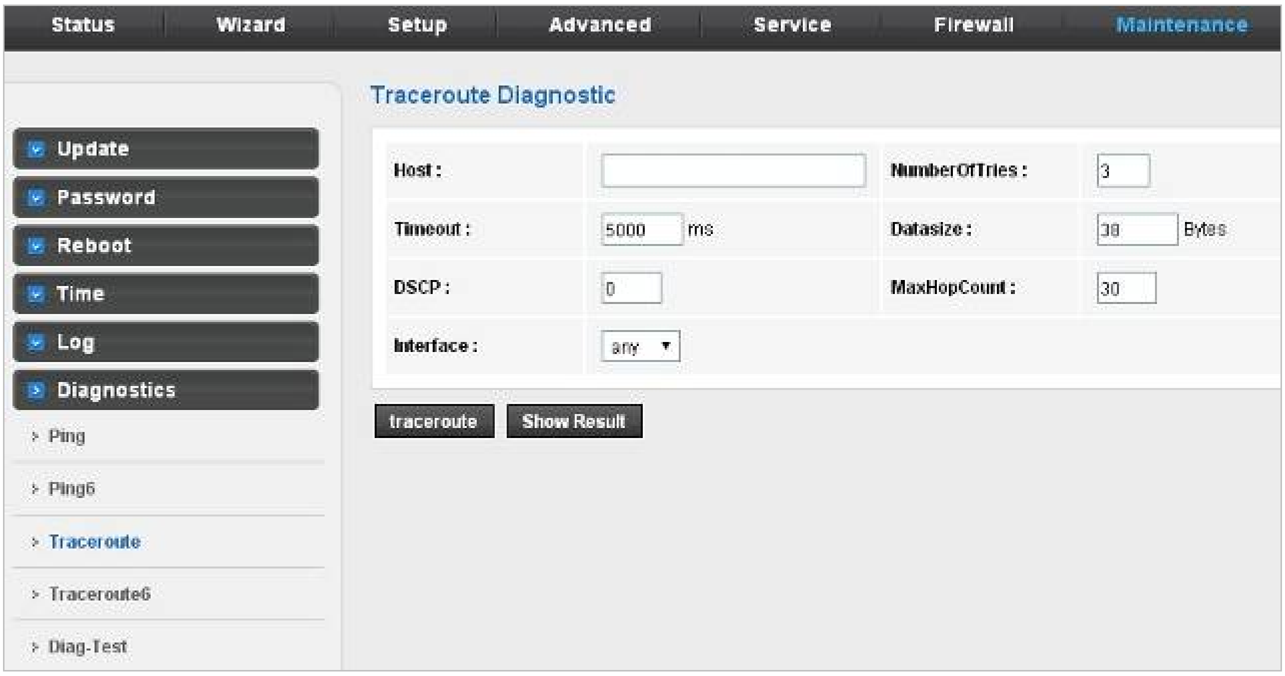
Figure 5-76 Ping6

The following table describes the parameters:

Field	Description
Host Address	Enter IPv6 address you want to ping.
Interface	Choose a WAN interface.

5.7.6.3 Traceroute

Choose **Diagnostic** >**Traceroute** and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the other side host on the Internet.



Traceroute Diagnostic

Host :		NumberOfTries :	3
Timeout :	5000 ms	Datasize :	38 Bytes
DSCP :	0	MaxHopCount :	30
Interface :	any		

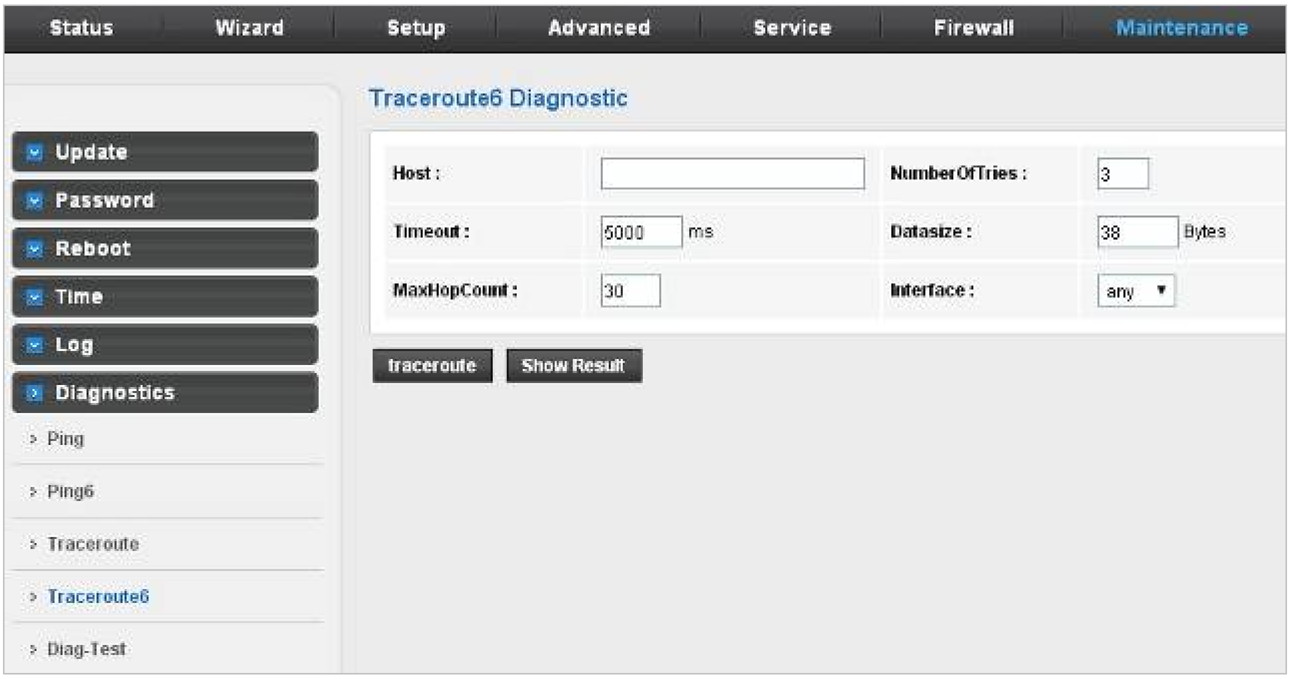
Figure 5-77 Traceroute

The following table describes the parameters:

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
DSCP	Differentiated Services Code Point, You should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.

5.7.6.4 Traceroute6

Choose **Diagnostic** >**Traceroute6** and the following page appears. By Traceroute Diagnostic, you can track the route path through the information which is from your computer to the other side host on the Internet.



Traceroute6 Diagnostic

Host :		NumberOfTries :	3
Timeout :	5000 ms	Datasize :	38 Bytes
MaxHopCount :	30	Interface :	any

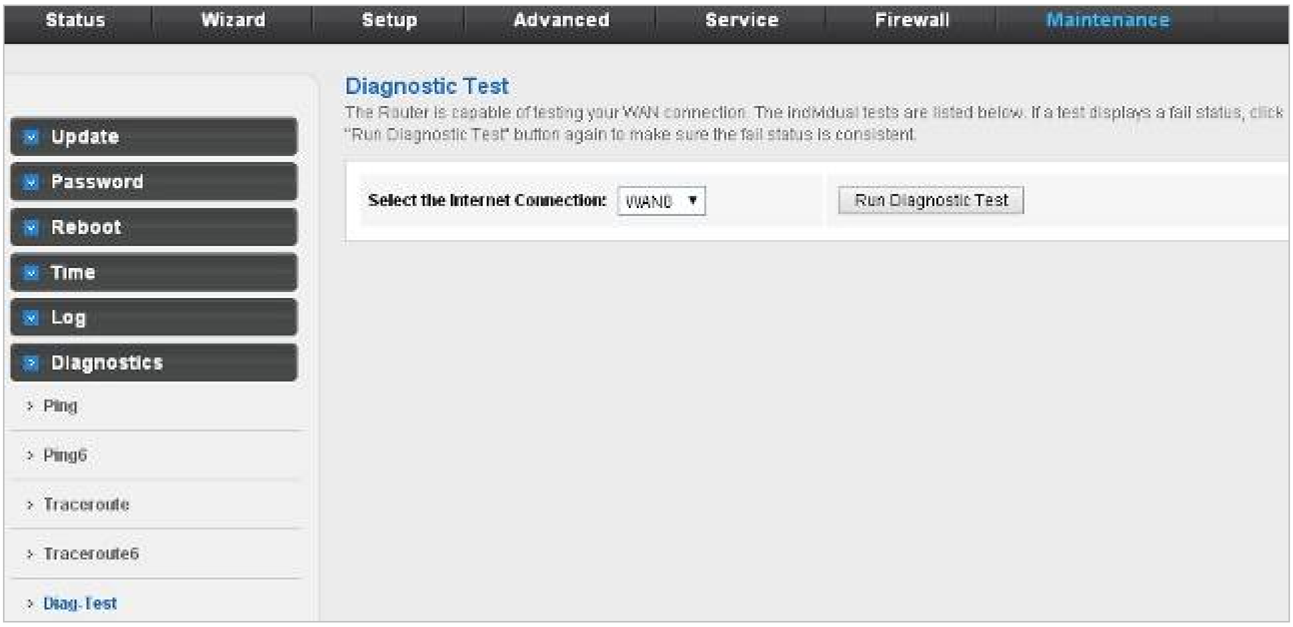
Figure 5-78 Traceroute6

The following table describes the parameters:

Field	Description
Host	Enter the destination host address for diagnosis.
NumberOfTries	Number of repetitions.
Timeout	Put in the timeout value.
Datasize	Packet size.
DSCP	Differentiated Services Code Point, You should set a value between 0-63.
MaxHopCount	Maximum number of routes.
Interface	Select the interface.

5.7.6.5 Diag-Test

Choose **Diagnostics** > **Diag-Test** and the page shown in the following figure appears. On this page, you can test the fiber router connection. You can also view the LAN status connection and fiber connection.



Diagnostic Test

The Router is capable of testing your WAN connection. The individual tests are listed below. If a test displays a fail status, click "Run Diagnostic Test" button again to make sure the fail status is consistent.

Select the Internet Connection: WAN0

Figure 5-79 Diag-Test

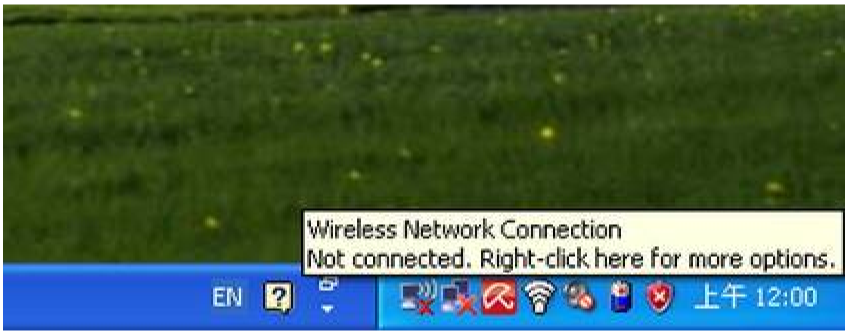
Click **Run Diagnostic Test** to start testing.

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the FRT-415N is configured to “**default**”.

6.1 Windows XP (Wireless Zero Configuration)

Step 1: Right-click on the **wireless network icon** displayed in the system tray



Wireless Network Connection
Not connected. Right-click here for more options.

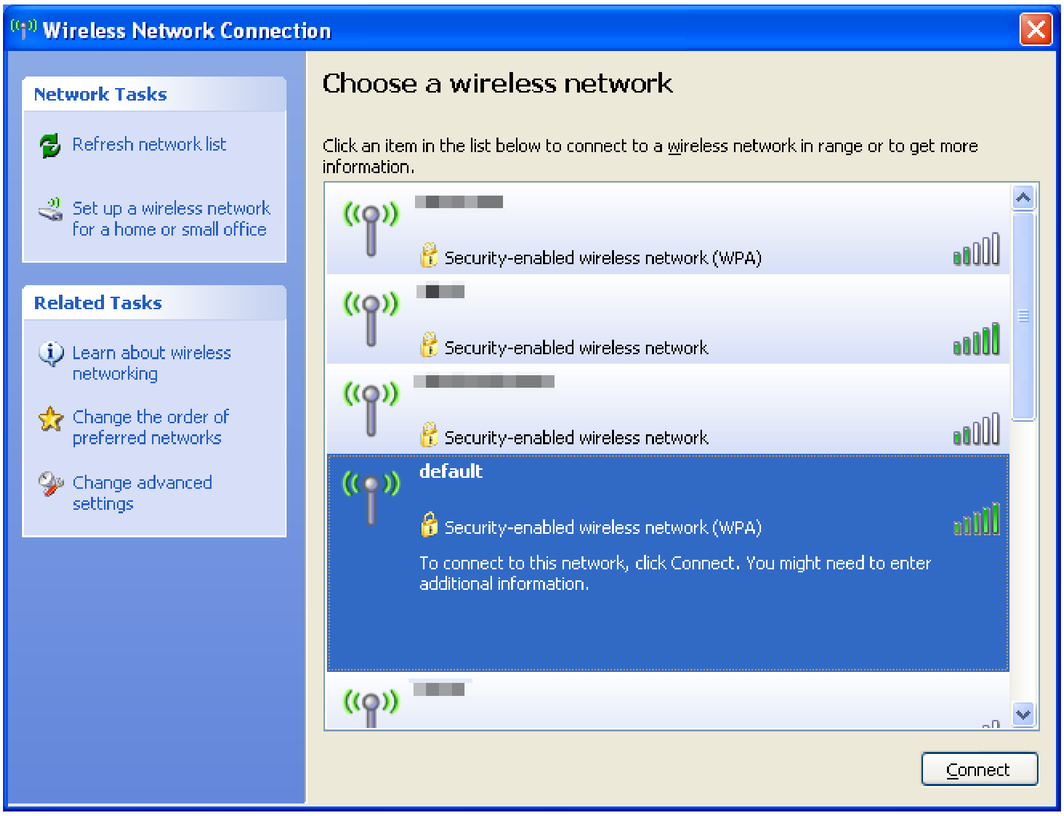
Figure 6-1 System Tray – Wireless Network Icon

Step 2: Select [**View Available Wireless Networks**]

Step 3: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [default]

(2) Click the [**Connect**] button



Wireless Network Connection

Network Tasks

- Refresh network list
- Set up a wireless network for a home or small office

Related Tasks

- Learn about wireless networking
- Change the order of preferred networks
- Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

[redacted]
Security-enabled wireless network (WPA)

[redacted]
Security-enabled wireless network

[redacted]
Security-enabled wireless network

default
Security-enabled wireless network (WPA)
To connect to this network, click Connect. You might need to enter additional information.

[redacted]

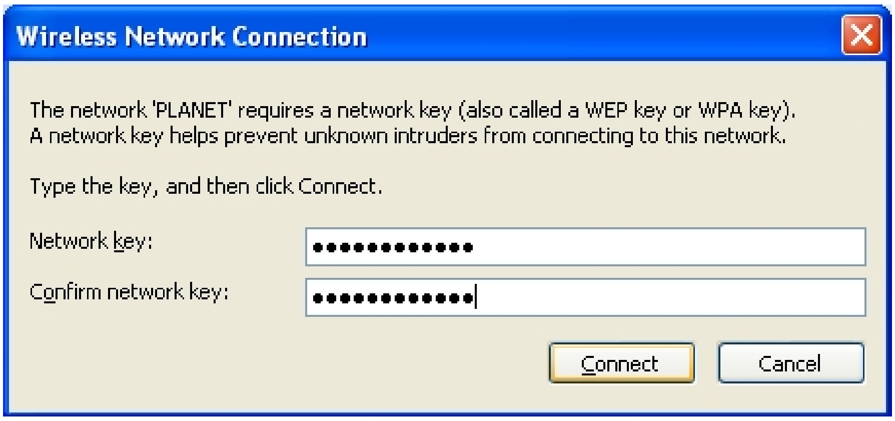
Figure 6-2 Choose a wireless network

Step 4: Enter the **encryption key** of the Wireless AP

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that is configured in section 5.3.3.2

(3) Click the [Connect] button



Wireless Network Connection

The network 'PLANET' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

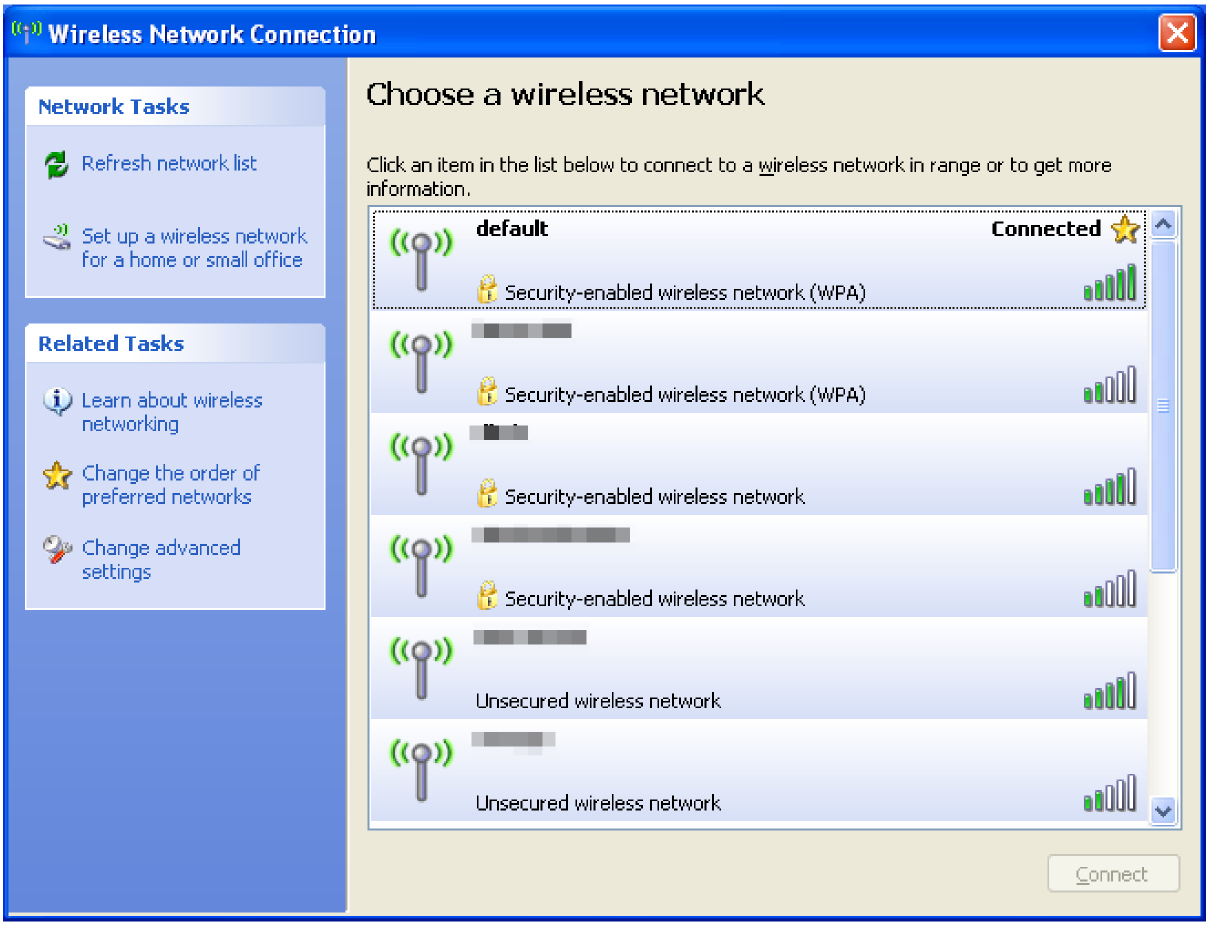
Type the key, and then click Connect.

Network key: ●●●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●●●

Figure 6-3 Enter the network key

Step 5: Check if "**Connected**" is displayed



Wireless Network Connection

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

default — Connected ☆ — Security-enabled wireless network (WPA)

[redacted] — Security-enabled wireless network (WPA)

[redacted] — Security-enabled wireless network

[redacted] — Security-enabled wireless network

[redacted] — Unsecured wireless network

[redacted] — Unsecured wireless network

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Figure 6-4 Choose a wireless network -- Connected

Note

Some laptops are equipped with a “Wireless ON/OFF” switch for the internal wireless LAN. Make sure the hardware wireless switch is switched to “ON” position.

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 to enable to detect and connect to wireless network. This built-in wireless network connection tool is similar to the wireless zero configuration tool in Windows XP.

Step 1: Right-click on the **network icon** displayed in the system tray

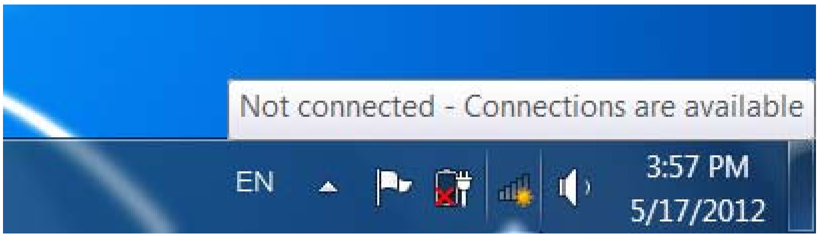
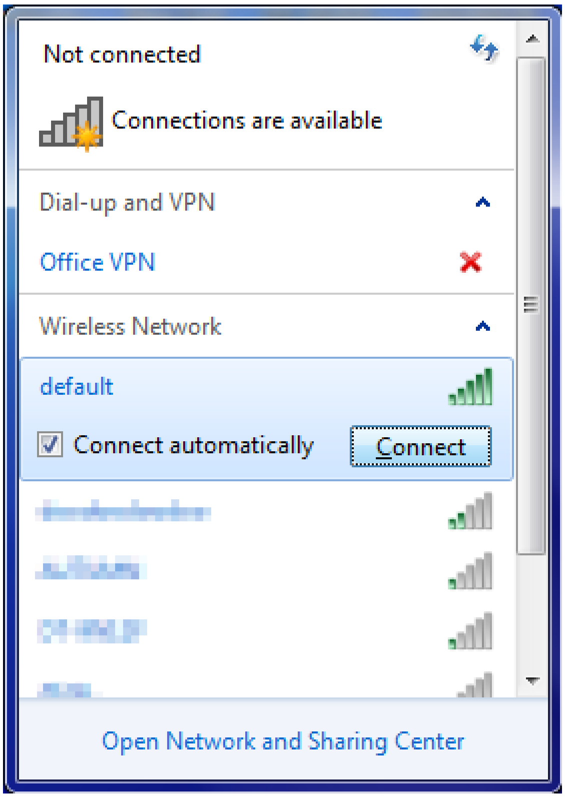

Not connected - Connections are available

Figure 6-5 Network icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [**default**]

(2) Click the [**Connect**] button


Not connected

Connections are available

Figure 6-6 WLAN AutoConfig

Note

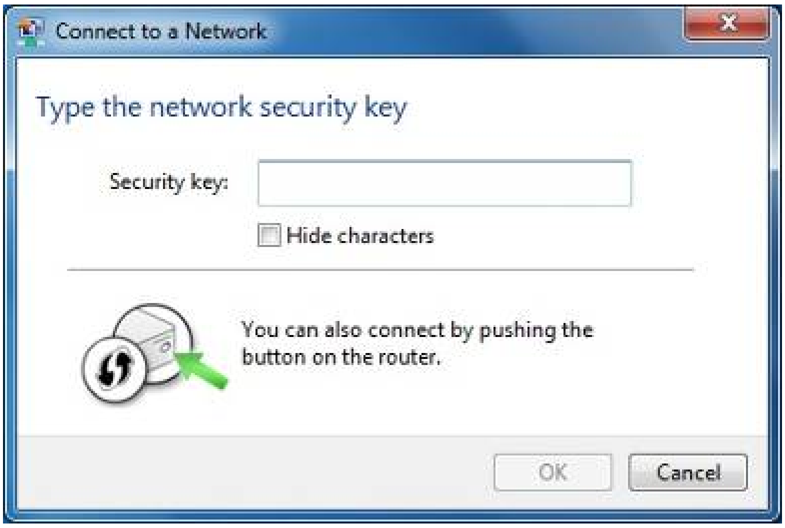
If you will be connecting to this Wireless AP in the future, check [**Connect automatically**].

Step 4: Enter the **encryption key** of the Wireless AP

(1) The Connect to a Network box will appear

(2) Enter the encryption key that is configured in section 5.3.3.2

(3) Click the [OK] button



Connect to a Network

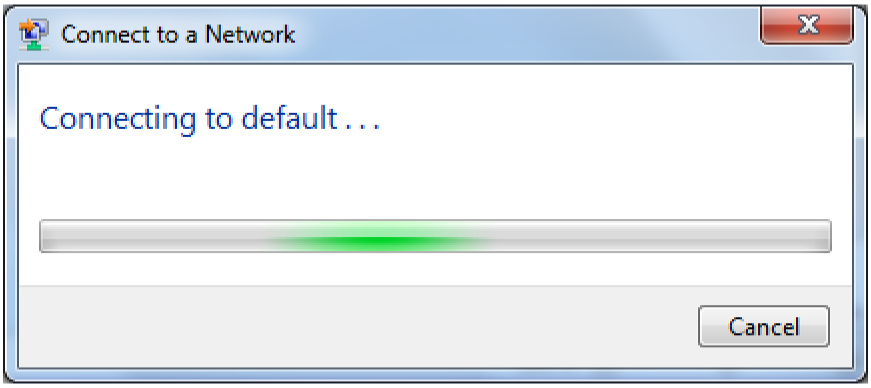
Type the network security key

Security key:

□ Hide characters

You can also connect by pushing the button on the router.

Figure 6-7 Type the network key

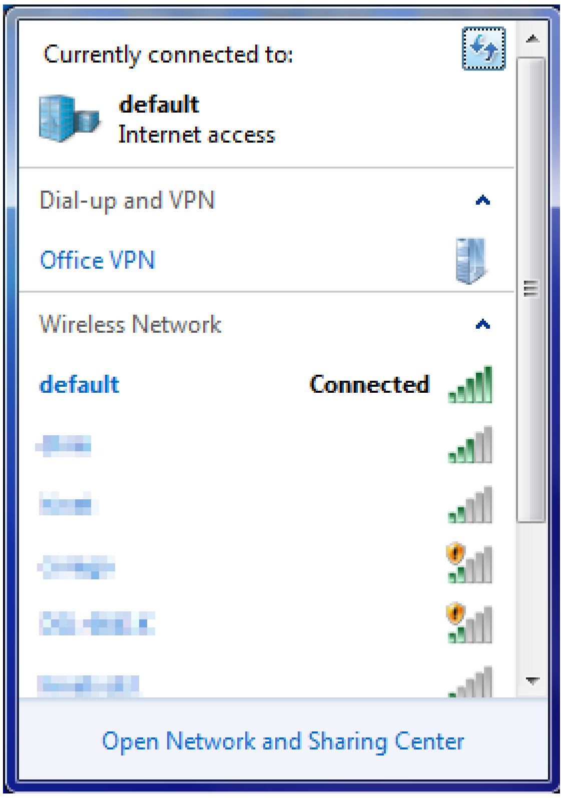


Connect to a Network

Connecting to default . . .

Figure 6-8 Connecting to a Network

Step 5: Check if "**Connected**" is displayed



Currently connected to:

default
Internet access

Dial-up and VPN

Office VPN

Wireless Network

default **Connected**

Open Network and Sharing Center

Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the FRT-415N is configured to “default”.

Step 1: Right-click on the **network icon** displayed in the system tray

The AirPort Network Connection menu will appear

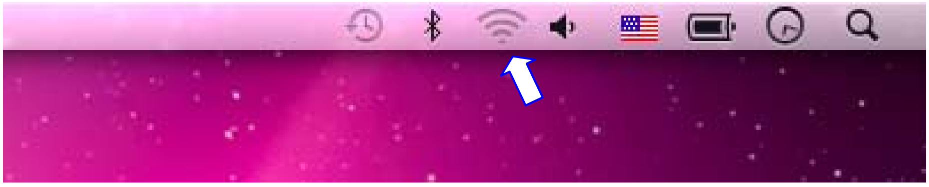


Figure 6-10 Mac OS – Network icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select and SSID [**default**]

(2) Double-click on the selected SSID

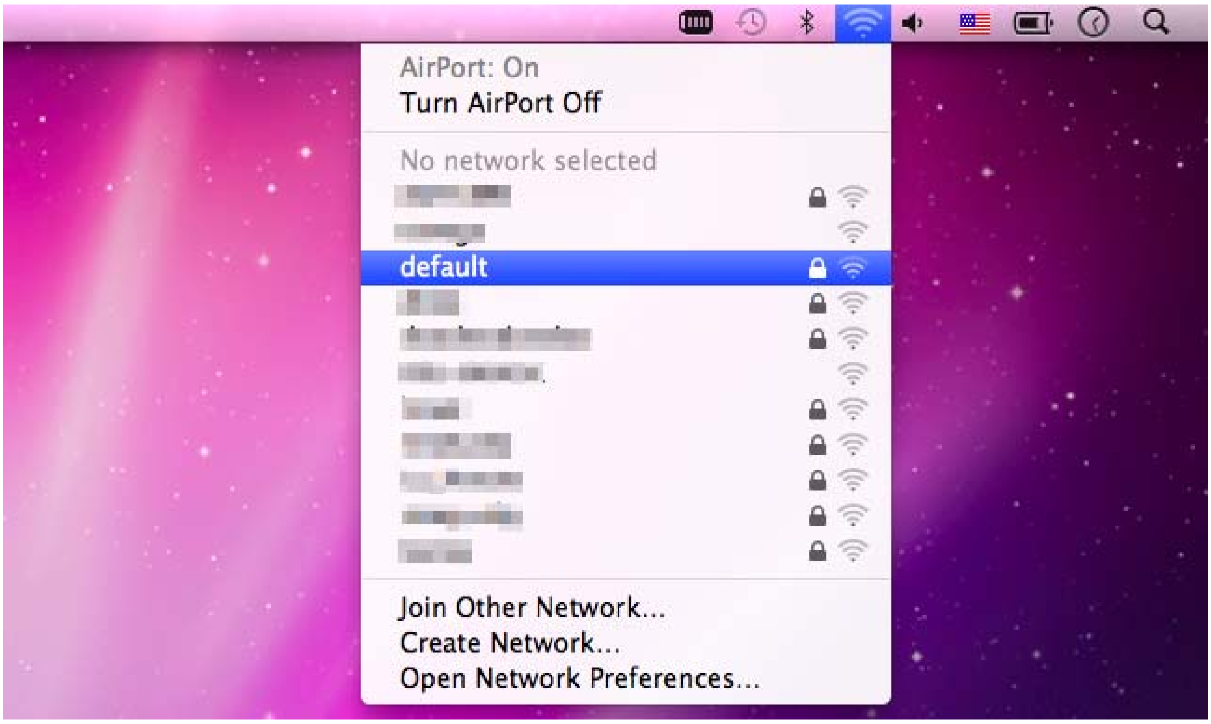
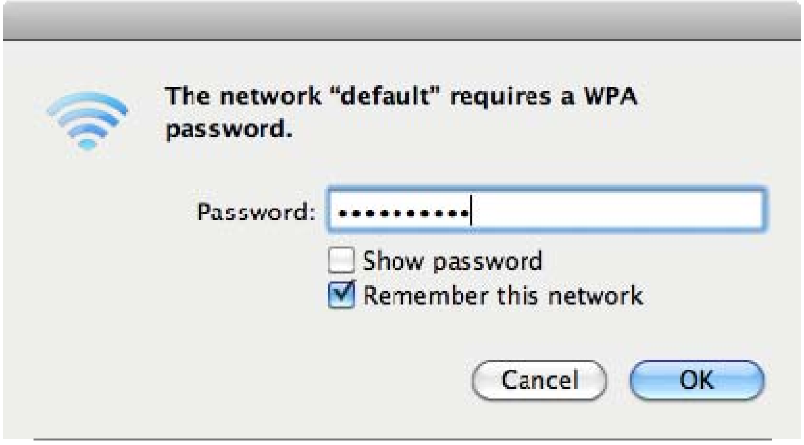


Figure 6-11 Highlight and select the wireless network

Step 4: Enter the **encryption key** of the Wireless AP

(1) Enter the encryption key that is configured in section 5.3.3.2

(2) Click the [OK] button



The network “default” requires a WPA password.

Password: ••••••••••

□ Show password

☑ Remember this network

Figure 6-12 Enter the Password

If you will be connecting to this Wireless AP in the future, check [**Remember this network**].

Step 5: Check if the AirPort is connected to the selected wireless network.

If “Yes”, then there will be a “check” symbol in the front of the SSID.

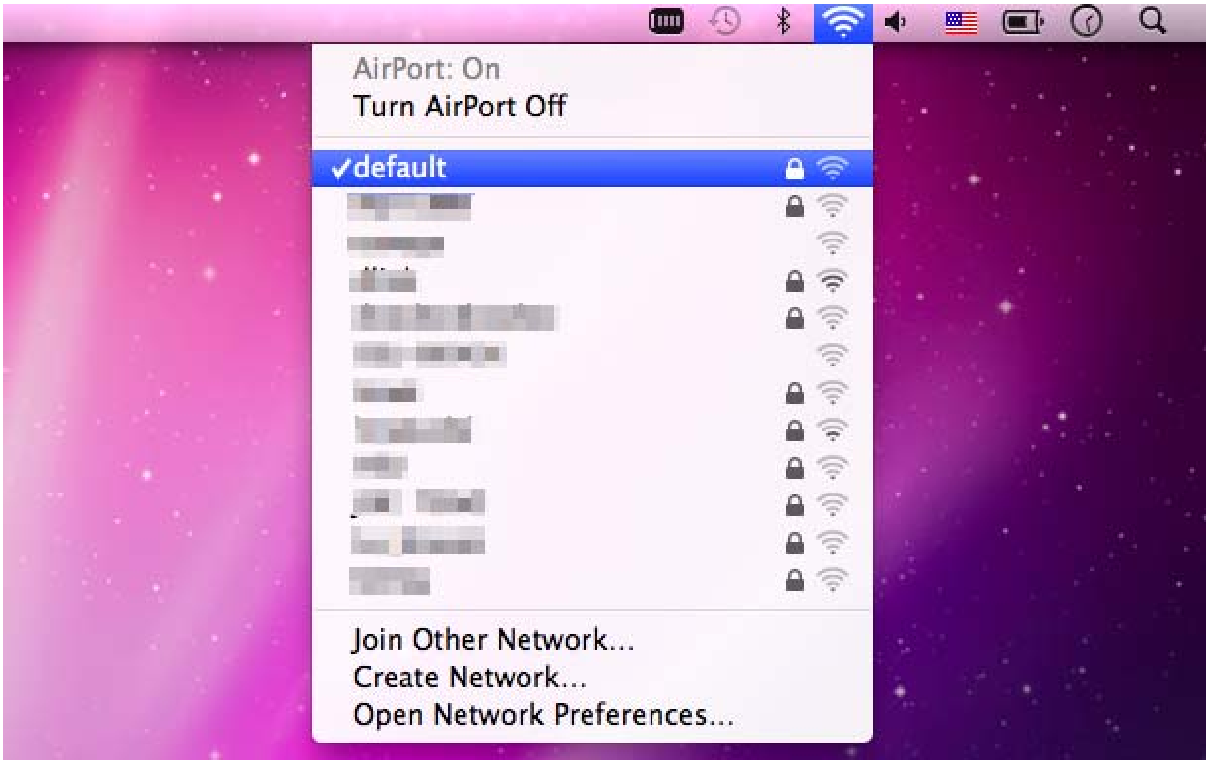


Figure 6-13 Connected to the Network

There is another way to configure the MAC OS X Wireless settings:

Step 1: Click and open the [**System Preferences**] by going to **Apple** > **System Preference** or **Applications**

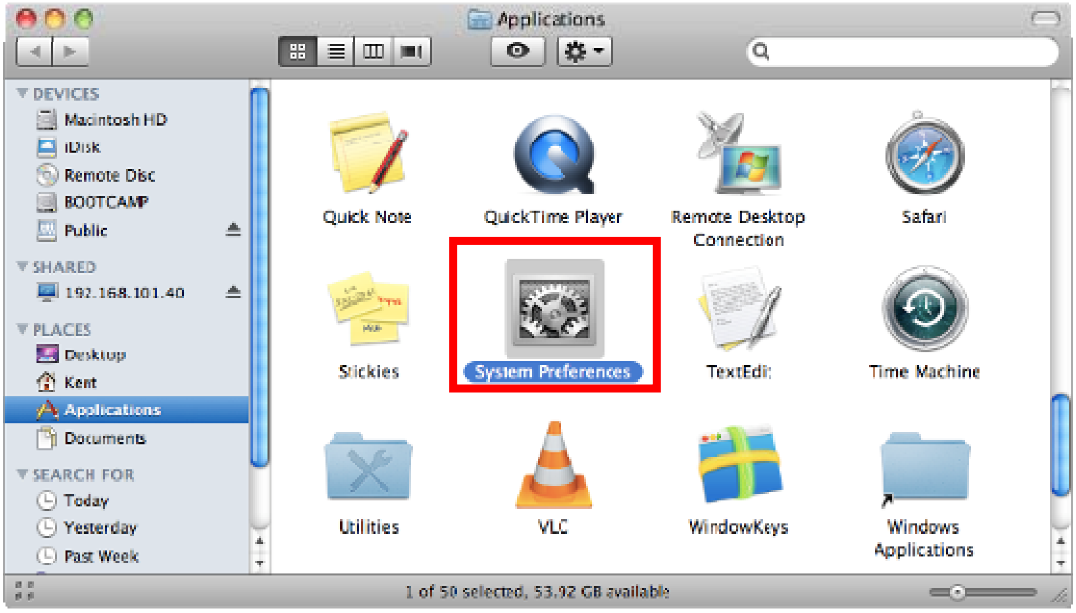


Figure 6-14 System Preferences

Step 2: Open **Network Preference** by clicking on the [**Network**] icon

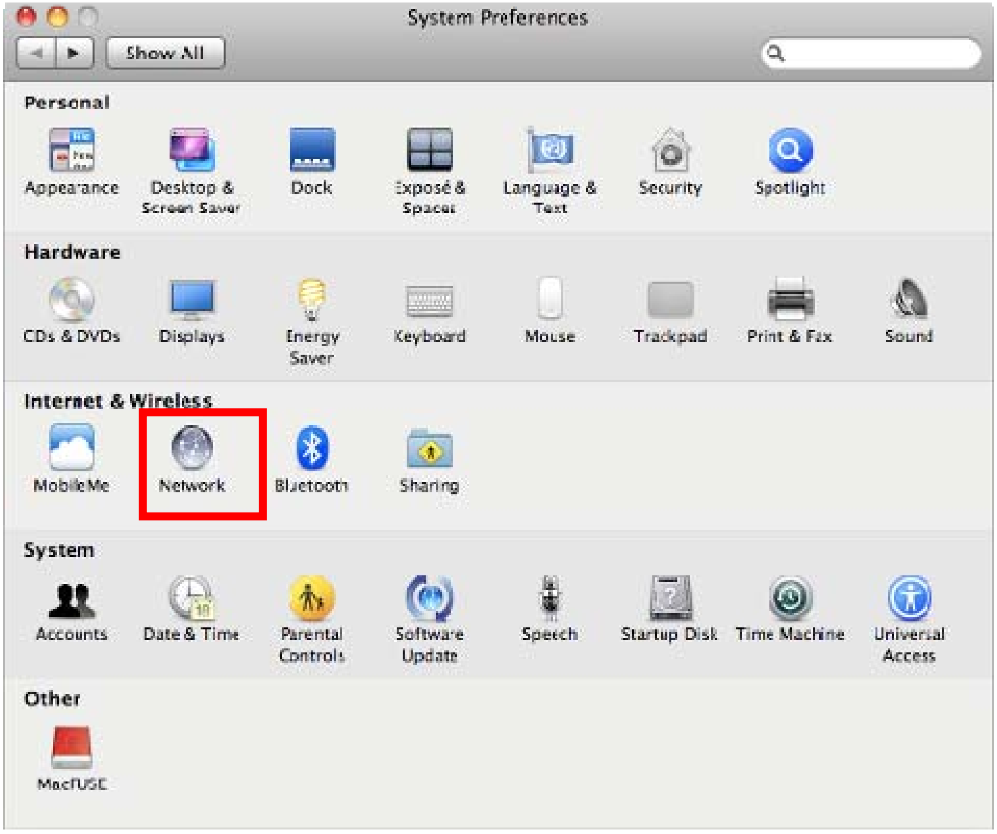


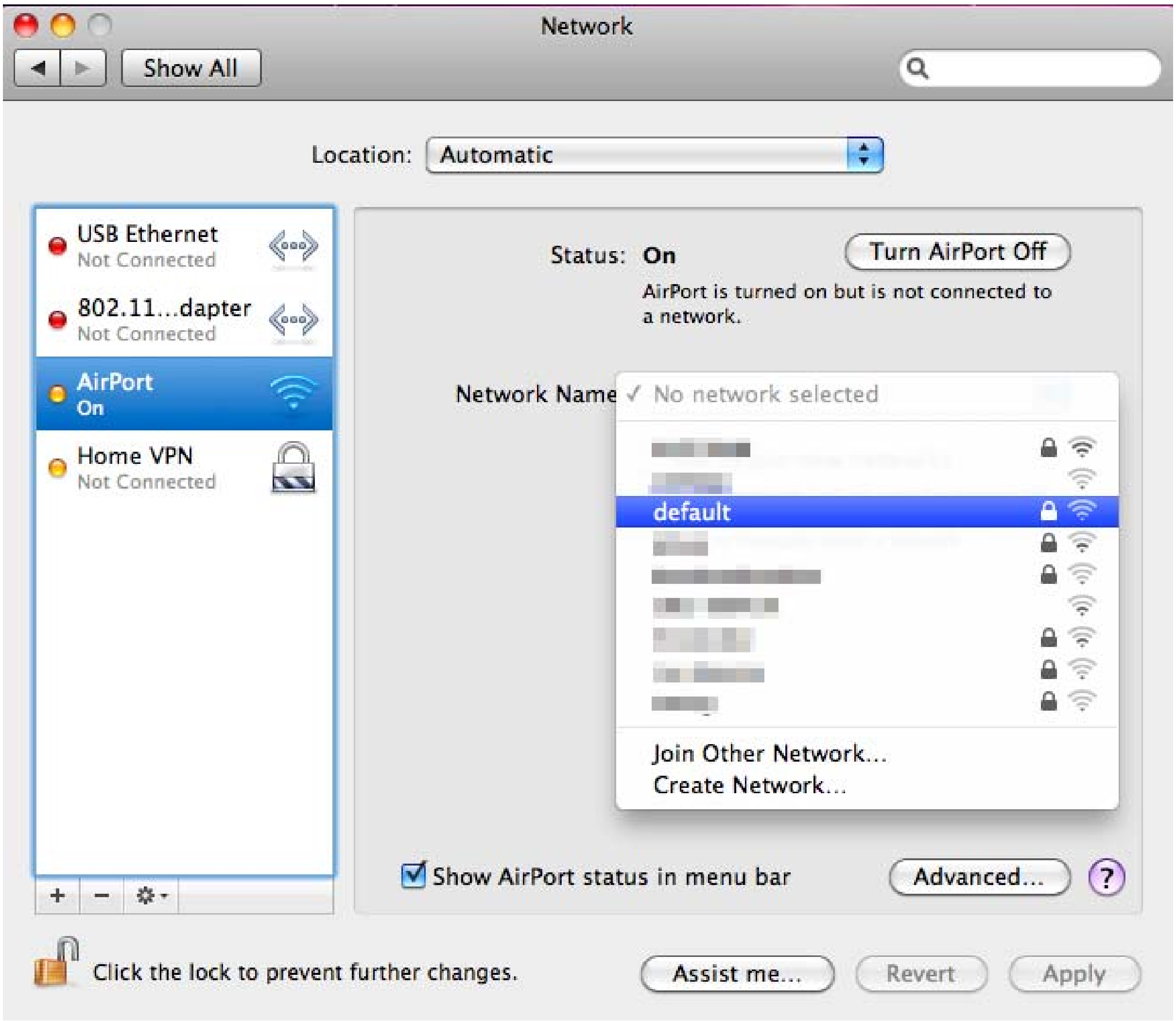
Figure 6-15 System Preferences -- Network

Step 3: Check Wi-Fi setting and select the available wireless network

(1) Choose the **AirPort** on the left-menu (make sure it is ON)

(2) Select Network Name [**default**] here

If this is the first time to connect to the Wireless AP, it should show "Not network selected".



Location: Automatic

Status: On

AirPort is turned on but is not connected to a network.

Network Name ✓ No network selected

☑ Show AirPort status in menu bar

Figure 6-16 Select the Wireless Network

6.4 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the FRT-415N is configured to “**default**”.

Step 1: Tap the [**Settings**] icon displayed in the home screen

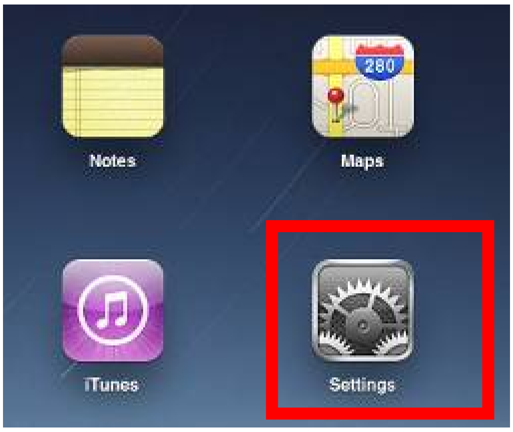


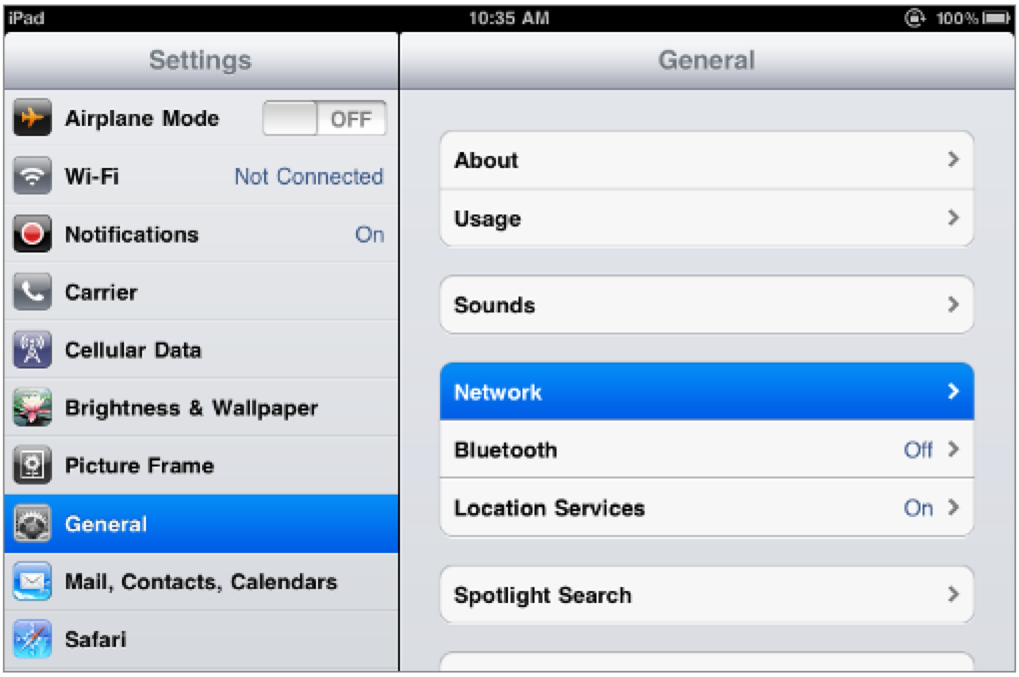
Figure 6-17 iPhone – Settings icon

Step 2: Check Wi-Fi setting and select the available wireless network

(3) Tap [**General**] \ [**Network**]

(4) Tap [**Wi-Fi**]

If this is the first time to connect to the Wireless AP, it should show “Not Connected”.


iPad 10:35 AM 100%

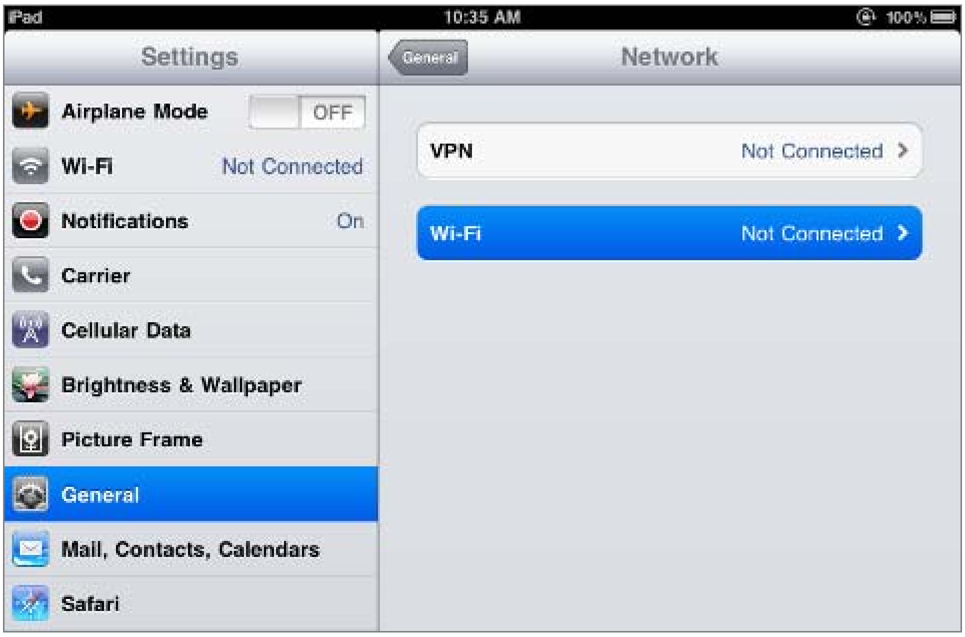
Settings

- Airplane Mode OFF
- Wi-Fi Not Connected
- Notifications On
- Carrier
- Cellular Data
- Brightness & Wallpaper
- Picture Frame
- General
- Mail, Contacts, Calendars
- Safari

General

- About
- Usage
- Sounds
- Network
- Bluetooth Off
- Location Services On
- Spotlight Search

Figure 6-18 Wi-Fi Setting


iPad 10:35 AM 100%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Carrier

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Mail, Contacts, Calendars

Safari

General Network

VPN Not Connected

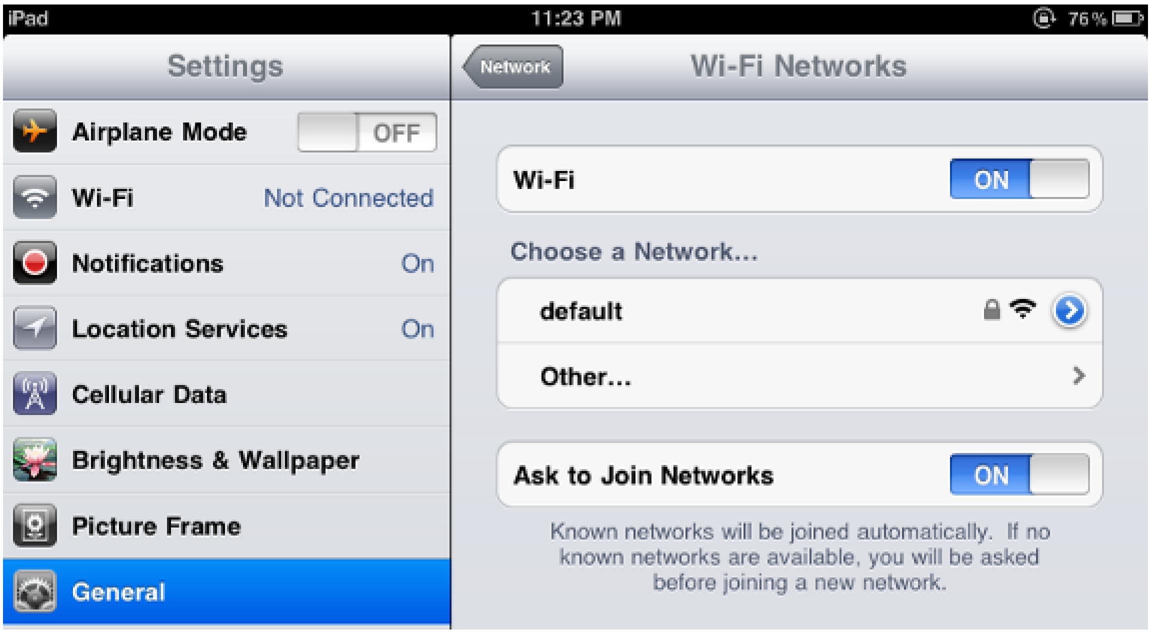
Wi-Fi Not Connected

Figure 6-19 Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

(2) Select SSID [**default**]


iPad 11:23 PM 76%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Location Services On

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Network Wi-Fi Networks

Wi-Fi ON

Choose a Network...

default

Other...

Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

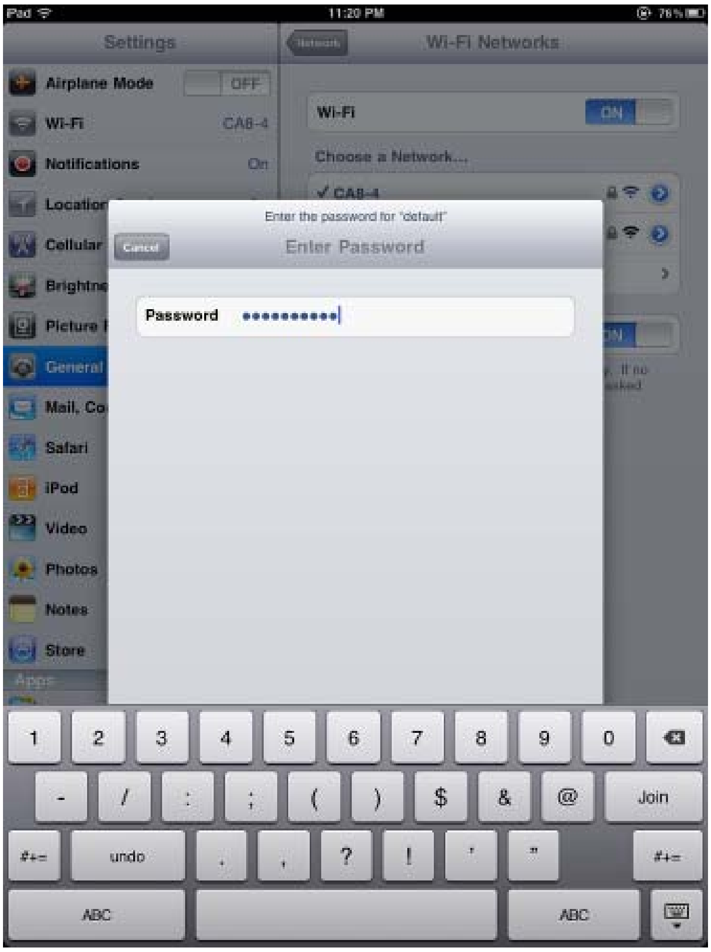
Figure 6-20 Turn on Wi-Fi

Step 4: Enter the **encryption key** of the Wireless AP

(1) The password input screen will be displayed

(2) Enter the encryption key that is configured in section 5.3.3.2

(3) Tap the [**Join**] button

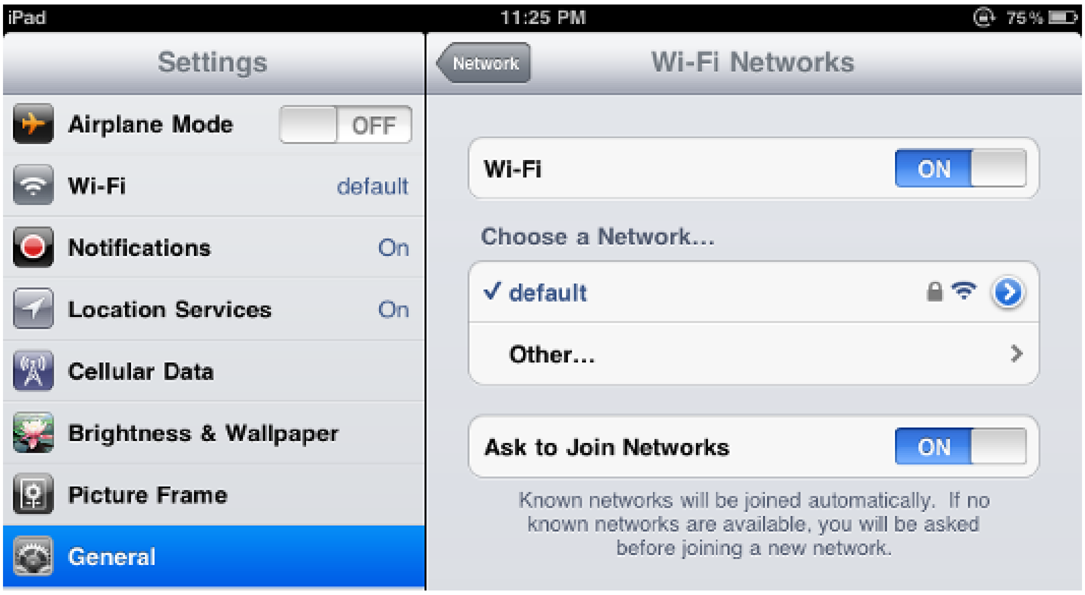


Airplane Mode OFF
Wi-Fi CA8-4
Notifications On
Wi-Fi ON
Password ●●●●●●●●●●●

Figure 6-21 iPhone -- Enter the Password

Step 5: Check if the device is connected to the selected wireless network.

If "Yes", then there will be a "check" symbol in the front of the SSID.



Airplane Mode OFF
Wi-Fi default
Notifications On
Location Services On
Wi-Fi ON
✓ default
Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Figure 6-22 iPhone -- Connected to the Network

Appendix A: Cable Profiles

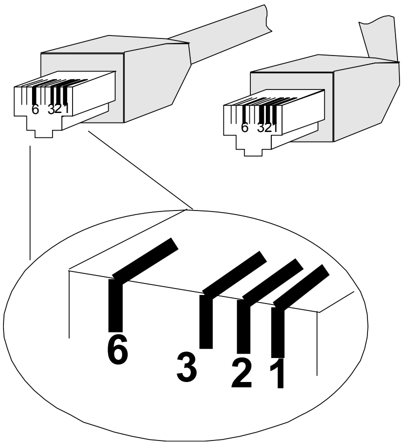
A.1 Device's RJ45 Pin Assignments

■ **10/100Mbps, 10/100BASE-TX**

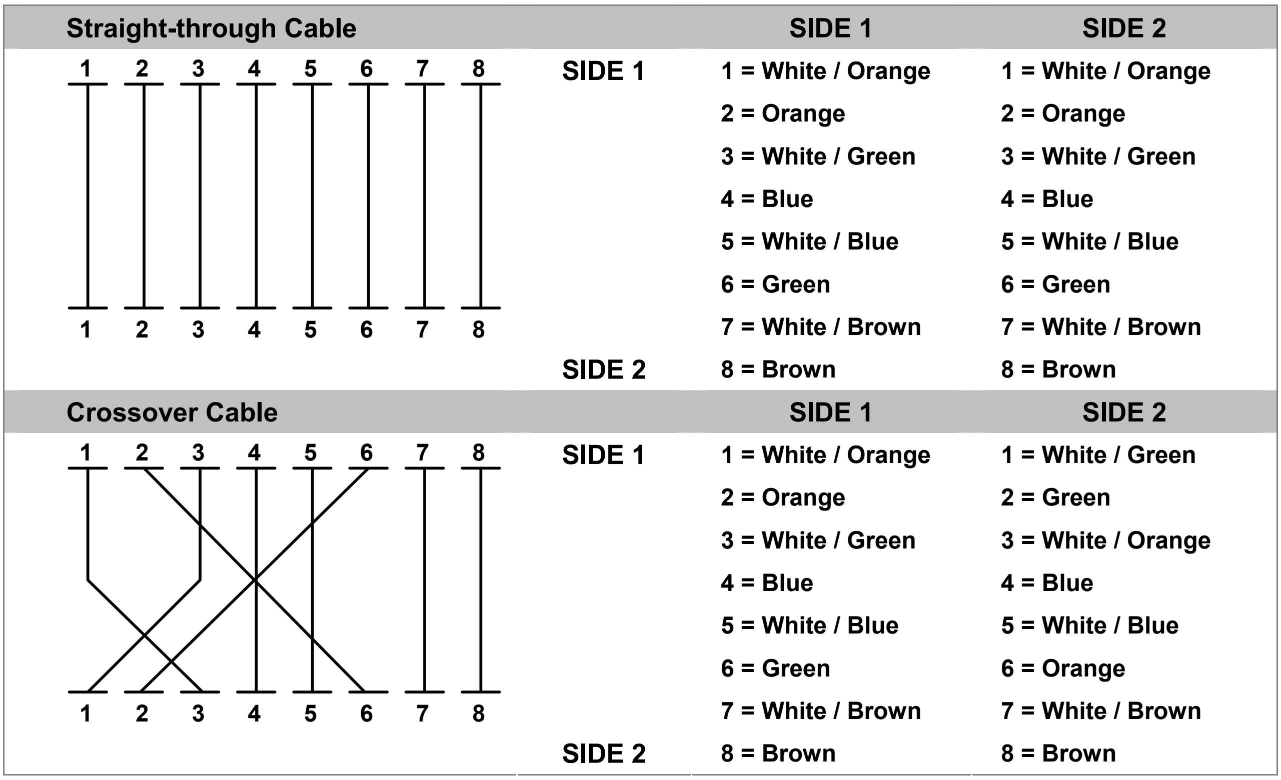
Contact	MDI	MDI-X
1	1 (TX +)	3
2	2 (TX -)	6
3	3 (RX +)	1
6	6 (RX -)	2
4, 5, 7, 8	Not used	Not used

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 RJ45 Cable Pin Assignment



There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight-through cable and crossover cable connection:



Straight-through Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange	1 = White / Orange
		2 = Orange	2 = Orange
		3 = White / Green	3 = White / Green
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Green
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown
Crossover Cable		**SIDE 1**	**SIDE 2**
	SIDE 1	1 = White / Orange	1 = White / Green
		2 = Orange	2 = Green
		3 = White / Green	3 = White / Orange
		4 = Blue	4 = Blue
		5 = White / Blue	5 = White / Blue
		6 = Green	6 = Orange
		7 = White / Brown	7 = White / Brown
	SIDE 2	8 = Brown	8 = Brown

Figure A-1: Straight-through and Crossover Cables

Please make sure your connected cables are with the same pin assignment and color as the above table before deploying the cables into your network.

A.3 Fiber Optic Cable Connection Parameter

The wiring details are shown below:

■ **Fiber Optic Patch Cables:**

Standard	Fiber Type	Cable Specification
100BASE-FX (1300nm)	Multi-mode	50/125μm or 62.5/125μm
100BASE-FX (1310nm)	Multi-mode	50/125μm or 62.5/125μm
	Single-mode	9/125μm
100BASE-BX-U (TX :1310/RX :1550) **100BASE-BX-D** (TX :1550/RX :1310)	Single-mode	9/125μm

A.4 Available Modules

The following list the available Modules for FRT-415N

MFB-FX	SFP-Port 100BASE-FX Transceiver (1310nm) - 2km
MFB-F20	SFP-Port 100BASE-FX Transceiver (1310nm) - 20km
MFB-F40	SFP-Port 100BASE-FX Transceiver (1310nm) - 40km
MFB-F60	SFP-Port 100BASE-FX Transceiver (1310nm) - 60km
MFB-FA20	SFP-Port 100BASE-BX Transceiver (WDM,TX:1310nm) - 20km
MFB-FB20	SFP-Port 100BASE-BX Transceiver (WDM,TX:1550nm) - 20km
MFB-TFX	SFP-Port 100BASE-FX Transceiver (1310nm) - 2km (-40 ~ 75 degrees C)

EC Declaration of Conformity

For the following equipment:

*Type of Product: 802.11n Wireless Internet Fiber Router
*Model Number: FRT-415N

* Produced by:
Manufacturer‘s Name : **Planet Technology Corp.**
Manufacturer‘s Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.)

is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE, Low Voltage Directive 2006/95/EC.
For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.8.1	(2012)
EN 301 489-17 V2.2.1	(2012)
EN 301 498-1 V1.9.2	(2011)
EN 62311	(2008)
EN 60950-1(2006 + A11: 2009 + A1:2010 + A12:2011 + A2:2013)	

Responsible for marking this declaration if the:

☒ **Manufacturer** □ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Director**

Taiwan	**20 Nov., 2015**	Kent Kang
Place	*Date*	*Legal Signature*

EC Declaration of Conformity

English	Hereby, **PLANET Technology Corporation**, declares that this **802.11n Wireless Internet Fiber Router** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.	**Lietuviškai**	Šiuo **PLANET Technology Corporation**,, skelbia, kad **802.11n Wireless Internet Fiber Router** tenkina visus svarbiausius 1999/5/EC direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost **PLANET Technology Corporation**, tímto prohlašuje, že tato **802.11n Wireless Internet Fiber Router** splňuje základní požadavky a další příslušná ustanovení směrnice 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation** n, kijelenti, hogy ez a **802.11n Wireless Internet Fiber Router** r megfelel az 1999/5/EK irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	**PLANET Technology Corporation**, erklærer herved, at følgende udstyr **802.11n Wireless Internet Fiber Router** overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF	**Malti**	Hawnhekk, **PLANET Technology Corporation**, jiddikjara li dan **802.11n Wireless Internet Fiber Router** jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Deutsch	Hiermit erklärt **PLANET Technology Corporation**, dass sich dieses Gerät **802.11n Wireless Internet Fiber Router** in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi)	**Nederlands**	Hierbij verklaart , **PLANET Technology Corporation**, dat **802.11n Wireless Internet Fiber Router** in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eesti keeles	Käesolevaga kinnitab **PLANET Technology Corporation**, et see **802.11n Wireless Internet Fiber Router** vastab Euroopa Nõukogu direktiivi 1999/5/EC põhinõuetele ja muudele olulistele tingimustele.	**Polski**	Niniejszym firma **PLANET Technology Corporation**, oświadcza, że **802.11n Wireless Internet Fiber Router** spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 1999/5/EC".
Ελληνικά	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ , **PLANET Technology Corporation**, ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ **802.11n Wireless Internet Fiber Router** ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ	**Português**	**PLANET Technology Corporation**, declara que este **802.11n Wireless Internet Fiber Router** está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Español	Por medio de la presente, **PLANET Technology Corporation**, declara que **802.11n Wireless Internet Fiber Router** cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE	**Slovensky**	Výrobca **PLANET Technology Corporation**, týmto deklaruje, že táto **802.11n Wireless Internet Fiber Router** je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
Français	Par la présente, **PLANET Technology Corporation**, déclare que les appareils du **802.11n Wireless Internet Fiber Router** sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE	**Slovensko**	**PLANET Technology Corporation**, s tem potrjuje, da je ta **802.11n Wireless Internet Fiber Router** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
Italiano	Con la presente , **PLANET Technology Corporation**, dichiara che questo **802.11n Wireless Internet Fiber Router** è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.	**Suomi**	**PLANET Technology Corporation**, vakuuttaa täten että **802.11n Wireless Internet Fiber Router** tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo **PLANET Technology Corporation**, apliecina, ka šī **802.11n Wireless Internet Fiber Router** atbilst Direktīvas 1999/5/EK pamatprasībām un citiem atbilstošiem noteikumiem.	**Svenska**	Härmed intygar, **PLANET Technology Corporation**, att denna **802.11n Wireless Internet Fiber Router** står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.