PLANET
Networking & Communication

User's Manual

300Mbps 802.11n Wireless Internet Fiber Router

► FRT-405N

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.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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, (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/remark
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 for 802.11n Wireless Internet Fiber Router
Model: FRT-405N
Rev: 2.0 (August, 2013)
Part No. EM-FRT-405N_v2 (**2080-B53060-000**)

Table of Contents

Chapter 1.Product Introduction

1.1 Package Contents

Thank you for choosing PLANET FRT-405N. Before installing the router, please verify the contents inside the package box.

FRT-405N Unit

Quick Installation Guide

CD-ROM

(User Manual included)

Power Adapter

12V/1A DC output

100~240V AC input

5dBi Antenna **x 2**

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

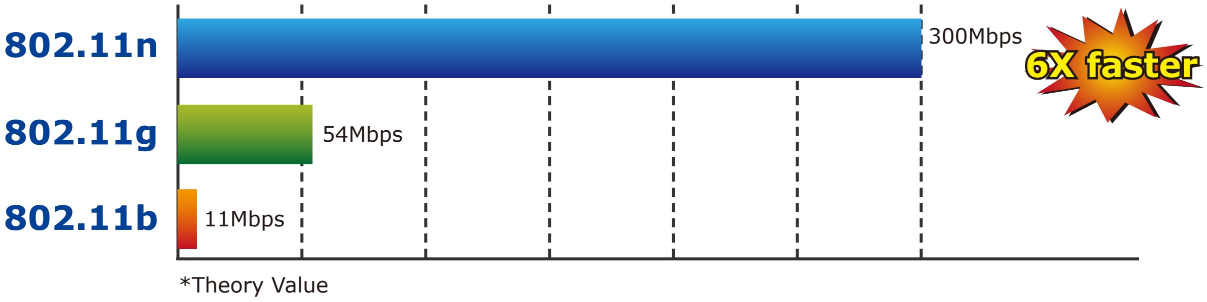
1.2 Product Description

Delivering High-Demand Service Connectivity for ISP / Triple Play Devices

With built-in 100Base-FX fiber interface, the FRT-405N supports different optic types for WAN and the distance can be up to 15~60 km through the Fiber connection. The FRT-405N is the ideal solution for FTTH (Fiber-to-the-home) applications. It can handle multiple high-throughput services such as **IPTV**, **on-line gaming**, **VoIP**, **Internet** access and keep the bandwidth usage smoothly. The FRT-405N also incorporates a 4-port 10/100Base-TX switching hub, which makes it easily creates or extends your LAN and prevents the attacks from Internet.

High-Speed 802.11n Wireless

With built-in IEEE 802.11b/g and 802.11n wireless network capability, the FRT-405N 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-405N supports most up-to-date encryptions including WEP, WPA-PSK and WPA2-PSK. Moreover, the FRT-405N supports WPS configuration with PBC/PIN type for users to easily connect to a secured wireless network.

Providing Superior Function

The FRT-405N provides user-friendly management interface to be managed easily through standard web browsers. For networking management features, the FRT-405N 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-405N 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-405N 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-405N provides long distance connection base on optical fiber transceiver which supports **FTTH** and **IPTV** applications.
  - **Multiple WAN Connection:** Upon the Internet (WAN port) connection, the FRT-405N supports Dynamic IP address (IP address is allocated upon connection), fixed IP address, PPPoE, PPTP and L2TP.
  - **Bridge and Router Application:** The FRT-405N supports two application modes: bridging and routing modes. Currently, the default mode is routing mode. Note: routing mode and bridging mode cannot be used simultaneously.

- **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-405N 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 ME, XP, or later.
  - **User Friendly Interface:** The FRT-405N can be managed and controlled through Web UI.
  - **DMZ Support:** The FRT-405N 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.
  - **VPN Pass-through Support:** PCs with VPN (Virtual Private Networking) software are transparently supported - no configuration is required.

- **LAN Features**

  - **4-Port Switch:** The FRT-405N 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-405N can act as a DHCP Server for devices on your local LAN.

- **Wireless Features**

  - **Supports IEEE 802.11b, g and 802.11n 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 up to 300Mbps data rate.
  - **Two External Antennas with MIMO Technology:** The FRT-405N provides farther coverage, less dead spaces and higher throughput with 2T2R MIMO technology.

- **WPS Push Button Control:** The FRT-405N 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-405N
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 detachable antenna
Optic Interface	**Connector**	SFP (Small form-factor Pluggable)
	Mode	Vary on module
	Distance	Vary on module
LED Indicators		PWR, WAN, LAN1-4, WLAN, WPS, Security
Button		1 x RESET button 1 x WPS button
Material		Plastic
Dimensions (W x D x H)		186 x 143 x 35 mm
Power		12V DC, 1A
Router Features		
Internet Connection Type		Shares data and Internet access for users, supporting the following internet accesses: ■ PPPoE ■ Dynamic IP ■ Static IP ■ PPTP ■ L2TP
Max. Session		15000
Fiber-optic cable		■ 50/125µm or 62.5/125µm multi-mode fiber cable, up to 2km. ■ 9/125µm single-mode cable, provide long distance for 15/20/35/50km or longer (very on SFP module)
Protocol / Feature		Router, Bridge and WISP mode WDS and WPS DMZ and Virtual Server 802.1D QoS DHCP Server / Client IGMP Proxy and DNS Proxy UPnP and DDNS
Routing Protocol		Static Routing RIPv1/2
VPN		VPN Pass-through
Security		Built-in NAT Firewall MAC / IP/ Port Filtering Content Filtering SPI Firewall support

System Management	Web-based (HTTP) configuration SNTP time synchronize System Log supports Remote Log Password protection for system management
Wireless Interface Specifications	
Wireless Standard	IEEE 802.11b, g and 802.11n
Frequency Band	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Modulation Type	DBPSK, DQPSK, QPSK, 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 14 Channels, depending on regulatory authorities
Antenna Connector	2 x 5dBi detachable Antenna
Wireless Data Encryption	64/128-bit WEP, WPA-PSK, WPA2-PSK, 802.1x encryption, and WPS PBC
Standards Conformance	
Standard	Fiber Interface Complaint with IEEE802.3 / 802.3u 10/100 Base-TX, 100Base-FX standard U0 Band Support (25KHz to 276KHz) Packet Transfer Mode Ethernet in the First Mile(PTM-EFM)
Environment Specifications	
Temperature / Humidity	Operating: 0~50 degrees C, 5%~ 90% (non-condensing), Storage: -20~70 degrees C, 0~95% (non-condensing)
Certification	FCC, CE

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-405N

The front panel provides a simple interface monitoring of the router. Figure 2-1 shows the front panel of the FRT-405N.

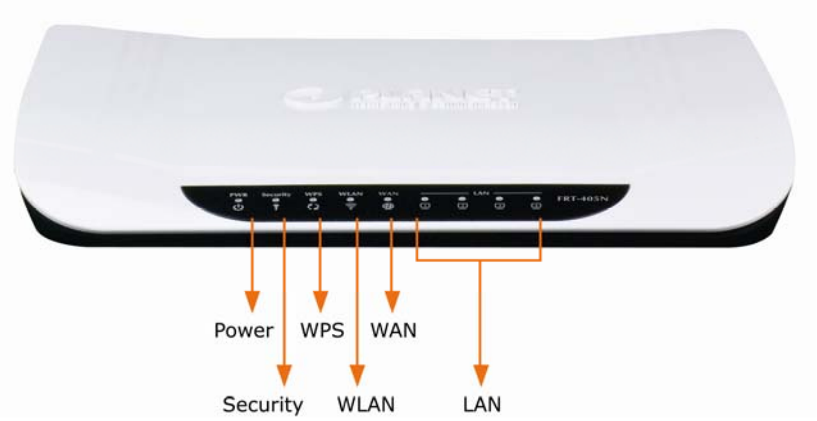


Figure 2-1 FRT-405N Front Panel

2.1.2 LED Indications of FRT-405N

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-405N.

Front Panel LED Definition

LED	State	Description
PWR	ON	When the router is powered on, and in ready state.
	OFF	When the router is powered off.
WPS	ON	WPS client registration is successful.
	Flashing	WPS client registration window is currently open.
	OFF	WPS is not available, or WPS is not enabled or initialized.
WLAN	ON	WLAN radio is on.
	Flashing	Data is being transmitted through WLAN.
	OFF	WLAN radio is off.
Security	ON	Enable WLAN encryption
	OFF	Disable WLAN encryption
WAN	Flashing	Router is trying to establish a WAN connection to device.
	ON	The WAN is connected successfully.
LAN1-4	Flashing	Data is being transmitted or received via the corresponding LAN port.
	ON	The port is up.

Table 2-1 The LED indication of FRT-405N

2.1.3 Rear Panel of FRT-405N

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-405N.

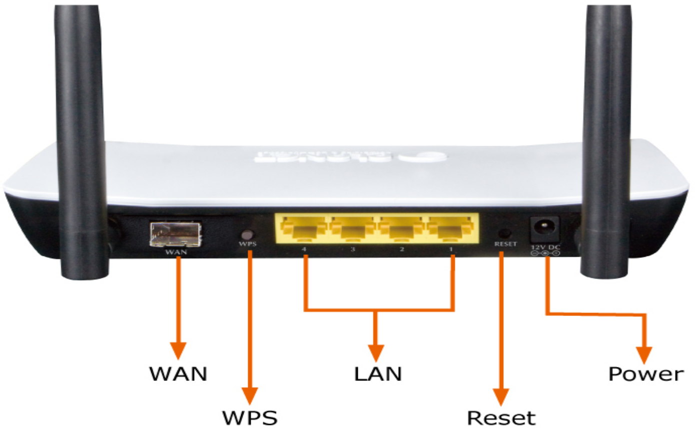


Figure 2-2 FRT-405N Rear Panel

Rear Panel Port and Button Definition

Connector	Description
POWER	Power connector with 12V DC 1 A
RESET	Press more than 3 seconds for reset to factory default setting.
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.
WPS	WPS on or off switch.
WAN	The SFP connector allows data communication between the router and the fiber network through a fiber wire

2.2 Cabling

- **100Base-TX and 100Base-FX**

  The 10/100Mbps RJ-45 ports come with Auto-Negotiation capability. Users only need to plug in working network device into one of the 10/100Mbps RJ-45 ports. The FRT-405N will automatically run in 10Mbps or 100Mbps after the negotiation with the connected device. The FRT-405N has one 100Base-FX SFP interface (Optional Multi-mode / Single-mode 100Base-FX SFP module)

- **Cabling**

  Each 10/100Base-TX ports use RJ-45 sockets - for connection of unshielded twisted-pair cable (UTP).

Port Type	Cable Type	Connector
10Base-T	Cat 3, 4, 5, 2-pair	RJ-45
100Base-TX	Cat.5, 5e, 6 UTP, 2-pair	RJ-45

Any Ethernet devices like Hubs / PCs can connect to the Fiber router by using straight-through wires. The 10/100Mbps RJ-45 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 a 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 the Figure 2-12 appears.

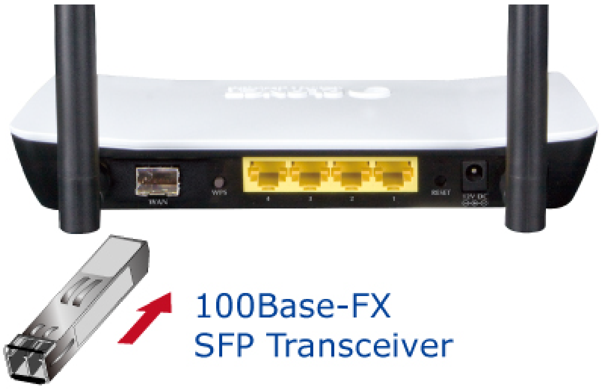


Figure 2-3 Plug in the SFP transceiver

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, 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 RJ-45 connectors
- PC of subscribers running Windows 98/ME, NT4.0, 2000/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-405N
2. It is recommended to use Internet Explore 7.0 or above to access the Router.

3.2 Installing the Router

Please connect the device to your computer as follows:

- Locate the FRT-405N in an optimum place and adjust the antenna for the best coverage. Figure 3-1 shows the antenna connection diagram.

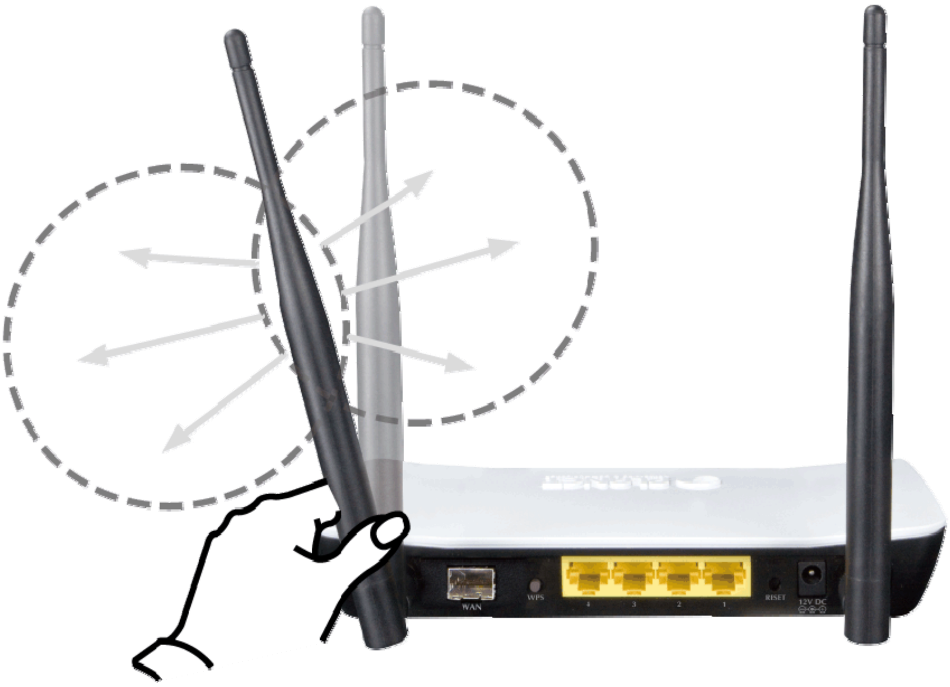


Figure 3-1: FRT-405N Antenna Adjustment Diagram

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

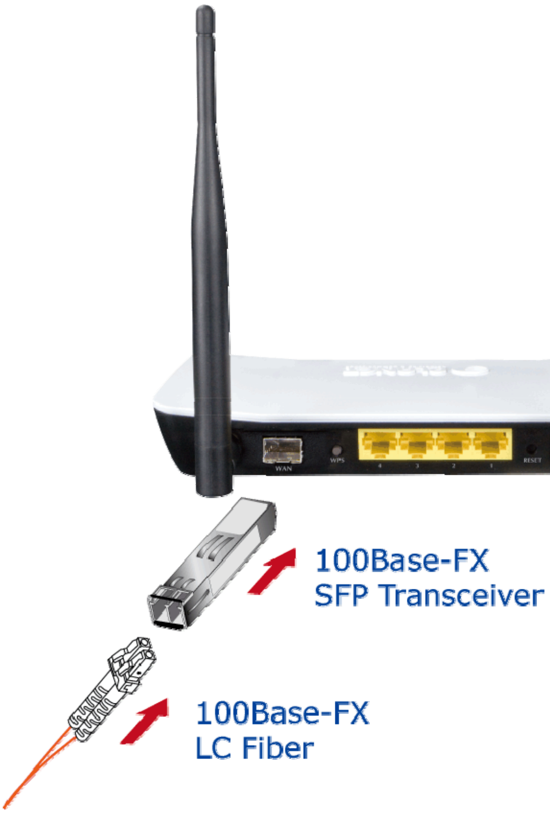


Figure 3-2: FRT-405N WAN port Connection Diagram

- Use Ethernet cable to connect "LAN" port of the modem and "LAN" port of your computer.
- Connect Power Adapter to the FRT-405N. Figure3-3 shows the power adapter connection diagram.

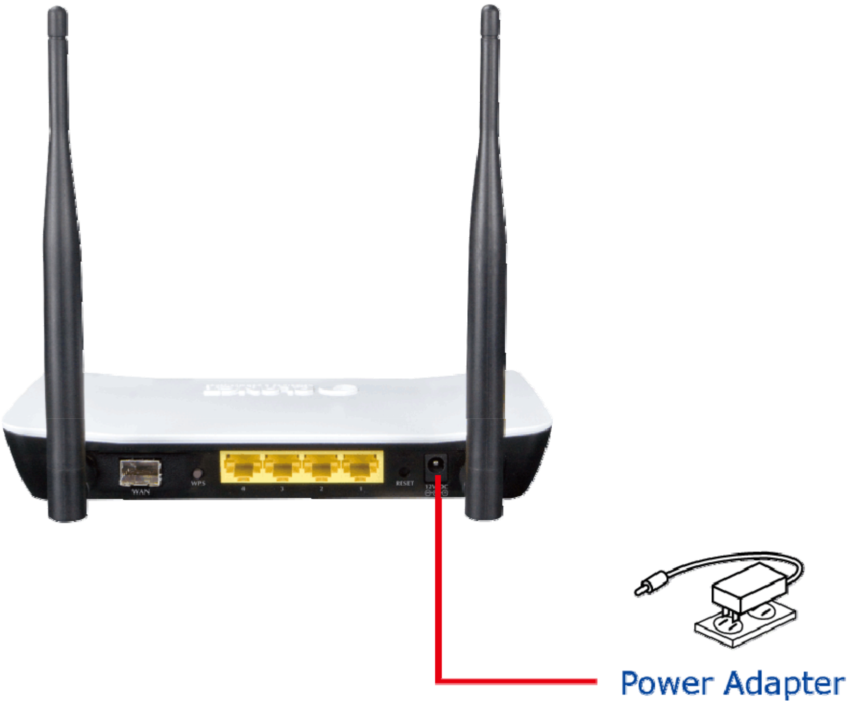


Figure 3-3: FRT-405N Power Adapter Connection Diagram

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

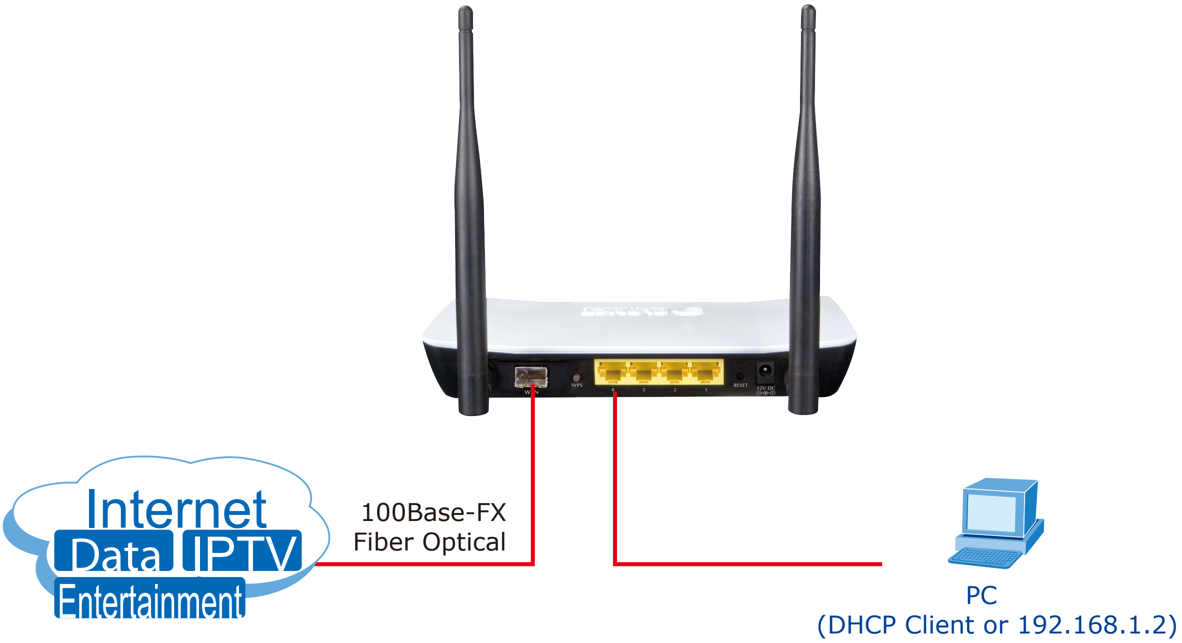


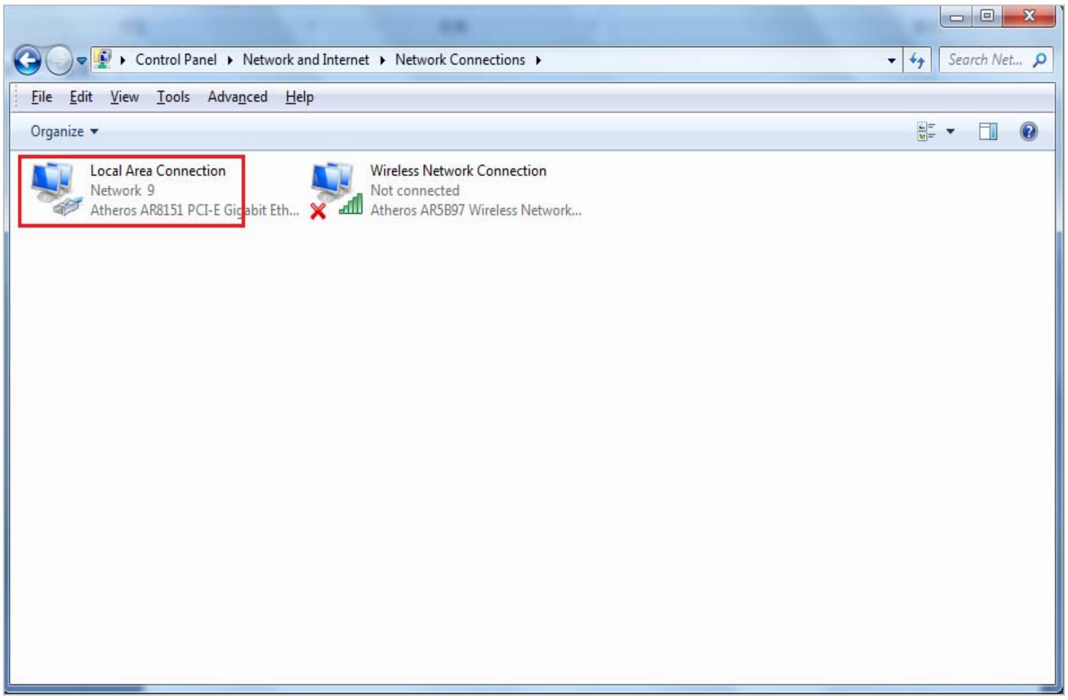
Figure 3-4: FRT-405N Connection Diagram

Chapter 4. Installation Guide

4.1 Configuring the Network Properties

Configuring PC in Windows 7

1. Go to **Start / Control Panel / Network and Internet / 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 4-1-1 Select Local Area Connection

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

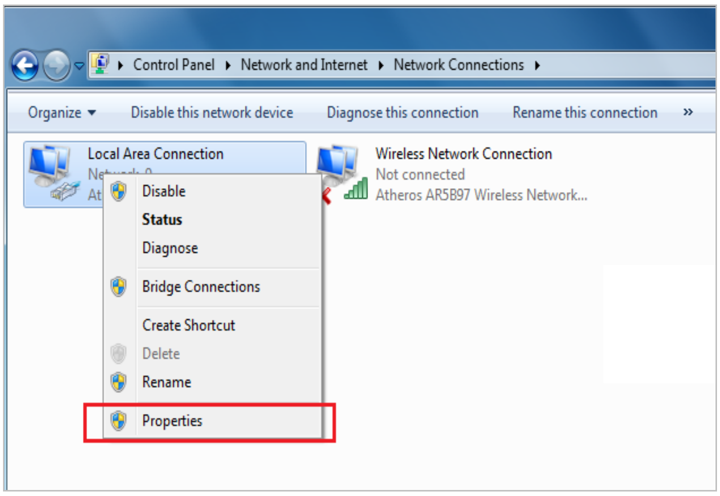
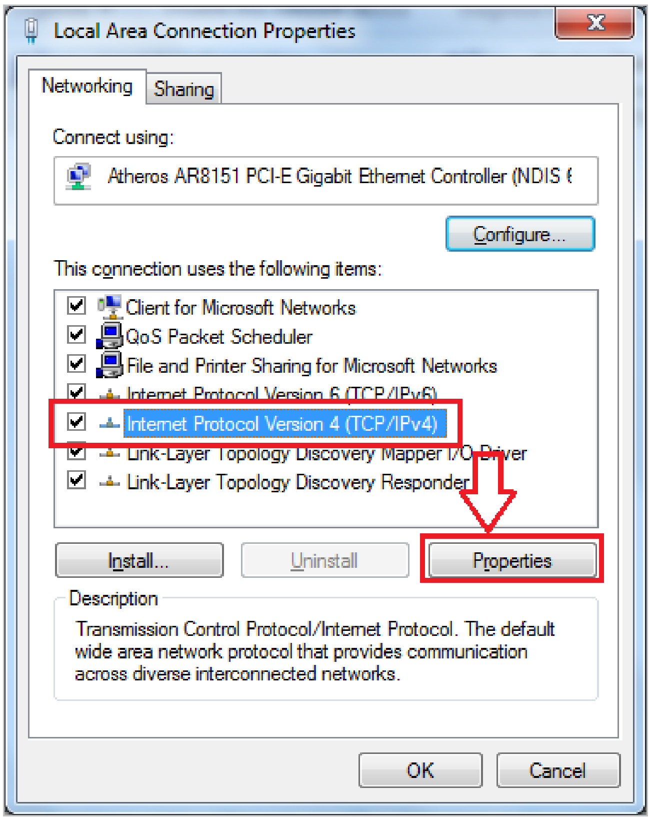


Figure 4-1-2 Network Connection Properties

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



Connect using:

Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6

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

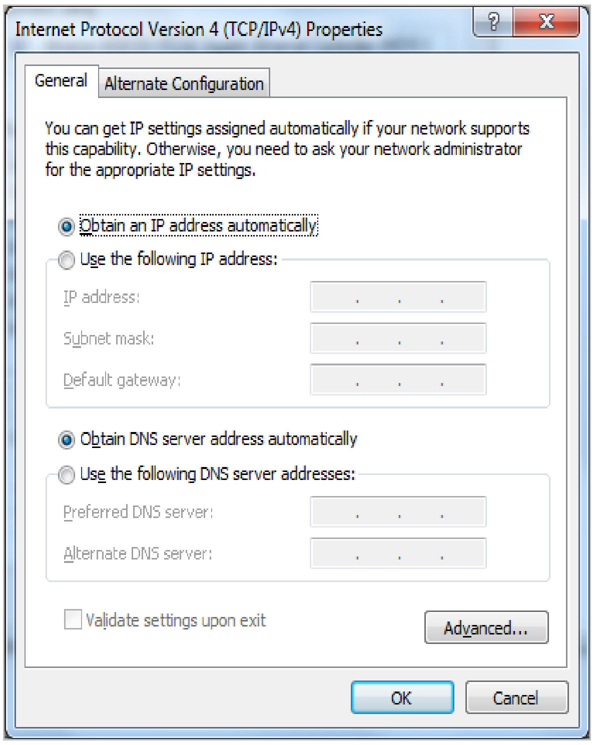
Description

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

Figure 4-1-3 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.



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

Figure 0-1-4 Obtain an IP address automatically

Configuring PC in Windows XP

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

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

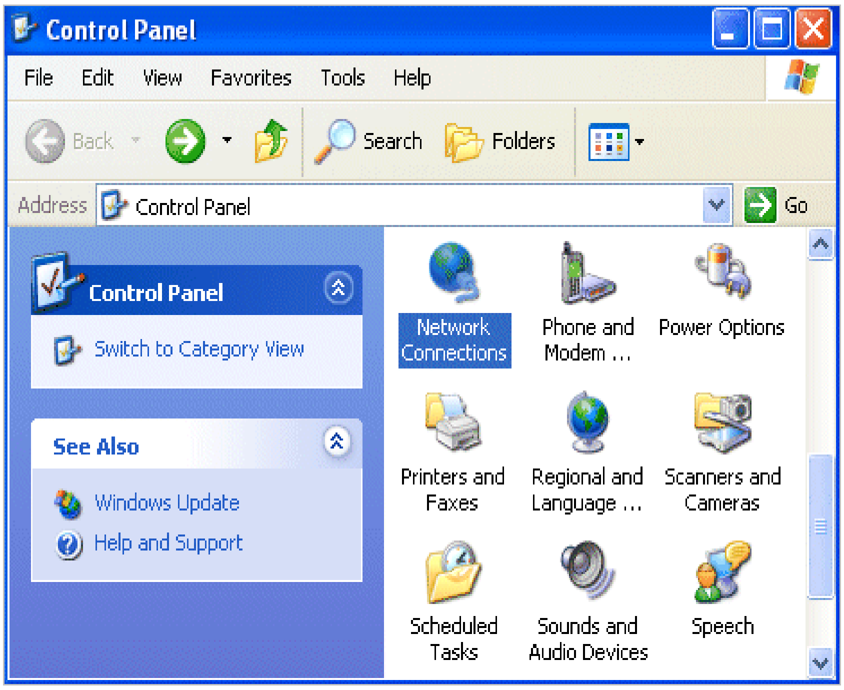
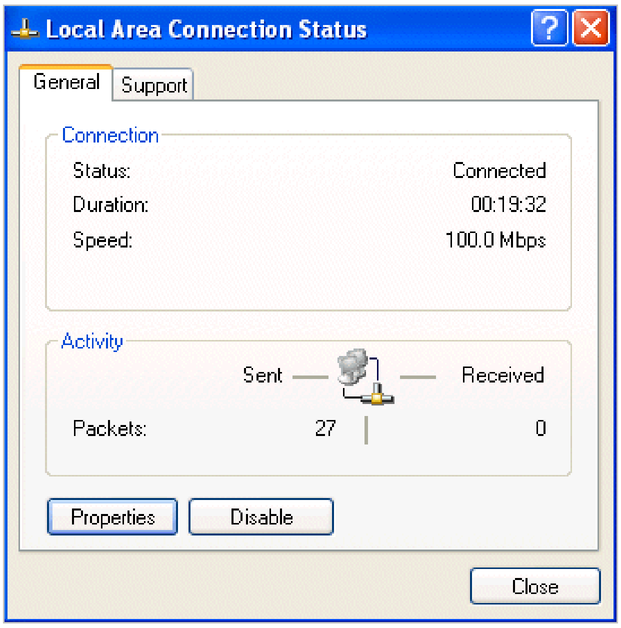


Figure 4-1-5 Select Network Connections

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

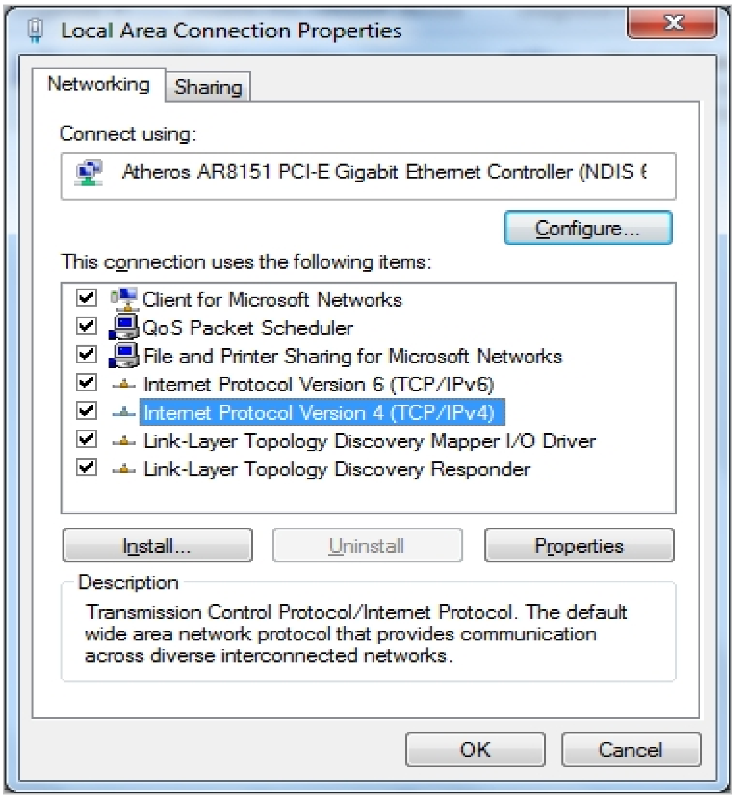


Status: Connected
Duration: 00:19:32
Speed: 100.0 Mbps

Packets: 27 0

Figure 4-1-6

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



Local Area Connection Properties

Connect using:

Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6

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

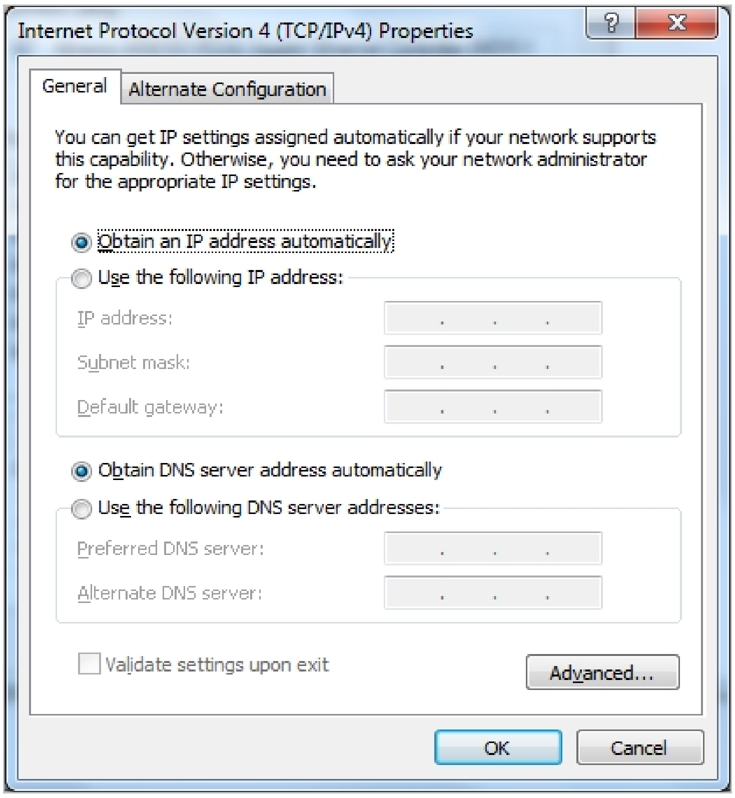
Description

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

Figure 4-1-7 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

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

Figure 4-1-8 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.

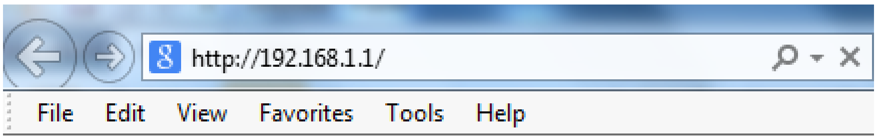
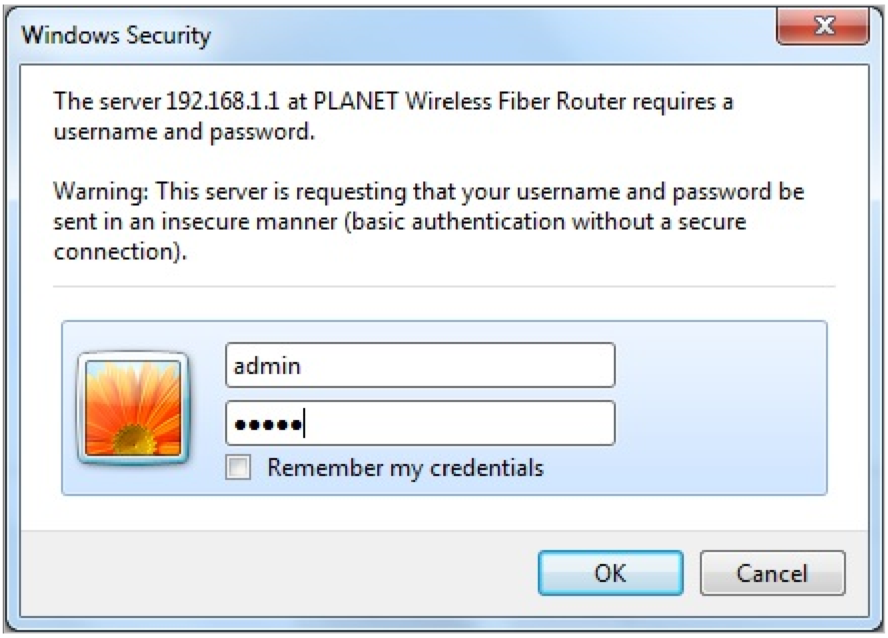

http://192.168.1.1/

Figure 4-2-1 Login the Router

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


Windows Security

The server 192.168.1.1 at PLANET Wireless Fiber Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

●●●●●

□ Remember my credentials

Figure 4-2-2 Login Window

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

Chapter 5. System Settings

Determine 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

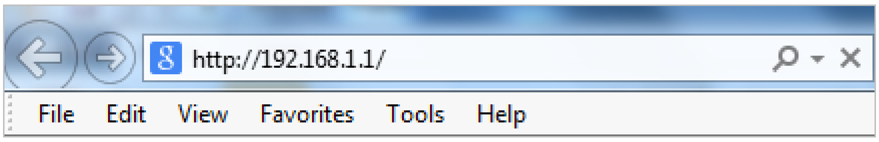
Unlike a simple hub or switch, the setup of the Fiber Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to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

Generally there are several different operating modes for your applications. And you can know which mode is necessary for your system from ISP. These modes are router, bridge, and PPPoE+NAT.

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.

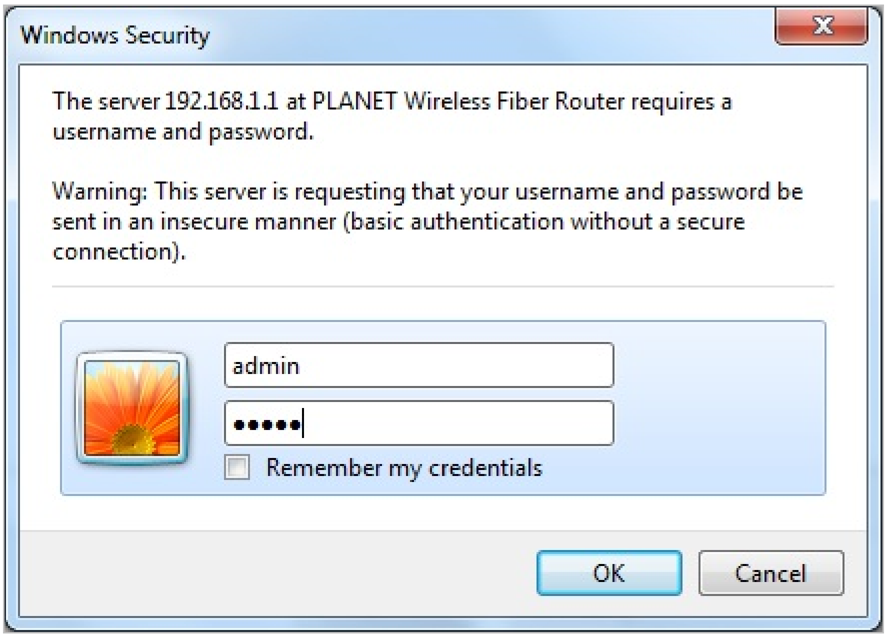
Save this address in your Favorites for future reference.



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 login the router and you can start to configure it now.


Windows Security

The server 192.168.1.1 at PLANET Wireless Fiber Router requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

•••••

□ Remember my credentials

Figure 5-2 Login Window

5.1 Operation Mode

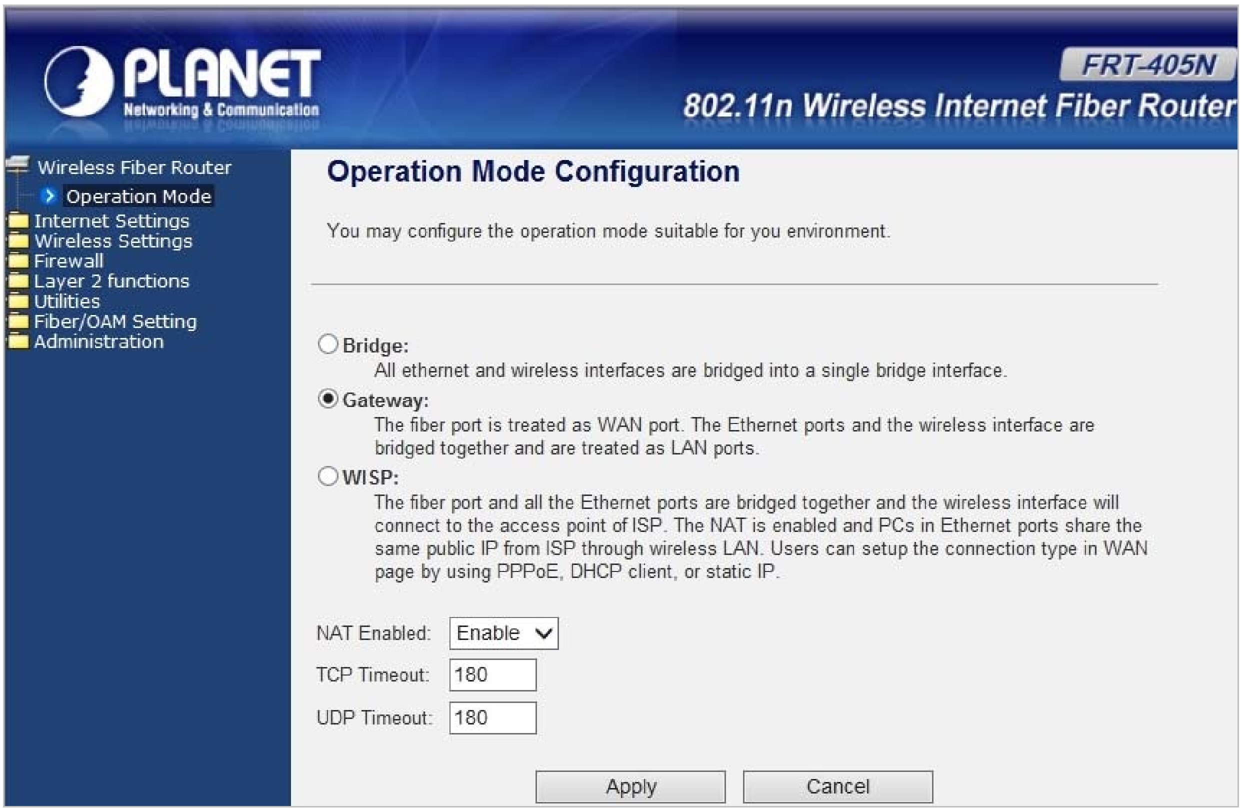
The FRT-405N supports three operation modes – Bridge, Gateway and WISP. Currently, the default setting is Gateway mode.

Please note that Bridge mode and Gateway mode cannot be used simultaneously.
For **Bridge mode**, all interfaces are bridged into a single bridge interface.
For **Gateway mode**, the fiber port is treated as WAN port. The other interfaces are bridged together and are treated as LAN ports.

For **WISP Mode**, all the Ethernet ports (including fiber port) are bridged together and the wireless interface of this router will come to WAN port for connecting to an ISP's Access Point as Internet connection. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be set up on WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP.

Note

If you select **Bridge mode** and **WAN configuration** in Internet Settings that are not available, firewall functions on the left page are not available, either.



Operation Mode Configuration

You may configure the operation mode suitable for you environment.

○ **Bridge:**
All ethernet and wireless interfaces are bridged into a single bridge interface.

● **Gateway:**
The fiber port is treated as WAN port. The Ethernet ports and the wireless interface are bridged together and are treated as LAN ports.

○ **WISP:**
The fiber port and all the Ethernet ports are bridged together and the wireless interface will connect to the access point of ISP. The NAT is enabled and PCs in Ethernet ports share the same public IP from ISP through wireless LAN. Users can setup the connection type in WAN page by using PPPoE, DHCP client, or static IP.

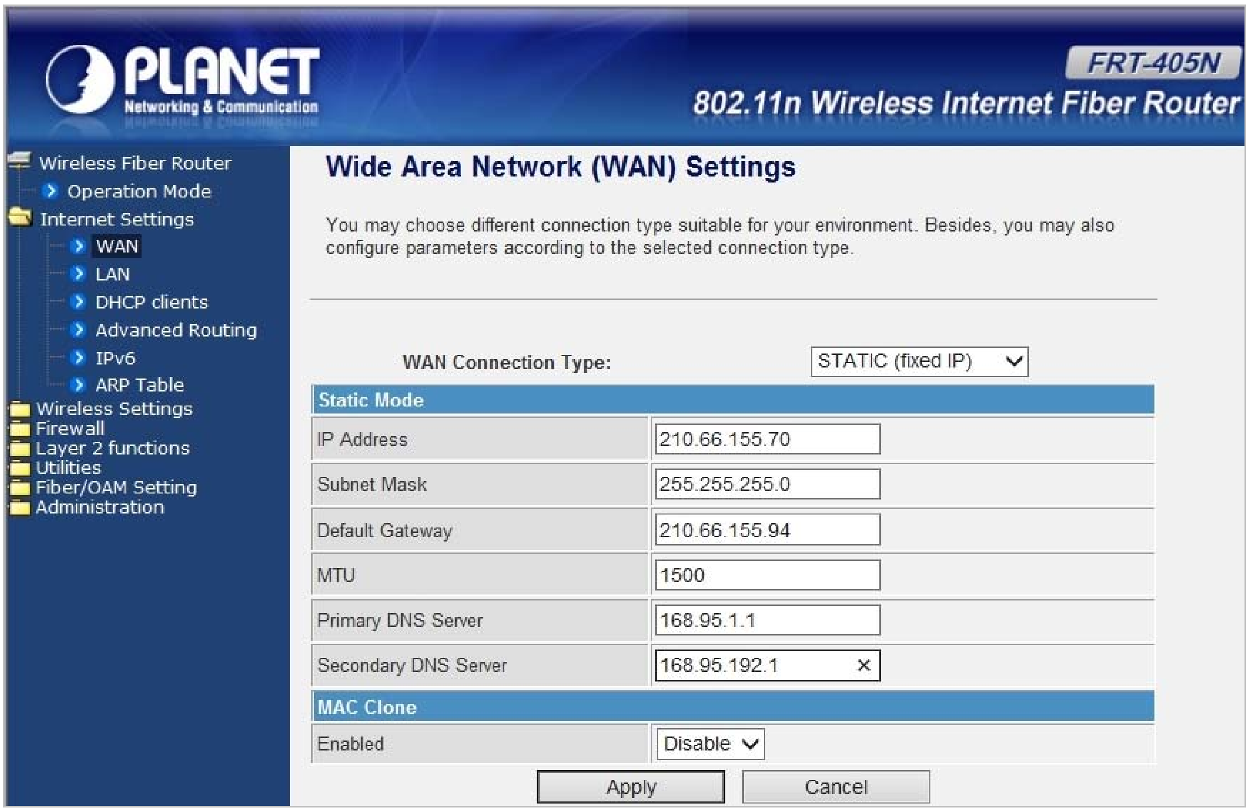
NAT Enabled: Enable
TCP Timeout: 180
UDP Timeout: 180

After finishing the settings, click **Apply** to save the settings and enable the new configuration to take effect. Click **Cancel** to close without saving.

5.2 Internet Settings

5.2.1 WAN

The WAN Settings screen allows you to specify the type of Internet connection. The WAN settings offer the following selections for the router's WAN port, STATIC (fixed IP), DHCP (Auto config), PPPoE, L2TP, and PPTP.



Wide Area Network (WAN) Settings

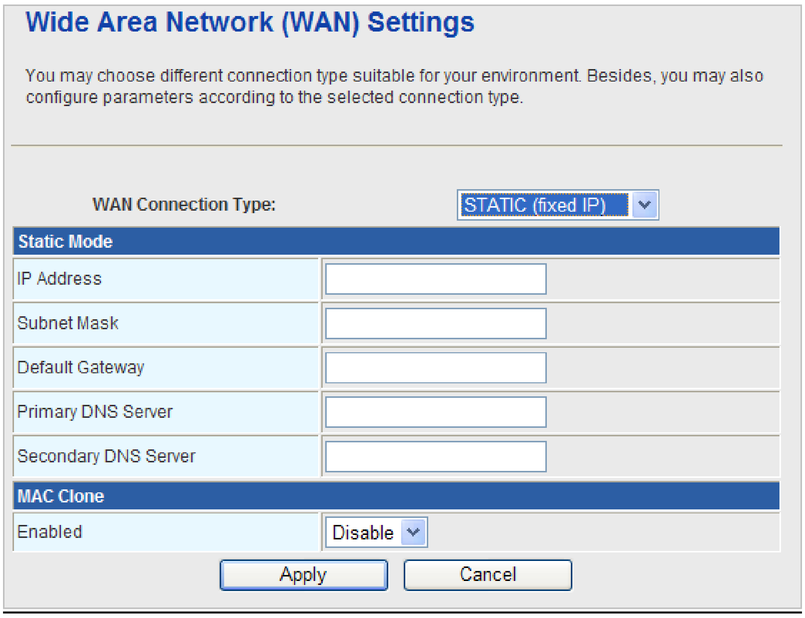
You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: STATIC (fixed IP)

Static Mode	
IP Address	210.66.155.70
Subnet Mask	255.255.255.0
Default Gateway	210.66.155.94
MTU	1500
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1
MAC Clone	
Enabled	Disable

■ STATIC (FIXED IP)

Select **STATIC (fixed IP)** in the **WAN Connection Type** drop-down list and the following page appears:



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: STATIC (fixed IP)

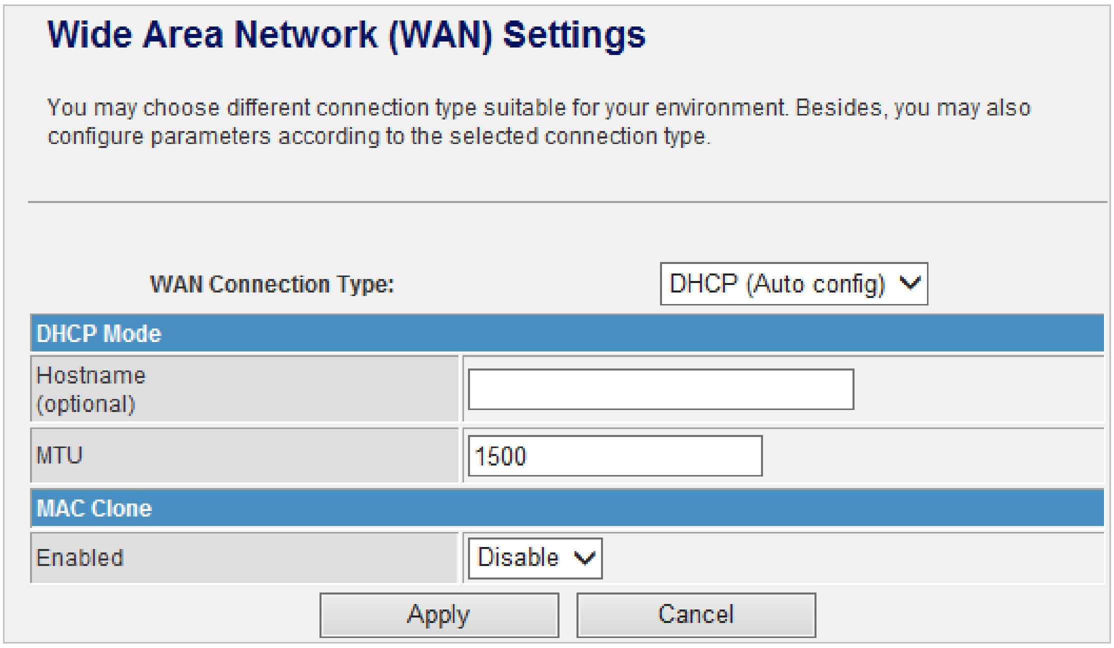
Static Mode	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
MAC Clone	
Enabled	Disable

The page includes the following fields:

Object	Description
IP Address	Enter the IP address in dotted-decimal notation provided by your ISP.
Subnet Mask	Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0
Default Gateway	Enter the gateway IP address in dotted-decimal notation provided by your ISP.
Primary/Secondary DNS	Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
MAC Clone	Enable or disable MAC clone.

■ DHCP (AUTO CONFIG)

Select **DHCP (Auto config)** in the **WAN Connection Type** drop-down list and the following page appears. If the WAN connection type is set to **DHCP**, the device automatically obtains the IP address, gateway and DNS address from the DHCP server on WAN interface.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config)

DHCP Mode	
Hostname (optional)	
MTU	1500

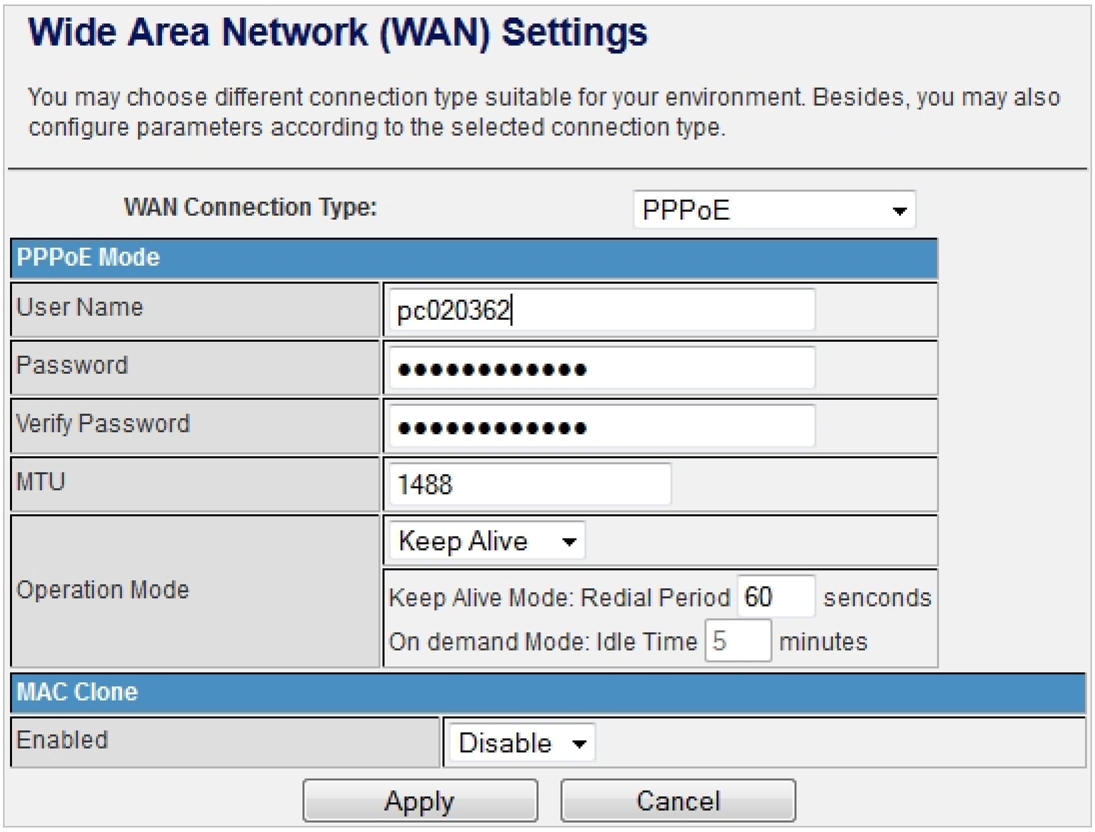
MAC Clone	
Enabled	Disable

The page includes the following fields:

Object	Description
Host Name	This option specifies the Host Name of the Router.
MAC Clone	Enable or disable MAC clone.

■ PPPOE

Select **PPPoE (ADSL)** in the **WAN Connection Type** drop-down list and the following page appears. If the WAN connection type is set to **PPPoE**, you can configure the following parameters to PPPoE dial up.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: PPPoE

PPPoE Mode	
User Name	pc020362
Password	●●●●●●●●●●●●
Verify Password	●●●●●●●●●●●●
MTU	1488
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes

MAC Clone	
Enabled	Disable

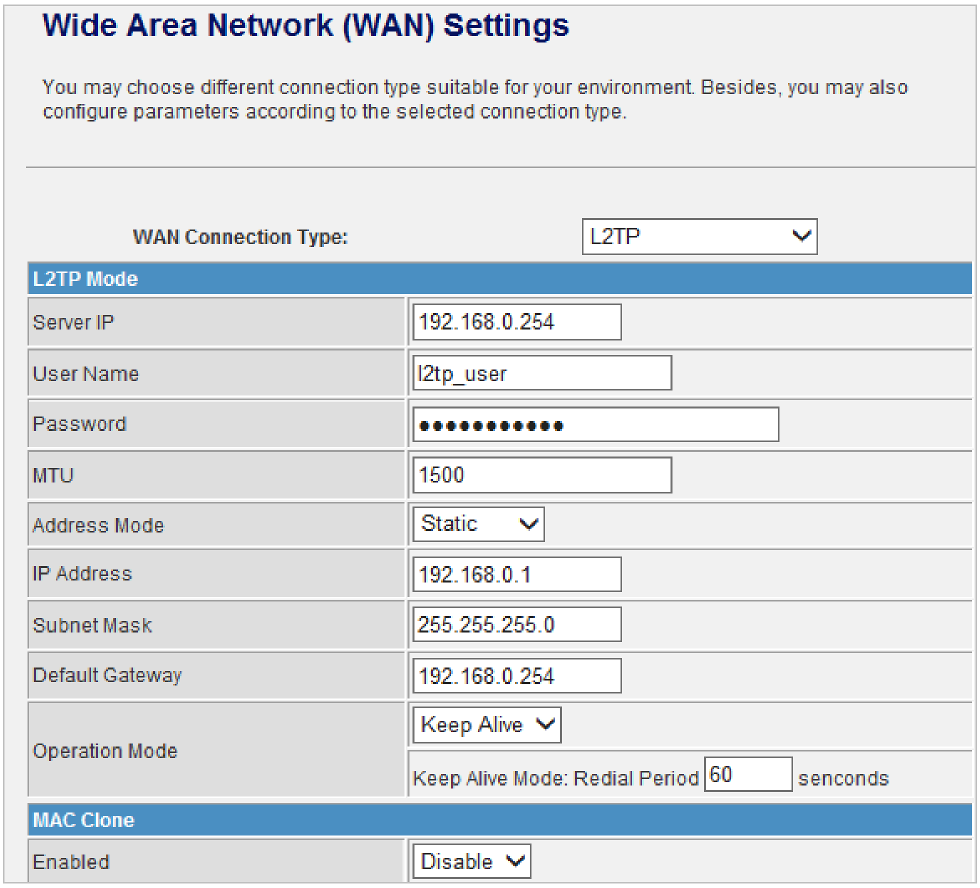
The page includes the following fields:

Object	Description
User Name/Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
Verify Password	Fill in the password again for verification.
Operation Mode	■ **Keep Alive:** Keep the PPPoE connection all the time. Please also configure the Redial Period field. ■ **On Demand:** Please configure the Idle Time field. When time is up, the PPPoE connection will disconnect. The connection will re-connect when any outgoing packet arise. ■ **Manual:** Close all function.
MAC Clone	Enable or disable MAC clone.

■ L2TP

Select **L2TP** in the **WAN Connection Type** drop-down list and the following page appears. There are two address modes: **Static** and **Dynamic**.

1. If you select **Static** in the **Address Mode** field, the page shown in the following figure appears:



Wide Area Network (WAN) Settings

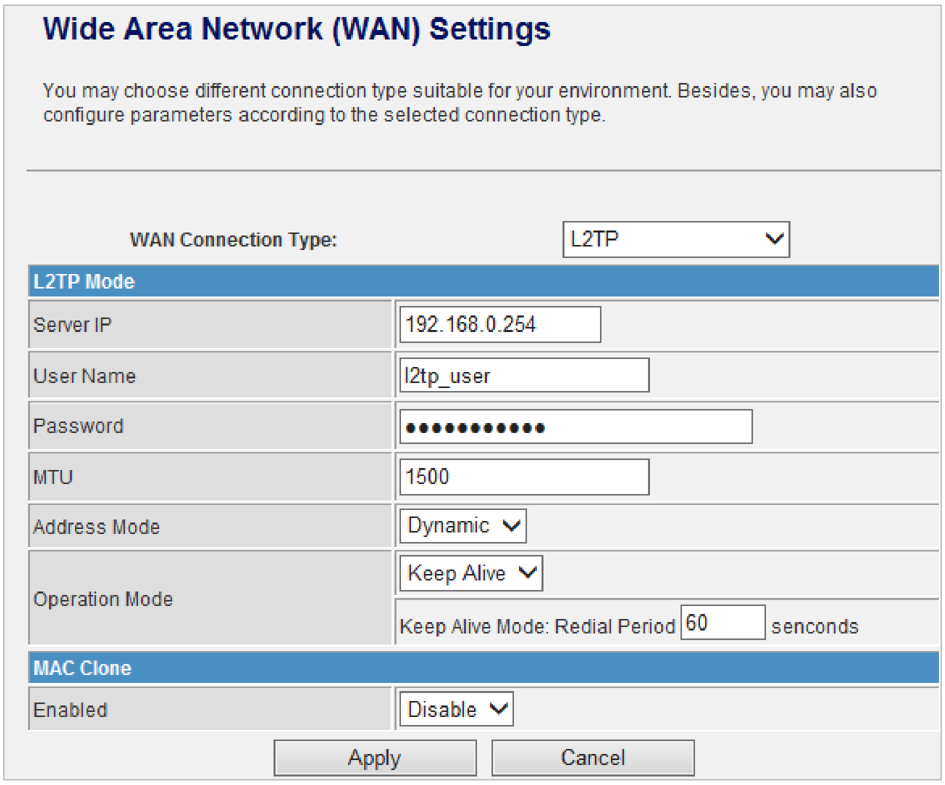
You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: L2TP

L2TP Mode	
Server IP	192.168.0.254
User Name	l2tp_user
Password	●●●●●●●●●●●
MTU	1500
Address Mode	Static
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds

MAC Clone	
Enabled	Disable

2. If you select **Dynamic** in the **Address Mode** field, the page shown in the following figure appears:



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: L2TP

L2TP Mode

Server IP	192.168.0.254
User Name	l2tp_user
Password	●●●●●●●●●●●
MTU	1500
Address Mode	Dynamic
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds

MAC Clone

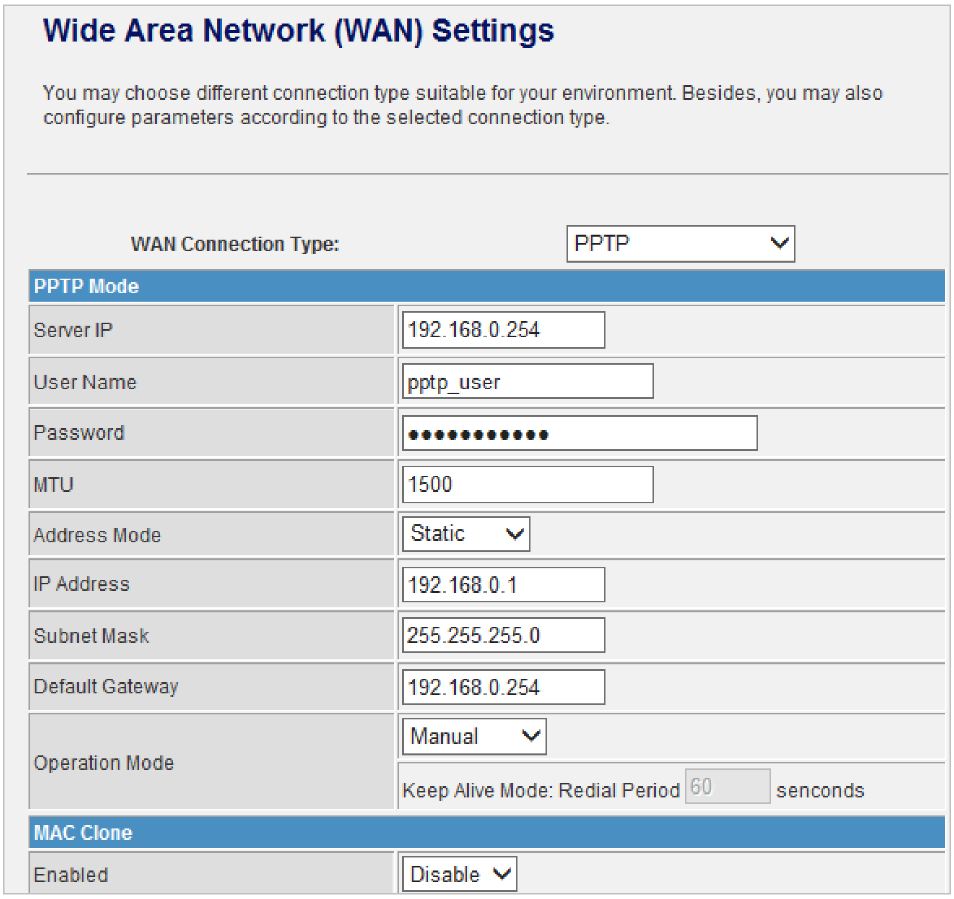
Enabled	Disable

The page includes the following fields:

Object	Description
Server IP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded L2TP client supported by this router to make a VPN connection. If you select the L2TP support on WAN interface, fill in the IP address for it.
User Name/Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
MTU	The Maximum Transmission Unit default setting is 1500.
Address Mode	■ **Static:** To configure the IP address information by manually, please fill in the related setting at below. ■ **Dynamic:** The option allows the machine to get IP address information automatically from DHCP server on WAN side.
IP Address	Fill in the IP address for WAN interface.
Subnet Mask	Fill in the subnet mask for WAN interface.
Default Gateway	Fill in the default gateway for WAN interface out going data packets.
Operation Mode	■ **Keep Alive:** Keep the L2TP connection all the time. Please also configure the Redial Period field. ■ **Manual:** All functions are disabling.
MAC Clone	Enable or disable MAC clone.

PPTP

Select **PPTP** in the **WAN Connection Type** drop-down list and the following page appears. There are two address modes: **Static** and **Dynamic**.



Wide Area Network (WAN) Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: PPTP

PPTP Mode	
Server IP	192.168.0.254
User Name	pptp_user
Password	●●●●●●●●●●●
MTU	1500
Address Mode	Static
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254
Operation Mode	Manual Keep Alive Mode: Redial Period 60 senconds
MAC Clone	
Enabled	Disable

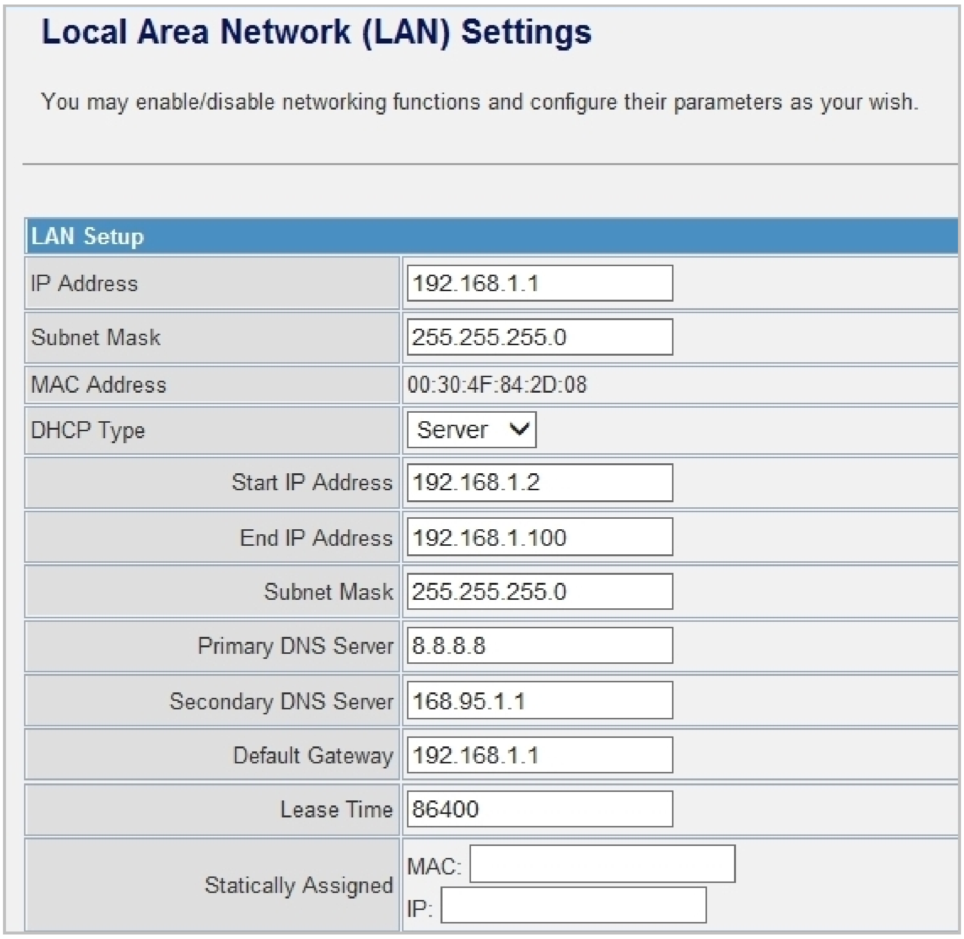
The page includes the following fields:

Object	Description
Server IP	Allow user to make a tunnel with remote site directly to secure the data transmission among the connection. User can use embedded PPTP client supported by this router to make a VPN connection. If you select the PPTP support on WAN interface, fill in the IP address for it.
User Name/Password	Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
MTU	The Maximum Transmission Unit default setting is 1500.
Address Mode	**Static:** To configure the IP address information by manually, please fill in the related setting at below. **Dynamic:** The option allows the machine to get IP address information automatically from DHCP server on WAN side.
IP Address	Fill in the IP address for WAN interface.

Subnet Mask	Fill in the subnet mask for WAN interface.
Default Gateway	Fill in the default gateway for WAN interface out going data packets.
Operation Mode	**Keep Alive:** Keep the PPTP connection all the time. Please also configure the Redial Period field. **Manual:** No function is enabling.
MAC Clone	Enable or disable MAC clone.

5.2.2 LAN

This page allows you to enable or disable networking functions and configure their parameters according to your practice.



Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

LAN Setup	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
MAC Address	00:30:4F:84:2D:08
DHCP Type	Server
Start IP Address	192.168.1.2
End IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Primary DNS Server	8.8.8.8
Secondary DNS Server	168.95.1.1
Default Gateway	192.168.1.1
Lease Time	86400
Statically Assigned	MAC: IP:

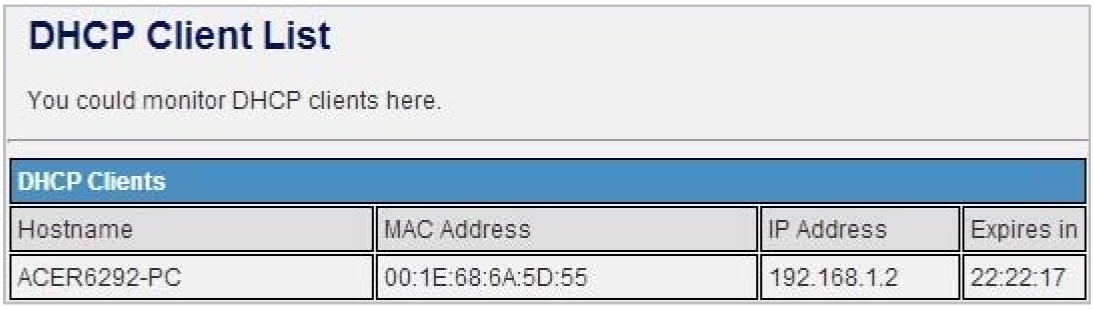
The page includes the following fields:

Object	Description
MAC Address	The physical address of the Router, as seen from the LAN. The value can't be changed.
IP Address	Enter the IP address of your Router or reset it in dotted-decimal notation (factory default: 192.168.1.1).
Subnet Mask	An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
MAC Address	MAC address of LAN port (Read-only).
DHCP Type	■ **Disable:** Disable DHCP server on LAN side. ■ **Server:** Enable DHCP server on LAN side.
Start IP Address	Fill in the start IP address to allocate a range of IP addresses; client

	with DHCP function set will be assigned an IP address from the range.
End IP Address	Fill in the end IP address to allocate a range of IP addresses; client with DHCP function set will be assigned an IP address from the range.
Subnet Mask	The subnet mask of dynamic IP.
Primary DNS Server	The primary DNS server address.
Secondary DNS Server	The secondary DNS server address.
Default Gateway	Fill in the default gateway for LAN interfaces out going data packets.
Lease Time	Fill in the lease time of DHCP server function.
Statically Assigned	Assign IP to the assigned MAC address. Enter the assigned MAC address and IP in the corresponding fields.
802.1d Spanning Tree	Select enable or disable the IEEE 802.1d Spanning Tree function from pull-down menu.
LLTD	Select enable or disable the Link Layer Topology Discover function from pull-down menu.
IGMP Proxy	Select enable or disable the IGMP proxy function from pull-down menu.
UPNP	Select enable or disable the UPnP protocol from pull-down menu.
Router Advertisement	You can select Enable or Disable.
PPPoE Relay	You can select Enable or Disable.
DNS Proxy	Select enable or disable the DNS Proxy function from pull-down menu.

5.2.3 DHCP clients

You can view the information about DHCP clients on the page.



DHCP Client List

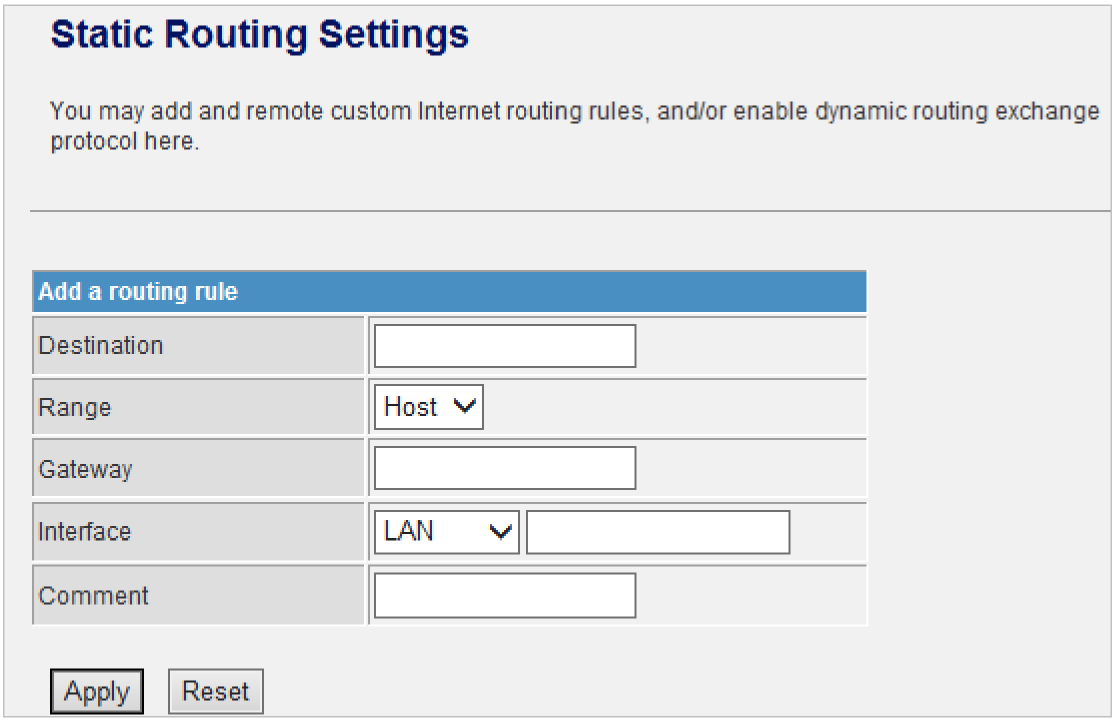
You could monitor DHCP clients here.

DHCP Clients

Hostname	MAC Address	IP Address	Expires in
ACER6292-PC	00:1E:68:6A:5D:55	192.168.1.2	22:22:17

5.2.4 Advanced Routing

You can add or delete routing rules, and enable or disable dynamic routing protocol on the page.



Static Routing Settings

You may add and remote custom Internet routing rules, and/or enable dynamic routing exchange protocol here.

Add a routing rule	
Destination	
Range	Host
Gateway	
Interface	LAN
Comment	

The page includes the following fields:

Object	Description
Destination	Enter the legal destination IP address.
Range	Destination IP address is a host address or the network address.
Gateway	Enter the specific gateway.
Interface	The interface for this route. You can select LAN, WAN and Custom.
Comment	Add the description of this route.

Current Routing Table in the System

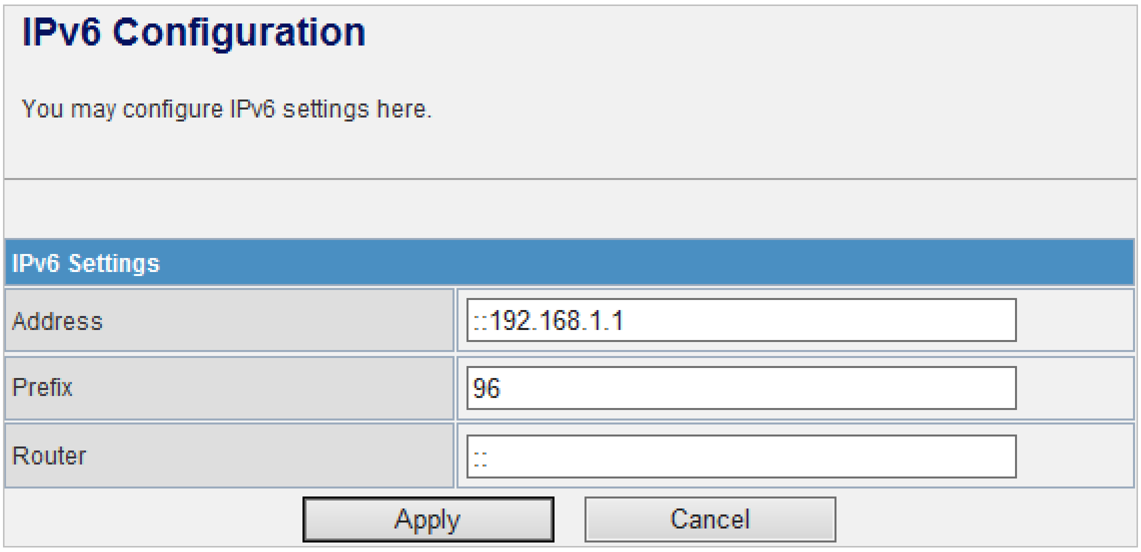
You can delete or reset the routing rules.

Dynamic Routing Settings

You can enable or disable the **RIP**.
After finishing the settings above, click **Apply** to enable the new routing rule to take effect. Otherwise, click **Reset** to cancel the new routing rule.

5.2.5 IPv6

You may set up rules to provide Quality of Service (QoS) guarantee for some specific applications. On the page, you can enable or disable Quality of Service.



IPv6 Configuration

You may configure IPv6 settings here.

IPv6 Settings

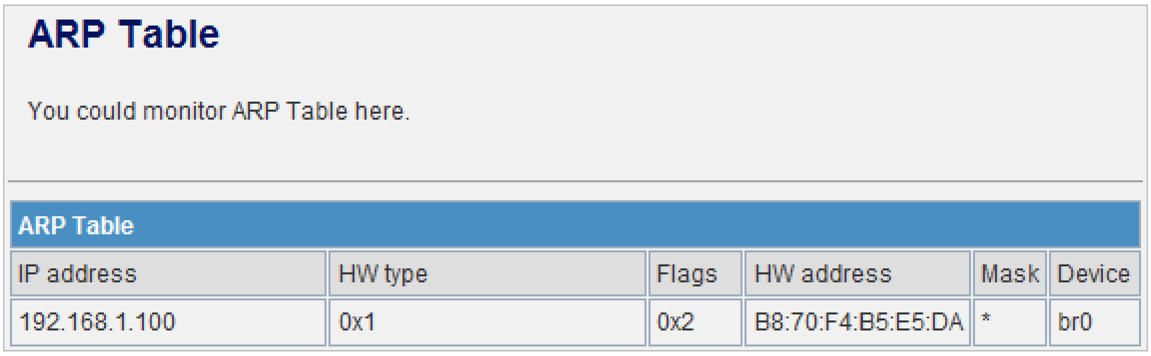
Address	::192.168.1.1
Prefix	96
Router	::

The page includes the following fields:

Object	Description
Address	You can set up IPV6 address here.
Prefix	You can set up the IPv6 Prefix here.
Router	You can set up the IPv6 router here.

5.2.6 ARP Table

You can view the information about ARP Table on the page.



ARP Table

You could monitor ARP Table here.

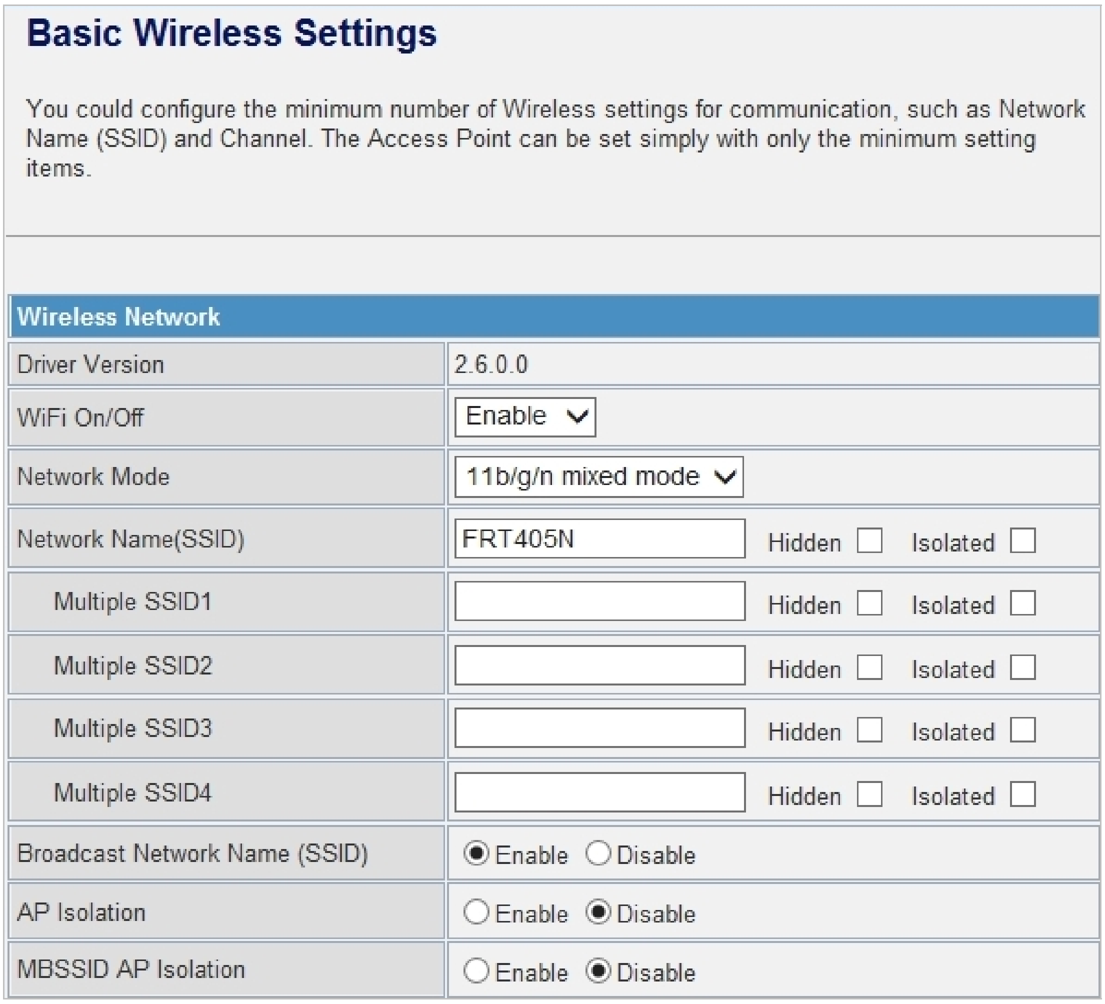
ARP Table

IP address	HW type	Flags	HW address	Mask	Device
192.168.1.100	0x1	0x2	B8:70:F4:B5:E5:DA	*	br0

5.3 Wireless Setting

5.3.1 Basic

You can configure the minimum number of wireless settings for communication, such as network name (SSID) and channel.



Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication, such as Network Name (SSID) and Channel. The Access Point can be set simply with only the minimum setting items.

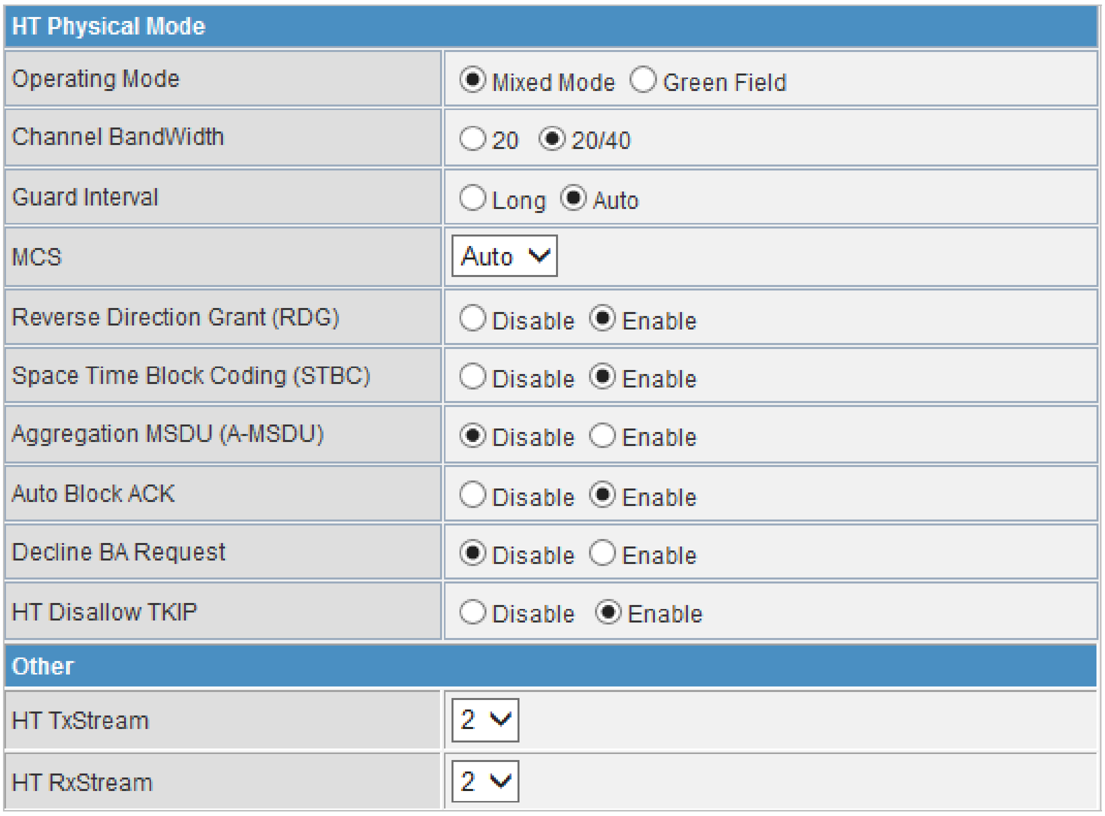
Wireless Network	
Driver Version	2.6.0.0
WiFi On/Off	Enable
Network Mode	11b/g/n mixed mode
Network Name(SSID)	FRT405N Hidden □ Isolated □
Multiple SSID1	Hidden □ Isolated □
Multiple SSID2	Hidden □ Isolated □
Multiple SSID3	Hidden □ Isolated □
Multiple SSID4	Hidden □ Isolated □
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable

The page includes the following fields:

Object	Description
Driver Version	Show the driver version.
WiFi On/Off	Enable or disable the wireless LAN.
Network Mode	This field determines the wireless mode which the Router works on.
Network Name (SSID)	Enter a value of up to 32 characters. The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security, the default SSID is set to be default. This value is case-sensitive. For example, *PLANET*

	is NOT the same as planet.
Multiple SSID 1/2/3/4	There are 4 multiple SSIDs. Enter their descriptive names that you want to use.
Broadcast Network Name (SSID)	Select **Enable** to allow the SSID broadcast on the network, so that the STA can find it. Otherwise, the STA cannot find it.
AP Isolation	**Enable** or **disable** AP Isolation. When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can enable this function.
MBSSID AP Isolation	Enable or disable MBSSID AP Isolation.
BSSID	Basic Service Set Identifier. This is the assigned MAC address of the station in the access point. This unique identifier is in Hex format and can only be edited when Multi BSSID is enabled in the previous screen.
Frequency (Channel)	A channel is the radio frequency used by wireless device. Channels available depend on your geographical area. You may have a choice of channels (for your region) and you should use a different channel from an adjacent AP to reduce the interference. The Interference and degrading performance occurs when radio signals from different APs overlap.

HT Physical Mode



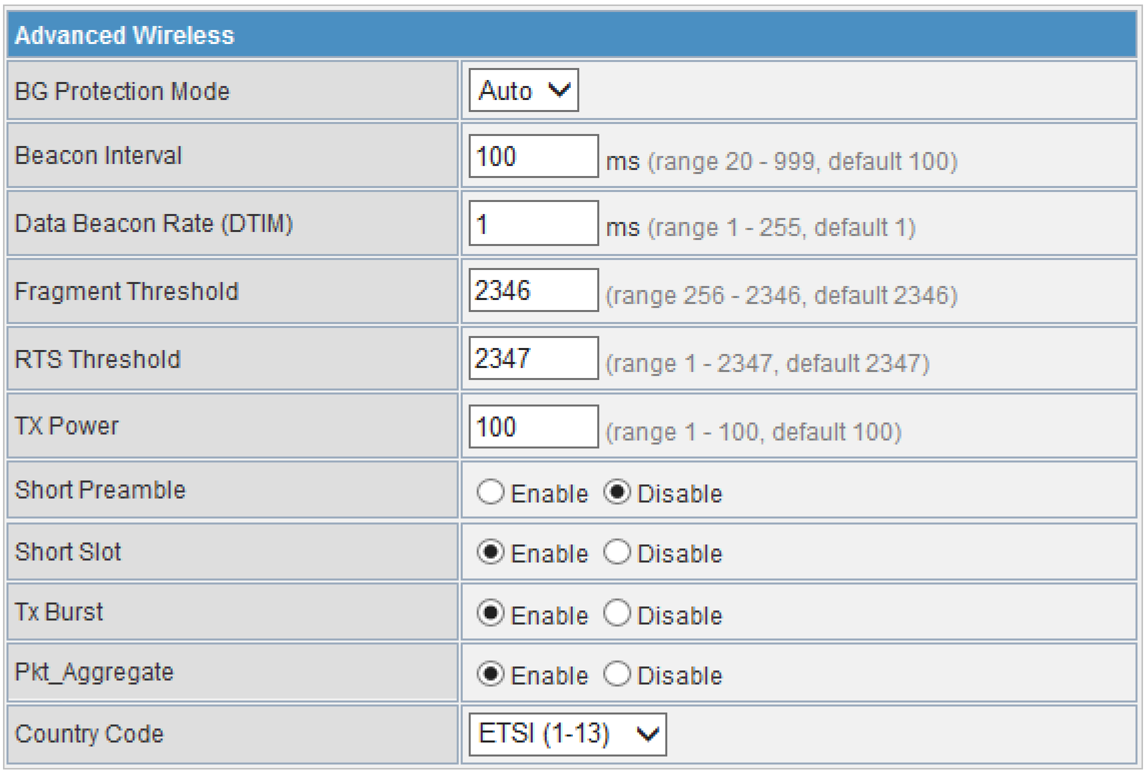
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant (RDG)	○ Disable ● Enable
Space Time Block Coding (STBC)	○ Disable ● Enable
Aggregation MSDU (A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
Other	
HT TxStream	2
HT RxStream	2

The page includes the following fields:

Object	Description
Operation Mode	Select Mixed Mode or Green Field.
Channel Bandwidth	Select 20 or 20/40.
Guard Interval	Select 20 or 20/40.
MCS	Select the proper value from 0 to 32. Auto is the default value.
Reverse Direction Grant (RDG)	The purpose of the 802.11n RD protocol is to more efficiently transfer data between two 802.11 devices during a TXOP by eliminating the need for either device to initiate a new data transfer. Select Disable or Enable.
Space Time Block Coding (STBC)	Space time block coding is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data-transfer. Select Disable or Enable.
Aggregation MSDU (A-MSDU)	A-MSDU aggregation, which allows several MAC-level service data units (MSDUs) to be aggregated into a single MPDU. Select Disable or Enable.
Auto Block ACK	Not to respond to each sent data (ACK), but to block unit (Block). Select Disable or Enable.
Decline BA Request	To decline the Block ACK request by the other devices. Select Disable or Enable.
HT Disallow TKIP	Using TKIP, the operation will be in 802.11g. Select Disable or Enable.
HT TxStream	Select 1 or 2.
HT RxStream	Select 1 or 2.

5.3.2 Advanced

This page includes more detailed settings for the AP. **Advanced Wireless Settings** page includes items that are not available on the **Basic Wireless Settings** page, such as basic data rates, beacon interval, and data beacon rate.



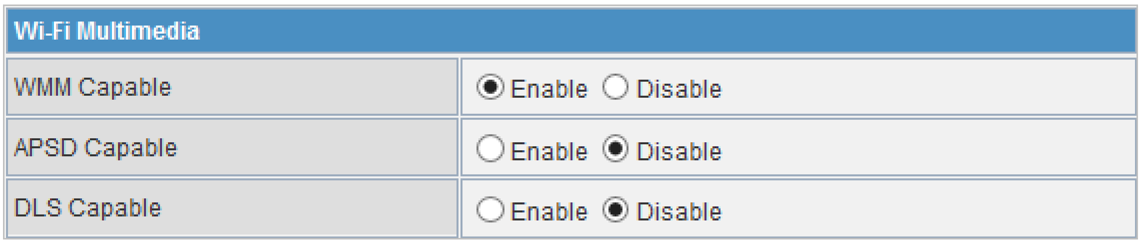
Advanced Wireless

BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
Country Code	ETSI (1-13)

The page includes the following fields:

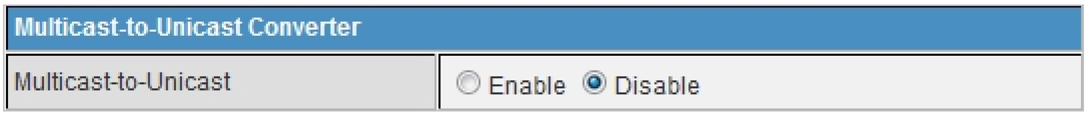
Object	Description
BG Protection Mode	It provides 3 options, including Auto, On, and Off. The default BG protection mode is **Auto**.
Beacon Interval	The interval time range is between 20ms and 999ms for each beacon transmission. The default value is 100ms.
Date Beacon Rate (DTM)	The DTM range is between 1 ms and 255 ms. The default value is 1ms.
Fragment Threshold	This is the maximum data fragment size (between 256 bytes and 2346 bytes) that can be sent in the wireless network before the router fragments the packet into smaller data frames. The default value is 2346.
RTS Threshold	**Request to send** (**RTS**) is designed to prevent collisions due to hidden node. A RTS defines the biggest size data frame you can send before a RTS handshake invoked. The RTS threshold value is between 1 and

	2347. The default value is 2347.
Tx Power	The Tx Power range is between 1 and 100. The default value is 100.
Short Preamble	Short preambles work with every wireless type other than older types with limited transmission rates in the 1 to 2 Mbps range. Select Disable or Enable.
Short Slot	Short slot time reduces the slot time from 20 microseconds to 9 microseconds, thereby increasing throughput. Select Disable or Enable.
Tx Burst	TX burst is a feature for wireless device speed up the connection in the same environment as it is without. Select Disable or Enable.
Pkt_Aggregate	Select Disable or Enable.
Country Code	Select the region which area you are. It provides three regions in the drop-down list.



Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
DLS Capable	○ Enable ● Disable

Object	Description
WMM Capable	WiFi Multimedia (WMM) refers to Qos over WiFi. It is suitable for simple applications that require QoS, such as Voice over IP (VoIP) Enable or disable WMM.
APSD Capable	Automatic power save delivery (APSD) is an efficient power management method. Enable or disable APSD.
DLS Capable	Direct-Link Setup (DLS) are able to automatically create a secure, direct link between them after accessing the Wi-Fi network, removing the need to transmit data through the access point. Enable or disable DLS.

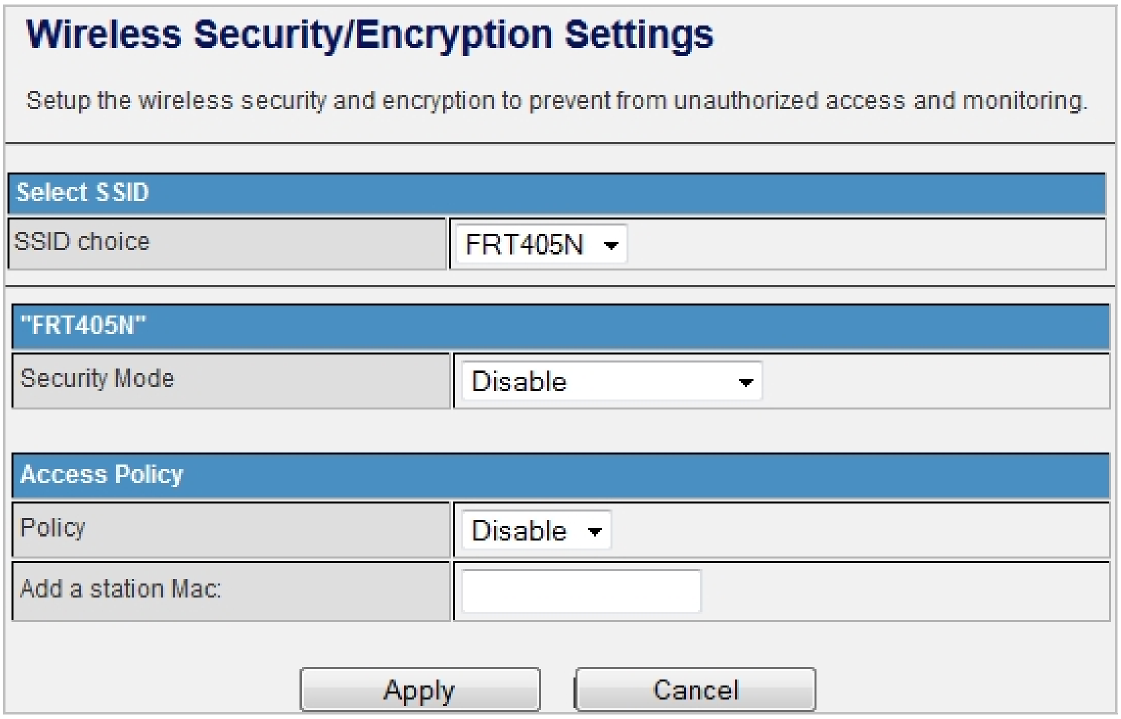


Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ Enable ● Disable

Object	Description
Multicast-to-Unicast	There are two main ways that Windows Media servers send data to Windows Media Player clients: multicast and unicast. Enable or Disable Multicast-to-Unicast

5.3.3 Security

Choose **Wireless Settings>Security** and the following page appears. It allows you to modify the settings to prevent the unauthorized accesses.



Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice: FRT405N

"FRT405N"

Security Mode: Disable

Access Policy

Policy: Disable

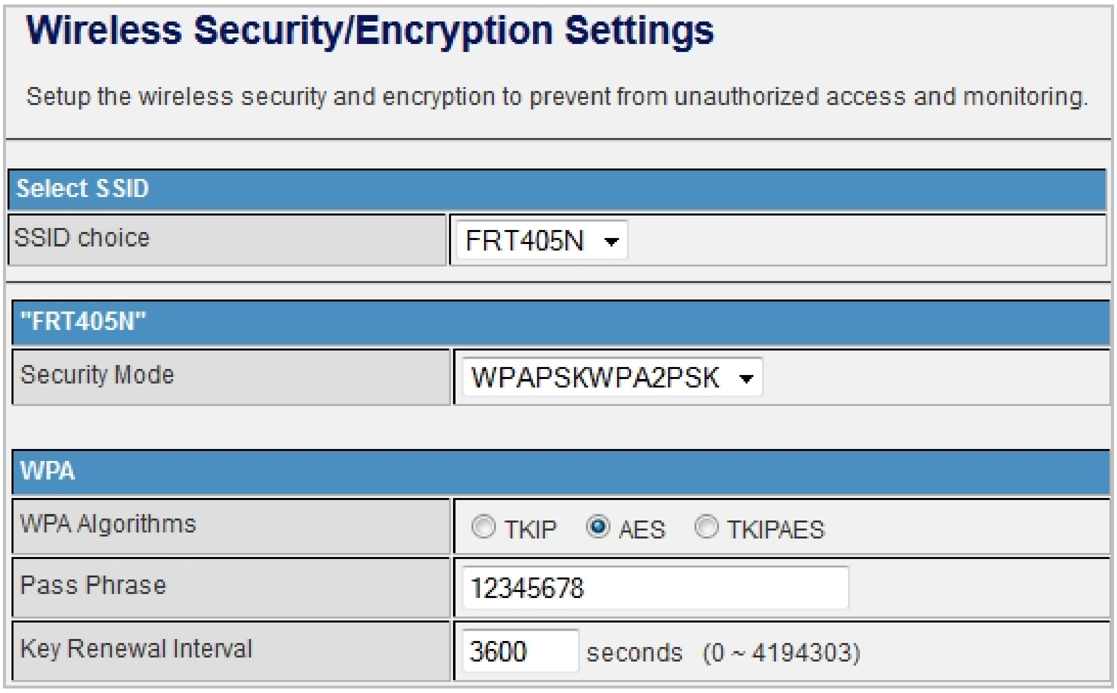
Add a station Mac:

The page includes the following fields:

Object	Description
SSID choice	Select SSID in the drop-down list**.**
Security Mode	There are 5 options, including **Disable, OPENWEP, WPA-PSK, WPA2-PSK, and WPAPSKWPA2PSK**.

[EXAMPLE]

Take WPAPSKWPA2PSK for example. Select WPAPSKWPA2PSK in the **Security Mode** down-list. The page shown in the following page appears:



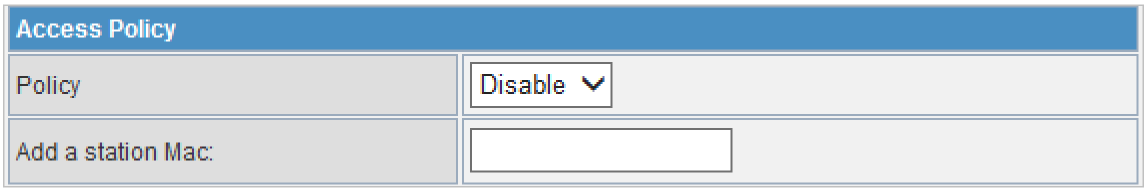
Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID	
SSID choice	FRT405N

"FRT405N"	
Security Mode	WPAPSKWPA2PSK

WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	12345678
Key Renewal Interval	3600 seconds (0 ~ 4194303)



Access Policy	
Policy	Disable
Add a station Mac:	

Access Policy

Object	Description
Policy	There are three options, including Disable, Allow, and Reject. Select Allow, only the clients whose MAC address is listed can access the router. Select Reject, the clients whose MAC address is listed are denied to access the router.
Add a station MAC	If you want to add a station MAC, enter the MAC address of the wireless station that are allowed or denied access to your router in this address field.

5.3.4 WDS

WDS (Wireless Distribution System) allows access points to communicate with one another wirelessly in a standardized way. It can also simplify the network infrastructure by reducing the amount of cabling required. Basically the access points will act as a client and an access point at the same time.

WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bi-directional, so the AP must know the MAC address of the other AP, and the other AP must have a WDS link back to the AP.

Dynamically assigned and rotated encryption key are not supported in a WDS connection. This means that WPA and other dynamic key assignment technologies may not be used. Only Static WEP keys may be used in a WDS connection, including any STAs that are associated with a WDS repeating AP.

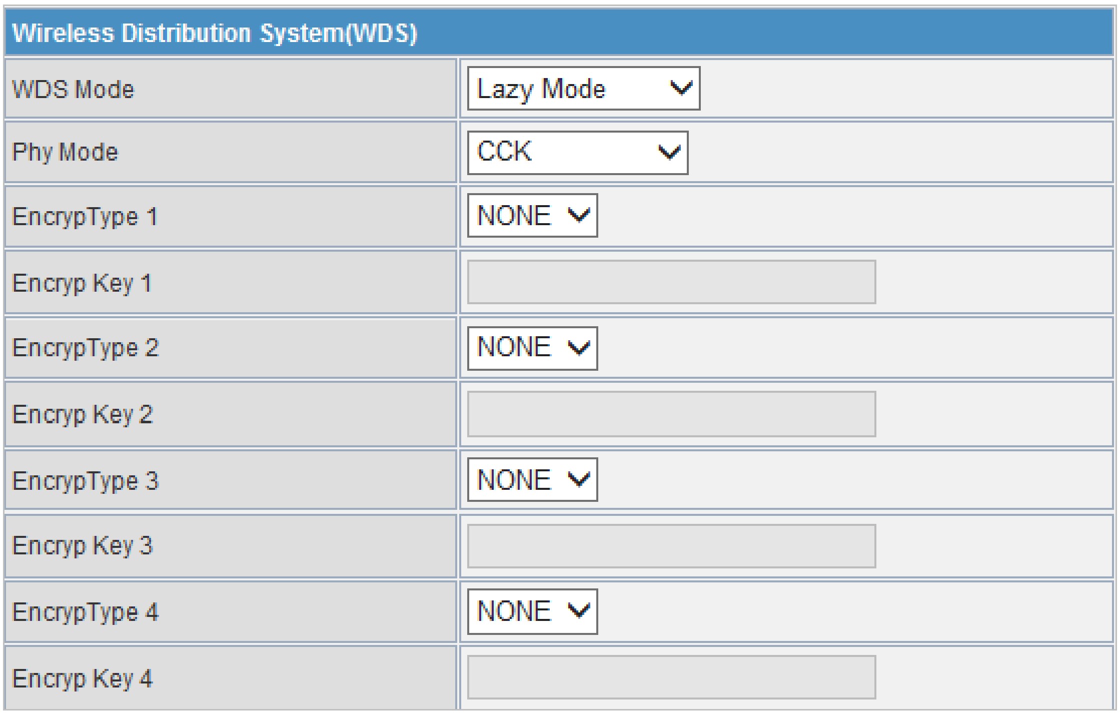
Enter the MAC address of the other APs that you want to link to and click enable. Supports up to 4 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses.

WDS Mode: There are four options, including **Disable**, **Lazy Mode**, **Bridge Mode**, and **Repeater Mode**.

Disable

Select Disable to disable the WDS mode.

Lazy Mode



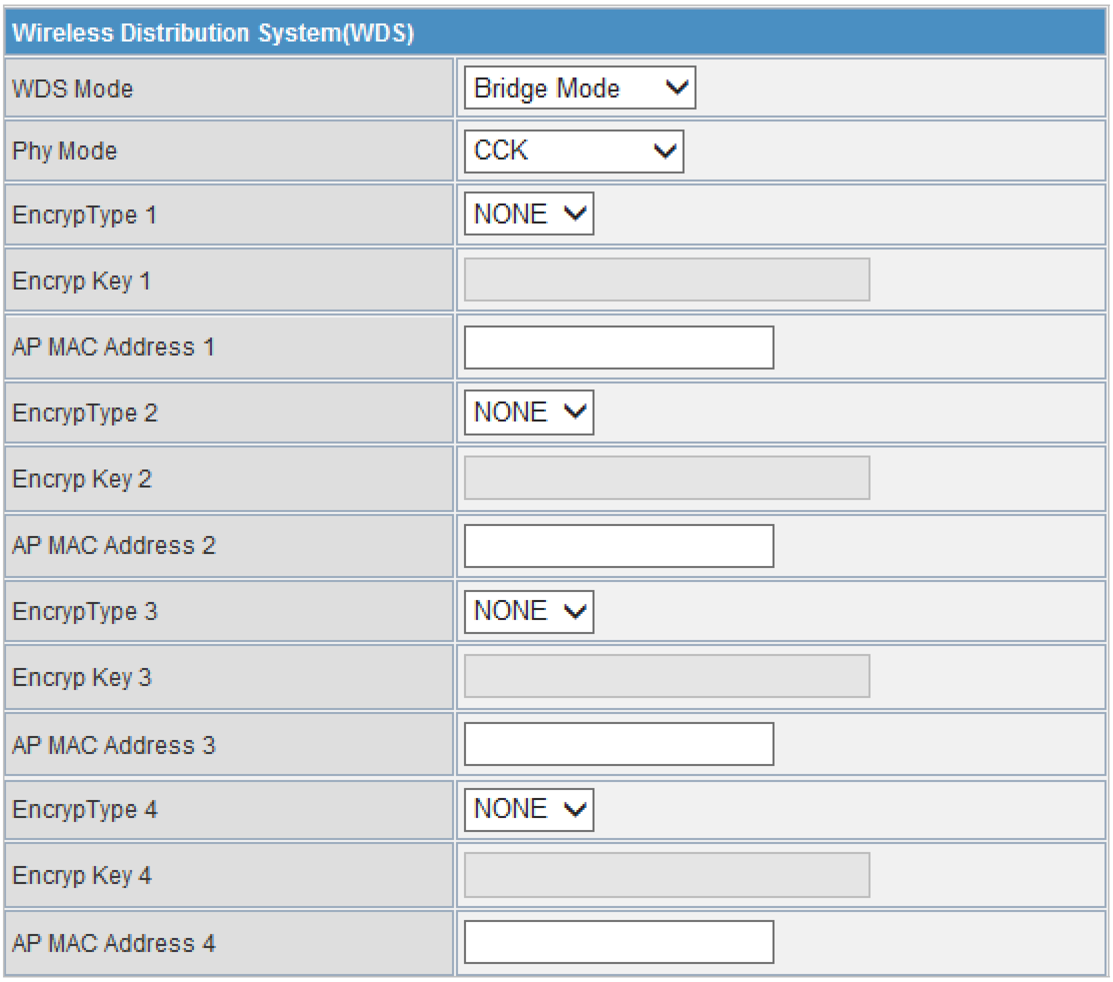
Wireless Distribution System(WDS)

WDS Mode	Lazy Mode
Phy Mode	CCK
EncrypType 1	NONE
Encryp Key 1	
EncrypType 2	NONE
Encryp Key 2	
EncrypType 3	NONE
Encryp Key 3	
EncrypType 4	NONE
Encryp Key 4	

The page includes the following fields:

Object	Description
Lazy Mode	The FRT-405N WDS Lazy mode is allowed the other FRT-405N WDS bridge / repeater mode link automatically.
Phy Mode	It provides 4 options, including **CCK**, **OFDM**, **HTMIX**, and **GREENFIELD**.
Encryp Type	It provides 4 options, including **None, WEP, TKIP,** and **AES**.

Bridge Mode/ Repeater Mode



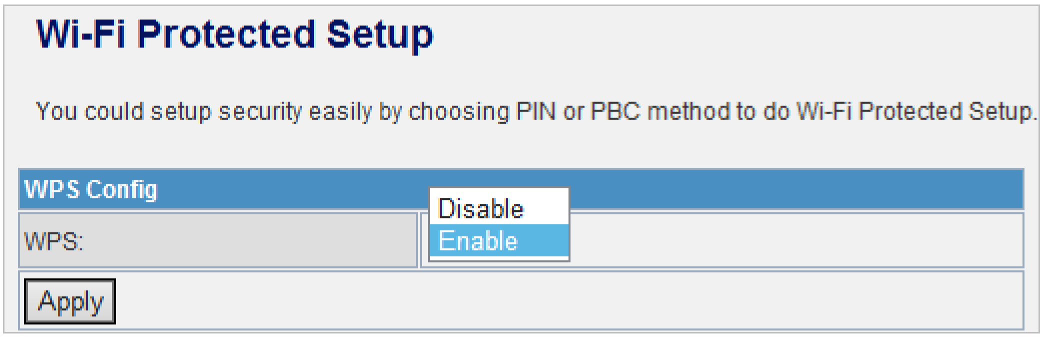
Wireless Distribution System(WDS)

WDS Mode	Bridge Mode
Phy Mode	CCK
EncrypType 1	NONE
Encryp Key 1	
AP MAC Address 1	
EncrypType 2	NONE
Encryp Key 2	
AP MAC Address 2	
EncrypType 3	NONE
Encryp Key 3	
AP MAC Address 3	
EncrypType 4	NONE
Encryp Key 4	
AP MAC Address 4	

Object	Description
WDS Mode	Select Bridge Mode or Repeater Mode.
Phy Mode	It provides 4 options, including **CCK**, **OFDM**, **HTMIX**, and **GREENFIELD**.
Encryp Type	It provides 4 options, including **None**, **WEP**, **TKIP**, and **AES**.
AP MAC Address	It provides 4 AP MAC Address. Enter the MAC address of the other APs.

5.3.5 WPS

You can enable or disable the WPS function on this page.

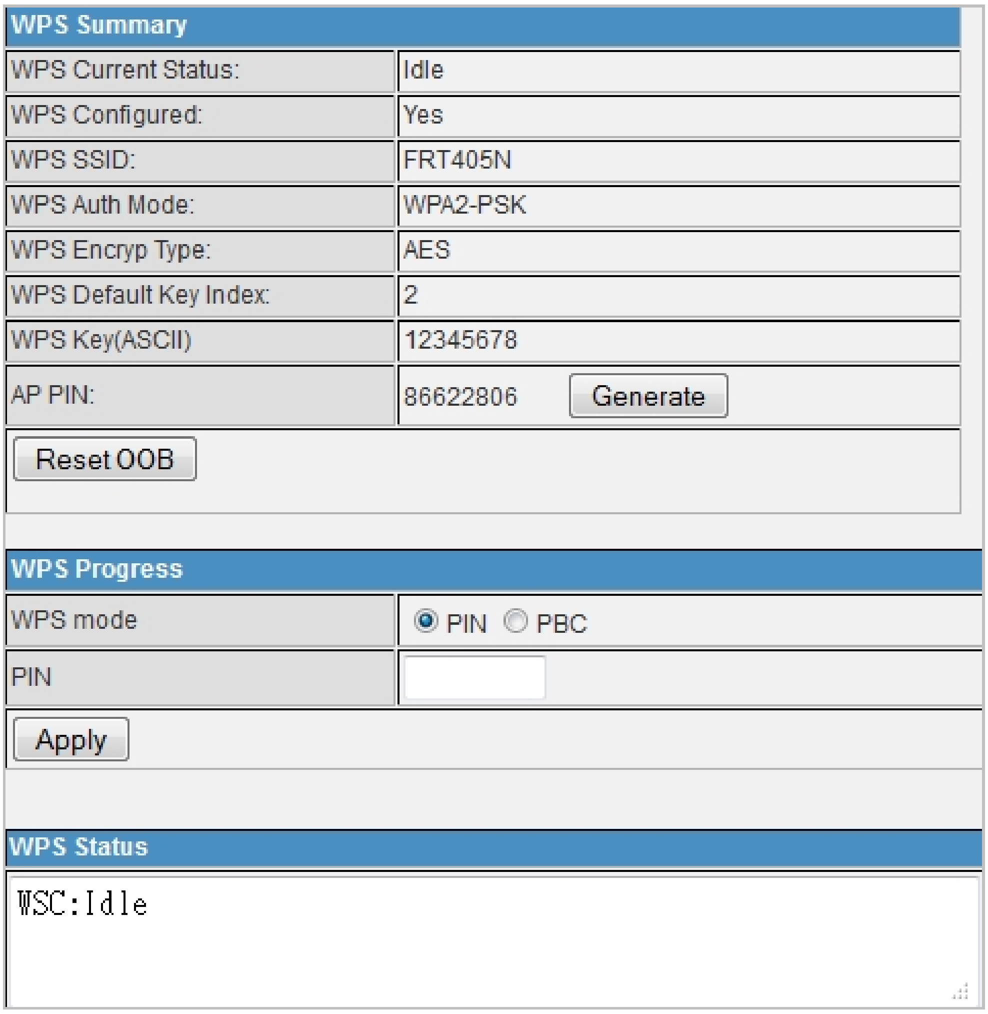


Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config	
WPS:	Disable Enable
Apply	

Select **Enable** in the WPS drop-down list. Click **Apply** and the following page appear.



WPS Summary	
WPS Current Status:	Idle
WPS Configured:	Yes
WPS SSID:	FRT405N
WPS Auth Mode:	WPA2-PSK
WPS Encryp Type:	AES
WPS Default Key Index:	2
WPS Key(ASCII)	12345678
AP PIN:	86622806 Generate
Reset OOB	

WPS Progress	
WPS mode	● PIN ○ PBC
PIN	
Apply	

WPS Status

```
WSC:Idle
```

WPS Summary

It displays the WPS information, such as WPS Current Status, WPS Configured, and WPS SSID.

Object	Description
Reset OOB	Reset to out of box (OoB) configuration

WPS Progress

There are two ways for you to enable WPS function: PIN or PBC. You can use a push button configuration (PBC) on the Wi-Fi router. If there is no button, enter 4 digit PIN code. Each STA supporting WPS comes with a hard-coded PIN code.

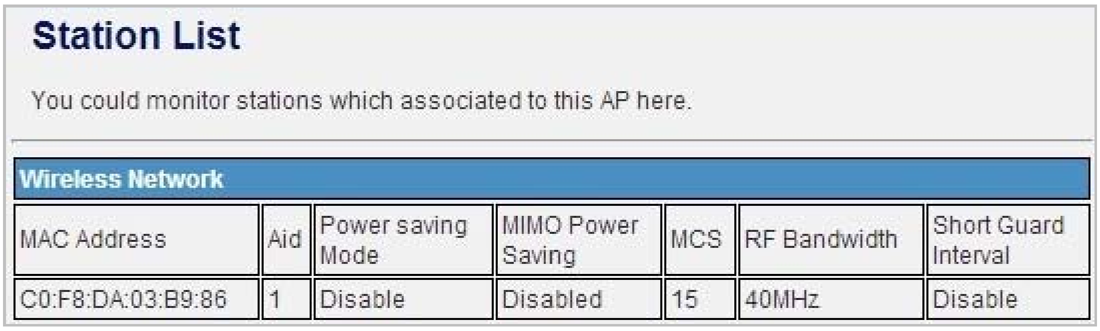
Object	Description
PIN	If you select PIN mode, you need to enter the PIN number in the field.

WPS Status

It displays the information about WPS status.

5.3.6 Station List

Through this page, you can easily identify the connected wireless stations. It automatically observes the ID of connected wireless station (if specified), MAC address, and current status.



Station List

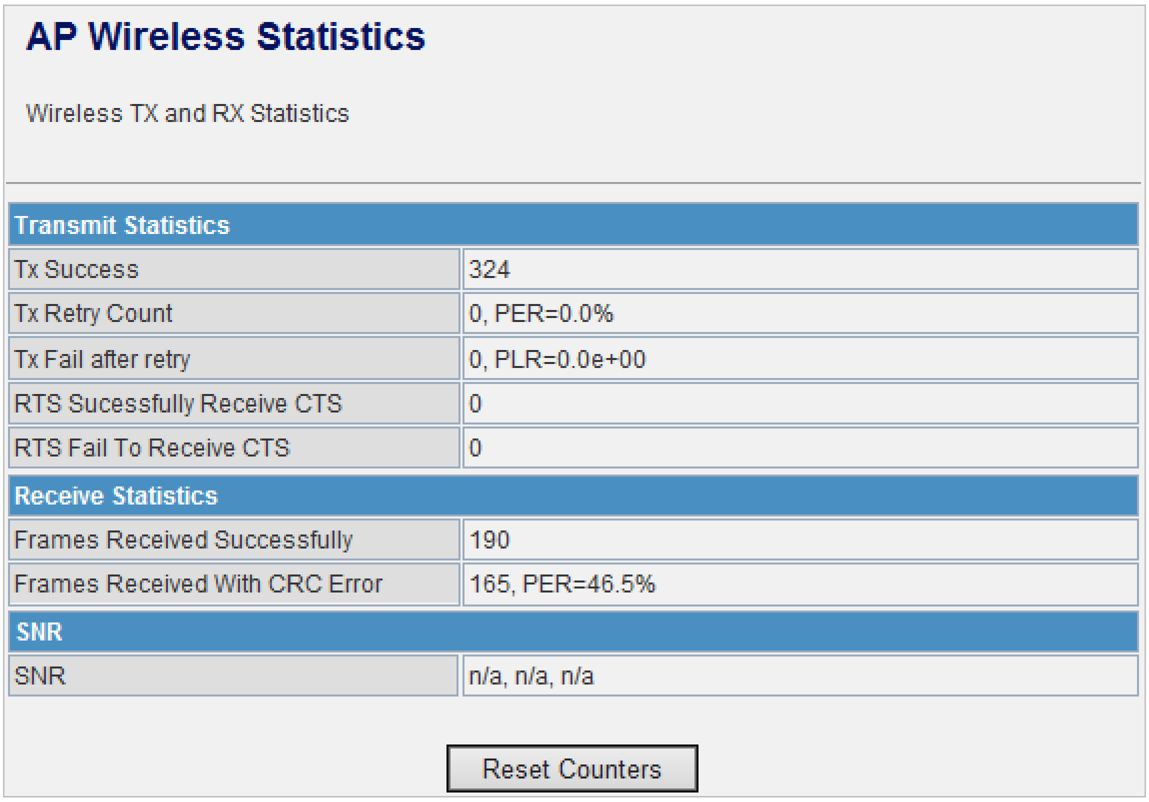
You could monitor stations which associated to this AP here.

Wireless Network

MAC Address	Aid	Power saving Mode	MIMO Power Saving	MCS	RF Bandwidth	Short Guard Interval
C0:F8:DA:03:B9:86	1	Disable	Disabled	15	40MHz	Disable

5.3.7 Statistics

This page will show you the connected TX, RX statistics.



AP Wireless Statistics

Wireless TX and RX Statistics

Transmit Statistics	
Tx Success	324
Tx Retry Count	0, PER=0.0%
Tx Fail after retry	0, PLR=0.0e+00
RTS Sucessfully Receive CTS	0
RTS Fail To Receive CTS	0
Receive Statistics	
Frames Received Successfully	190
Frames Received With CRC Error	165, PER=46.5%
SNR	
SNR	n/a, n/a, n/a

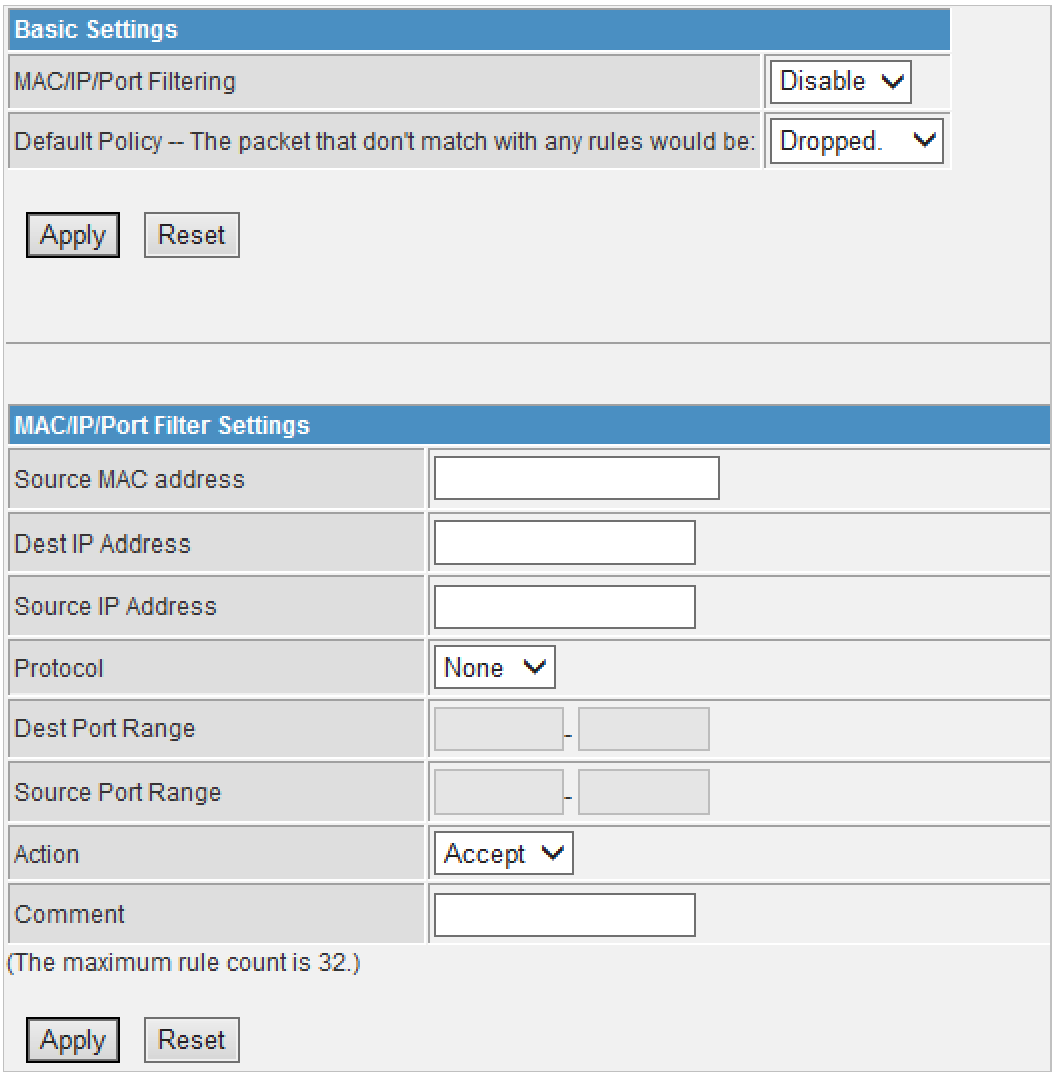
5.4 Firewall

The VDSL Router provides the fully firewall functions, such as MAC/IP/Port Filtering, Port Forwarding, DMZ, SPI Firewall and Content Filtering. It serves as an Internet firewall to protect your network from being accessed by outside users.

5.4.1 MAC/IP/Port Filtering

Use the MAC/IP/Port filters to deny / allow particular LAN IP addresses from accessing the Internet. You can deny / allow specific port numbers or all ports for a specific IP address.

You may set up firewall rules to protect your network from malicious activity on the Internet. It is also convenient for you to delete these settings.



Basic Settings

MAC/IP/Port Filtering	Disable
Default Policy -- The packet that don't match with any rules would be:	Dropped.

MAC/IP/Port Filter Settings

Source MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Accept
Comment	

(The maximum rule count is 32.)

Basic Settings

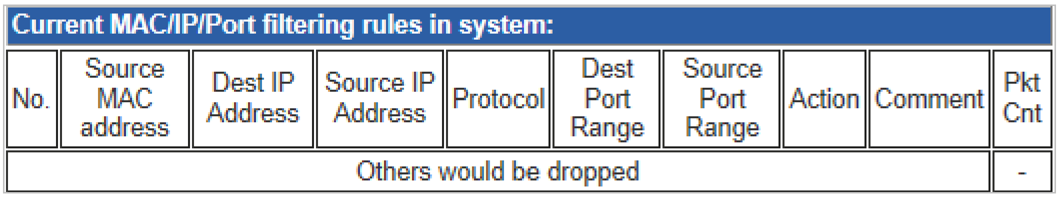
Object	Description
MAC/IP/Port Filtering	Enable or disable the MAC/IP/Port filtering function.
Default Policy	The Packet that does not match any rules would be dropped or accepted.

MAC/IP/Port Filter Settings

Object	Description
Source MAC address	Enter the MAC address that matches the source address of the packet (optional).
Dest IP Address	Enter the IP address that matches the destination address of the packet (optional).
Source IP Address	Enter the IP address that matches the source address of the packet (optional).
Protocol	There are 4 options, including none, TCP, UDP and ICMP.
Destination Port Range	After setting a valid protocol, you may enter the UPD or TCP destination port range.
Source Port Range	After setting a valid protocol, you may enter the UPD or TCP source port range.
Action	Select **Drop** or **Accept** in the drop down list.
Comment	Add description for this rule.

Note

The maximum rule number you can add is 32.



Current MAC/IP/Port filtering rules in system:

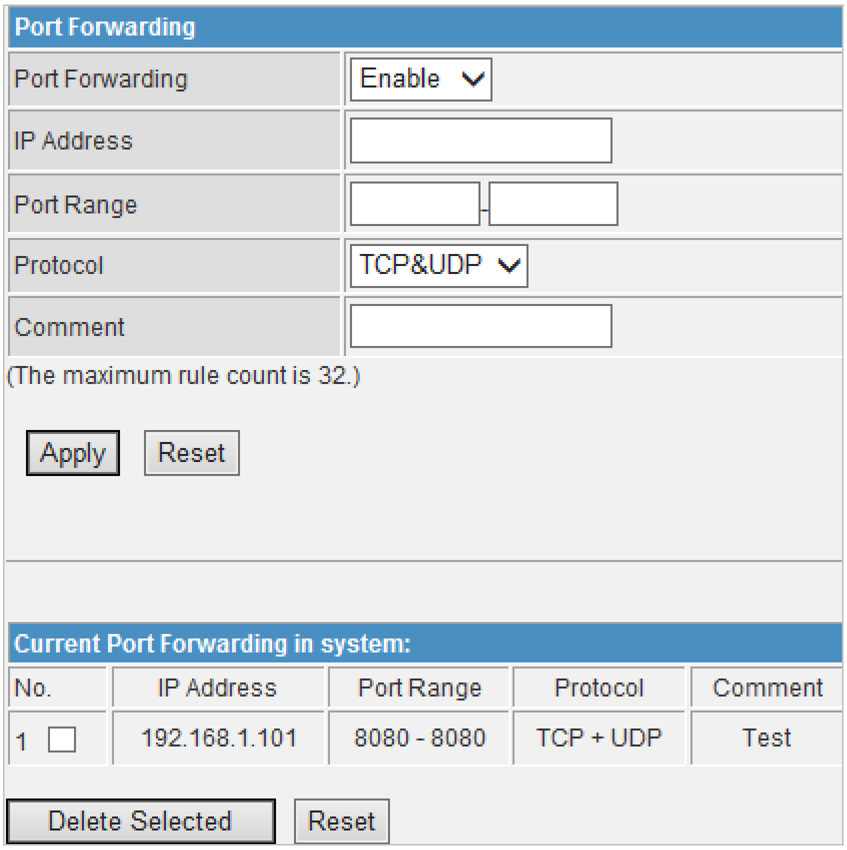
No.	Source MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Pkt Cnt
Others would be dropped									-

Current MAC/IP/Port Filtering Rules in System

If you want to delete some rules in the table above, select the rules, and then click **Delete Selected**. Otherwise, click **Reset**.

5.4.2 Port Forwarding (Virtual Server)

This page allows you to configure to re-direct a particular range of service port numbers from the Internet network to a particular LAN IP address, and set virtual server to provide services on the Internet.



Port Forwarding

Port Forwarding	Enable
IP Address	
Port Range	-
Protocol	TCP&UDP
Comment	

(The maximum rule count is 32.)

Current Port Forwarding in system:

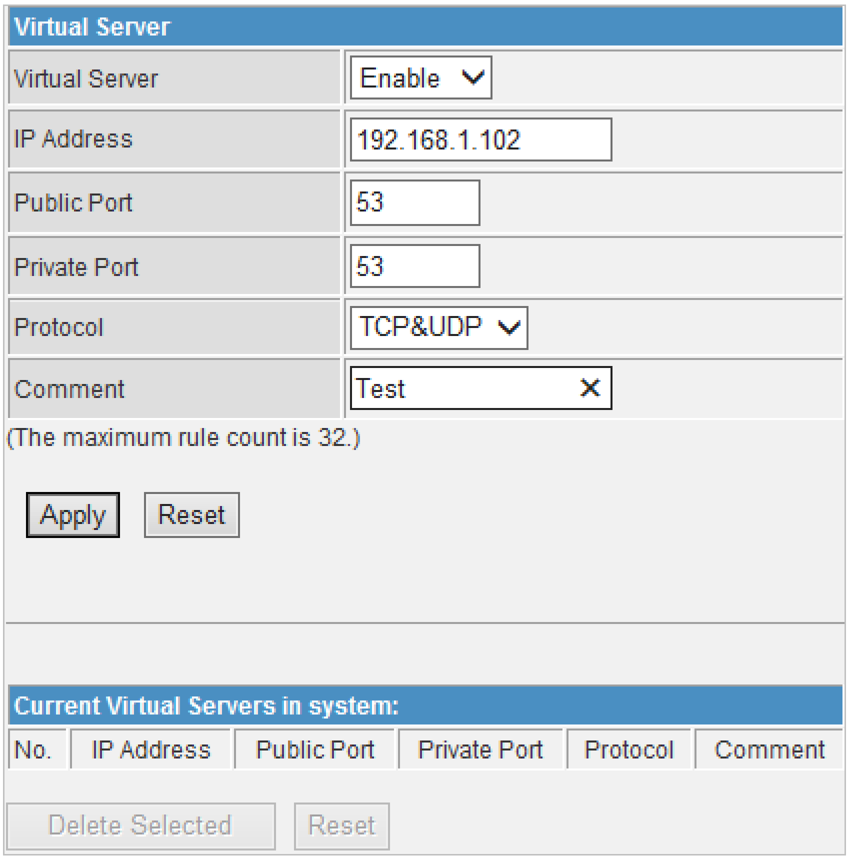
No.	IP Address	Port Range	Protocol	Comment
1 □	192.168.1.101	8080 - 8080	TCP + UDP	Test

Port Forwarding Settings

Object	Description
Virtual Server Settings	Enable or disable this function. After selecting **Enable**, you can set the following parameters.
IP Address	Enter the virtual server IP address in internal network.
Port Range:	You can setup your port range for your WAN side.
Protocol	There are 3 options, including none, TCP&UDP, TCP and UDP.
Comment	Add description for this rule.

Note

The maximum rule number you can add is 32.



Virtual Server

Virtual Server	Enable
IP Address	192.168.1.102
Public Port	53
Private Port	53
Protocol	TCP&UDP
Comment	Test

(The maximum rule count is 32.)

Current Virtual Servers in system:

No.	IP Address	Public Port	Private Port	Protocol	Comment

Virtual Server Settings

Object	Description
Virtual Server Settings	Enable or disable this function. After selecting **Enable**, you can set the following parameters.
IP Address	Enter the virtual server IP address in internal network.
Public Port	Enter the WAN service port.
Private Port	Enter the LAN service port.
Protocol	There are 3 options, including none, TCP&UDP, TCP and UDP.
Comment	Add description for this rule.

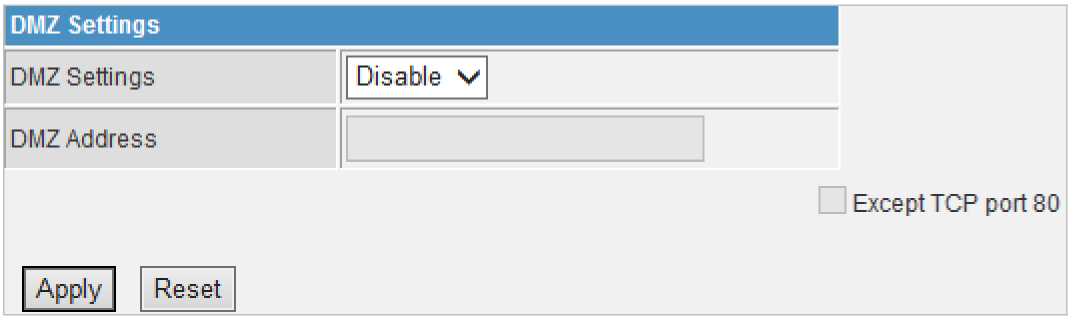
Note

The maximum rule number you can add is 32.

5.4.3 DMZ

DMZ (De-militarized Zone) allows a single computer on your LAN to expose ALL of its ports to the Internet. Enter the IP address of that computer as a DMZ (De-militarized Zone) host with unrestricted Internet access. When doing this, the DMZ host is no longer behind the firewall.

This page allows you to set a De-militarized Zone (DMZ) to separate internal network and Internet.



DMZ Settings

DMZ Settings	Disable
DMZ Address	

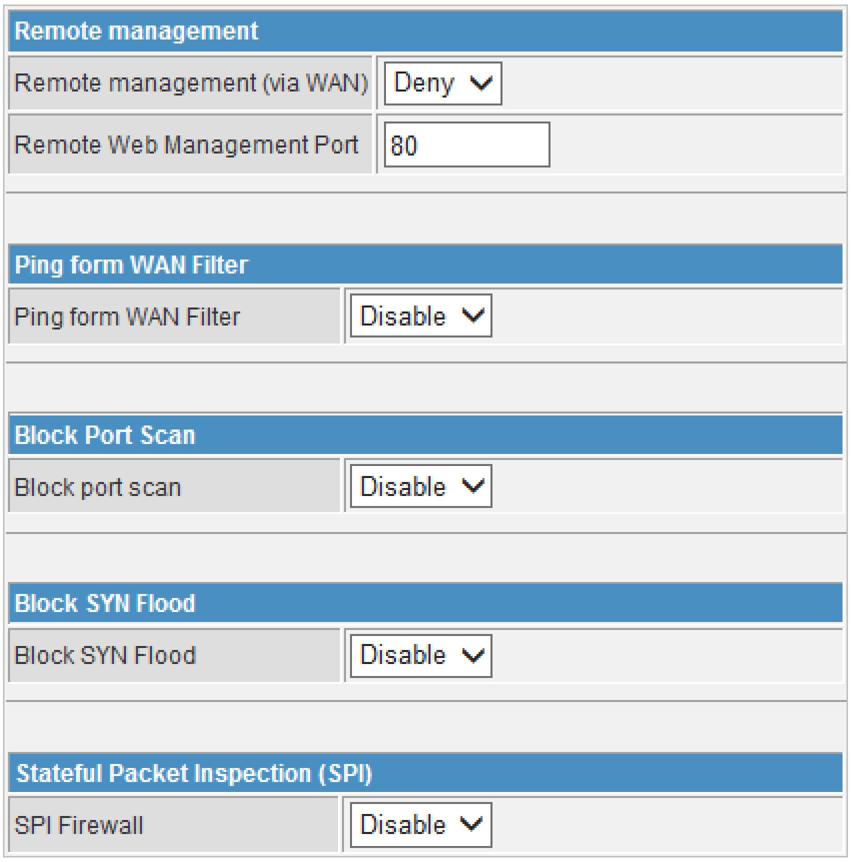
□ Except TCP port 80

DMZ Settings: Enable or disable this function. After selecting Enable, you can set the DMZ IP address.

DMZ IP Address: Enter the DMZ host IP address.

5.4.4 System Security Settings

Choose **Firewall > System Security** and the following page appears. This page allows you to configure the system firewall to protect Router from attacking.



Remote management

Remote management (via WAN): Deny

Remote Web Management Port: 80

Ping form WAN Filter

Ping form WAN Filter: Disable

Block Port Scan

Block port scan: Disable

Block SYN Flood

Block SYN Flood: Disable

Stateful Packet Inspection (SPI)

SPI Firewall: Disable

Remote Management

Object	Description
Remote management (via WAN)	Deny or allow remote management through web.
Remote Web management Port	The default remote management port is 80. You can change the remote management port for your needs. e.g. 8080.

Ping from WAN Filter

Object	Description
Ping from WAN Filter	You may select enable or disable to determine whether to filter the ping package which comes from the external network.

Block Port Scan

Object	Description
Block Port Scan	You may select enable or disable to determine whether to block the scanning which comes from the external network.

Block SYN Flood

Object	Description
Block SYN Flood	You may select enable or disable to determine whether to block the SYN Flood attacks come from the external network.

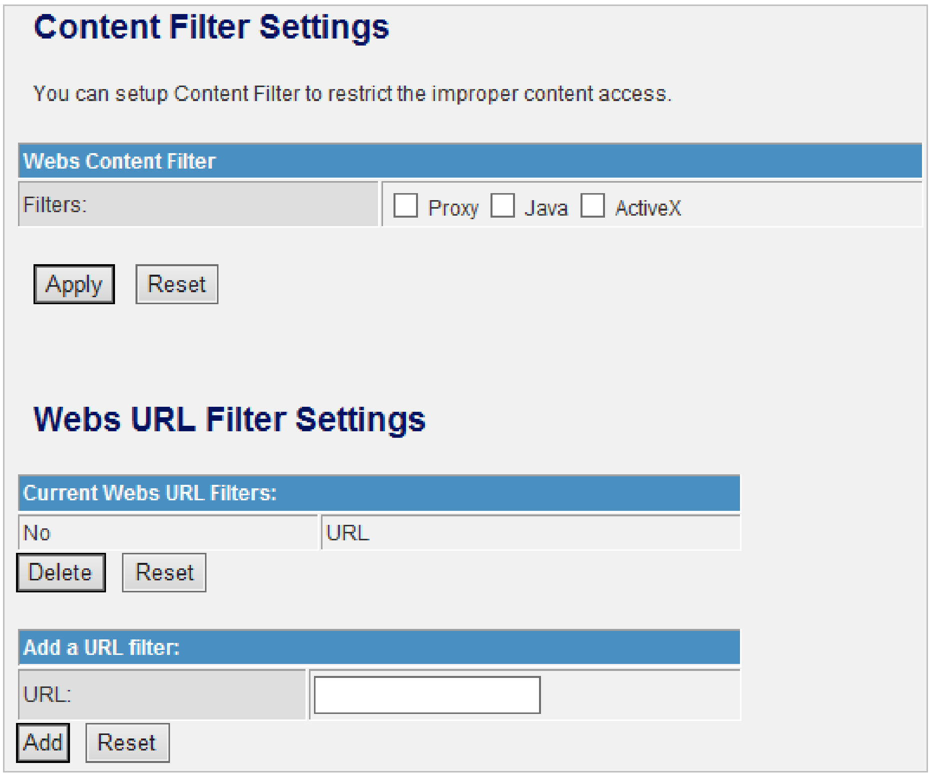
Stateful Packet Inspection (SPI)

Object	Description
SPI Firewall	You may disable or enable the SPI firewall.

5.4.5 Content Filtering

This page is used to configure the Blocked FQDN (Such as tw.yahoo.com) and filtered keyword. Here you can add / delete FQDN and filtered keyword.

Choose **Firewall > Content Filtering** and the following page appears. You can set content filter to restrict the improper content access.



Content Filter Settings

You can setup Content Filter to restrict the improper content access.

Webs Content Filter

Filters: □ Proxy □ Java □ ActiveX

Webs URL Filter Settings

Current Webs URL Filters:

No	URL

Add a URL filter:

URL:

Webs Content Filters

Object	Description
Webs Content Filters	If you want to block some applications as Proxy, Java and ActiveX of web pages please select the check box and click "Apply".

Current Webs URL Filters

Object	Description
Current Webs URL Filters	If you want to delete some filters in the table above, select the rules, and then click **Delete**. Otherwise, click **Reset**.

Add a URL filter

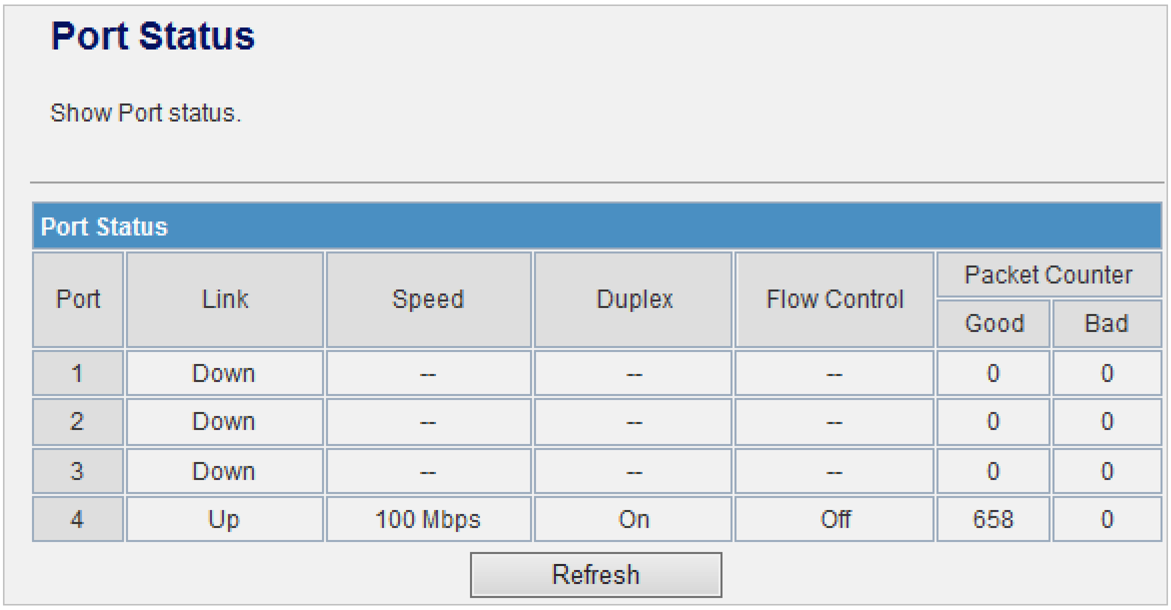
Object	Description
Add a URL filter	Enter the FQDN and click "Add" to apply this URL filter rule. Click **Add** to add a URL filter. Otherwise, click **Reset** to cancel the URL filter.

5.5 Layer 2 functions

A single layer-2 network may be partitioned to create multiple distinct broadcast domains. Such a domain is referred to as a Virtual LAN or VLAN. Network administrators set up VLANs to provide the segmentation services traditionally provided by routers in LAN configuration. This page allows you to set the VLAN.

5.5.1 Port Status

Choose **Layer 2 Function** > **Port Status** and the following page appears. This page displays each port's Speed, Duplex mode, Flow Control status.



Port Status

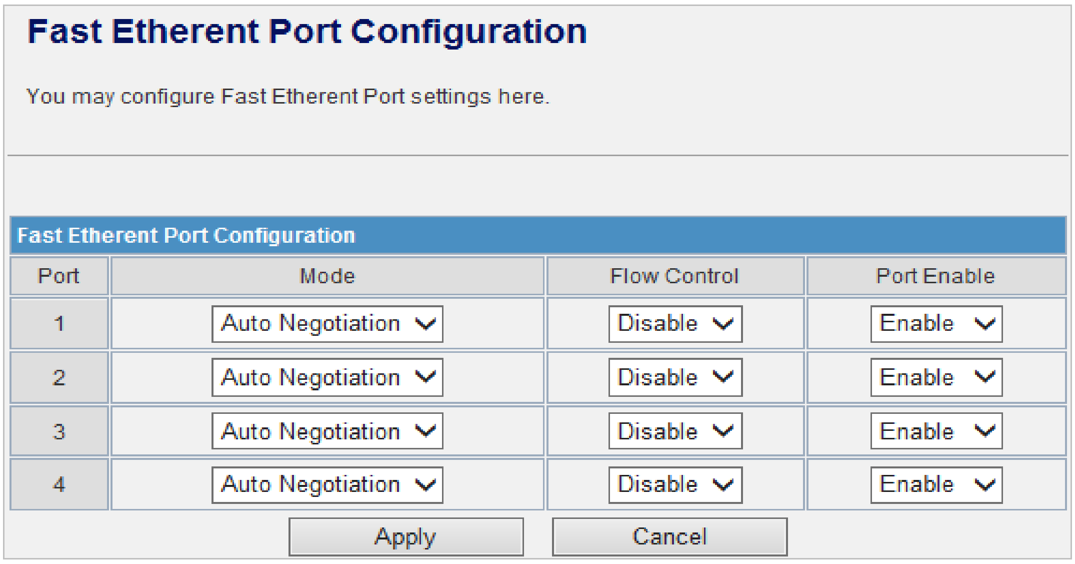
Show Port status.

Port Status

Port	Link	Speed	Duplex	Flow Control	Packet Counter	
					Good	Bad
1	Down	--	--	--	0	0
2	Down	--	--	--	0	0
3	Down	--	--	--	0	0
4	Up	100 Mbps	On	Off	658	0

5.5.2 Port Setting

This page allows you to select a different Mode, Flow Control or Port Enable.



Fast Etherent Port Configuration

You may configure Fast Etherent Port settings here.

Fast Etherent Port Configuration

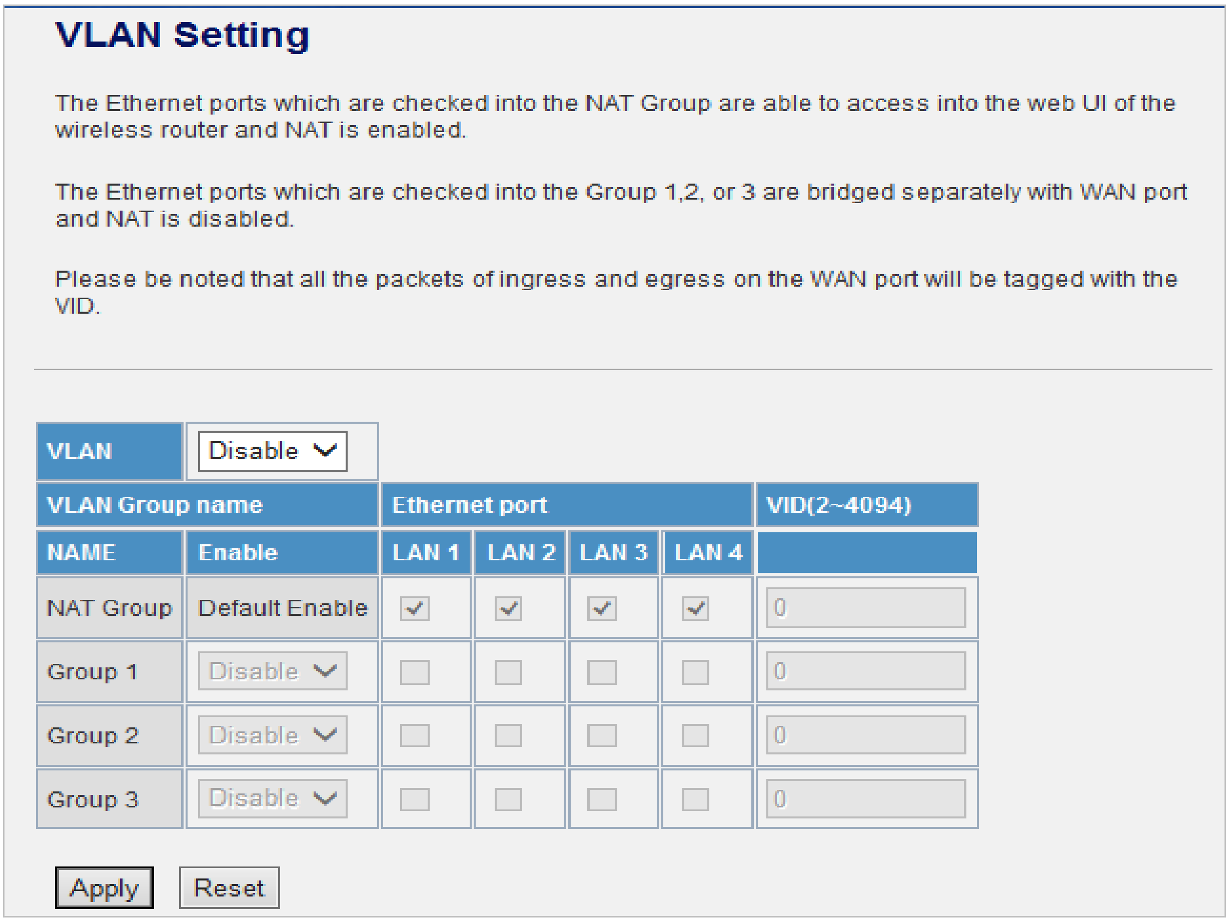
Port	Mode	Flow Control	Port Enable
1	Auto Negotiation	Disable	Enable
2	Auto Negotiation	Disable	Enable
3	Auto Negotiation	Disable	Enable
4	Auto Negotiation	Disable	Enable

The page includes the following fields:

Object	Description
Port	This is the LAN port number for this row.
Mode	You can choose 5 modes. ■ **Auto Negotiation** ■ **100 Full** ■ **100 Half** ■ **10 Full** ■ **10 Half** Please select the check box and click "**Apply**".
Flow Control	You can choose Enable or Disable.
Port Enable	You can choose Enable or Disable.

5.5.3 VLAN Setting

You can enable or disable the VLAN setting. There are four groups that can be set. The first one is NAT group and the others are bridged with WAN port.



VLAN Setting

The Ethernet ports which are checked into the NAT Group are able to access into the web UI of the wireless router and NAT is enabled.

The Ethernet ports which are checked into the Group 1,2, or 3 are bridged separately with WAN port and NAT is disabled.

Please be noted that all the packets of ingress and egress on the WAN port will be tagged with the VID.

VLAN	Disable

VLAN Group name		Ethernet port				VID(2~4094)
NAME	Enable	LAN 1	LAN 2	LAN 3	LAN 4	
NAT Group	Default Enable	☑	☑	☑	☑	0
Group 1	Disable	□	□	□	□	0
Group 2	Disable	□	□	□	□	0
Group 3	Disable	□	□	□	□	0

VLAN Mode Setting

- **Mode:** You can enable or disable the VLAN here.

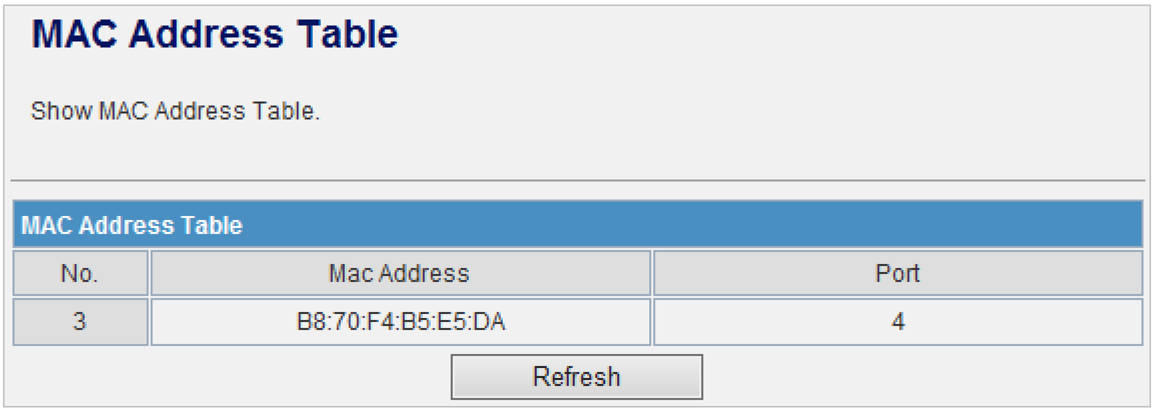
VLAN Member Configuration

Object	Description
VLAN Group:	You can select enable or disable.
VID:	Set the VID here for each Virtual LAN.
LAN1~4:	It means the LAN port on the router.
PVID:	You can set the PVID for each port here.

Click **Apply** to enable the configuration to take effect. Click **Cancel** to cancel the new configuration.

5.5.4 MAC Address Table

This page shows MAC Address Table.



MAC Address Table

Show MAC Address Table.

MAC Address Table		
No.	Mac Address	Port
3	B8:70:F4:B5:E5:DA	4

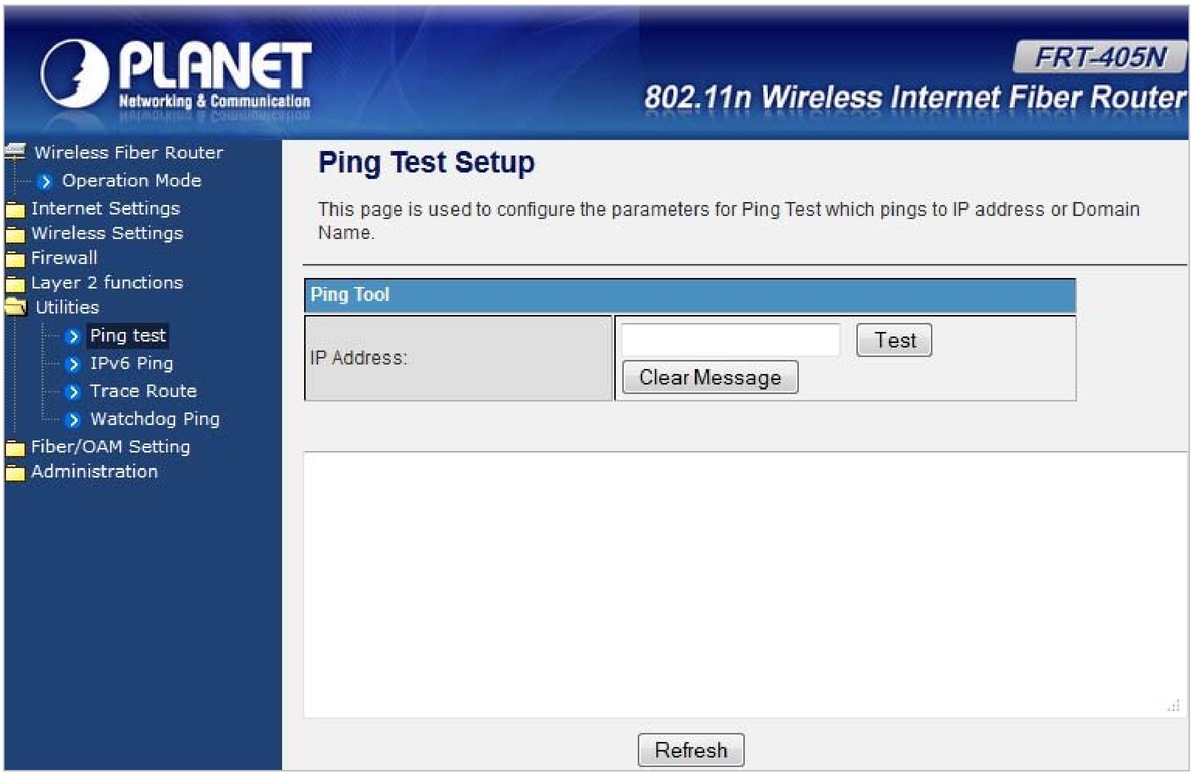
Click **Refresh** button to renew the list above immediately.

5.6 Utilities

The FRT-405N provides four functions for users to use.

5.6.1 Ping Test Setup

This page is used to configure the parameters for Ping Test which pings to IP address or Domain Name.



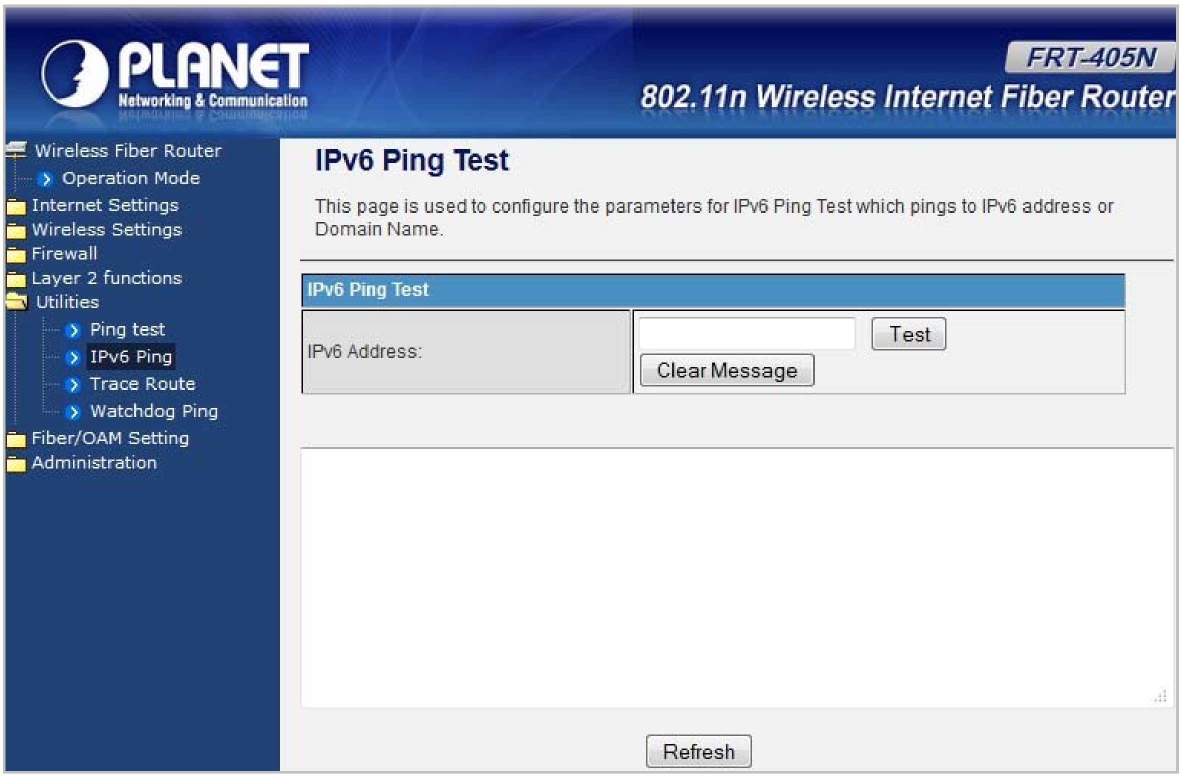
Ping Test Setup

This page is used to configure the parameters for Ping Test which pings to IP address or Domain Name.

Ping Tool	
IP Address:	

5.6.2 IPv6 Ping Test

This page is used to configure the parameters for IPv6 Ping Test which pings to IPv6 address or Domain Name.



IPv6 Ping Test

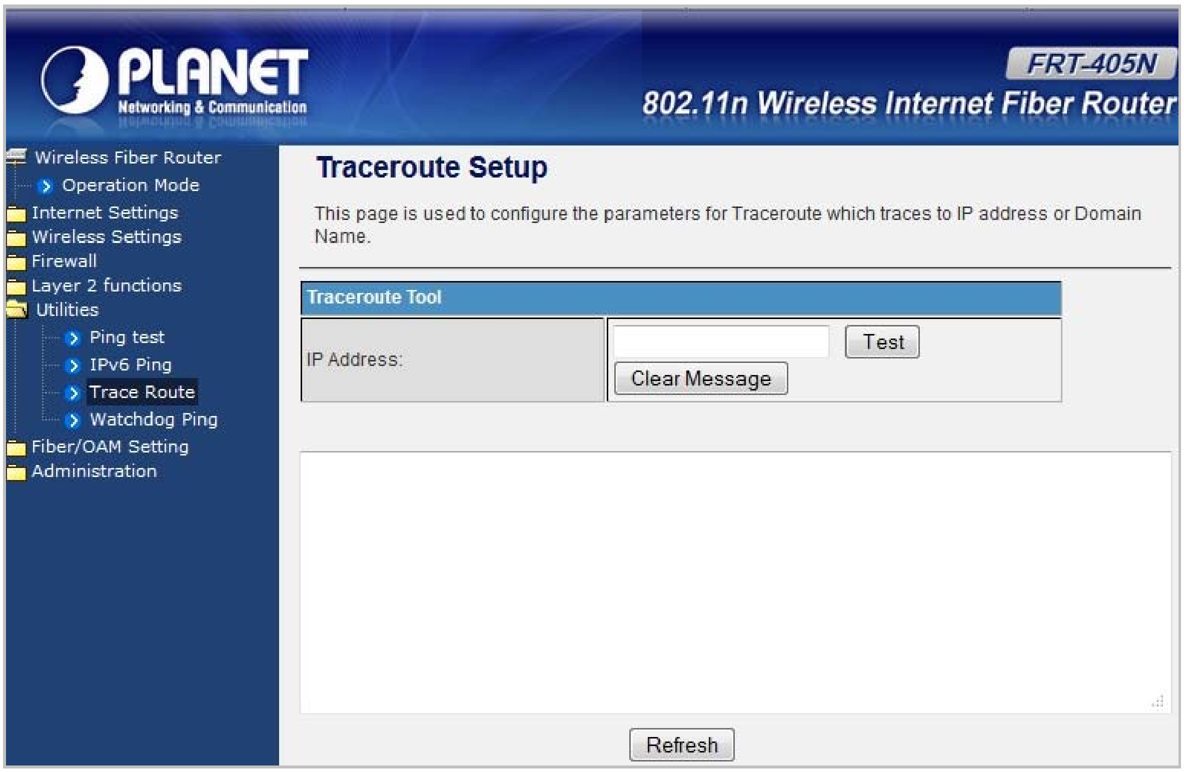
This page is used to configure the parameters for IPv6 Ping Test which pings to IPv6 address or Domain Name.

IPv6 Ping Test

IPv6 Address:

5.6.3 Trace Route

This page is used to configure the Traceroute which traces to IP address or Domain Name.



Traceroute Setup

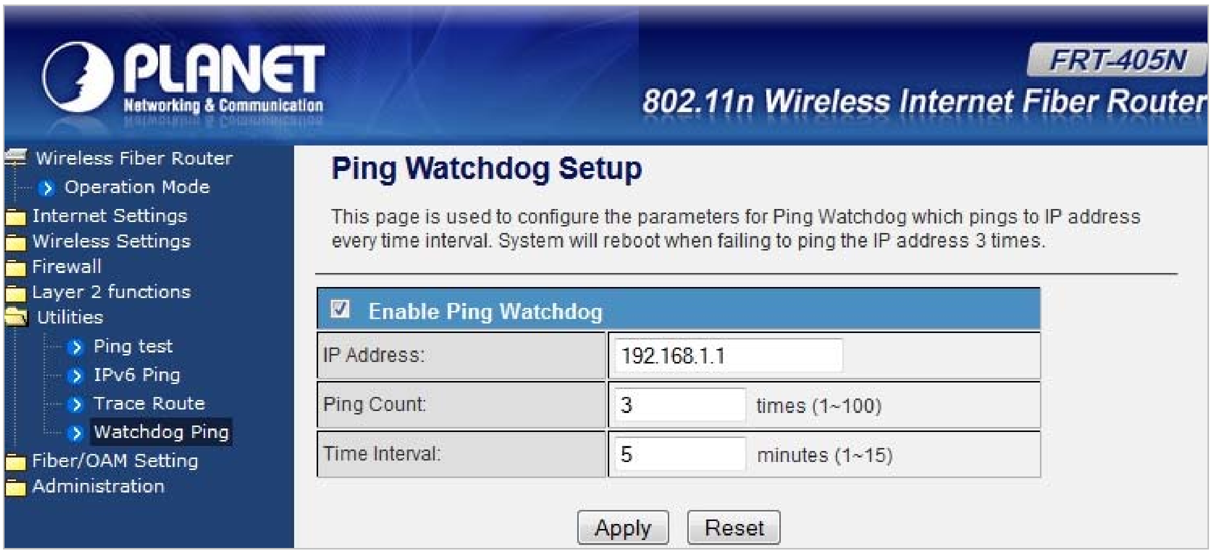
This page is used to configure the parameters for Traceroute which traces to IP address or Domain Name.

Traceroute Tool

IP Address:

5.6.4 Watch Dog Ping

On this page you can enable Ping Watchdog. And configure the parameters for Ping Watchdog which pings to IP address every time interval. System will reboot when failing to ping the IP address 3 times.



Ping Watchdog Setup

This page is used to configure the parameters for Ping Watchdog which pings to IP address every time interval. System will reboot when failing to ping the IP address 3 times.

☑ Enable Ping Watchdog

IP Address: 192.168.1.1

Ping Count: 3 times (1~100)

Time Interval: 5 minutes (1~15)

The page includes the following fields:

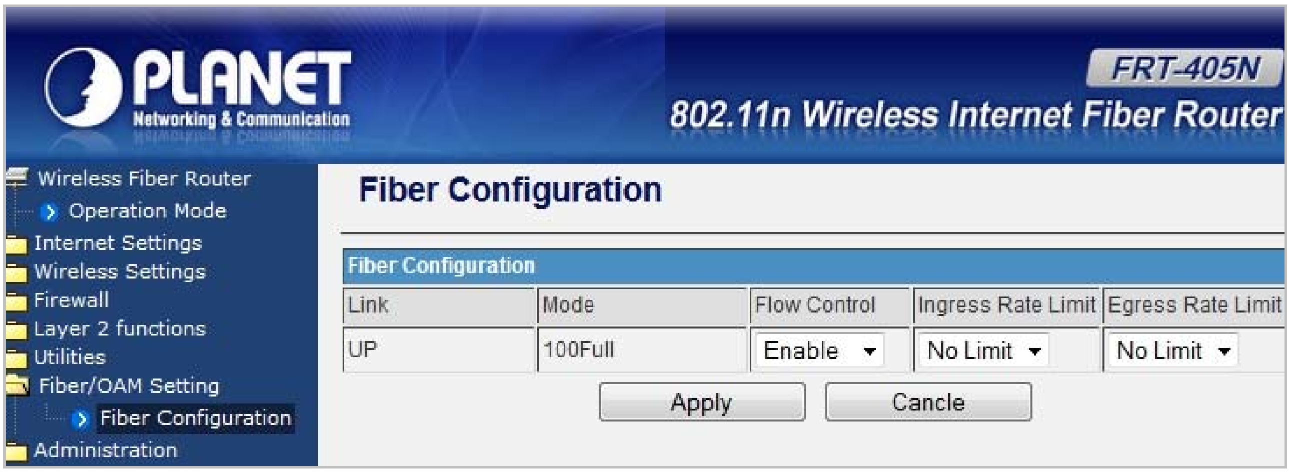
Object	Description
Ping Count	Set times from 1 to 100.
Time Interval	Set minutes from 1 to 15.

5.7 Fiber/OAM Setting

You can configure fiber setting in this part. It includes Flow Control, Ingress Rate Limit, Egress Rate Limit.

5.7.1 Fiber Configuration

Choose **Fiber/OAM Setting > Fiber Configuration,** and the following page appears. This function allows displaying the Fiber port status, Mode, Flow Control and Rate limit. The Link Status in the screen displays the current connection speed and duplex mode.



Fiber Configuration

Fiber Configuration

Link	Mode	Flow Control	Ingress Rate Limit	Egress Rate Limit
UP	100Full	Enable	No Limit	No Limit

Fiber Configuration

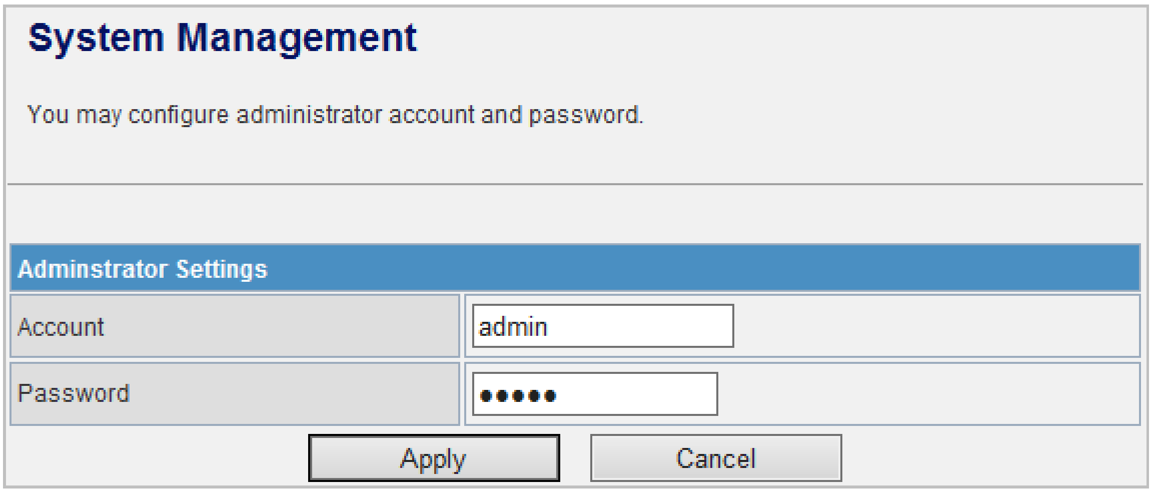
Object	Description
Link	Display the Link situation.
Mode	Display the network speed.
Flow Control	Enable or Disable Flow Control function. ■ Enable: 802.3x flow control is enabled on Full-Duplex mode or Half-Duplex mode ■ Disable: No flow control function.
Ingress Rate Limit	The value of inbound traffic limitation. Set the Ingress Rate Limit to **No Limit**, **512K**, **1M**, **2M**, **4M**, **8M**, **10M**, **50M**
Egress Rate Limit	The value of outbound traffic limitation. Set the Egress Rate Limit to **No Limit**, **512K**, **1M**, **2M**, **4M**, **8M**, **10M**, **50M**

5.8 Administration

You can configure admin management in this part. It includes Management, Update Firmware, Setting Management, Reboot, Status, Statistics and System Log.

5.8.1 Management

Choose **Administration > Management,** and the following page appears. You may configure administrator account and password on the page.



System Management

You may configure administrator account and password.

Adminstrator Settings

Account	admin
Password	●●●●●

Administrator Settings

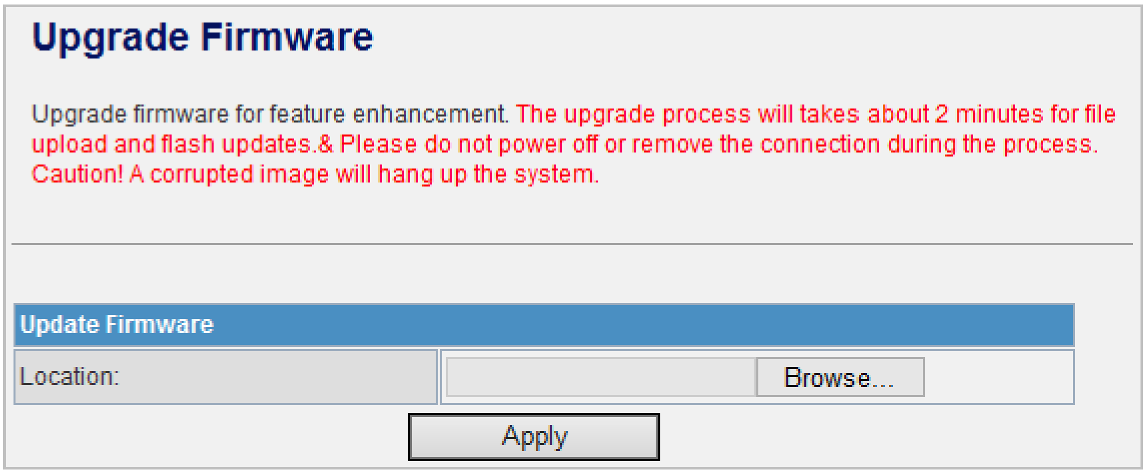
Object	Description
Account	Enter the user name of the administrator in the field.
Password	Enter the user name of the administrator in the field.

5.8.2 Uploading Firmware

Choose **Administration > Upload Firmware** and the following page appears. On this page, you may upgrade the correct new version firmware to obtain new functionality. It takes about 2 minutes to upload and upgrade the flash.

Note

If the firmware is uploaded in an improper way, the system would core dump.



Upgrade Firmware

Upgrade firmware for feature enhancement. The upgrade process will takes about 2 minutes for file upload and flash updates.& Please do not power off or remove the connection during the process. Caution! A corrupted image will hang up the system.

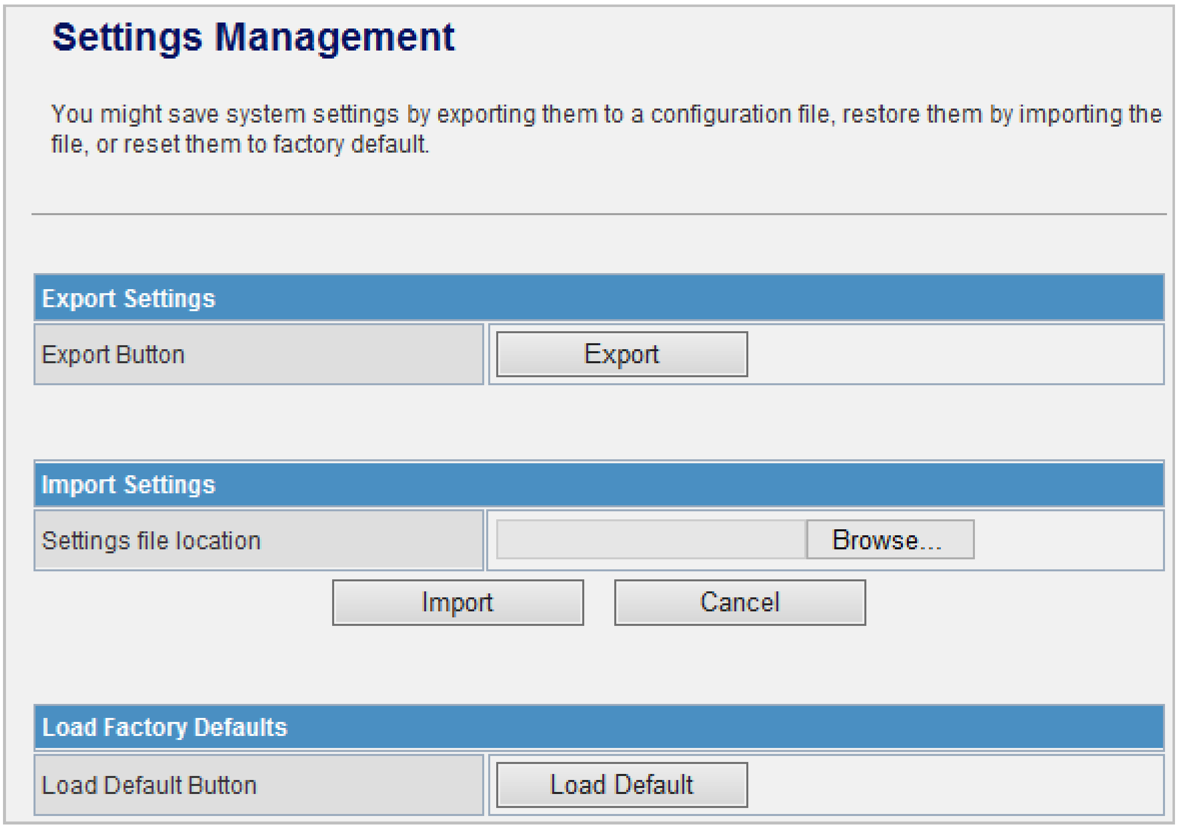
Update Firmware	
Location:	Browse...

Updating Firmware

Object	Description
Location	Click **Browse** to select the firmware file, and click **Apply** to upgrade the firmware.

5.8.3 Setting Management

Choose **Administration > Settings Management** and the following page appears. You may save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to the factory default.



Settings Management

You might save system settings by exporting them to a configuration file, restore them by importing the file, or reset them to factory default.

Export Settings	
Export Button	Export

Import Settings	
Settings file location	Browse...

Load Factory Defaults	
Load Default Button	Load Default

Exporting Settings

Object	Description
Export Button	Click the **Export** to export the settings

Importing Settings

Object	Description
Import Settings	Click **Browse** to select the configuration file, and then click
Import	Upload the configuration file. Click **Cancel** to cancel the uploading operation.

Loading Factory Defaults

Object	Description
Load Default	Click **Load Default** to make Router return to the default settings.

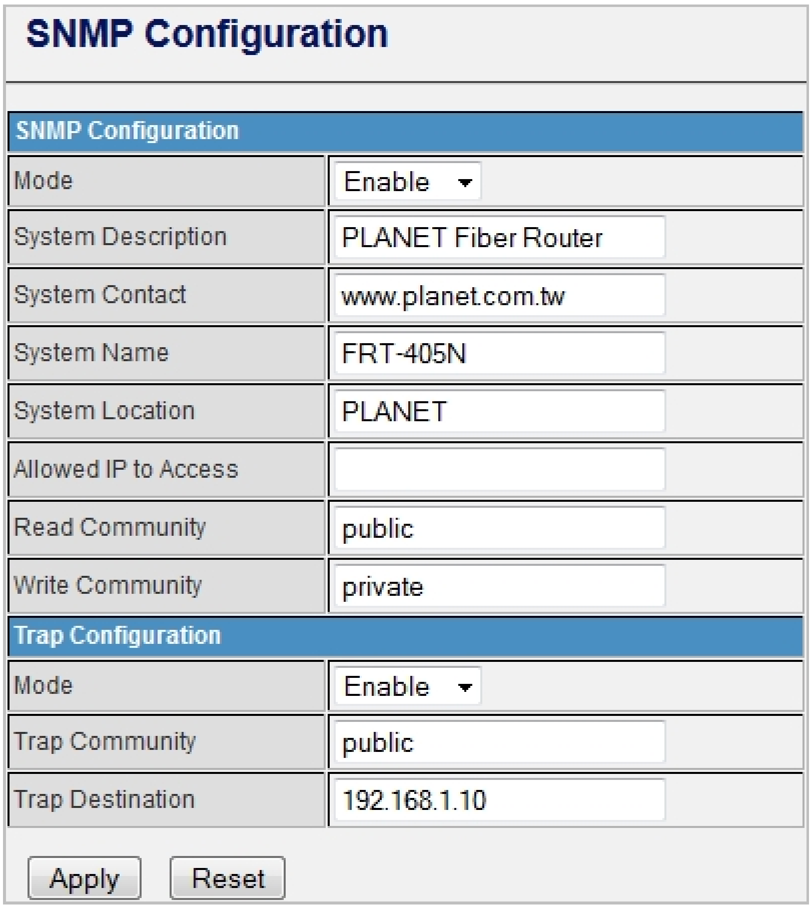
5.8.4 SNMP Configuration

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is widely used in local area networks (LAN) for collecting information, and managing and monitoring, network devices, such as servers, printers, hubs, switches, and routers from a management host.

Managed devices that support SNMP including software are referred to as an SNMP agent, which usually interacts with third-party SNMP management software to enable the sharing of network status information between monitored devices and applications and the SNMP management system.

A defined collection of variables (managed objects) are maintained by the SNMP agent and used to manage the device. These objects are defined in a **Management Information Base (MIB)**, which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

Choose **Administration > SNMP configuration** and the following page appears. You may enable SNMP Configuration and Trap Configuration settings.



SNMP Configuration

SNMP Configuration	
Mode	Enable
System Description	PLANET Fiber Router
System Contact	www.planet.com.tw
System Name	FRT-405N
System Location	PLANET
Allowed IP to Access	
Read Community	public
Write Community	private
Trap Configuration	
Mode	Enable
Trap Community	public
Trap Destination	192.168.1.10

The page includes the following fields:

SNMP Configuration

Object	Description
Mode	Indicates the SNMP mode operation. Possible modes are: ■ **Enabled**: Enable SNMP mode operation. ■ **Disabled**: Disable SNMP mode operation.
System Description	Describe the model of the device.
System Contact:	Set the name to access the router. Usually set the administrator's name.
System Name:	Set the router's name, such as "**FRT-405N**".
System Location:	Set the router's network location.
Allowed IP to access	Show you the IP that allowed to access.
Read Community:	Indicates the community read access string to permit reading this router's SNMP information.

	The default is **Public**.
Write Community:	Indicates the community write access string to permit reading and re-writing this router's SNMP information. The default is **Private**.

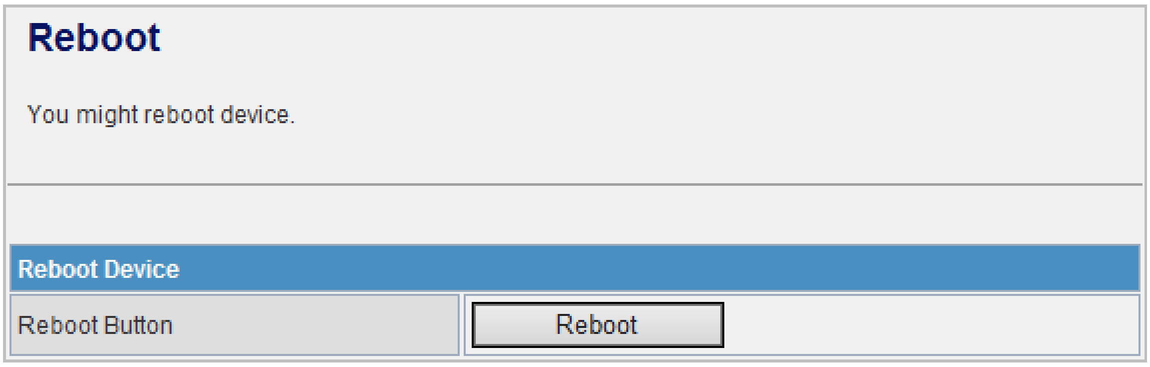
Trap Configuration

Object	Description
Mode :	Indicates the SNMP trap mode operation. Possible modes are: ■ **Enabled**: Enable SNMP trap mode operation. ■ **Disabled**: Disable SNMP trap mode operation.
Trap Community:	Enter the community string for the trap station.
Trap Destination :	Enter the IP address of the trap manager.

Click **Apply** to enable the configuration to take effect. Click **Reset** button to reset the whole configuration to default.

5.8.5 Reboot

The **Reboot** screen allows you to restart your router with its current settings. Click the "Reboot" button and the device will restart.



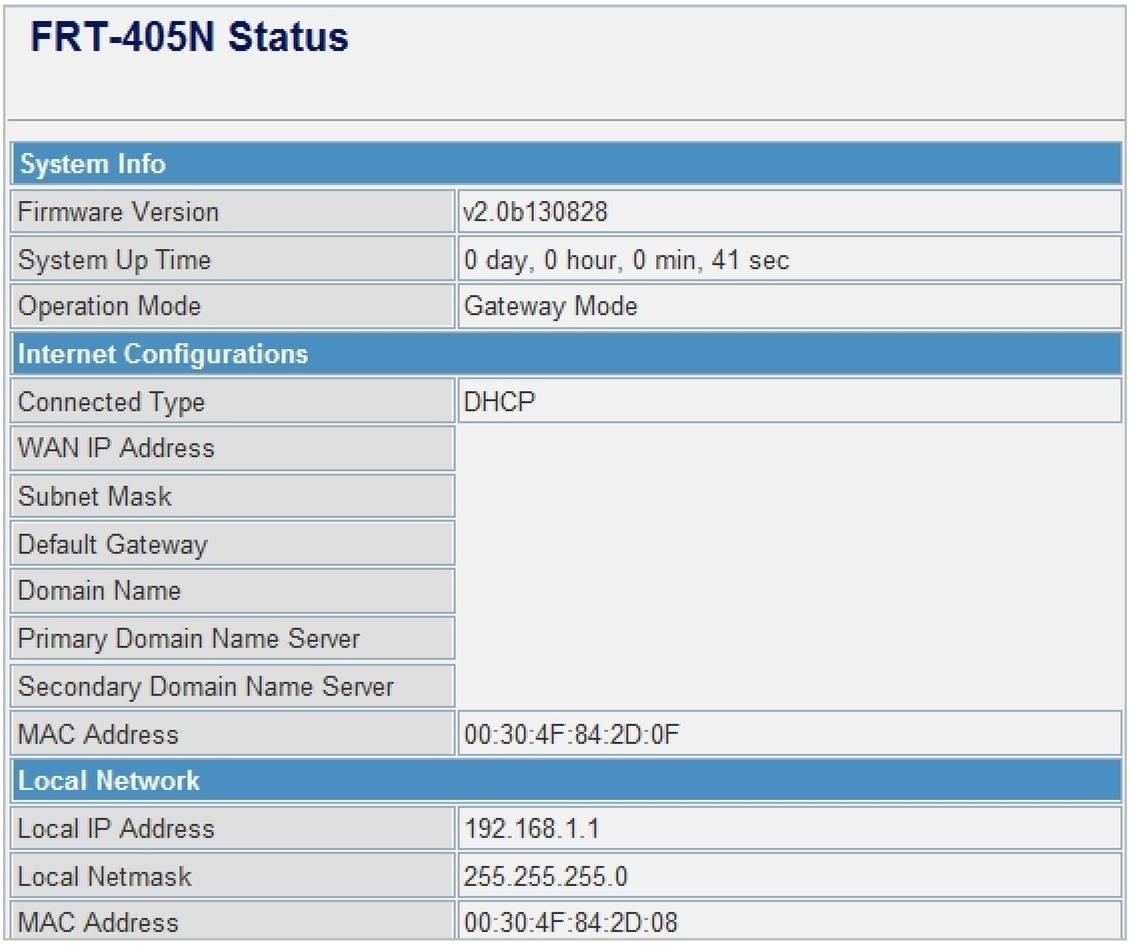
Reboot

You might reboot device.

Reboot Device	
Reboot Button	Reboot

5.8.6 Status

Choose **Administration > Status** and the following page appears. It displays the information about Router status, including system information, Internet configurations, and local network.

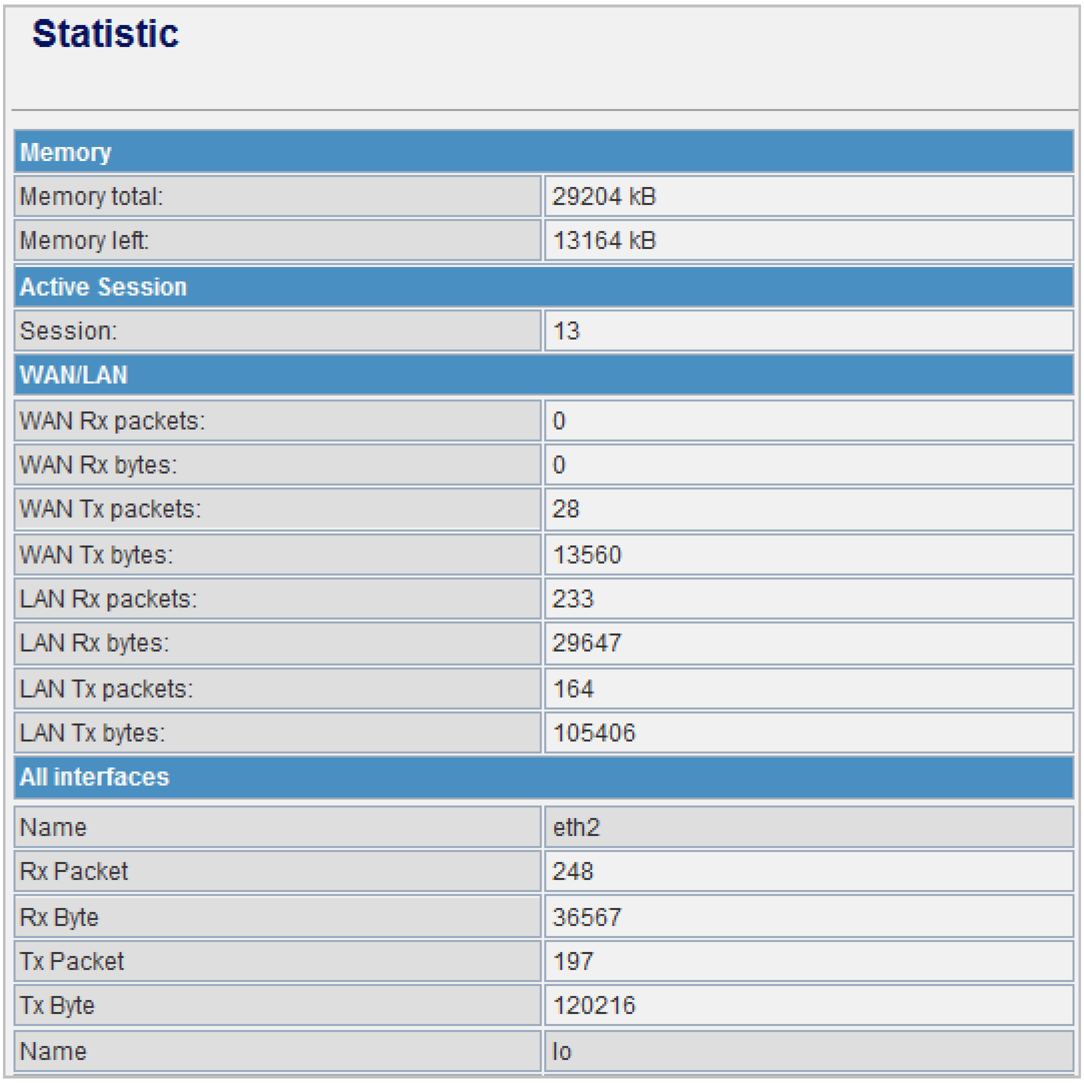


FRT-405N Status

System Info	
Firmware Version	v2.0b130828
System Up Time	0 day, 0 hour, 0 min, 41 sec
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	DHCP
WAN IP Address	
Subnet Mask	
Default Gateway	
Domain Name	
Primary Domain Name Server	
Secondary Domain Name Server	
MAC Address	00:30:4F:84:2D:0F
Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:30:4F:84:2D:08

5.8.7 Statistics

You can see the Statistic information on this screen. It includes the Traffic for all interfaces.

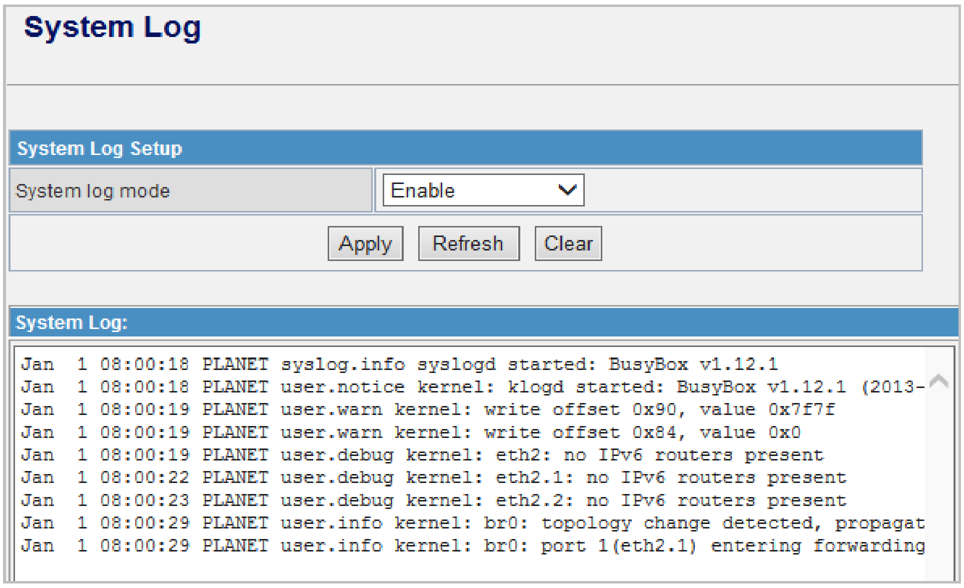


Statistic

Memory	
Memory total:	29204 kB
Memory left:	13164 kB
Active Session	
Session:	13
WAN/LAN	
WAN Rx packets:	0
WAN Rx bytes:	0
WAN Tx packets:	28
WAN Tx bytes:	13560
LAN Rx packets:	233
LAN Rx bytes:	29647
LAN Tx packets:	164
LAN Tx bytes:	105406
All interfaces	
Name	eth2
Rx Packet	248
Rx Byte	36567
Tx Packet	197
Tx Byte	120216
Name	lo

5.8.8 System Log

The system log dialog allows you to view the system log and click the “Refresh” button to refresh the system event logs. Choose **Administration > System Log** and the following page appears. You are allowed to view and disable / enable the system log on this page.



System Log

System Log Setup

System log mode	Enable

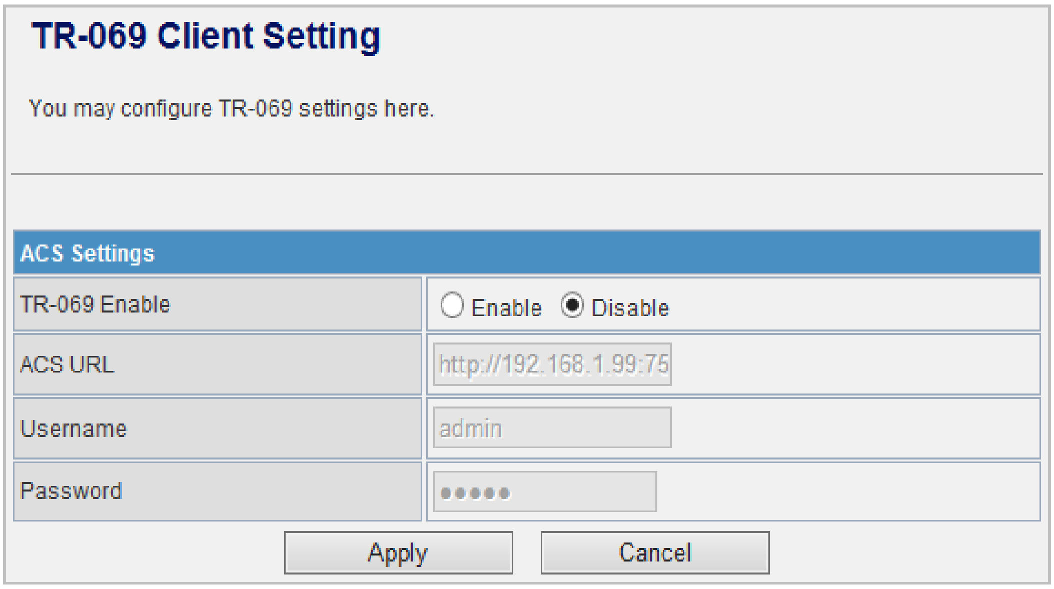
System Log:

```
Jan  1 08:00:18 PLANET syslog.info syslogd started: BusyBox v1.12.1
Jan  1 08:00:18 PLANET user.notice kernel: klogd started: BusyBox v1.12.1 (2013-
Jan  1 08:00:19 PLANET user.warn kernel: write offset 0x90, value 0x7f7f
Jan  1 08:00:19 PLANET user.warn kernel: write offset 0x84, value 0x0
Jan  1 08:00:19 PLANET user.debug kernel: eth2: no IPv6 routers present
Jan  1 08:00:22 PLANET user.debug kernel: eth2.1: no IPv6 routers present
Jan  1 08:00:23 PLANET user.debug kernel: eth2.2: no IPv6 routers present
Jan  1 08:00:29 PLANET user.info kernel: br0: topology change detected, propagat
Jan  1 08:00:29 PLANET user.info kernel: br0: port 1(eth2.1) entering forwarding
```

Click **Refresh** to refresh the log. Click **Clear** to clear the log.

5.8.9 TR-069 Client

Choose **Administration > TR-069 Client** and the following page appears. You are allowed to disable or enable the function on this page.



TR-069 Client Setting

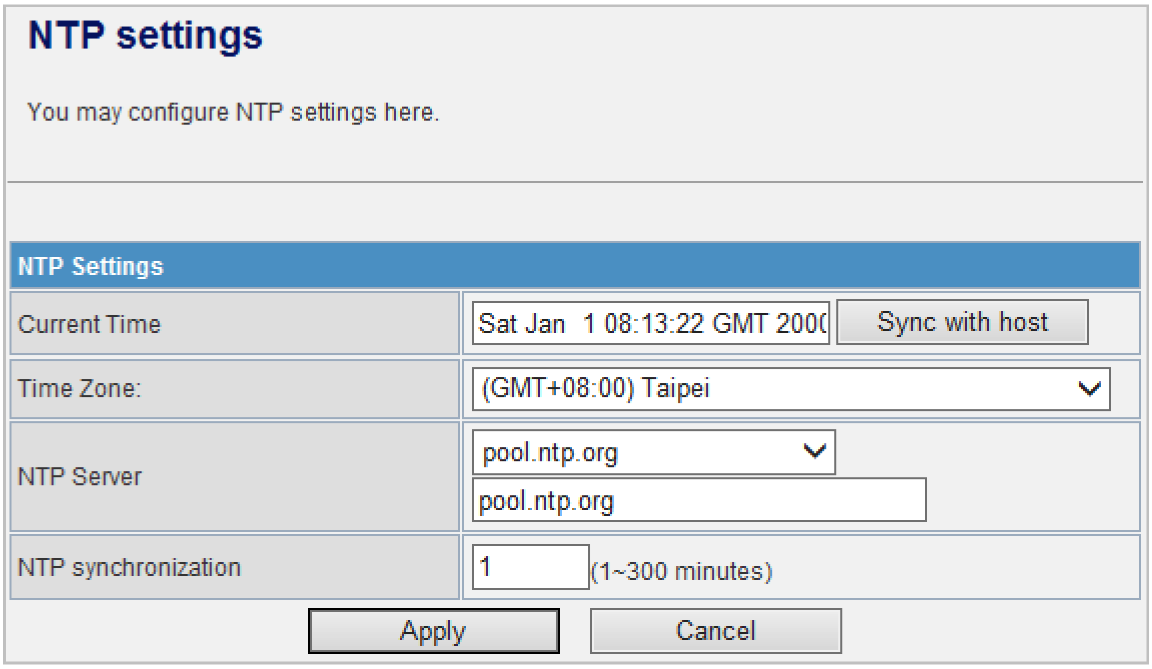
You may configure TR-069 settings here.

ACS Settings

TR-069 Enable	○ Enable ● Disable
ACS URL	http://192.168.1.99:75
Username	admin
Password	●●●●●

5.8.10 NTP

Choose **Administration > NTP** and the following page appears. You may configure NTP settings on this page.



NTP settings

You may configure NTP settings here.

NTP Settings	
Current Time	Sat Jan 1 08:13:22 GMT 200(
Time Zone:	(GMT+08:00) Taipei
NTP Server	pool.ntp.org pool.ntp.org
NTP synchronization	1 (1~300 minutes)

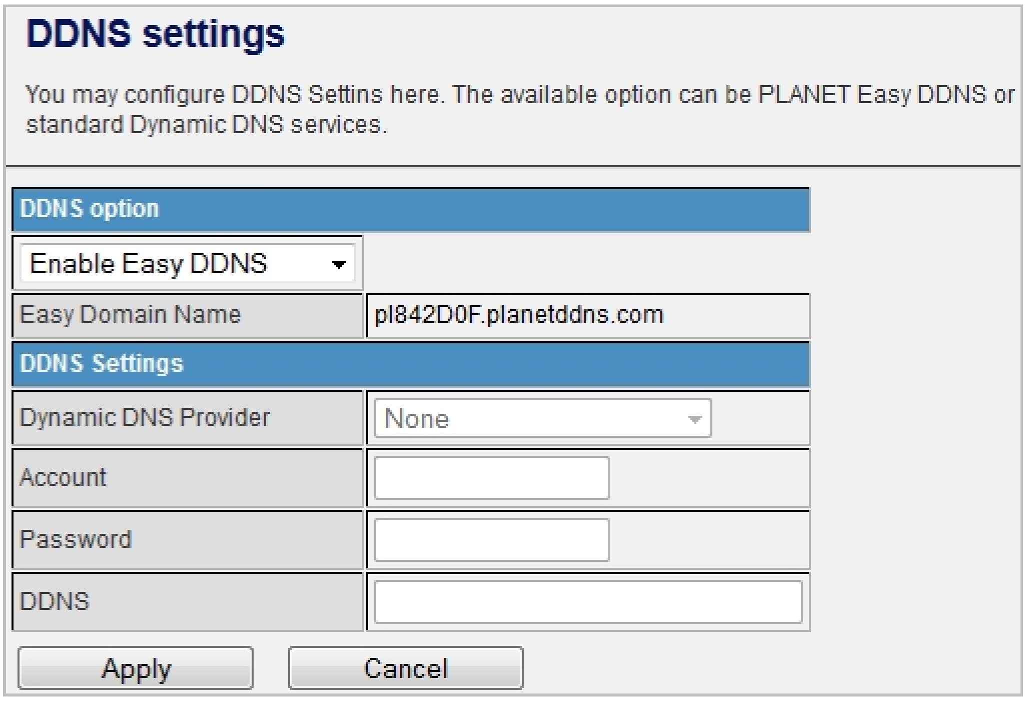
NTP Settings

Object	Description
Current Time	Display the current date and time. Click **Sync with host**, the current time is synchronized by your PC which is connected to Router.
Time Zone	Select the proper time zone in the drop-down list.
NTP Server	Enter the IP address or domain name of NTP server.
NTP synchronization	Enter the time interval for synchronization. From 1 to 300 minutes.

5.8.11 DDNS

The Wireless Router offers the **DDNS** (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as PLANET DDNS or dynamic DNS. The Dynamic DNS client service provider will give you a password or key.

Choose **Administration > DDNS** and the following page appears. You can choose Disable, Enable Easy DDNS and Dynamic DDNS settings on this page.



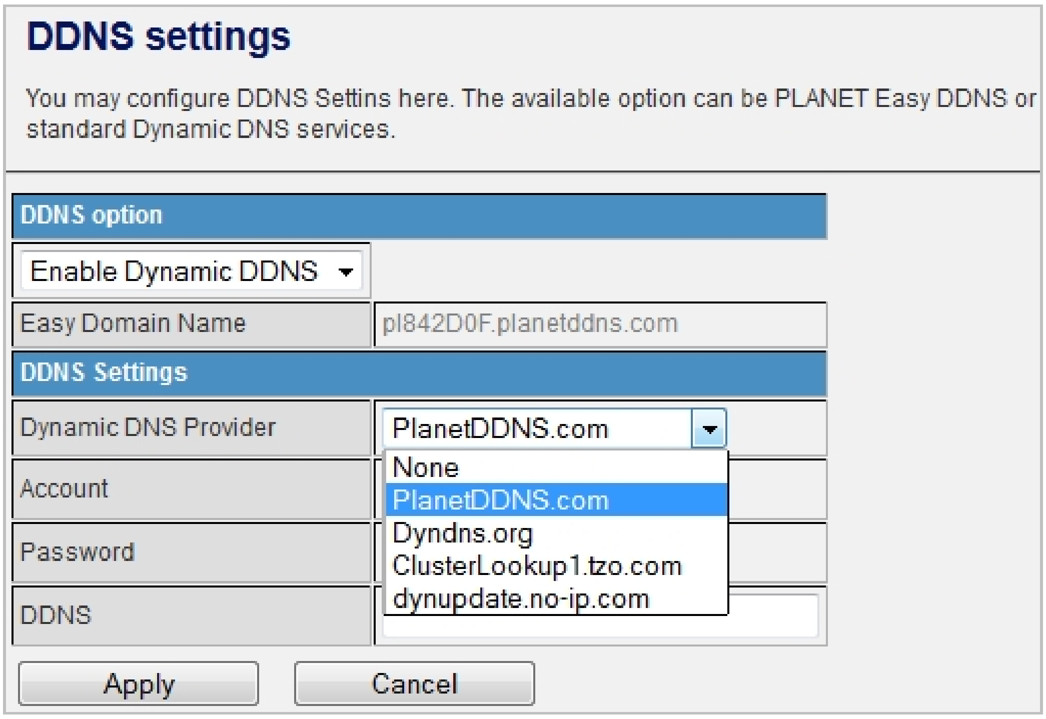
DDNS settings

You may configure DDNS Settins here. The available option can be PLANET Easy DDNS or standard Dynamic DNS services.

DDNS option	
Enable Easy DDNS ▾	
Easy Domain Name	pl842D0F.planetddns.com
DDNS Settings	
Dynamic DNS Provider	None ▾
Account	
Password	
DDNS	

Easy DDNS

Planet Easy DDNS is a way help to get your Domain Name with just one click. Once you enabled the Easy DDNS, your Planet Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the web page or bottom label of the device. (For example, 00-30-4F-12-34-07, it will be converted into PL123407.planetddns.com)



DDNS settings

You may configure DDNS Settins here. The available option can be PLANET Easy DDNS or standard Dynamic DNS services.

DDNS option

Enable Dynamic DDNS

Easy Domain Name: pl842D0F.planetddns.com

DDNS Settings

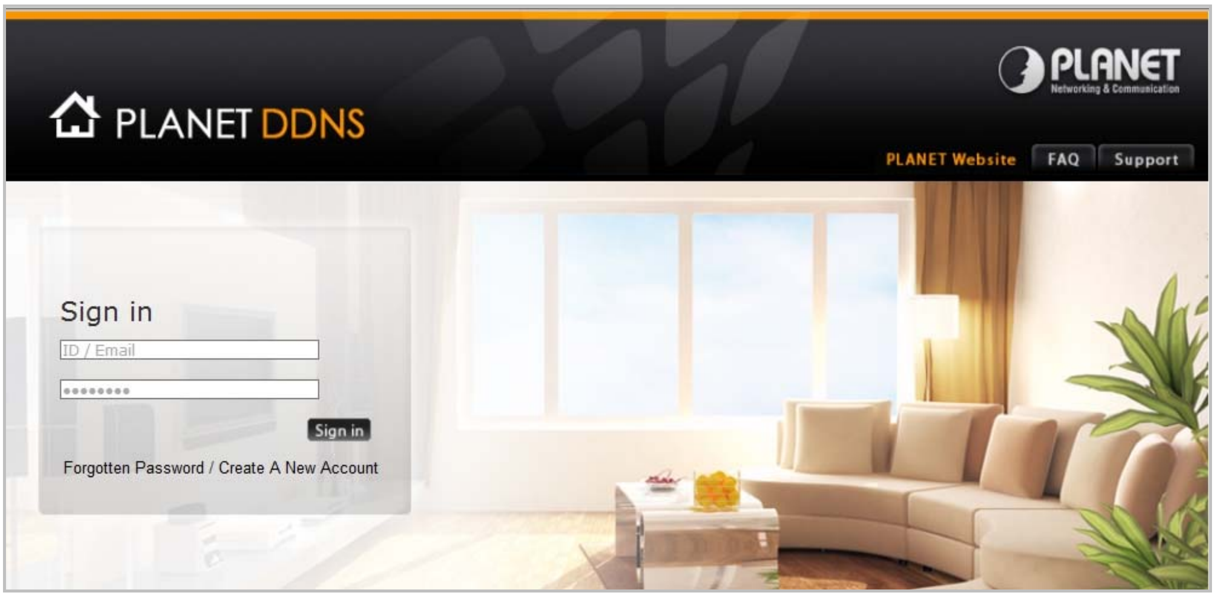
Dynamic DNS Provider: PlanetDDNS.com

DDNS Settings

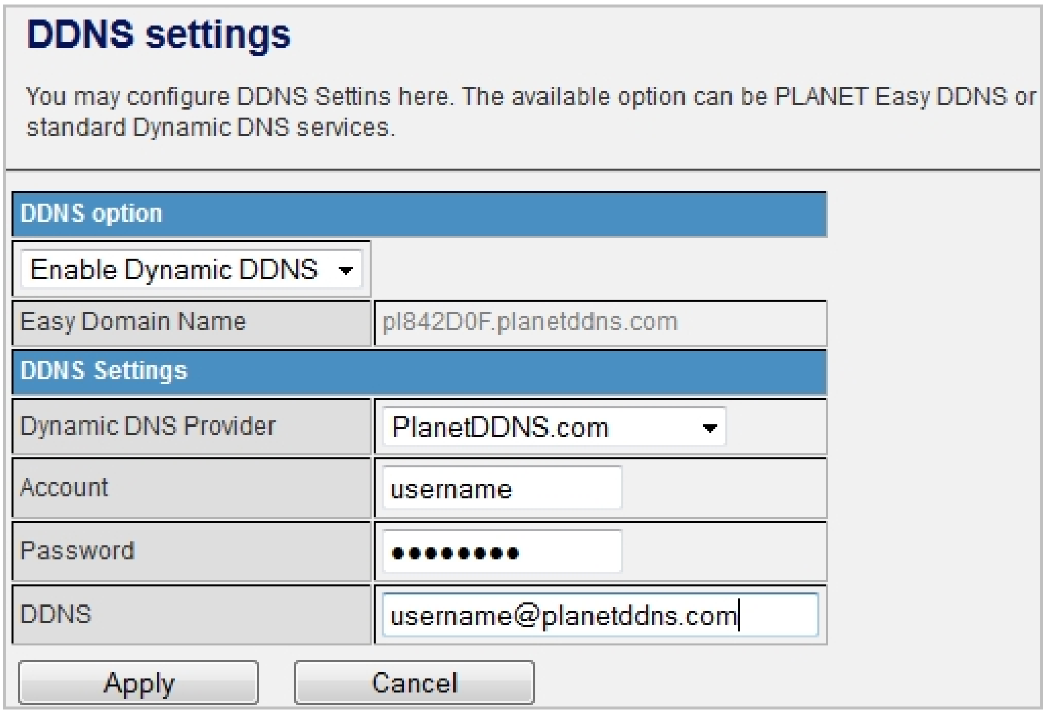
Object	Description
Dynamic DNS Provider	Select the proper dynamic DNS provider in the drop-down list. After selecting a dynamic DNS provider, you are allowed to set the following parameters.
Account	Enter the username of DDNS provider in the field.
Password	Enter the password of DDNS provider in the field.
DDNS	Enter the domain name of your device.

Planet DDNS

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 **Dynamic DNS Provider > PlanetDDNS.com**



DDNS settings

You may configure DDNS Settins here. The available option can be PLANET Easy DDNS or standard Dynamic DNS services.

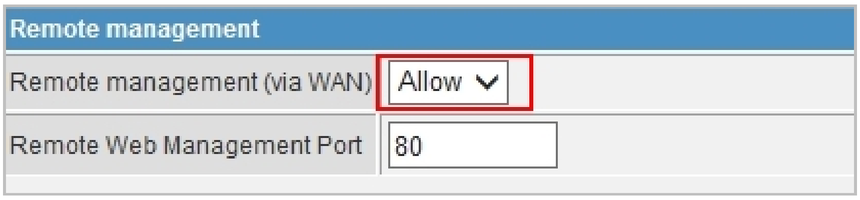
DDNS option	
Enable Dynamic DDNS	
Easy Domain Name	pl842D0F.planetddns.com
DDNS Settings	
Dynamic DNS Provider	PlanetDDNS.com
Account	username
Password	••••••••
DDNS	username@planetddns.com

Step 1. Type the User Name for your DDNS account.

Step 2. Type the Password for your DDNS account.

Step 3. Type the Domain Name you received from dynamic DNS service provider.

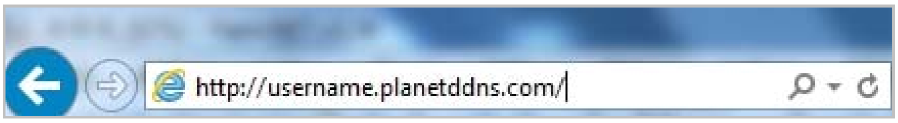
Go to **Firewall >System Security> Remote management** and choose **Allow** to allow remote access from WAN port.



Remote management

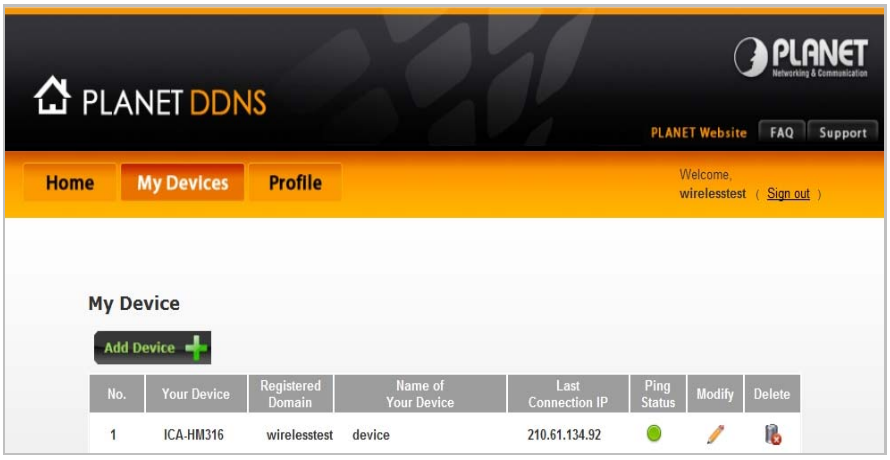
Remote management (via WAN)	Allow
Remote Web Management Port	80

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.

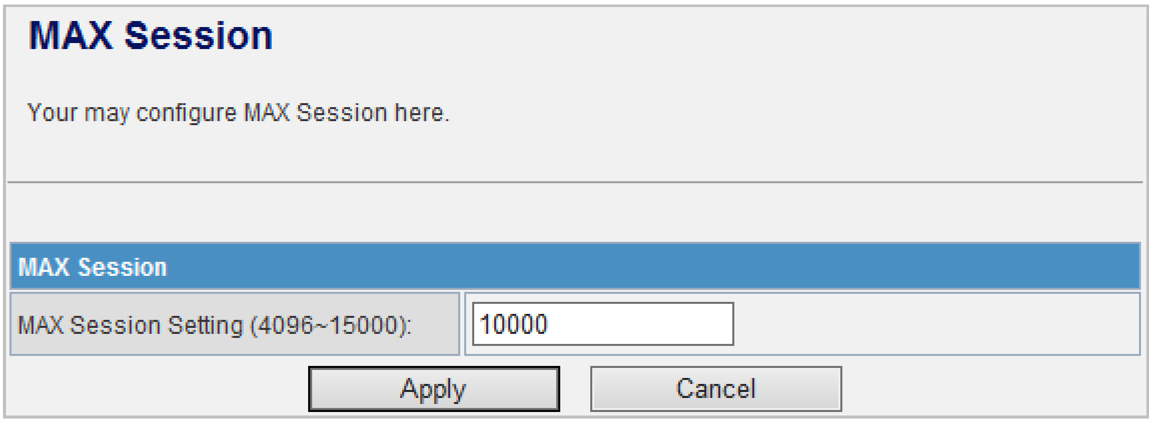


My Device

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	●	✎	🗑

5.8.12 Max Session

Choose **Administration > Max Session** and the following page appears. You may configure Max Session on this page.



MAX Session

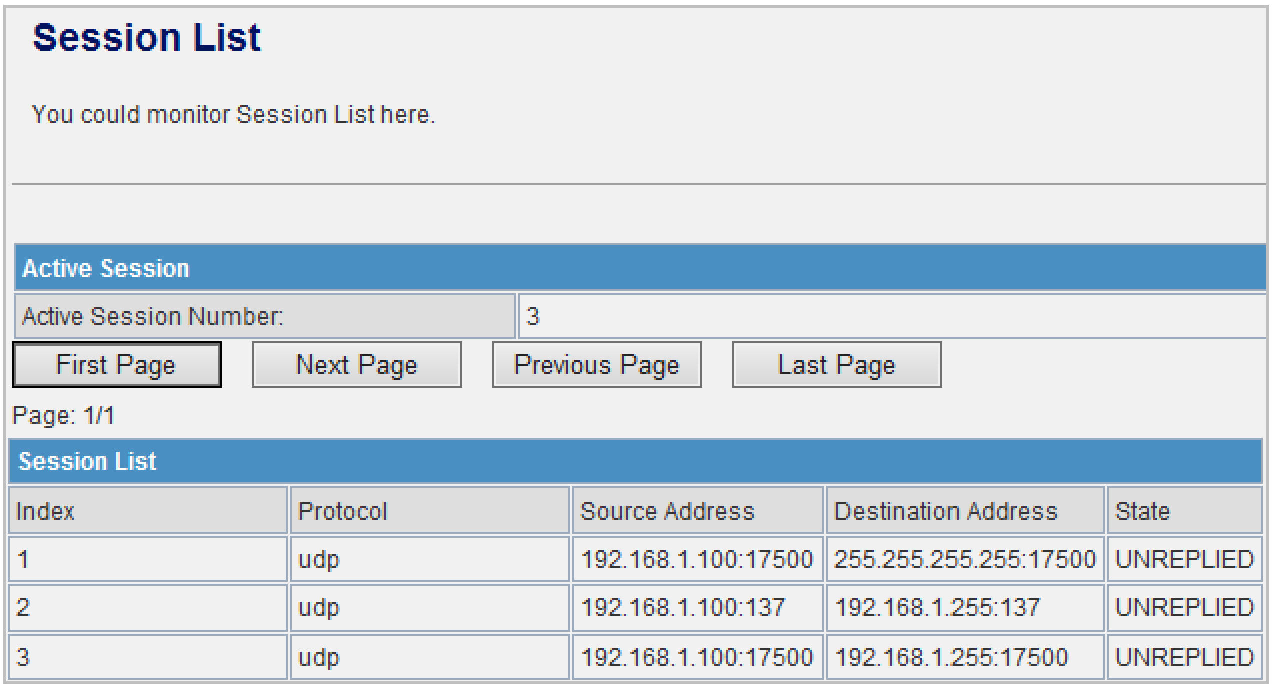
Your may configure MAX Session here.

MAX Session

MAX Session Setting (4096~15000):	10000

5.8.13 Session List

Choose **Administration > Session List** and the following page appears. You may monitor Session List on this page.



Session List

You could monitor Session List here.

Active Session

Active Session Number:	3

Page: 1/1

Session List

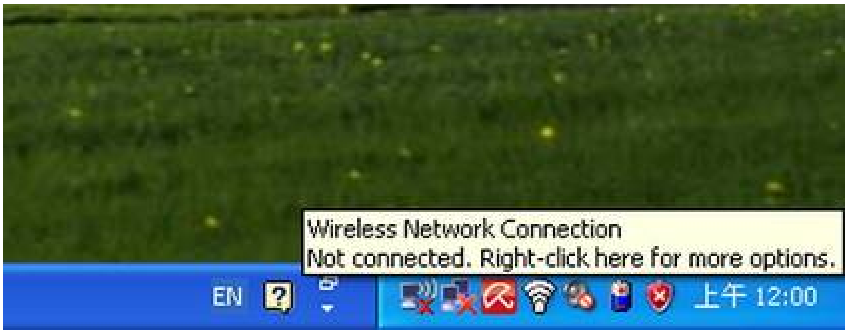
Index	Protocol	Source Address	Destination Address	State
1	udp	192.168.1.100:17500	255.255.255.255:17500	UNREPLIED
2	udp	192.168.1.100:137	192.168.1.255:137	UNREPLIED
3	udp	192.168.1.100:17500	192.168.1.255:17500	UNREPLIED

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the FRT-405N 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.

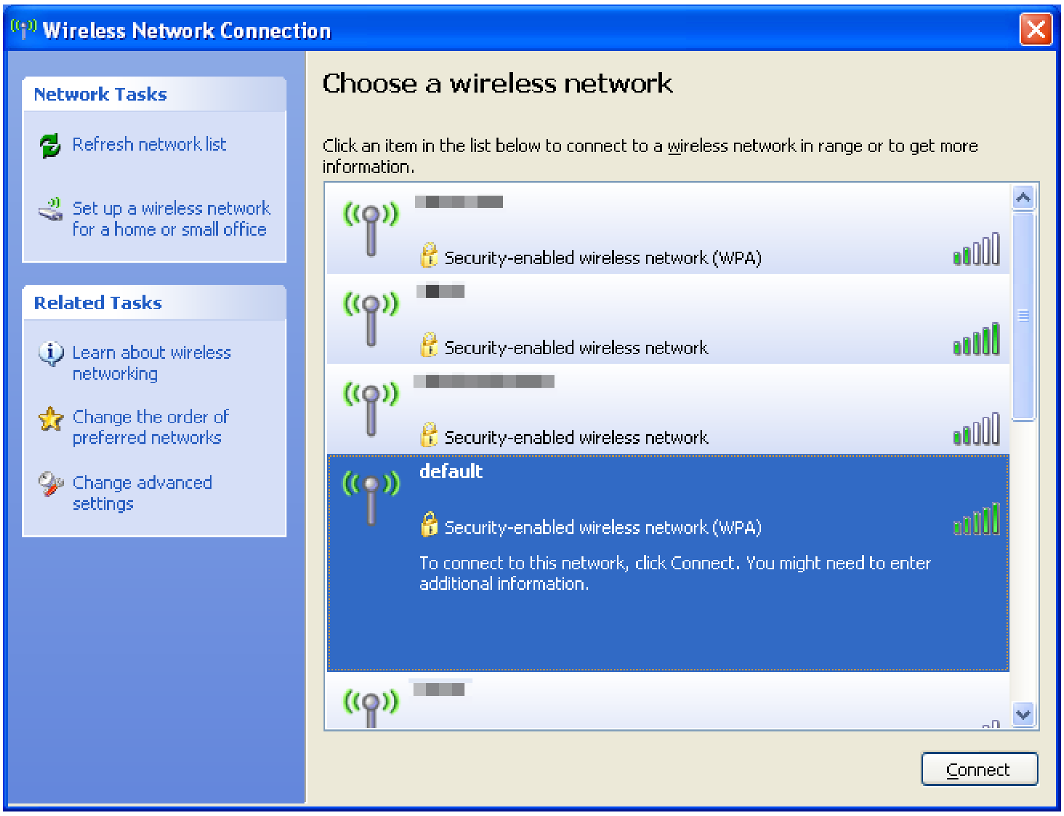
Figure 6-1 System Tray – Wireless Network Icon

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]

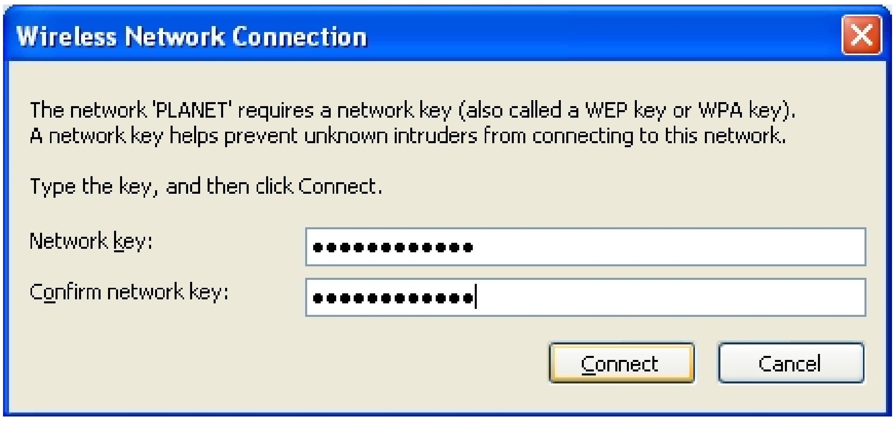
Figure 6-2 Choose a wireless network

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

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that configured in section 5.3.3

(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.

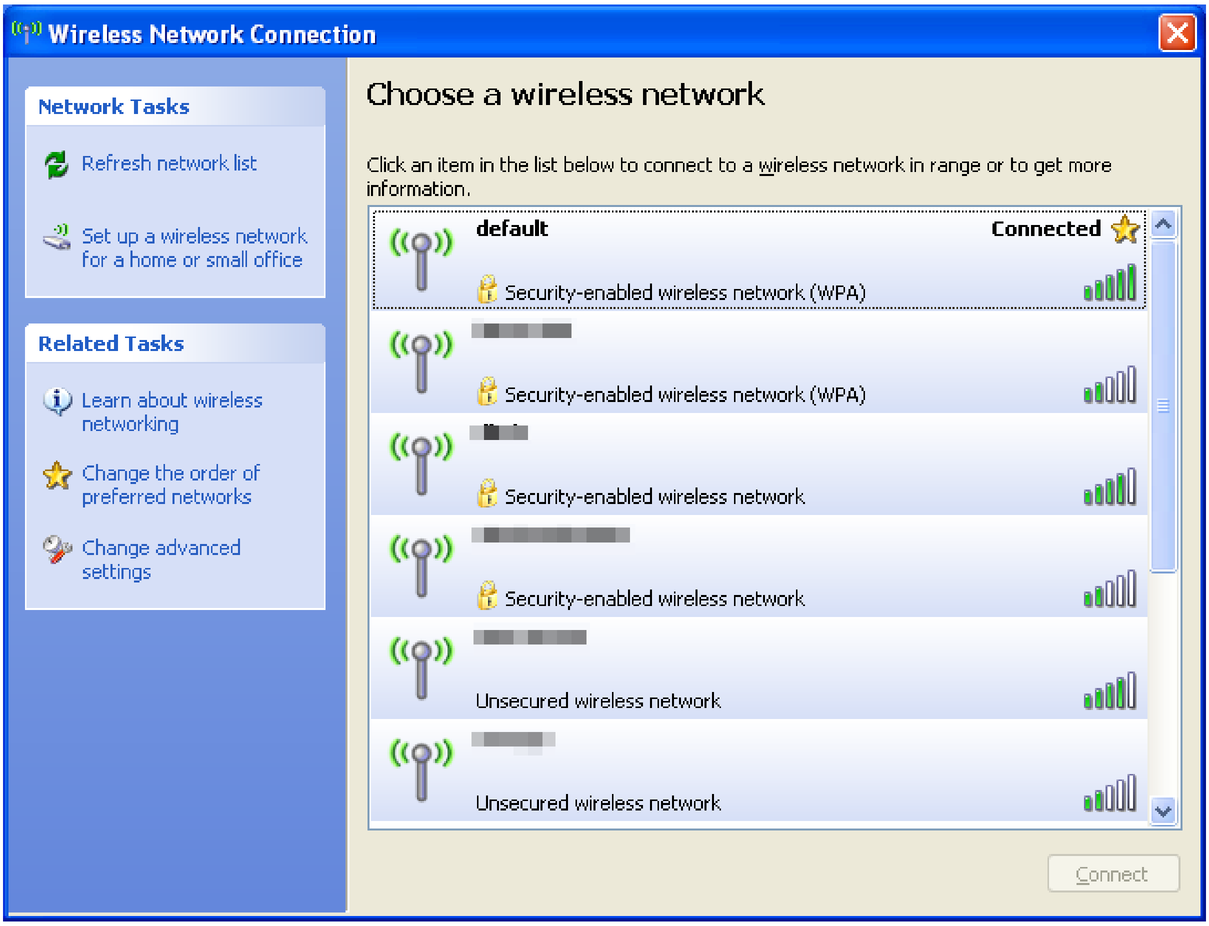
Type the key, and then click Connect.

Network key: ●●●●●●●●●●●●●

Confirm network key: ●●●●●●●●●●●●●

Figure 6-3 Enter the network key

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



Wireless Network Connection

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.

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

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 switch to “ON” position.

6.2 Windows 7 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

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

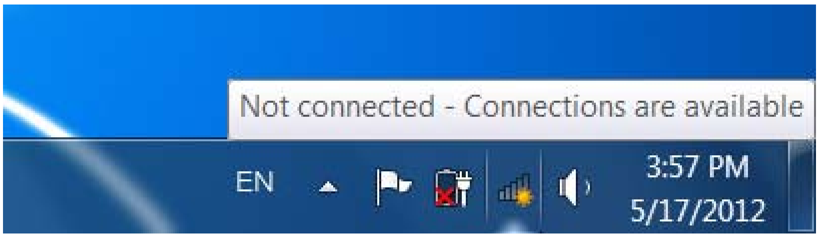


Figure 6-5 Network icon

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

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

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

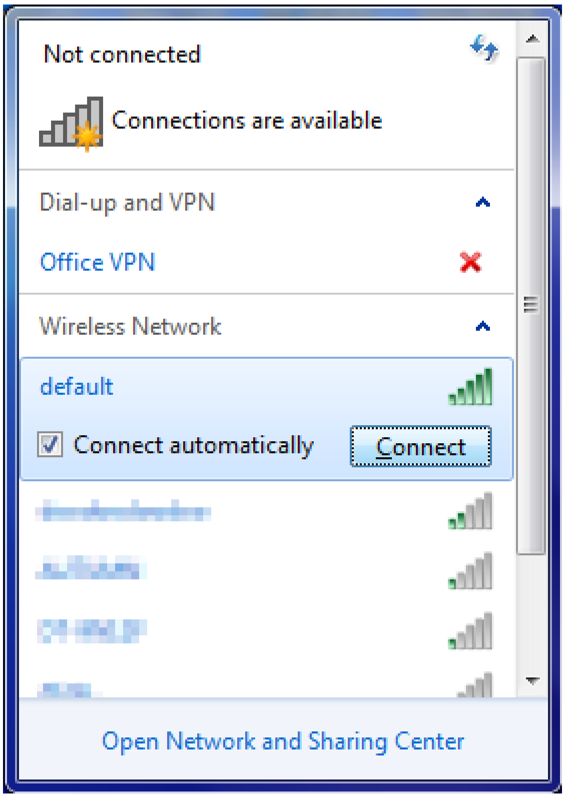


Figure 6-6 WLAN AutoConfig

Note

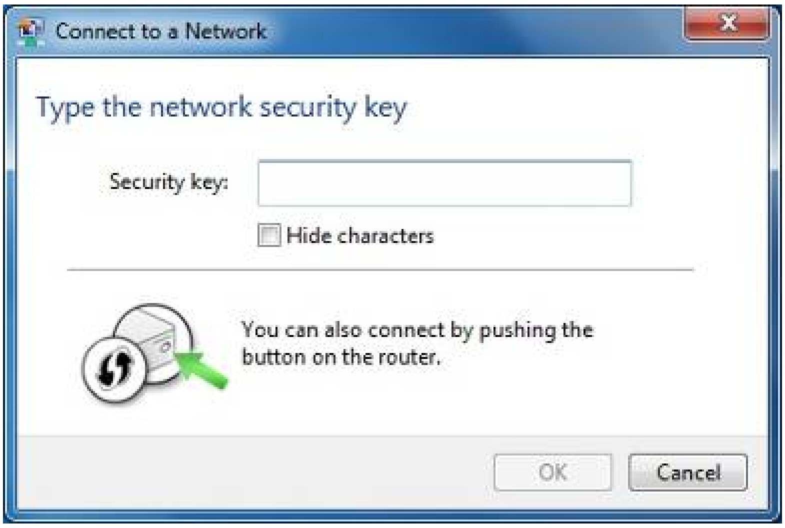
If you will be connecting to this Wireless AP in the future, check [**Connect automatically**].

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 configured in section 5.3.3

(3) Click the [OK] button


Connect to a Network

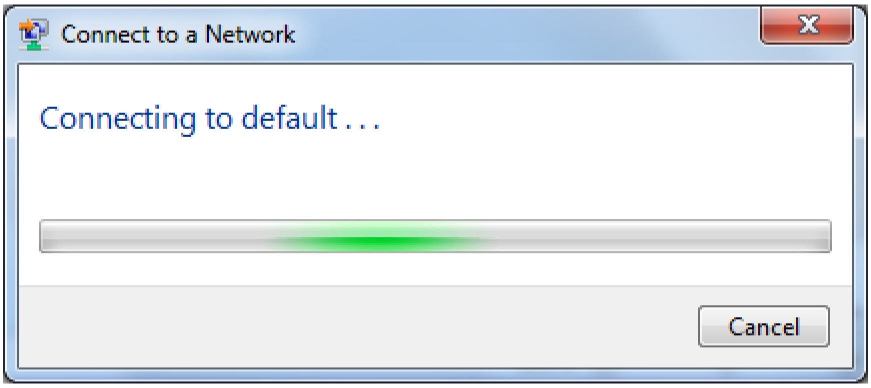
Type the network security key

Security key:

□ Hide characters

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

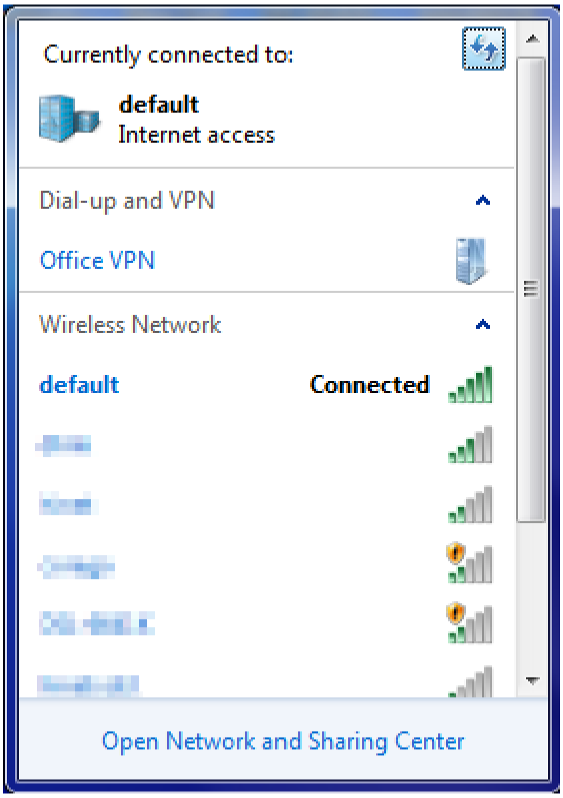
Figure 6-7 Type the network key


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

Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the FRT-405N is configured to “default”.

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

The AirPort Network Connection menu will appear

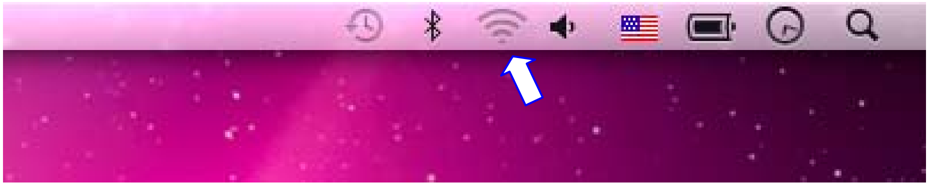


Figure 6-10 Mac OS – Network icon

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

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

(2) Double-click on the selected SSID

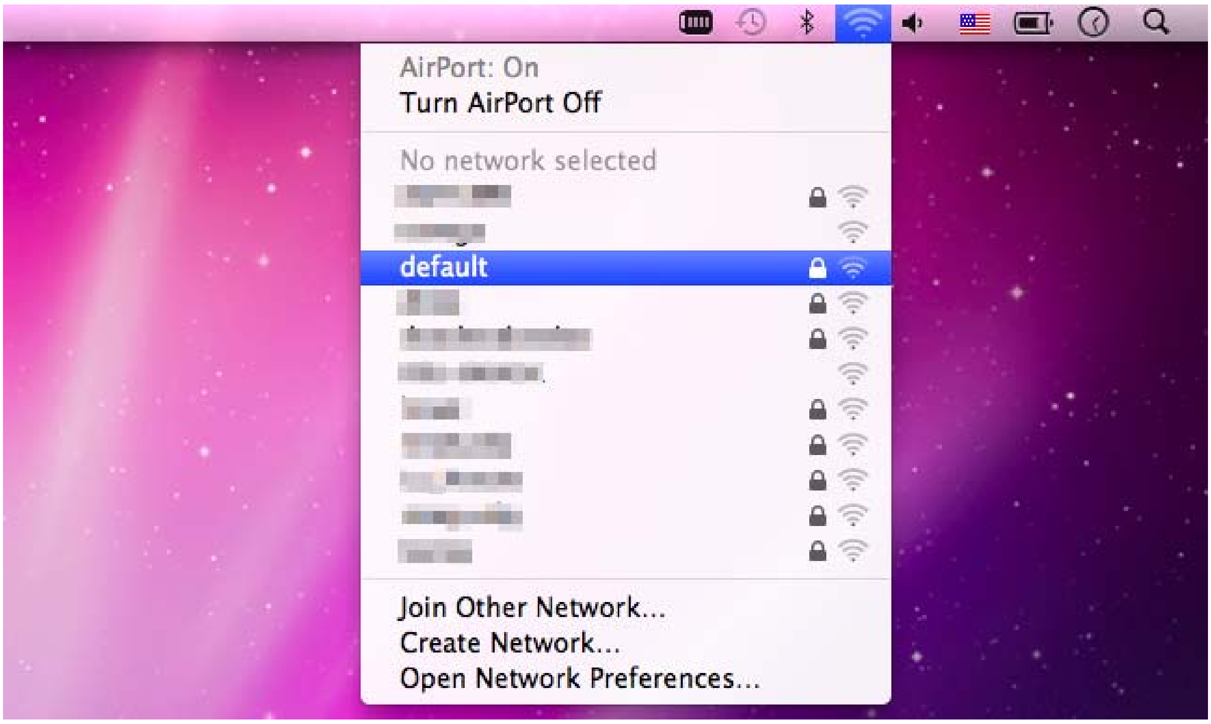
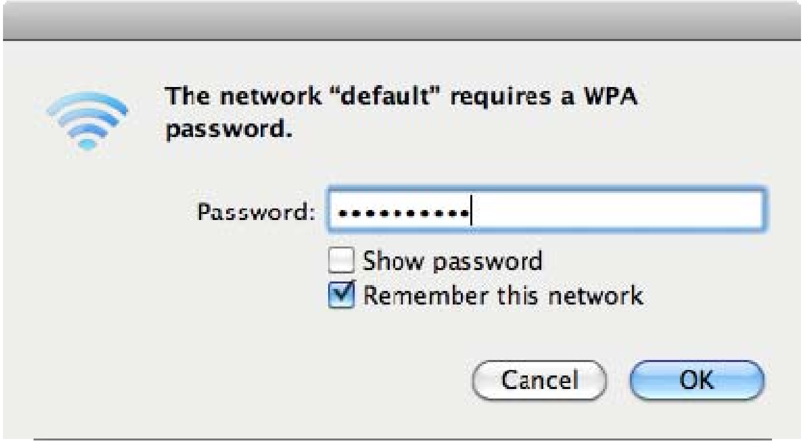


Figure 6-11 Highlight and select the wireless network

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

(1) Enter the encryption key that configured in section 5.3.3

(2) Click the [OK] button



The network "default" requires a WPA password.

Password: ••••••••••

☐ Show password

☑ Remember this network

Figure 6-12 Enter the Password

Note

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.

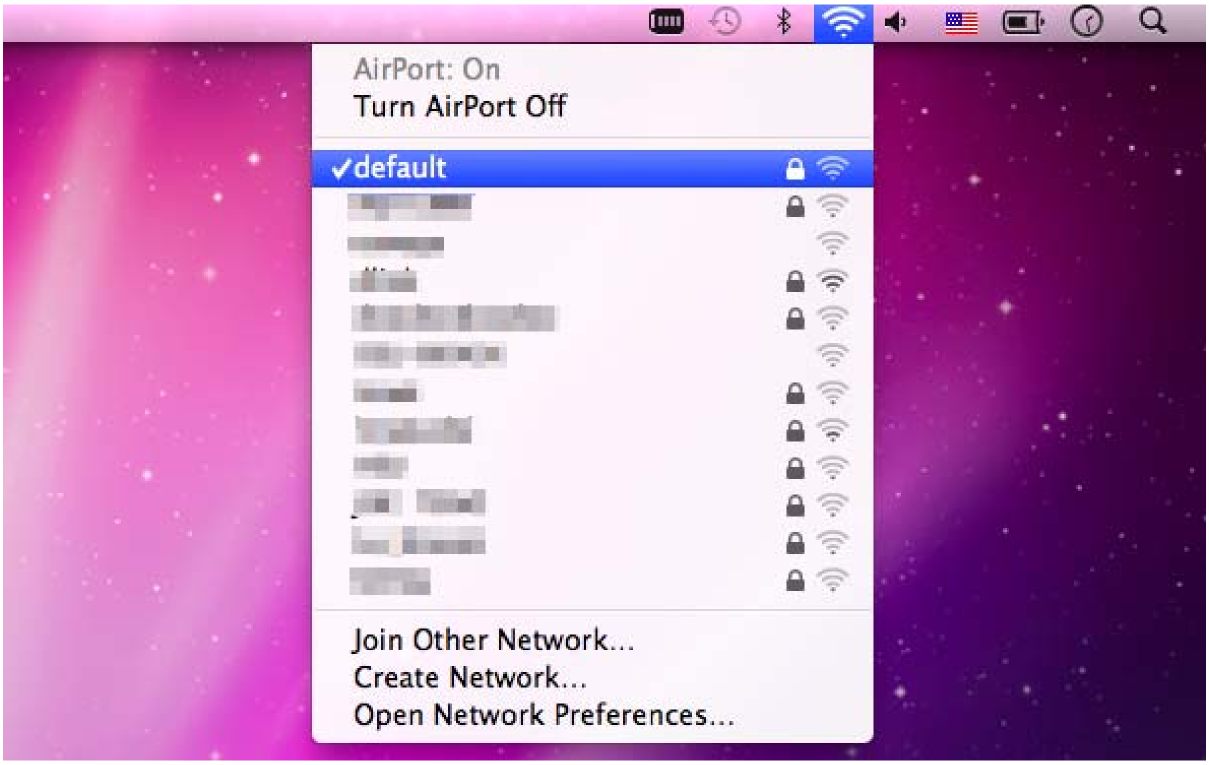


Figure 6-13 Connected to the Network

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**

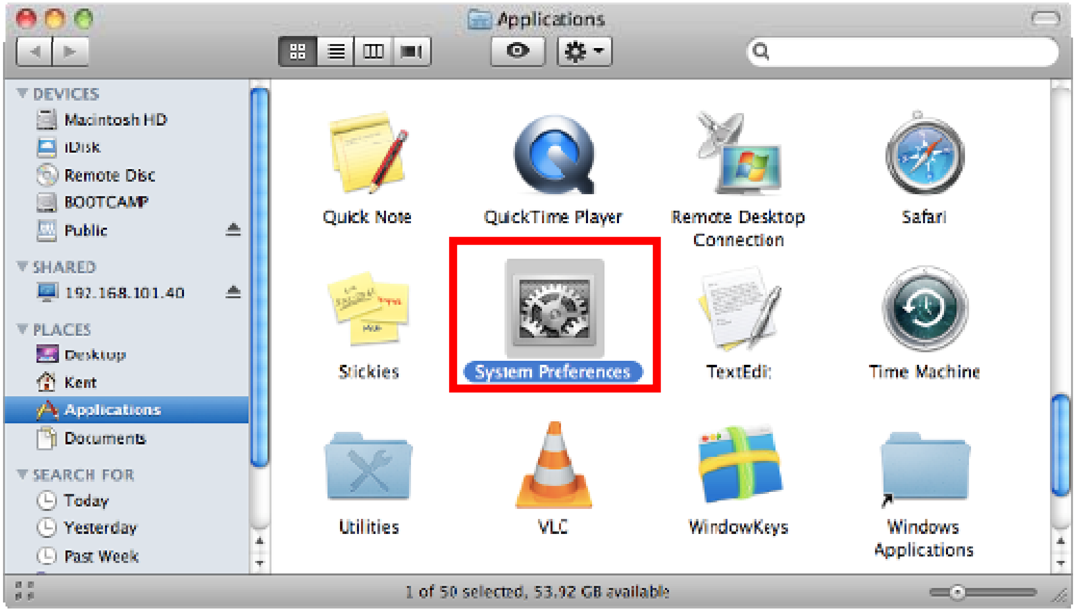


Figure 6-14 System Preferences

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

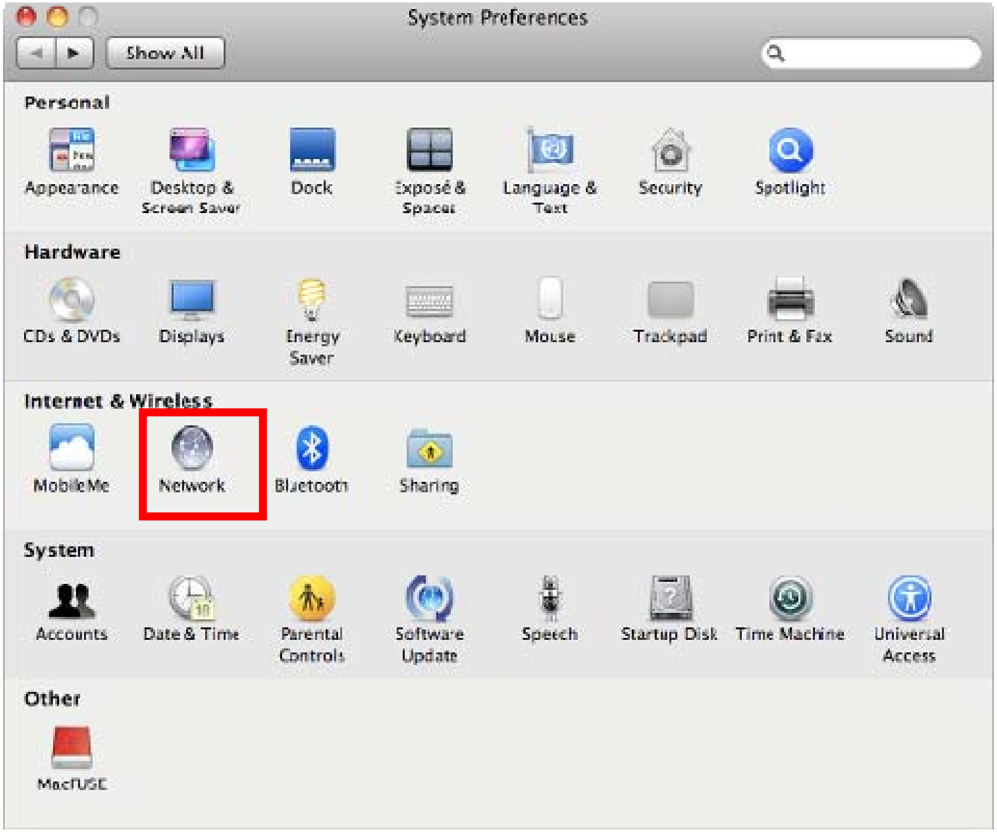


Figure 6-15 System Preferences -- Network

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”.

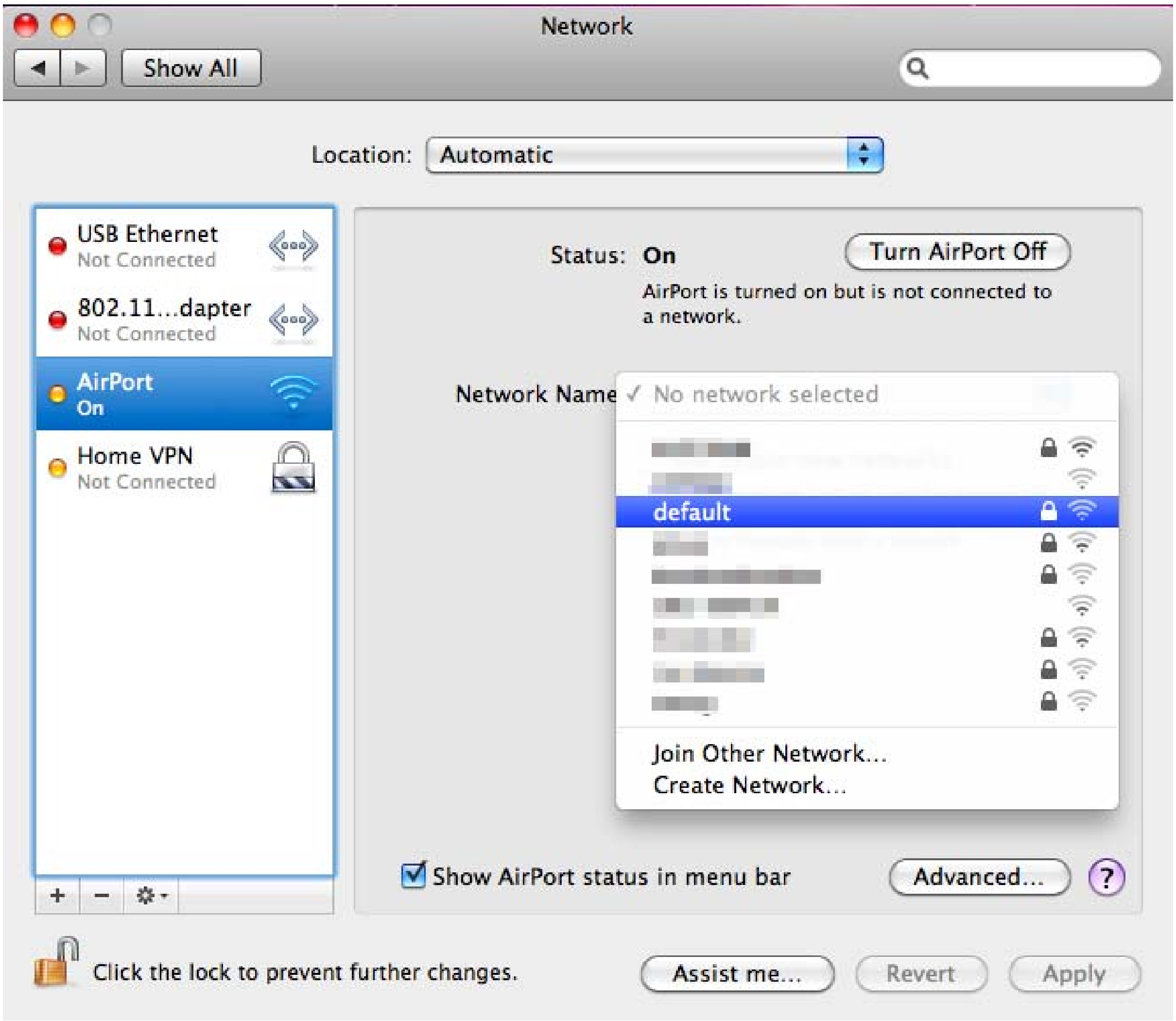


Figure 6-16 Select the Wireless Network

6.4 iPhone / iPod Touch / iPad

In the following sections, the **default SSID** of the FRT-405N is configured to "**default**".

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

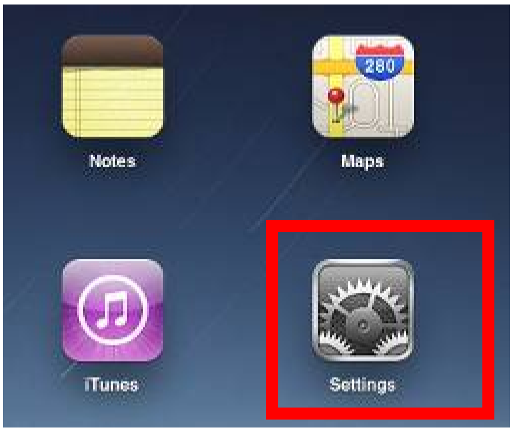


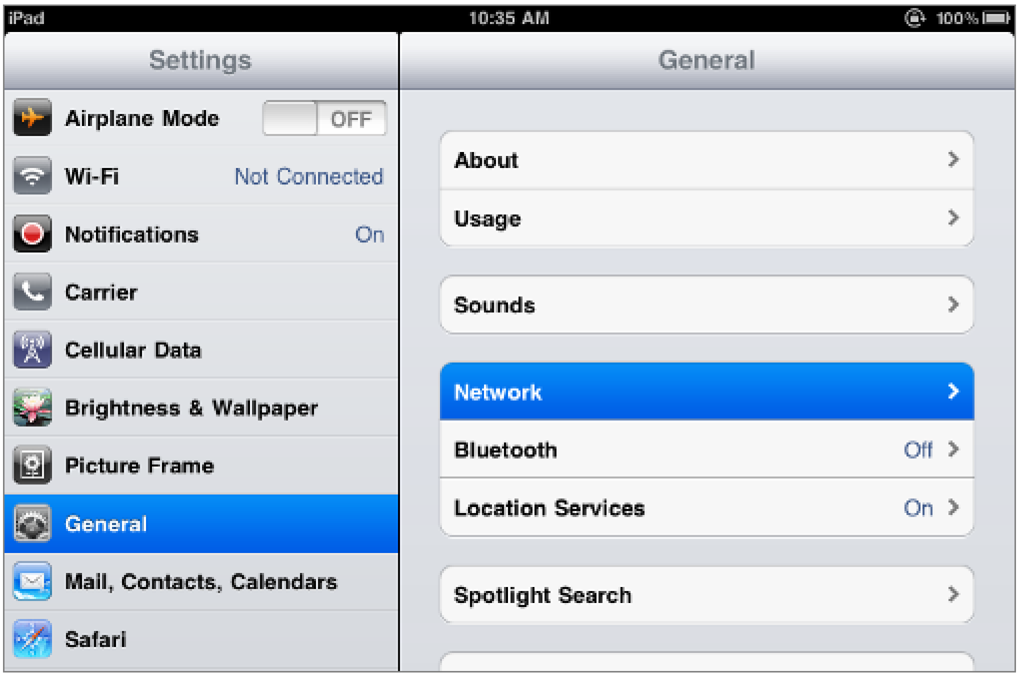
Figure 6-17 iPhone – Settings icon

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

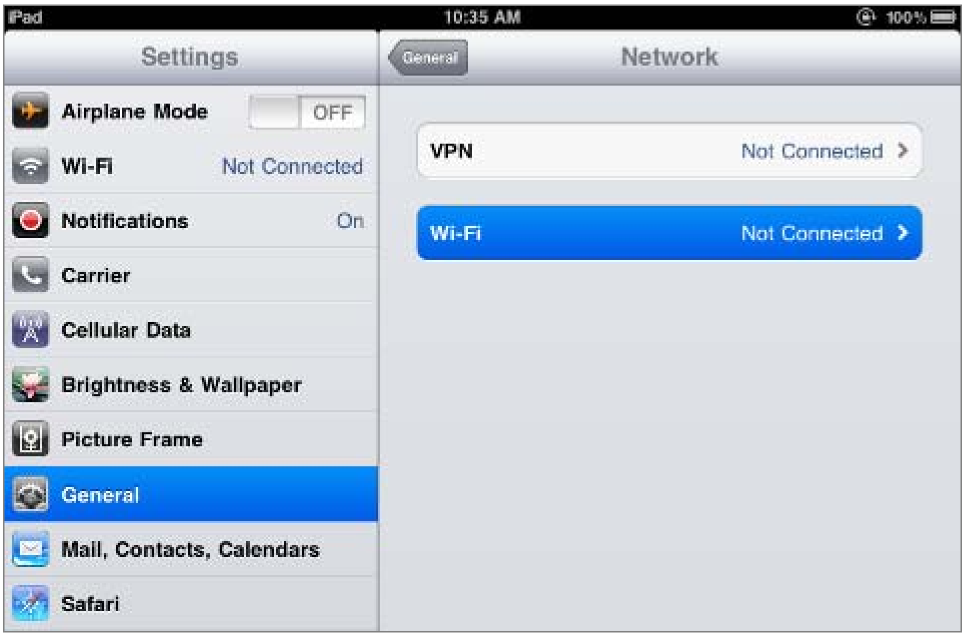
Network

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

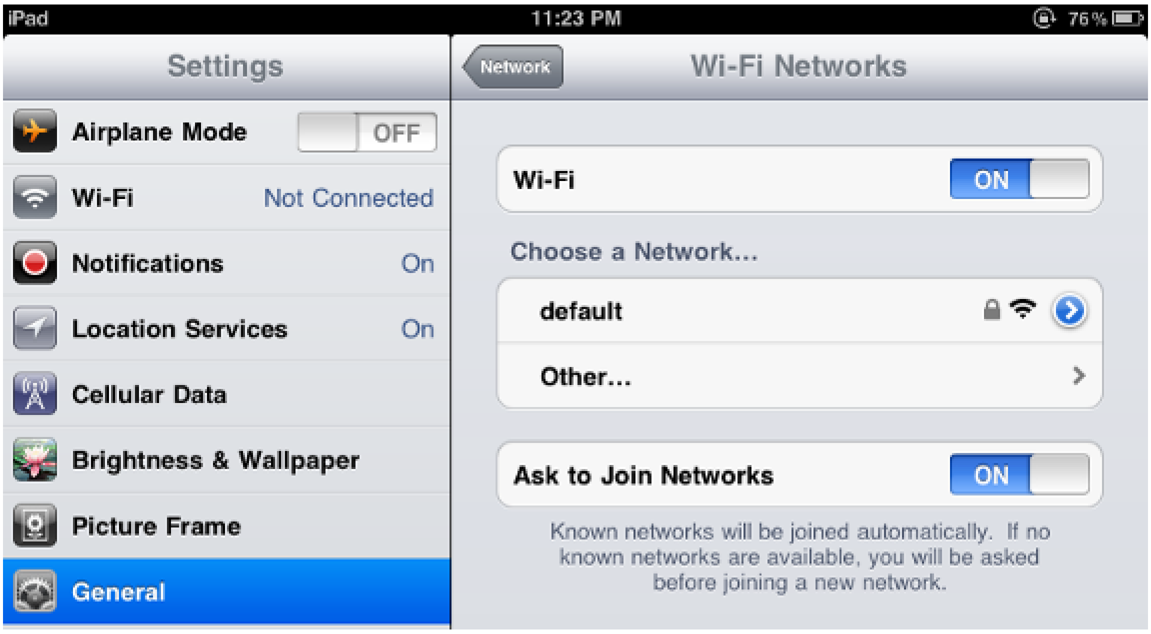
Wi-Fi Not Connected

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.

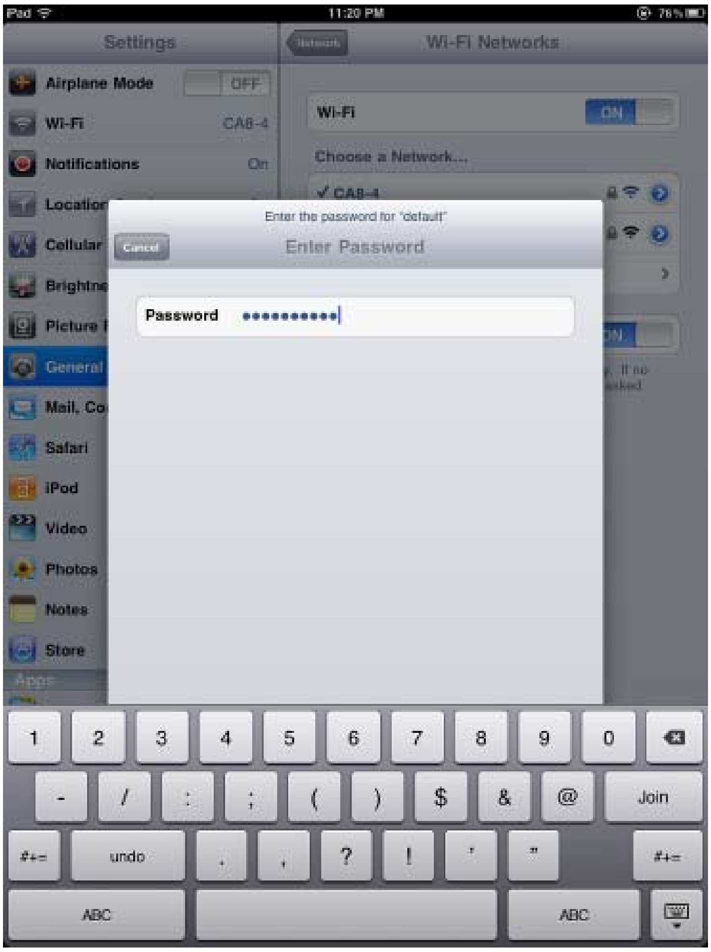
Figure 6-20 Turn on Wi-Fi

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

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



iPad 11:20 PM 76%

Settings

Airplane Mode OFF

Wi-Fi CA8-4

Notifications On

Wi-Fi Networks

Wi-Fi ON

Choose a Network...

✓ CA8-4

Enter the password for "default"

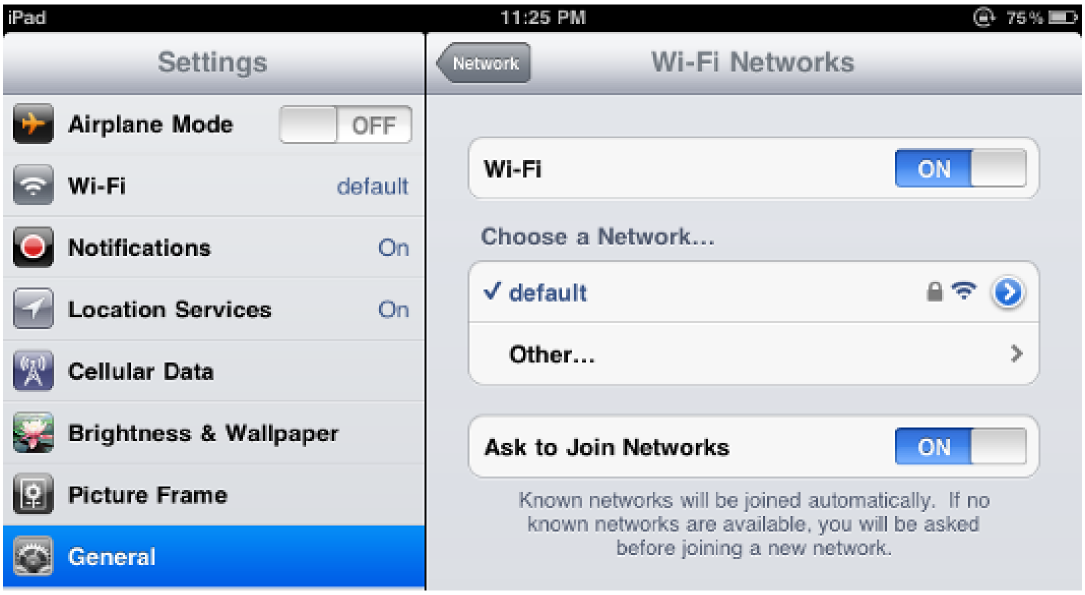
Enter Password

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.



iPad 11:25 PM 75%

Settings

Airplane Mode OFF

Wi-Fi default

Notifications On

Location Services On

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 6-22 iPhone -- Connected to the Network

Appendix A: Cable Profiles

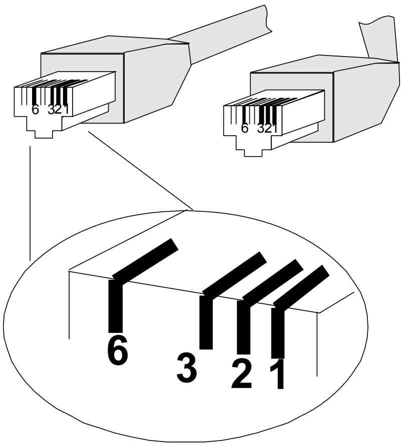
A.1 Device‘s RJ-45 Pin Assignments

■ **10/100Mbps, 10/100Base-TX**

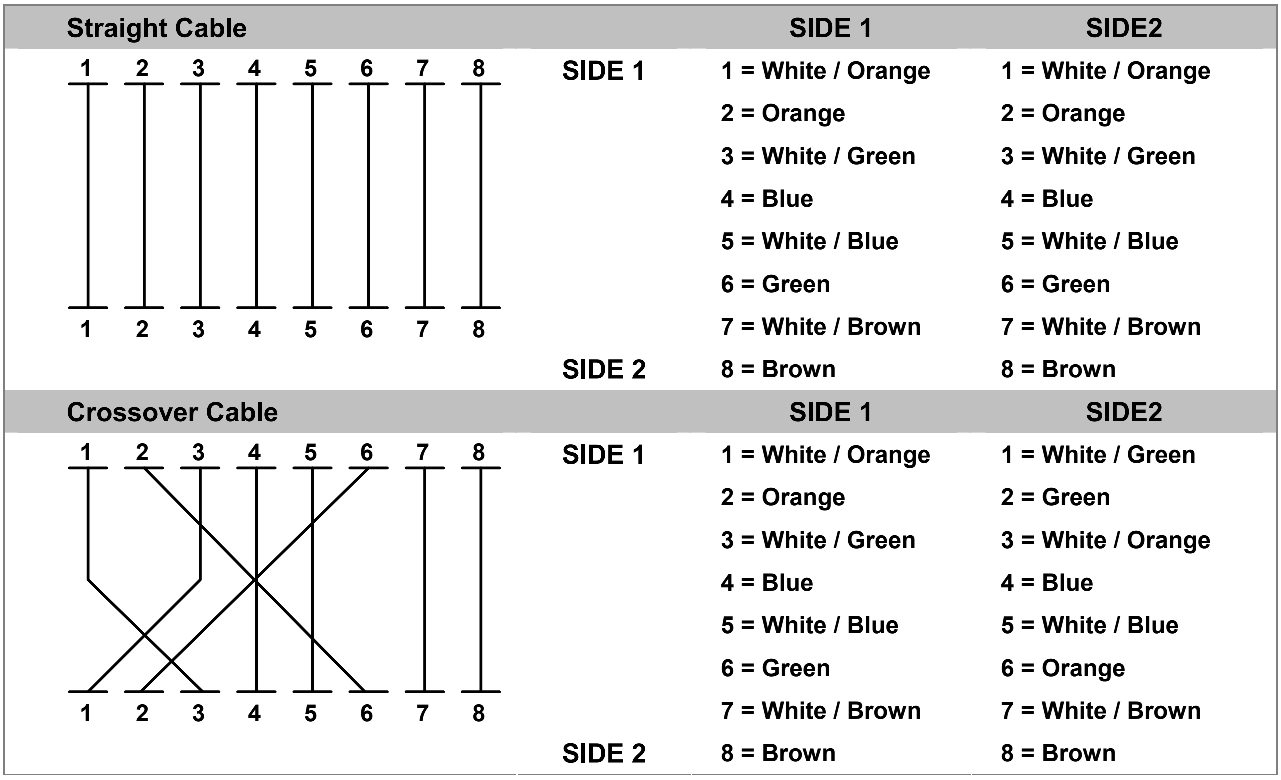
Contact	MDI	MDI-X
1	1 (TX +)	3
2	2 (TX -)	6
3	3 (RX +)	1
6	6 (RX -)	2
4, 5, 7, 8	Not used	Not used

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 RJ-45 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 cable and crossover cable connection:



Straight Cable	SIDE 1	SIDE2
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	SIDE2
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 Cable

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

A.3 Fiber Optical Cable Connection Parameter

The wiring details are shown below:

- **Fiber Optical 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-40x / 40xN

MFB-FX	SFP-Port 100Base-FX Transceiver (1310nm) -2km
MFB-F20	SFP-Port 100Base-FX Transceiver (1310nm) - 20km
MFB-FA20	SFP-Port 100Base-BX Transceiver (WDM,TX:1310nm) -20km
MFB-FB20	SFP-Port 100Base-BX Transceiver (WDM,TX:1550nm) -20km

Appendix B: Planet Smart Discovery Utility

To easily list the FRT-405N in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution.

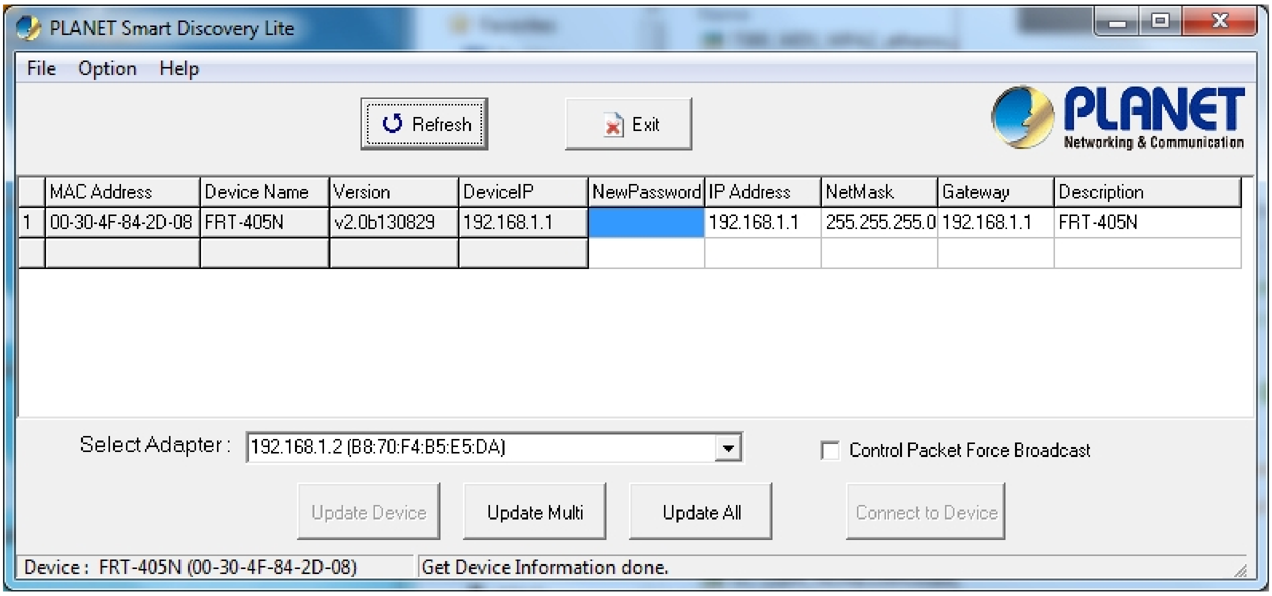
The following installation instructions guide you to running the Planet Smart Discovery Utility.

Step 1: Deposit the **Planet Smart Discovery Utility** in administrator PC.

Step 2: Run this utility and the following screen appears.

Planet_Utility.exe
PLANET Corp.

Step 3: Press **"Refresh"** button for current connected devices in the discovery list as shown in the following screen:



PLANET Smart Discovery Lite

	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description
1	00-30-4F-84-2D-08	FRT-405N	v2.0b130829	192.168.1.1		192.168.1.1	255.255.255.0	192.168.1.1	FRT-405N

Select Adapter : 192.168.1.2 (B8:70:F4:B5:E5:DA)

□ Control Packet Force Broadcast

Device : FRT-405N (00-30-4F-84-2D-08)   Get Device Information done.

Step 3: Press **"Connect to Device"** button and then the Web login screen appears.

Note

The fields in white background can be modified directly, and then you can apply the new setting by clicking the "**Update Device**" button.

Appendix C: Glossary

Address mask
A bit mask select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address
and one or more bits of the local portion. Sometimes it called subnet mask.

VDSL

VDSL2 (Very High-Bit-Rate Digital Subscriber Line 2), G.993.2 is the newest and most advanced standard of xDSL broadband wire line communications.

ADSL
Asymmetric digital subscriber line

AAL5
ATM Adaptation Layer - This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ATM
Asynchronous Transfer Mode - A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology,
real time, and demand led switching for efficient use of network resources.

AWG
American Wire Gauge - The measurement of thickness of a wire

Bridge
A device connects two or more physical networks and forward packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are repeaters which simply forward electrical signals from one cable to the other and full-fledged routers which make routing decisions based on several criteria.

Broadband
Characteristic of any network multiplexes independent network carriers onto a single cable. Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another. Broadcast a packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

CO

Central Office. Refers to equipment located at a Telco or service provider's office.

CPE

Customer Premises Equipment located in a user's premises

DHCP (Dynamic Host Configuration Protocol)

DHCP is software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. DHCP eliminates having to manually assign permanent IP addresses to every device on your network. DHCP software typically runs in servers and is also found in network devices such as Routers.

DMT

Discrete Multi-Tone frequency signal modulation

Downstream rate

The line rate for return messages or data transfers from the network machine to the user's premises machine.

DSLAM

Digital Subscriber Line Access Multiplex

Dynamic IP Addresses

A dynamic IP address is an IP address that is automatically assigned to a client station (computer, printer, etc.) in a TCP/IP network. Dynamic IP addresses are typically assigned by a DHCP server, which can be a computer on the network or another piece of hardware, such as the Router. A dynamic IP address may change every time your computer connects to the network.

Encapsulation

The technique layer protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), and followed by the application protocol data.

Ethernet

One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps.

FTP

File Transfer Protocol. The Internet protocol (and program) transfer files between hosts.

Hop count

A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML

Hypertext Markup Language - The page-coding language for the World Wide Web.

HTML browser

A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http

Hypertext Transfer Protocol - The protocol carry world-wide-web (www) traffic between a www browser computer and the www server being accessed.

ICMP

Internet Control Message Protocol - The protocol handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address

An IP address is assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department
of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual
addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where x is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

Internet Protocol (IP)

The network layer protocol for the Internet protocol suite

IP address

The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

ISP

Internet service provider - A company allows home and corporate users to connect to the Internet.

MAC

Media Access Control Layer - A sub-layer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB

Management Information Base - A collection of objects can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

NAT

Network Address Translation - A proposal for IP address reuse, where the local IP address is mapped to a globally unique address.

NVT

Network Virtual Terminal

PAP

Password Authentication Protocol

PORT

The abstraction used in Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

POTS

Plain Old Telephone Service - This is the term describe basic telephone service.

PPP

Point-to-Point-Protocol - The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

PPPoE

PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

Remote server

A network computer allows a user to log on to the network from a distant location.

RFC

Request for Comments - Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFC can be found at www.ietf.org.

Route

The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks.
In the Internet, each datagram is routed separately.

Router

A system is responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics".

Routing Table

Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

Routing Information Protocol

Routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

SNMP

Simple Network Management Protocol - The network management protocol of choice for TCP/IP-based Internet.

SOCKET

(1) The Berkeley UNIX mechanism for creating a virtual connection between processes.
(2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

Spanning-Tree Bridge Protocol (STP)

Spanning-Tree Bridge Protocol (STP) - Part of an IEEE standard. A mechanism for detecting and preventing loops from occurring in a multi-bridged environment.
When three or more LAN's segments are connected via bridges, a loop can occur. Because of a bridge forwards all packets that are not recognized as being local,
some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

Spoofing

A method of fooling network end stations into believing that keep alive signals have come from and returned to the host. Polls are received and returned locally at
either end

Static IP Address

A static IP address is an IP address permanently assigned to computer in a TCP/IP network. Static IP addresses are usually assigned to networked devices that are consistently accessed by multiple users, such as Server PCs, or printers. If you are using your Router to share your cable or DSL Internet connection, contact your ISP to see if they have assigned your home a static IP address. You will need that address during your Router's configuration.

Subnet

For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

TCP

Transmission Control Protocol - The major transport protocol in the Internet suite of protocols provides reliable, connection-oriented full-duplex streams.

TFTP

Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often boot diskless workstations and other network devices such as routers over a network (typically a LAN).

Telnet

The virtual terminal protocol in the Internet suite of protocols - Allows users of one host to log into a remote host and act as normal terminal users of that host.

Transparent bridging

The intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses, and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

UDP

User Datagram Protocol - A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagram without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UNI signaling

User Network Interface signaling for ATM communications.

Virtual Connection (VC)

A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

WAN

Wide area network - A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).

PLANET
Networking & Communication

EC Declaration of Conformity

For the following equipment:

*Type of Product: 802.11n Wireless Internet Fiber Router (mini-GBIC, SFP) with 4-port switch
*Model Number: FRT-405N

* 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.
For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328 V1.7.1	(2006-10)
EN 301 489-17 V2.1.1	(2009-05)
EN 301 489-1 V1.9.2	(2011-09)
EN 62311	(2008)
EN 60950-1	(2006+A11:2009+A1:2010+A12:2011)

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 : **Product Manager**

Taiwan — *Place*

30st Sep., 2013 — *Date*

Kent Kang — *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**, kijelenti, hogy ez a **802.11n Wireless Internet Fiber Router** 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 orporation,** dat **802.11n Wireless Internet Fiber Router** in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
Eestikeeles	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.