PLANET
Networking & Communication

Wired / Wireless

Internet Fiber Router

FRT-401 / 401S15 / 405

FRT-401N / 401NS15 / 405

User's Manual

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. Connect 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, and (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.

CE mark Warning

This is a class B device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

Energy Saving Note of the Device

This power required device does not support Stand by mode operation.
For energy saving, please remove the DC-plug or push the hardware Power Switch to OFF position to disconnect the device from the power circuit.
Without remove the DC-plug or switch off the device, the device will still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the DC-plug for the device if this device is not intended to be active.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC 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.

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 and have to collect such WEEE separately.

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.

Revision

User’s Manual for Wired / Wireless Internet Fiber Router

Model : FRT-401 / 401S15 / 405
FRT-401N / 401NS15 / 405N

Rev: 1.0 (Apr. 2010)

Part No. EM-FRT40x_FRT40xN_v1.0

Table of Contents

1. Introduction

With growing network services such as HDTV, IPTV, voice-over-IP (VoIP) and Multimedia broadband applications, and the demand of bandwidth rises quickly. The current Broadband environment has not already accorded with needing; the FTTH (fiber-to-the-home) would be the most promising NGN (Next Generation Networking) application to fulfill the demand.

The PLANET Wired / Wireless Internet Fiber Router, FRT-40x and FRT-40xN series, provides office and residential users the ideal solution for sharing a high-speed fiber Internet connection and four-10/100Mbps Fast Ethernet backbone. The Fiber Router is a perfect FTTH Digital Home Router which can provide very high performance access to Internet, both downstream and upstream up to 100Mbps through the fiber interface. The PLANET Internet Fiber Router supports several common optical connectors for WAN connection, such as 100BASE-BX, 100BASE-LX, 100BASE-FX and Small Form Factor Pluggable (SFP). The Fiber Router can be implemented easily for optical fiber deployment.

With built-in IEEE 802.11b/g and 802.11n wireless network capability, the **FRT-40xN series** allows any computer and wireless-enabled network device connect to it without additional cabling. New 802.11n wireless capability gives you the highest speed of wireless experience ever. With a compatible wireless adapter installed in your PC, the files can be transferred at up to **300Mbps**. The radio coverage is also doubled to offer the high speed wireless connection even in a wide space of your office or house.

To secure the **wireless communication**, the **FRT-40xN** supports most up-to-date encryption, WEP, WPA-PSK and WPA2-PSK. In order to simplify the security settings, the FRT-40xN supports **WPS** configuration with PBC/PIN type for users to easily connect to a secured wireless network.

The PLANET Fiber Router provides **QoS** features to make the network services smooth. Traffic priority can be assigned by the router to guarantee some important and specific transmissions, especially for real-time streaming multimedia applications such as the **on-line gaming**, **VoIP**, and **IPTV** to keep the bandwidth usage smoothly. Furthermore, the Fiber Router not only provides basic router functions such as DHCP server, Virtual Server, DMZ, and UPnP, but also provides full firewall functions including Network Address Translation (NAT), IP / Port / MAC Filtering and Content Filtering. It serves as an Internet firewall to protect your network from being accessed by unauthorized users.

1.1 Feature

1. **Fiber Interface** support
2. Complies with IEEE 802.3, IEEE 802.3u 10/100Base-TX, 100Base-FX standard
3. Long distance connection based on optical fiber transceiver
4. Choice of fiber-connector from SC, MT-RJ / VF-45 and WDM, multi-mode / single-mode fiber / 100Base SFP
5. Co-work with PLANET 100Base-FX Media Conversion and MFB-Series Transceiver
6. QoS support
7. 802.1Q VLAN support
8. Supports **FTTH / IPTV** applications
9. Built-in 4-port 10/100 Mbps Ethernet switch
10. Router / Bridge / WISP mode support (WISP mode is noly for wireless model)
11. SPI Firewall security for Anti-DoS Prevention
12. Supports IP / Port / MAC Filtering and Content Filtering
13. TS-1000 and 802.3ah OAM support
14. Supports SNMP v1/v2c
15. IEEE 802.11n wireless technology compliant with 802.11b/g standard **(For wireless model)**
16. Capable of up to 300Mbps wireless data rate **(For wireless model)**
17. WPS / WMM support **(For wireless model)**
18. Supports 64/128-bit WEP, WPA–TKIP(PSK), WPA2-AES(PSK), 802.1x **(For wireless model)**

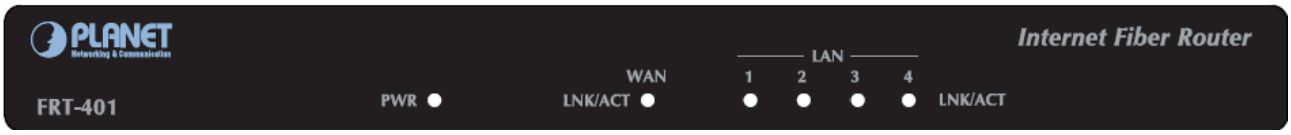
1.2 Package Contents

- Wired / Wireless Fiber Router Unit x 1
- Power Adapter x 1
- Quick Installation Guide x 1
- User’s Manual CD x 1
- Antenna x 2 **(Foe Wireless Model)**

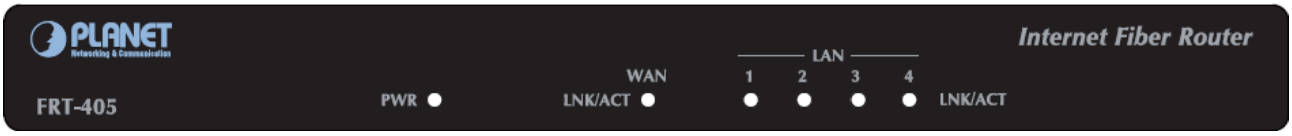
1.3 Physical Details

FRT-401 / FRT-401S15 / FRT-405

Front Panel



FRT-401 / FRT-401S15

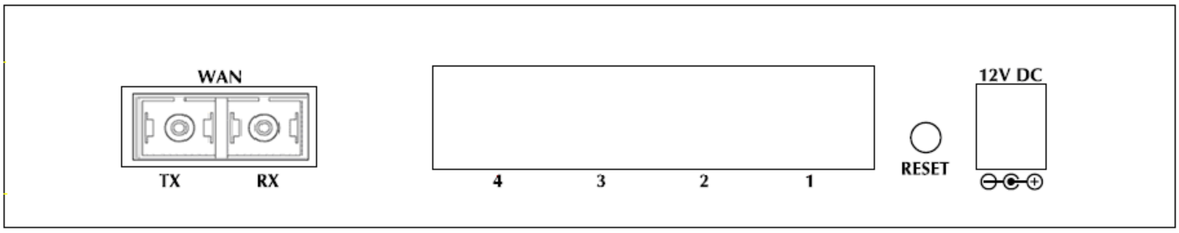


FRT-405

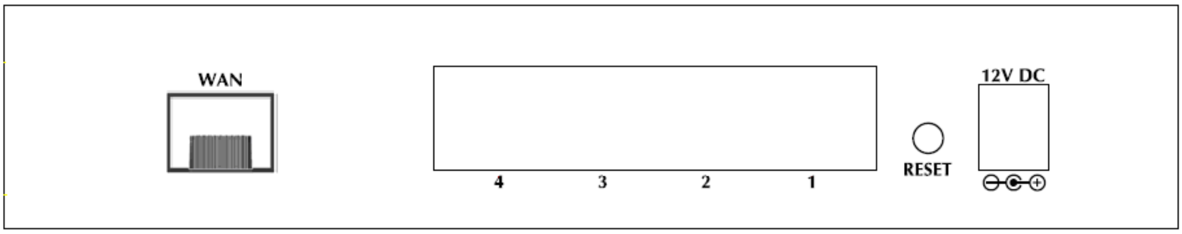
Front Panel LED definition

LED	State	Description
PWR	ON	When the router is powered on, and in ready state.
	OFF	When the router is powered off.
WAN	Flashing	Data is being transmitted or received via the fiber connection.
	ON	The optical fiber connection connected successfully.
LAN1-4	Flashing	Data is being transmitted or received via the corresponding LAN port.
	ON	The port is up.

Front Panel



FRT-401 / FRT-401S15



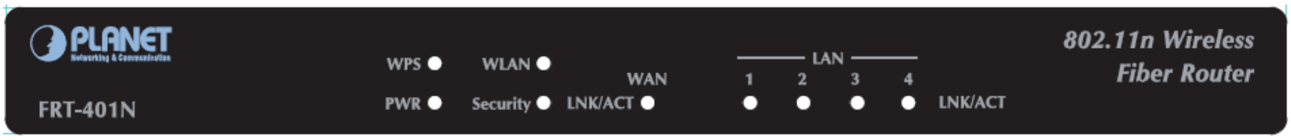
FRT-405

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.
WAN	One Fiber-optic Interface, SC or SFP connector-type

FRT-401N / FRT-401NS15 / FRT-405N

Front Panel



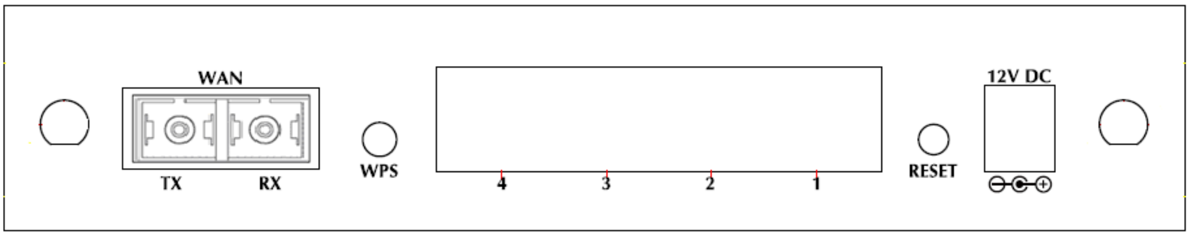
FRT-401N / FRT-401NS15

FRT-405N

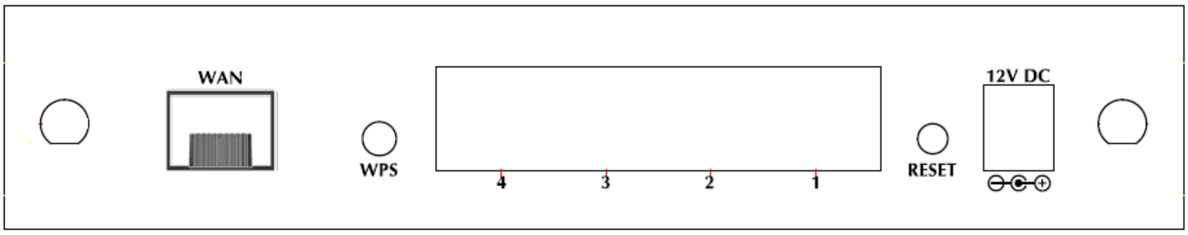
Front Panel LED definition

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	Data is being transmitted or received via the fiber connection.
	ON	The optical fiber connection connected successfully.
LAN1-4	Flashing	Data is being transmitted or received via the corresponding LAN port.
	ON	The port is up.

Front Panel



FRT-401N / FRT-401NS15



FRT-405N

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	One Fiber-optic Interface, SC or SFP connector-type

2. Installation

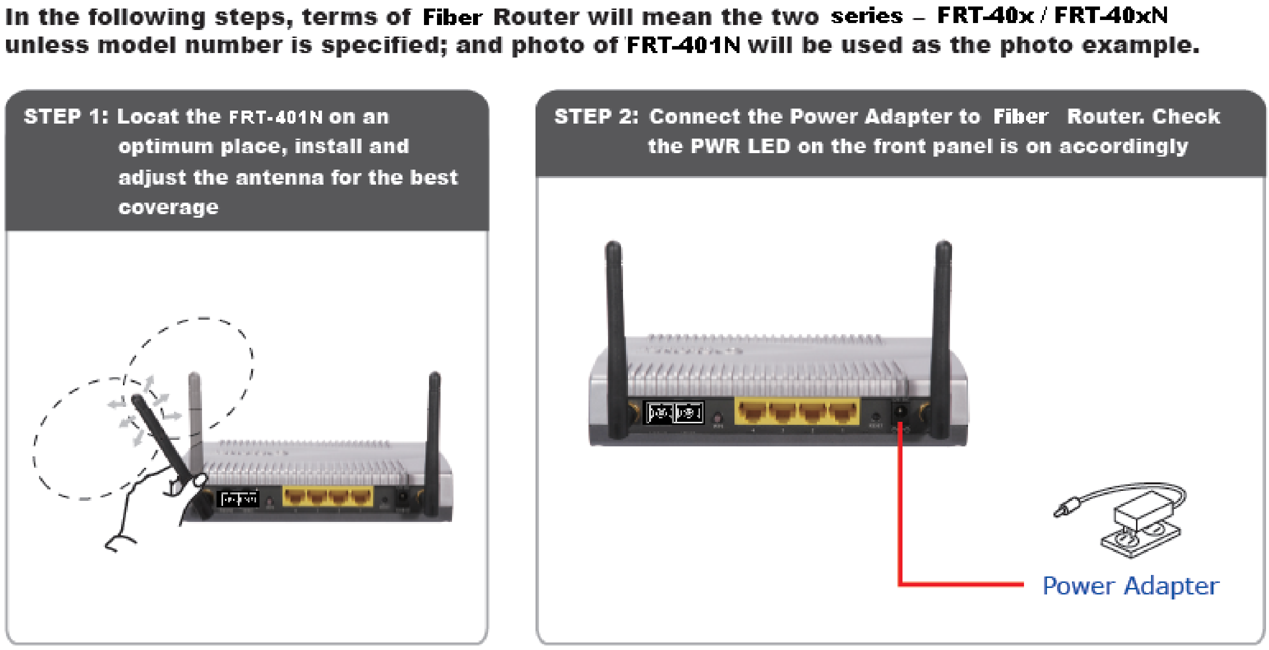
This chapter offers information about installing your router. If you are not familiar with the hardware or software parameters presented here, please consult your service provider for the values needed.

2.1 System Requirement

1. Personal computer (PC)
2. Pentium III 266 MHz processor or higher
3. 128 MB RAM minimum
4. 20 MB of free disk space minimum
5. RJ45 Ethernet Port

2.2 Hardware Installation

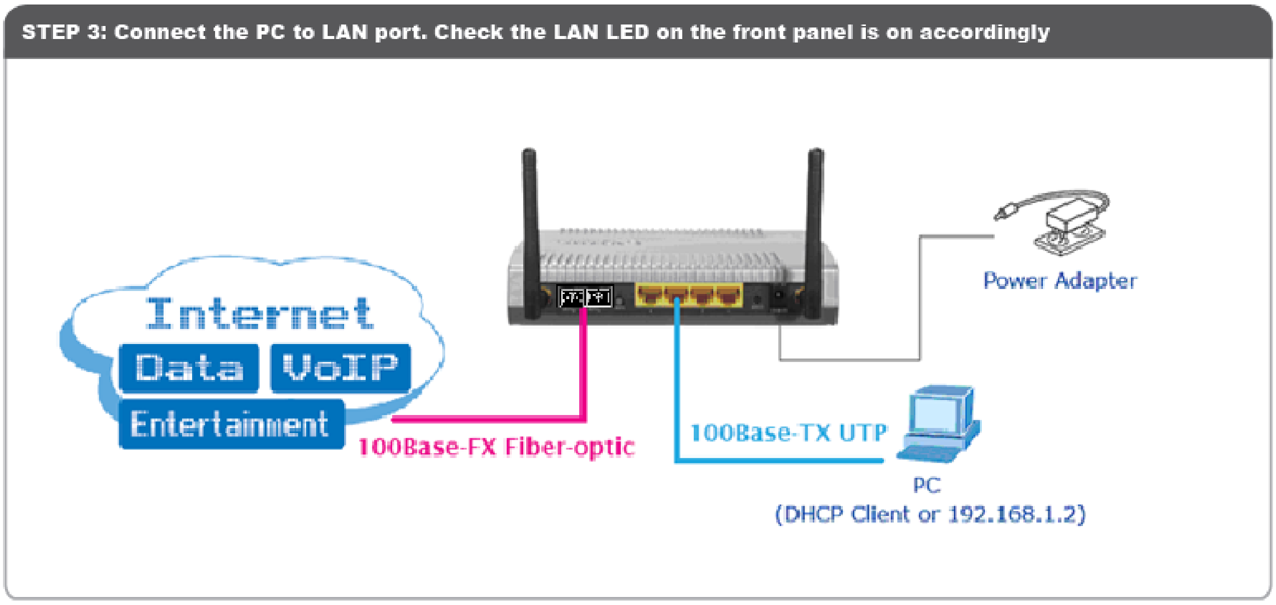
This section describes how to install your Internet Fiber Router and make connections to the Fiber Network. Please read the following topics and perform the procedures in the order being presented. The hardware installation of PLANET Fiber Router do not need software configuration. To install your Fiber Router on a desktop or shelf, simply complete the following steps.



In the following steps, terms of Fiber Router will mean the two series – FRT-40x / FRT-40xN unless model number is specified; and photo of FRT-401N will be used as the photo example.

STEP 1: Locat the FRT-401N on an optimum place, install and adjust the antenna for the best coverage

STEP 2: Connect the Power Adapter to Fiber Router. Check the PWR LED on the front panel is on accordingly

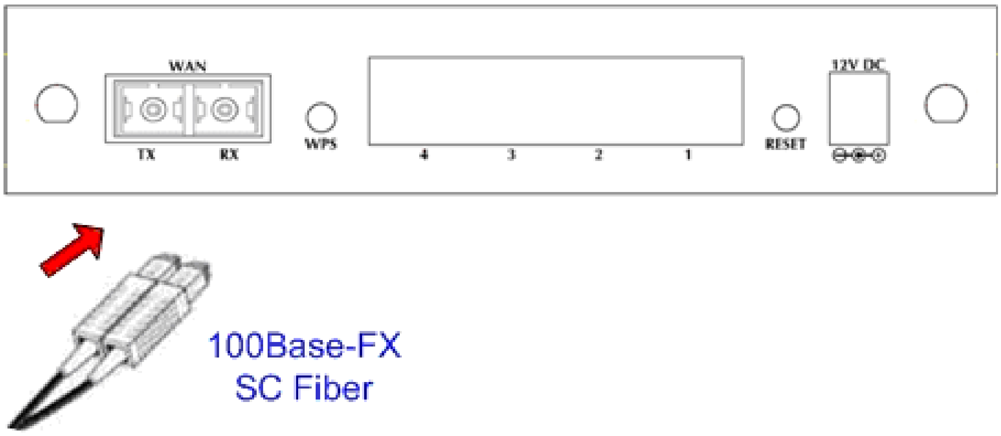

STEP 3: Connect the PC to LAN port. Check the LAN LED on the front panel is on accordingly
Internet
Data
VoIP
Entertainment
100Base-FX Fiber-optic
100Base-TX UTP
Power Adapter
PC
(DHCP Client or 192.168.1.2)

Connect the Fiber-optic cable to WAN port. Check the WAN LED on the front panel is on accordingly.

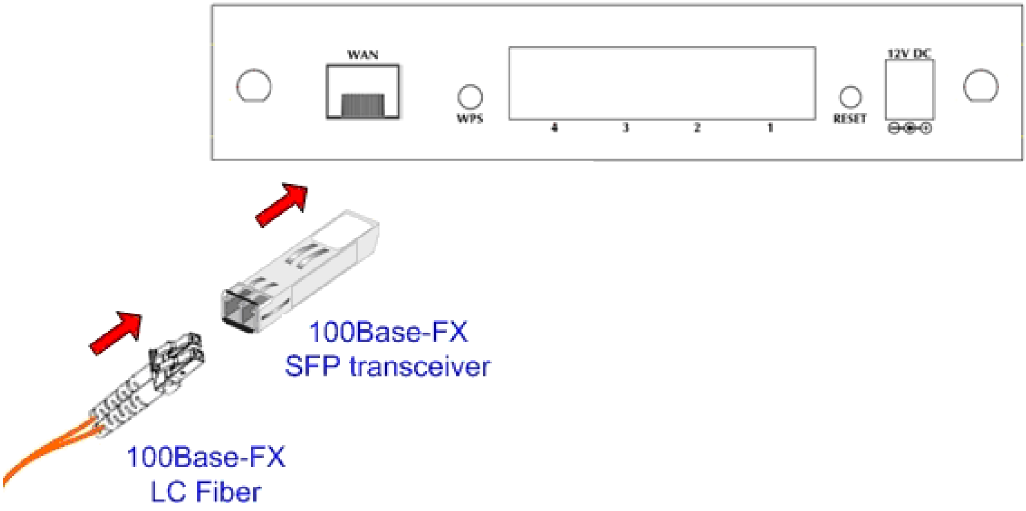
The Fiber types of PLANET Wired / Wireless Fiber Router as the following:

- **FRT-401 / FRT-401N:** 100Base-FX (SC, MM)
- **FRT-401S15 / FRT-401NS15:** 100Base-FX (SC, SM, 15Km)
- **FRT-405 / FRT-405N:** 100Base-FX SFP (LC, MM/SM)

FRT-401 / FRT-401N / FRT-401S15 / FRT-401NS15



FRT-405 / FRT-405N

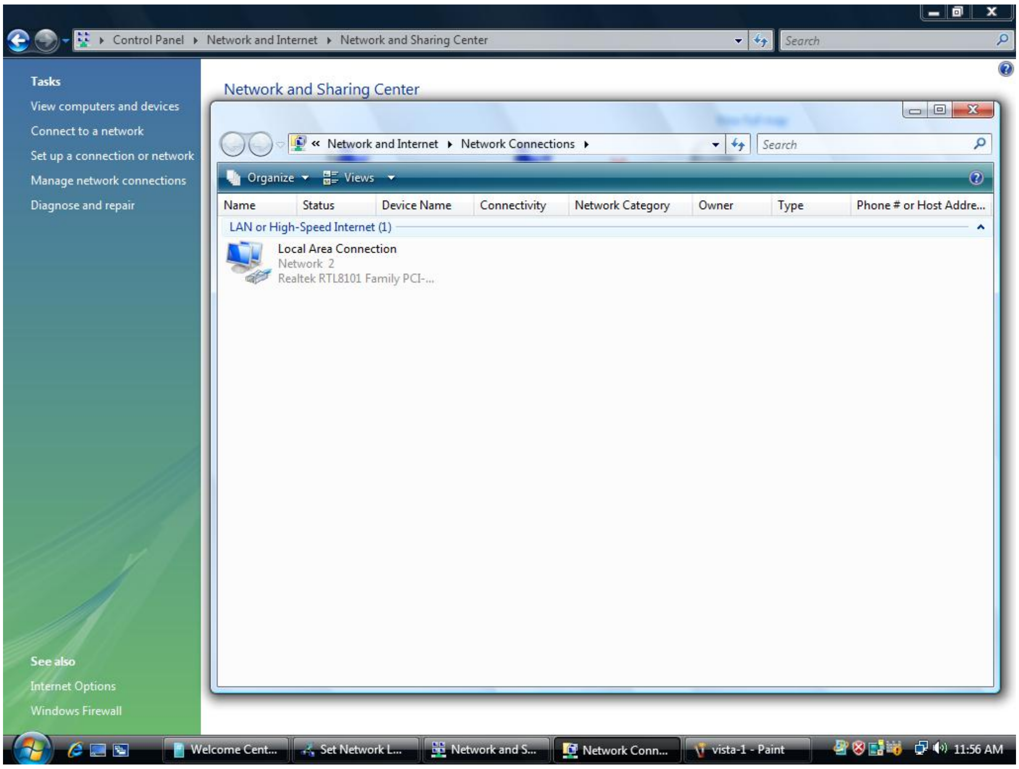


2.3 Configuring the Network Properties

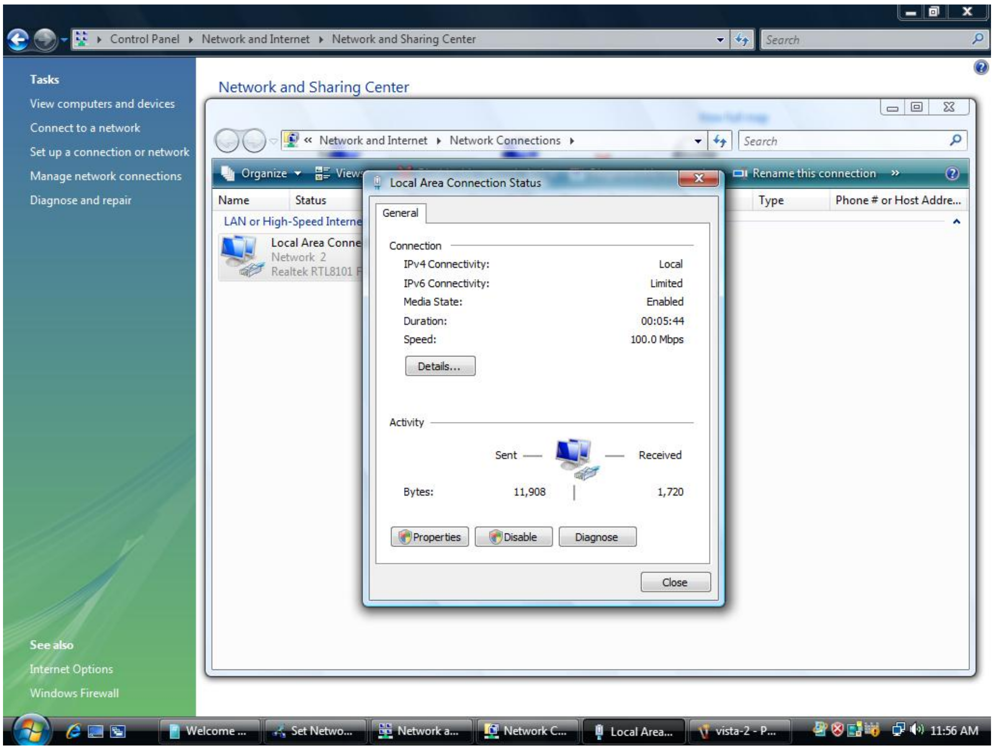
Configuring PC in Windows Vista

1. Go to **Start / Control Panel / Network and Internet / Network and Sharing Center**. Double-click on **Network Connections.**

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



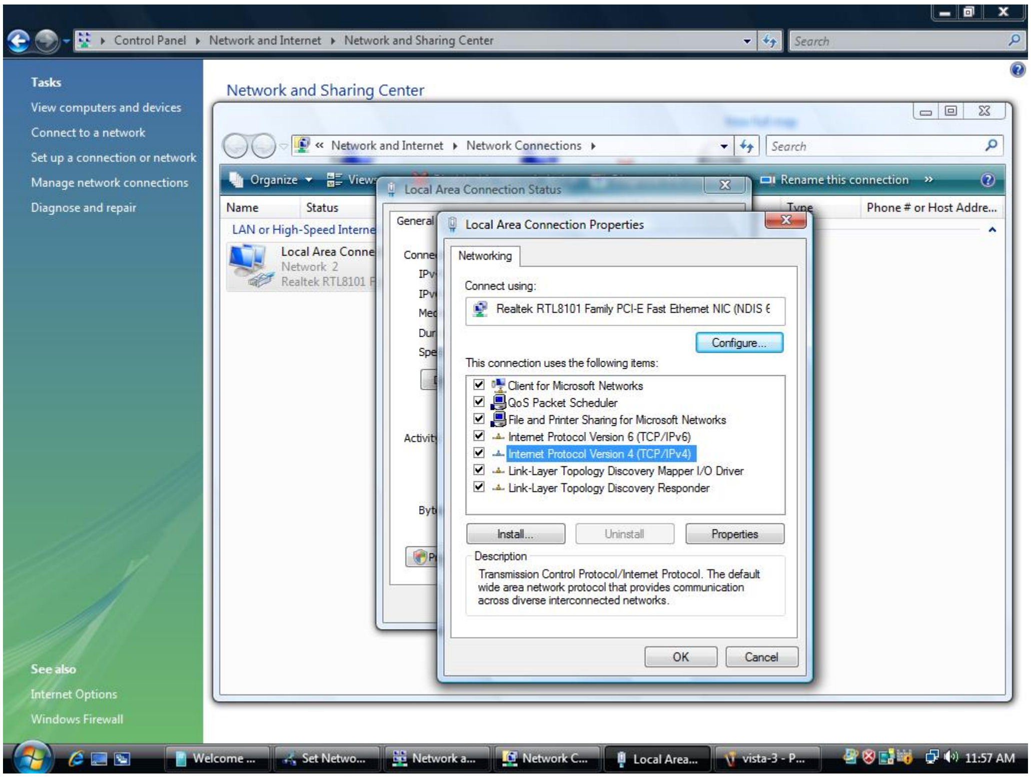
3. In the **Local Area Connection Status** window, click **Properties**.



Connection
IPv4 Connectivity: Local
IPv6 Connectivity: Limited
Media State: Enabled
Duration: 00:05:44
Speed: 100.0 Mbps

Activity
Sent — — Received
Bytes: 11,908 | 1,720

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



Connect using:

Realtek RTL8101 Family PCI-E Fast Ethernet NIC (NDIS 6

This connection uses the following items:

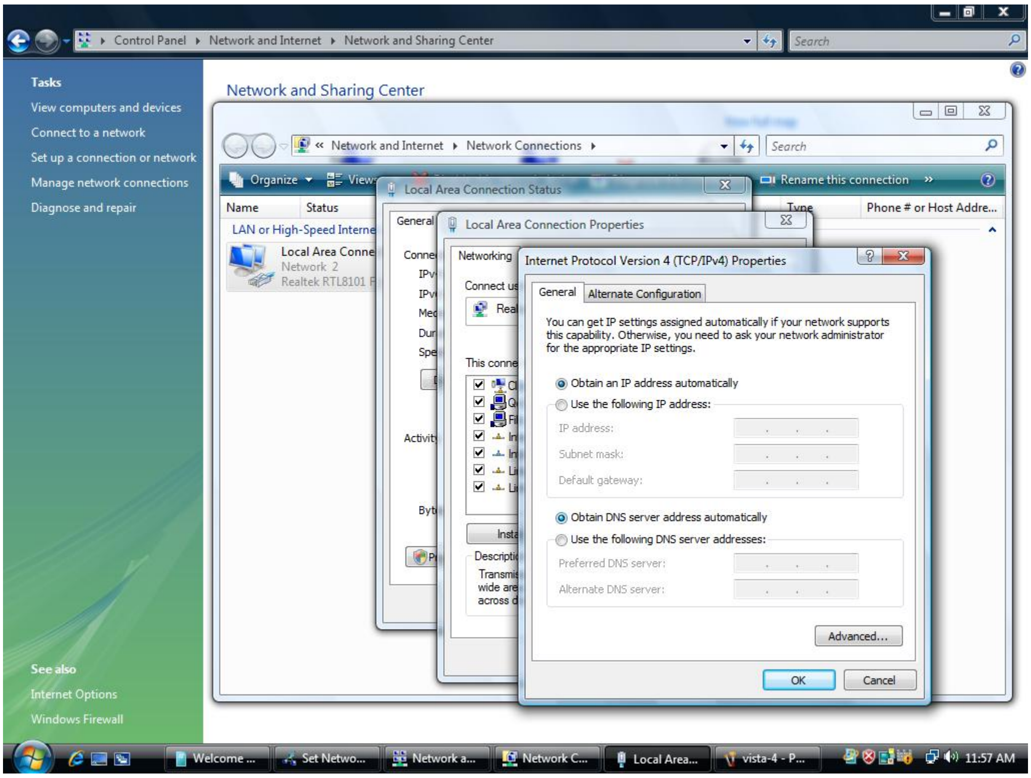
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

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

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

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


Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
See also
Internet Options
Windows Firewall
Network and Sharing Center
« Network and Internet ▸ Network Connections ▸
Organize
Views
Rename this connection
Name
Status
Type
Phone # or Host Addre...
LAN or High-Speed Interne
Local Area Conne
Network 2
Realtek RTL8101 F
Local Area Connection Status
Local Area Connection Properties
Networking
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
Advanced...
OK
Cancel
Welcome ...
Set Netwo...
Network a...
Network C...
Local Area...
vista-4 - P...
11:57 AM

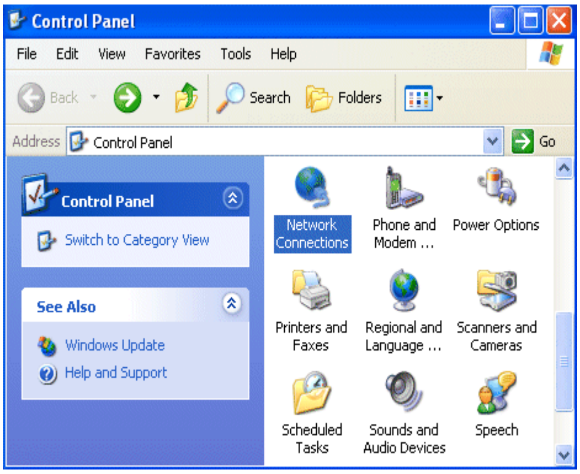
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

- ● 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: . . .

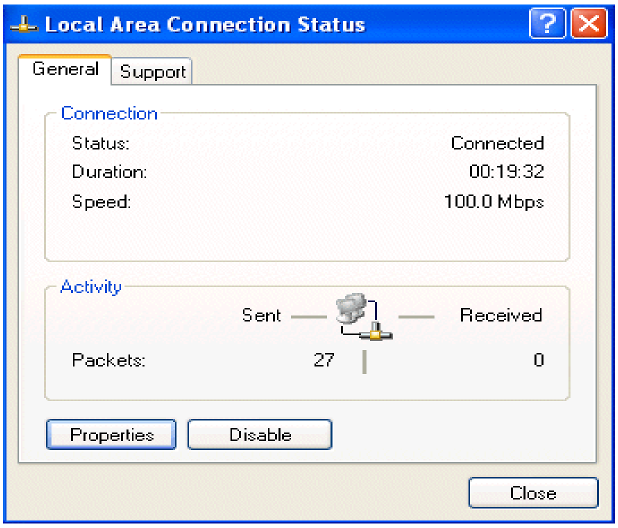
Configuring PC in Windows XP

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

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



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



Connection

Status: Connected

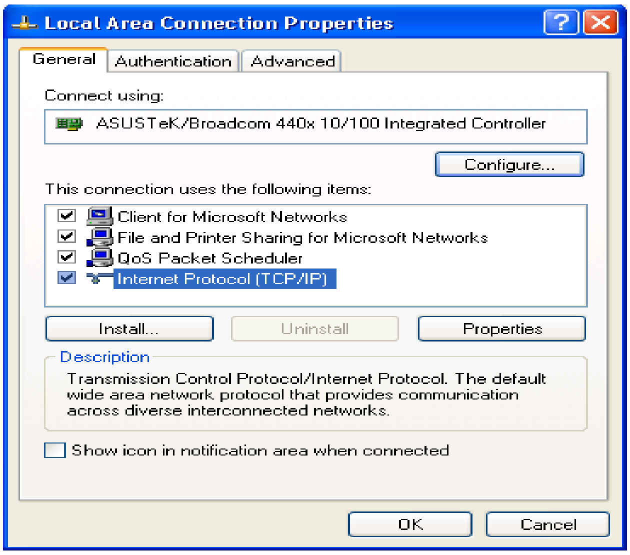
Duration: 00:19:32

Speed: 100.0 Mbps

Activity

	Sent	Received
Packets:	27	0

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



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

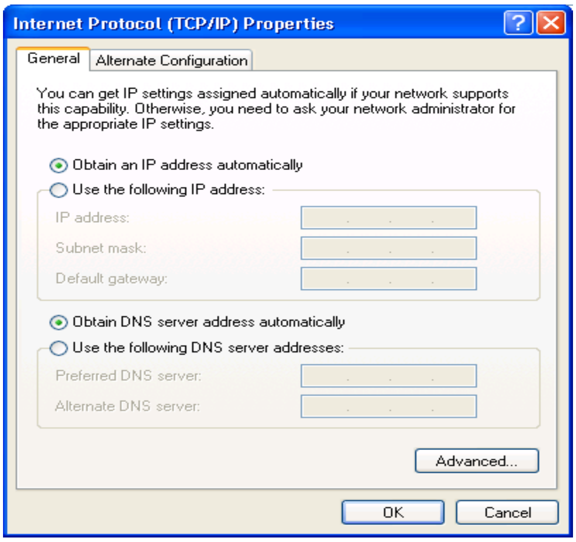
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

OK | Cancel

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

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



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

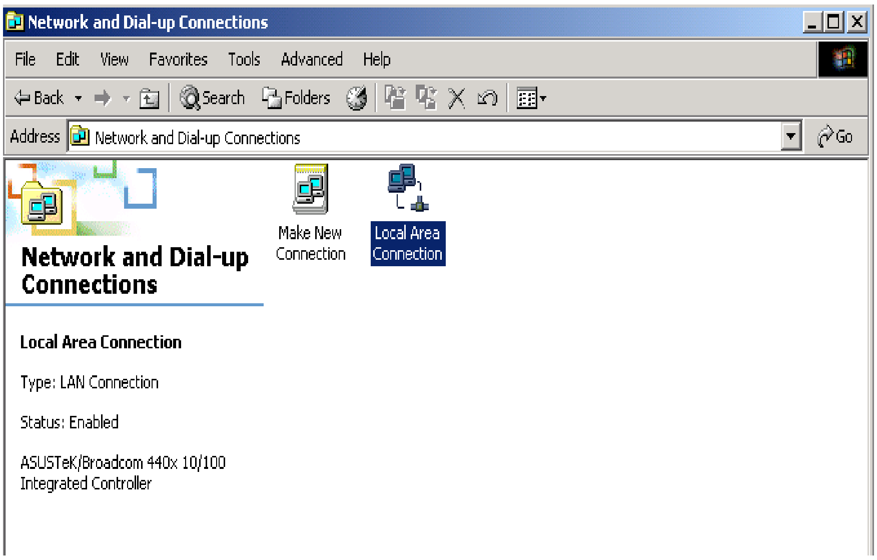
Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Local Area Connection

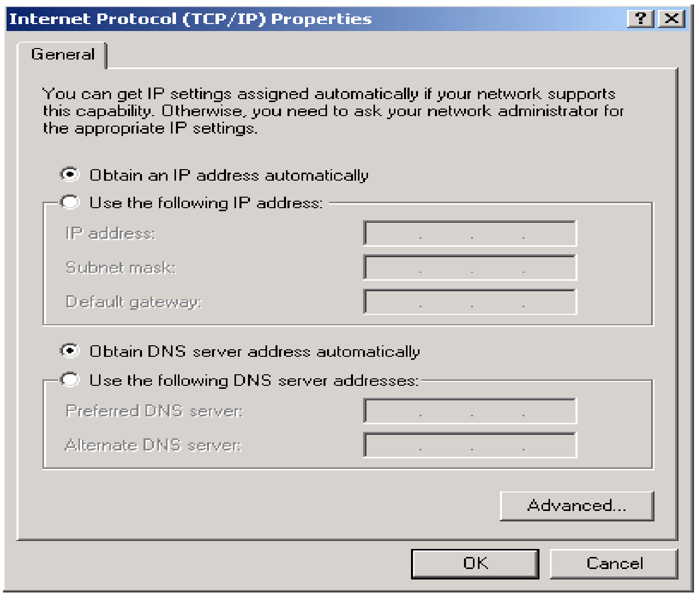
Local Area Connection

Type: LAN Connection

Status: Enabled

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

3. In the **Local Area Connection Status** window click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
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

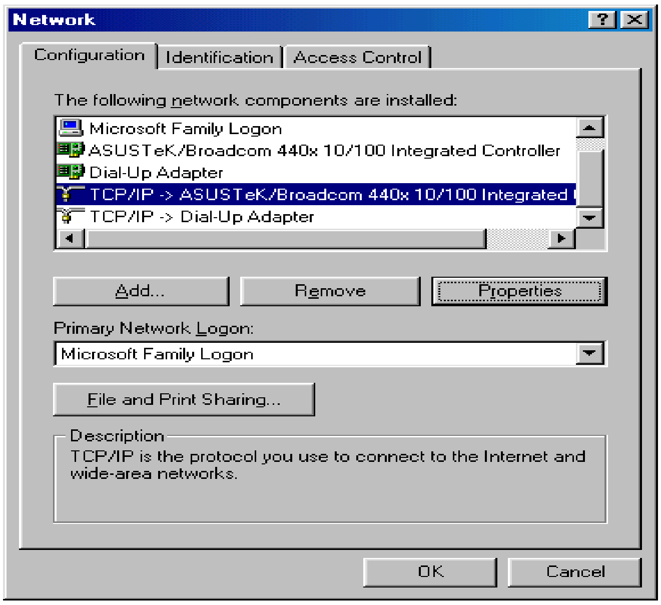
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Configuring PC in Windows 98/Me

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP → NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.



The following network components are installed:

- Microsoft Family Logon
- ASUSTeK/Broadcom 440x 10/100 Integrated Controller
- Dial-Up Adapter
- TCP/IP -> ASUSTeK/Broadcom 440x 10/100 Integrated
- TCP/IP -> Dial-Up Adapter

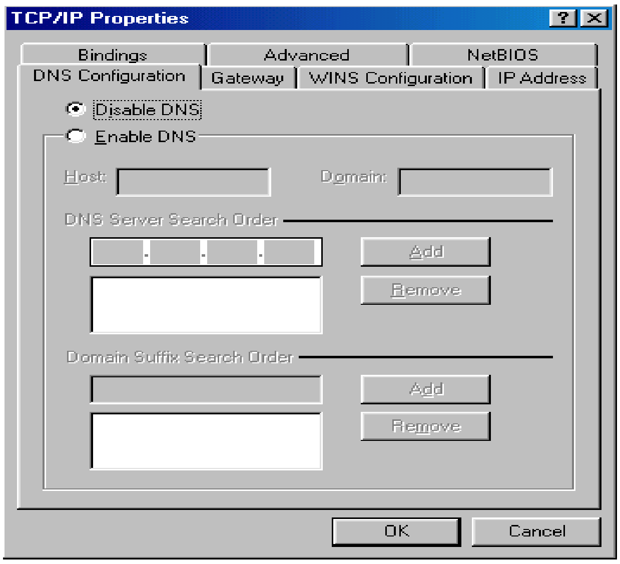
Primary Network Logon: Microsoft Family Logon

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3. Select the **Obtain an IP address automatically** radio button.

4. Then select the **DNS Configuration** tab.

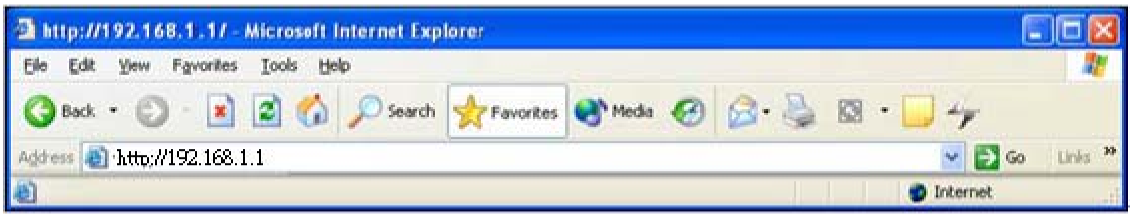
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



● Disable DNS
○ Enable DNS

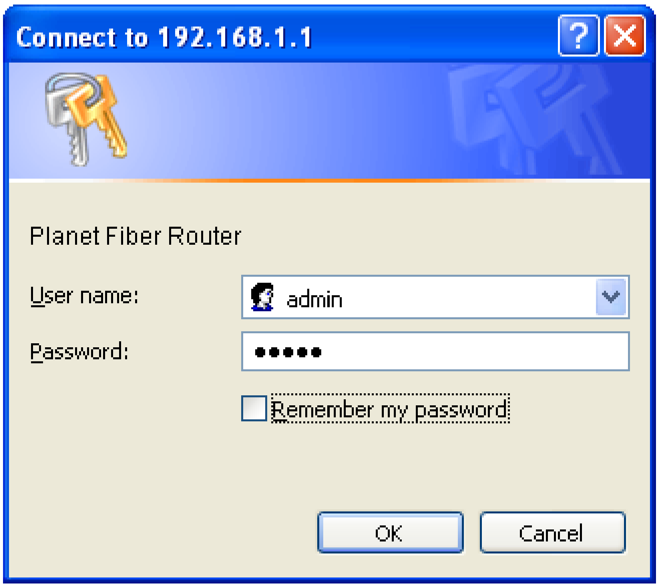
2.4 Configuring with Web Browser

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/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Internet

Address http://192.168.1.1

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”**.



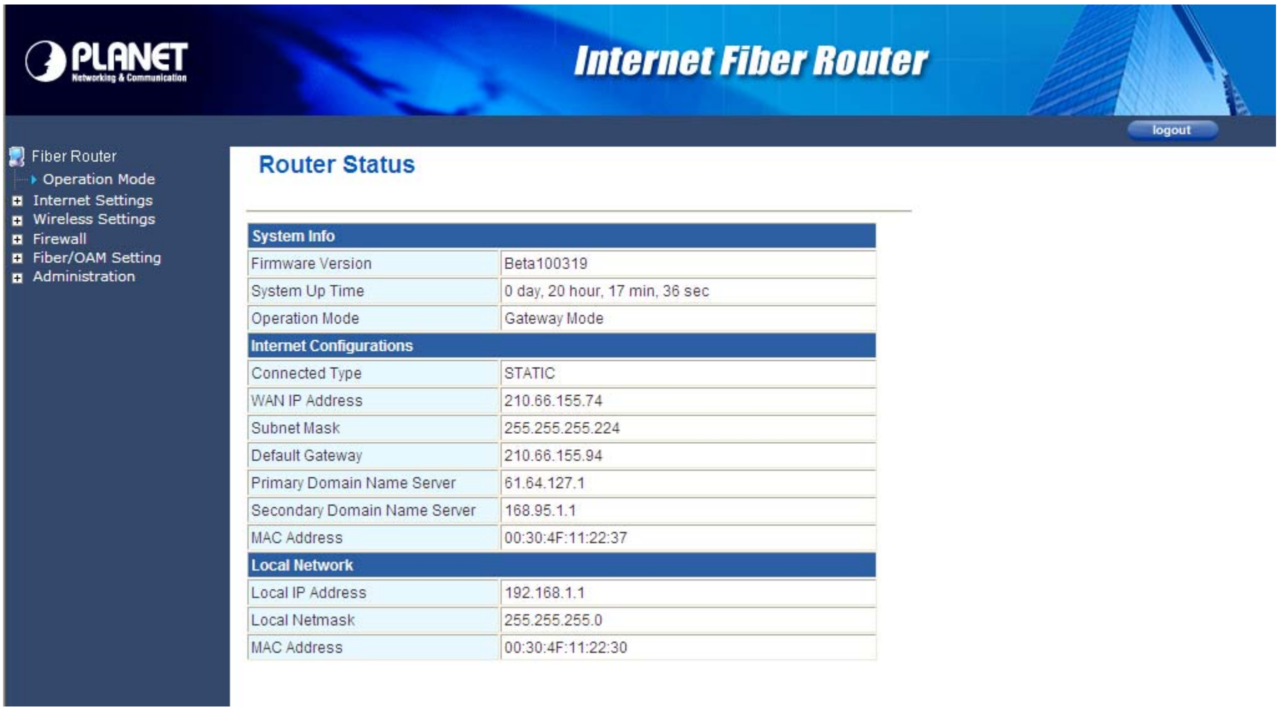
Planet Fiber Router

User name: admin

Password: ●●●●●

□ Remember my password

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.



Router Status

System Info	
Firmware Version	Beta100319
System Up Time	0 day, 20 hour, 17 min, 36 sec
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	STATIC
WAN IP Address	210.66.155.74
Subnet Mask	255.255.255.224
Default Gateway	210.66.155.94
Primary Domain Name Server	61.64.127.1
Secondary Domain Name Server	168.95.1.1
MAC Address	00:30:4F:11:22:37
Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:30:4F:11:22:30

3. Web Configuration Management

Determine your connection settings

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

Connecting the Fiber Router to your network

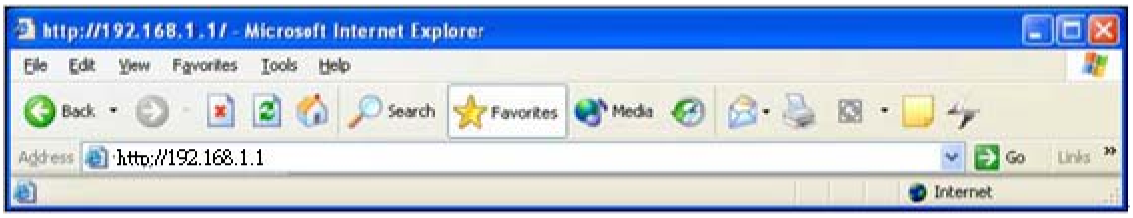
Unlike a simple hub or switch, the setup of the Fiber Router consists of more than simply plugging everything together. Because the Router acts as a DHCP server, you will have to set some values within the Router, and also configure your networked PCs to accept the IP Addresses the Router chooses to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

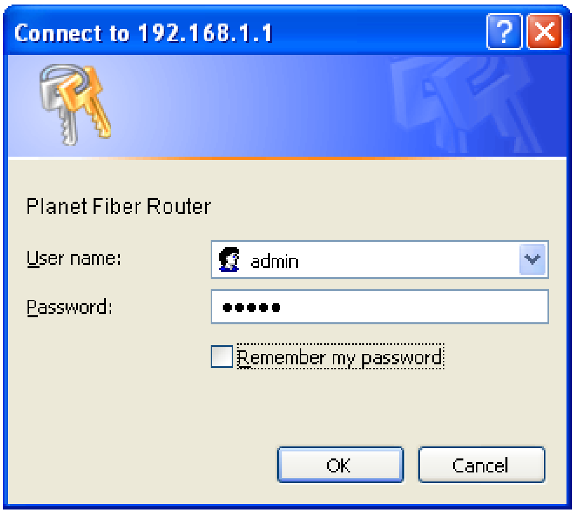
Save this address in your Favorites for future reference.



http://192.168.1.1/ - Microsoft Internet Explorer

Address http://192.168.1.1

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.



Connect to 192.168.1.1

Planet Fiber Router

User name: admin

Password: •••••

□ Remember my password

3.1 Operation Mode

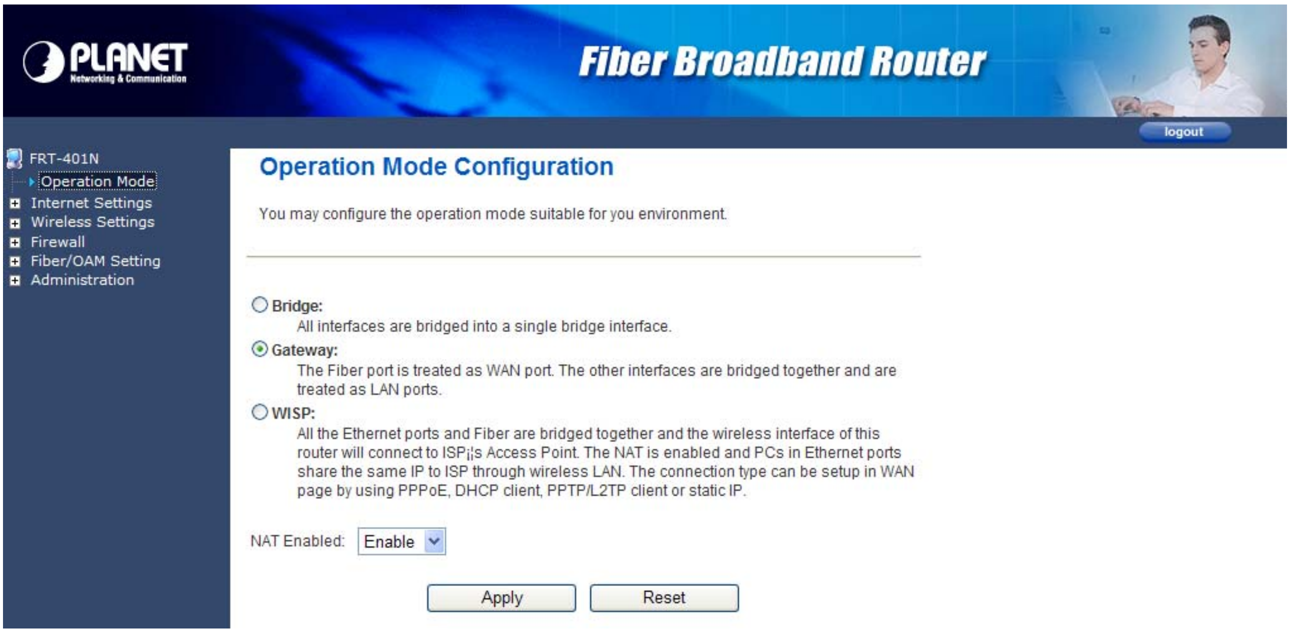
The Fiber Router supports three operation modes – Router, Bridge and WISP **(WISP mode is only supported for wireless fiber router)**. Currently, it comes pre-configured with Router mode. Note that, routing mode and bridging mode cannot be used simultaneously.

For **Bridge mode**, all interfaces are bridged into a single bridge interface.

For **Router mode**, the Fiber port is treated as WAN port. The other interfaces are bridged together and are treated as LAN ports.

For **WISP Mode (For wireless model)**, all the Ethernet ports are bridged together and the wireless interface of this router will connect to ISP's Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP.

⚠	If you select **Bridge operation mode**, WAN configuration in Internet Settings are not available. (Firewall functions on the left page are not available.)



Operation Mode Configuration

You may configure the operation mode suitable for you environment.

○ Bridge:
All interfaces are bridged into a single bridge interface.

● Gateway:
The Fiber port is treated as WAN port. The other interfaces are bridged together and are treated as LAN ports.

○ WISP:
All the Ethernet ports and Fiber are bridged together and the wireless interface of this router will connect to ISP¡¦s Access Point. The NAT is enabled and PCs in Ethernet ports share the same IP to ISP through wireless LAN. The connection type can be setup in WAN page by using PPPoE, DHCP client, PPTP/L2TP client or static IP.

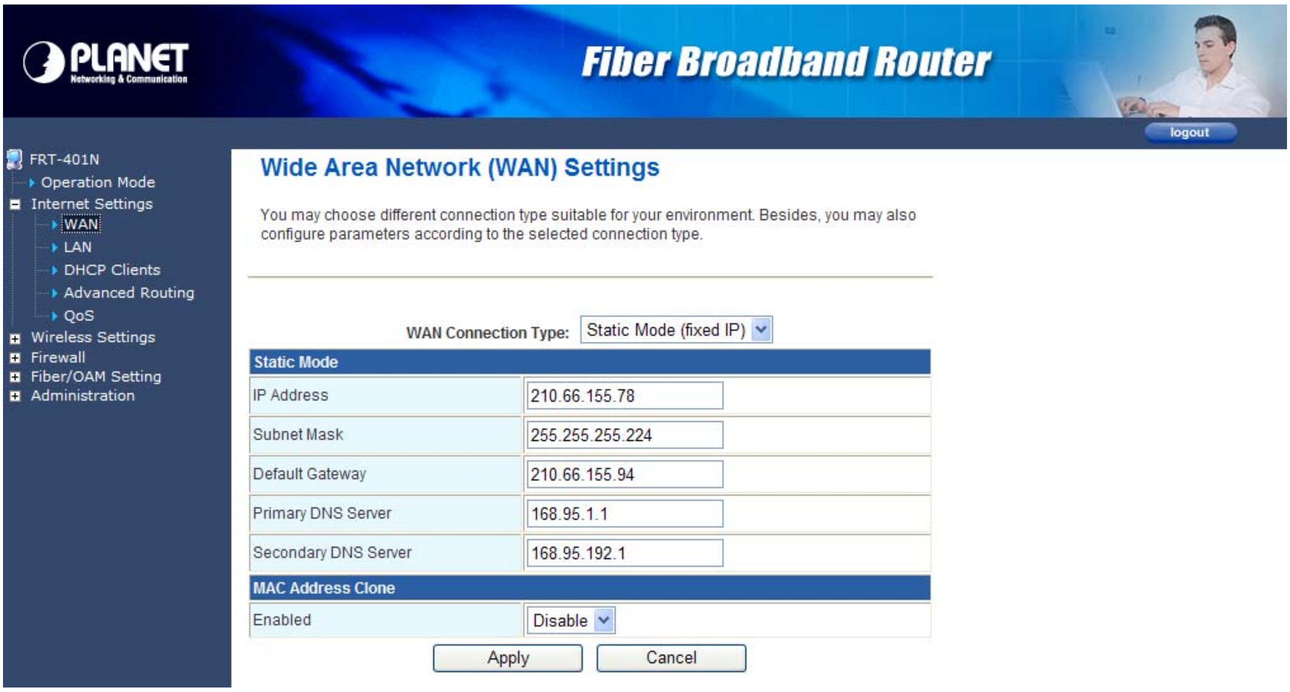
NAT Enabled: Enable

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

3.2 Internet Settings

3.2.1 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

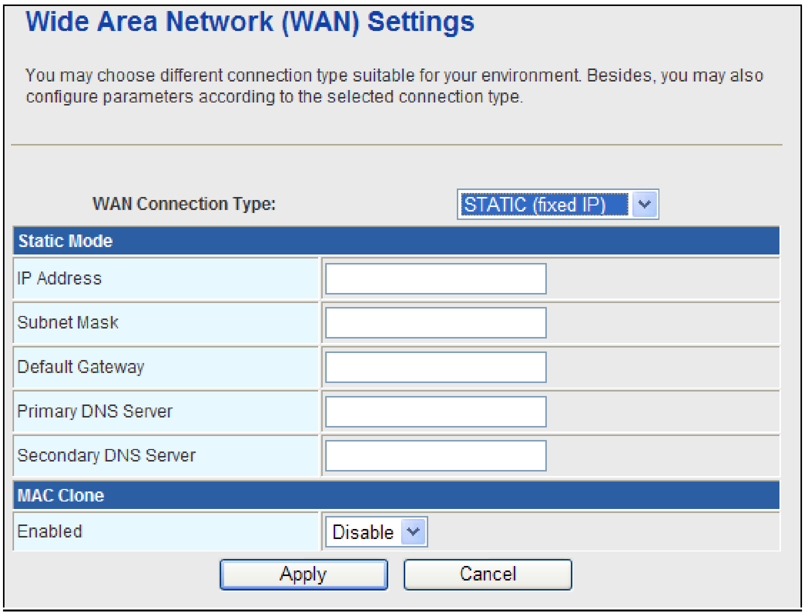
You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: Static Mode (fixed IP)

Static Mode	
IP Address	210.66.155.78
Subnet Mask	255.255.255.224
Default Gateway	210.66.155.94
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.192.1
MAC Address 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

Static Mode

- **IP Address:** Enter the IP address of WAN port.
- **Subnet Mask:** Enter IP subnet mask of WAN port.
- **Default Gateway:** Enter the default gateway address of WAN port.
- **Primary DNS Server:** Primary DNS Server f of WAN port.
- **Secondary DNS Server:** Secondary DNS Server of WAN port.

MAC Clone

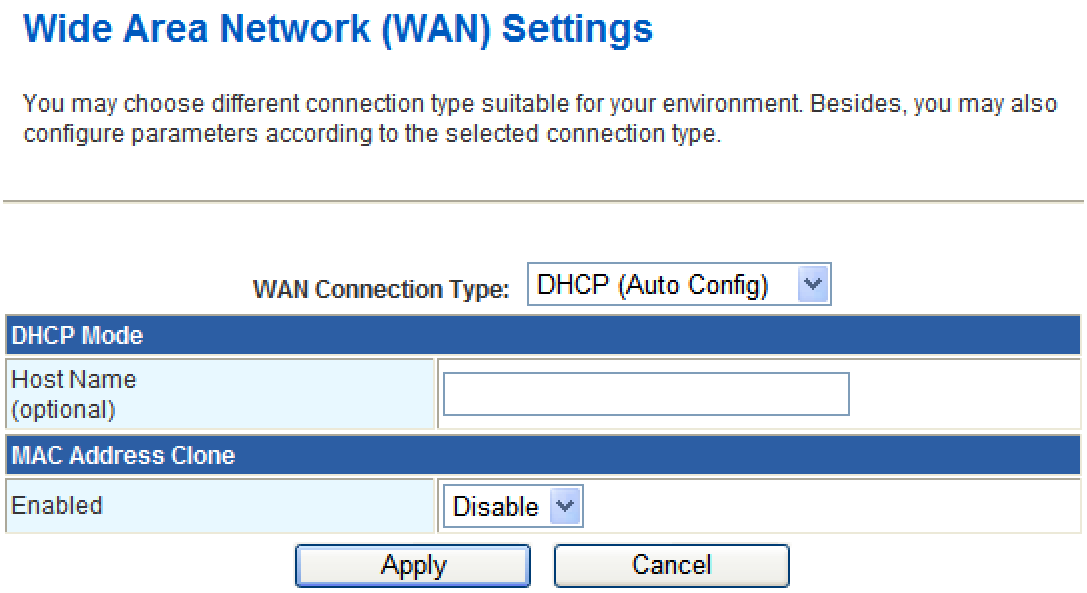
MAC Clone provides WAN to connect to a MAC address.

- **Enabled:** Enable or disable MAC clone.

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

➢ 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	
Host Name (optional)	
MAC Address Clone	
Enabled	Disable

MAC Clone

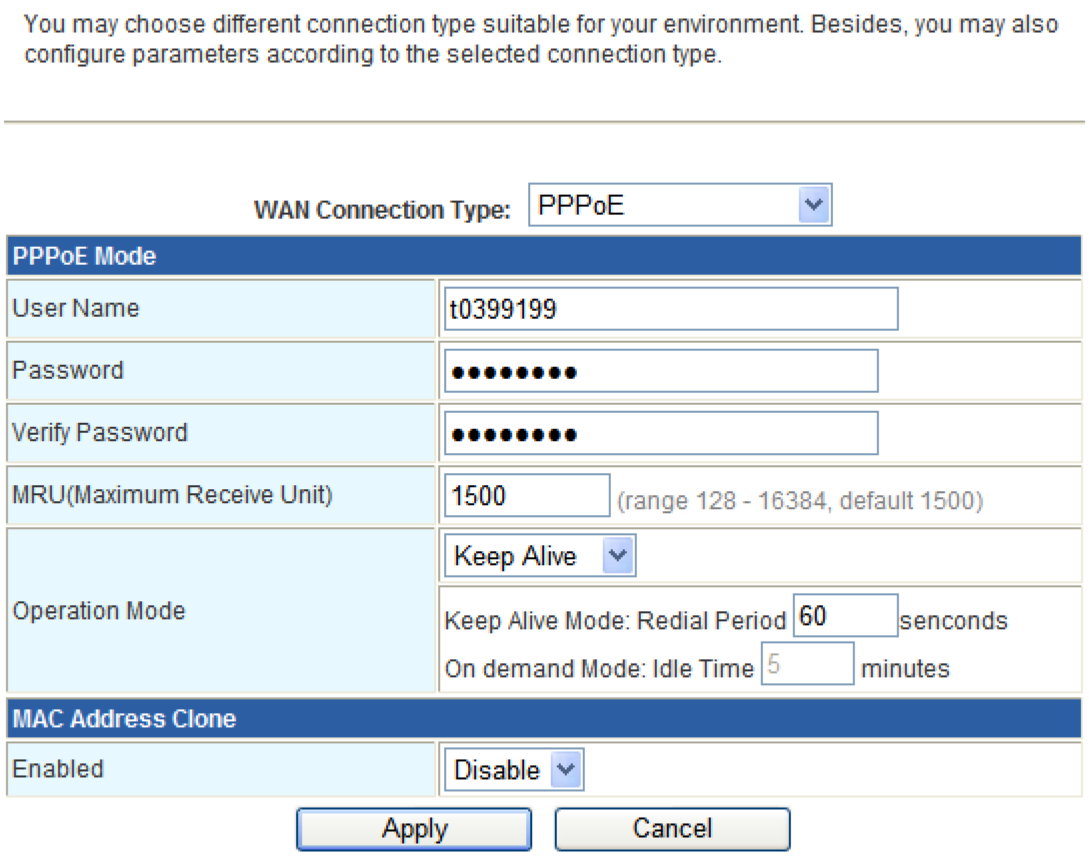
MAC Clone provides WAN to connect to a MAC address.

- **Enabled:** Enable or disable MAC clone.

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

➢ 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.



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	t0399199
Password	●●●●●●●●
Verify Password	●●●●●●●●
MRU(Maximum Receive Unit)	1500 (range 128 - 16384, default 1500)
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes
MAC Address Clone	
Enabled	Disable

PPPoE Mode

- **User Name:** User name of PPPoE account
- **Password:** Password of PPPoE account
- **Verify Password:** Enter the password of PPPoE account again.
- **Operation Mode:** It provides two types of operation modes.
  - **Keep Alive** means keeping on-line mode. You can set the redial period in the field. When the redial period expires, Router will execute dial-up again to keep online.
  - **On Demand** means executing dial-up on demand. Within the preset idle time, if Router does not detect the flow of the user continuously, Router automatically stops the PPPOE connection. Once it detects the flow (e.g., accessing a webpage), the router restarts the PPPOE dial-up.

MAC Clone

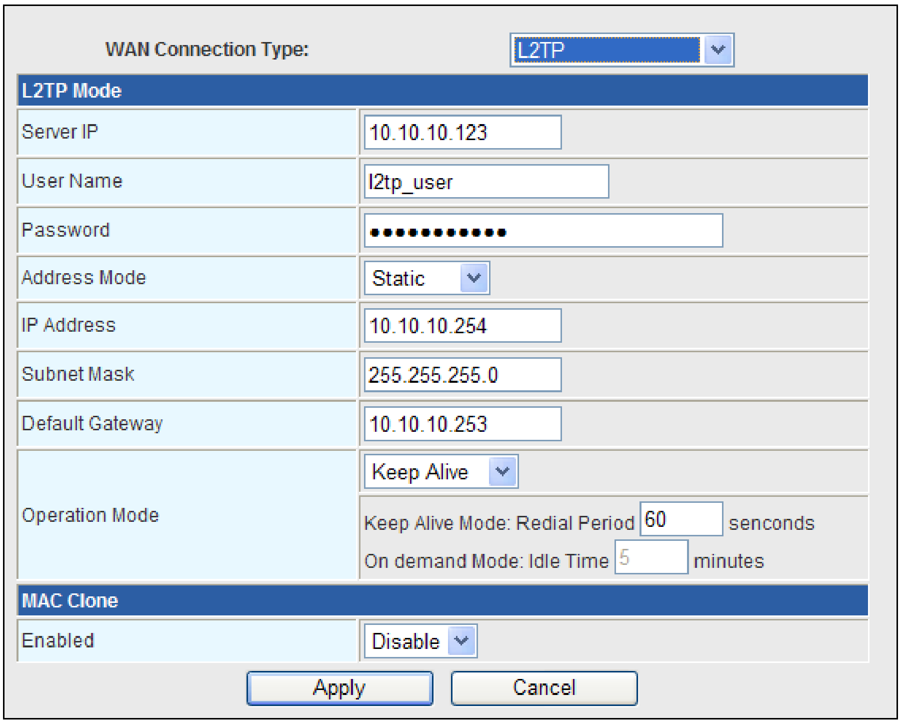
- **Enabled:** Enable or disable.

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

➢ 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.



WAN Connection Type: L2TP

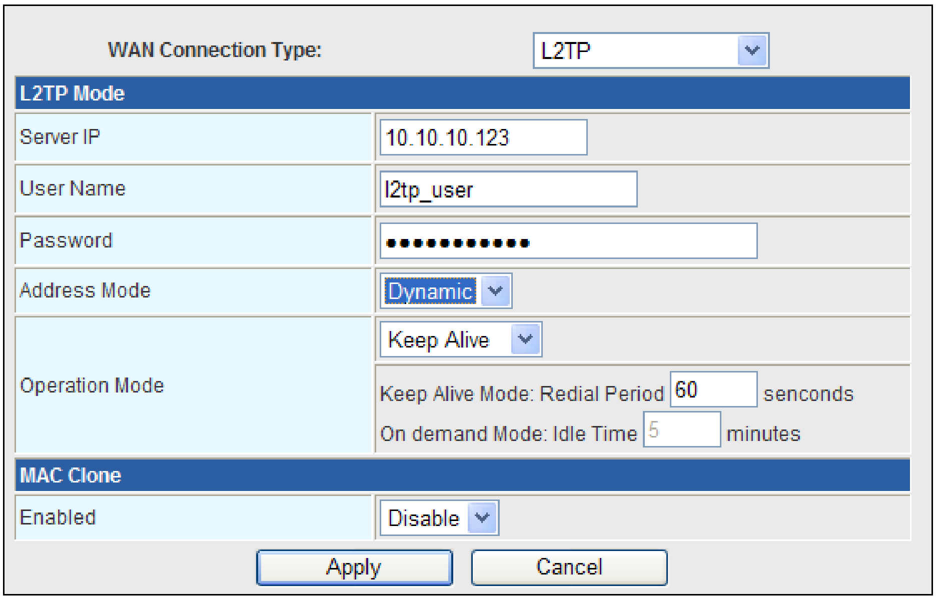
L2TP Mode

Server IP	10.10.10.123
User Name	l2tp_user
Password	●●●●●●●●●●●
Address Mode	Static
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.253
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes

MAC Clone

Enabled	Disable

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



WAN Connection Type: L2TP

L2TP Mode

Server IP	10.10.10.123
User Name	l2tp_user
Password	●●●●●●●●●●●
Address Mode	Dynamic
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes

MAC Clone

Enabled	Disable

L2TP Mode

- **Server IP:** Address of L2TP server.
- **User Name:** The user name of L2TP account.
- **Password:** The password of L2TP account.
- **IP Address:** IP address of WAN port.
- **Subnet Mask:** Subnet mask of WAN port.
- **Default Gateway:** The default gate way of WAN port.
- **Operation Mode:** It provides two types of operation modes.
    - **Keep Alive** means keeping on-line mode. You can set the redial period in the field. When the redial period expires, Router will execute dial-up again to keep online.
    - **On Demand** means executing dial-up on demand. Within the preset idle time, if Router does not detect the flow of the user continuously, Router automatically stops the PPPOE connection. Once it detects the flow (e.g., accessing a webpage), the router restarts the PPPOE dial-up.

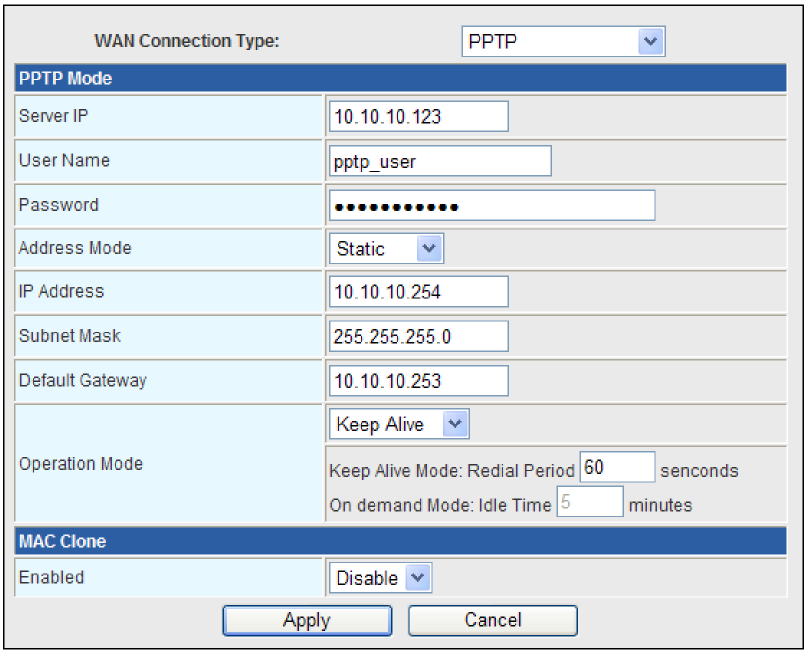
MAC Clone

- **Enabled:** Enable or disable.

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

➢ PPTP

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



WAN Connection Type:	PPTP
PPTP Mode	
Server IP	10.10.10.123
User Name	pptp_user
Password	●●●●●●●●●●●
Address Mode	Static
IP Address	10.10.10.254
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.253
Operation Mode	Keep Alive Keep Alive Mode: Redial Period 60 senconds On demand Mode: Idle Time 5 minutes
MAC Clone	
Enabled	Disable

PPTP Mode

- **Server IP:** Address of PPTP server.
- **User Name:** The user name of PPTP account.
- **Password:** The password of PPTP account.
- **IP Address:** IP address of WAN port.
- **Subnet Mask:** Subnet mask of WAN port.
- **Default Gateway:** The default gate way of WAN port.
- **Operation Mode:** It provides two types of operation modes.
  - **Keep Alive** means keeping on-line mode. You can set the redial period in the field. When the redial period expires, Router will execute dial-up again to keep online.
  - **On Demand** means executing dial-up on demand. Within the preset idle time, if Router does not detect the flow of the user continuously, Router automatically stops the PPPOE connection. Once it detects the flow (e.g., accessing a webpage), the router restarts the PPPOE dial-up.

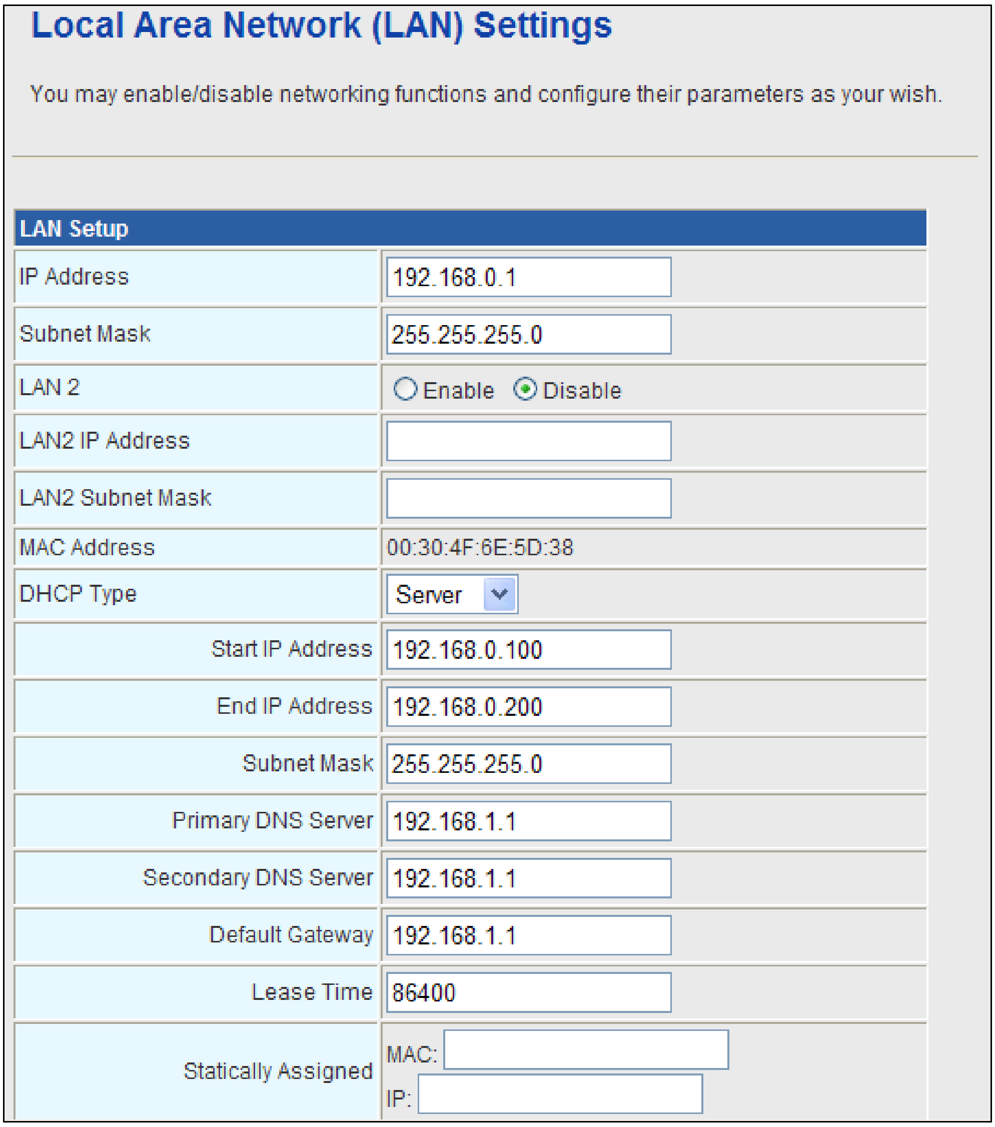
MAC Clone

- **Enabled:** Enable or disable.

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

3.2.2 LAN

This page allows you may 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	192.168.0.1
Subnet Mask	255.255.255.0
LAN 2	○ Enable ● Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:30:4F:6E:5D:38
DHCP Type	Server
Start IP Address	192.168.0.100
End IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Primary DNS Server	192.168.1.1
Secondary DNS Server	192.168.1.1
Default Gateway	192.168.1.1
Lease Time	86400
Statically Assigned	MAC: IP:

- **IP Address:** Enter the IP address of LAN port.
- **Subnet mask:** Enter the subnet mask of LAN port.
- **LAN2:** The second IP switch of LAN port. You can enable or disable this function.
- **LAN2 IP Address:** The second IP address of LAN port.
- **LAN2 Subnet Mask:** The second IP Subnet Mask of LAN port.
- **MAC Address:** MAC address of LAN port (Read-only).
- **DHCP Type:** You can select **Server** or **Disable**. If you select Disable, the DHCP service of LAN port is disabled. After selecting Server, you can set the following items.
- **Start IP Address:** The first IP address that DHCP server assigns.
- **End IP Address:** The last IP address that DHCP server assigns.
- **Subnet Mask:** The subnet mask of dynamic IP.

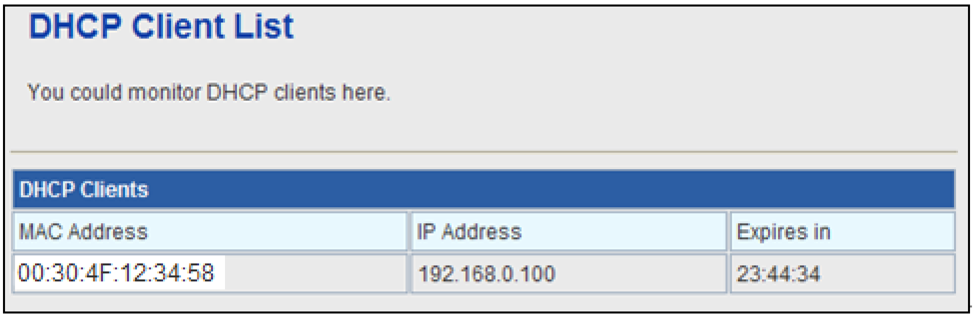
- **Primary DNS Server:** The primary DNS server address.
- **Secondary DNS Server:** The secondary DNS Server address.
- **Default Gateway:** The default gateway that DHCP server assigns.
- **Lease Time:** Lease time of the IP address.
- **Statically Assigned:** Assign IP to the assigned MAC address. Enter the assigned MAC address and IP in the corresponding fields.
- **802.1d Spanning Tree:** Spanning Tree Protocol. You can select Enable or Disable.
- **IGMP Proxy:** You can select Enable or Disable.
- **UPNP:** Universal Plug and Play (UPNP).You can select Enable or Disable.
- **Router Advertisement:** You can select Enable or Disable.
- **DNS Proxy:** You can select Enable or Disable.

After finishing setting, click **Apply** to save the settings and make the new configuration take effect.

Click **Cancel** to close without saving.

3.2.3 DHCP clients

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



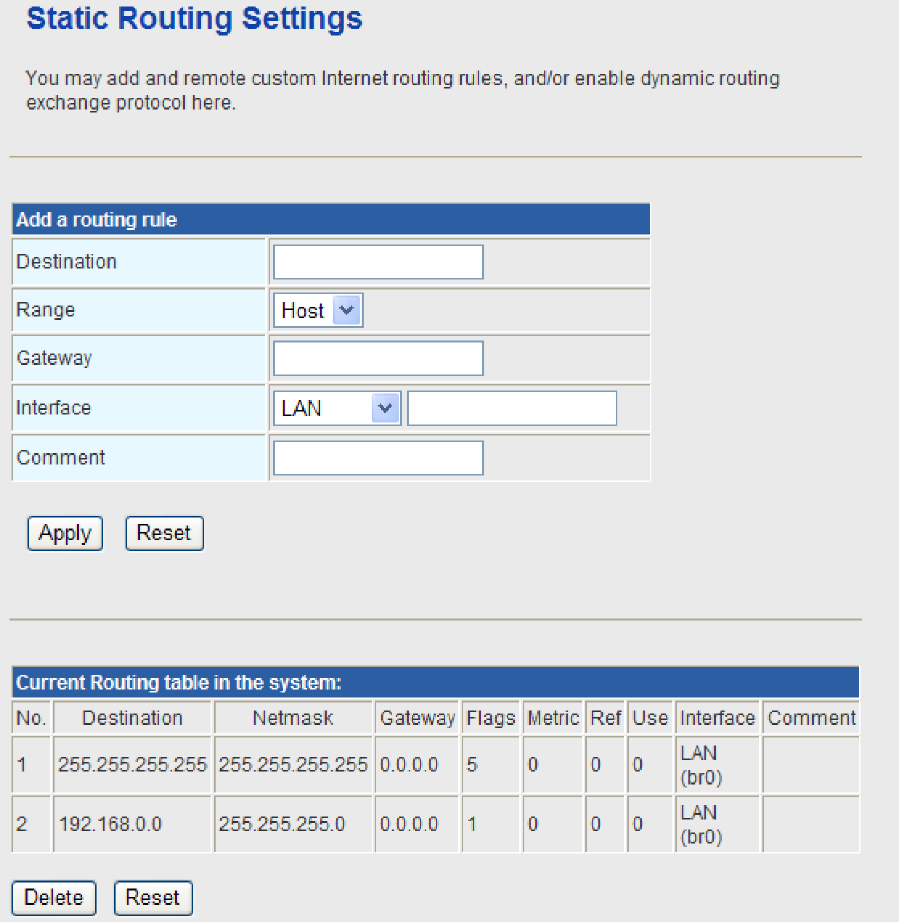
DHCP Client List

You could monitor DHCP clients here.

DHCP Clients		
MAC Address	IP Address	Expires in
00:30:4F:12:34:58	192.168.0.100	23:44:34

3.2.4 Advanced Routing

You can add or delete routing rules, enable or disable dynamic routing protocol in 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	

Current Routing table in the system:

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN (br0)	
2	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN (br0)	

Add a routing rule

- **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.

After finishing the setting above, click **Apply** to make the new routing rule take effect. Otherwise, click **Reset** to cancel the new routing rule.

Current Routing table in the system

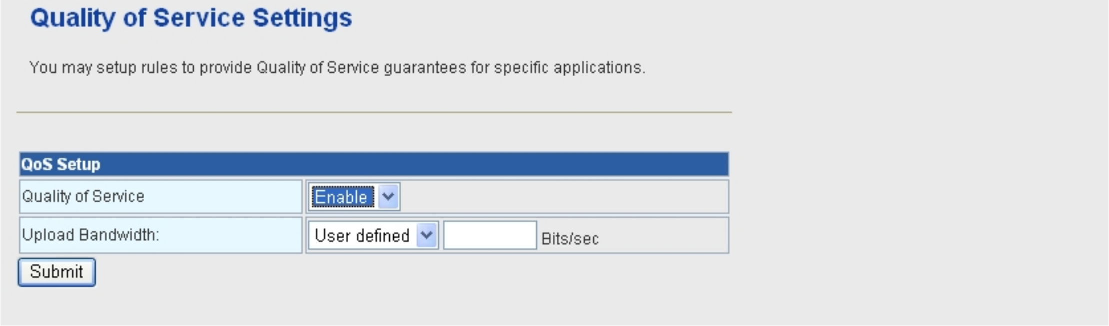
You can delete or reset the routing rules.

Dynamic Routing Settings

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

3.2.5 QoS

You may set up rules to provide Quality of Service (QoS) guarantee for some specific applications. In the page, you can enable or disable Quality of Service. After enabling QoS, you can set upload bandwidth and download bandwidth.



Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup

Quality of Service: Enable

Upload Bandwidth: User defined Bits/sec

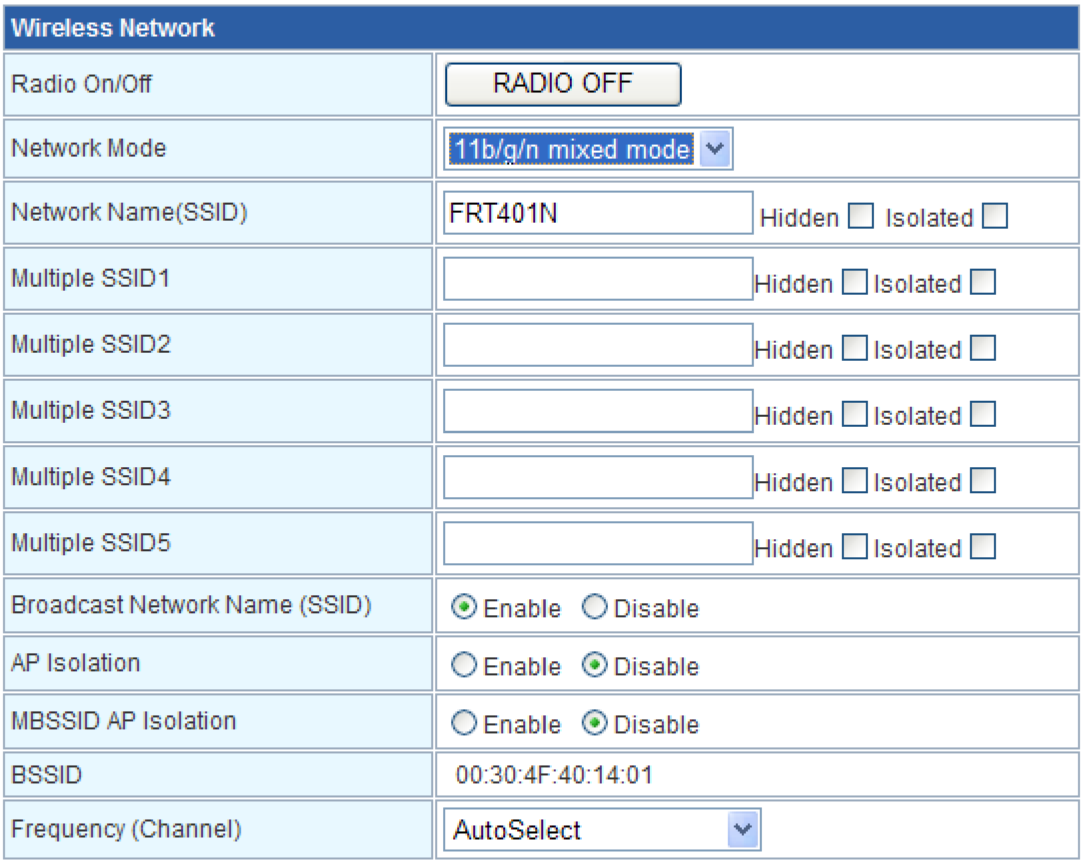
- **Upload Bandwidth:** You can select the proper bandwidth in the drop-down list. The value is from **64K** to **60M**. You can also set the bandwidth by selecting **User defined** and enter the proper bandwidth in the field.
- **Download Bandwidth:** You can select the proper bandwidth in the drop-down list. The value is from **64K** to **60M**. You can also set the bandwidth by select **User defined** and enter the proper bandwidth in the field.

After finishing the setting above, click **Submit** to save the new configuration.

3.3 Wireless Setting (For FRT-401N / 401NS15 / 405N)

3.3.1 Basic

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



Wireless Network

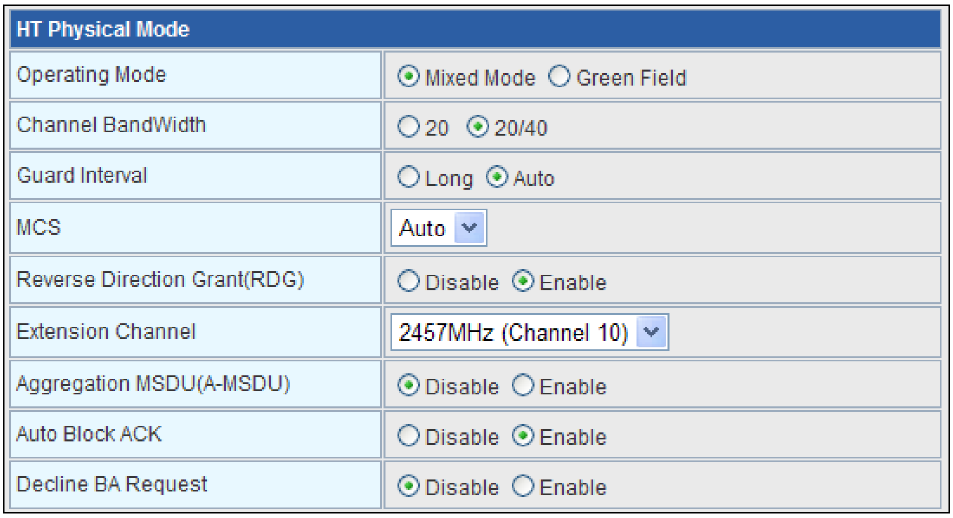
Radio On/Off	RADIO OFF
Network Mode	11b/g/n mixed mode
Network Name(SSID)	FRT401N Hidden □ Isolated □
Multiple SSID1	Hidden □ Isolated □
Multiple SSID2	Hidden □ Isolated □
Multiple SSID3	Hidden □ Isolated □
Multiple SSID4	Hidden □ Isolated □
Multiple SSID5	Hidden □ Isolated □
Broadcast Network Name (SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:30:4F:40:14:01
Frequency (Channel)	AutoSelect

Wireless Network

- **Radio On/Off:** Enable or disable the wireless LAN.
- **Network Mode:** There are 6 modes: 11b only, 11g only, 11n only, 11b/g mixed, and 11b/g/n mixed mode.
- **Network Name (SSID):** The service set identification (SSID) is a unique name to identify the router in the wireless LAN. Wireless stations associating to the router must have the same SSID. Enter a descriptive name. Its length is up to 32 characters.
- **Multiple SSID 1/2/3/4/5:** There are 5 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 can not 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



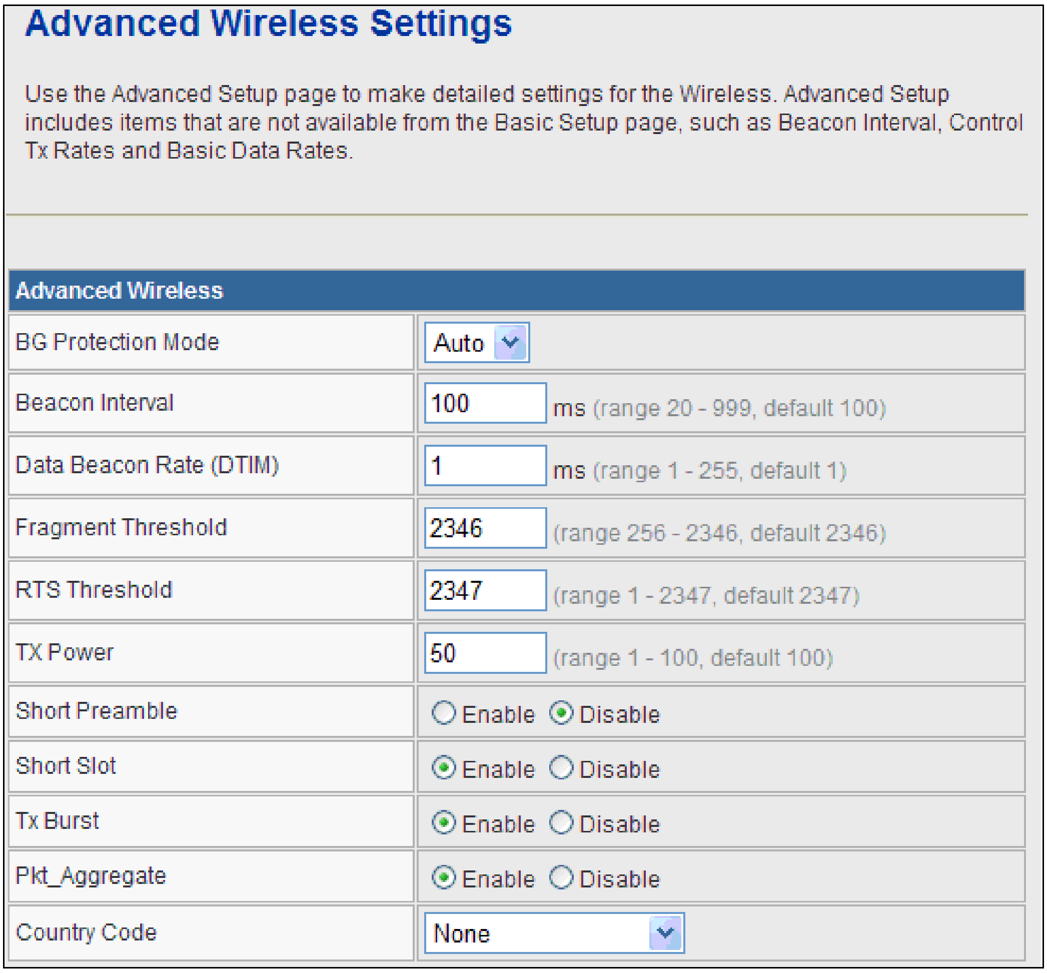
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
MCS	Auto
Reverse Direction Grant(RDG)	○ Disable ● Enable
Extension Channel	2457MHz (Channel 10)
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable

HT Physical Mode

- **Operation Mode:** Select Mixed Mode or Green Field.
- **Channel Bandwidth:** Select 20 or 20/40.
- **Guard Interval:** Select Long or Auto.
- **MCS:** Select the proper value between 0 and15 or 32. Auto is the default value.
- **Reverse Direction Grant (RDG):** Select Disable or Enable.
- **Extension Channel:** Select the proper extension channel in the drop-down list.
- **Aggregation MSDU (A-MSDU):** Select Disable or Enable.
- **Auto Block ACK:** Select Disable or Enable.
- **Decline BA Request:** Select Disable or Enable.

3.3.2 Advanced

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



Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless. Advanced Setup includes items that are not available from the Basic Setup page, such as Beacon Interval, Control Tx Rates and Basic Data Rates.

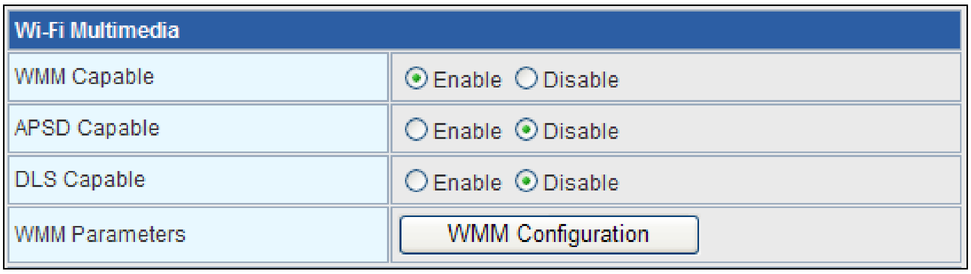
Advanced Wireless	
BG Protection Mode	Auto
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	50 (range 1 - 100, default 100)
Short Preamble	○ Enable ● Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
Country Code	None

Advanced Wireless

- **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.

  If the RTS threshold value is greater than the fragment threshold value, the RTS handshake does not occur. Because the data frames are fragmented before they reach the RTS size.
- **Tx Power:** The Tx Power range is between 1 and 100. The default value is 100.
- **Short Preamble:** Select Disable or Enable.

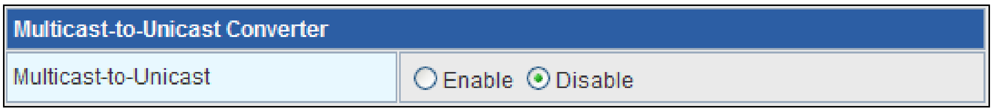
- **Short Slot:** Select Disable or Enable.
- **Tx Burst:** Select Disable or Enable.
- **Pkt_Aggregate:** Select Disable or Enable.
- **Country Code:** Select the region which area you are. It provides six regions in the drop-down list.



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

Wi-Fi Multimedia

- **WMM Capable:** Enable or disable WMM.
- **APSD Capable:** Enable or disable APSD.
- **WMM Parameter:** Click WMM Configuration button to pop up WMM Parameters of Access Point page. You can configure WMM parameters in the page.



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

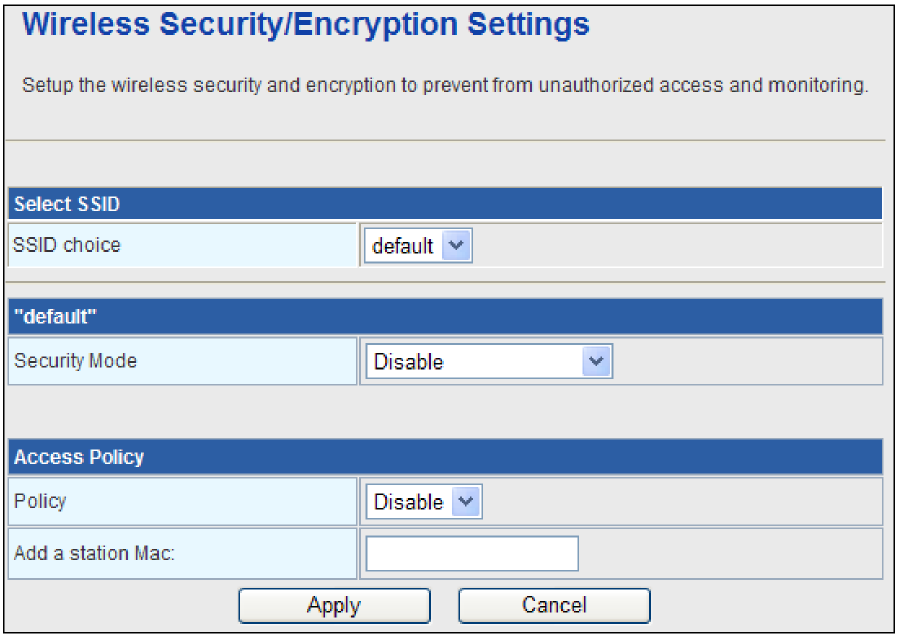
Multicast-to-Unicast Converter

Multicast-to-Unicast Converter: Enable or disable Multicast-to-Unicast Converter.

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

3.3.3 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	default

"default"	
Security Mode	Disable

Access Policy	
Policy	Disable
Add a station Mac:	

Select SSID

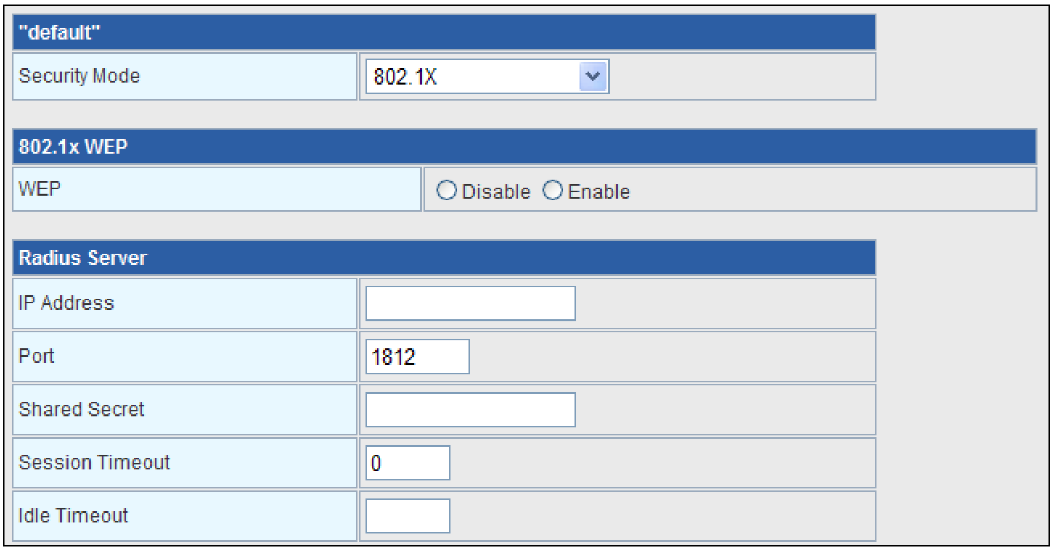
SSID choice: Select SSID in the drop-down list**.**

Security

Security Mode: There are 11 options, including **Disable, OPEN, SHARED, WEPAUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPAPSKWPA2PSK, WPA1WPA2,** and **802.1X**.

[EXAMPLE]

Take 802.1x for example. Select 802.1x in the **Security Mode** down-list. The page shown in the following page appears.



"default"	
Security Mode	802.1X

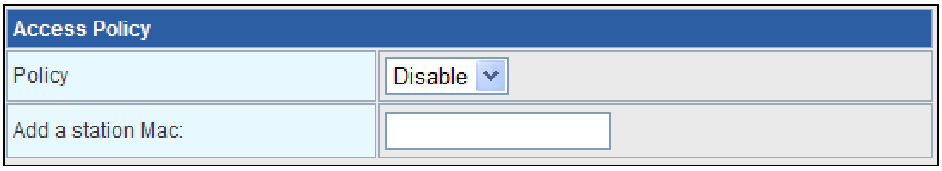
802.1x WEP	
WEP	○ Disable ○ Enable

Radius Server	
IP Address	
Port	1812
Shared Secret	
Session Timeout	0
Idle Timeout	

- **WEP:** Disable or enable WEP.

Radius Server

- **IP Address:** Enter the IP address of Radius Server.
- **Port:** The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
- **Shared Secret:** Enter a password as the key to be shared between the external authentication server and the access point. The key is not send over the network. This key must be the same on the external authentication server and your router.
- **Session Timeout:** Set the time interval for session. Enter the proper value in the field.
- **Idle Timeout:** Set the idle time interval. Enter the proper value in the field.



Access Policy	
Policy	Disable
Add a station Mac:	

Access Policy

- **Policy:** There are three options, including Disable, Allow, and Reject. You can choose Disable, Allow or 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.

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

3.3.4 WDS

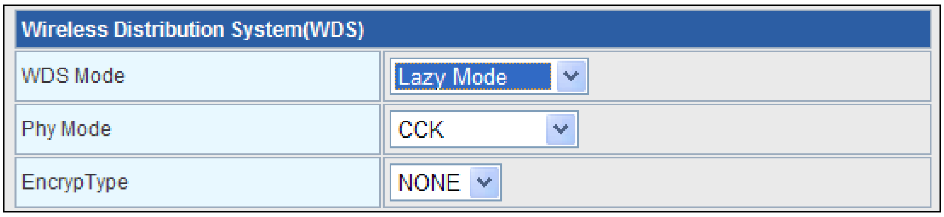
Wireless Distribution System (WDS)

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

- **Disable**

Select Disable to disable the WDS mode.

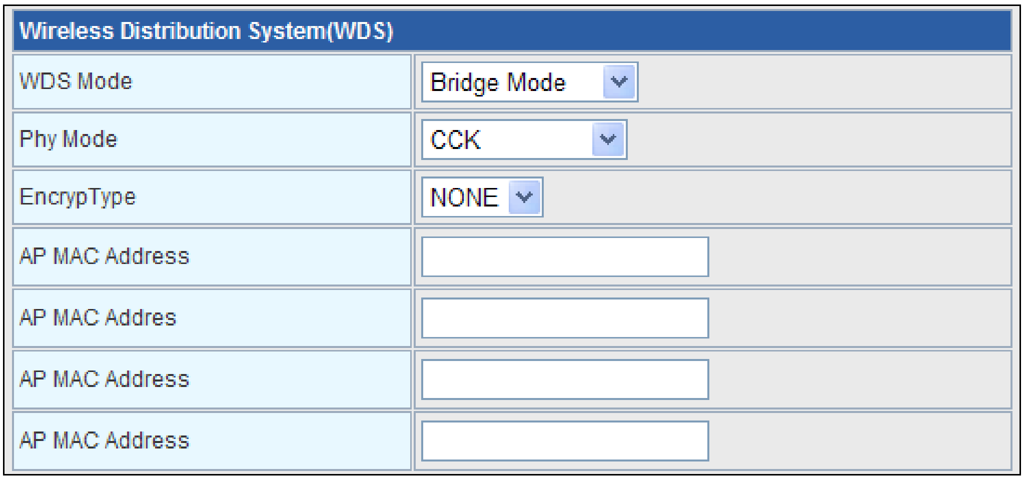
- **Lazy Mode**



Wireless Distribution System(WDS)	
WDS Mode	Lazy Mode
Phy Mode	CCK
EncrypType	NONE

- **WDS Mode:** Select Lazy Mode. The FRT-40xN WDS Lazy mode is allowed the other FRT-40xN 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	NONE
AP MAC Address	
AP MAC Addres	
AP MAC Address	
AP MAC Address	

- **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.

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.

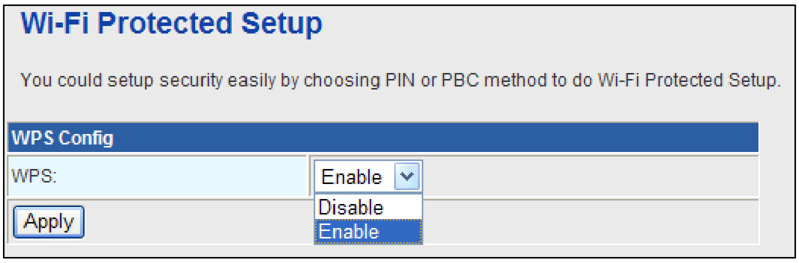
Supports up to 4 point to multipoint WDS links, check Enable WDS and then enable on the MAC addresses.

Example of a WDS topology:

AP1 <-- WDS --> Master AP (our AP) <-- WDS --> AP3<-- WDS --> AP4

3.3.5 WPS

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

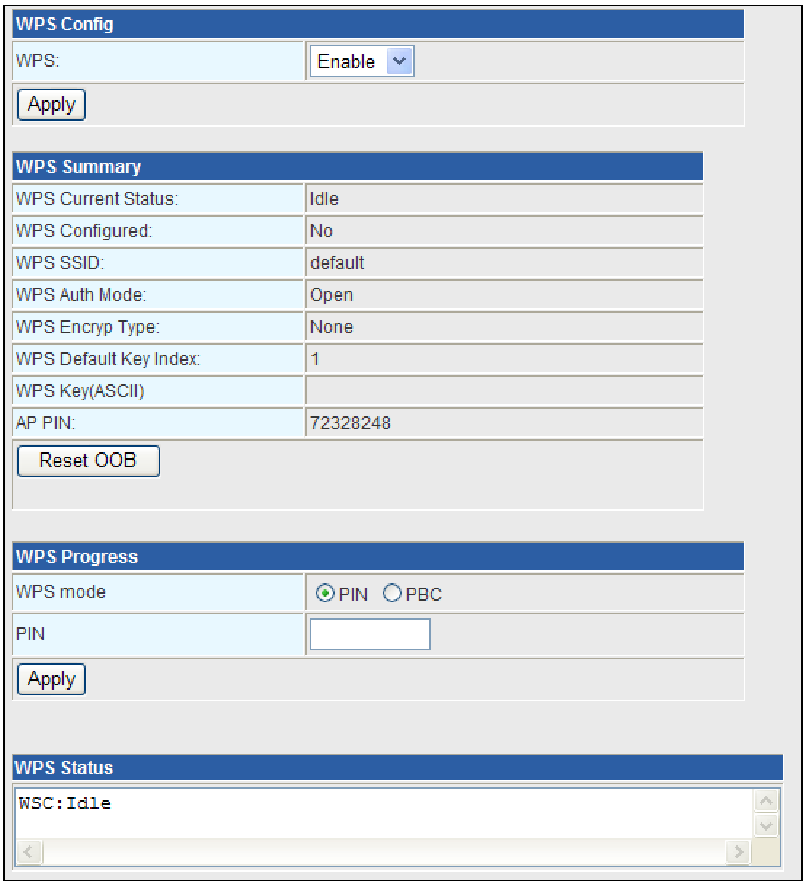


Wi-Fi Protected Setup

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

WPS Config	
WPS:	Enable

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



WPS Config	
WPS:	Enable

WPS Summary	
WPS Current Status:	Idle
WPS Configured:	No
WPS SSID:	default
WPS Auth Mode:	Open
WPS Encryp Type:	None
WPS Default Key Index:	1
WPS Key(ASCII)	
AP PIN:	72328248

WPS Progress	
WPS mode	● PIN ○ PBC
PIN	

```
WSC:Idle
```

WPS Summary

It displays the WPS information, such as WPS Current Status, WPS Configured, and WPS SSID.
Reset OOB: Reset to out of box (OoB) configuration

WPS Progress

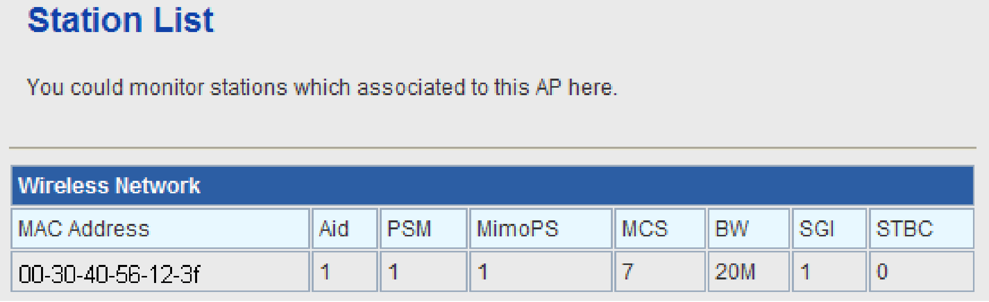
- **WPS mode:** There are two way for you to enable WPS function: **PIN, PBC**. You can use a push button configuration (PBC) on the Wi-Fi router. If there is no button, enter a 4- or 8-digit PIN code. Each STA supporting WPS comes with a hard-coded PIN code.
- **PIN:** If you select PIN mode, you need enter the PIN number in the field.

WPS Status

It displays the information about WPS status.

3.3.6 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, SSID, and current status.



Station List

You could monitor stations which associated to this AP here.

Wireless Network							
MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
00-30-40-56-12-3f	1	1	1	7	20M	1	0

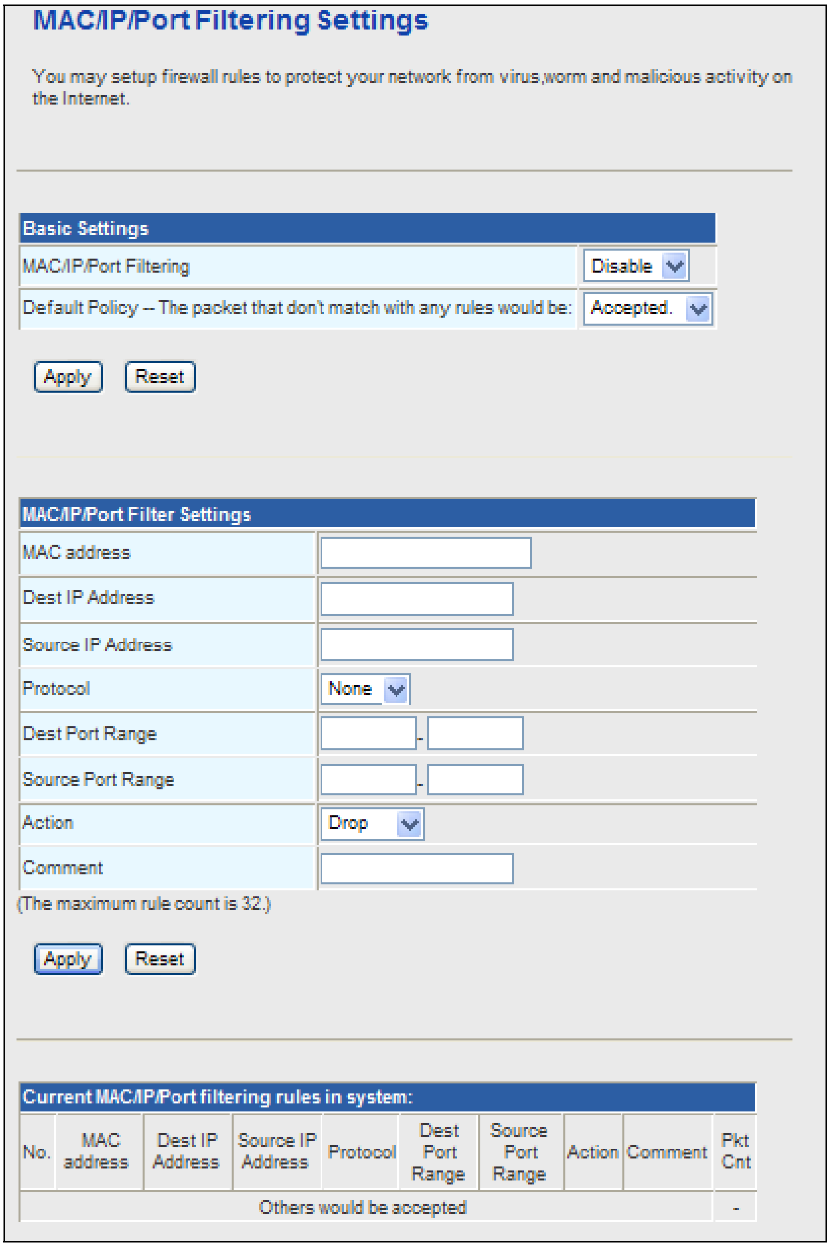
3.4 Firewall

The Fiber Router provides the fully firewall functions, such as IP/Port/MAC 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.

3.4.1 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.



MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus,worm and malicious activity on the Internet.

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

MAC/IP/Port Filter Settings	
MAC address	
Dest IP Address	
Source IP Address	
Protocol	None
Dest Port Range	-
Source Port Range	-
Action	Drop
Comment	

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system:

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

Basic Settings

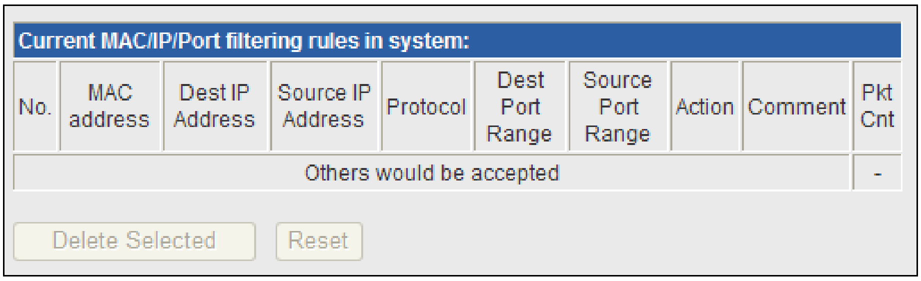
- **MAC/IP/Port Filtering:** Enable or disable the MAC/IP/Port filtering function.
- **Default Policy:** The Packet that does not match any rules would be dropped or accepted.

MAC/IP/Port Filter Settings

- **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.
- **Dest 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.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

⚠	The maximal rule number you can add is 32.



Current MAC/IP/Port filtering rules in system:

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

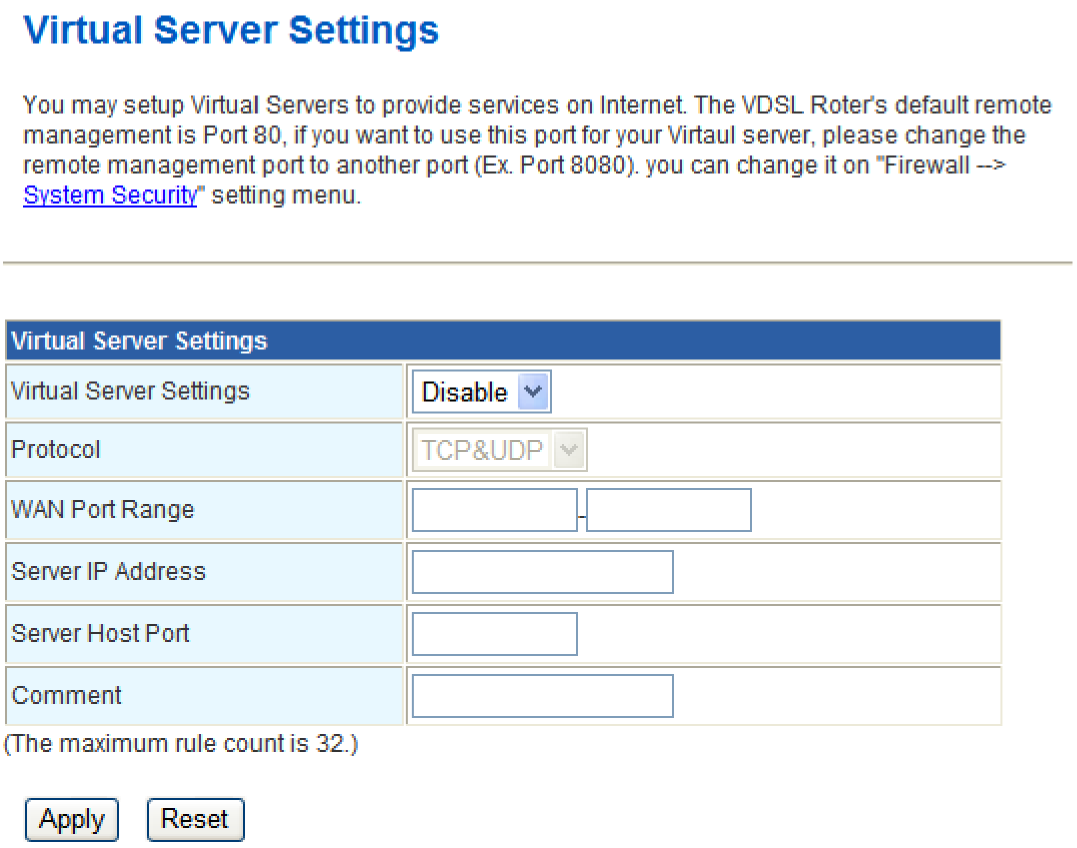
Current MAC/IP/Port filtering rules in system

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

3.4.2 Port Forwarding (Virtual Server)

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

This page allows you to set virtual server to provide services on the Internet.



Virtual Server Settings

You may setup Virtual Servers to provide services on Internet. The VDSL Roter's default remote management is Port 80, if you want to use this port for your Virtaul server, please change the remote management port to another port (Ex. Port 8080). you can change it on "Firewall --> System Security" setting menu.

Virtual Server Settings	
Virtual Server Settings	Disable
Protocol	TCP&UDP
WAN Port Range	-
Server IP Address	
Server Host Port	
Comment	

(The maximum rule count is 32.)

Virtual Server Settings

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

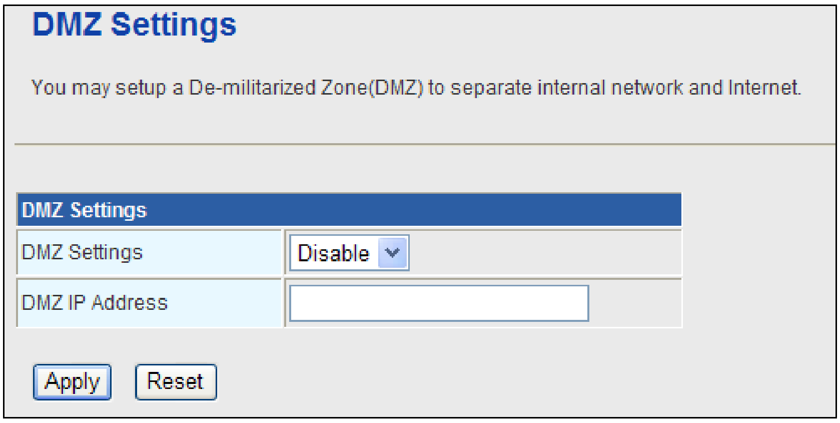
⚠	The maximal rule number you can add is 32.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

3.4.3 DMZ

DMZ (Demilitarized 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 (Demilitarized 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

You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

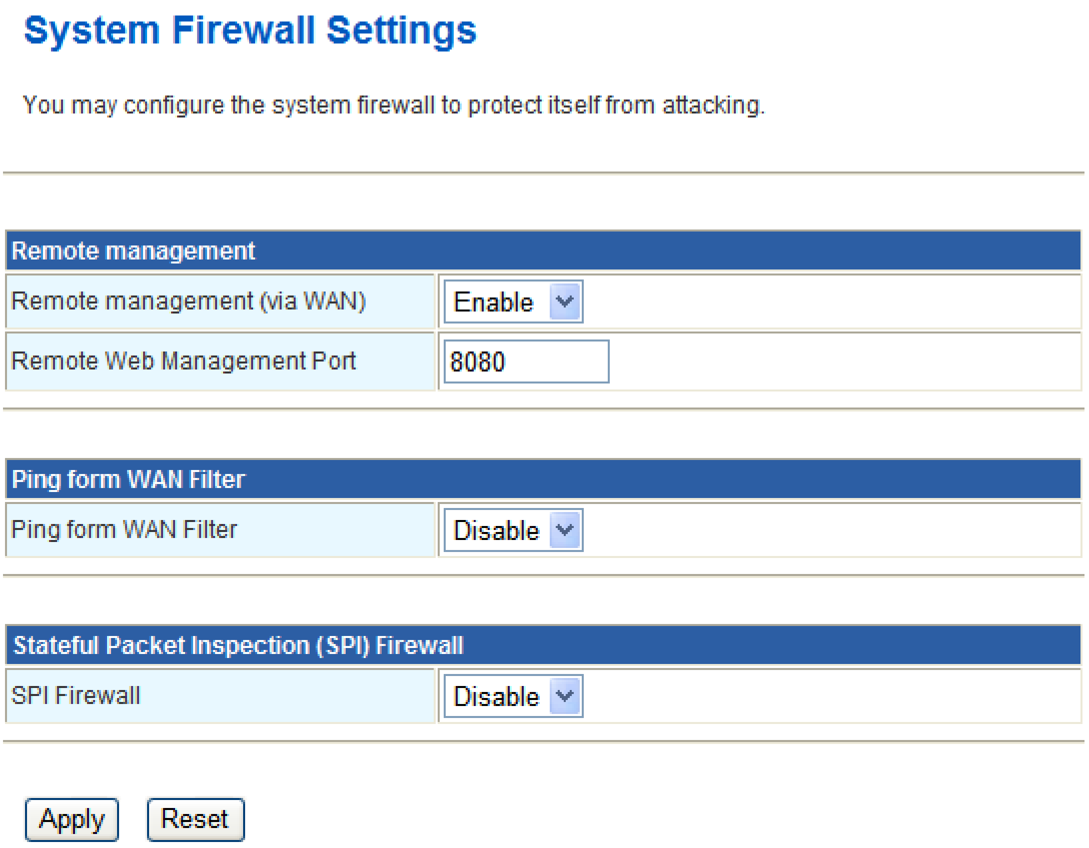
DMZ Settings	
DMZ Settings	Disable
DMZ IP Address	

- **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.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

3.4.4 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.



System Firewall Settings

You may configure the system firewall to protect itself from attacking.

Remote management	
Remote management (via WAN)	Enable
Remote Web Management Port	8080

Ping form WAN Filter	
Ping form WAN Filter	Disable

Stateful Packet Inspection (SPI) Firewall	
SPI Firewall	Disable

Remote Management

Remote management (via WAN): Deny or allow remote management through web.

Remote management Port: The default remote management port is 80, you can change the remote management port for your needs. **Ex. 8080**.

Ping from WAN Filter

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

Stateful Packet Inspection (SPI)

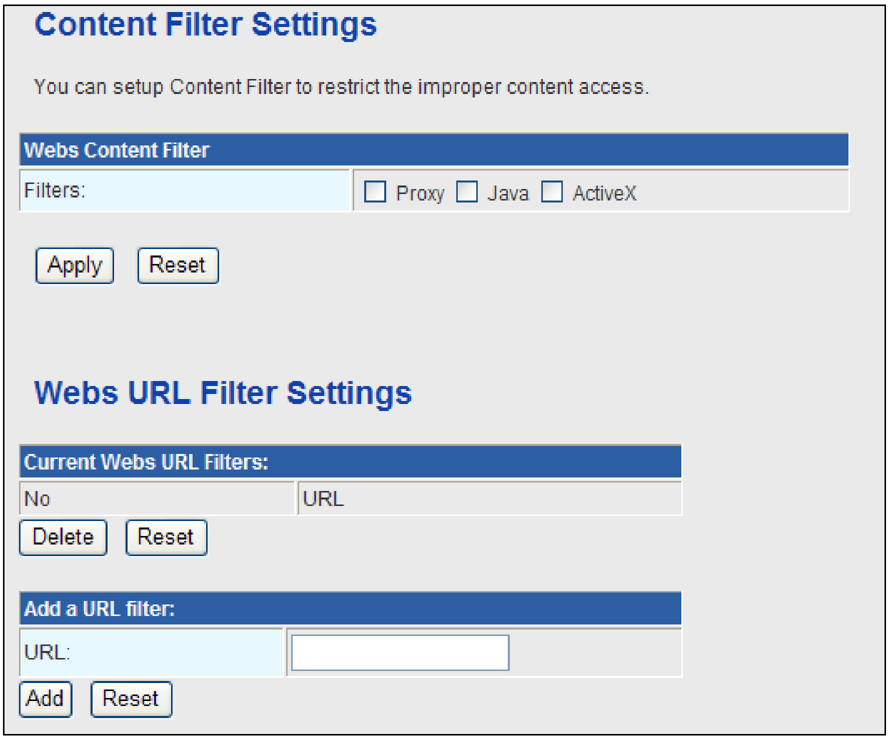
SPI Firewall: You may disable or enable the SPI firewall.

Click **Apply** to make the configuration take effect. Click **Reset** to cancel the new configuration.

3.4.5 Content Filtering

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

URL: Enter the URL String and click “Add” to apply this URL filter rule.
Click **Add** to add a URL filter. Otherwise, click **Reset** to cancel the URL filter.

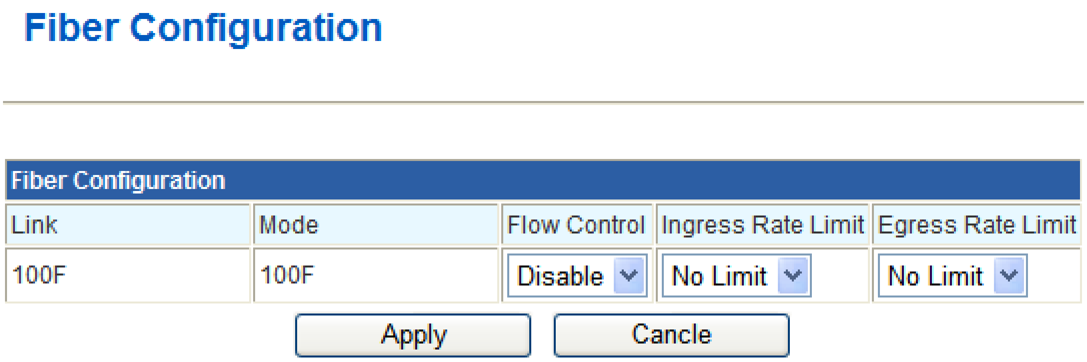
The URL Filter allows you to block access to undesirable Web site

- To use this feature, you must define "filter strings". If the "filter string" appears in a requested URL, the request is blocked.

3.5 Fiber / OAM Setting

3.5.1 Fiber Configuration

This function allows displaying the Fiber port's 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
100F	100F	Disable	No Limit	No Limit

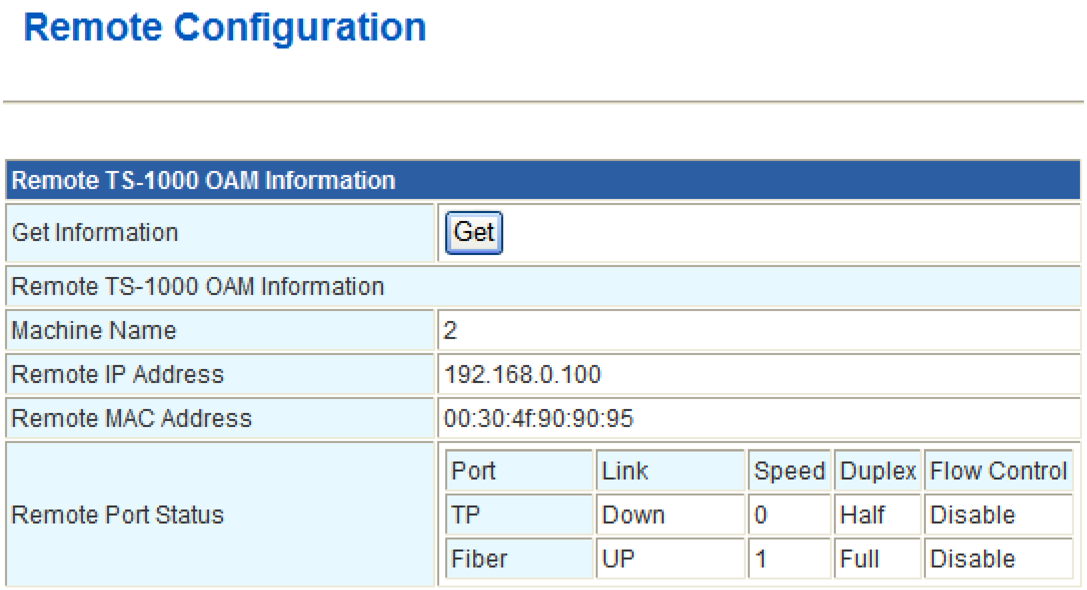
• **Flow Control**	Allow **Enable** or **Disable** flow control for selected port. • **Enable** – 802.3x flow control is enabled on Full-Duplex mode or Backpressure is enabled on Half-Duplex mode • **Disable** – No flow control or backpressure function on no matter Full-Duplex or Half-Duplex mode Default value: **Disable**
• **Ingress Rate Limit**	The value of inbound traffic limitation in kilobit-per-second (kbps). The possible values are : • **No Limit** • **512K** • **1M** • **2M** • **4M** • **8M** • **10M** • **50M** Default value: **No Limit**
• **Egress Shaping**	The value of outbound traffic limitation in kilobit-per-second (kbps). The possible values are : • **No Limit** • **512K** • **1M** • **2M** • **4M** • **8M** • **10M** • **50M** Default value : **No Limit**

3.5.2 Remote Configuration

The Remote TS-1000 Configuration is an advanced remote device monitor feature that allows you to Remote monitor and automatic notify status indication.

■ Remote TS-1000 OAM Information

The Fiber Router supports the TS-1000 and 802.3ah OAM, you can check the status and information of remote device by OAM. Click the “Get” to gat the OAM information from remote devices. It will show the IP, MAC and Port status.



Remote Configuration

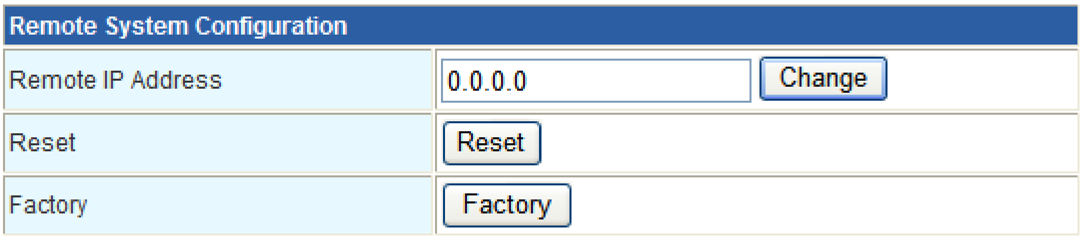
Remote TS-1000 OAM Information	
Get Information	Get
Remote TS-1000 OAM Information	
Machine Name	2
Remote IP Address	192.168.0.100
Remote MAC Address	00:30:4f:90:90:95
Remote Port Status	

Port	Link	Speed	Duplex	Flow Control
TP	Down	0	Half	Disable
Fiber	UP	1	Full	Disable

Notice:	**The TS-1000 OAM function must work with manageable device that supports TS-1000 OAM function.**

■ Remote System Configuration

The users can manage the remote device from local Fiber Router; you can setup the IP address, reset and restore factory default for remote device.



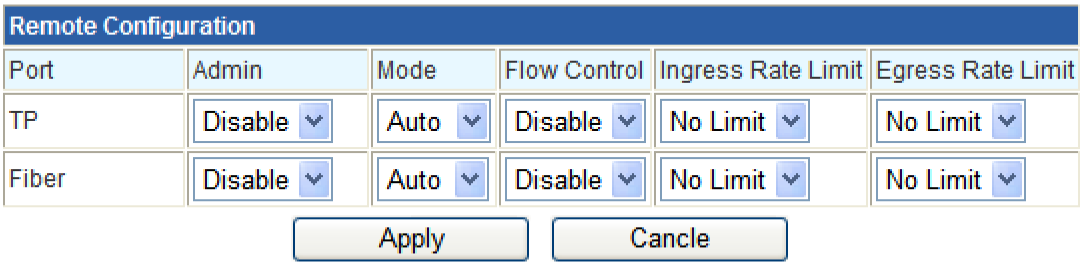
Remote System Configuration	
Remote IP Address	0.0.0.0 Change
Reset	Reset
Factory	Factory

1. **IP address:** Enter the IP address and click the “Change”, it will modify the IP address of remote device.

2. **Reset:** Click the “Reset” button to reboot the remote device.
3. **Factory:** Click the “Factory” button to restore the default settings of remote device.

■ Remote Port Configuration

The users can manage the remote port from local Fiber Router; you can setup the Port Mode, Flow Control, Rate Limit for remote device.



Remote Configuration

Port	Admin	Mode	Flow Control	Ingress Rate Limit	Egress Rate Limit
TP	Disable	Auto	Disable	No Limit	No Limit
Fiber	Disable	Auto	Disable	No Limit	No Limit

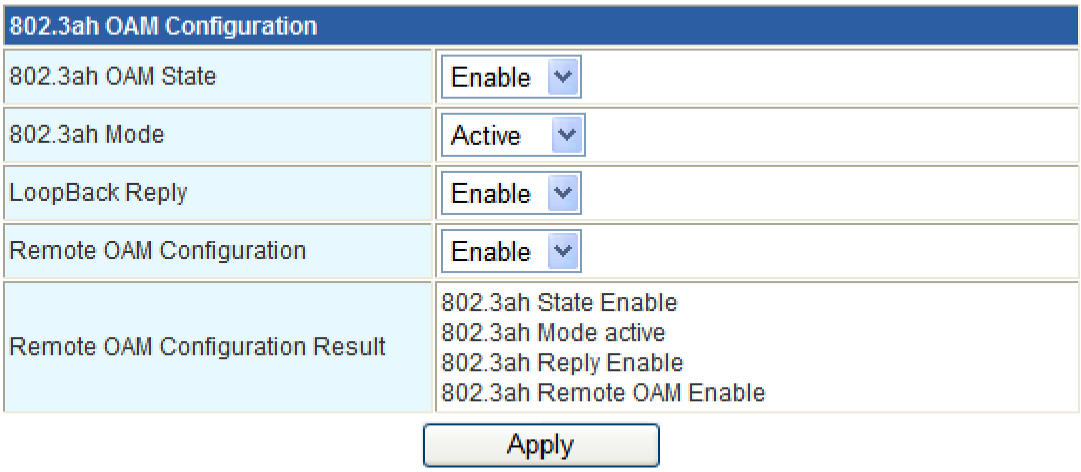
3.5.3 OAM Configuration

- **802.3ah OAM Configuration**

When enable 802.3ah OAM function, all 802.3ah OAMPDU packets will trap to embedded CPU. Software will implement auto discovery procedure. With hardware support, software controls the 802.3ah remote loop back procedure. Hardware can also detect dying gasp even and interrupt CPU to send dying gasp even notification OAMPDU. All other functions defined by 802.3ah are implemented using embedded CPU.

When remote device is in loop back mode, hardware can support change looped test frame's DA, SA or both as user defined. Hardware can also set to don't change looped test frame.

This function provides 802.3ah Setup of Managed Media Converter. Press the "Apply" button to save the current configuration of Managed Media Converter. Below Figure and Table describes the 802.3ah Setup object of Managed Media Converter.



802.3ah OAM Configuration

802.3ah OAM State	Enable
802.3ah Mode	Active
LoopBack Reply	Enable
Remote OAM Configuration	Enable
Remote OAM Configuration Result	802.3ah State Enable 802.3ah Mode active 802.3ah Reply Enable 802.3ah Remote OAM Enable

The 802.3ah OAM Configuration Web page includes the following configurable data:

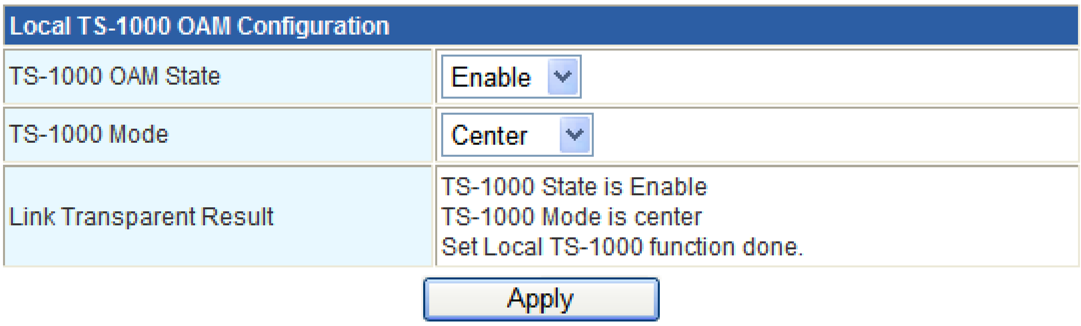
802.3ah OAM State	Provide disable or enable the 802.3ah OAM State function. Default mode is **Enable**.
802.3ah OAM Mode	Allow to choose **"Active"** or **"Passive"** for 802.3ah OAM Mode.
Loopback Reply	Provide disable or enable the Loopback Reply function. Default mode is **Enable**.
Remote OAM Configure	Provide disable or enable the Remote OAM Configure function. Default mode is **Enable**.
Remote OAM Configuration Result	Display the Remote OAM Configuration Result.
Apply button	Press this button for save current configuration of Managed Media Converter.

Table Descriptions of the 802.3ah Setup Web Page Screen Objects

■ Local TS-1000 OAM Configuration

Local TS-1000 OAM Setup

This function provides Local TS-1000 OAM Setup of Managed Media Converter. Press the "Apply" button to save the current configuration of Managed Media Converter. The below screen and Table describes the Local TS-1000 OAM Setup object of Managed Media Converter.



Local TS-1000 OAM Configuration

TS-1000 OAM State	Enable
TS-1000 Mode	Center
Link Transparent Result	TS-1000 State is Enable TS-1000 Mode is center Set Local TS-1000 function done.

Figure Local TS-1000 OAM Setup Web Page screen

The Local TS-1000 OAM Setup Web page includes the following configurable data:

TS-1000 OAM State	Provide disable or enable the TS-1000 OAM operation mode.
TS-1000 Mode	Provide two TS-1000 modes for operation, the available options are: **Terminal** **Center**
Link Transparent	Provide disable or enable the Link Transparent function. Default mode is **Disable**.
Link Transparent Result	Display the link transparent result.
Apply button	Press this button for save current configuration of Managed Media Converter.

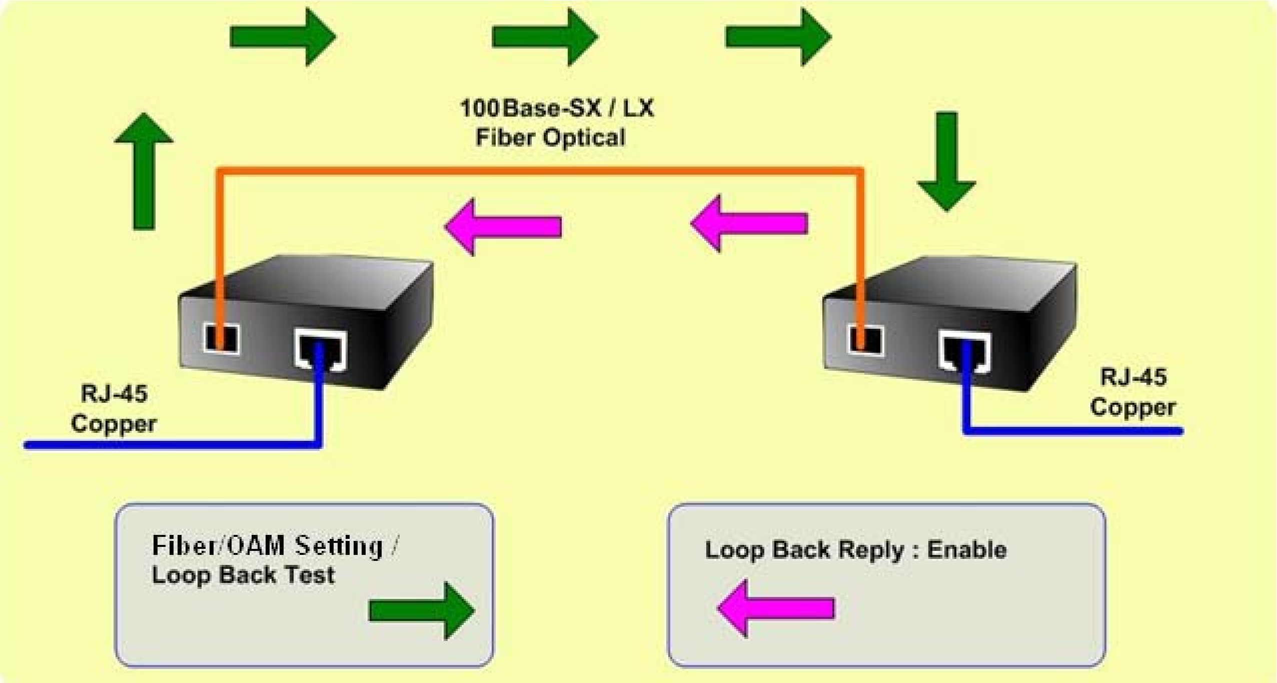
Table Descriptions of the Local TS-1000 OAM Setup Web Page Screen Objects

Notice:	**The TS-1000 OAM function must work with manageable device that supports TS-1000 OAM function.**

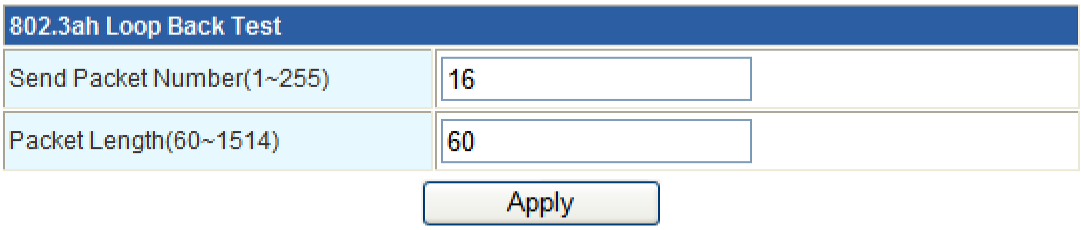
3.5.4 Loop back test

■ 802.3ah Loop Back Test

The 802.3ah Loop Back Test allows manual run this loop back test to check the interconnection between two devices. To assure the Remote 802.3ah function can work correctly.



This function provides 802.3ah Loop Back Test of Fiber devices. Press the **"Apply"** button to run 802.3ah Loop Back Test and see the 802.3ah Loop Back Test Result of Fiber devices. The below screen and Table describes the 802.3ah Loop Back Test object of Fiber Router.



802.3ah Loop Back Test	
Send Packet Number(1~255)	16
Packet Length(60~1514)	60

Figure 802.3ah Loop Back Test Web Page screen

The 802.3ah Loop Back Test Web page includes the following configurable data:

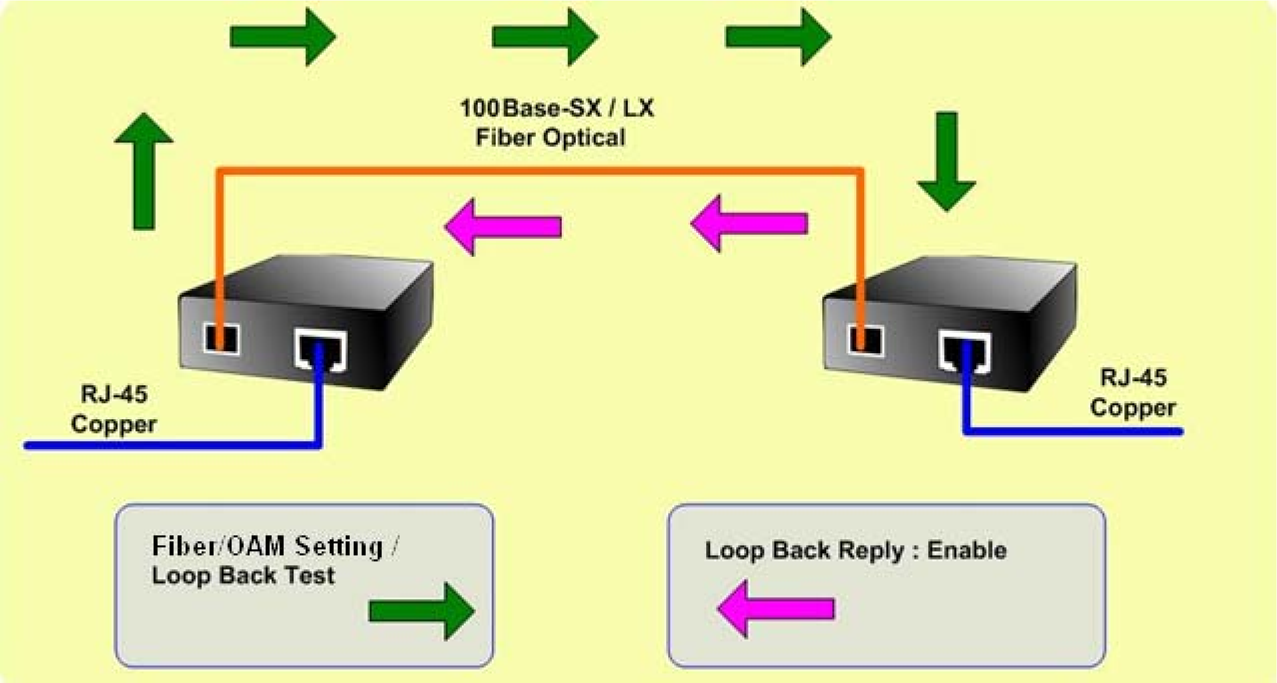
802.3ah Loop Back Test	
Send Packet Number	Allow input the number for packet send and the available options is 1 to 255. Default is **16**.
Packet Length (Not include CRC)	Allow input the number for Packet Length and the available options is 60 to 1514. Default is **60**.
Apply button	Press this button for save current configuration of Fiber Router.
802.3ah Loop Back Test Result	
Result	Display the 802.3ah Loop Back Test Result. Fail or Pass.

Table Descriptions of the 802.3ah Loop Back Test Web Page Screen Objects

✍ ***Notice:***	**The 802.3ah function must work with manageable device that supports 802.3ah function.**

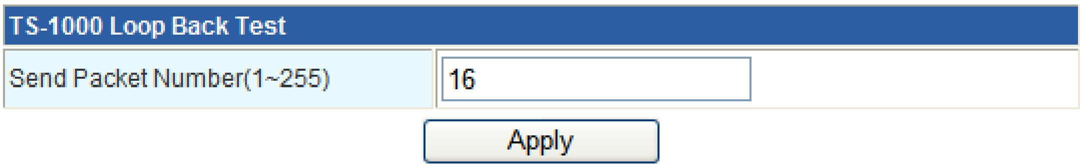
- **TS-1000 Loop Back Test**

The TS-1000 Loop Back Test allows manual run this loop back test to check the interconnection between two Fiber devices. To assure the Remote TS-1000 OAM function can work correctly.



In-band and out-band Loop back

This function provides TS-1000 Loop Back Test of Fiber devices. Press the **"Apply"** button to run Loop Back Test and see the TS-1000 Loop Back Test Result of Fiber Route. The below screen and Table describes the TS-1000 Loop Back Test object of Managed Media Converter.



TS-1000 Loop Back Test

Send Packet Number(1~255)	16

Figure Remote TS-1000 Loop Back Test Web Page screen

The TS-1000 Loop Back Test Web page includes the following configurable data:

TS-1000 Loop Back Test	
Send Packet Number	Allow input the number for packet send and the available options is 1 to 255. Default is **16**.
Apply button	Press this button for save current configuration of Fiber Router.
TS-1000 Loop Back Test Result	
Result	Display the TS-1000 Loop Back Test Result. Fail or Pass.
Result counter	Display the value of Counter Result.

Table Descriptions of the TS-1000 Loop Back Test Web Page Screen Objects

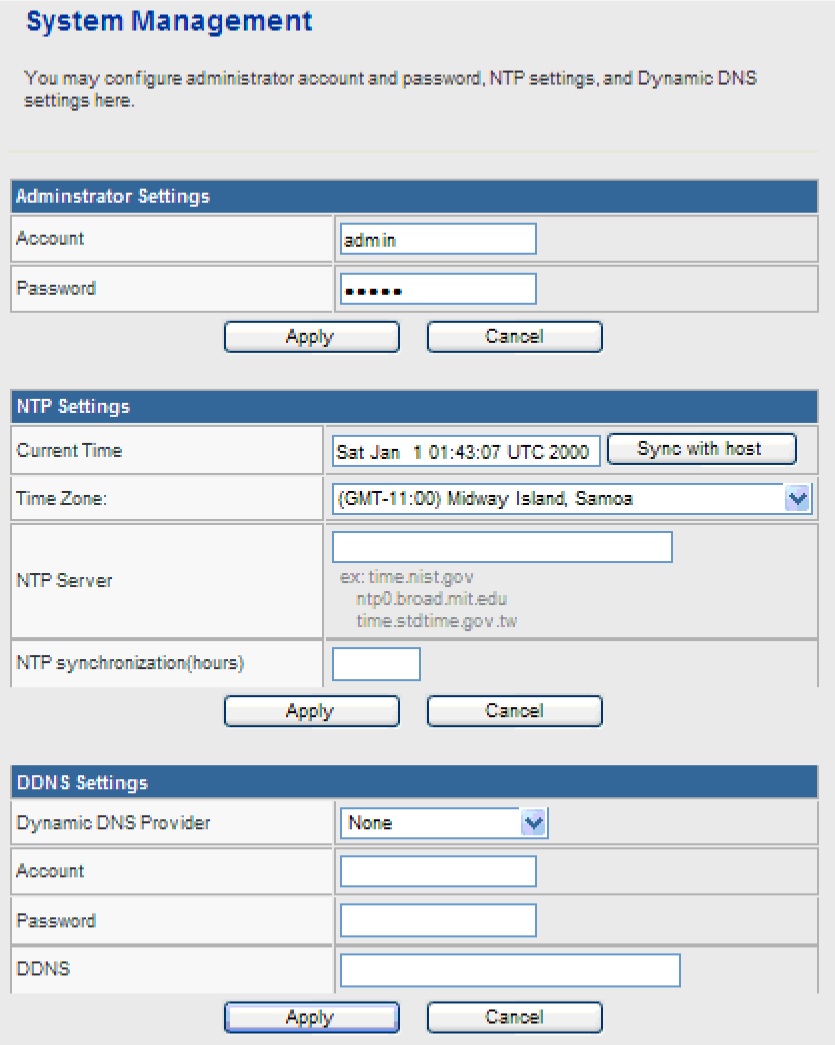
✍ *Notice:*	**The TS-1000 OAM function must work with manageable device that supports TS-1000 OAM function.**

3.6 Administration

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

3.6.1 Management

Choose **Administration > Management,** and the following page appears. You may configure administrator account and password, NTP settings, and dynamic DNS settings in the page.



System Management

You may configure administrator account and password, NTP settings, and Dynamic DNS settings here.

Adminstrator Settings	
Account	admin
Password	●●●●●

NTP Settings	
Current Time	Sat Jan 1 01:43:07 UTC 2000
Time Zone:	(GMT-11:00) Midway Island, Samoa
NTP Server	ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	

DDNS Settings	
Dynamic DNS Provider	None
Account	
Password	
DDNS	

Administrator Settings

- **Account:** Enter the username of the administrator in the field.
- **Password:** Enter the password of the administrator in the field.

NTP Settings

- **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 (hours):** Enter the time interval for synchronization.

DDNS Settings

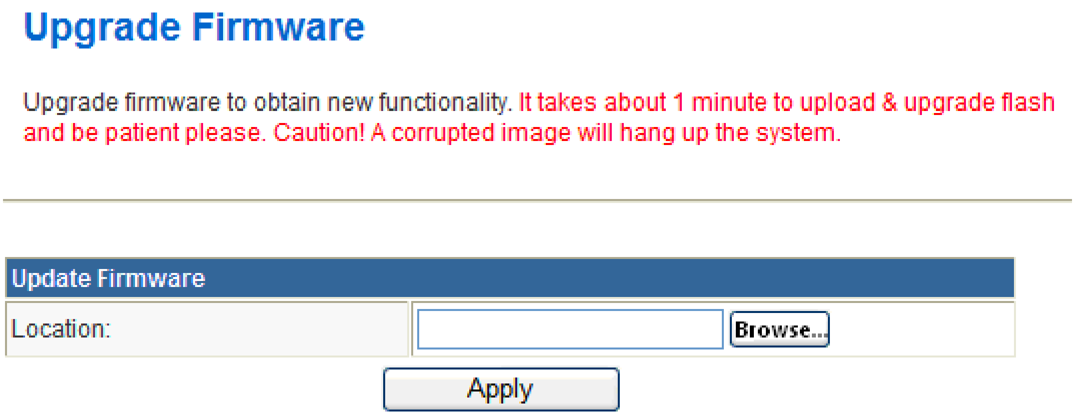
- **Dynamic DNS Provider:** Select the proper dynamic DNS provider in the drop-down list. After selecting a dynamic DNS provider, you are allowed to set the following parameters.
- **Account:** Enter the username of DDNS provider in the field.
- **Password:** Enter the password of DDNS provider in the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

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

3.6.2 Upload Firmware

Choose **Administration > Upload Firmware** and the following page appears. In this page, you may upgrade the correct new version firmware to obtain new functionality. It takes about 1 minute to upload upgrade flash.

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



Upgrade Firmware

Upgrade firmware to obtain new functionality. It takes about 1 minute to upload & upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

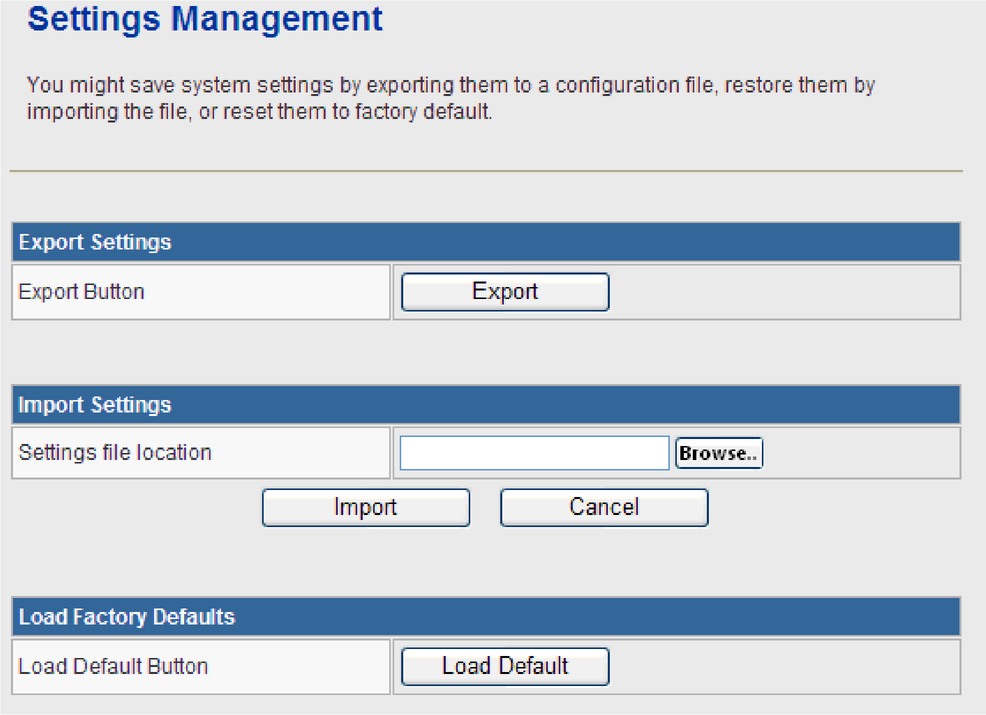
Update Firmware	
Location:	Browse...

Update Firmware

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

3.6.3 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

Import Settings

Settings file location

Load Factory Defaults

Load Default Button

Export Settings

Export Button: Click the **Export** to export the settings.

Import Settings

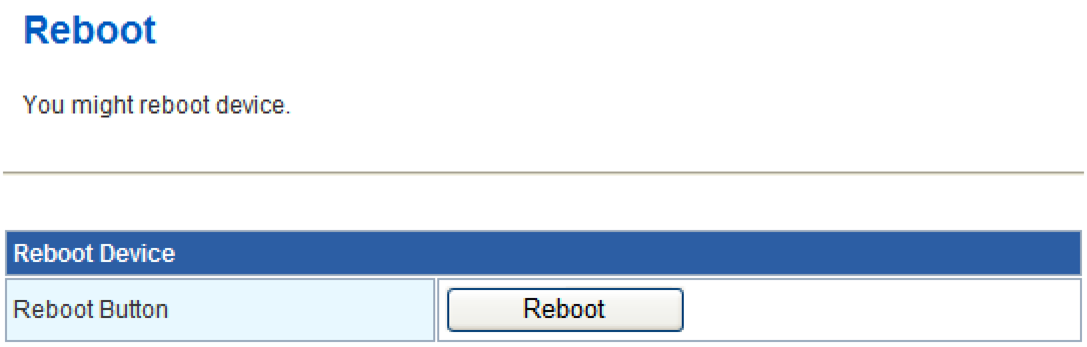
Settings file location: Click **Browse** to select the configuration file, and then click **Import** to upload the configuration file. Click **Cancel** to cancel the uploading operation.

Load Factory Defaults

Load Default Button: Click **Load Default** to make Router return to the default settings.

3.6.4 Reboot

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



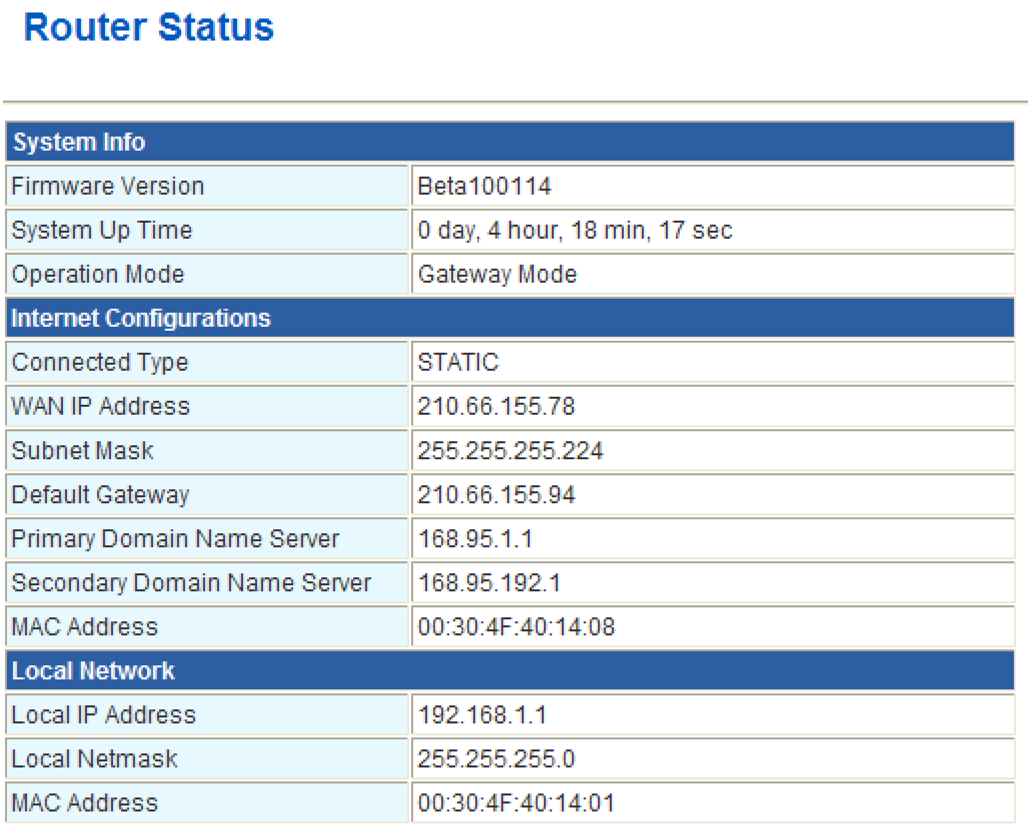
Reboot

You might reboot device.

Reboot Device	
Reboot Button	Reboot

3.6.5 Status

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

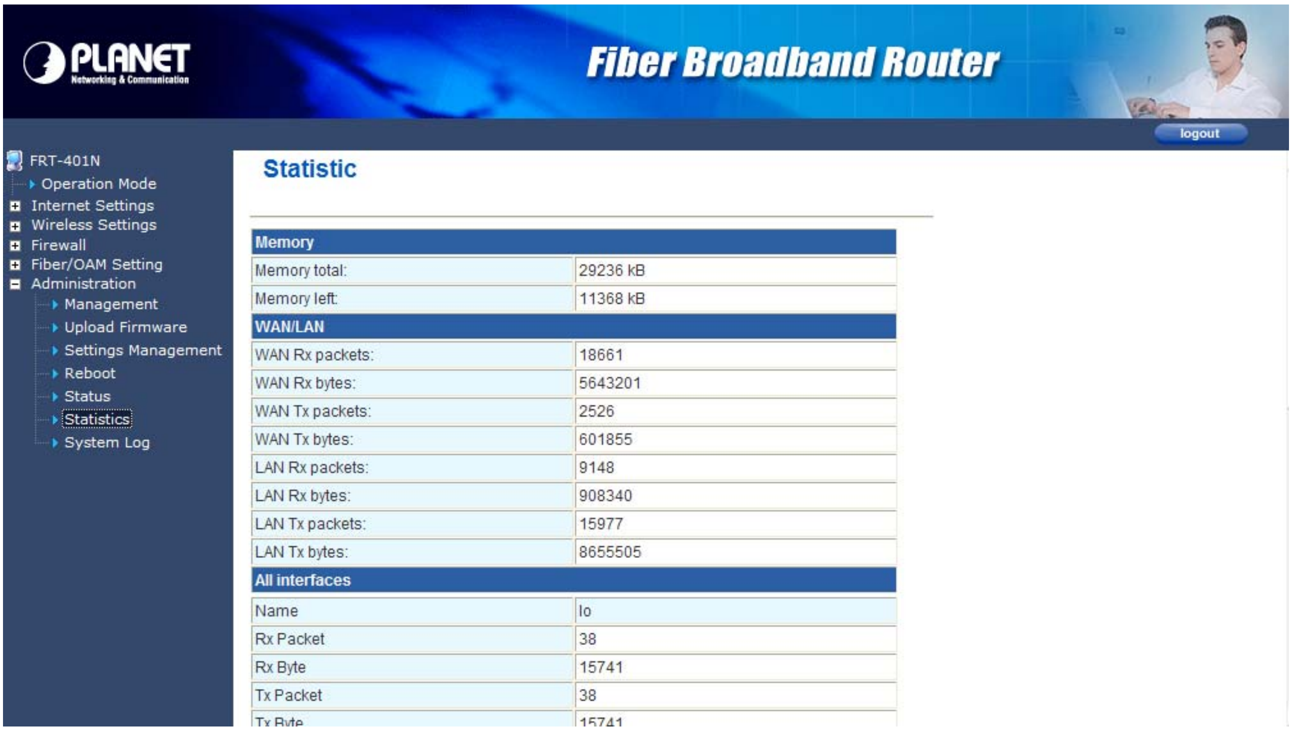


Router Status

System Info	
Firmware Version	Beta100114
System Up Time	0 day, 4 hour, 18 min, 17 sec
Operation Mode	Gateway Mode
Internet Configurations	
Connected Type	STATIC
WAN IP Address	210.66.155.78
Subnet Mask	255.255.255.224
Default Gateway	210.66.155.94
Primary Domain Name Server	168.95.1.1
Secondary Domain Name Server	168.95.192.1
MAC Address	00:30:4F:40:14:08
Local Network	
Local IP Address	192.168.1.1
Local Netmask	255.255.255.0
MAC Address	00:30:4F:40:14:01

3.6.6 Statistics

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

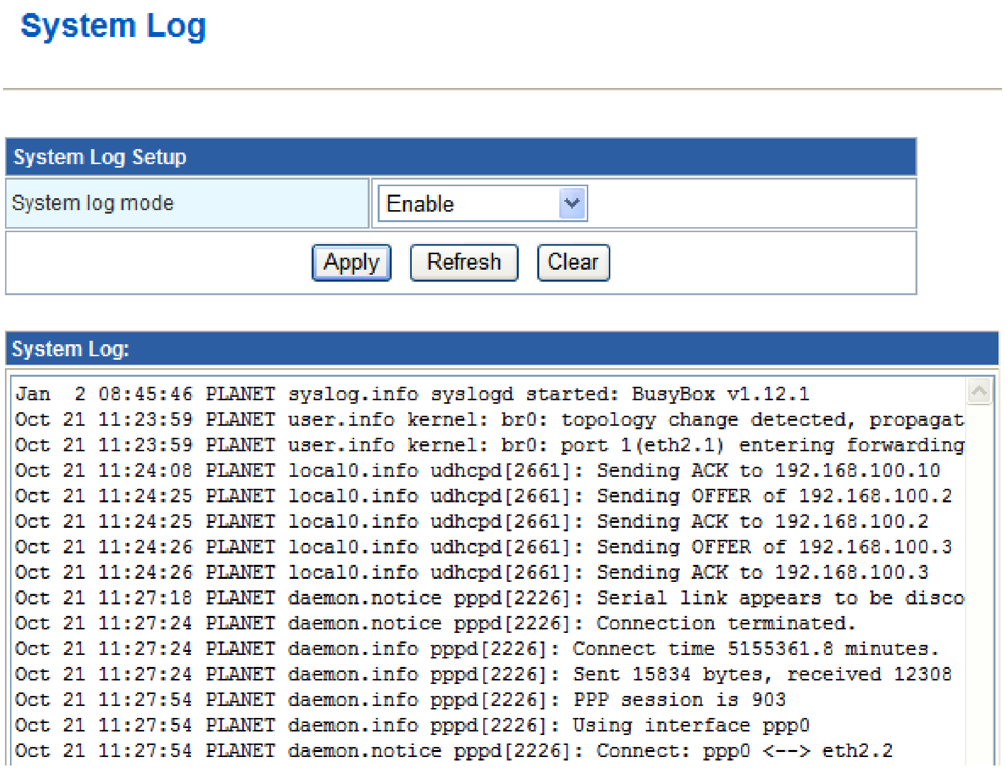


Statistic

Memory	
Memory total:	29236 kB
Memory left:	11368 kB
WAN/LAN	
WAN Rx packets:	18661
WAN Rx bytes:	5643201
WAN Tx packets:	2526
WAN Tx bytes:	601855
LAN Rx packets:	9148
LAN Rx bytes:	908340
LAN Tx packets:	15977
LAN Tx bytes:	8655505
All interfaces	
Name	lo
Rx Packet	38
Rx Byte	15741
Tx Packet	38
Tx Byte	15741

3.6.7 System Log

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



System Log

System Log Setup

System log mode	Enable

System Log:

```
Jan  2 08:45:46 PLANET syslog.info syslogd started: BusyBox v1.12.1
Oct 21 11:23:59 PLANET user.info kernel: br0: topology change detected, propagat
Oct 21 11:23:59 PLANET user.info kernel: br0: port 1(eth2.1) entering forwarding
Oct 21 11:24:08 PLANET local0.info udhcpd[2661]: Sending ACK to 192.168.100.10
Oct 21 11:24:25 PLANET local0.info udhcpd[2661]: Sending OFFER of 192.168.100.2
Oct 21 11:24:25 PLANET local0.info udhcpd[2661]: Sending ACK to 192.168.100.2
Oct 21 11:24:26 PLANET local0.info udhcpd[2661]: Sending OFFER of 192.168.100.3
Oct 21 11:24:26 PLANET local0.info udhcpd[2661]: Sending ACK to 192.168.100.3
Oct 21 11:27:18 PLANET daemon.notice pppd[2226]: Serial link appears to be disco
Oct 21 11:27:24 PLANET daemon.notice pppd[2226]: Connection terminated.
Oct 21 11:27:24 PLANET daemon.info pppd[2226]: Connect time 5155361.8 minutes.
Oct 21 11:27:24 PLANET daemon.info pppd[2226]: Sent 15834 bytes, received 12308
Oct 21 11:27:54 PLANET daemon.info pppd[2226]: PPP session is 903
Oct 21 11:27:54 PLANET daemon.info pppd[2226]: Using interface ppp0
Oct 21 11:27:54 PLANET daemon.notice pppd[2226]: Connect: ppp0 <--> eth2.2
```

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

Appendix A

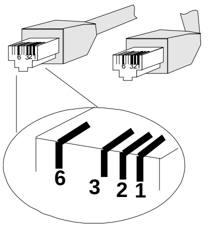
A.1 Device‘s RJ-45 Pin Assignments

- **10/100Mbps, 10/100Base-TX**

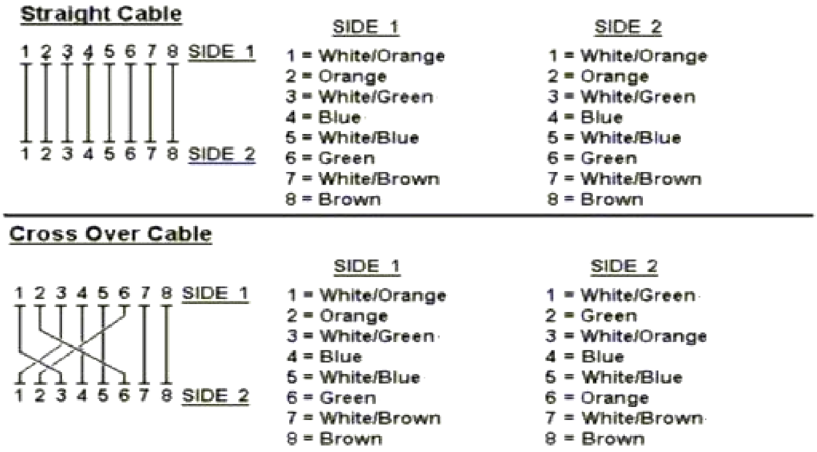
Contact	MDI	MDI-X
1	1 (TX +)	3
2	2 (TX -)	6
3	3 (RX +)	1
6	6 (RX -)	2
4, 5, 7, 8	Not used	Not used

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

1 = White/Orange
2 = Orange
3 = White/Green
4 = Blue
5 = White/Blue
6 = Green
7 = White/Brown
8 = Brown

SIDE 2

1 = White/Orange
2 = Orange
3 = White/Green
4 = Blue
5 = White/Blue
6 = Green
7 = White/Brown
8 = Brown

Cross Over Cable

SIDE 1

1 = White/Orange
2 = Orange
3 = White/Green
4 = Blue
5 = White/Blue
6 = Green
7 = White/Brown
8 = Brown

SIDE 2

1 = White/Green
2 = Green
3 = White/Orange
4 = Blue
5 = White/Blue
6 = Orange
7 = White/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 as 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: Specification

FRT-401 / FRT-401S15 / FRT-405

Product		**Internet Fiber Router**		
Model		**FRT-401**	**FRT-401S15**	**FRT-405**
Ports	**WAN**	1 x 100Base-FX port		
	LAN	4 x 10/100Base-TX port		
Optic Interface	**Connector**	**SC**		**SFP**
	Mode	**Multi-mode**	**Single-mode**	**Vary on module**
	Distance	**2km**	**15km**	**Vary on module**
Optic wavelength		850nm	1310nm	-
Launch Power(dBm)	Max.	-14	-7	-
	Min.	-19.0	-20	-
Receive Sensitivity		-34.5	-28	-
Maximum Input power		-14	-8	-
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)		
LED Indicators		PWR, Fiber, LAN1-4		
Button		1 x RESET button		
Software				
Max. Sessions		4096		
Protocol / Feature		Router and Bridge mode Static Routing and RIPv1/2 DMZ and Virtual Server 802.1D 802.1Q VLAN support QoS SNTP DHCP Server / Client IGMP Proxy and DNS Proxy Universal Plug and Play (UPnP) Compliant DDNS (Dynamic Domain Name System)		
VPN		VPN Pass-Through		
Security		Built-in NAT Firewall MAC / IP/ Port Filtering Content Filtering SPI Firewall support Password protection for system management		
Management		Web-based configuration Available Syslog support TR-069* SNMP v1/v2c TS-1000 and 802.3ah OAM support		

** Feature Enhance by Future FW upgradeable.*

FRT-401N / FRT-401NS15 / FRT-405N

Product		**802.11n Wireless Internet Fiber Router**		
Model		**FRT-401N**	**FRT-401NS15**	**FRT-405N**
Ports	**WAN**	1 x 100Base-FX port		
	LAN	4 x 10/100Base-TX port		
	Wireless	1 x 802.11b/g/n Access Point, 2 x antennas detachable		
Optic Interface	**Connector**	**SC**		**SFP**
	Mode	**Multi-mode**	**Single-mode**	**Vary on module**
	Distance	**2km**	**15km**	**Vary on module**
Optic wavelength		850nm	1310nm	-
Launch Power(dBm)	Max.	-14	-7	-
	Min.	-19.0	-20	-
Receive Sensitivity		-34.5	-28	-
Maximum Input power		-14	-8	-
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)		
LED Indicators		PWR, WPS, WLAN, Security, Fiber, LAN1-4		
Button		1 x RESET button, 1 x WPS button		
Software				
Max. Sessions		4096		
Protocol / Feature		Router, Bridge and WISP mode WDS and WPS Static Routing and RIPv1/2 DMZ and Virtual Server 802.1D 802.1Q VLAN support QoS SNTP DHCP Server / Client IGMP Proxy and DNS Proxy Universal Plug and Play (UPnP) Compliant DDNS (Dynamic Domain Name System)		
Wireless	**Wireless Standard**	Compliant with IEEE 802.11n, 802.11g and 802.11b standards		
	Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)		
	Channels	Maximum 14 Channels, depending on regulatory authorities		
	Antenna	2 x 2dBi detachable Antenna		
	Wireless Data Encryption	64 bit / 128 bit WEP, WPA-PSK, WPA, WPA2, 802.1x encryption, and WPS PBC		
	Wireless Data Rate	IEEE 802.11b: 1/2/5.5/11Mbps IEEE 802.11g: 6/9/12/18/24/36/48/54Mbps IEEE 802.11n: 14/29/43/58/87/116/130/144Mps in 20MHz, 30/60/90/120/180/240/270/300Mbps in 40MHz		
	WDS	WDS repeater support		
VPN		VPN Pass-Through		

Security	Built-in NAT Firewall MAC / IP/ Port Filtering Content Filtering SPI Firewall support Password protection for system management
Management	Web-based configuration Available Syslog support TR-069* SNMP v1/v2c TS-1000 and 802.3ah OAM support

** Feature Enhance by Future FW upgradeable.*

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.

VDSL2

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).