LevelOne

User Manual

FBR-1461

ADSL2+ Modem Router w/ QoS

V2.0 – 0809

Table of Contents

Default Settings

IP Address	192.168.0.1
Admin / Password	admin / password

Chapter 1
Introduction

1.1 Introducing the FBR-1461

Thank you for purchasing the FBR-1461 Modem Router. Your new router is an all-in-one unit that combines an ADSL2/2+ modem, router and Ethernet network switch to provide everything you need to get the machines on your network connected to the Internet over an ADSL broadband connection.

The FBR-1461 router complies with ADSL2+ standards for deployment worldwide and supports downstream rates of up to 24 Mbps and upstream rates of up to 1 Mbps. Designed for small office, home office and residential users, the router enables even faster Internet connections. You can enjoy ADSL services and broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

The FBR-1461 supports PPPoA (RFC 2364 – PPP (Point-to-Point Protocol) over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with your ISP. Your new router also supports VC-based and LLC-based multiplexing.

The perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection, the FBR-1461 allows multiple users to have high-speed Internet access simultaneously.

Your new router also serves as an Internet firewall, protecting your network from access by outside users. Not only does it provide a natural firewall function with Network Address Translation (NAT), it also provides rich firewall features to secure your network. All incoming data packets are monitored and filtered. You can also configure your new router to block internal users from accessing the Internet.

The FBR-1461 provides two levels of security support. First, it masks LAN IP addresses making them invisible to outside users on the Internet, so it is much more difficult for a hacker to target a machine on your network. Second, it can block and redirect certain ports to limit the services that outside users can access. To ensure that games and other Internet applications run properly, you can open specific ports for outside users to access internal services on your network.

The Integrated DHCP (Dynamic Host Control Protocol) client and server services allow multiple users to get IP addresses automatically when the router boots up. Simply set local machines as a DHCP client to accept a dynamically assigned IP address from the DHCP server and reboot. Each time a local machine is powered up; the router recognizes it and assigns an IP address to instantly connect it to the LAN.

For advanced users, Virtual Service (port mapping) functions allow the product to provide limited visibility to local machines with specific services for outside users. For instance, a dedicated web server can be connected to the Internet via the router and then incoming requests for web pages that are received by the router can be rerouted to your dedicated local web server, even though the server now has a different IP address.

Virtual Server can also be used to re-task services to multiple servers. For instance, you can set the router to allow separated FTP, Web, and Multiplayer game servers to share the same Internet-visible IP address while still protecting the servers and LAN users from hackers.

1.2 Features

Express Internet Access – ADSL2/2+ capable

The FBR-1461 complies with ADSL worldwide standards. Supporting downstream rates of 8Mbps with ADSL, the router is capable of up to 12/24 Mbps with ADSL2/2+, and upstream rates of up to 1 Mbps. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio which are easier and faster than ever. The router is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); and G.dmt.bisplus (ITU G.992.5)

Fast Ethernet Switch

A 4-port 10/100Mbps fast Ethernet switch is built-in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports, with auto detection allowing you to use either straight or cross-over Ethernet cables.

Multi-Protocol to Establish a Connection

The router supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516) to establish a connection with an ISP. The router also supports VC-based and LLC-based multiplexing.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors, and it makes setting up a network simple and affordable. UPnP architecture leverages TCP/IP and the Web to enable proximity networking in addition to control and data transfer among networked devices. With this feature enabled, you can seamlessly connect to Net Meeting or MSN Messenger.

Network Address Translation

Network Address Translation (NAT) allows multiple users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateways (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.

Firewall

NAT technology supports simple firewalls and provides options for blocking access from the Internet, like Telnet, FTP, TFTP, WEB, SNMP and IGMP.

Domain Name System Relay

Domain Name System (DNS) relay provides an easy way to map a domain name with a user-friendly name such as www.google.com with an IP address. When a local machine sets its DNS server to the router’s IP address, every DNS conversion request packet from the PC to this router is forwarded to the real DNS on the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. To use the service, you must first apply for an account from a DDNS service such as http://www.dyndns.org/.

PPP over Ethernet (PPPoE)

The FBR-1461 provides an embedded PPPoE client function to establish a connection. You get greater access speed without changing the operation concept, while sharing the same ISP account and paying for one access account. No PPPoE client software is required for the local computer. Automatic Reconnect and Disconnect Timeout (Idle Timer) functions are also provided.

Quality of Service (QoS)

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by Internal IP address, External IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don’t saturate upload bandwidth, or office browsing doesn’t bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

Virtual Server:

You can specify which services are visible to outside users. The router detects an incoming service request and forwards it to the specific local computer for handling. For example, you can assign a PC in a LAN to act as a Web server inside and expose it to the outside network. Outside users can browse inside the web server directly while it is protected by NAT. A DMZ host setting is also provided for local computers exposed to the outside Internet network.

Dynamic Host Configuration Protocol (DHCP) Client and Server

On a WAN site, the DHCP client obtains an IP address from the Internet Service Provider (ISP) automatically. On a LAN site, the DHCP server allocates a range of client IP addresses, including subnet masks and DNS IP addresses and distributes them to local computers. This provides an easy way to manage the local IP network.

Rich Packet Filtering

This feature filters the packet based on IP addresses as well as Port numbers. Filtering packets to and from the Internet provides a higher level of security control.

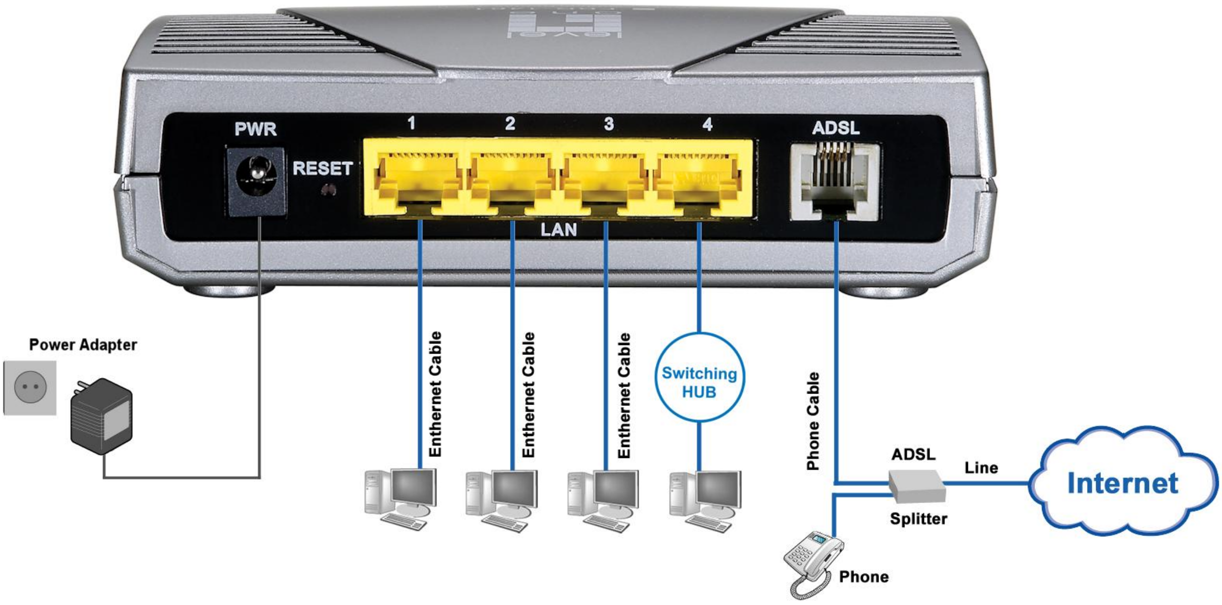
Web-based GUI

A web-based GUI offers easy configuration and management. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

You can upgrade the router with the latest firmware through its web-based GUI.

1.3.1 Applications of the FBR-1461



Chapter 2
Product Overview

2.1 Package Contents

FBR-1461 ADSL2+ Router

CD-ROM containing the online manual

RJ-11 ADSL/Telephone Cable

Ethernet (CAT-5 LAN) Cable

AC-DC power adapter (12V DC, 1A)

Quick Installation Guide

2.2 Important Notes

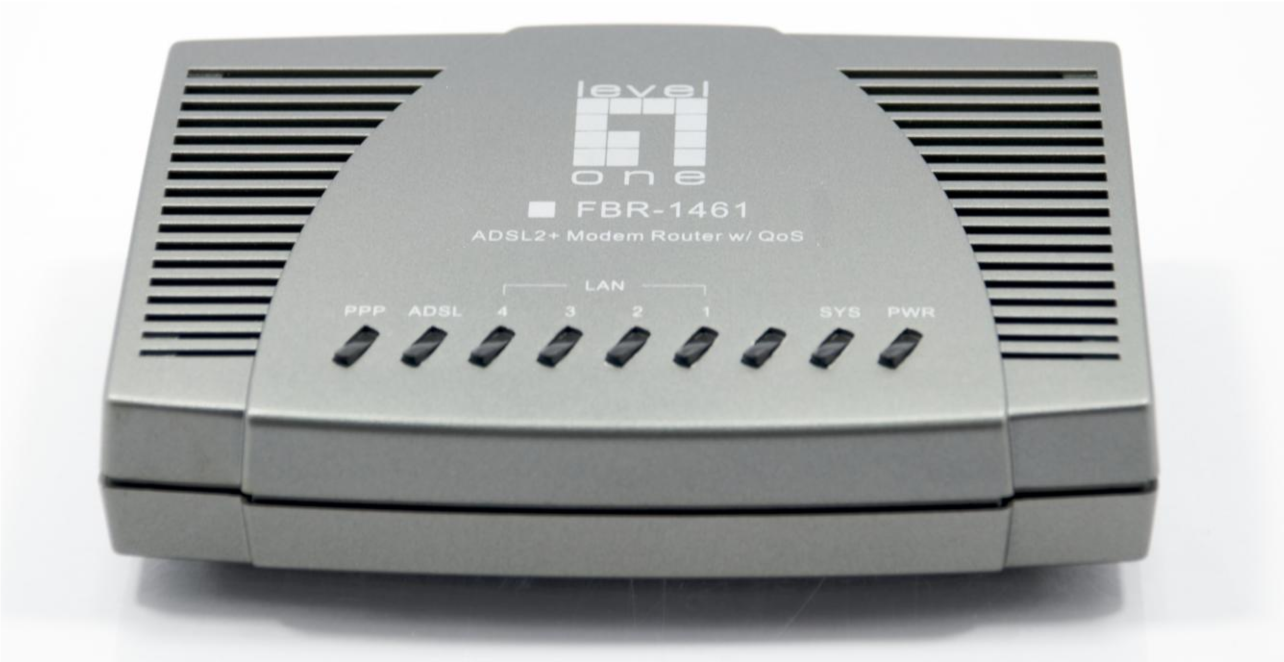
Warning:

- ✓ Do not use the FBR-1461 in high humidity or high temperatures.
- ✓ Do not use the same power source for the FBR-1461 as other equipment.
- ✓ Do not open or repair the case yourself. If the FBR-1461 is too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.

Attention:

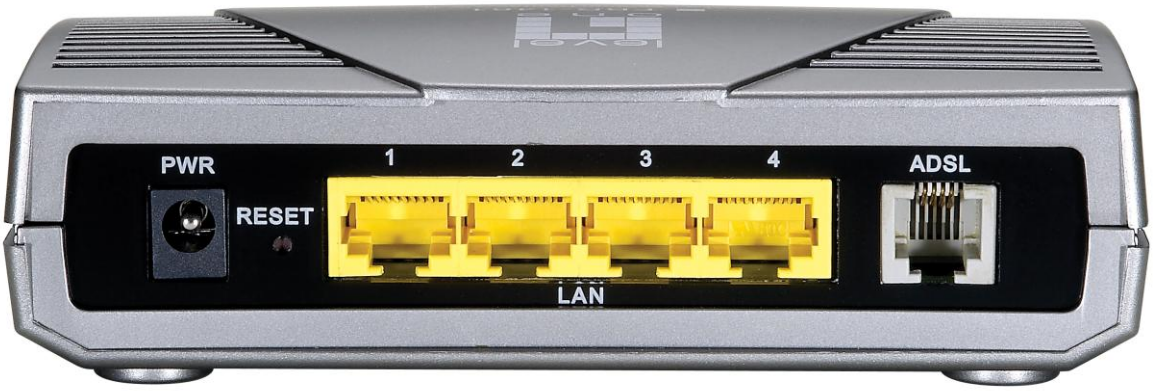
- ✓ Place the FBR-1461 on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

2.3.1 The Front LEDs - FBR-1461



LED		Meaning
1	**PPP :**	Lit green when WAN port gets IP address successfully.
2	**ADSL:**	Blinking when attempting to connect to ADSL DSLAM Lit when successfully connected to an ADSL DSLAM
3.	**LAN:**	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps. Blinking when data is Transmitted / Received.
4	**SYS:**	When system is booting up or in firmware upgrading stage, it will flash. ON: System is ready.
5	**PWR :**	ON: Power on

2.4.1 The Rear Ports - FBR-1461



Port		Description
1	**PWR**	Connect the supplied power adapter to this jack.
2	**RESET**	After the router is powered on, press this reset button using the end of paper clip or other small pointed object to reset the router and to restore it to factory default settings. 1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash). 2. Recovery procedures for a lost web interface password:
3	**LAN**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
4	**LINE**	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the ADSL/Telephone network.

The detail instruction in Reset Button

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):
Hold the *Reset Button* on the back of the modem in. Keep this button held in and turn on the modem. Once the lights on the modem have stopped flashing, release the *Reset Button.* The modem's emergency-reflash web interface will then be accessible via http://192.168.0.1 where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

Note:

Before powering on the router to enter the recovery process, please configure the IP address of the PC as 192.168.0.100 and proceed with the following step by step guide.

1. Power the router off.
2. Hold the "Reset Button”.
3. Power on the router. Then Router's IP will reset to Emergency IP address (Say 192.168.0.1)
4. Download the firmware.

2.5 Cabling

One of the most common causes of problems is because of bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analog modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and to ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed being the wrong way around can cause problems with your ADSL connection, which includes frequent disconnections.

Chapter 3
Installation

You can configure the FBR-1461 router through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux and Windows 98/NT/2000/XP/Vista include a web browser as a standard application.

3.1 Before Configuration

PCs must have a properly installed Ethernet interface which connects to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **192.168.0.1** and the subnet mask is **255.255.255.0** (i.e. any attached PC must be in the same subnet, and have an IP address in the range between 192.168.0.2 and 192.168.0.254). The easiest way is to configure the PC is to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface you are advised to **uninstall** any kind of software firewall on your PCs, as they can cause problems when trying to access the 192.168.0.1 IP address of the router.

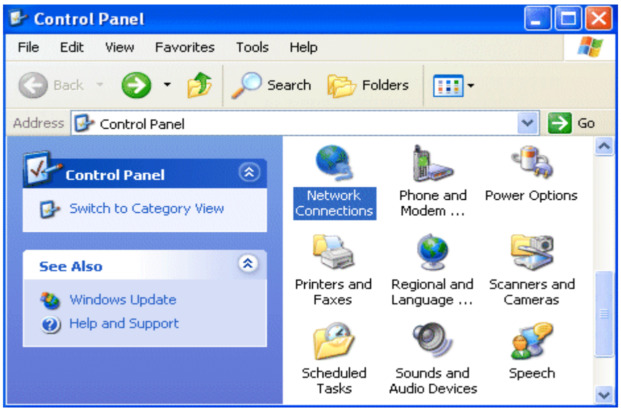
Please follow the steps below for installation on your PC's network environment. First of all, check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

Note:

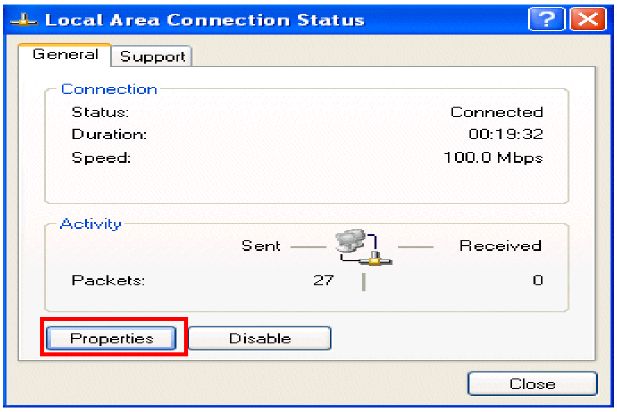
Any TCP/IP capable workstation can be used to communicate with or through the FBR-1461. To configure other types of workstations, please consult the manufacturer's documentation.

Configuring a 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**.



Status: Connected

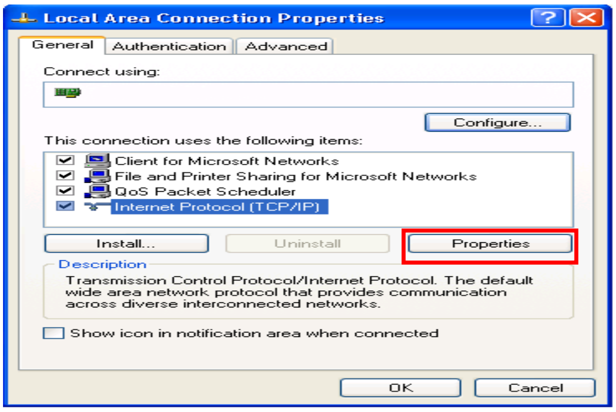
Duration: 00:19:32

Speed: 100.0 Mbps

Sent — Received

Packets: 27 | 0

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



Connect using:

This connection uses the following items:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ QoS Packet Scheduler

☑ Internet Protocol (TCP/IP)

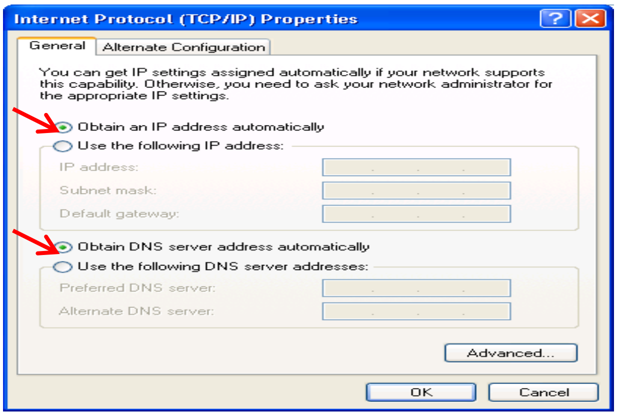
Description

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

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:

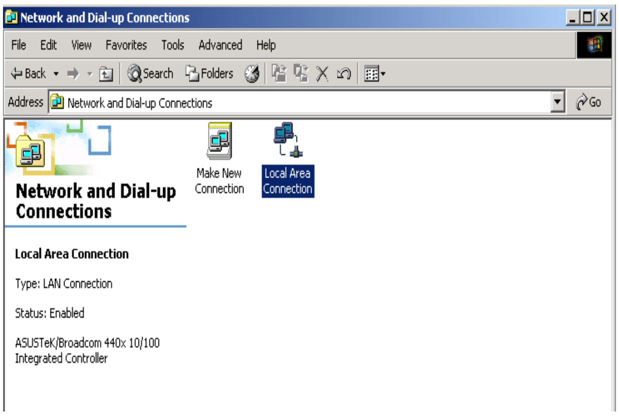
Preferred DNS server:

Alternate DNS server:

Configuring a 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
Make New Connection
Local Area Connection

Network and Dial-up Connections

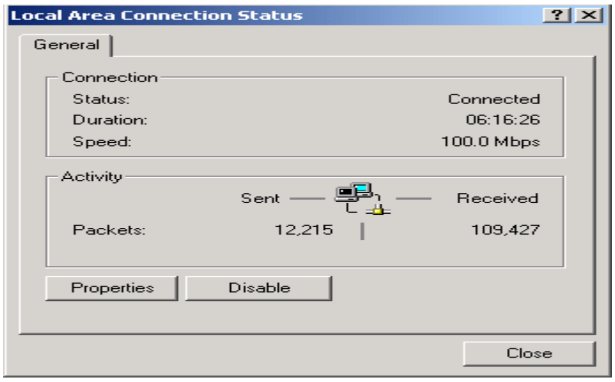
Local Area Connection

Type: LAN Connection

Status: Enabled

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

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



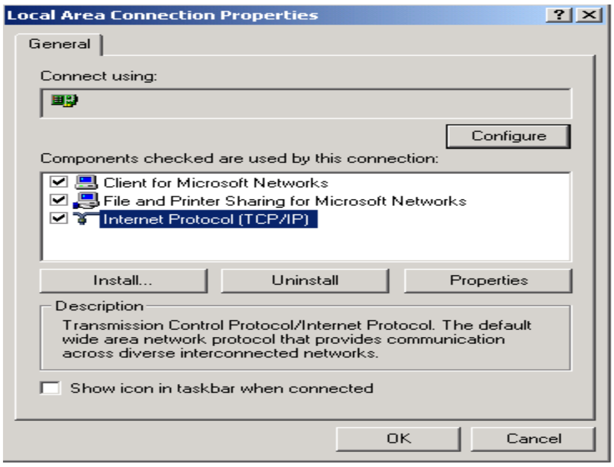
Connection

Status:	Connected
Duration:	06:16:26
Speed:	100.0 Mbps

Activity

	Sent	Received
Packets:	12,215	109,427

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



Connect using:

Components checked are used by this connection:

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

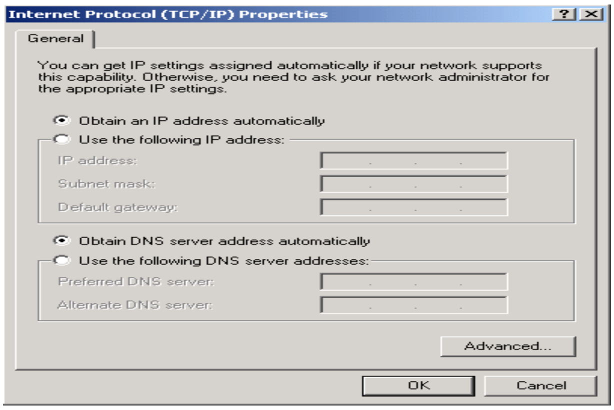
Description

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

□ Show icon in taskbar when connected

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:

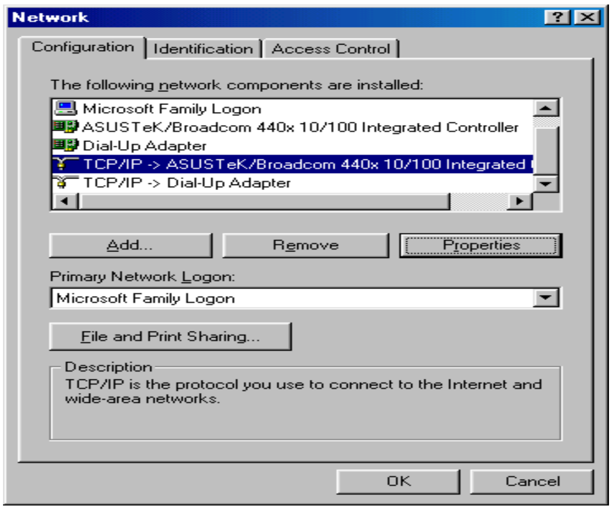
Preferred DNS server:

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.



Network

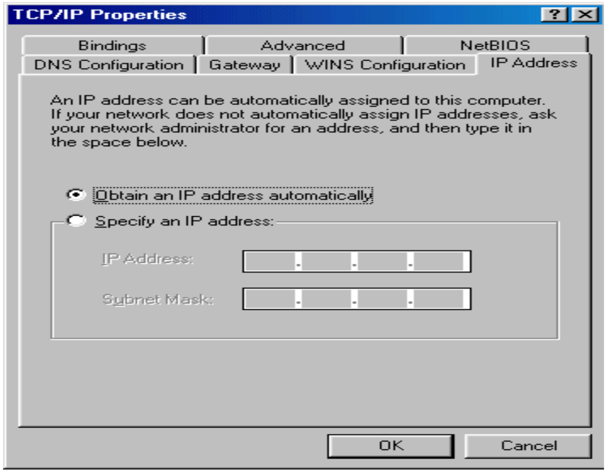
The following network components are installed:

- 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.



TCP/IP Properties

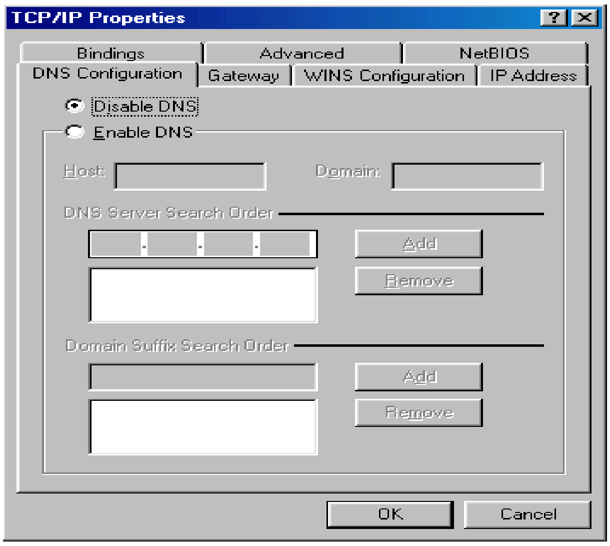
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically
○ Specify an IP address:

IP Address: . . .
Subnet Mask: . . .

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

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



TCP/IP Properties

● Disable DNS
○ Enable DNS

Host: Domain:

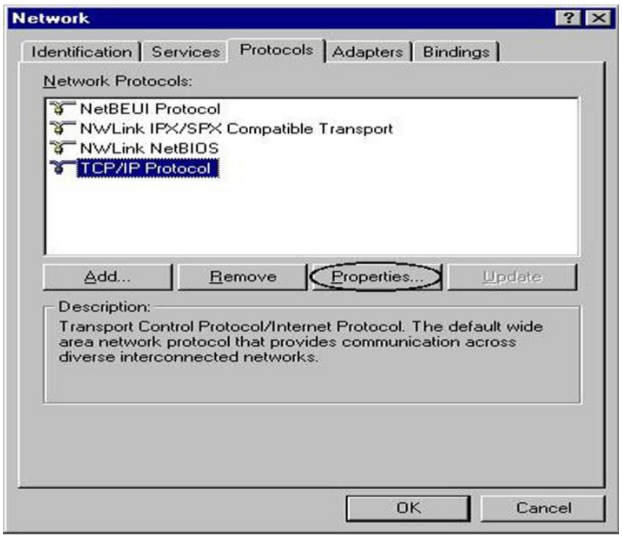
DNS Server Search Order

Domain Suffix Search Order

Configuring PC in Windows NT4.0

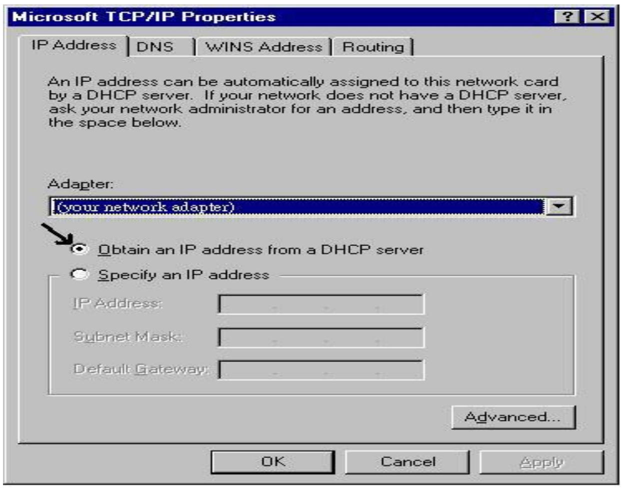
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**.



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

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address from a DHCP server

3.2 Factory Default Settings

Before configuring the FBR-1461 router, you need to know the following default settings.

Web Interface: (Username and Password)

Username: admin

Password: password

The default username and password are "**admin**" and "**password**" respectively.

Attention:

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

LAN Device IP Settings:

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

ISP setting in WAN site:

PPPoE

DHCP Server:

DHCP server is enabled.

Start IP Address: 192.168.1.2

IP pool counts: 253

3.3 LAN and WAN Port Addresses

The parameters of LAN and WAN ports are preset at the factory. The default values are shown below.

LAN Port		**WAN Port**
IP address	192.168.0.1	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP, but you have to set the username and password first.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled in ports 1, 2, 3, and 4	
IP addresses for distribution to PCs	253 IP addresses continuing from 192.168.0.2 through 192.168.0.254	

3.4 Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of services are provided, such as PPPoE, PPPoA, MPoA or Pure Bridge.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC1483 Bridged	VPI/VCI, VC-based/LLC-based multiplexing to use Bridged Mode.
RFC1483 Routed	VPI/VCI, VC-based/LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).

3.5 Configuring with your FBR-1461

Note:

1. To configure this device, you must have IE 5.0 / Netscape 4.5 or above installed
2. You may configure the router for Internet access in two ways:

   (A) Easy Sign On   (B) Web Configuration

Easy Sign On:

After setting up the router with the appropriate cables plugged, proceed to load your internet browser.

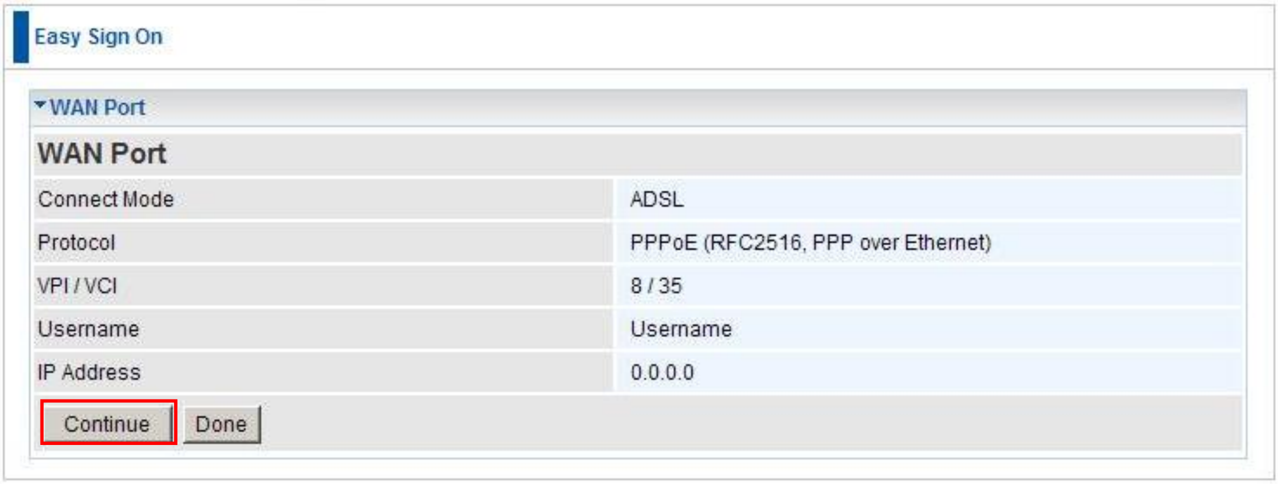
The Easy Sign On will start automatically and request you to enter some basic information obtained from your Service Provider. Once completed, you should be able to access the Internet.

Follow the Easy Sign On Wizard and it will guide you to complete the basic network configuration.

Note:

If Easy Sign-On does not start, please type in the address **http://192.168.0.1**, enter Username and Password (see page 2) and click **Quick Start**. The Quick Start process is the same as Easy Sign-On.

1. Click continue.



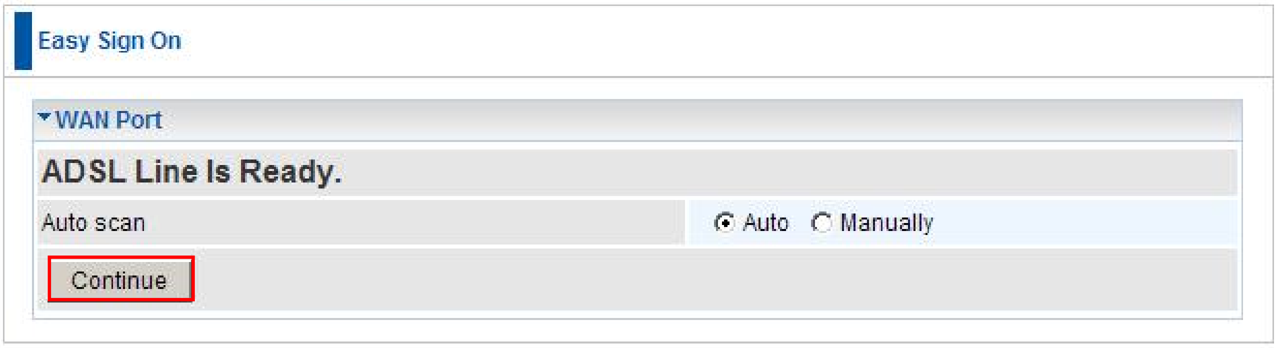
WAN Port

Connect Mode	ADSL
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

2. Choose “Auto” or “Manually” to scan ADSL settings.

Note:

If automatic detection does not work, please ask your ISP and enter the Protocol, VPI and VCI manually.



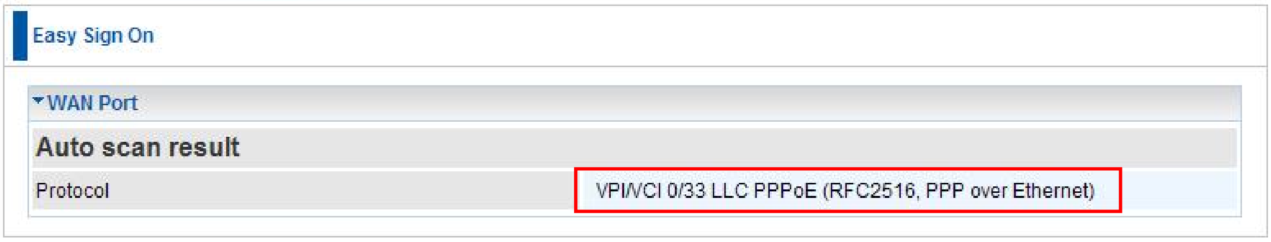
Easy Sign On

WAN Port

ADSL Line Is Ready.

Auto scan	● Auto ○ Manually

3. The Auto scan result is displayed



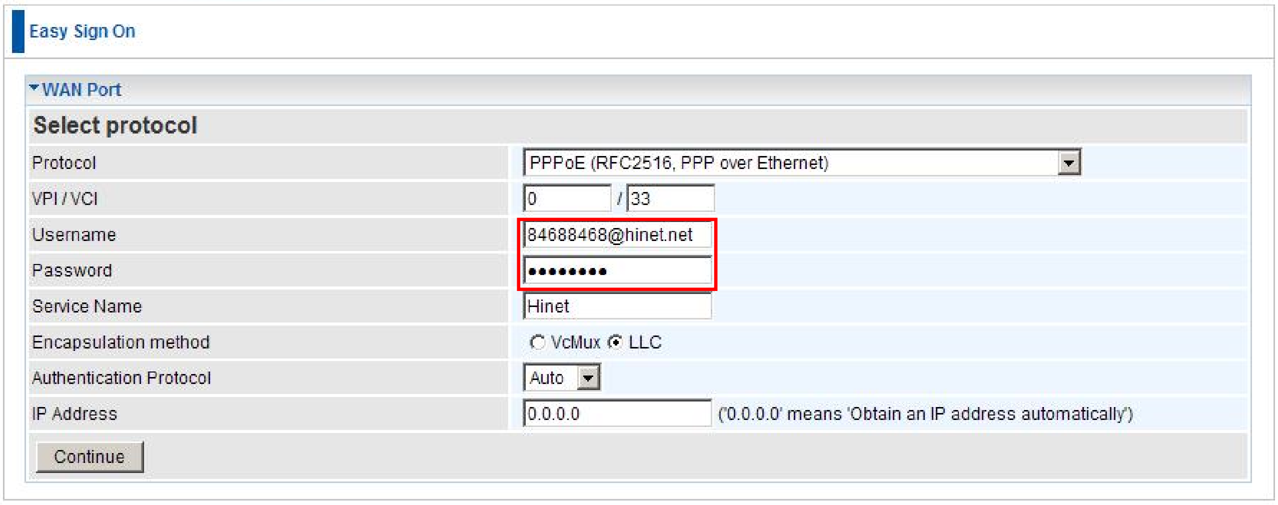
Easy Sign On

WAN Port

Auto scan result

Protocol	VPI/VCI 0/33 LLC PPPoE (RFC2516, PPP over Ethernet)

4. Please enter **“Username”** and **“Password”** as supplied by your ISP (Internet Service Provider) and click continue.



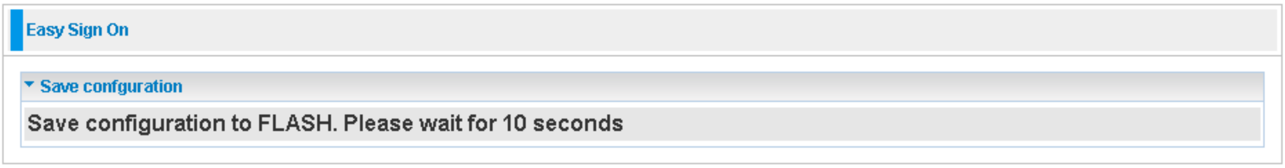
Easy Sign On

WAN Port

Select protocol

Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	0 / 33
Username	84688468@hinet.net
Password	••••••••
Service Name	Hinet
Encapsulation method	○ VcMux ● LLC
Authentication Protocol	Auto
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')

5. You’ve have completed the WAN port setup and now your Configuration will be saved.

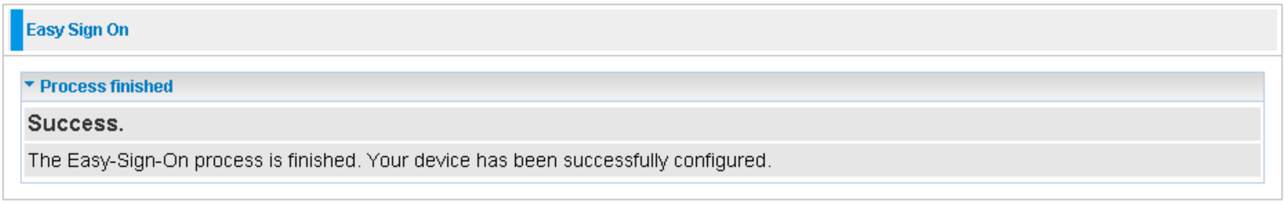


Easy Sign On

Save confguration

Save configuration to FLASH. Please wait for 10 seconds

6. Congratulations!! You’ve completed the setup procedure and you are now ready to surf the Internet, enjoy.



Easy Sign On

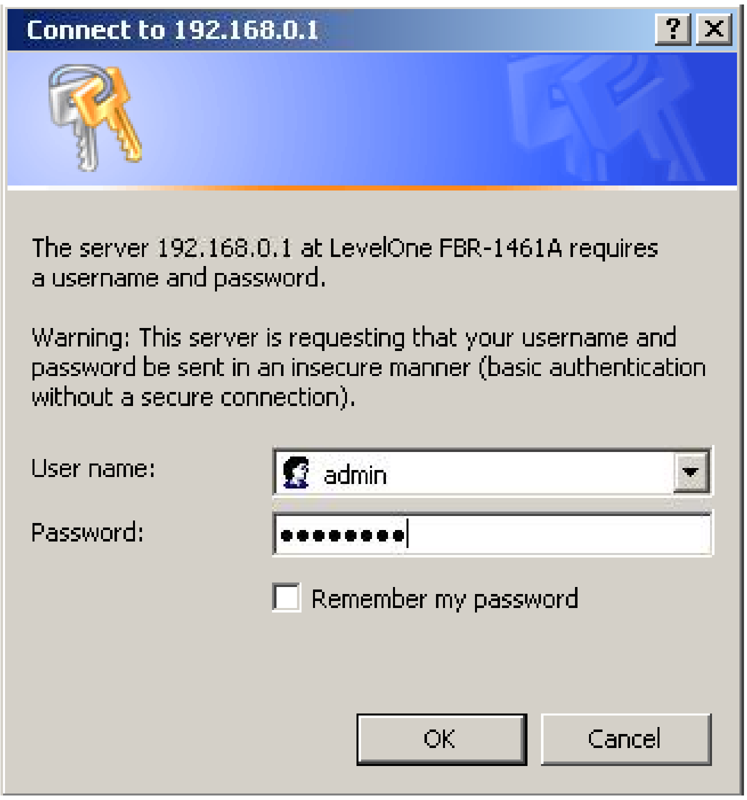
Process finished

Success.

The Easy-Sign-On process is finished. Your device has been successfully configured.

Web Configuration:

Open your web browser, enter the IP address of your router, which by default is **192.168.0.1**, and press the “Enter” key, a user name and password window prompt appears. The default username and password are **“admin”** and **“password”.**



The server 192.168.0.1 at LevelOne FBR-1461A requires a username and password.

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

User name: admin

Password: •••••••••

□ Remember my password

Congratulations! You have successfully logged on to your FBR-1461 Modem Router!

Chapter 4

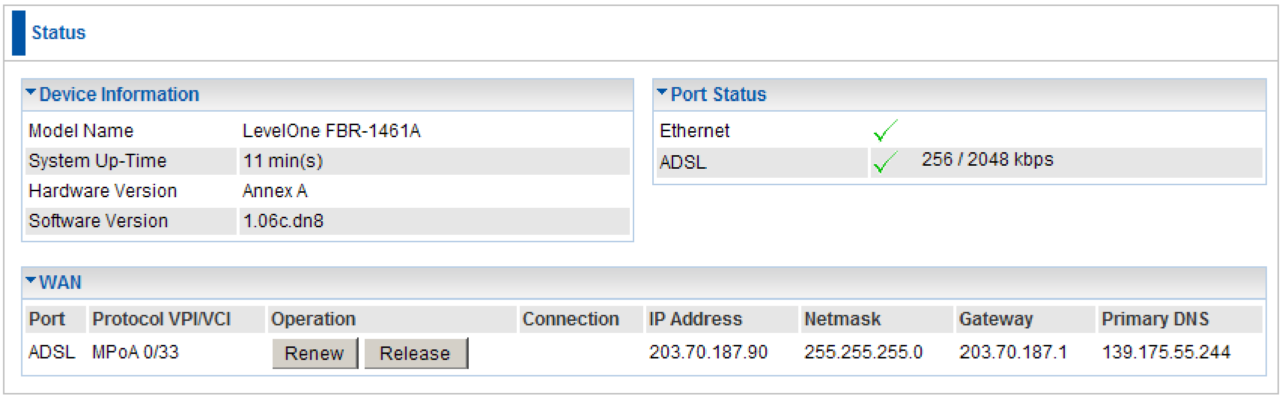
Basic Configuration

Once you have logged on to your FBR-1461 Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Advance** (Switch to Advance Configuration mode)
- **Status**
- **Quick Start**
- **WAN**

4.1 Status

This page shows you the current status of the FBR-1461.



Status

Device Information

Model Name	LevelOne FBR-1461A
System Up-Time	11 min(s)
Hardware Version	Annex A
Software Version	1.06c.dn8

Port Status

Ethernet	✓	
ADSL	✓	256 / 2048 kbps

WAN

Port	Protocol VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL	MPoA 0/33	Renew Release		203.70.187.90	255.255.255.0	203.70.187.1	139.175.55.244

Device Information

- **Model Name:** The model name of the device.
- **System Up-Time:** Records system up-time.
- **Hardware Version:** Device version
- **Software Version:** Firmware version

Port Status

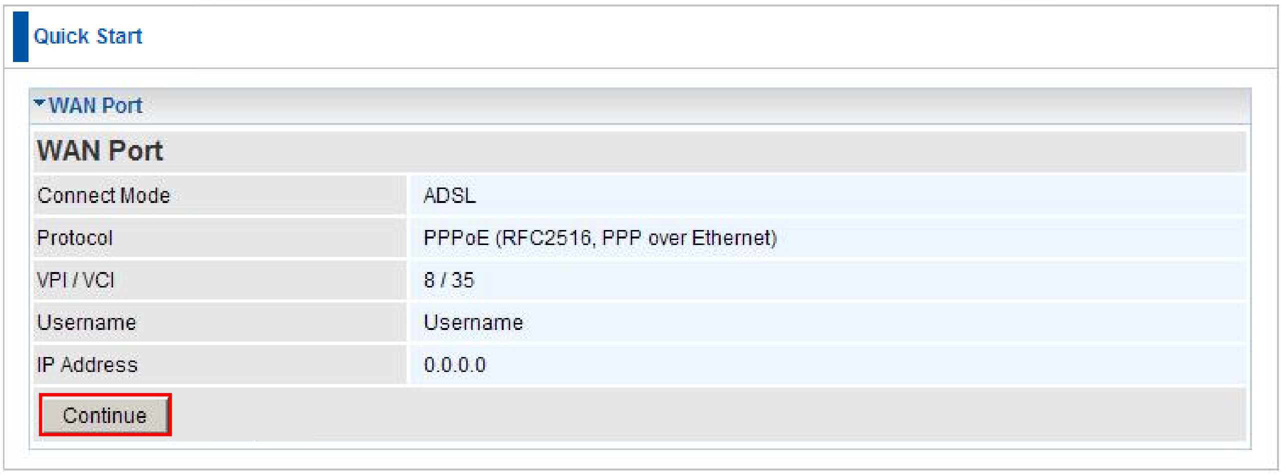
- **Port Status**：User can look up to see if they are connected to Ethernet, ADSL or Wireless.

WAN

- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** Current available operation.
- **Connection:** The current connection status.
- **IP Address:** WAN port IP address.
- **Netmask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.
- **Primary DNS:** The IP address of the primary DNS server.

4.2 Quick Start

This wizard is similar to Easy Sign On, and will guide you through setting up your FBR-1461. Click Continue to start the wizardz.

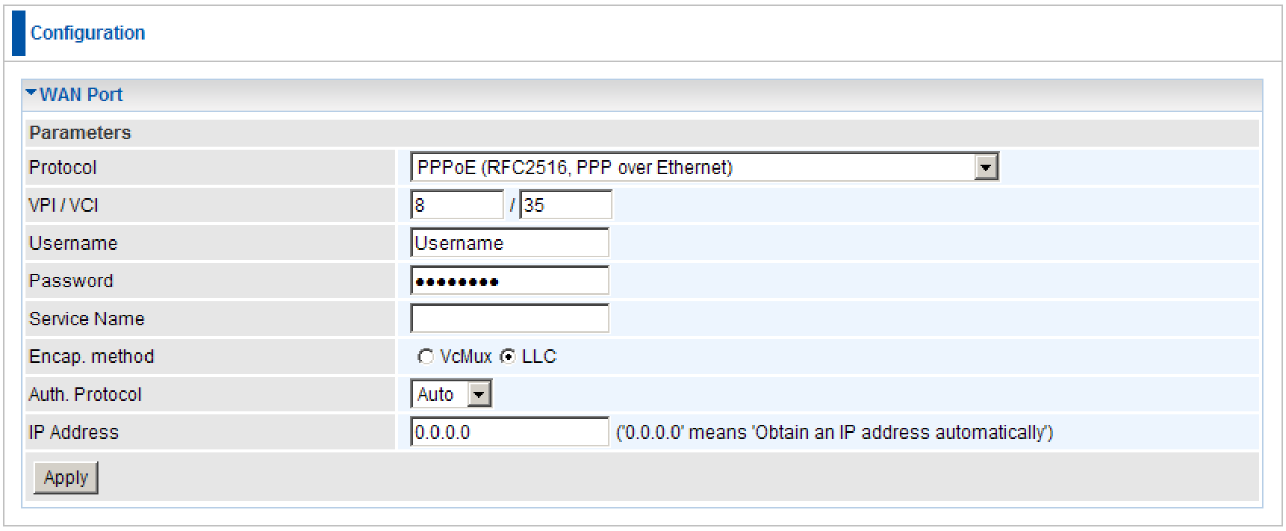


WAN Port

Connect Mode	ADSL
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

4.3 WAN

Here you can manually enter the ADSL settings provided by your Service Provider. Use this if the Easy Sign On, or Quick Start cannot successfully auto-detect your ADSL settings.



Configuration

WAN Port

Parameters	
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
Password	••••••••
Service Name	
Encap. method	○ VcMux ● LLC
Auth. Protocol	Auto
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')

- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)
- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Auth. Protocol:** Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

Chapter 5

Advance Configuration

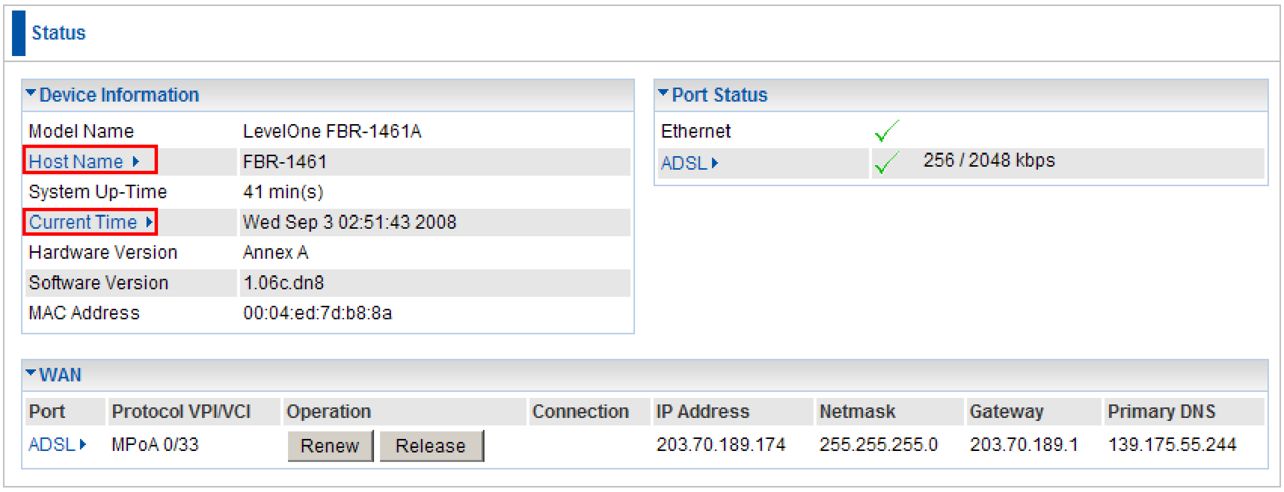
Once you have logged on to your FBR-1461 Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Basic** (Switch to Basic Configuration Mode)
- **Status** (ADSL Status, ARP Table, DHCP Table, System Log, Firewall Log, UPnP Portmap)
- **Quick Start**
- **Configuration** (LAN, WAN, System, Firewall, QoS, Virtual Server, Time Schedule and Advanced)

The following sections provide an overview of the settings available for configuring your router.

5.1 Status

This page shows you the current status of the FBR-1461, with advanced options such as Host Name and Time settings.



Status

Device Information

Model Name	LevelOne FBR-1461A
Host Name ▸	FBR-1461
System Up-Time	41 min(s)
Current Time ▸	Wed Sep 3 02:51:43 2008
Hardware Version	Annex A
Software Version	1.06c.dn8
MAC Address	00:04:ed:7d:b8:8a

Port Status

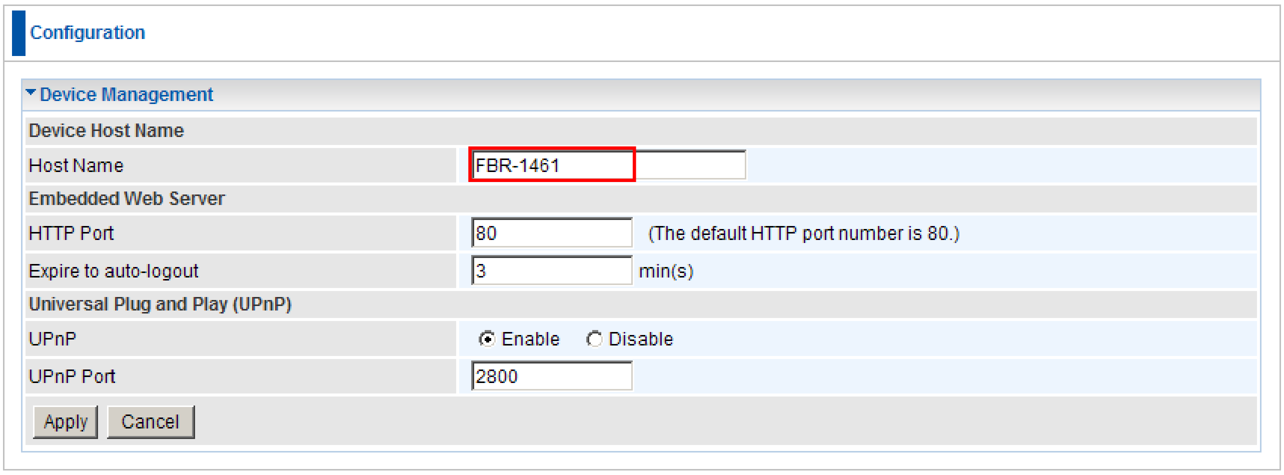
Ethernet	✓	
ADSL ▸	✓	256 / 2048 kbps

WAN

Port	Protocol VPI/VCI	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
ADSL ▸	MPoA 0/33	Renew Release		203.70.189.174	255.255.255.0	203.70.189.1	139.175.55.244

Device Information

- **Model Name:** The model name of the device.
- **Host Name:** Provide a name for the router for identification purposes. Host Name lets you change the router name. Click on **Host Name** to direct you to the following page:



Configuration

Device Management

Device Host Name	
Host Name	FBR-1461
Embedded Web Server	
HTTP Port	80 (The default HTTP port number is 80.)
Expire to auto-logout	3 min(s)
Universal Plug and Play (UPnP)	
UPnP	● Enable ○ Disable
UPnP Port	2800

Apply Cancel

- **System Up-Time:** Records system up-time.
- **Current time:** Set the current time. See the Time Zone section for more information.
- **Hardware Version:** Device version.
- **Software Version:** Firmware version.
- **MAC Address:** The LAN MAC address.

WAN

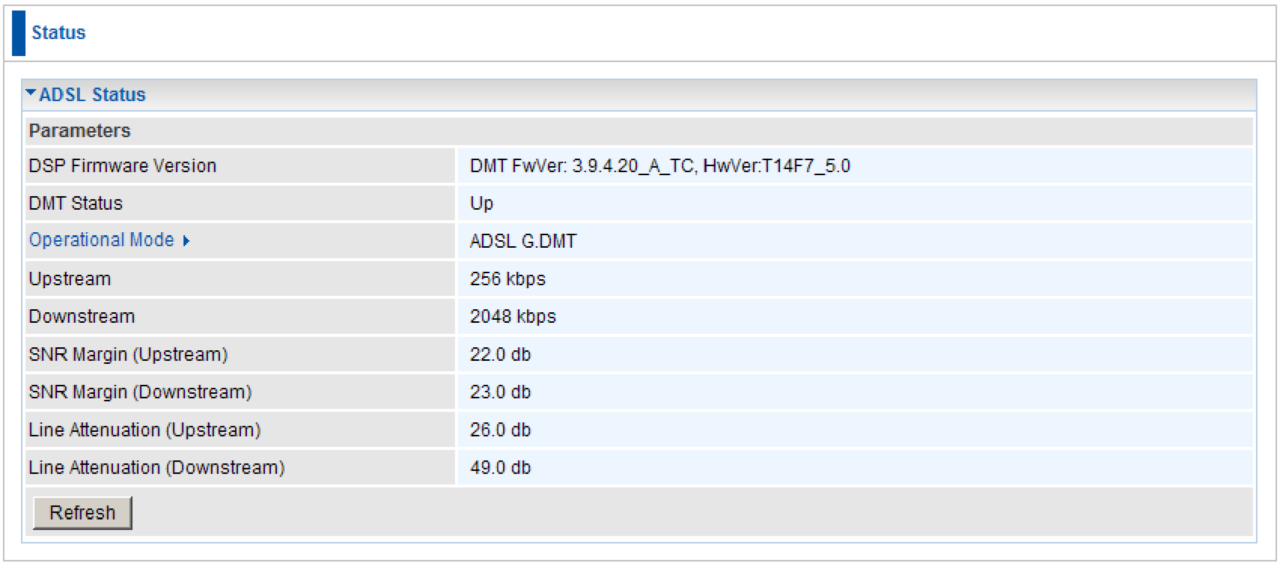
- **Port:** Name of the WAN connection.
- **Protocol VPI/VCI:** Virtual Path Identifier and Virtual Channel Identifier
- **Operation:** Current available operation.
- **Connection:** The current connection status.
- **IP Address:** WAN port IP address.
- **Netmask:** WAN port IP subnet mask.
- **Gateway:** The IP address of the default gateway.
- **Primary DNS:** The IP address of the primary DNS server.

Port Status

- **Port Status**：User can look up to see if they are connected to Ethernet, ADSL or Wireless.

5.1.1 ADSL Status

This page shows you the current status of the FBR-1461’s ADSL connection.

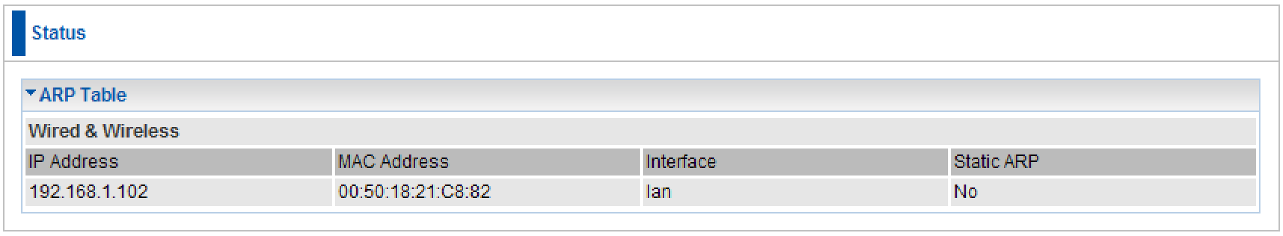


Parameters	
DSP Firmware Version	DMT FwVer: 3.9.4.20_A_TC, HwVer:T14F7_5.0
DMT Status	Up
Operational Mode ▸	ADSL G.DMT
Upstream	256 kbps
Downstream	2048 kbps
SNR Margin (Upstream)	22.0 db
SNR Margin (Downstream)	23.0 db
Line Attenuation (Upstream)	26.0 db
Line Attenuation (Downstream)	49.0 db

- **DSP Firmware Version:** DSP code version
- **DMT Status:** Current DMT Status
- **Operational Mode:** To show the state when user select “AUTO” on connect mode.
- **Upstream:** Upstream rate.
- **Downstream:** Downstream rate.
- **SNR Margin (Upstream):** This is noise margin in upstream.
- **SNR Margin (Downstream):** This is noise margin in downstream.
- **Line Attenuation (Upstream):** This is attenuation of signal in upstream.
- **Line Attenuation (Downstream):** This is attenuation of signal in downstream.

5.1.2 ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.



Status

ARP Table

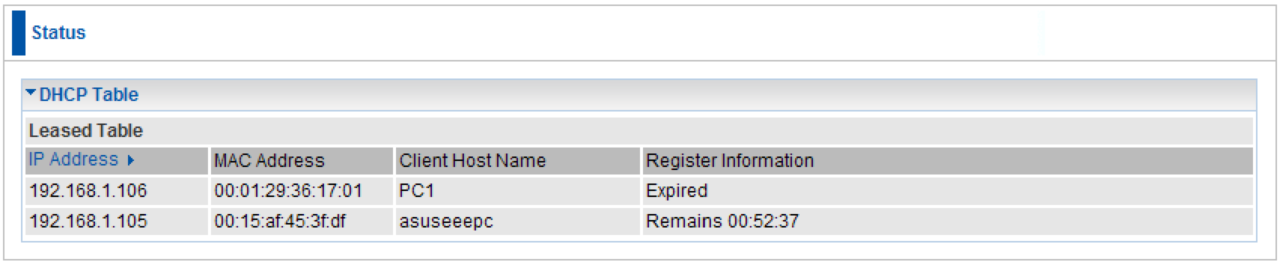
Wired & Wireless

IP Address	MAC Address	Interface	Static ARP
192.168.1.102	00:50:18:21:C8:82	lan	No

- **IP Address:** It is IP Address of internal host that join this network.
- **MAC Address:** The MAC address of internal host.

5.1.3 DHCP Table

This page shows you the network clients (Notebooks or PCs) that are allocated IP Addresses by the FBR-1461's DHCP Server.



Status

DHCP Table

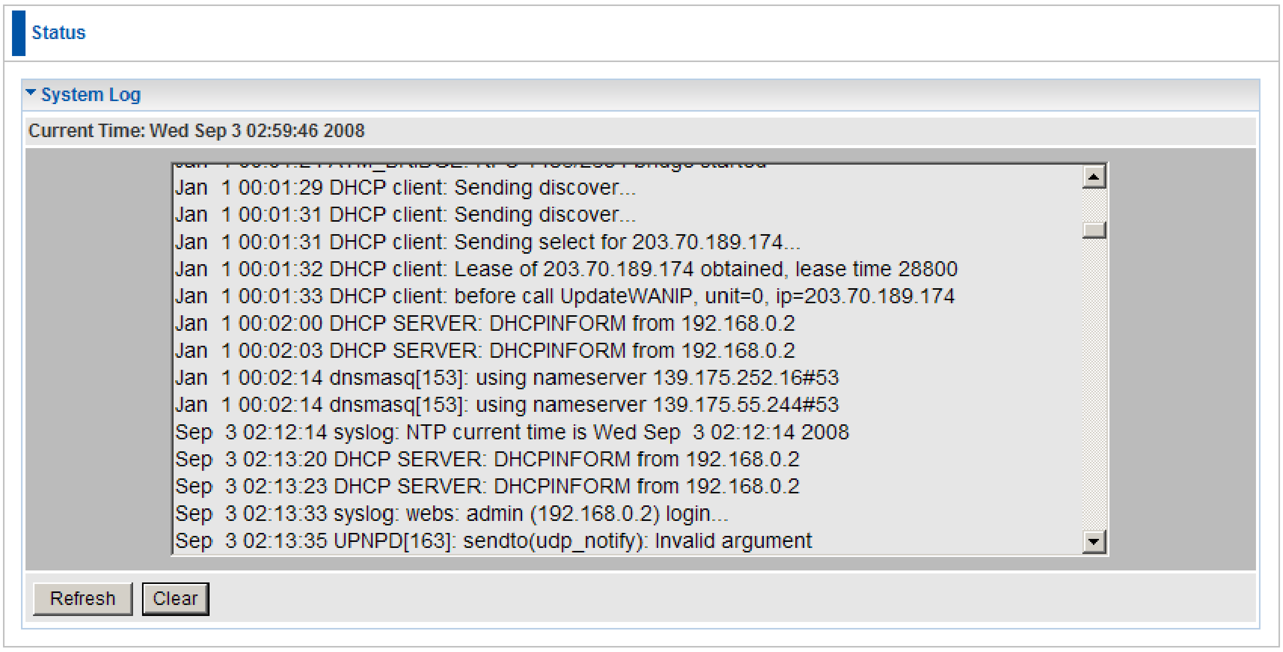
Leased Table

IP Address ▸	MAC Address	Client Host Name	Register Information
192.168.1.106	00:01:29:36:17:01	PC1	Expired
192.168.1.105	00:15:af:45:3f:df	asuseeepc	Remains 00:52:37

- **IP Address:** The current corresponding DHCP-assigned dynamic IP address of the device.
- **MAC Address:** The MAC Address of internal dhcp client host.
- **Client Host Name:** The Host Name of internal dhcp client.
- **Register Information:** Register time information

5.1.4 System Log

Display system logs accumulated up to the present time. You can trace historical information with this function.

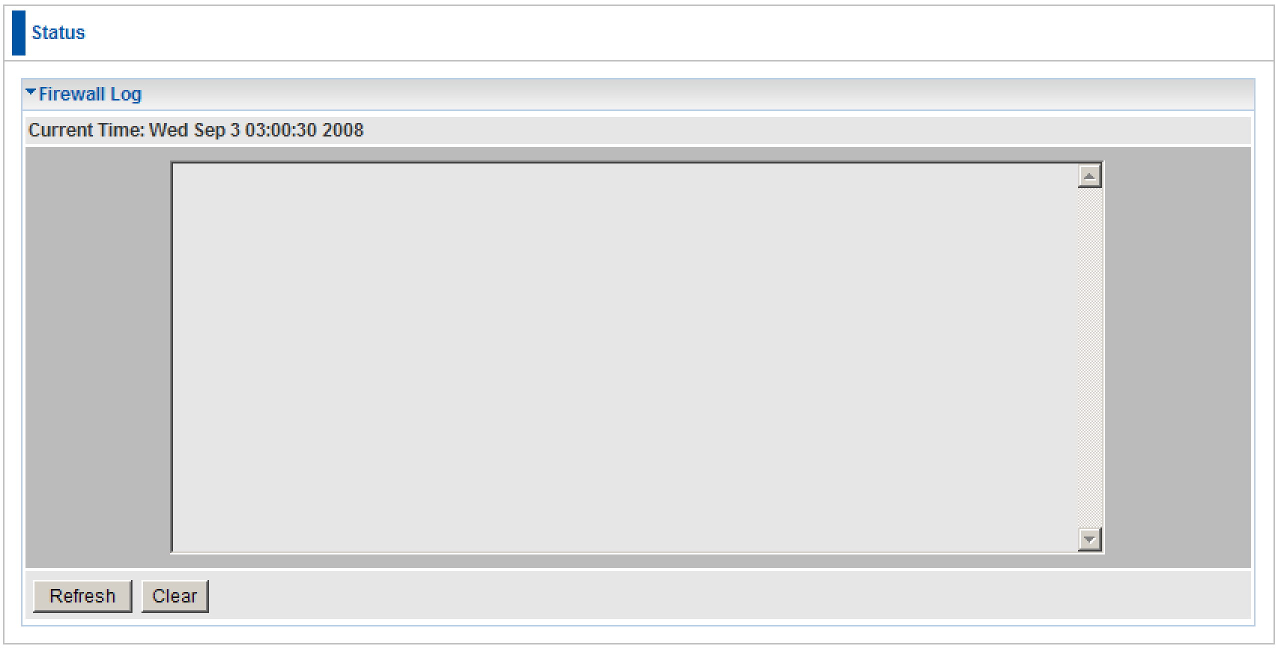


Current Time: Wed Sep 3 02:59:46 2008

```
Jan  1 00:01:29 DHCP client: Sending discover...
Jan  1 00:01:31 DHCP client: Sending discover...
Jan  1 00:01:31 DHCP client: Sending select for 203.70.189.174...
Jan  1 00:01:32 DHCP client: Lease of 203.70.189.174 obtained, lease time 28800
Jan  1 00:01:33 DHCP client: before call UpdateWANIP, unit=0, ip=203.70.189.174
Jan  1 00:02:00 DHCP SERVER: DHCPINFORM from 192.168.0.2
Jan  1 00:02:03 DHCP SERVER: DHCPINFORM from 192.168.0.2
Jan  1 00:02:14 dnsmasq[153]: using nameserver 139.175.252.16#53
Jan  1 00:02:14 dnsmasq[153]: using nameserver 139.175.55.244#53
Sep  3 02:12:14 syslog: NTP current time is Wed Sep  3 02:12:14 2008
Sep  3 02:13:20 DHCP SERVER: DHCPINFORM from 192.168.0.2
Sep  3 02:13:23 DHCP SERVER: DHCPINFORM from 192.168.0.2
Sep  3 02:13:33 syslog: webs: admin (192.168.0.2) login...
Sep  3 02:13:35 UPNPD[163]: sendto(udp_notify): Invalid argument
```

5.1.5 Firewall Log

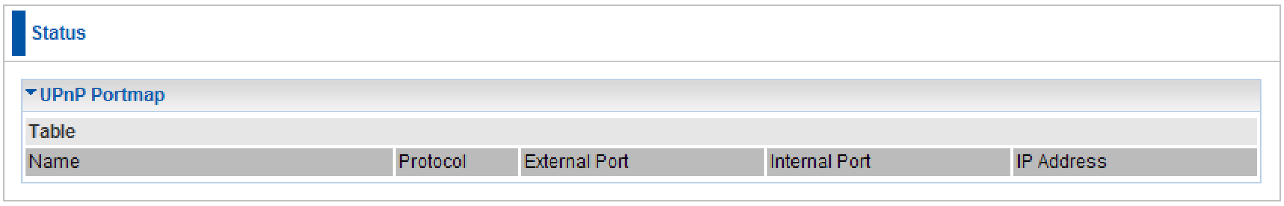
Firewall Log displays log information of any unexpected action with your firewall settings. This page displays the router's Firewall Log entries. The log shows log entries when you have enabled Intrusion Detection or Block WAN PING in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



Current Time: Wed Sep 3 03:00:30 2008

5.1.6 UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). Please see the Advanced section of this manual for more details on UPnP and the router's UPnP configuration options.

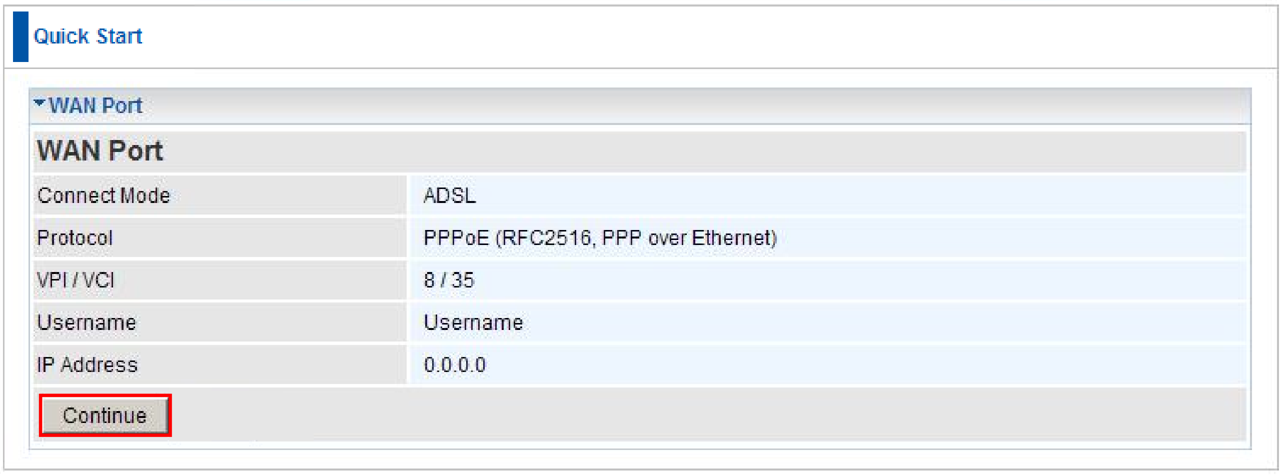


Table

Name	Protocol	External Port	Internal Port	IP Address

5.2 Quick Start

This wizard is similar to Easy Sign On, and will guide you through setting up your FBR-1461. Click ”Continue” to start the wizard.



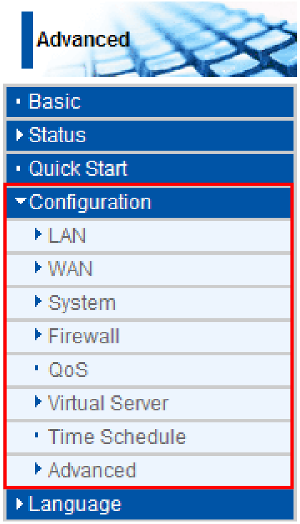
WAN Port

Connect Mode	ADSL
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI / VCI	8 / 35
Username	Username
IP Address	0.0.0.0

- **Connect mode:** ADSL
- **Protocol:** The current ATM protocol in the device
- **VPI / VCI:** The current value of VPI / VCI in the device
- **IP address:** To show current value of IP address in the device.

5.3 Configuration

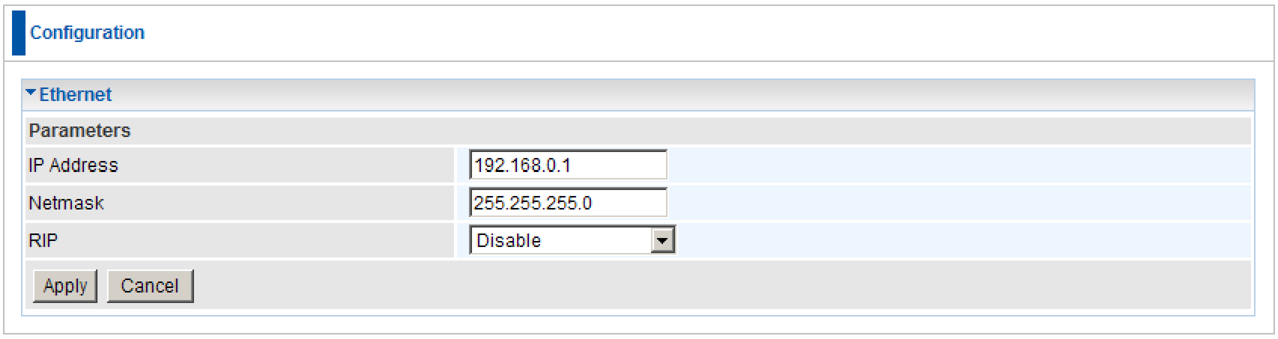
Click this item to access the following sub-items that configure the ADSL router: **LAN, WAN, System, Firewall, QoS, Virtual Server, Time Schedule** and **Advanced.**
These functions are described in the following sections.



5.3.1 LAN (Local Area Network)

A Local Area Network (LAN) is a shared communication system to which many computers are attached and is limited to the immediate area, usually the same building or floor of a building.
There are six items within the LAN section: **Ethernet, IP Alias, Wireless, Wireless Security,** and **DHCP Server**.

5.3.1.1 Ethernet



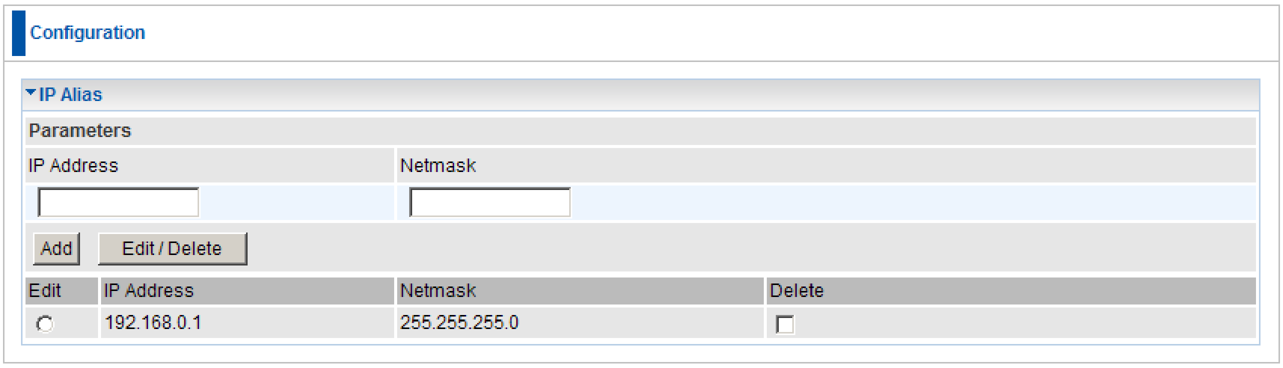
Parameters	
IP Address	192.168.0.1
Netmask	255.255.255.0
RIP	Disable

The router supports more than one Ethernet IP addresses in the LAN, and with distinct LAN subnets through which you can access the Internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.0.1.

- **IP Address:** The default IP on this router.
- **Netmask:** The default subnet mask on this router.
- **RIP:** RIP v1, RIP v2 Broadcast, RIP v2 Multicast and RIP v1+v2 Broadcast.

5.3.1.2 IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



Edit	IP Address	Netmask	Delete
○	192.168.0.1	255.255.255.0	□

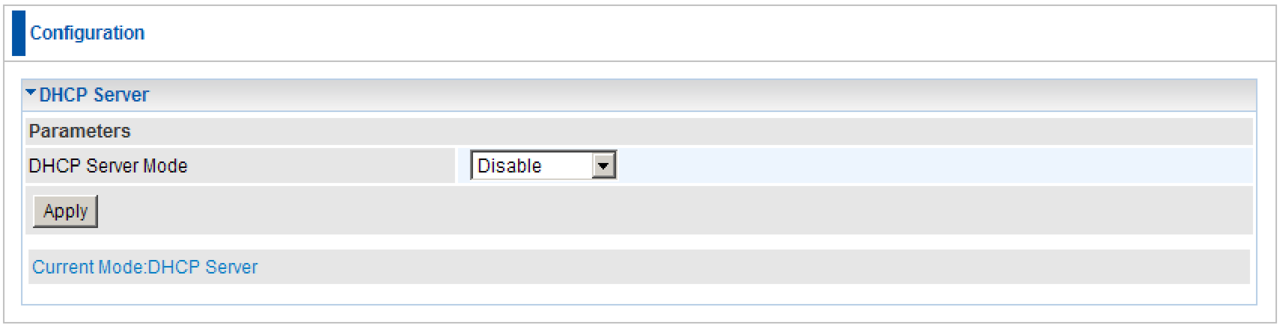
- **IP Address:** Specify an IP address on this virtual interface.
- **Netmask:** Specify a subnet mask on this virtual interface.

5.3.1.6 DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

DHCP Server Mode: Disable

To disable the router's DHCP Server, check **Disabled** and then click **Apply.** When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (the default is 192.168.0.1).

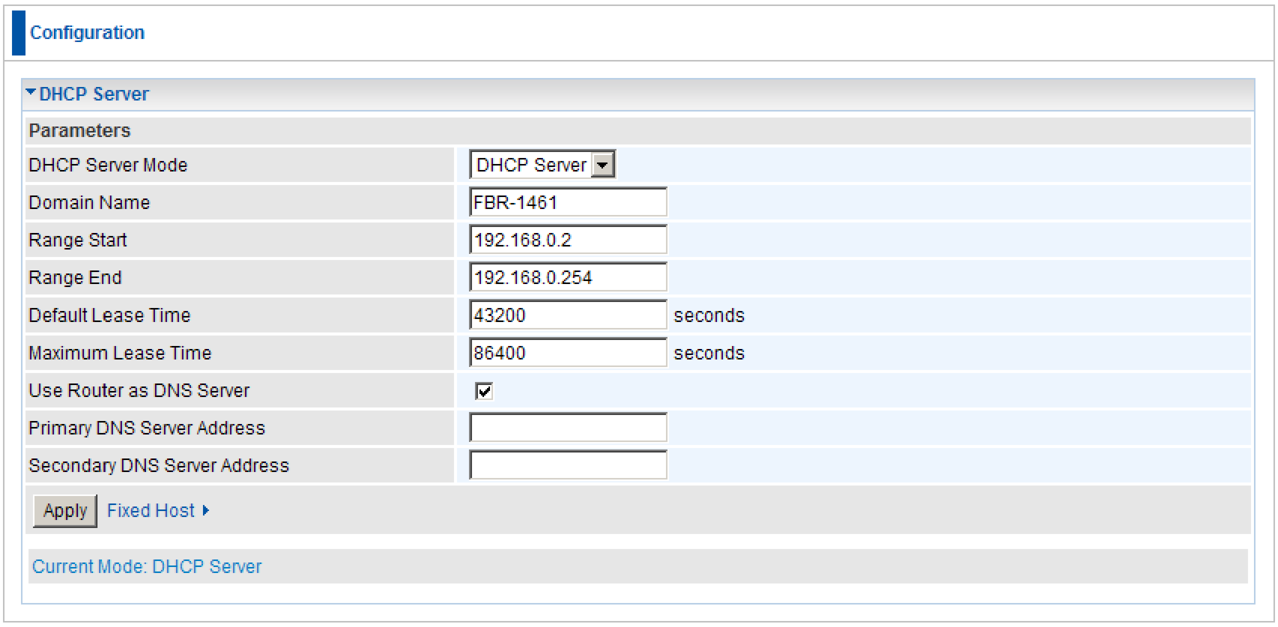


DHCP Server Mode: Disable

Current Mode:DHCP Server

DHCP Server Mode: DHCP Server

To configure the router's DHCP Server, check **DHCP Server**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router performs the domain name lookup, finds the IP address from the outside network automatically and forwards it back to the requesting PC in the LAN (your Local Area Network).



Configuration

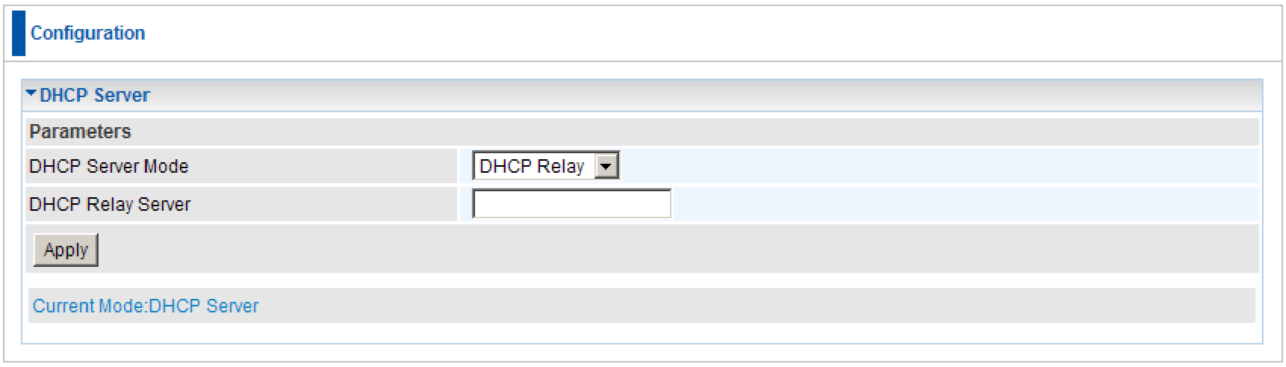
▼DHCP Server

Parameters	
DHCP Server Mode	DHCP Server ▾
Domain Name	FBR-1461
Range Start	192.168.0.2
Range End	192.168.0.254
Default Lease Time	43200 seconds
Maximum Lease Time	86400 seconds
Use Router as DNS Server	☑
Primary DNS Server Address	
Secondary DNS Server Address	

Current Mode: DHCP Server

- **DHCP Server Mode: DHCP Relay**

If you check **DHCP Relay** and then you must enter the IP address of the DHCP server which assigns an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click **Apply** to enable this function.



Configuration

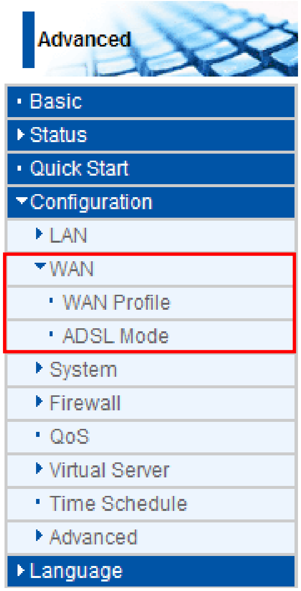
▼DHCP Server

Parameters	
DHCP Server Mode	DHCP Relay ▾
DHCP Relay Server	

Current Mode:DHCP Server

5.3.2 WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are two items within the **WAN** section: **WAN Profile** and **ADSL Mode.**

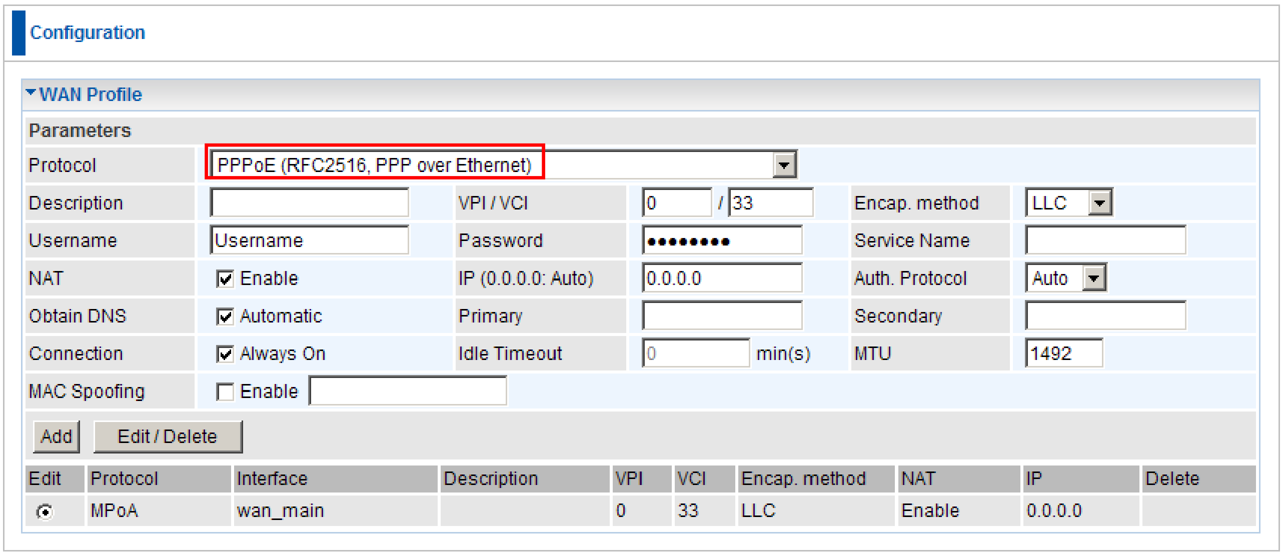


5.3.2.1 WAN Profile

Profile Port--ADSL

PPPoE Connection

PPPoE (PPP over Ethernet) provides access control in a manner similar to dial-up services using PPP.



Configuration

▾WAN Profile

Parameters					
Protocol	PPPoE (RFC2516, PPP over Ethernet) ▾				
Description		VPI / VCI	0 / 33	Encap. method	LLC ▾
Username	Username	Password	●●●●●●●●	Service Name	
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Auto ▾
Obtain DNS	☑ Automatic	Primary		Secondary	
Connection	☑ Always On	Idle Timeout	0 min(s)	MTU	1492
MAC Spoofing	☐ Enable				

Add | Edit / Delete

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
●	MPoA	wan_main		0	33	LLC	Enable	0.0.0.0	

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive)
- **Service Name:** This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

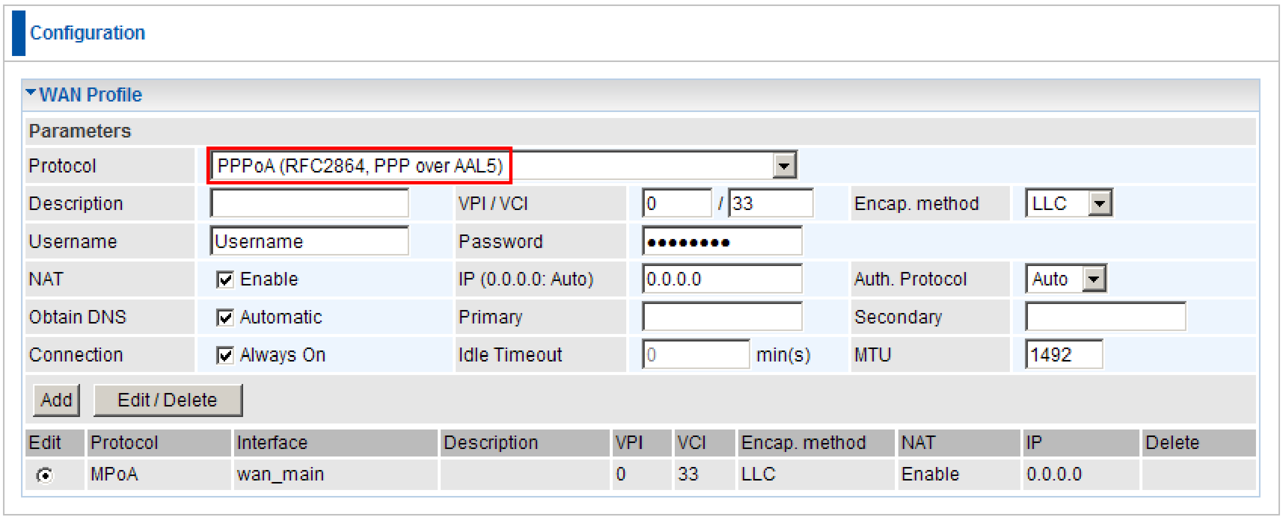
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Auth. Protocol:** Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
- **Connection:**

  ⊙**Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

  ⊙**Connect to Demand (un-select Always On):** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.
- **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.
- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

PPPoA Connection

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). It provides access control and billing functionality in a manner similar to dial-up services using PPP.



Configuration

WAN Profile

Parameters

Protocol	PPPoA (RFC2864, PPP over AAL5)				
Description		VPI / VCI	0 / 33	Encap. method	LLC
Username	Username	Password	••••••••		
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Auto
Obtain DNS	☑ Automatic	Primary		Secondary	
Connection	☑ Always On	Idle Timeout	0 min(s)	MTU	1492

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
●	MPoA	wan_main		0	33	LLC	Enable	0.0.0.0	

- **Description:** User-definable name for the connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encapsulation method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP
- **Username:** Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.
- **Password:** Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Authentication Protocol:** Default is **Auto**. Your ISP should advises you on whether to use **Chap** or **Pap.**
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

- **Connection:**

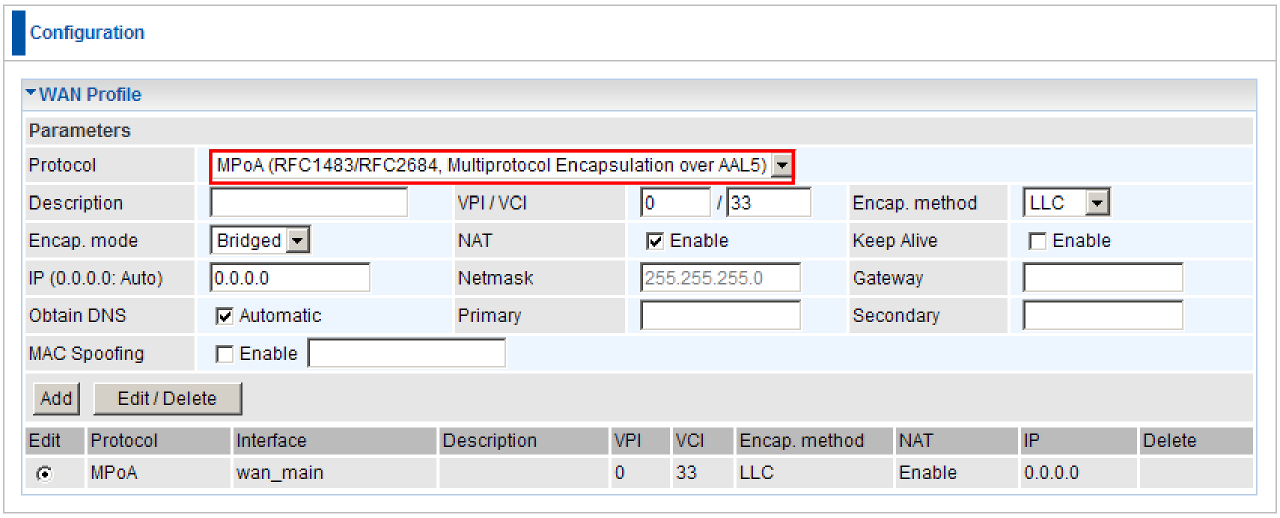
  ⦿ **Always on:** The router will establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

  ⦿ **Connect to Demand (un-select Always On):** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time.

- **Idle Timeout:** Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. The minimum value is 10 minutes.

- **MTU:** Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that the IP attempts to send through the interface.

MPoA Connection

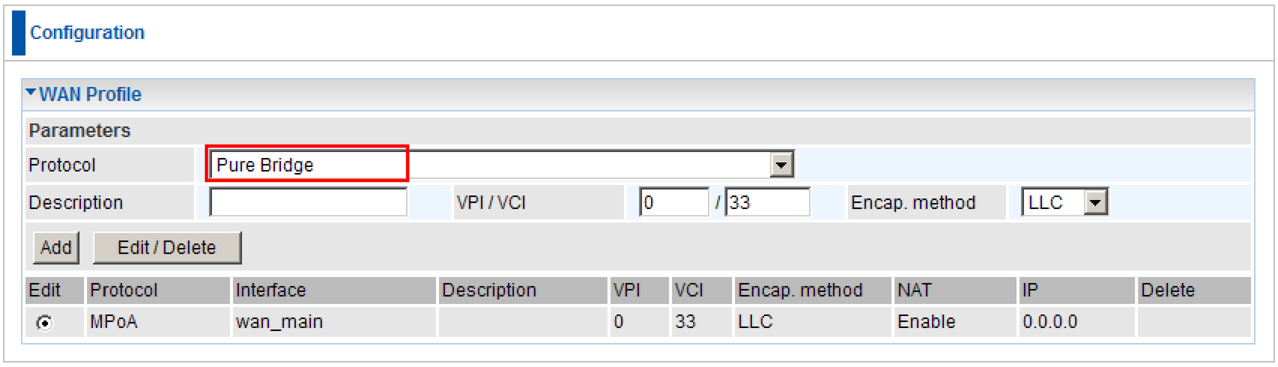


Protocol	MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5) ▾				
Description		VPI / VCI	0 / 33	Encap. method	LLC ▾
Encap. mode	Bridged ▾	NAT	☑ Enable	Keep Alive	☐ Enable
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	255.255.255.0	Gateway	
Obtain DNS	☑ Automatic	Primary		Secondary	
MAC Spoofing	☐ Enable				

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
◉	MPoA	wan_main		0	33	LLC	Enable	0.0.0.0	

- **Description:** Your description of this connection.
- **VPI and VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, the default is LLC. Select the one provided by your ISP.
- **Encap. mode:** Choose whether you want the device to function as bridge mode or routing mode.
- **NAT:** The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.
- **IP Address:** Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.
- **Netmask:** The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given)
- **Gateway:** Enter the IP address of the default gateway.
- **Obtain DNS Automatically:** Select this check box to use DNS.
- **Primary DNS/ Secondary DNS:** Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Pure Bridge Connections



Parameters

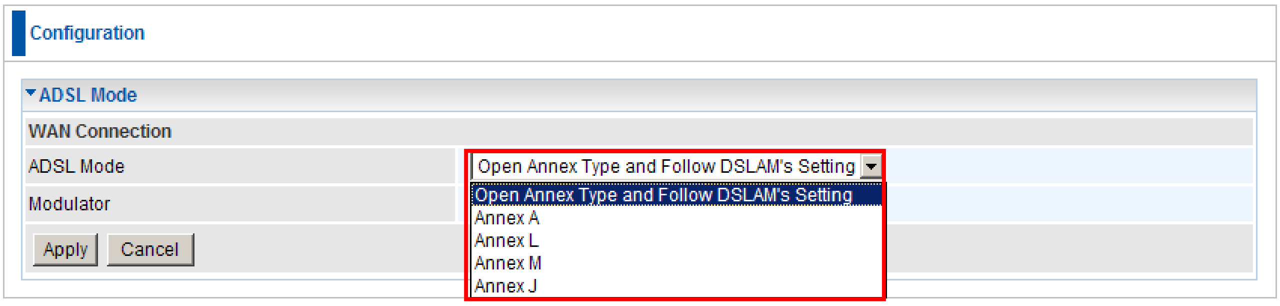
Protocol	Pure Bridge				
Description		VPI / VCI	0 / 33	Encap. method	LLC

Edit	Protocol	Interface	Description	VPI	VCI	Encap. method	NAT	IP	Delete
●	MPoA	wan_main		0	33	LLC	Enable	0.0.0.0	

- **Description:** A user-definable name for this connection.
- **VPI/VCI:** Enter the VPI and VCI information provided by your ISP.
- **Encap. method:** Select the encapsulation format, this is provided by your ISP.

5.3.2.3 ADSL Mode

FBR-1461A (Annex A)



Configuration

ADSL Mode

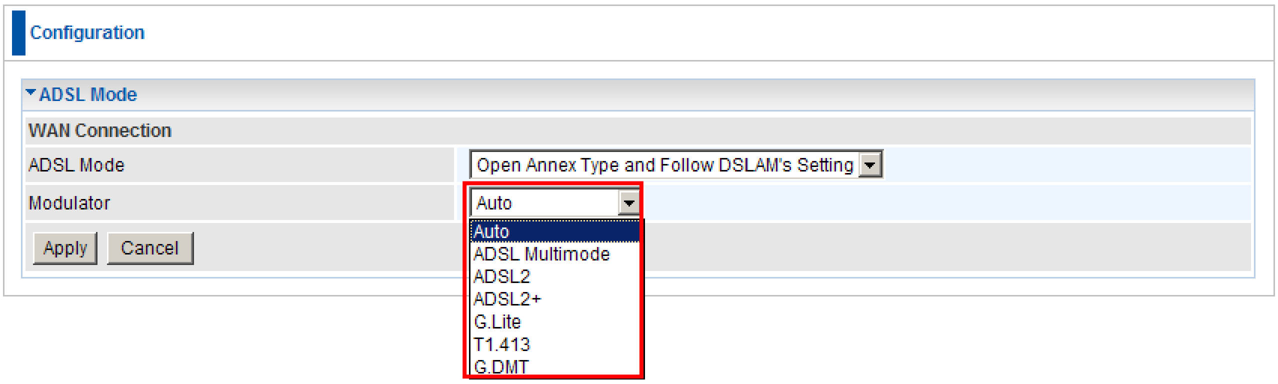
WAN Connection

ADSL Mode: Open Annex Type and Follow DSLAM's Setting

Modulator

- **ADSL Mode:** There are four modes “**Open Annex Type and Follow DSLAM’s Setting**”, ”**Annex A**”, ”**Annex L**”, ”**Annex M**” and **“Annex J”** that user can select for this connection.

- **Modulator:** There are seven modes “**AUTO**”,”**ADSL multimode**”,”**ADSL2**”,”**ADSL2+**”, **“G.Lite:**”, **“T1.413”** and **“G.DMT”** that user can select for this connection.



Configuration

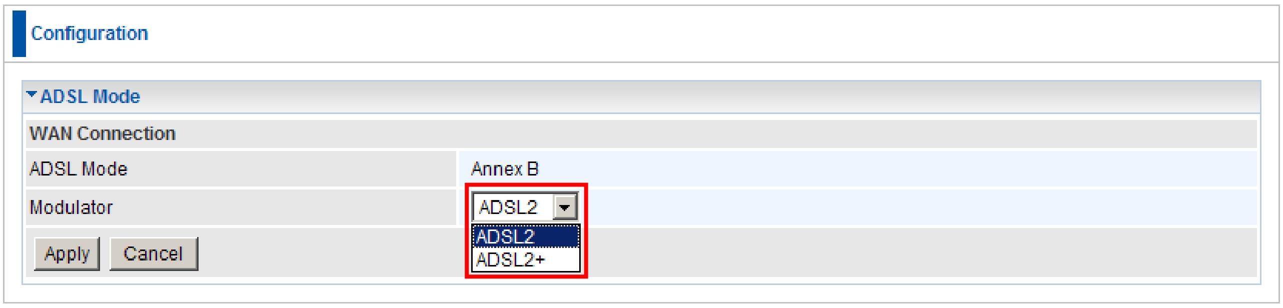
ADSL Mode

WAN Connection

ADSL Mode: Open Annex Type and Follow DSLAM's Setting

Modulator: Auto

FBR-1461B (Annex B)



Configuration

ADSL Mode

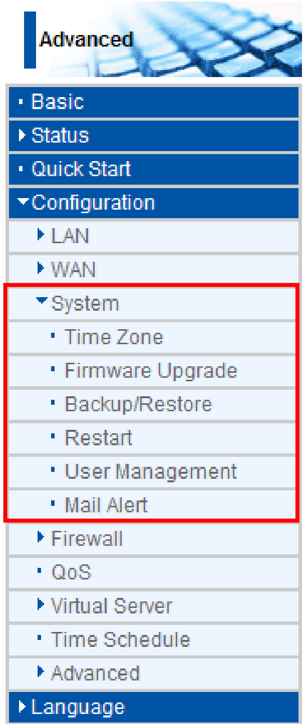
WAN Connection	
ADSL Mode	Annex B
Modulator	ADSL2

FBR-1461B is Annex B only.

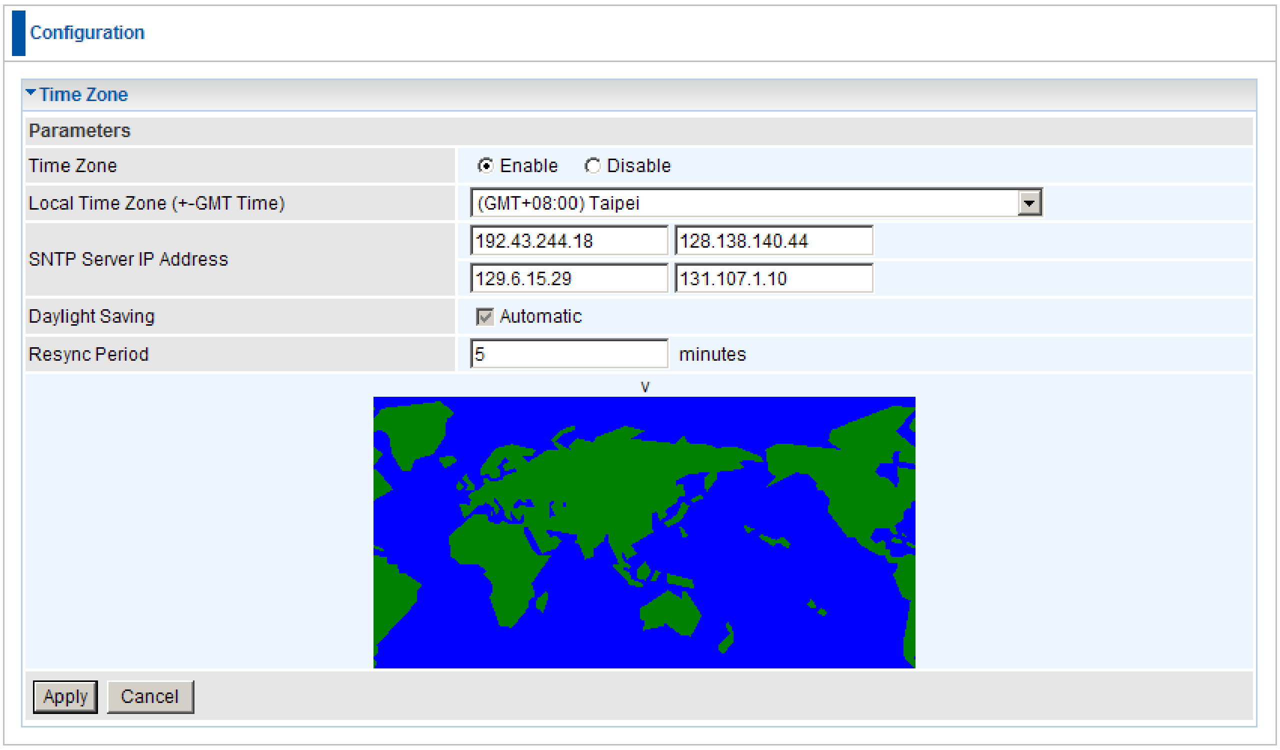
- **Modulator:** There are two modes”**ADSL2**” and”**ADSL2+**” that user can select for this connection.

5.3.3 System

There are six items within the **System** section: **Time Zone, Firmware Upgrade, Backup/Restore, Restart**, **User Management** and **Mail Alert.**



5.3.3.1 Time Zone



Configuration

▾ Time Zone

Parameters	
Time Zone	● Enable ○ Disable
Local Time Zone (+-GMT Time)	(GMT+08:00) Taipei
SNTP Server IP Address	192.43.244.18 128.138.140.44 129.6.15.29 131.107.1.10
Daylight Saving	☑ Automatic
Resync Period	5 minutes

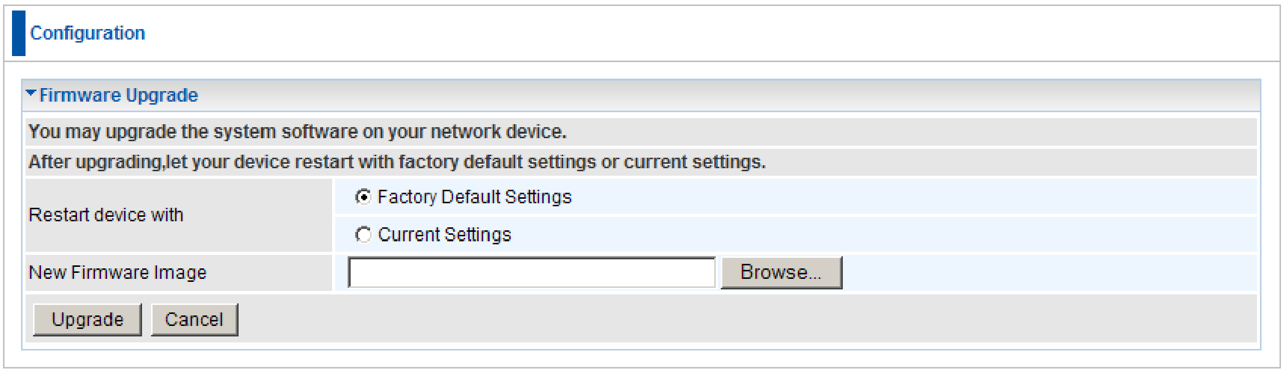
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router retrieves the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Resync Period (in minutes) is the periodic interval the router waits before it resynchronizes the router's time with that of the specified SNTP server. To avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

5.3.3.2 Firmware Upgrade

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified. Your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** allows you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.



You may upgrade the system software on your network device.

After upgrading,let your device restart with factory default settings or current settings.

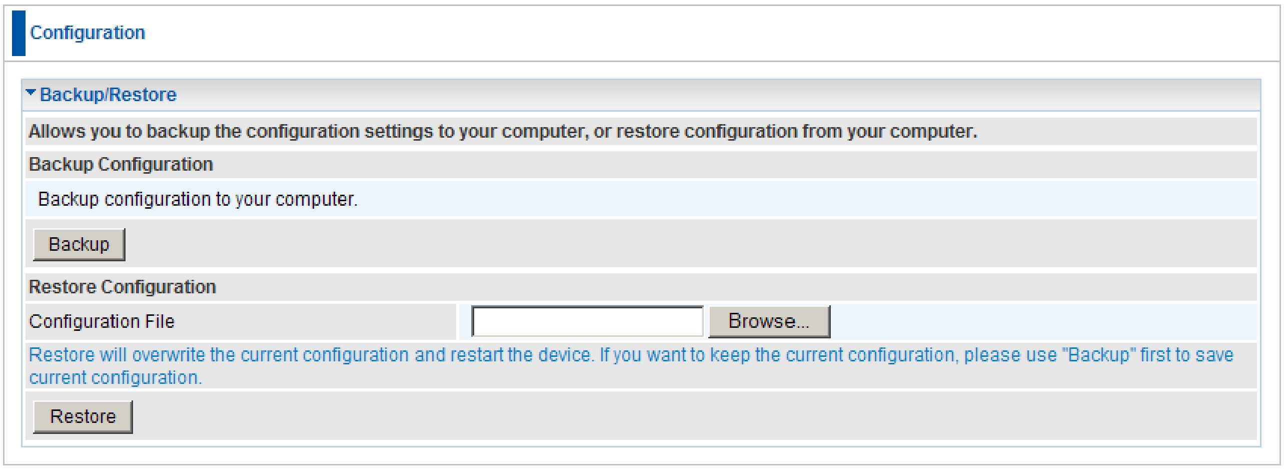
Restart device with	● Factory Default Settings ○ Current Settings
New Firmware Image	Browse...

- **Restart Device with:** To choose "Factory Default Settings" or "Current Settings" which uses your current setting on the new firmware (it is highly advised to use Factory Default Settings over Current Settings for a clean firmware upgrade).
- **New Firmware Image:** Type in the location of the file you wish to upload in this field or click **Browse…** to locate it.
- **Browse…:** Click **Browse…** to find the file with the **.afw** file extension that you wish to upload. Remember that you must decompress compressed (.zip) files before you can upgrade from the file.
- **Upgrade**: Click **upgrade** to begin the upload process. This process may take up to three minutes.

Warning:

DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Improper operation may damage the router. Please see section 2.4 for emergency recovery procedures.

5.3.3.3 Backup / Restore



Configuration

Backup/Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Backup

Restore Configuration

Configuration File | Browse...

Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

Restore

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

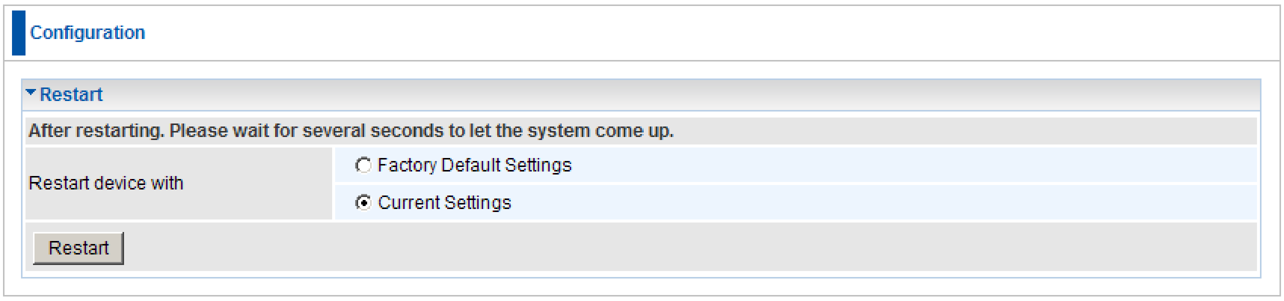
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse…** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

Select the settings files you wish to use, and press **Restore** to load those settings into the router.

5.3.3.4 Restart Router

Click **Restart** with option **Current Settings** to reboot your router and save the current configuration to device.



Configuration

Restart

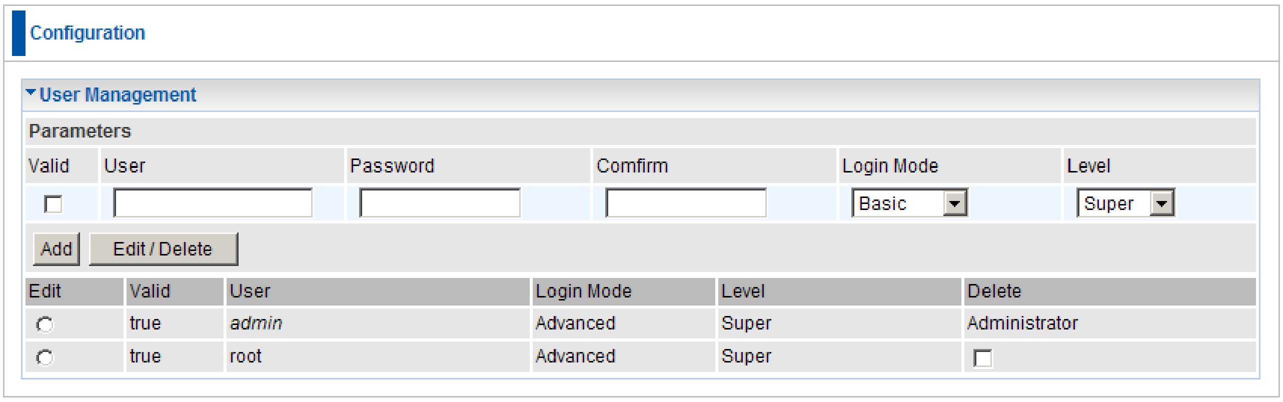
After restarting. Please wait for several seconds to let the system come up.

Restart device with	○ Factory Default Settings ● Current Settings

Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

5.3.3.5 User Management



Configuration

User Management

Parameters

Valid	User	Password	Comfirm	Login Mode	Level
□				Basic	Super

Add Edit / Delete

Edit	Valid	User	Login Mode	Level	Delete
○	true	*admin*	Advanced	Super	Administrator
○	true	root	Advanced	Super	□

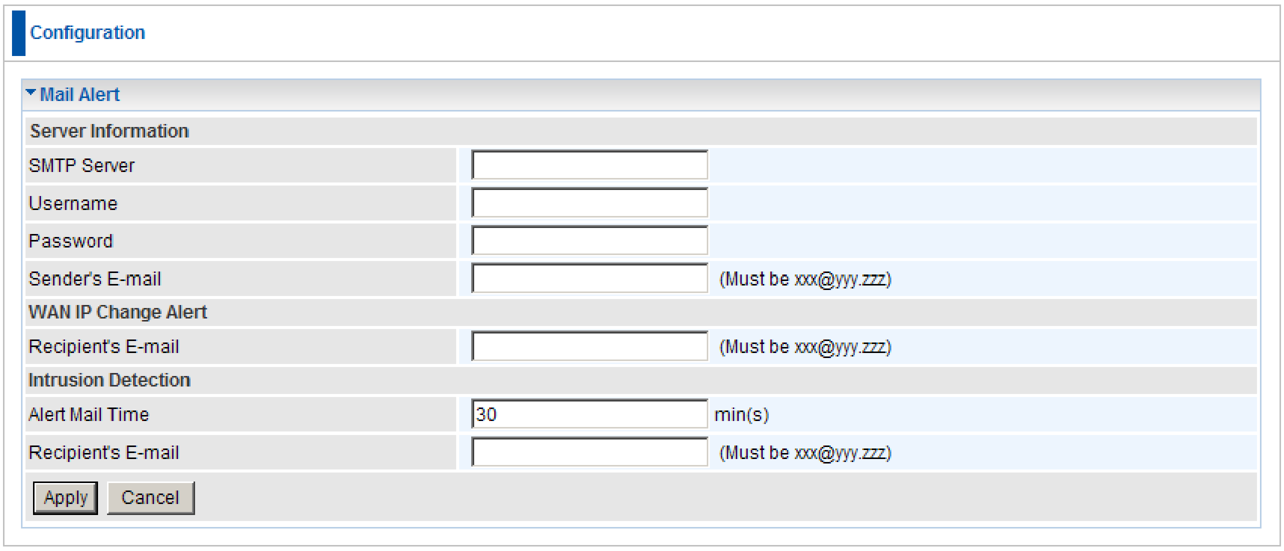
In order to prevent unauthorized access to your router's configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked **Edit** on the account you want to edit**,** the information of the account will be displayed above. Just go ahead and change the password. You can change the user's **password**, whether their account is active and **Valid**. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; however you can delete any other created accounts by clicking ticking the box under **Delete** and then press the **Edit/Delete** button.

You are strongly advised to change the password on the default “**admin**” account when you receive your router, and any time you reset your configuration to Factory Defaults.

5.3.3.6 Mail Alert

Send a log via email, if WAN IP is changed or if intruders accessing your computer without permission



Configuration

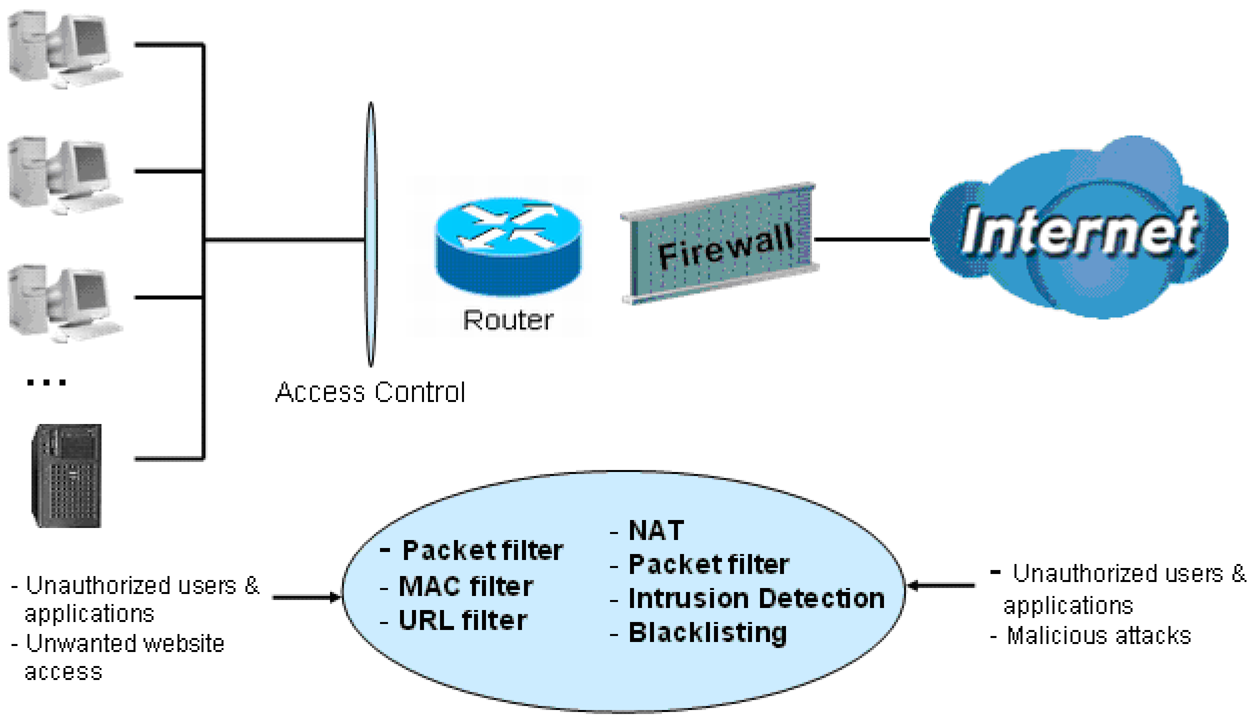
▾ Mail Alert

Server Information		
SMTP Server		
Username		
Password		
Sender's E-mail		(Must be xxx@yyy.zzz)
WAN IP Change Alert		
Recipient's E-mail		(Must be xxx@yyy.zzz)
Intrusion Detection		
Alert Mail Time	30	min(s)
Recipient's E-mail		(Must be xxx@yyy.zzz)

5.3.4 Firewall

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the **WAN** configuration section for more details on NAT.



Firewall & Filter

Firewall: Prevents access from outside your network.

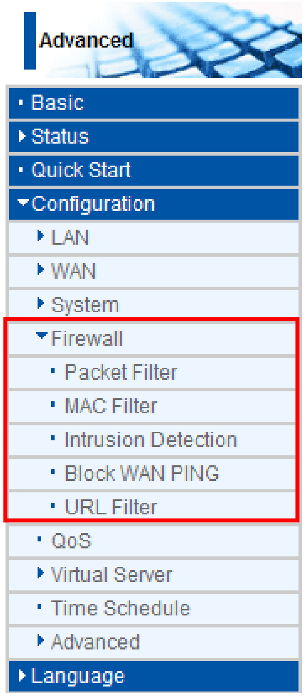
NAT natural firewall: This masks LAN users’ IP addresses, which are invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when the NAT function is enabled.

Note:

When using Virtual Servers (port mapping) your PCs are exposed to the ports specified opened in your firewall packet filter settings.

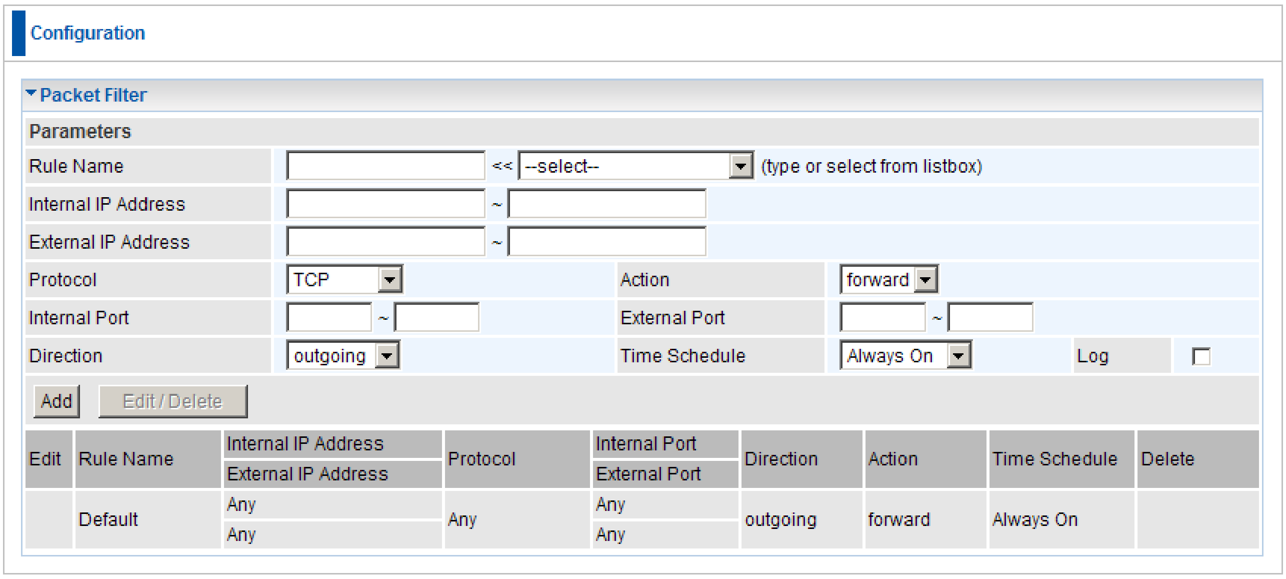
- **Firewall Security and Policy (General Settings)**: Inbound direction of Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet.
- **Intrusion Detection**: Enable Intrusion Detection to detect, prevent, and log malicious attacks.
- **MAC Filter rules**: Prevents unauthorized computers accessing the Internet.
- **URL Filter**: Blocks PCs on your local network from unwanted websites.

A detailed explanation of each of the following five items appears in the **Firewall** section below: **Packet Filter**, **MAC Filter, Intrusion detection, Block WAN PING** and **URL Filter.**



5.3.4.1 Packet Filter

Packet filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. This configuration program allows you to set up to 6 different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is **"or"** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Configuration

Packet Filter

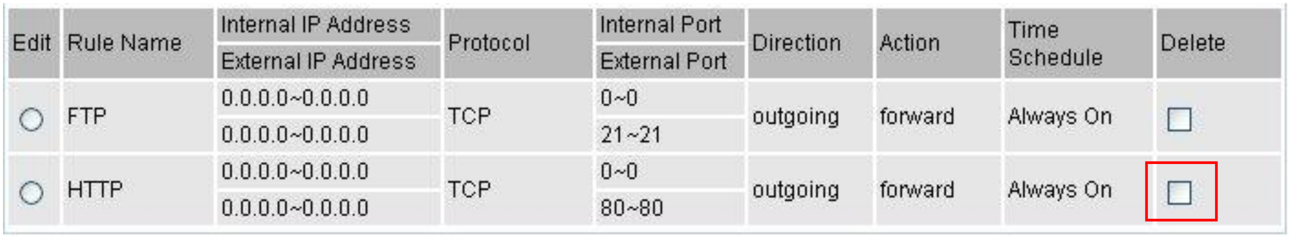
Parameters					
Rule Name	<< --select-- (type or select from listbox)				
Internal IP Address	~				
External IP Address	~				
Protocol	TCP	Action	forward		
Internal Port	~	External Port	~		
Direction	outgoing	Time Schedule	Always On	Log	□

Edit	Rule Name	Internal IP Address External IP Address	Protocol	Internal Port External Port	Direction	Action	Time Schedule	Delete
	Default	Any Any	Any	Any Any	outgoing	forward	Always On	

- **Rule Name:** Users-define description to identify this entry. The maximum name length is 32 characters, and then can choose application that they want from listbox.
- **Internal IP Address / External IP Address:** This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Input the range you want to filter out. If you leave empty or 0.0.0.0, it means any IP address.
- **Protocol:** Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to.
- Select **TCP** if you wish to search for the connection-based application service on the remote server using the port number. Or select **UDP** if you want to search for the connectionless application service on the remote server using the port number.
- **Action:** If a packet matches this filter rule, **Forward (allows the packets to pass)** or **Drop (disallow the packets to pass)** this packet.
- **Internal Port:** This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535.** It is recommended that this option be configured by an advanced user.
- **External Port:** This is the Port or Port Range that defines the application.
- **Direction:** Determine whether the rule is for outgoing packets or for incoming packets.
- **Time Schedule:** It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.
- **Log:** Choose “log” if you wish to generate logs when the filer rule is applied to a packet.
- **Add:** Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

- **Edit:** Check the Rule No. you wish to edit, and then click “Edit”.

Delete: Check the Rule No. you wish to delete, and then click “Delete”.



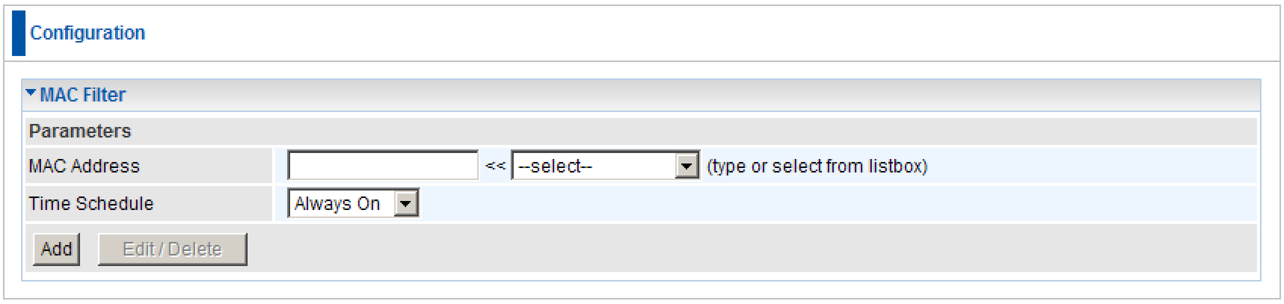
Edit	Rule Name	Internal IP Address	Protocol	Internal Port	Direction	Action	Time Schedule	Delete
		External IP Address		External Port				
○	FTP	0.0.0.0~0.0.0.0	TCP	0~0	outgoing	forward	Always On	□
		0.0.0.0~0.0.0.0		21~21				
○	HTTP	0.0.0.0~0.0.0.0	TCP	0~0	outgoing	forward	Always On	□
		0.0.0.0~0.0.0.0		80~80				

Attention:
If the DHCP server option is enabled, you must be very careful in assigning IP addresses of a filtered private IP range to avoid conflicts because you do not know which PC in the LAN is assigned which IP address. The easiest and safest way is that the filtered IP address is assigned to a specific PC that is not allowed to access an outside resource such as the Internet. You configure the filtered IP address manually for this PC, but it stays in the same subnet with the router.

5.3.4.2 MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network’s interface (i.e. its Network Interface Card or Ethernet card). Using your router’s MAC Address Filter function, you can configure to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules; you can add the filter rules to meet your requirements.



Configuration

MAC Filter

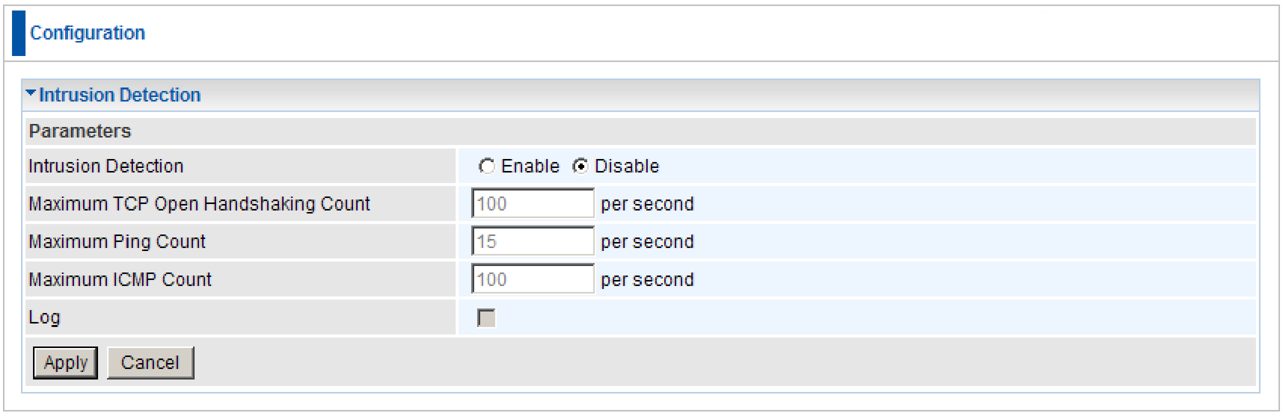
Parameters

MAC Address	<< --select-- (type or select from listbox)
Time Schedule	Always On

MAC Address: Enter the MAC addresses you wish to manage.
Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

5.3.4.3 Intrusion Detection

Check Enable if you wish to detect intruders accessing your computer without permission. The router automatically detects and blocks a DoS (Denial of Service) attack if a user enables this function. This kind of attack is not to access confidential data on the network; instead, it aims to disrupt specific equipment or the entire network. If this happens, users will have trouble accessing the network resources.



Configuration

Intrusion Detection

Parameters	
Intrusion Detection	○ Enable ● Disable
Maximum TCP Open Handshaking Count	100 per second
Maximum Ping Count	15 per second
Maximum ICMP Count	100 per second
Log	□

Intrusion Detection: Check Enable if you wish to detect intruders accessing your computer without permission.

Maximum TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Maximum Ping Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Maximum ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Check Log if you wish to generate logs when the filer rule is applied to the Intrusion Detection.

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log but it will not be able to protect against such attacks.

Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes

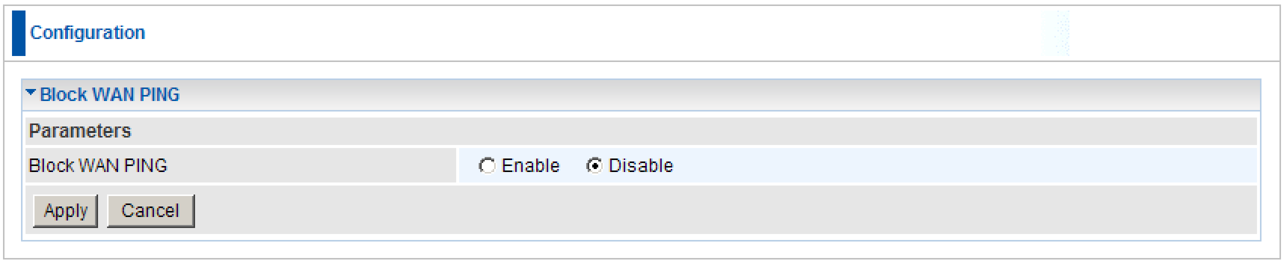
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP **Src Port:** Source Port

Dst Port: Destination Port **Dst IP:** Destination IP

5.3.4.4 Block WAN PING

Check Enable if you wish to exclude outside PING requests from reaching this router.



Configuration

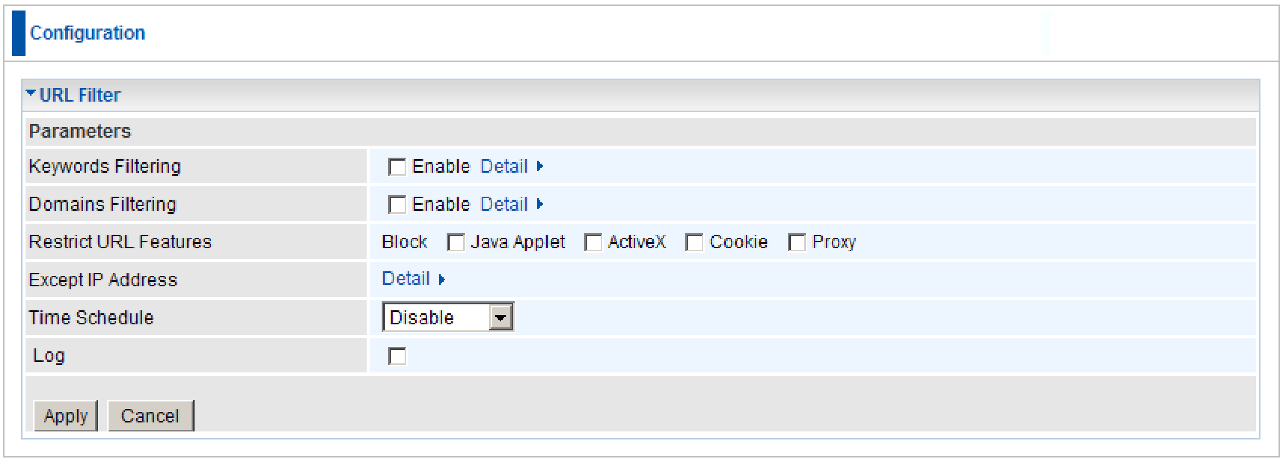
Block WAN PING

Parameters

Block WAN PING ○ Enable ● Disable

5.3.4.5 URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of **http://www.example.com**) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



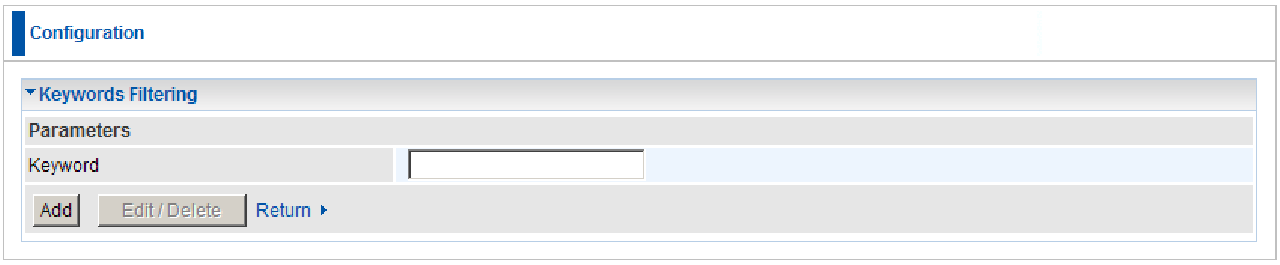
Configuration

▾URL Filter

Parameters	
Keywords Filtering	□ Enable Detail ▸
Domains Filtering	□ Enable Detail ▸
Restrict URL Features	Block □ Java Applet □ ActiveX □ Cookie □ Proxy
Except IP Address	Detail ▸
Time Schedule	Disable
Log	□

Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list is checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, the URL http://www.abc.com/abcde.html would be dropped since the keyword “abcde” occurs in the URL.



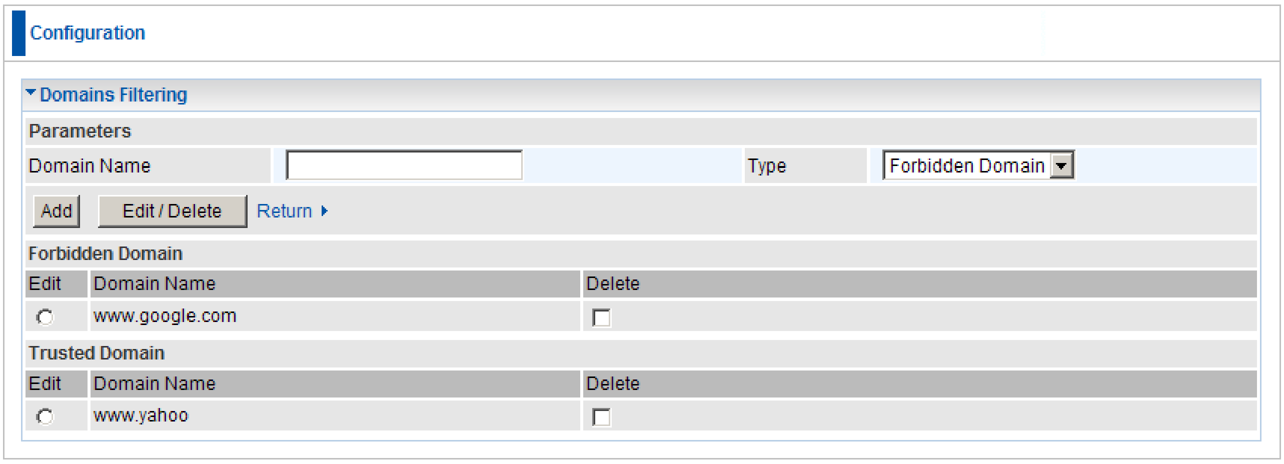
Configuration

▾Keywords Filtering

Parameters	
Keyword	

Domains Filtering: Checks the domain name in URLs accessed against your list of domains to block or allow. If it matches, the URL request is sent (Trusted) or dropped (Forbidden). The checking procedure is:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
3. If the packet matches neither of the above, it is sent to the remote web server.
4. Please be note that the completed URL, "www" + domain name shall be specified. For example to block traffic to www.google.com.au, enter "www.google" or "www.google.com"



Configuration

Domains Filtering

Parameters

Domain Name		Type	Forbidden Domain

Add | Edit / Delete | Return

Forbidden Domain

Edit	Domain Name	Delete
○	www.google.com	□

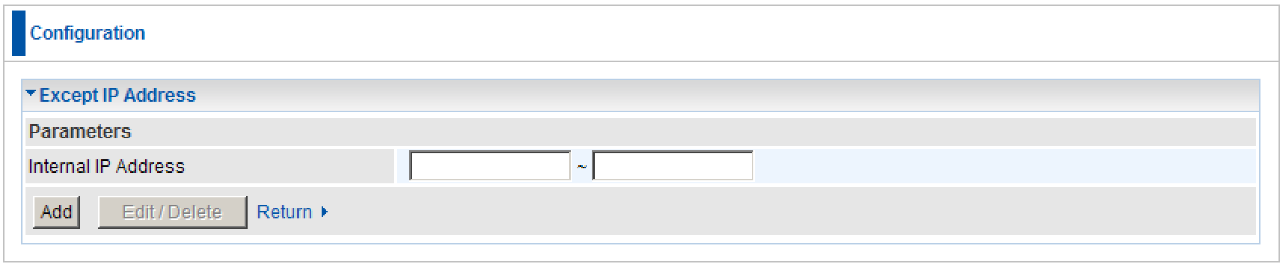
Trusted Domain

Edit	Domain Name	Delete
○	www.yahoo	□

Restrict URL Features: This function enhances the restriction to your URL rules.

- **Block Java Applet:** Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.
- **Block ActiveX:** Blocks ActiveX
- **Block Cookies:** Blocks Cookies
- **Block Proxy:** Blocks Proxy

Except IP Address:



Configuration

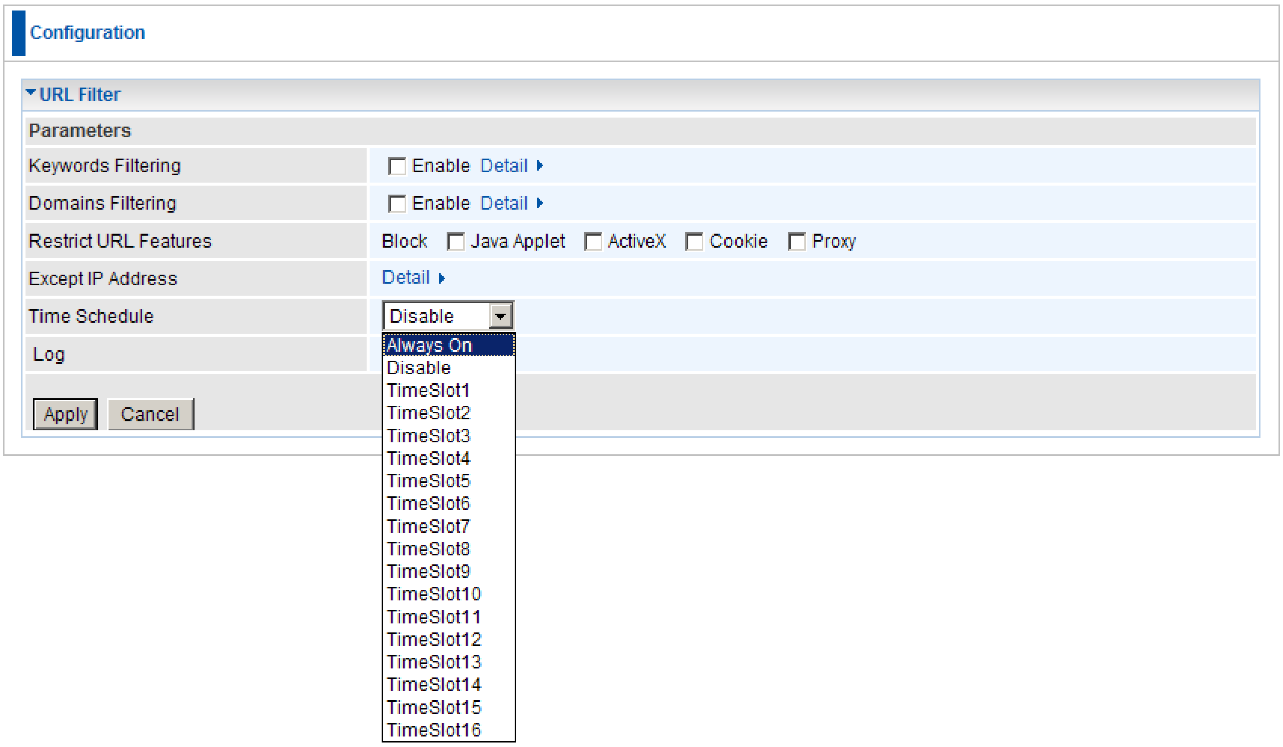
Except IP Address

Parameters

Internal IP Address: ~

Add | Edit / Delete | Return

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.



Keywords Filtering	□ Enable Detail
Domains Filtering	□ Enable Detail
Restrict URL Features	Block □ Java Applet □ ActiveX □ Cookie □ Proxy
Except IP Address	Detail
Time Schedule	Disable
Log	

Log: Click “Log” if you wish to generate logs when the filer rule is applied to the URL Filter.

5.3.5 QoS (Quality of Service)

Quality of Service Introduction

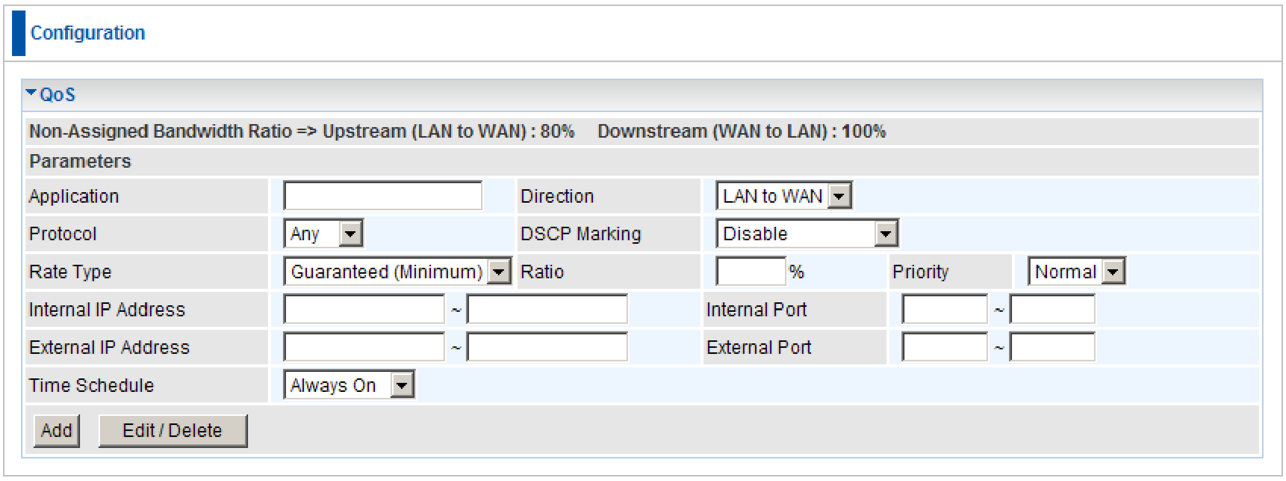
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in the routers is such a breakthrough for home users and office users.

QoS: Keeping Your Net Connection Fast and Responsive

Configurable by internal IP address, external IP address, protocol, and port, the Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring bandwidth-consumption data like gaming packets, latency-sensitive application like voice, or even mission critical files, move through the router at lightning speed, even under heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

QoS Setup

Please choose the **QoS** in the **Configuration** item of the left window as depicted below.



Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 80%   Downstream (WAN to LAN) : 100%

Parameters

Application		Direction	LAN to WAN		
Protocol	Any	DSCP Marking	Disable		
Rate Type	Guaranteed (Minimum)	Ratio	%	Priority	Normal
Internal IP Address	~		Internal Port	~	
External IP Address	~		External Port	~	
Time Schedule	Always On				

After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: A name that identifies an existing policy.

Direction: The traffic flow direction to be controlled by the QoS policy.

There are two settings to be provided in the Router:

- ⊙ **LAN to WAN:** You want to control the traffic flow from the local network to the outside world. e.g., you have a FTP server inside the local network and you want to have a limited traffic rate controlled by the QoS policy. So, you need to add a policy with LAN to WAN direction setting.
- ⊙ **WAN to LAN**: Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

Protocol: The Protocol will be controlled. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

- ⊙ **ANY:** No protocol type is specified.
- ⊙ **TCP**
- ⊙ **UDP**
- ⊙ **ICMP**
- ⊙ **GRE:** For PPTP VPN Connections.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify traffic based on DSCP value and send packets to next Router.

Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

DSCP Mapping Table

ADSL2+ Router	**Standard DSCP**
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Rate Type: 2 types are provided:

⊙ **Limited (Maximum):** specify a limited data rate for this policy. It also is the maximal rate for this policy. As above FTP server example, you may want to "throttle" the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.

⊙ **Guaranteed (Minimum):** specify a minimal data rate for this policy. For example, you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidth. You can use this type. Then, if there is available bandwidth that is not used, it will be given to this policy by following priority assignment.

Ratio: Assign the data ratio for this policy to be controlled. For examples, we want to only allow 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is 20%*256*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for a ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

Priority: Specify the priority for the bandwidth that is not used. For examples, you may specify two different QoS policies for different applications. Both applications need a minimal bandwidth and need more bandwidth, beside the assigned one, if there is any available/non-used one available. So, you may specify which application can have higher priority to acquire the non-used bandwidth.

⊙ **High**
⊙ **Normal**: The default is normal priority.
⊙ **Low**

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

Internal IP Address: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

Internal Port: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

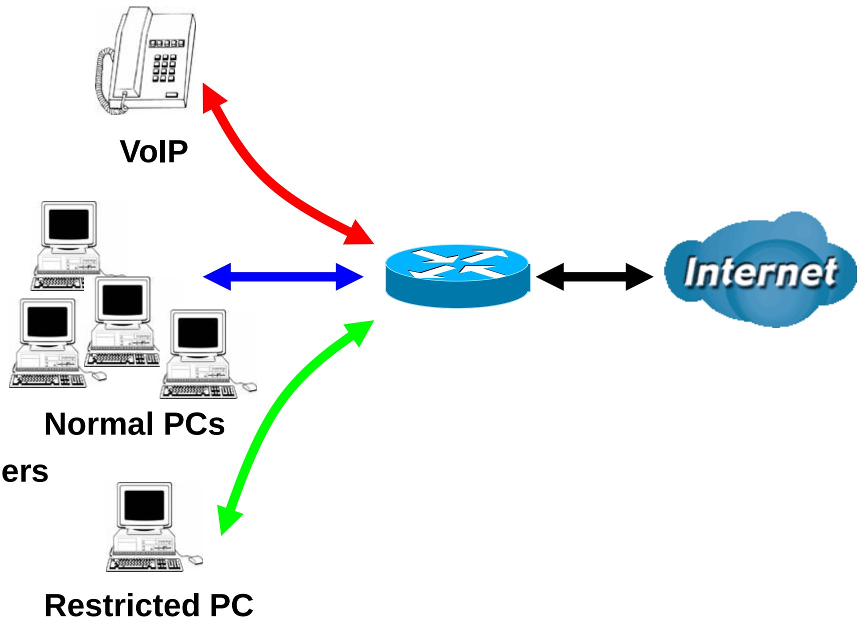
External IP Address: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

External Ports: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

Time Schedule: Scheduling your prioritization policy.

QoS example for your Network

Connection Diagram



ADSL Subscription Rate

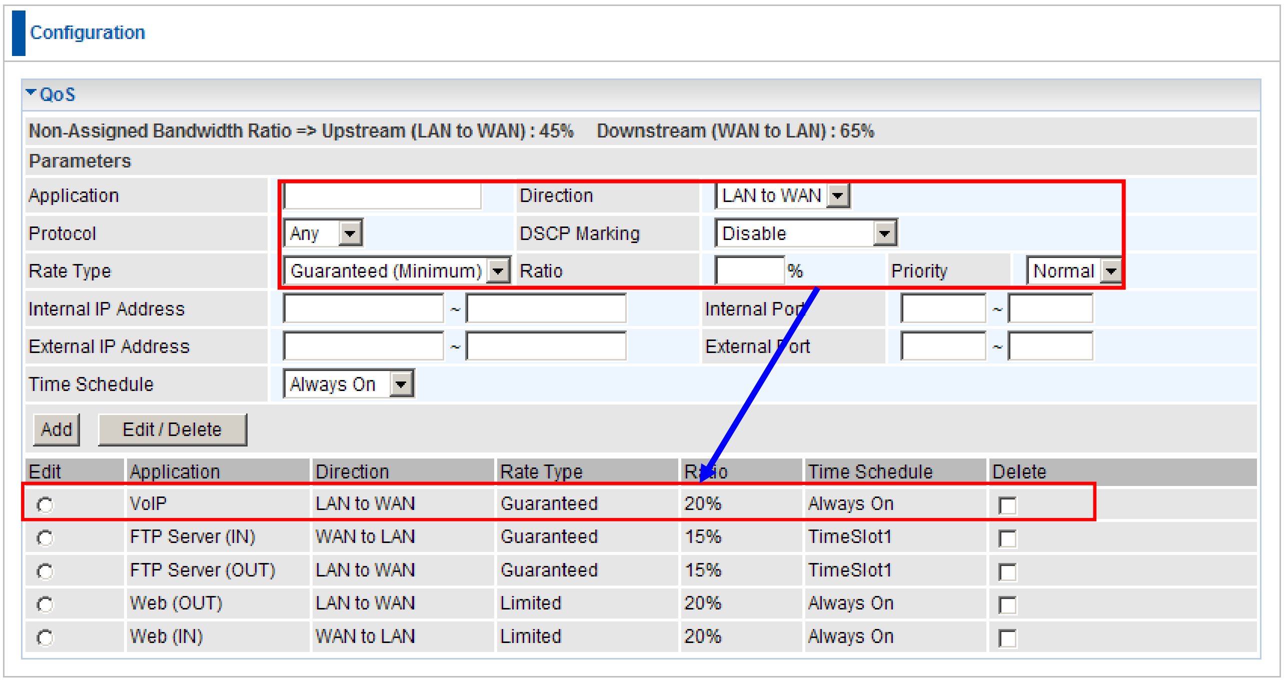
Upstream: 256 kbps

Downstream: 2048 Mbps

Example QoS Plan

Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.1.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with DSCP marking Class 1 Gold Service.	Always
FTP Sever	192.168.1.100	Incoming and Outgoing	outgoing :minimal 30%. Data rate. incoming :minimal 30%. Data rate. Both with low priority for non-used bandwidth.	Only Working Hours 9:00 to 17:00 Monday to Friday.
HTTP web browsing users	80	Incoming and Outgoing	outgoing : limited 20%. Data rate. incoming : limited 30%. Data rate.	Always

Example QoS Setup



Configuration

QoS

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 45%   Downstream (WAN to LAN) : 65%

Parameters

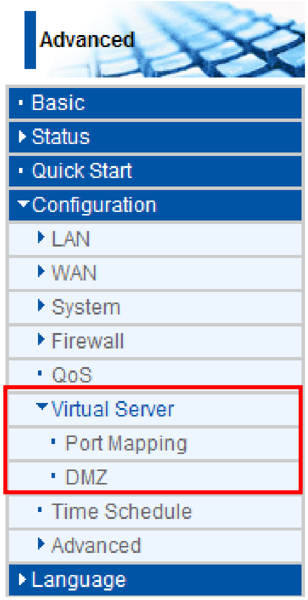
Application		Direction	LAN to WAN		
Protocol	Any	DSCP Marking	Disable		
Rate Type	Guaranteed (Minimum)	Ratio	%	Priority	Normal
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	~		
Time Schedule	Always On				

Edit	Application	Direction	Rate Type	Ratio	Time Schedule	Delete
○	VoIP	LAN to WAN	Guaranteed	20%	Always On	□
○	FTP Server (IN)	WAN to LAN	Guaranteed	15%	TimeSlot1	□
○	FTP Server (OUT)	LAN to WAN	Guaranteed	15%	TimeSlot1	□
○	Web (OUT)	LAN to WAN	Limited	20%	Always On	□
○	Web (IN)	WAN to LAN	Limited	20%	Always On	□

VoIP application

Voice is latency-sensitive application. Most VoIP devices are used SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

5.3.6 Virtual Server



In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

The reason is that when using NAT, your publicly accessible IP address is used by and points to your router, which needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for information on NAT.

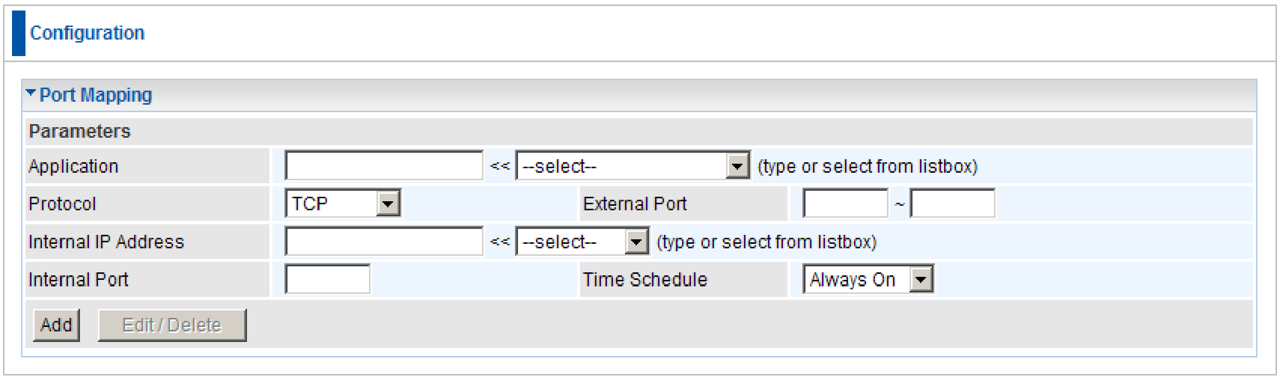
The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic ports, or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA's website at: http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	**Protocol**	**Description**
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

5.3.6.1 Port Mapping



Configuration

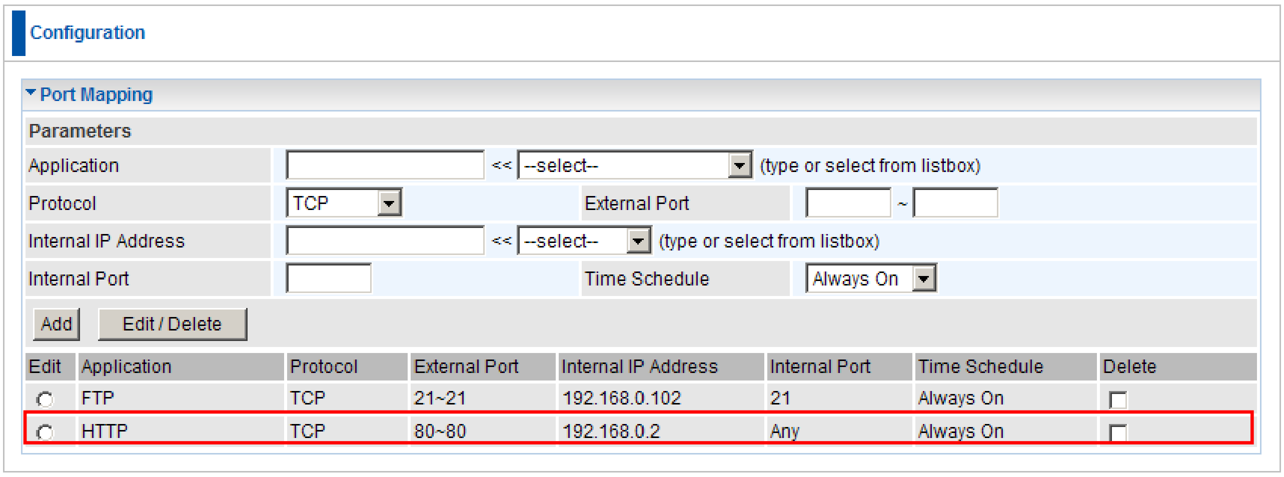
Port Mapping

Parameters			
Application	<< --select-- (type or select from listbox)		
Protocol	TCP	External Port	~
Internal IP Address	<< --select-- (type or select from listbox)		
Internal Port		Time Schedule	Always On

- **Application:** Select the service you wish to configure
- **Protocol:** Automatic when you choose Application from listbox or select a protocol type which you want.
- **External Port & Internal Port:** Enter the public port number & range you wish to configure.
- **Internal IP Address:** Enter the IP address of a specific internal server to which requests from the specified port is forwarded.
- **Add:** Click to add a new virtual server rule. Click again and the next figure appears.
- **Edit:** Check the Rule No. you wish to edit and then click “Edit/Delete”.
- **Delete:** Check the Rule No. you wish to delete, then click “Edit/Delete”.

Since NAT acts as a “natural” Internet firewall, your router protects your network from access by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request to the router for a specified port is received, it is forwarded to the corresponding internal server.

For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.



Parameters

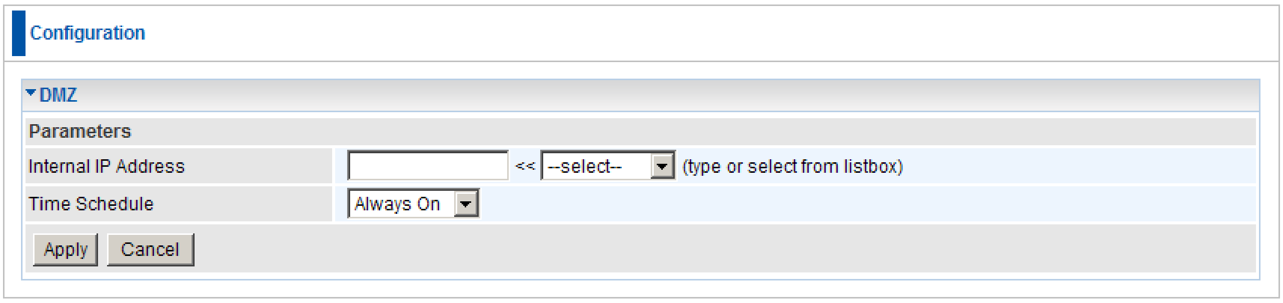
Application	<< --select-- (type or select from listbox)		
Protocol	TCP	External Port	~
Internal IP Address	<< --select-- (type or select from listbox)		
Internal Port		Time Schedule	Always On

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
○	FTP	TCP	21~21	192.168.0.102	21	Always On	□
○	HTTP	TCP	80~80	192.168.0.2	Any	Always On	□

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by the particular application. Most applications use TCP or UDP, however you can specify other protocols using the drop-down **Protocol** menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

5.3.6.2 DMZ

DMZ: The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets are checked by the Firewall and NAT algorithms, it is then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.



Configuration

▾DMZ

Parameters	
Internal IP Address	<< --select-- (type or select from listbox)
Time Schedule	Always On

Note:

Using port mapping does have security implications, since outside users are able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires instead of simply using DMZ or creating a Virtual Server entry for “All” protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

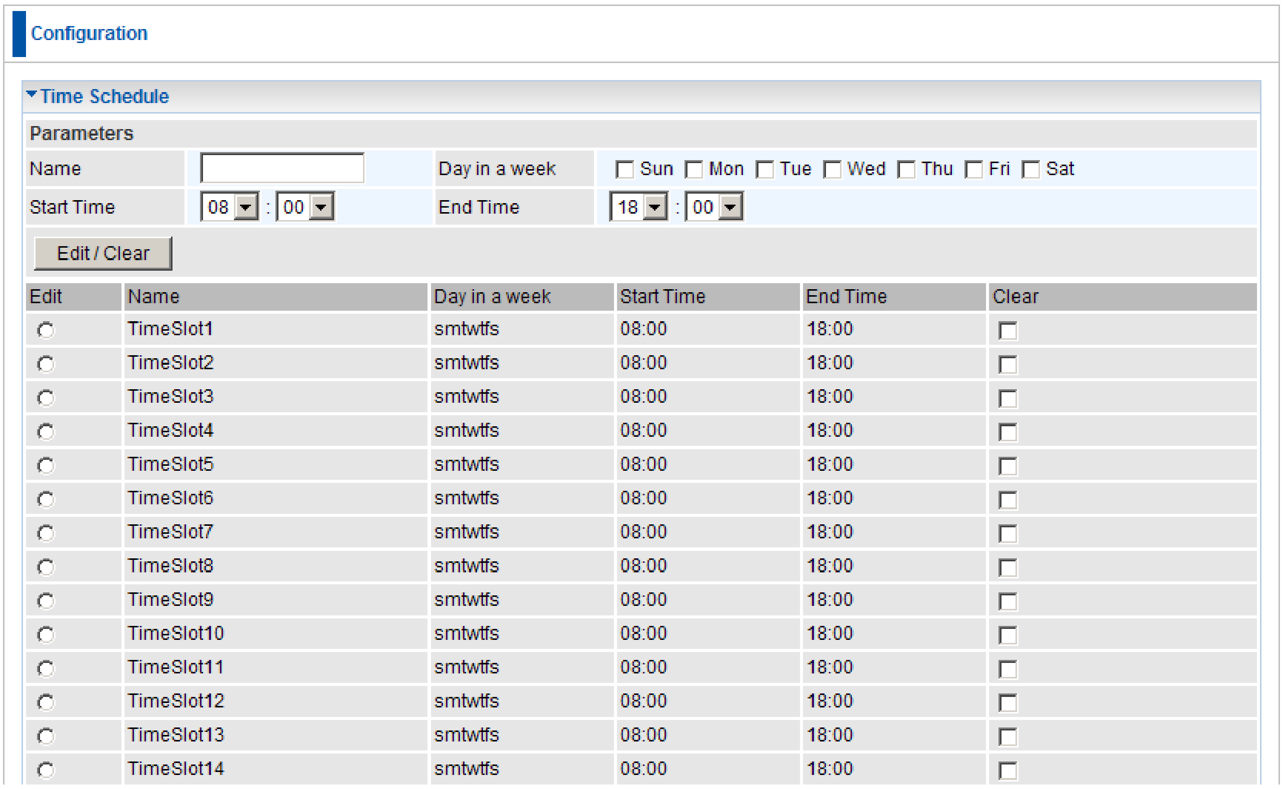
Attention:

1. If you disable the NAT option in the WAN-ISP section, the Virtual Server function becomes invalid.
2. If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign a static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

5.3.7 Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.



Configuration

▾Time Schedule

Parameters

Name		Day in a week	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Start Time	08 : 00	End Time	18 : 00

Edit / Clear

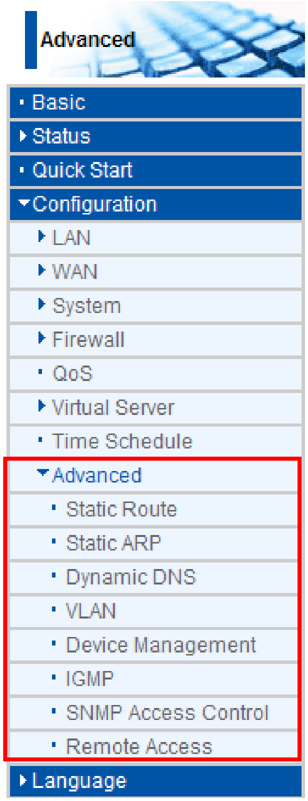
Edit	Name	Day in a week	Start Time	End Time	Clear
○	TimeSlot1	smtwtfs	08:00	18:00	□
○	TimeSlot2	smtwtfs	08:00	18:00	□
○	TimeSlot3	smtwtfs	08:00	18:00	□
○	TimeSlot4	smtwtfs	08:00	18:00	□
○	TimeSlot5	smtwtfs	08:00	18:00	□
○	TimeSlot6	smtwtfs	08:00	18:00	□
○	TimeSlot7	smtwtfs	08:00	18:00	□
○	TimeSlot8	smtwtfs	08:00	18:00	□
○	TimeSlot9	smtwtfs	08:00	18:00	□
○	TimeSlot10	smtwtfs	08:00	18:00	□
○	TimeSlot11	smtwtfs	08:00	18:00	□
○	TimeSlot12	smtwtfs	08:00	18:00	□
○	TimeSlot13	smtwtfs	08:00	18:00	□
○	TimeSlot14	smtwtfs	08:00	18:00	□

- **Name:** A user-define description to identify this time portfolio.
- **Day in a week:** The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.
- **Start Time:** The default is set at 8:00 AM. You may specify the start time of the schedule.
- **End Time:** The default is set at 18:00 (6:00PM). You may specify the end time of the schedule. Select the **Apply** button to apply your changes.

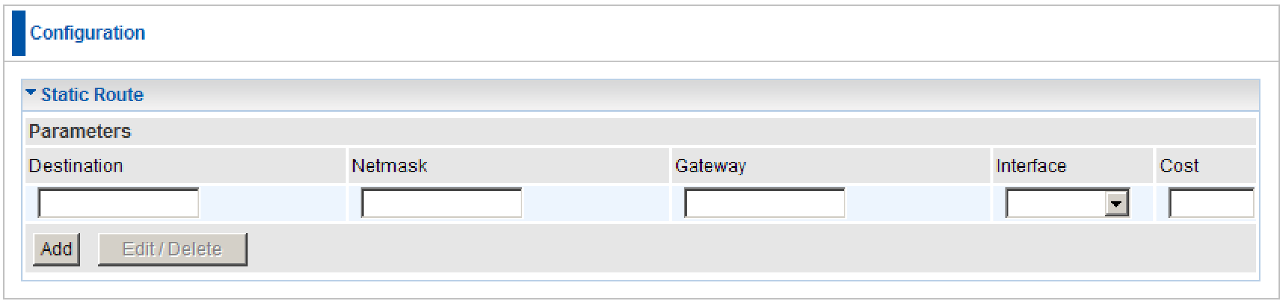
5.3.8 Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

There are seven items within the **Advanced** section: **Static Route, Dynamic DNS, VLAN, Device Management, IGMP, SNMP Access Control** and **Remote Access.**

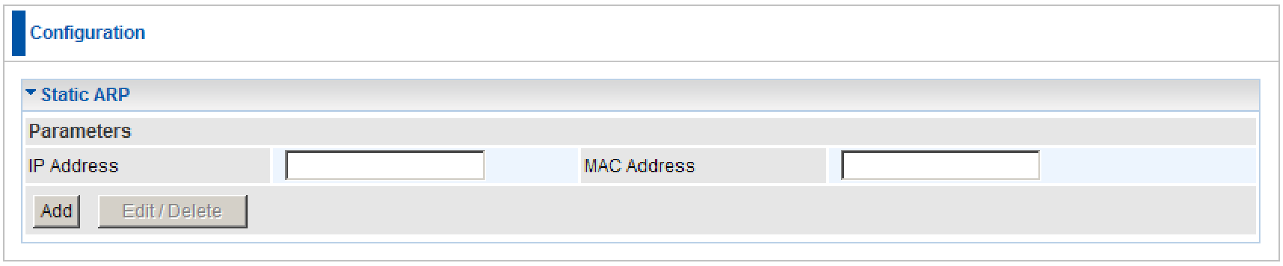


5.3.8.1 Static Route



- **Destination:** The destination subnet IP address.
- **Netmask:** Subnet mask of the destination IP addresses based on above destination.
- **Gateway:** The gateway IP address to which packets are forwarded.
- **Interface:** Select the interface through which packets are forwarded.
- **Cost:** Represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

5.3.8.2 Static ARP

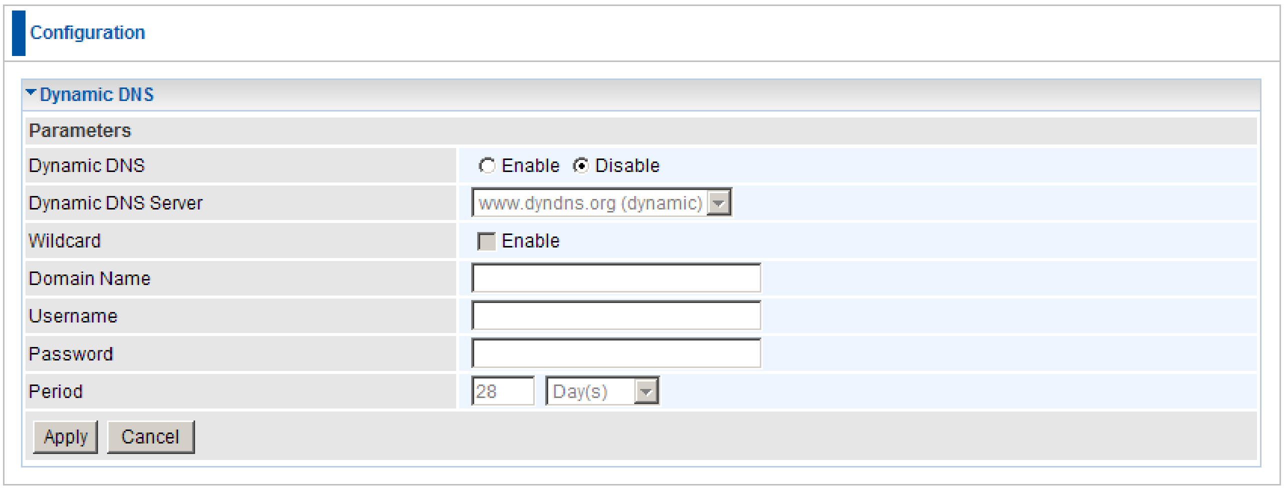


- **IP Address:** The IP address you want to give to the LAN client.
- **MAC Address:** The MAC Address of LAN client.

5.3.8.3 Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/



Configuration

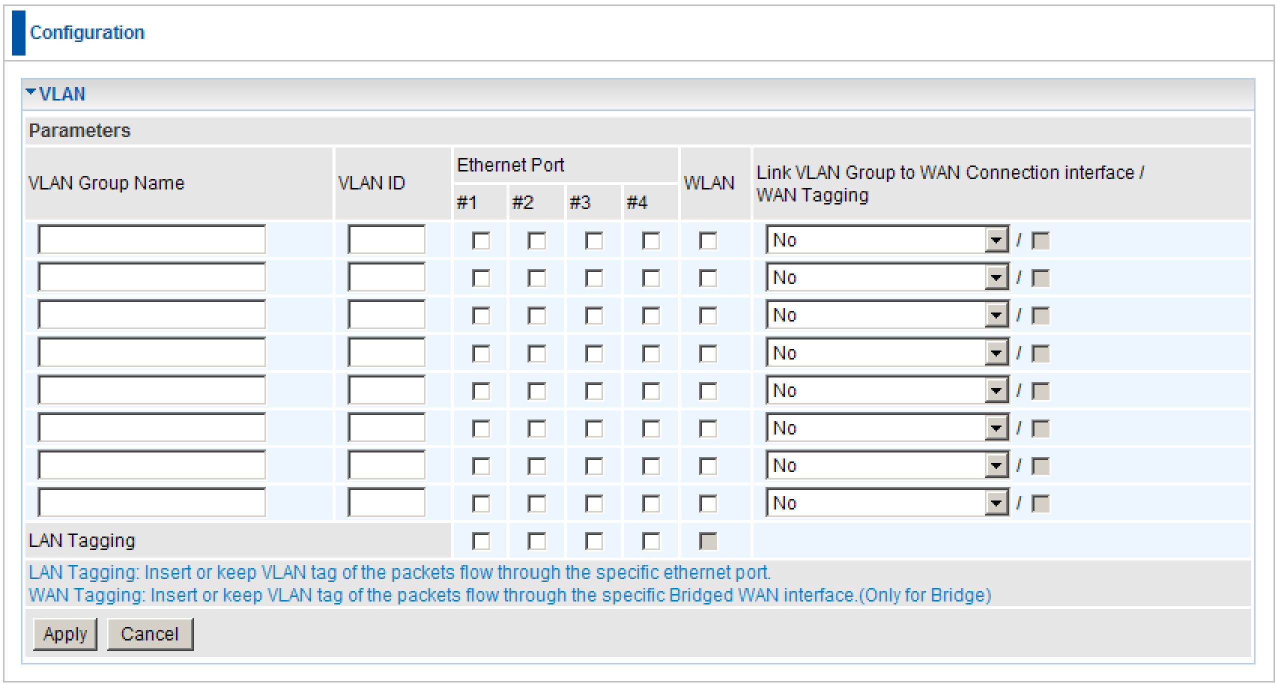
Dynamic DNS

Parameters	
Dynamic DNS	○ Enable ● Disable
Dynamic DNS Server	www.dyndns.org (dynamic)
Wildcard	□ Enable
Domain Name	
Username	
Password	
Period	28 Day(s)

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The fields following are activated and required.
- **Dynamic DNS Server:** Select the DDNS service you have established an account with.
- **Wildcard:** Select this check box to enable the DYNDNS Wildcard.
- **Domain Name, Username and Password:** Enter your registered domain name and your username and password for this service.
- **Period:** Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

5.3.8.3 VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.



Configuration

VLAN

Parameters

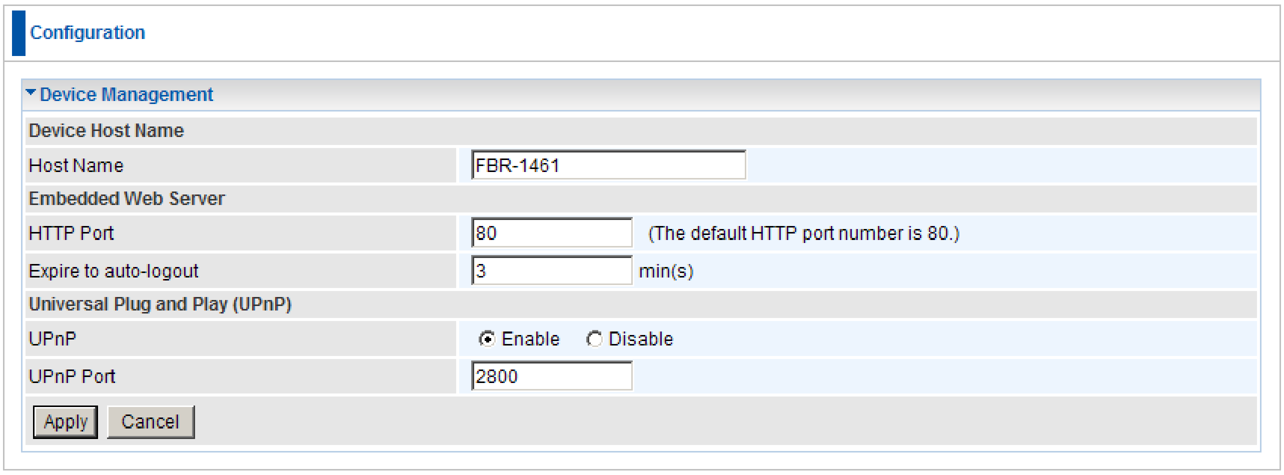
VLAN Group Name	VLAN ID	Ethernet Port				WLAN	Link VLAN Group to WAN Connection interface / WAN Tagging
		#1	#2	#3	#4		
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
		□	□	□	□	□	No / □
LAN Tagging		□	□	□	□	□	

LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.
WAN Tagging: Insert or keep VLAN tag of the packets flow through the specific Bridged WAN interface.(Only for Bridge)

- **LAN Group Name:** The name you will give to this VLAN.
- **VLAN ID:** The ID tag you will give to this VLAN.
- **Ethernet Port:** Select the Port that you want to tag.
- **WLAN:** Select this if you also want the wireless network to have this tag.
- **Link VLAN Group to WAN:** If you want to link the VLAN to the WAN interface.

5.3.8.4 Device Management

The Device Management advanced configuration settings allow you to control your router's security options and device monitoring features.



Configuration

Device Management

Device Host Name	
Host Name	FBR-1461
Embedded Web Server	
HTTP Port	80 (The default HTTP port number is 80.)
Expire to auto-logout	3 min(s)
Universal Plug and Play (UPnP)	
UPnP	● Enable ○ Disable
UPnP Port	2800

Embedded Web Server:

HTTP Port: The port number of the router's embedded web server (for web-based configuration uses. The default value is the standard HTTP port, 80. You may specify an alternative if, for example, you are running a web server on a PC within your LAN.

For Example: User A changes HTTP port number to **100**, specifies their own IP address of **192.168.0.55**, and sets the logout time to be **100** minutes. The router only allows User A access from the IP address **192.168.0.55** to logon to the Web GUI by typing: **http://192.168.0.1:100** in their web browser. After 100 minutes, the device automatically logs out User A.

Universal Plug and Play (UPnP):

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

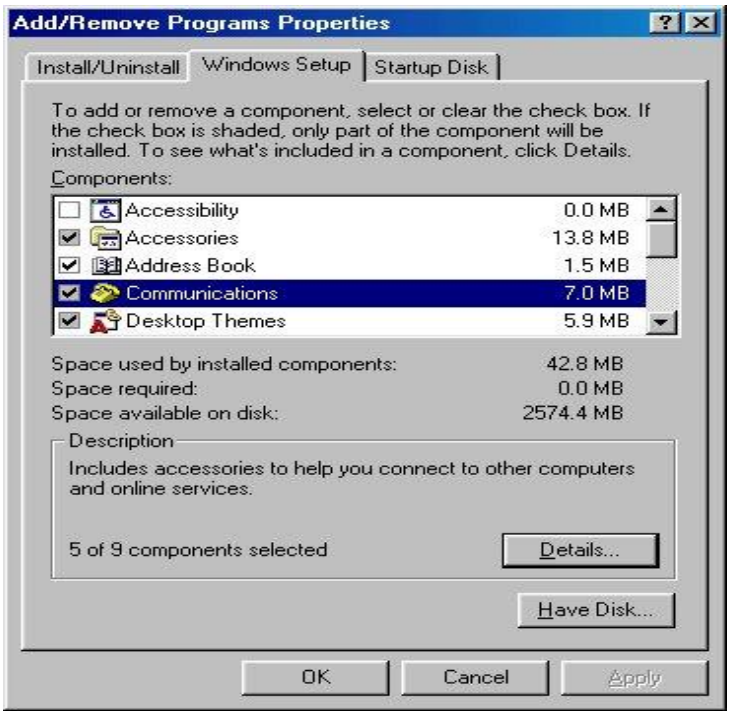
- **Disable:** Check to disable the router's UPnP functionality.
- **Enable:** Check to enable the router's UPnP functionality.
- **UPnP Port:** The Default setting is 2800. It is highly recommended you use this port value.
- If this value conflicts with other ports already in use you may wish to change the port.

Installing UPnP in Windows 98 Example

Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

□	Accessibility	0.0 MB
☑	Accessories	13.8 MB
☑	Address Book	1.5 MB
☑	Communications	7.0 MB
☑	Desktop Themes	5.9 MB

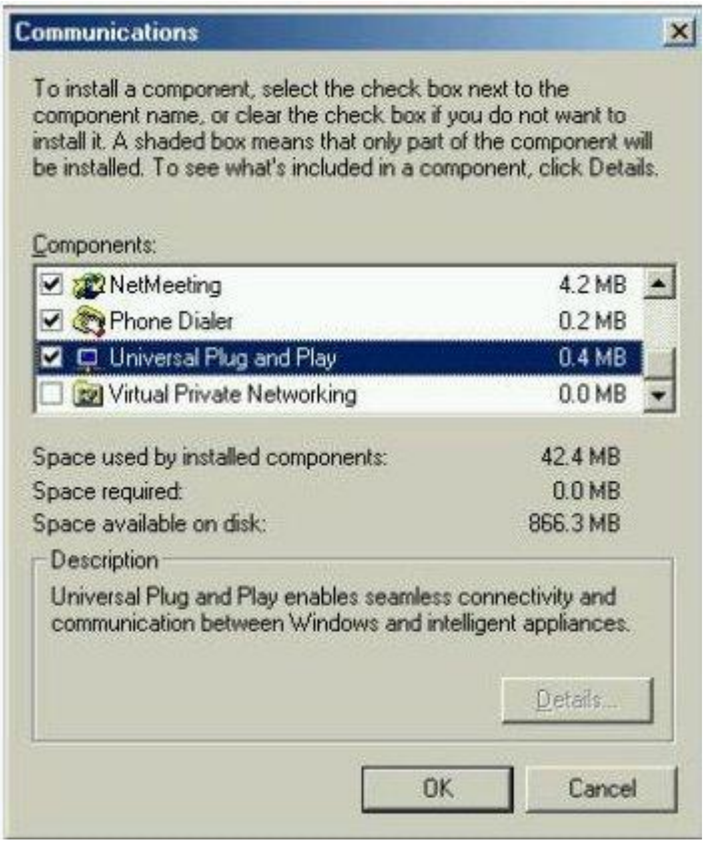
Space used by installed components:	42.8 MB
Space required:	0.0 MB
Space available on disk:	2574.4 MB

Description

Includes accessories to help you connect to other computers and online services.

5 of 9 components selected

Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components:	42.4 MB
Space required:	0.0 MB
Space available on disk:	866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

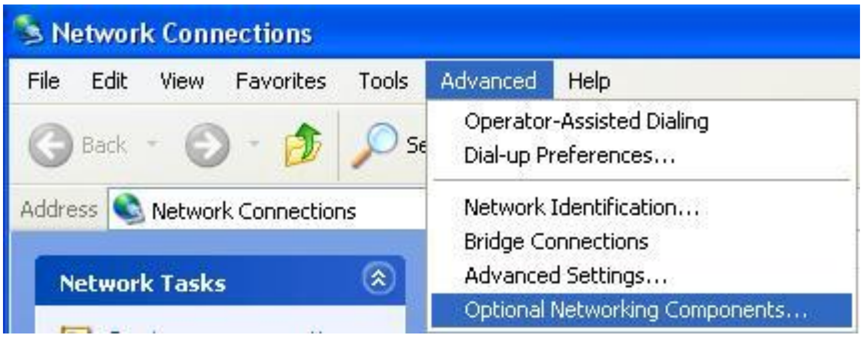
Step 5: Restart the computer when prompted.

<u>Follow the steps below to install the UPnP in Windows XP.</u>

Step 1: Click Start and Control Panel.

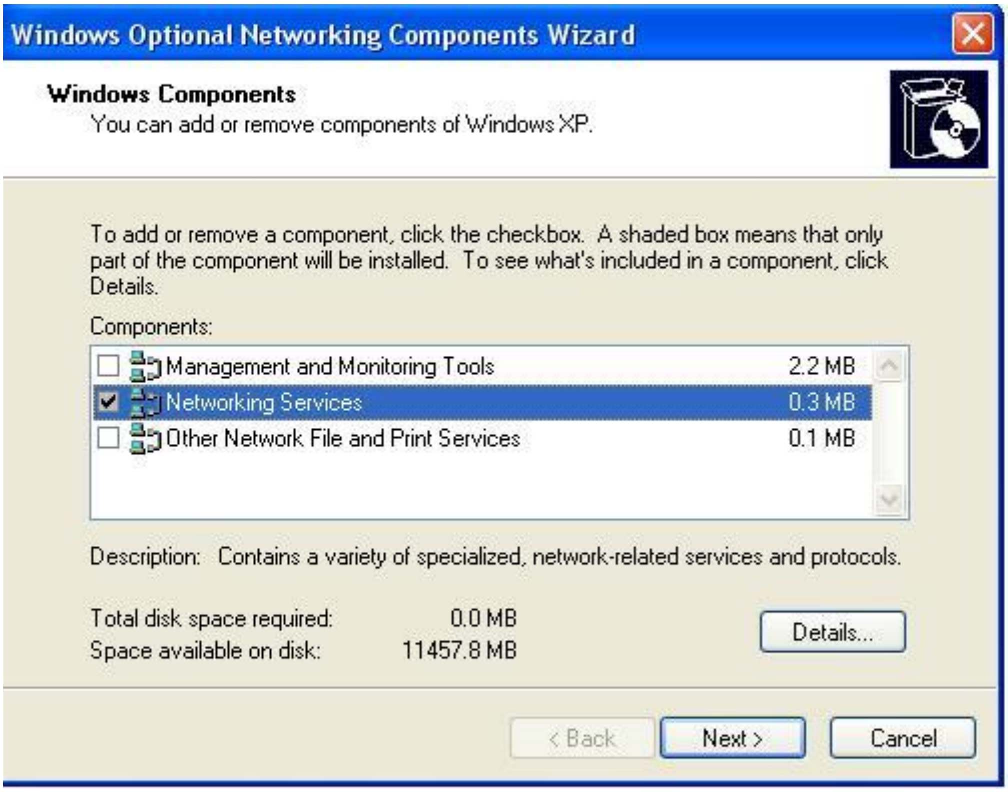
Step 2: Double-click Network Connections.

Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….



The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



Windows Optional Networking Components Wizard

Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

- ☐ Management and Monitoring Tools 2.2 MB
- ☑ Networking Services 0.3 MB
- ☐ Other Network File and Print Services 0.1 MB

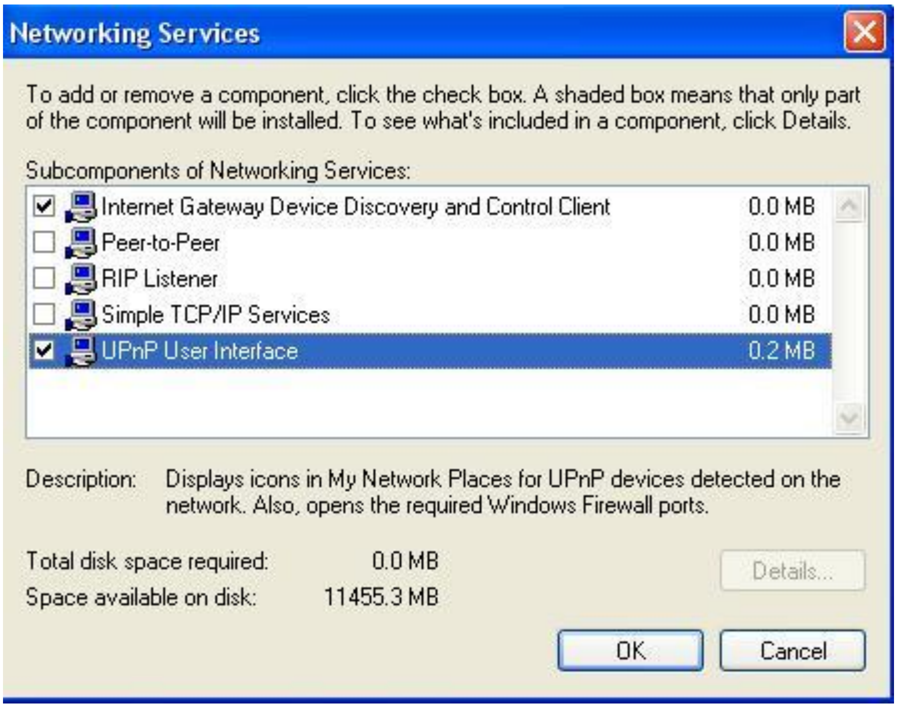
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 11457.8 MB

Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click **OK** to go back to the Windows Optional Networking Component Wizard window and click **Next**.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

- ☑ Internet Gateway Device Discovery and Control Client 0.0 MB
- ☐ Peer-to-Peer 0.0 MB
- ☐ RIP Listener 0.0 MB
- ☐ Simple TCP/IP Services 0.0 MB
- ☑ UPnP User Interface 0.2 MB

Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.

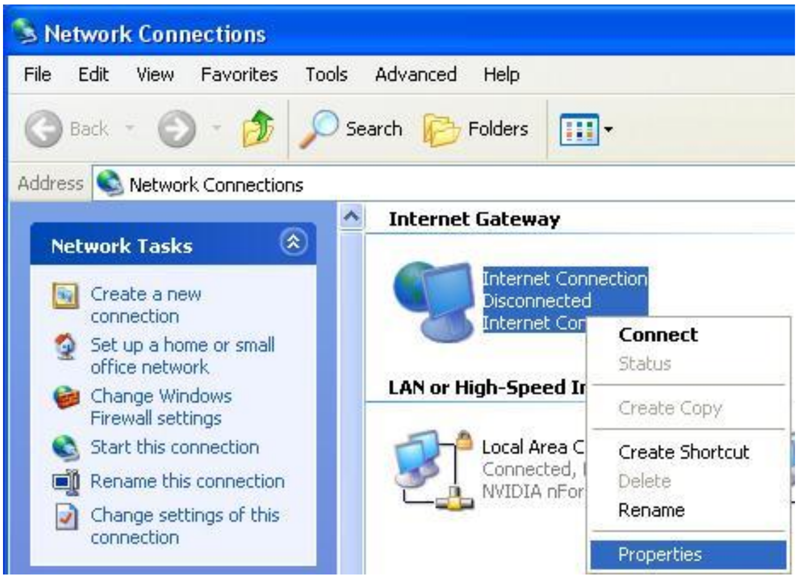
Total disk space required: 0.0 MB

Space available on disk: 11455.3 MB

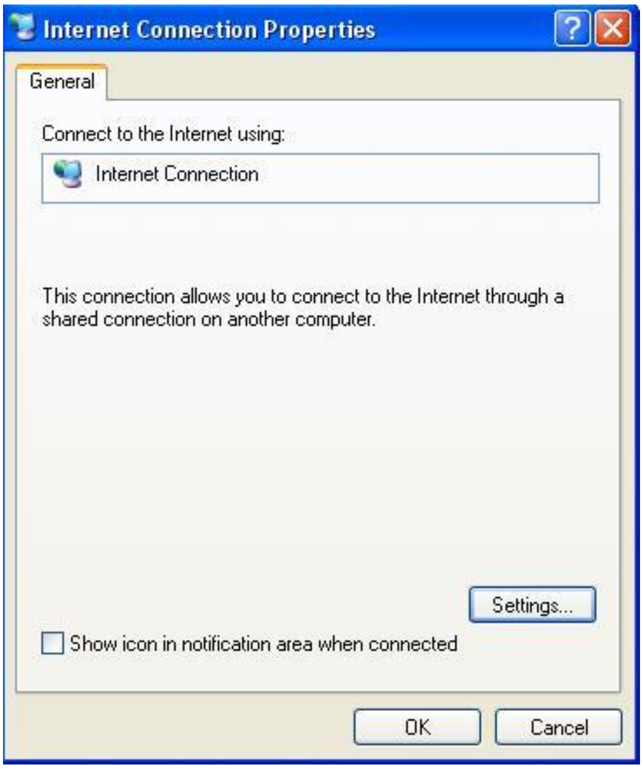
Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2: Right-click the icon and select Properties.



Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



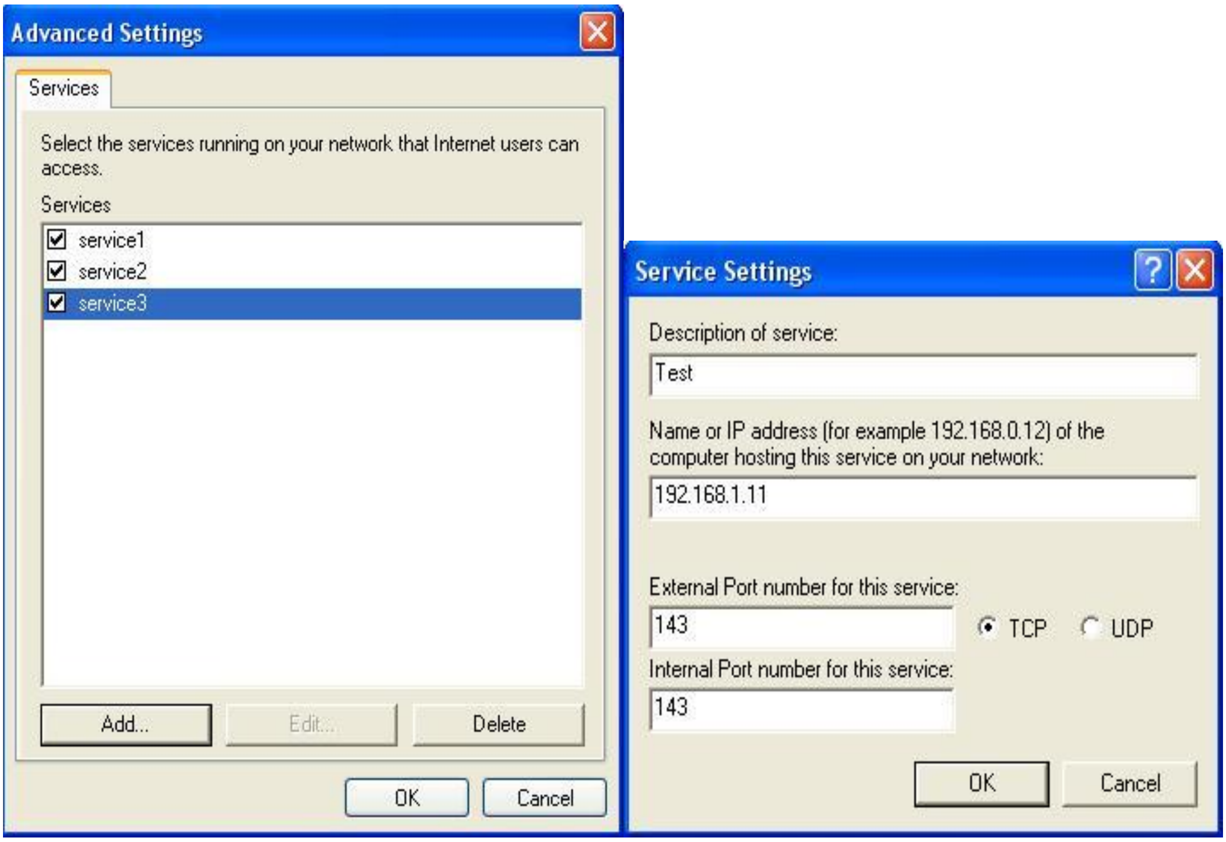
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

□ Show icon in notification area when connected

Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.


Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services

- ☑ service1
- ☑ service2
- ☑ service3

Service Settings

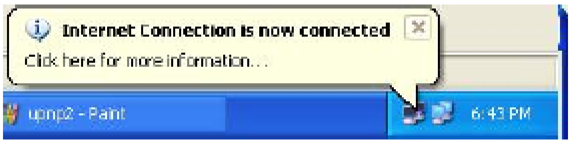
Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

External Port number for this service:
143 ● TCP ○ UDP

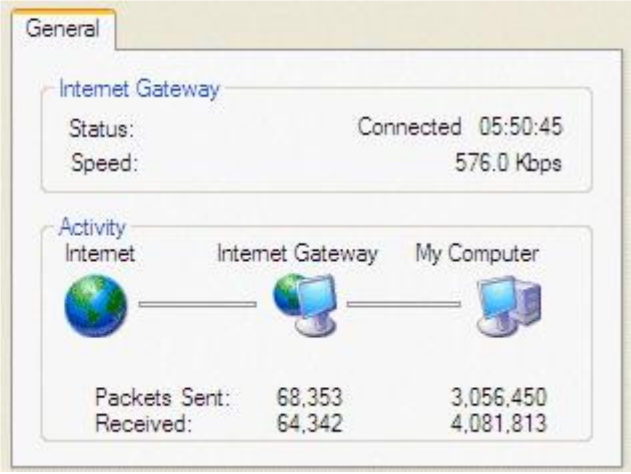
Internal Port number for this service:
143

Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray


Internet Connection is now connected

Click here for more information...

Step 6: Double-click on the icon to display your current Internet connection status.



Internet Gateway

Status: Connected 05:50:45

Speed: 576.0 Kbps

Activity

	Internet Gateway	My Computer
Packets Sent:	68,353	3,056,450
Received:	64,342	4,081,813

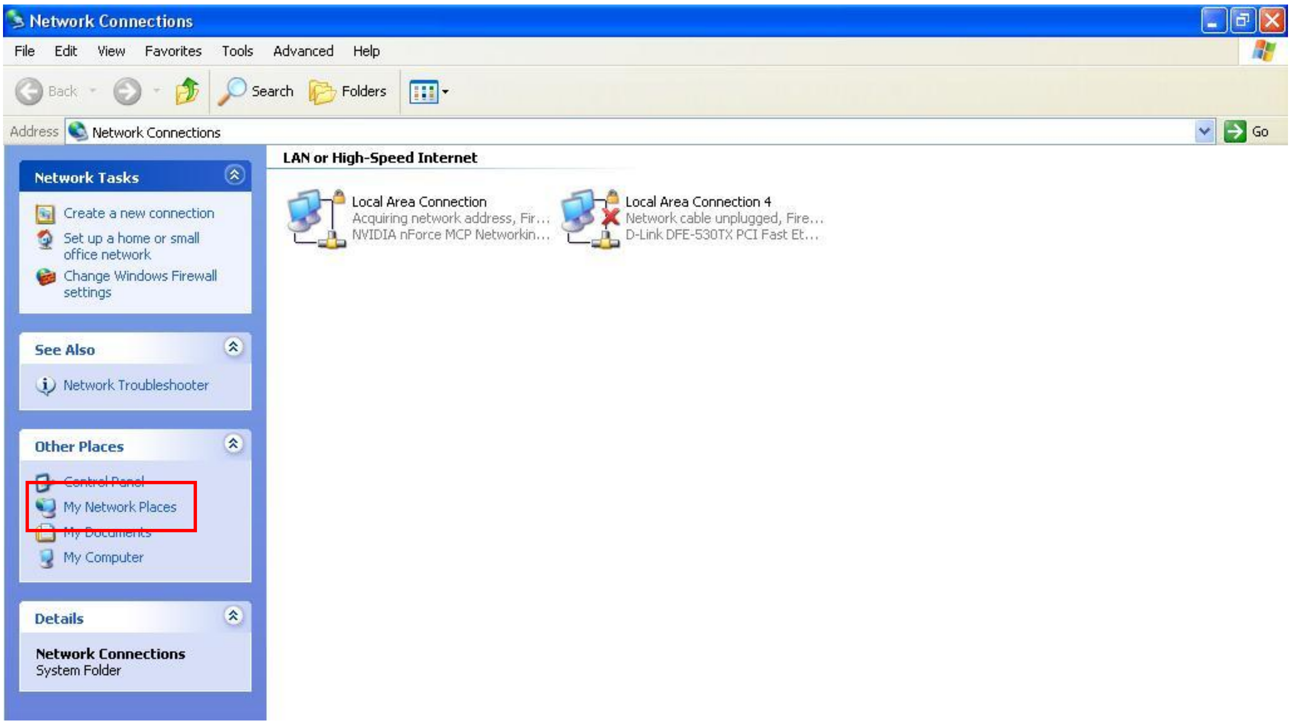
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the FBR-1461 without first finding out the IP address of the router. This helps if you do not know the router's IP address. Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



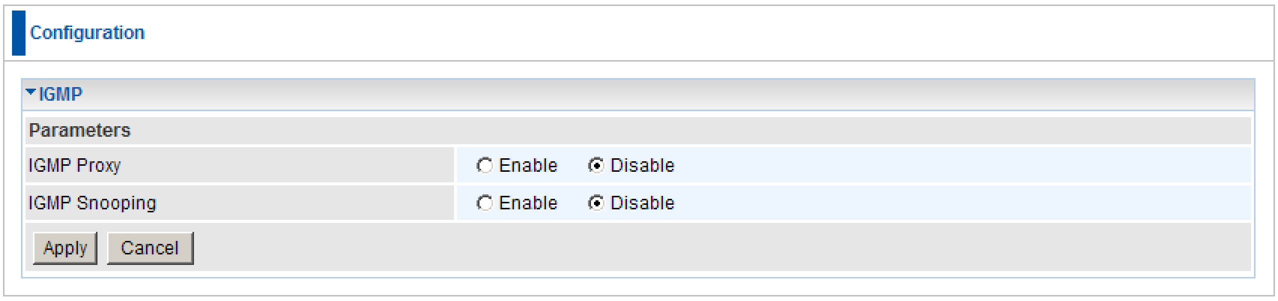
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your FBR-1461 and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your FBR-1461 and select Properties. A properties window displays basic information about the FBR-1461.

5.3.8.5 IGMP

IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.



Configuration

▾IGMP

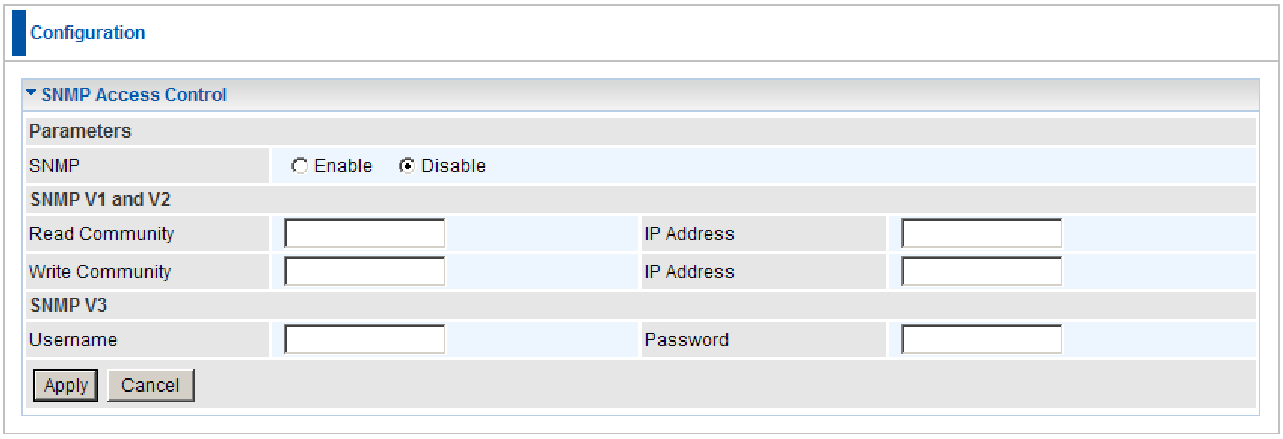
Parameters	
IGMP Proxy	○ Enable ● Disable
IGMP Snooping	○ Enable ● Disable

IGMP Proxy: Accepting multicast packet. Default is set to **Disable.**

IGMP Snooping: Allowing switched Ethernet / Wireless to check and make correct forwarding decisions. Default is set to **Disable.**

5.3.8.6 SNMP Access Control

Software on a PC within the LAN is required in order to utilize this function – Simple Network Management Protocol.



Configuration

▾SNMP Access Control

Parameters			
SNMP	○ Enable ● Disable		
SNMP V1 and V2			
Read Community		IP Address	
Write Community		IP Address	
SNMP V3			
Username		Password	

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user obtains this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users from this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access right from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPV2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

☑ System group

☑ Interfaces group

☑ Address Translation group

☑ IP group

☑ ICMP group

☑ TCP group

☑ UDP group

☒ EGP (not applicable)

☑ Transmission

☑ SNMP group

From RFC1650 (EtherLike-MIB):

☑ dot3Stats

From RFC 1493 (Bridge MIB):

☑ dot1dBase group

☑ dot1dTp group

☑ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

☑ pppLink group

☒ pppLqr group

From RFC 1472 (PPP/Security MIB):

☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

☑ PPP Bridge Group

From RFC1573 (IfMIB):

☑ ifMIBObjects Group

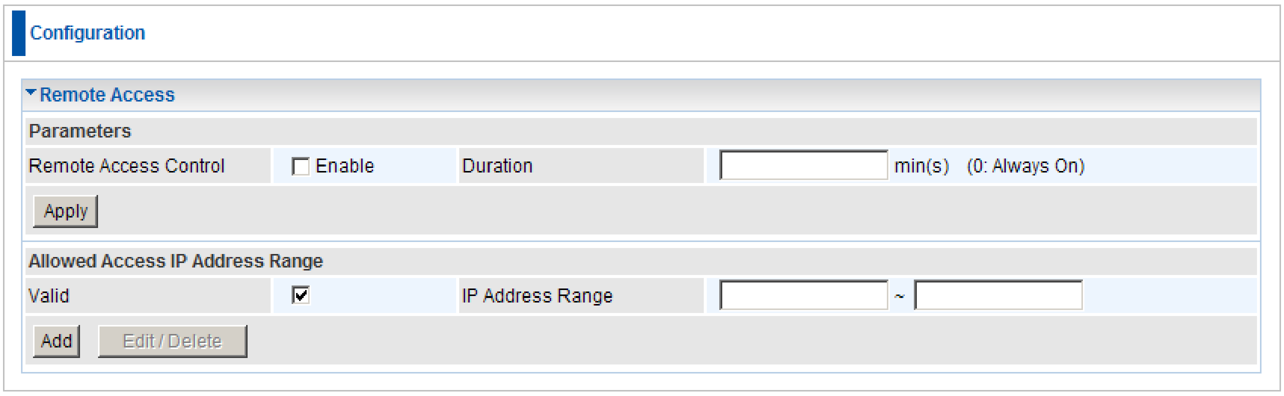
From RFC1695 (atmMIB):

☑ atmMIBObjects

From RFC 1907 (SNMPv2):

only snmpSetSerialNo OID

5.3.8.7 Remote Access



Configuration

▾ Remote Access

Parameters

Remote Access Control	□ Enable	Duration	min(s) (0: Always On)

Allowed Access IP Address Range

Valid	☑	IP Address Range	~

Remote Access Control:

Enable: Select Enable to allow management access from remote side (mostly from internet).

Duration: Set how many minutes to allow management access from remote side. Zero means always on.

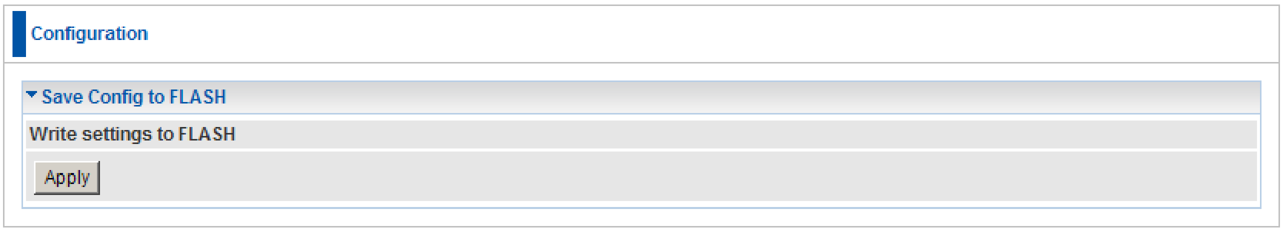
Allowed Access IP Address Range:

Valid: Select Valid to allow remote management from these IP ranges.

IP Address Range: Specify what ip address to be allowed to access device from remote side. Click “Add” to insert management ip address list.

5.4 Save Configuration to Flash

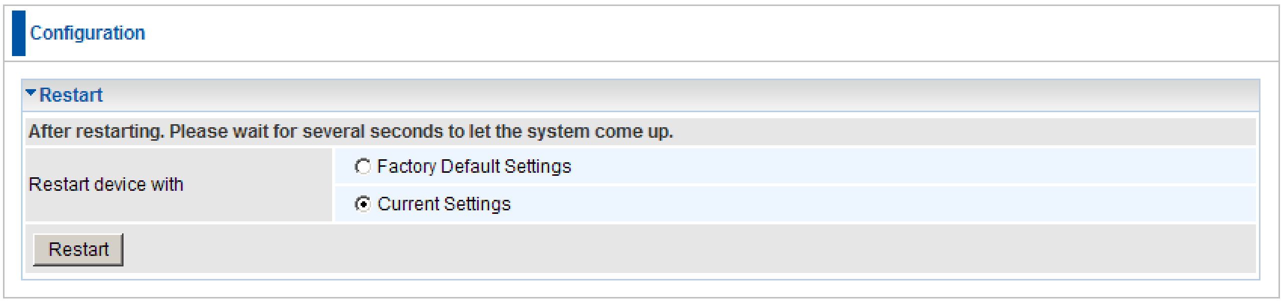
After changing the router’s configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click “**Save Config**“ and click “**Apply**” to write your new configuration to FLASH.



Write settings to FLASH

5.5 Restart

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).



After restarting. Please wait for several seconds to let the system come up.

Restart device with ○ Factory Default Settings ● Current Settings

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to reset to factory default settings.

5.6 Logout

To exit the router’s web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 30 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Logout

Chapter 6

Troubleshooting

If your ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.

Problems with the WAN Interface

Problem	Corrective Action
Initialization of the PVC connection (“linesync”) failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router. If you still have problems, you may need to verify these settings with your ISP.

Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting. Verify that the IP address and the subnet mask are consistent between the router and the workstations.