FBR-1461

ADSL2/2+ Modem Router

1W 4L QoS

User Manual

V1.0

Table of Content

1. Introduction

Thank you for purchasing the FBR-1461 ADSL2+ Modem/Router by LevelOne. Your new router is an all-in-one unit that combines an ADSL modem, ADSL 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.

1.1. 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) and IPoA (RFC1577) to establish a connection with an ISP. The router also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard

A web-based GUI and quick installation wizard help you easily install the FBR-1461. Enter your ISP information and begin browsing the Internet immediately.

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.Level1.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 ay lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination 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 do not 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.

Static and RIP1/2 Routing

An easy static routing table or RIP1/2 routing protocol supports routing capability.

Simple Network Management Protocol (SNMP)

SNMP allows convenient remote management of the router.

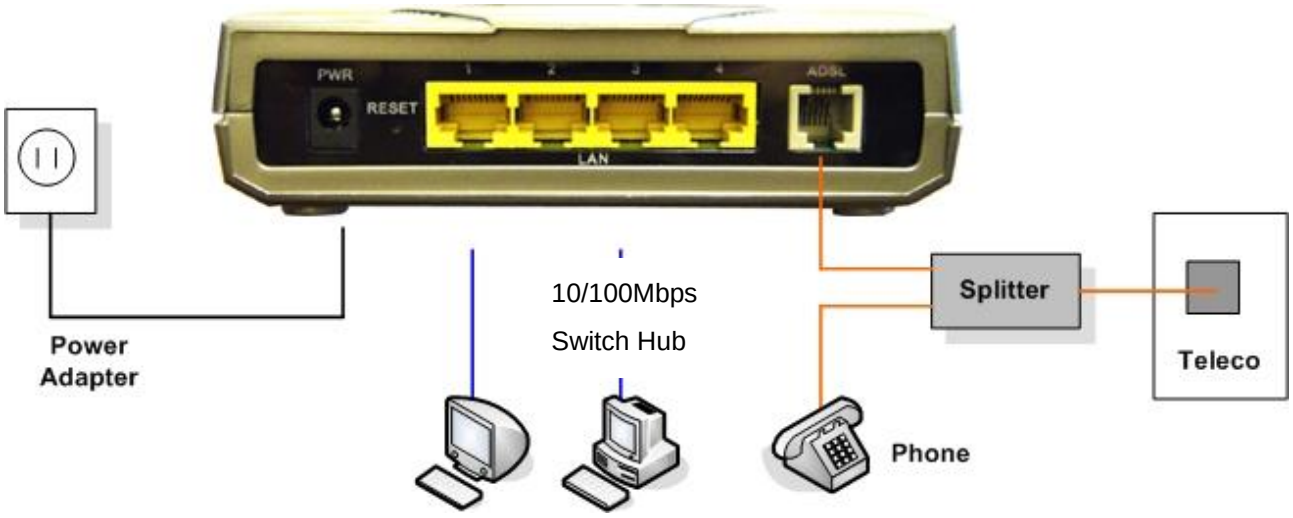
Web-based GUI

A web-based GUI offers easy configuration and management. User-friendly and with on-line help, 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.

1.2. Application Diagram



1.3. Package Contents

FBR-1461 ADSL2+ Router
RJ-11 ADSL/telephone Cable
Ethernet Cat.5 Cable
AC-DC power adapter (12V DC, 1A)
CD-ROM containing the online manual
Quick Installation Guide

1.4. 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.

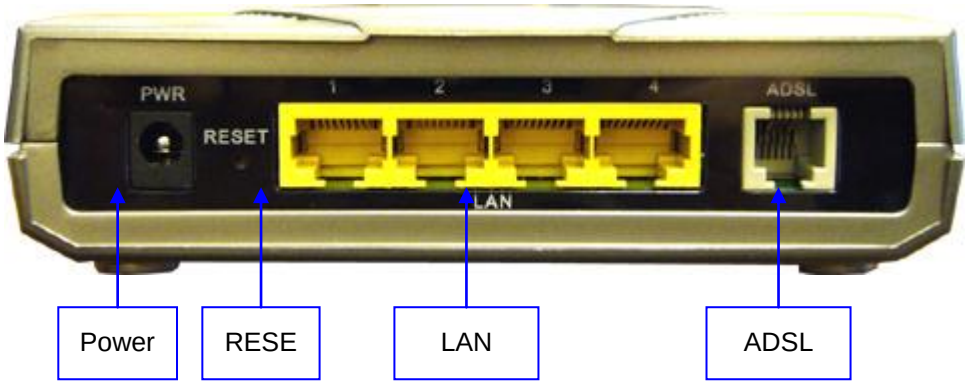
Attention:

- ✓ 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.

1.5. Front Panel

LED		Description
1	PPP	Steady glow when there is a PPPoA / PPPoE connection.
2	ADSL	Lights when successfully connected to an ADSL DSLAM (linesync).
3	LAN Port 1-4	Steady glow when connected to an Ethernet device. Glows green for 100Mbps; Orange for 10Mbps. Blinking light when data is Transmitted / Received.
4	SYS	Lights when the system is ready.
5	PWR	Lights when the power is ON.

1.6. Rear Panel



Port		Description
1	PWR	Connect the supplied power adapter to this jack.
2	RESET	After the router is powered on, press this recessed button using the end of paper clip or other small pointed object to reset the router or to restore it to factory default settings. 0-3 seconds: reset the device 6 seconds above: restore to factory default settings
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	ADSL (LINE)	Connect the supplied RJ-11 (telephone) cable to this port when connecting to the ADSL/telephone network.

1.7. Reset to Factory Default

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash): Hold the Emergency/Failure Recovery 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 Emergency/Failure Recovery Button. The modem's emergency-reflash web interface will then be accessible via http://192.168.1.254/ 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.

2. Recovery procedures for a lost web interface password:
After turning the router on press the Emergency/Failure Recovery Button on the back of the modem, and hold the button in until all lights on the modem flash and it reboots with factory default settings. The login will be reset to admin and the password will be reset to admin, and the modem will be accessible via its default IP address at http://192.168.1.254/

1.8. Cabling

One of the most common causes of problems is 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 LevelOne 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 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 frequent disconnections.

2. 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, Mac and Windows 98SE/2000/XP/Me include a web browser as a standard application.

2.1. Before Configuration

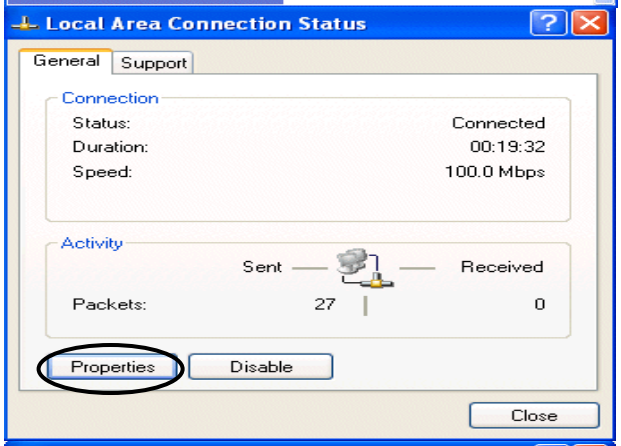
PCs must have a properly installed Ethernet interface and connect to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 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 of 192.168.1.1 to 192.168.1.253). The easiest way is to configure the PC to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router web interface you are advised to uninstall any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router.

Please follow the steps below for installation on your PC network environment. First of all, check your PC 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.

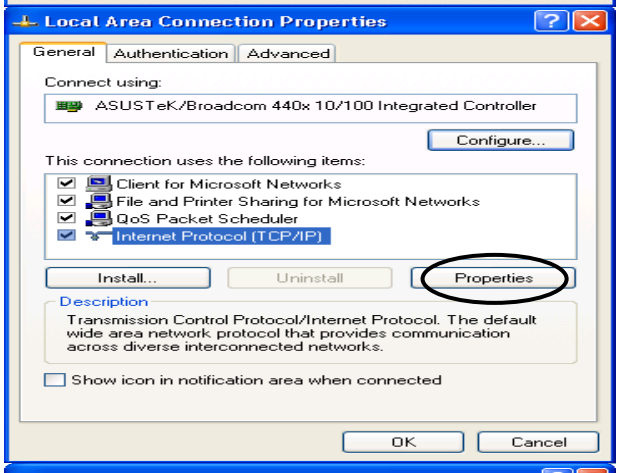
2.1.1. Configuring a PC in Windows XP

Go to Start / Control Panel (in Classic View).
In the Control Panel, double-click on Network Connections
Double-click Local Area Connection.

In the Local Area Connection Status window, click Properties.

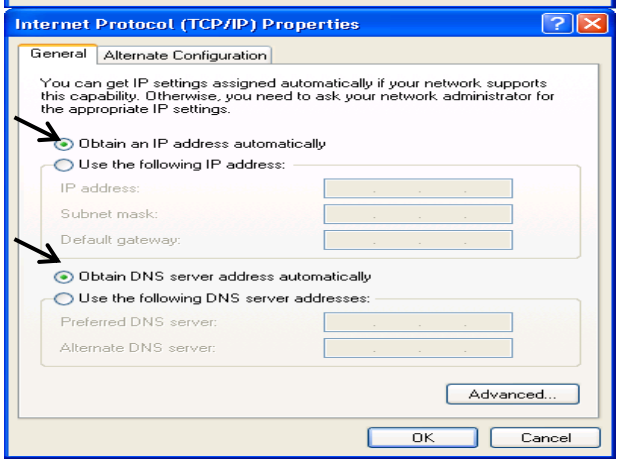


Select Internet Protocol (TCP/IP) and click Properties.



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

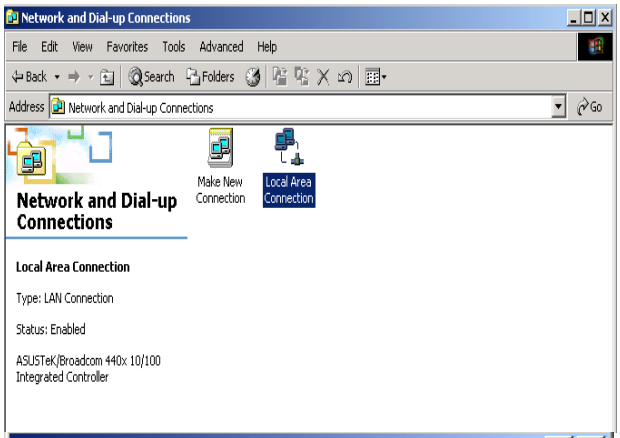
Click OK to finish the configuration.



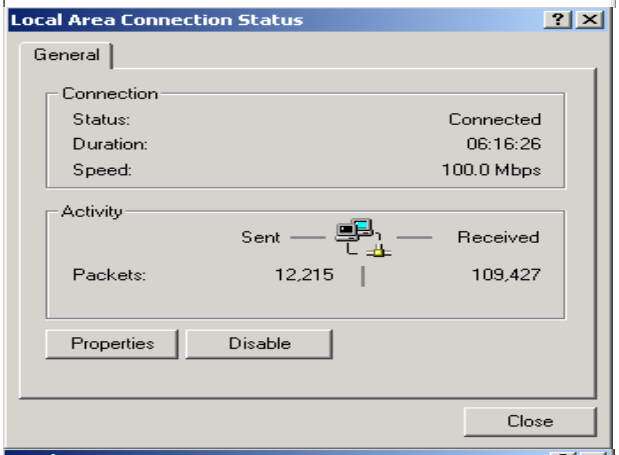
2.1.2. Configuring a PC in Windows 2000

1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.

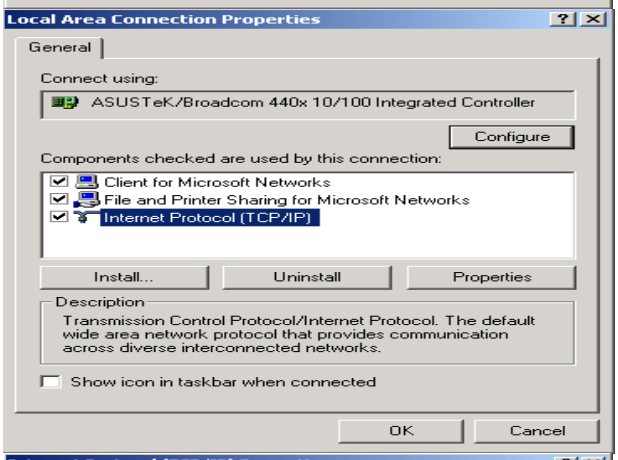
2. Double-click Local Area Connection.



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

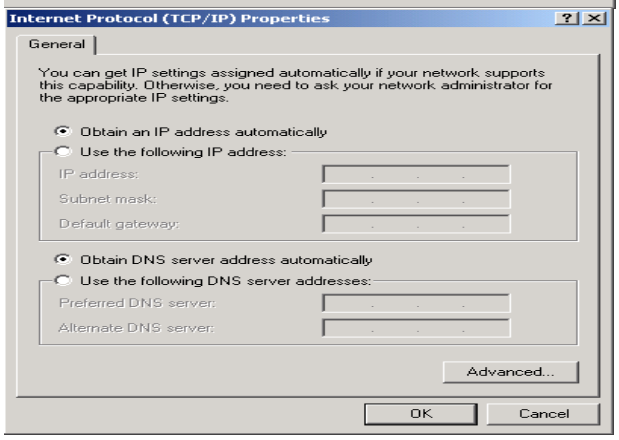


4. Select Internet Protocol (TCP/IP) and click Properties.



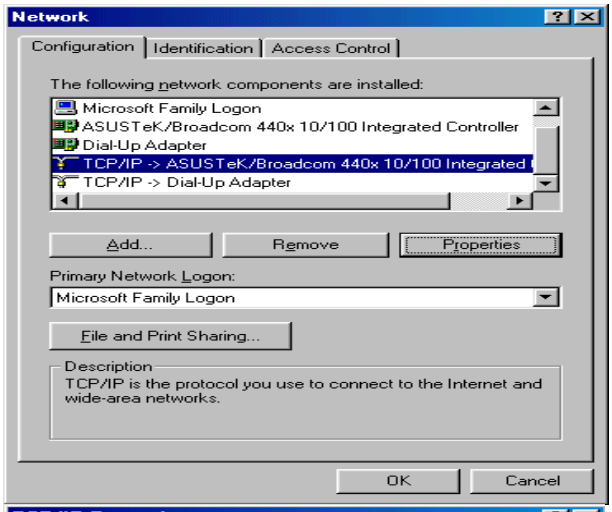
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.

6. Click OK to finish the configuration.



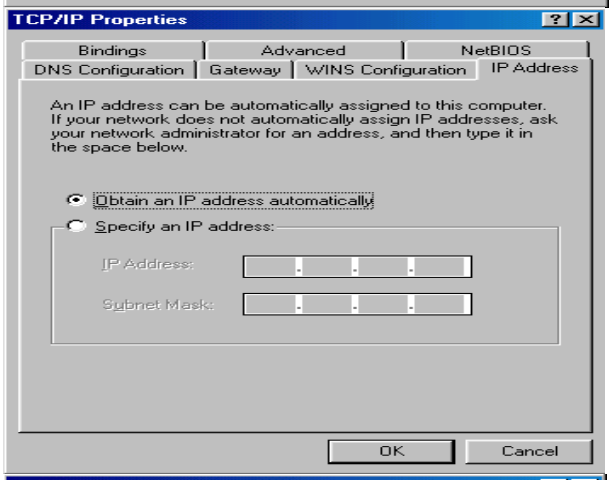
2.1.3. Configuring a PC in Windows 98SE/Me

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



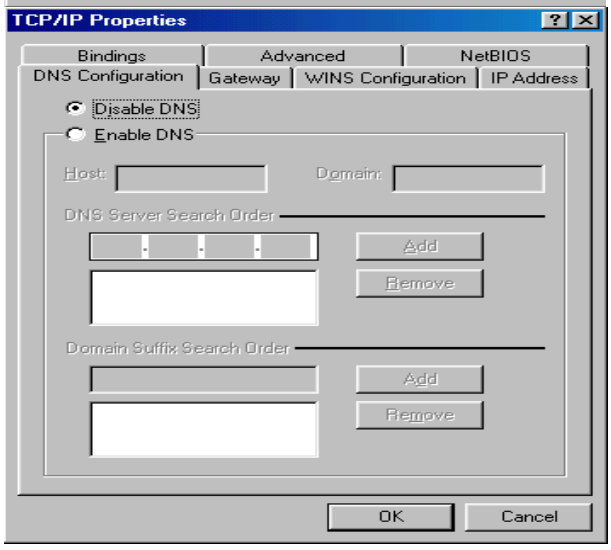
2.Select TCP/IP ->NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.

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



4.Then select the DNS Configuration tab.

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



2.2. Default Settings

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

Web Interface:
Username: admin
Password: admin

LAN Device IP Settings:
IP Address: 192.168.1.254
Subnet Mask: 255.255.255.0

ISP setting in WAN site:
PPPoE

DHCP Server:
DHCP server is enabled.
Start IP Address: 192.168.1.100
IP pool counts: 100

2.3. 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	192.168.1.254	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	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

2.4. Configuring with your ADSL Modem Router

To configure this device, you must have IE 5.0 / Netscape 4.5 or above installed

You may configure the router for Internet access in two ways: **Easy Sign-On** (EZSO) and **Web Configuration**

2.4.1. Easy Sign On (PPPoE / PPPoA / DHCP)

PPPoE

With EZSO built-in, you can simply plug cables in as first installation and turn on host computer to surf Internet through WEB browser like IE. You do not need to login into the router and search the router WEB GUI configuration page to find out the right web page for configuring your PPPoE/PPPoA credentials. EZSO feature in LevelOne routers will do it for you. When you are trying to surf the internet through WEB browser, the PPPoE dialogue will be visible and nothing but that. After you have successfully submitting the credentials, everything will be fine and work neatly.

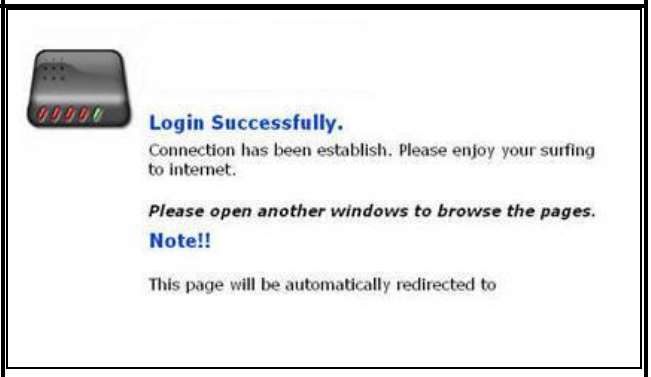
1. Please wait when the connection is trying.	2.Enter the username and password provide by your ISP.
	
3. If login failed, Please check and input the correct username and password again.	4. Login Successfully.
	

PPPoA

1. Please wait when the connection is trying.	2.Enter the username and password provide by your ISP.
	
3. If login failed, Please input the correct username and password again.	4. Login Successfully.
	

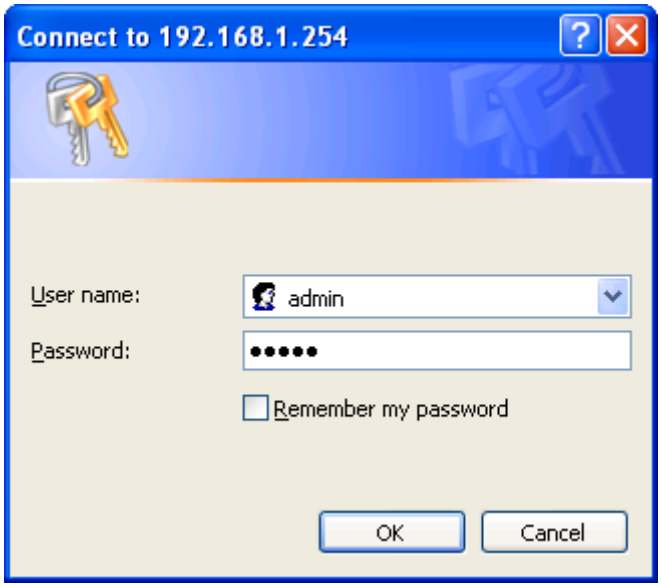
DHCP

With this method, user does not need to access router to configure it and set lot of parameters. Besides, it eliminates the complicated way to configure the device and will definitely reduce the service call from users.

1. Please wait when the connection is trying.	2. Login Successfully.
	

2.4.2. Web Configuration:

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**, a user name and password window prompt appears. The default username and password are **admin** and **admin**.



Congratulations! You have successfully logged on to your ADSL2+ Modem Router

3. Configuration

Once you have logged on to your FBR-1461 ADSL2+ 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:

Status
ARP Table, Routing Table, DHCP Table, System Log, Security Log

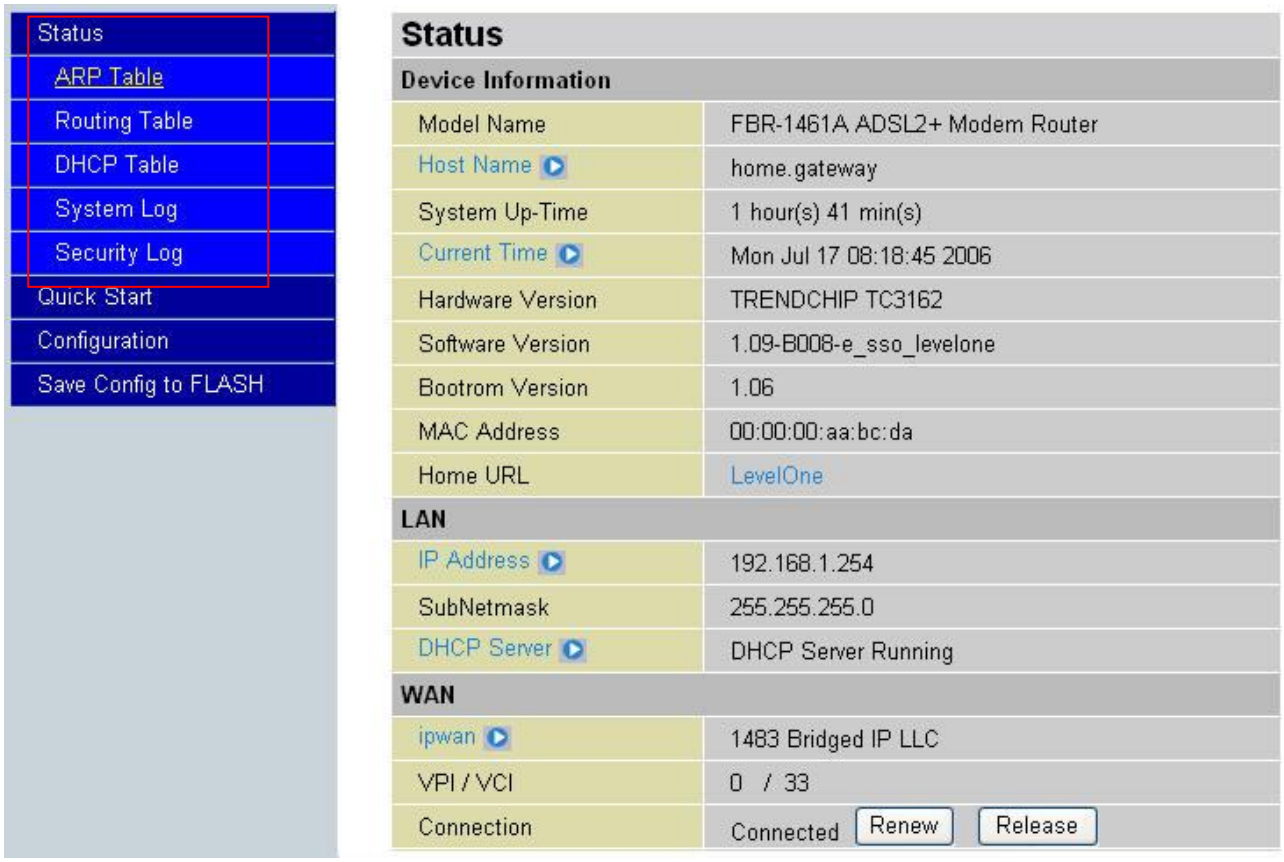
Quick Start

Configuration
LAN, WAN, System, Firewall, QoS, Virtual Server, Advanced

Save Config to FLASH

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

3.1. Status



Device Information

Model Name: Shows device model name

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name.

System Up-Time: Records system up-time.

Current time: Set the current time. See the Time Zone section for more information.

Hardware Version: Chipset version

Software Version: Firmware version

Bootrom Version: Boot ROM version

MAC Address: The WAN MAC address

Home URL: Connects to the LevelOne Website.

LAN

IP Address: LAN port IP address.

Sub Net Mask: LAN port IP subnet mask.

DHCP Server: DHCP status.

WAN

IP WAN: Name of the WAN connection.

VPI/VCI: Virtual Path Identifier and Virtual Channel Identifier

Connection: Shows connection status. You can click on **Disconnect** or **Connect** to re-establish connection when PPPoE/PPPoA with Dynamic IP selected. Or click **Renew** (Click to renew IP address) and click **Release** (Click to drop current IP address) if RFC 1483 Routed mode selected.

3.1.1. ARP Table

The router ARP (Address Resolution Protocol) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine the MAC address of the network interface of your PCs to use with the router Firewall - MAC Address Filter function. See the Firewall section of this manual for more information.

ARP Table

IP <> MAC List

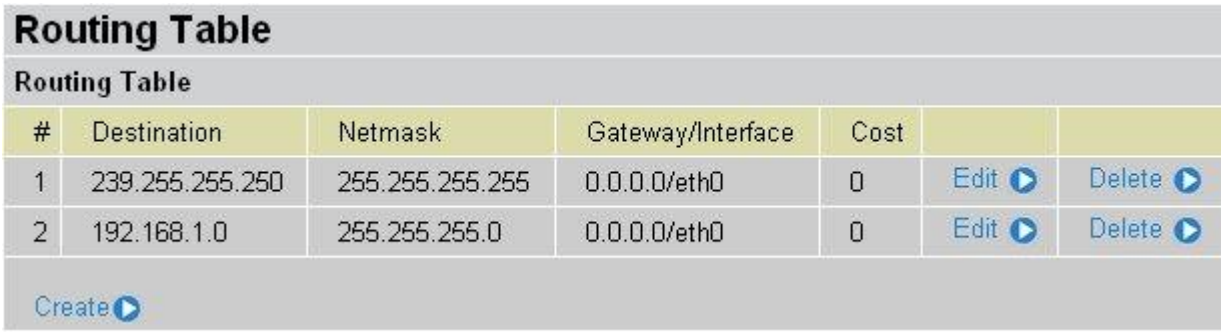
IP Address	MAC Address	Interface	Static
192.168.1.125	00:11:6B:18:7D:F7	iplan	no

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).
MAC Address: MAC (Media Access Control) address for each device on your LAN.
Interface: The interface name (on the router) that this IP Address connects to.
Static: Static status of the ARP table entry:

no for dynamically-generated ARP table entries

yes for static ARP table entries added by the user

3.1.2. Routing Table



Routing Table:
#: Item number
Destination: IP address of the destination network.
Netmask: The destination netmask address.
Gateway/Interface: IP address of the gateway or existing interface that this route uses.
Cost: The cost of transmission for routing purposes. The number need not be precise, but it must be between 0 and 65535.

Edit: Click here to change current route table setting
Delete: Click here to delete current route table
Create: Click to add new route table

Pls refer to Chapter 3.3.7 Advanced for create Static Route

3.1.3. DHCP Table

DHCP Table

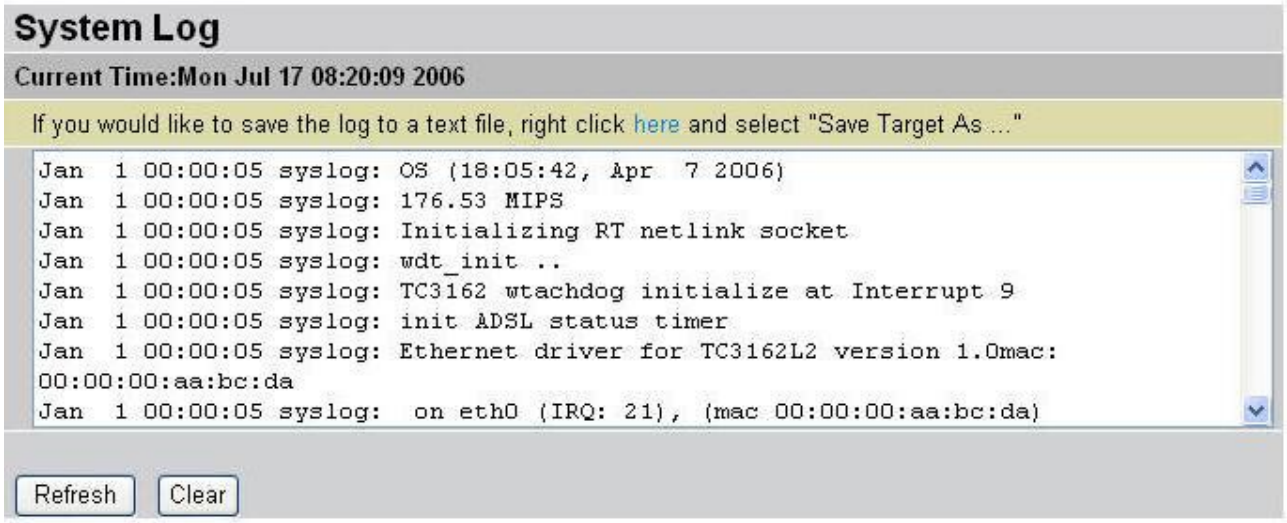
Leased Table

IP Address	MAC Address	Client Host Name	Register Time
192.168.1.102	00:c0:9f:99:d3:50	[redacted]	2006/07/17 08:16:51 - 2006/07/17 20:16:51
192.168.1.100	00:0d:61:1f:ec:3f	cvc	2006/07/17 07:09:31 - 2006/07/17 07:09:31
192.168.1.101	00:0d:61:1f:ec:3f	cvc	2006/07/17 07:09:31 - 2006/07/17 19:09:31

Leased Table, DHCP assigned IP addresses information.
IP Address: IP addresses of devices on your LAN (Local Area Network).
MAC Address: The MAC Address that you want to assign the fixed IP address
Client Host Name: Expired IP addresses information
Register Time: Register time information

3.1.4. System Log

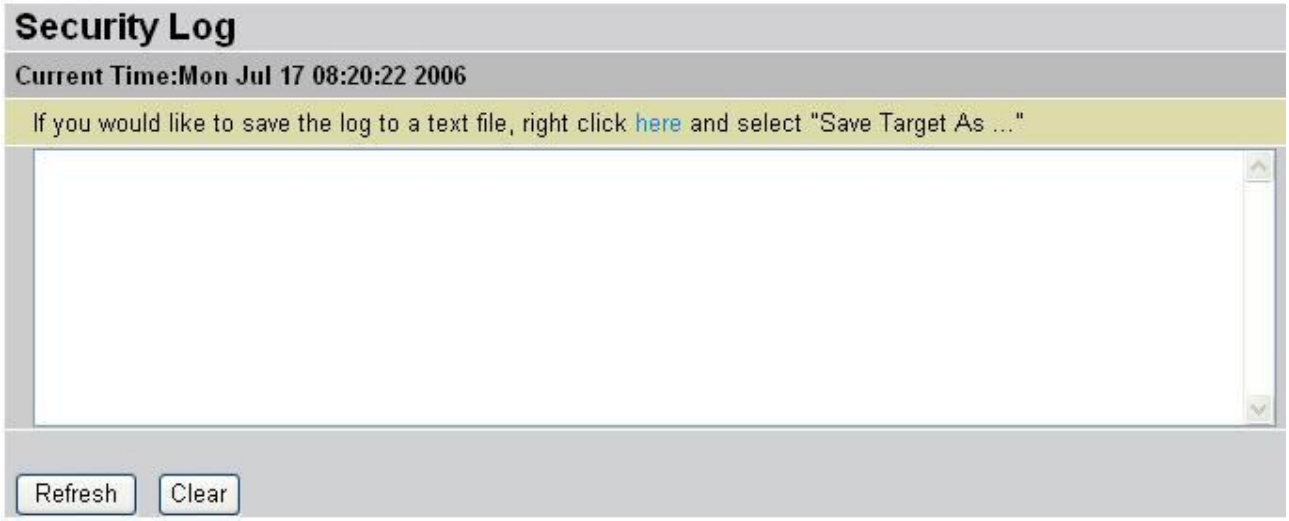
Display system logs accumulated up to the present time. You can trace historical information with this function. You can also save log file by right click **here** and select **Save Target As..**



Refresh: Update log information
Clear: Clean up log information

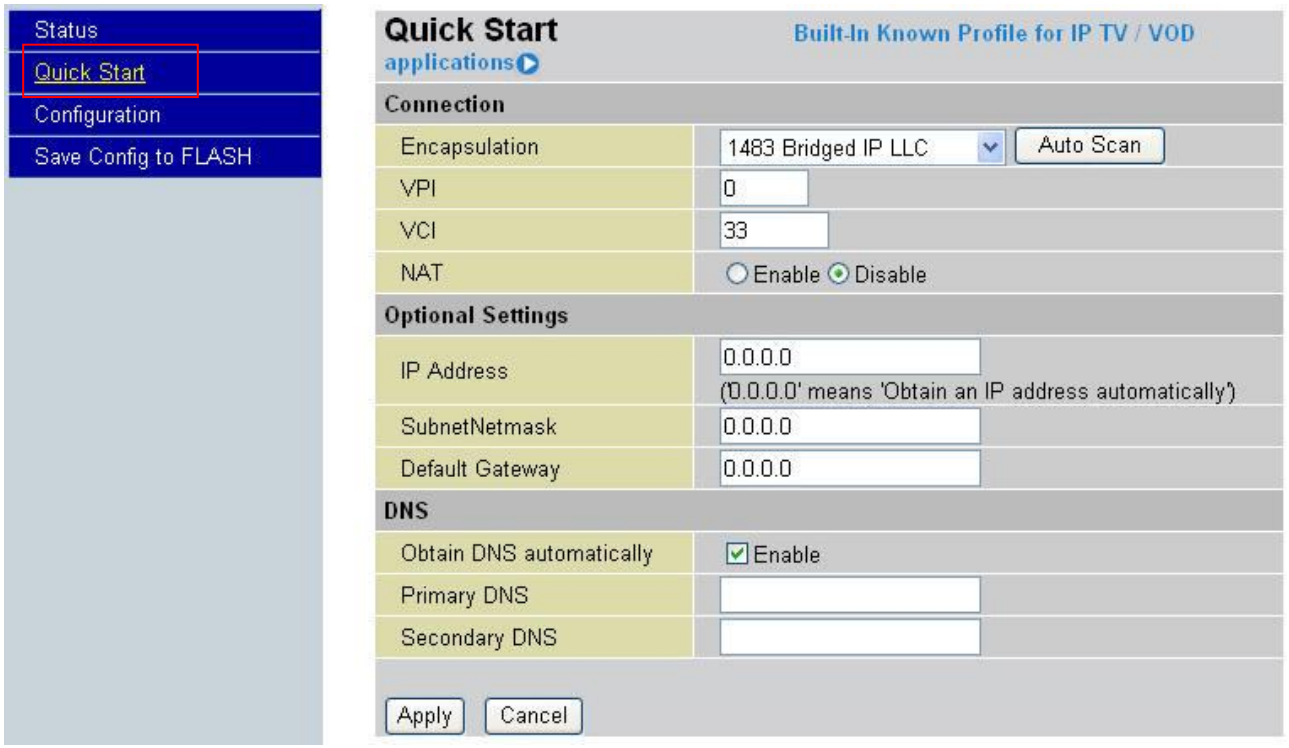
3.1.5. Security Log

This screen displays security log information. If a hacker attacks your server, he is isolated by the firewall function and the router records related information. This helps you know where the hacker comes from.



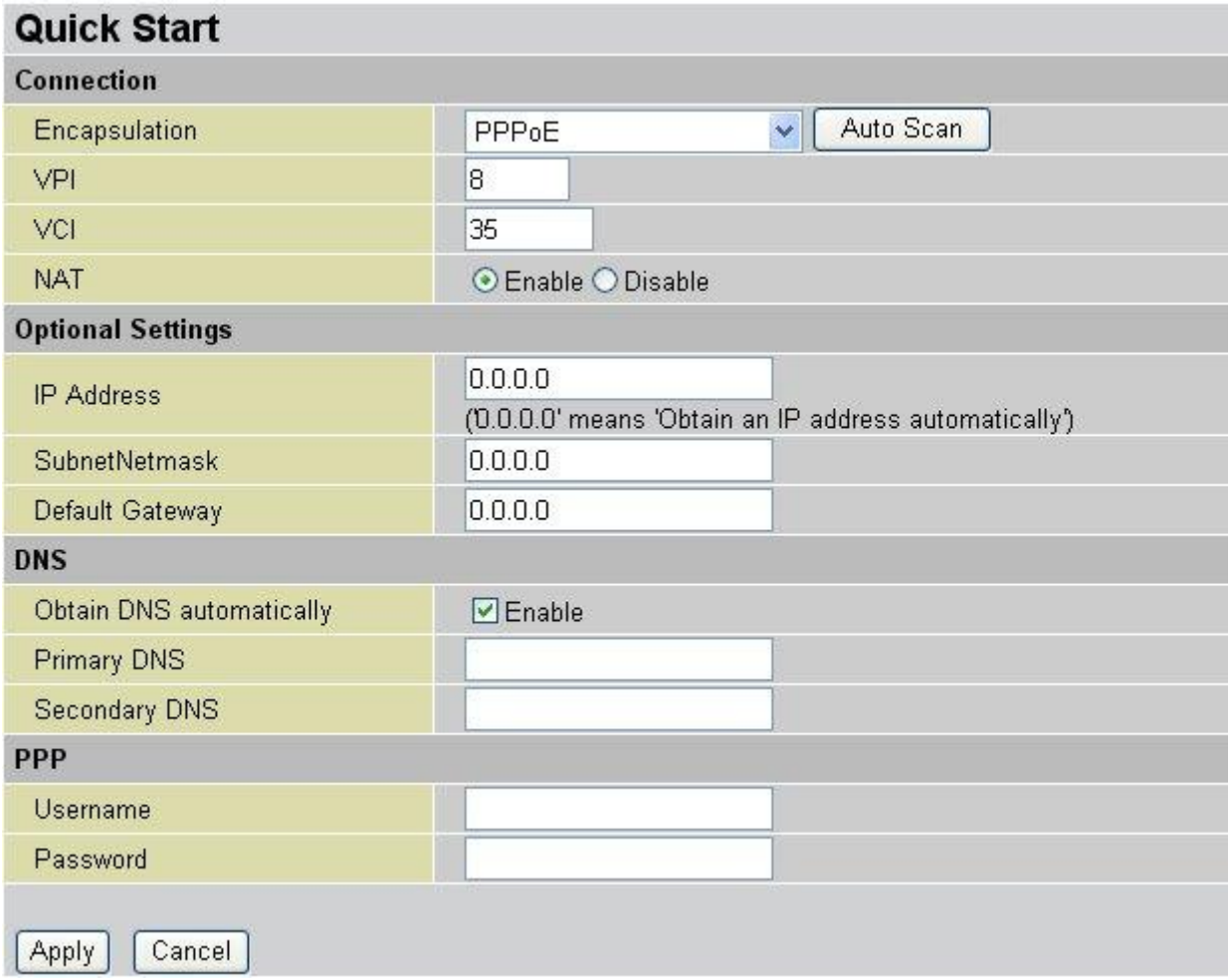
Refresh: Update log information
Clear: Clean up log information

3.2. Quick Start



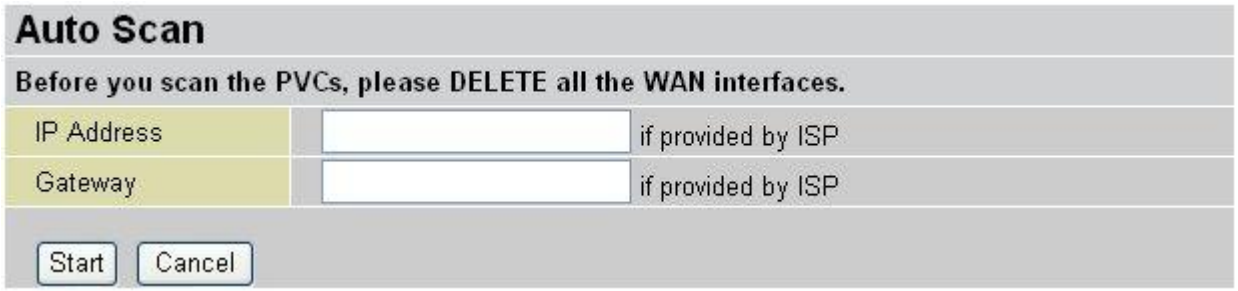
For detailed instructions on configuring WAN settings, see the WAN section of this manual. The information you need for the Quick Start wizard to get you online are your login (often in the form of username@ispname), your password, and the encapsulation type.

Your ISP can supply all the details you need. Alternatively, if you have deleted the current WAN Connection in the WAN - ISP section of the interface, you can use the router PVC Scan feature to determine the Encapsulation types offered by your ISP.



- **Connection**

Encapsulation: Select the encapsulation type your ISP uses or choose **Auto Scan**



Click Start to begin scanning for encapsulation types offered by your ISP. Autoscan windows shows processing and wait few seconds to complete scan. If the scan is successful, you are presented with a list of supported options.

VPI: Enter the VPI assigned to you. This field may already be configured.
VCI: Enter the VCI assigned to you. This field may already be configured.
NAT: Select **Enable** or **Disable** NAT function

- **Optional Setting**

IP Address: Type your ISP assigned IP address in the IP Address text box.
Subnet Mask: Enter a subnet mask in dotted decimal notation.
Default Gateway: You must specify a gateway IP address (supplied by your ISP)

- **DNS**

Obtain DNS automatically: Select this check box to use DNS.
Primary 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.
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.

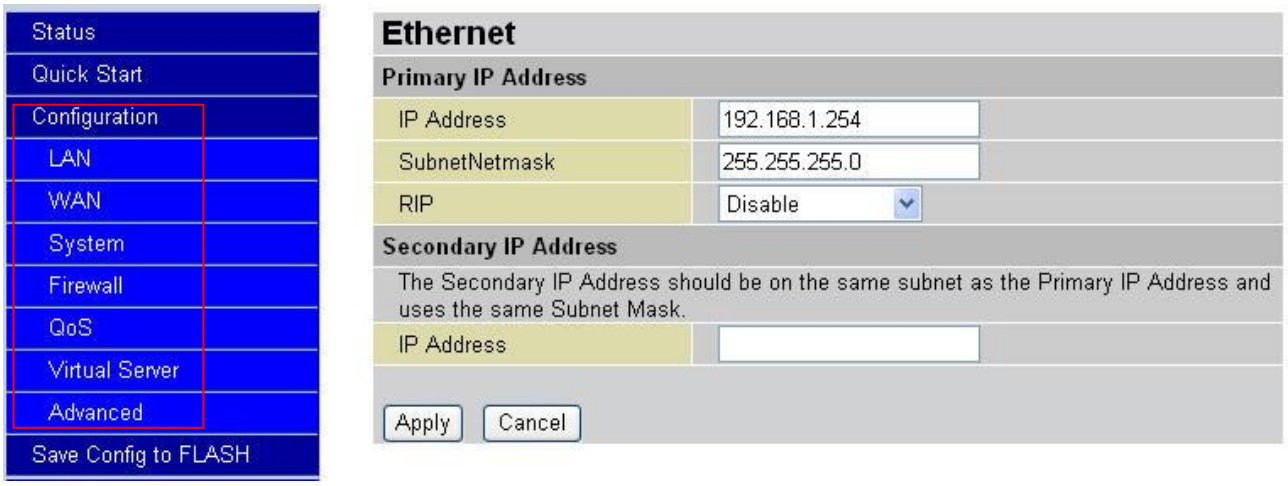
- **PPP**

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is usually 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).

Apply: Click to save settings
Cancel: Click to discard changes

3.3. Configuration

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

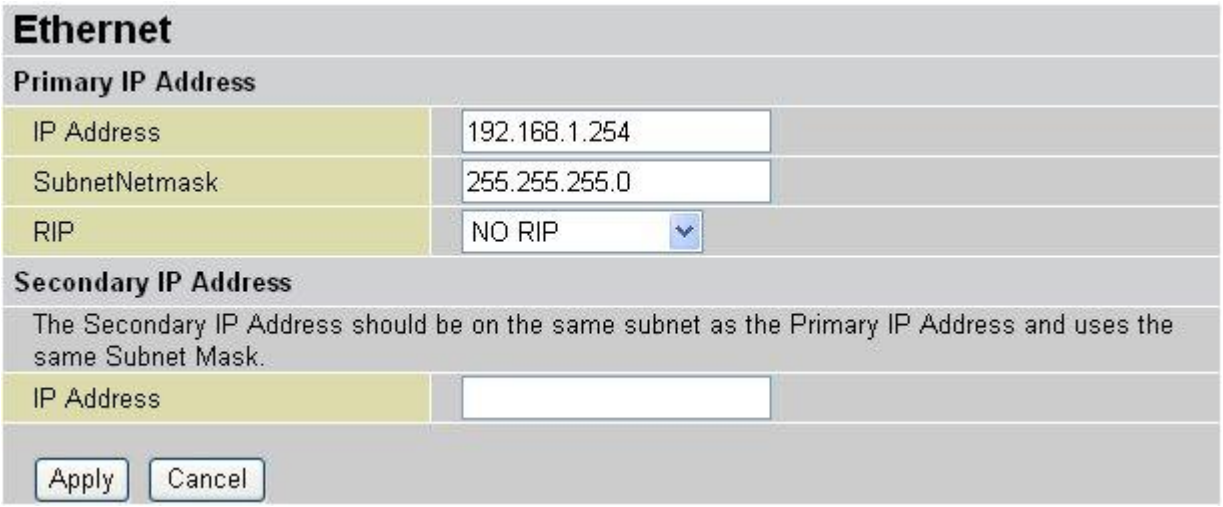


3.3.1. LAN (Local Area Network)

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 two items within the LAN section: Ethernet, and DHCP Server.

Ethernet



The router supports two Ethernet IP addresses in the LAN, and two different LAN subnets through which you can access the Internet at the same time. Users usually only have one

subnet in their LAN, so there is no need to configure a Secondary IP address.

Primary IP Address: Enter IP address and Subnet Mask to meet your network requirement. The default IP address for the router is 192.168.1.254

RIP: RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

Secondary IP Address: Enter the Secondary IP Address to add more subnets to meet your network requirement. The Secondary IP Address should be the same subnet as the Primary Subnet Mask.

Apply: Click to save settings

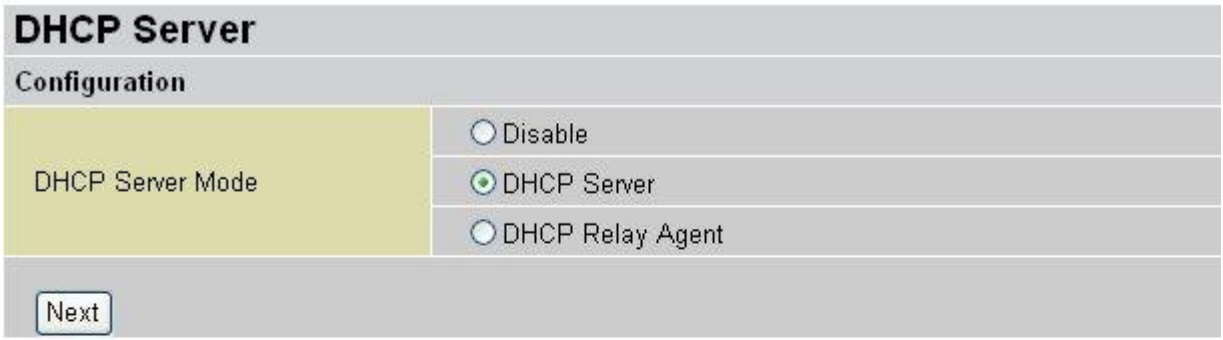
Cancel: Click to discard changes

Note:

The Subnet mask of the Secondary IP Address depends on the setting of the Primary IP Address.

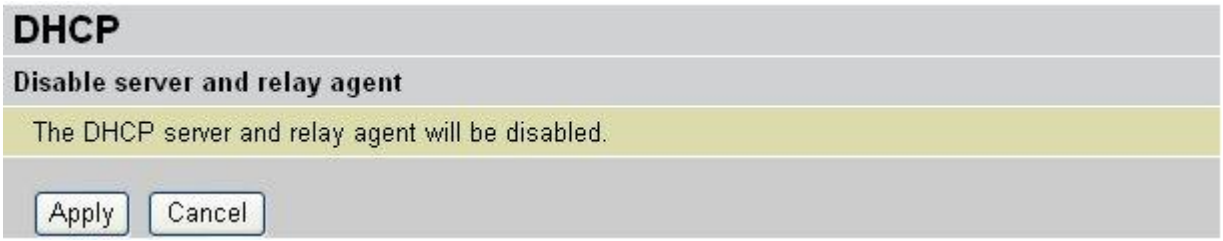
DHCP Server

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 Status	
Status	DHCP Server Running
Subnet Definitions	
Subnet Value	192.168.1.0
SubnetNetmask	255.255.255.0
Domain Name	home.gateway
DNS Server	192.168.1.254
Maximum/Default Lease Time	86400 / 43200 seconds
IP Range	192.168.1.100 - 192.168.1.199

To disable the router's DHCP Server, check **Disable** and click **Next** then click **Apply**. When the DHCP Server is disabled you 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 192.168.1.254)

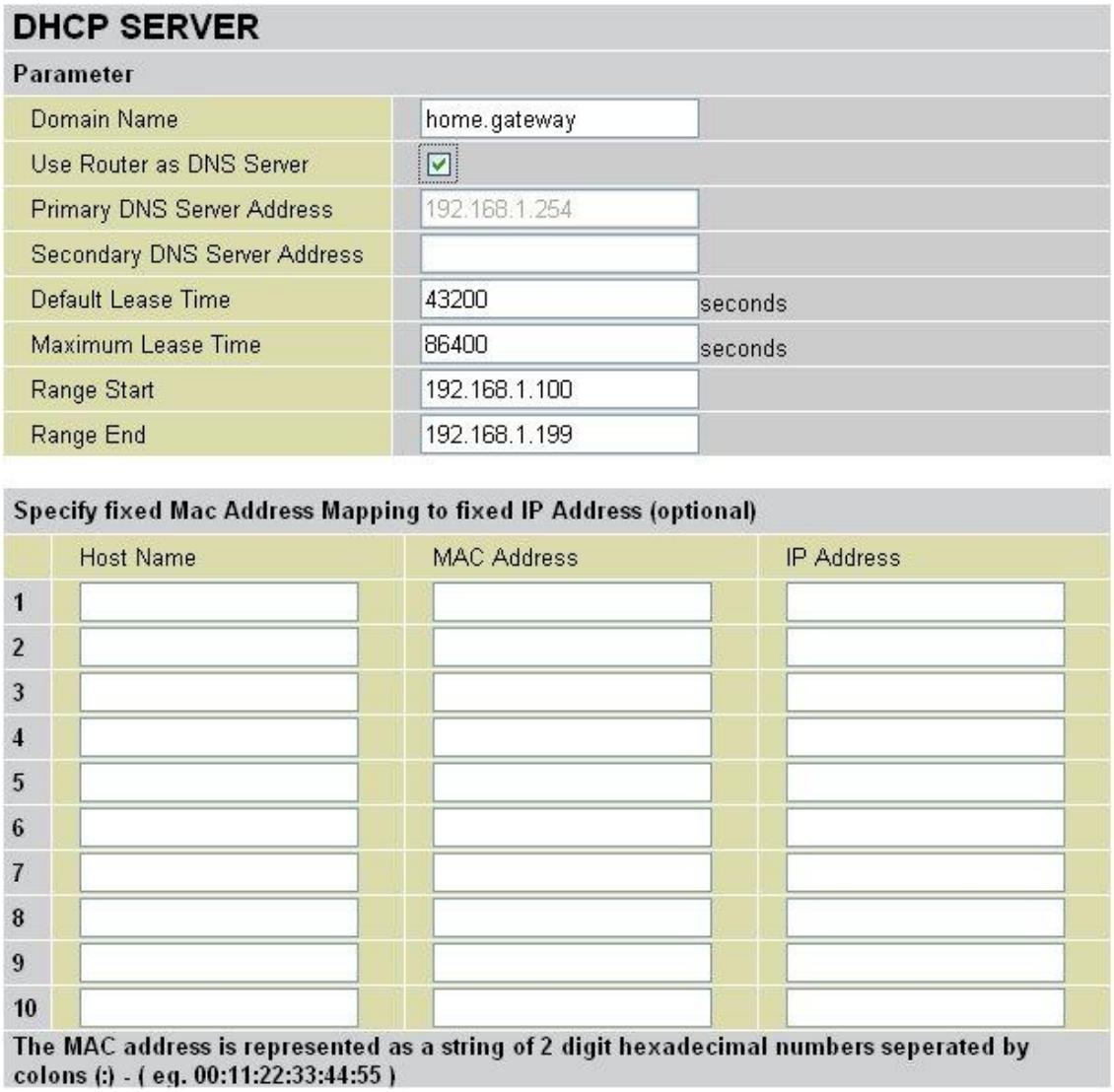


To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the **Domain Name**, **Use Router as DNS Server**, **DNS Server Address**(Primary and Secondary), **Default Lease Time**, **Maximum Lease Time** (Lease time for each assigned IP address, it's the period of time the IP address assigned will be valid), **IP pool** (starting IP address and ending IP address range)

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). You need to enter **DNS Server Address**(Primary and Secondary) manually if unchecked.

Router can assign fixed IP address to specified MAC address. Enter Host Name, MAC Address and IP Address into **Specify fixed Mac Address Mapping to fixed IP Address** table. When cleint (PC) connect to router and reqest an IP address, then fixed IP address will assgined permanently.



If you check DHCP Relay Agent and click Next 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.

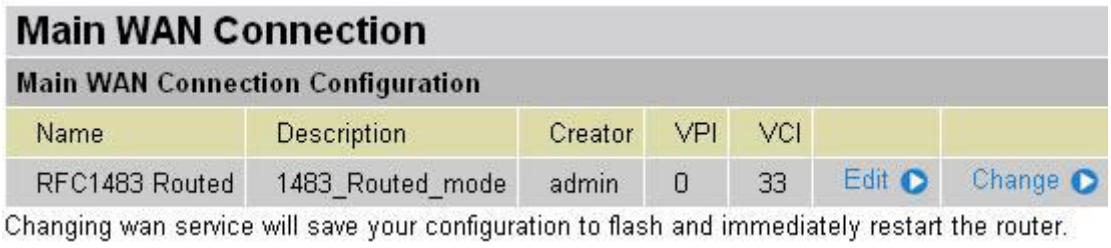
3.3.2. WAN (Wide Area Network)

A WAN (Wide Area Network) is an outside connection to another network or the Internet. There are three items within the WAN section: ISP, DNS and ADSL.

ISP

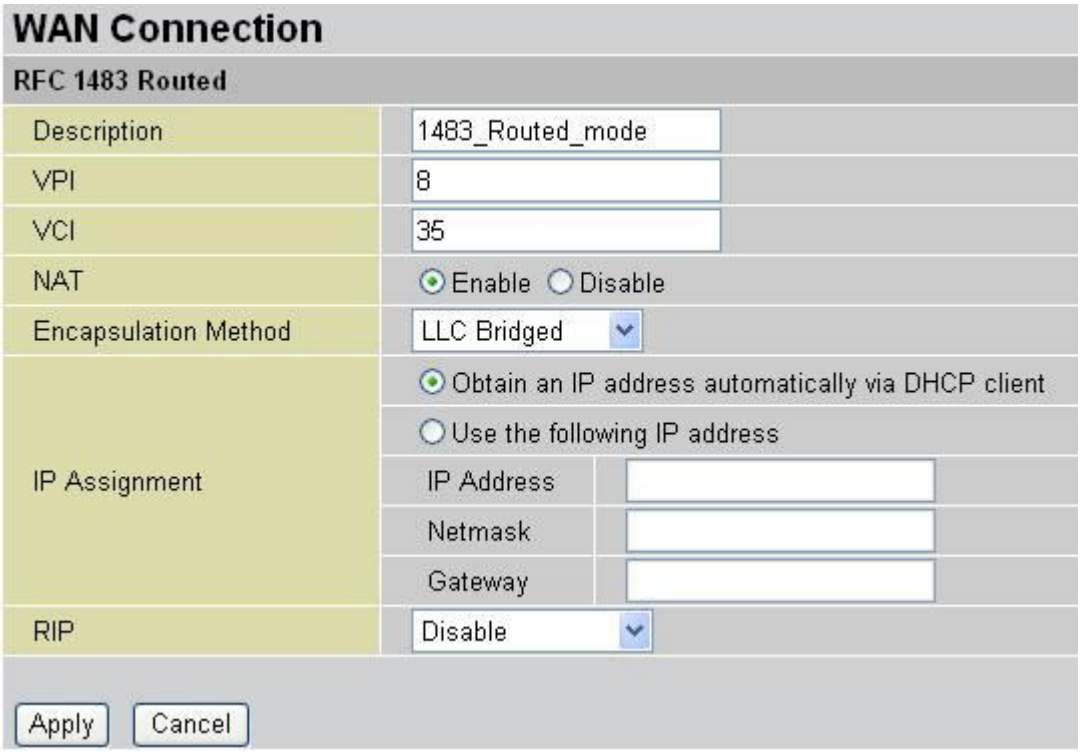
The factory default is PPPoE. If your ISP uses this access protocol, click Edit to input other parameters as below. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking Change.

A simpler alternative is to select Quick Start from the main menu on the left. See the Quick Start section of the manual for more information.



You can change current setting by click **Edit**, or click **Change** to select different connection type.

RFC 1483 Routed Connections



Description: Your description of this connection.

VPI and VCI: Enter the information provided by your ISP.

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.

Encapsulation method: Select the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP.

IP Assignment

DHCP client: Enable or disable the DHCP client, specify if the router can get an IP address from the Internet Service Provider (ISP) automatically or not.

Obtain an IP address automatically via DHCP client to enable the DHCP client function or click **Use the following IP address** to specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

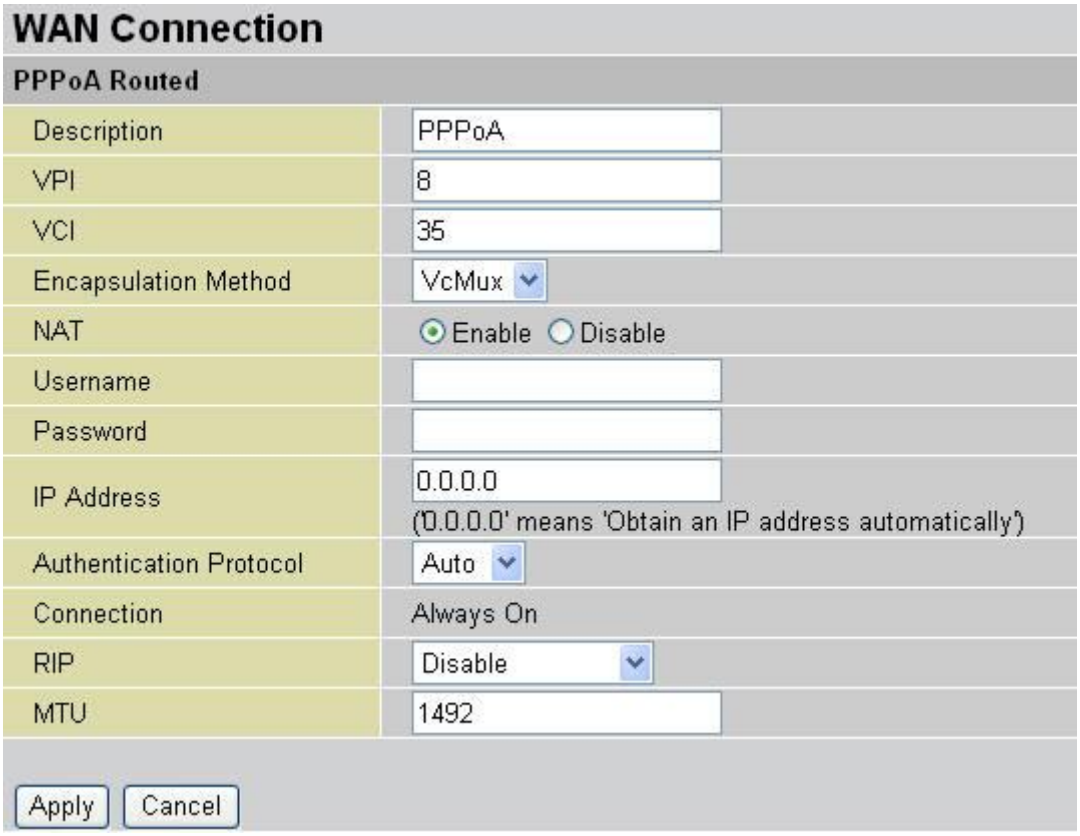
RIP: Disable, RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

Apply: Click to save settings

Cancel: Click to discard changes

PPPoA Routed Connections

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.



Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

Encapsulation method: Select the encapsulation format, VcMux or LLC. Select the one provided by your ISP.

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.

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).

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to automatically obtain an IP address from your ISP.

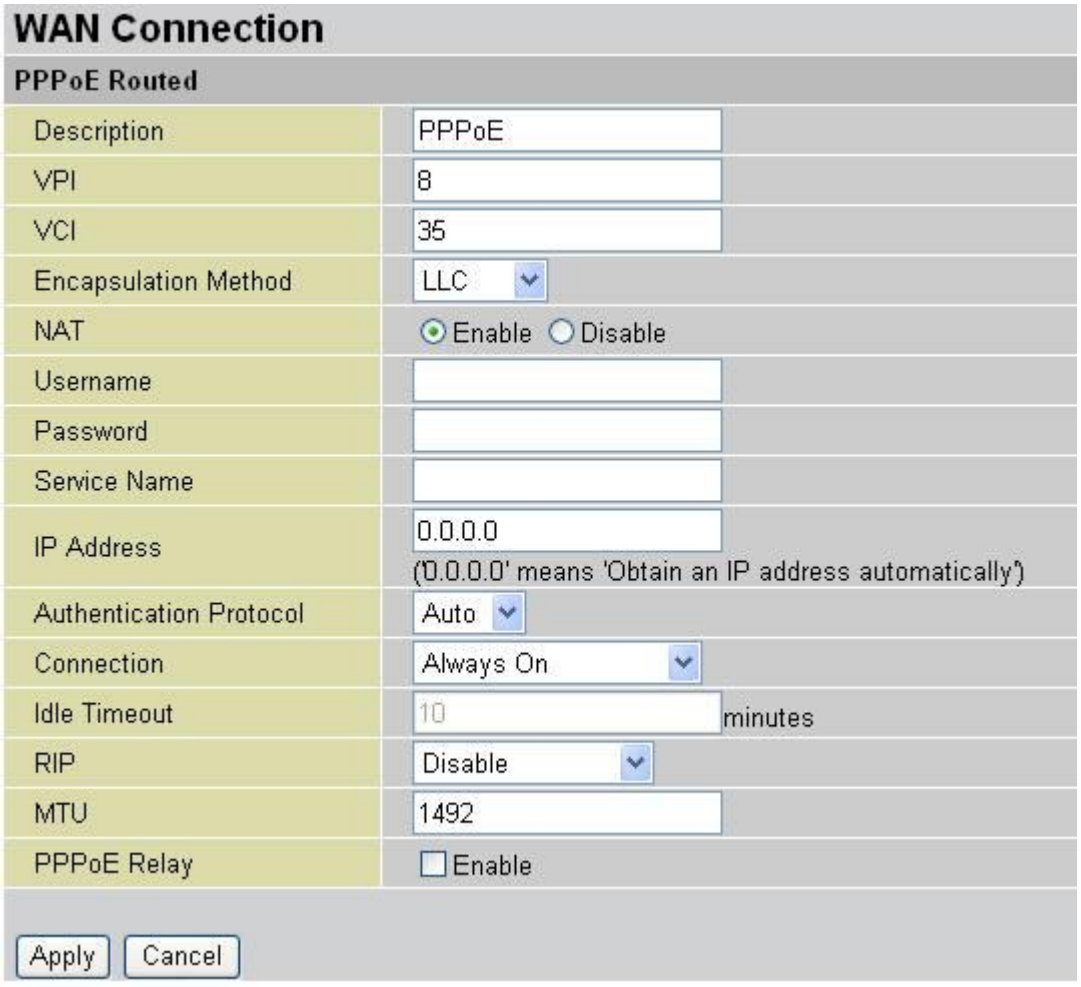
Authentication Protocol: Default is Auto. Your ISP advises you whether to use Chap or Pap.

Connection: PPPoA session shows always on

RIP: Disable, RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that the IP attempts to send through the interface.
Apply: Click to save settings
Cancel: Click to discard changes

PPPoE Routed Connections

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



Description: A user-definable name for this connection.
VPI/VCI: Enter the information provided by your ISP.
Encapsulation method: Select the encapsulation format, VcMux or LLC. Select the one provided by your ISP.
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.

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 20 alphanumeric characters.

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 advises on using Chap or Pap.

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: 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).

Idle Timeout: Auto-disconnect the gateway when there is no activity on the line for a predetermined period of time.

RIP: Disable, RIP v1, RIP v2, RIP v1+v2 and RIP v2 Multicast.

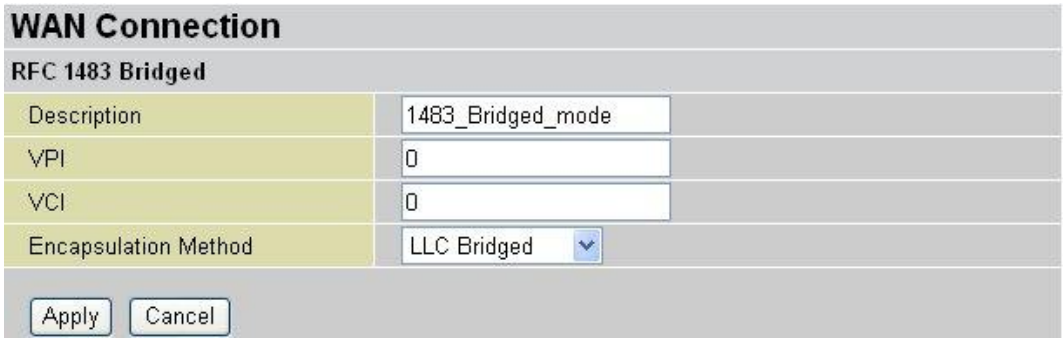
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

PPPoE Relay: Select PPPoE Relay check box to Enable it, if required.

Apply: Click to save settings

Cancel: Click to discard changes

RFC 1483 Bridged Connections

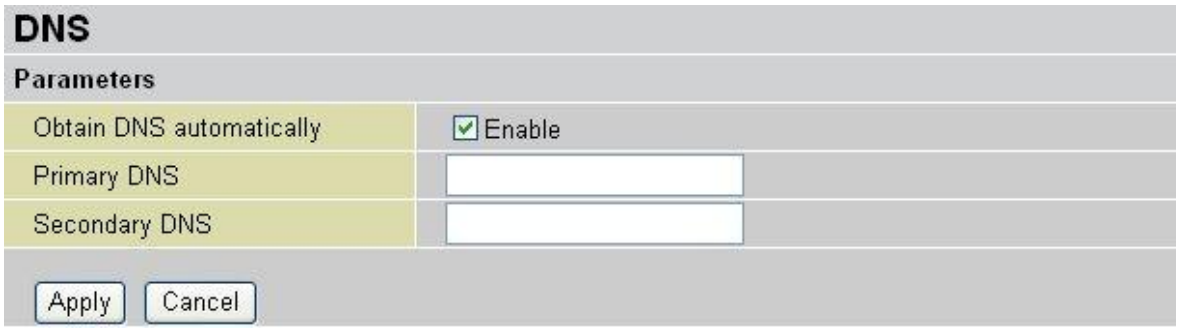


Description: A user-definable name for this connection.

VPI/VCI: Enter the information provided by your ISP.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

DNS

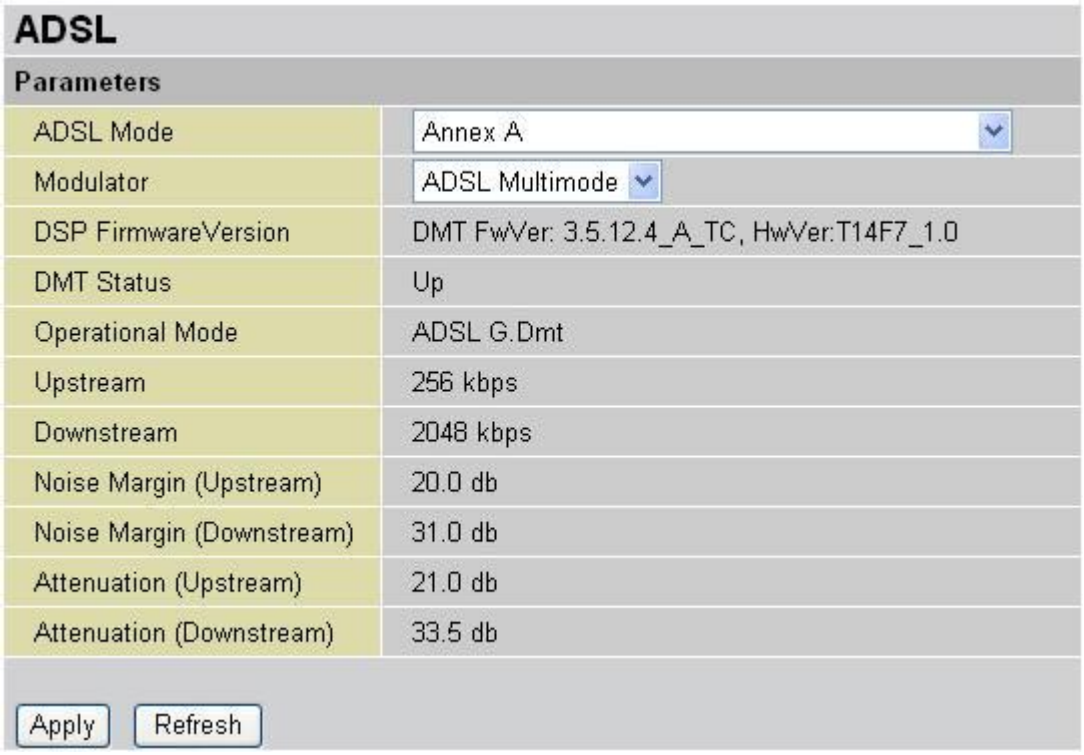


A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.Level1.com and an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 192.168.1.254. You can think of an IP address as a telephone number for devices on the Internet, and the DNS allows you to find the telephone number for any particular domain name. Since an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP provides the DNS IP address automatically. You may leave the configuration field blank. Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the Primary DNS IP address, or enter Secondary DNS IP address for additional list.

If you choose one of the other protocols, RFC1483 Routed or Bridged, check with your ISP, as it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS Server address on your PC to the LAN IP address of this router.

ADSL



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 few modes **AUTO**, **ADSL multimode**, **ADSL2**, **ADSL2+**, **G.Lite**, **T1.413** and **G.DMT** that user can select

DSP Firmware Version: DSP code version

DMT Status: DMT Status

Operational Mode: To show the state when user select “AUTO” on connect mode.

Upstream: Upstream rate

Downstream: Downstream rate

Noise Margin (Upstream) / Noise Margin (Downstream)

Shows noise ratio, a measurement performed in the frequency domain.

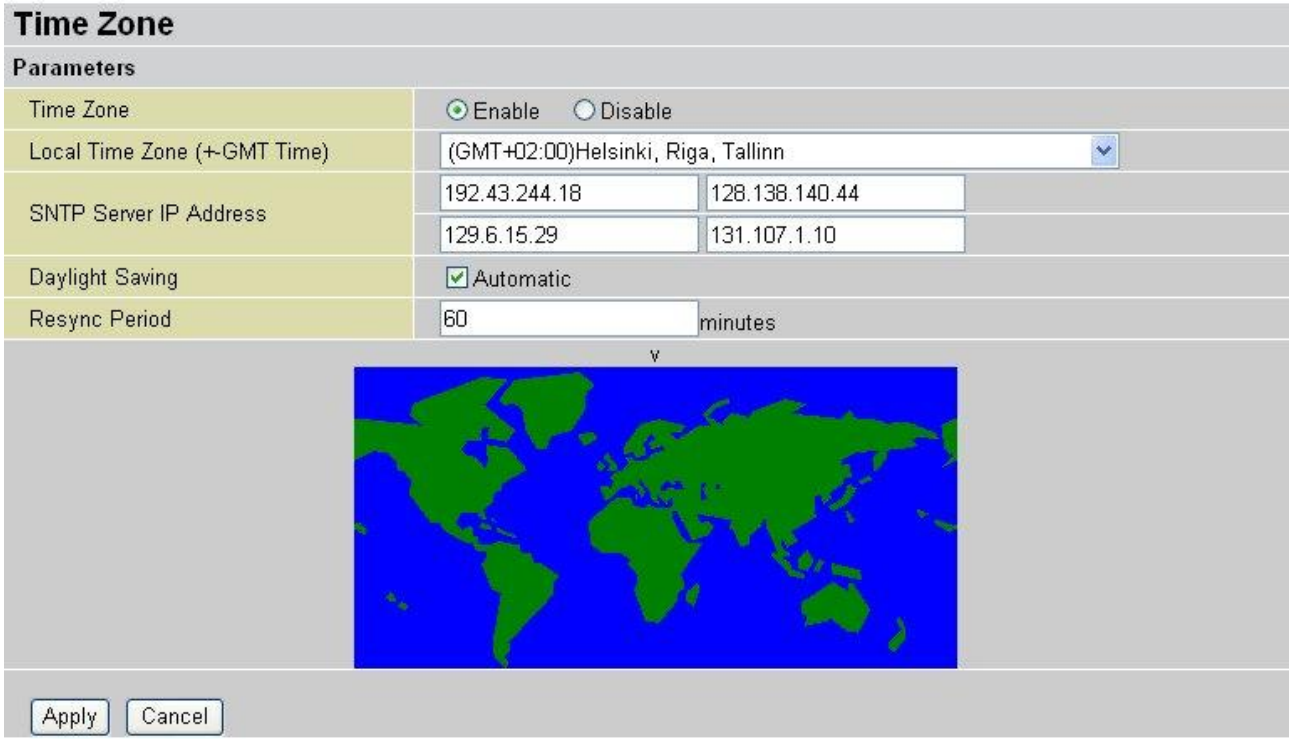
Attenuation (Upstream) / Attenuation (Downstream)

Attenuation is a measure of the loss of signal strength or light power that occurs as light pulses propagate through a run of multimode or single-mode fiber. Measurements are typically defined in terms of decibels or dB/km. The further you are away from the exchange the higher your attenuation figure will be as the signal loss increases.

3.3.3. System

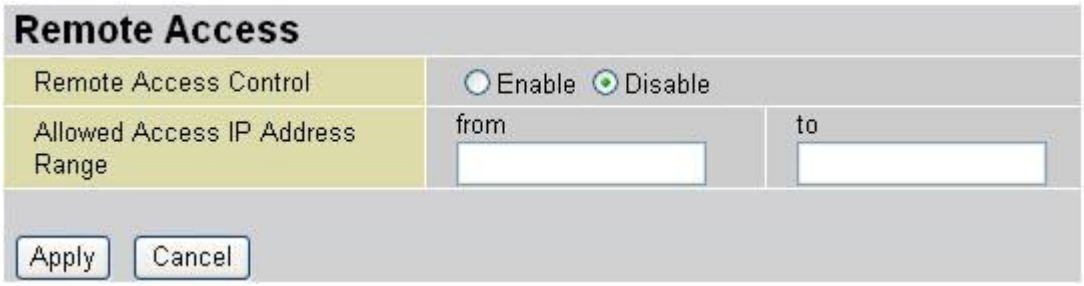
There are six items within the System section: Time Zone, Remote Access, Firmware Upgrade, Backup/Restore, Restart and User Management.

Time Zone



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 list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use. For the Daylight Saving, select **Automatic** check box to enable daylight saving. **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.

Remote Access

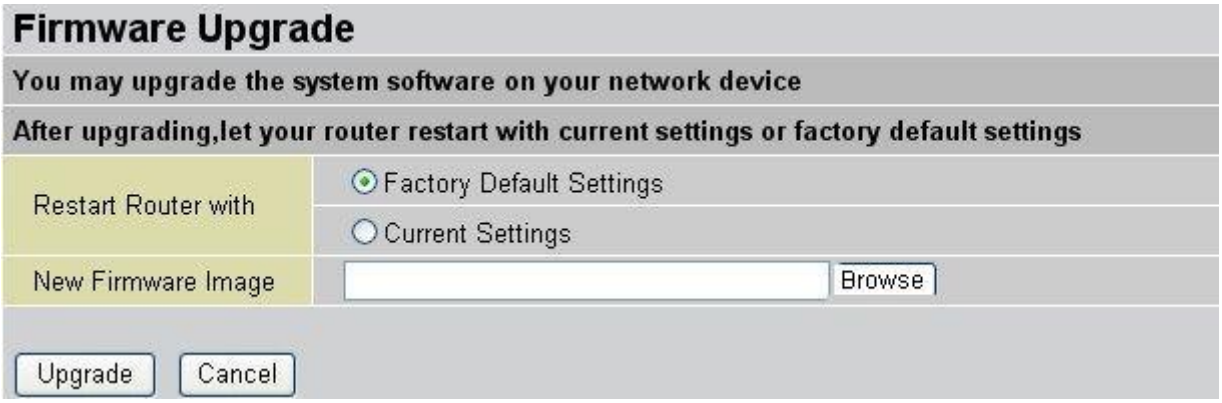


To permit remote administration of the router (i.e. from outside your LAN), click Enable. You may change **Allowed Access IP Address Range** to specify IP address for more secure administration.

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. Your router allows you to upgrade the software it runs to take advantage of these changes.

Click 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.



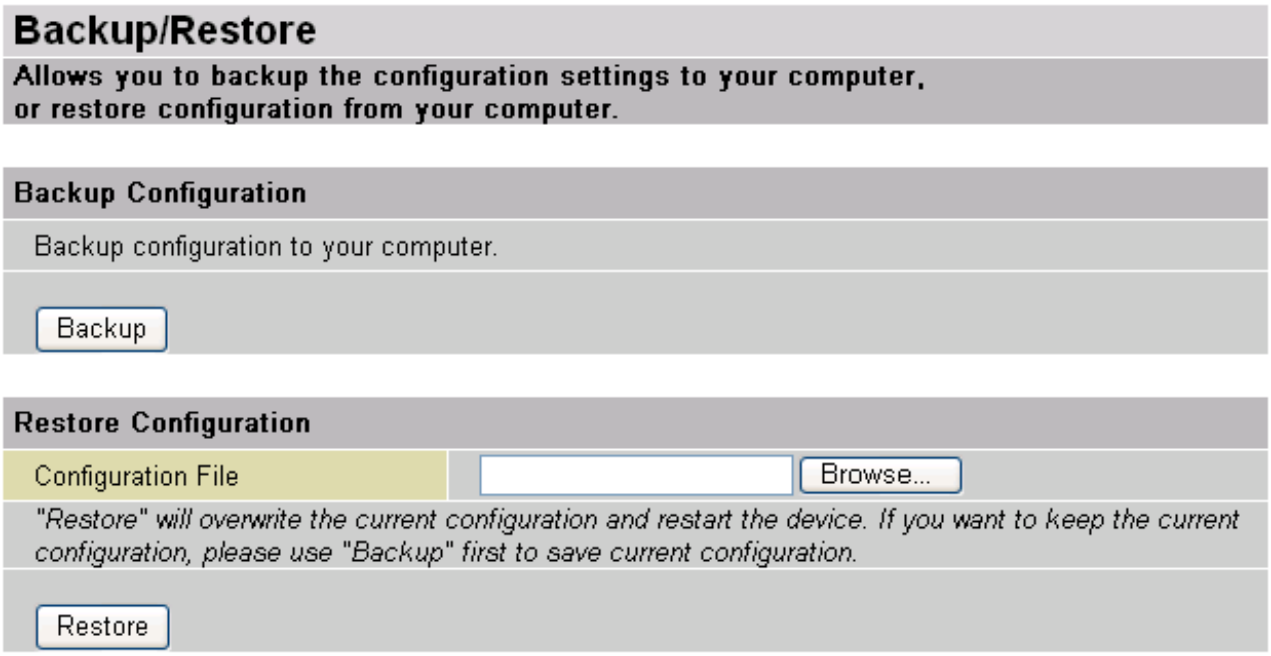
Restart Router with: To choose "Factory Default Setting" or "Current Settings"

New Firmware Image: Type in the location of the file you wish to upload in this field or click **Browse** to find the .afw file you wish to upload. Remember that you must decompress compressed (.zip) files before you can upload them.

Upgrade: Click upgrade to begin the upload process. This process may take up to two minutes.

Cancel: Discard your changes.

Backup / 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.

Backup Configuration

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

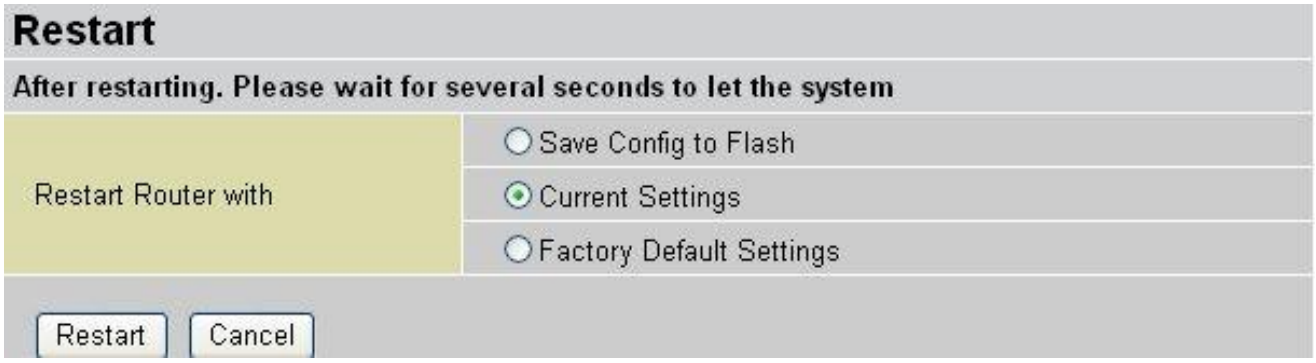
Restore Configuration

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.

Restart

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



Save Config 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.

Current Settings

Select option Current Settings to reboot your router (and restore your last saved configuration).

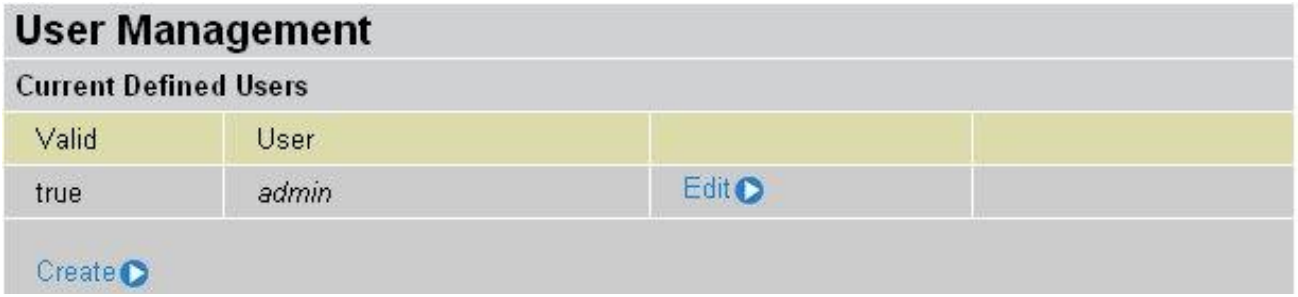
Factory Default Settings

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.

You may also reset your router to factory settings by holding in the small Reset pinhole button on the back of your router for 10-12 seconds while the router is turned on.

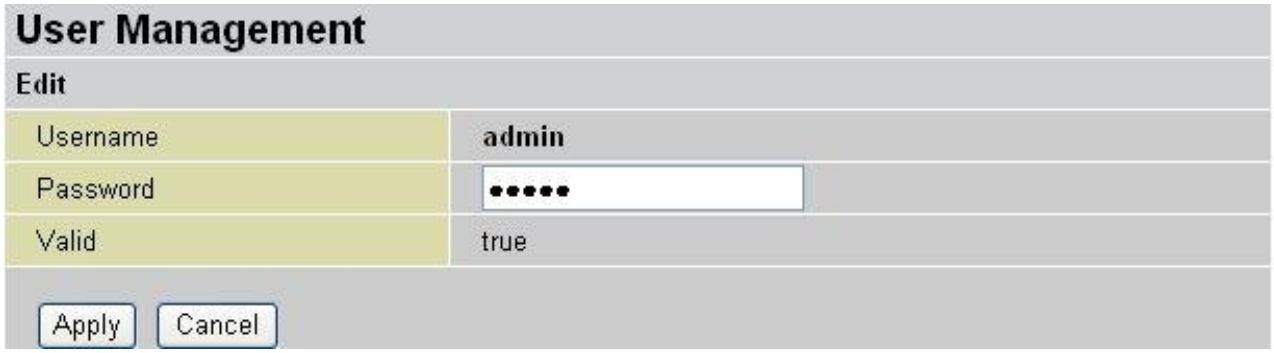
Restart: Click this button to restart router.

User Management



To prevent unauthorized access to your router's configuration interface, all users are required 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 **Create** new users who are able to access the device's configuration interface. Once you have clicked on **Edit** of user listed, you are shown the following options:



You can change the user's password, whether their account is active and Valid, as well as add a comment to each user account. 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 **Cancel** when editing the user. **Apply**: Click to save settings

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.

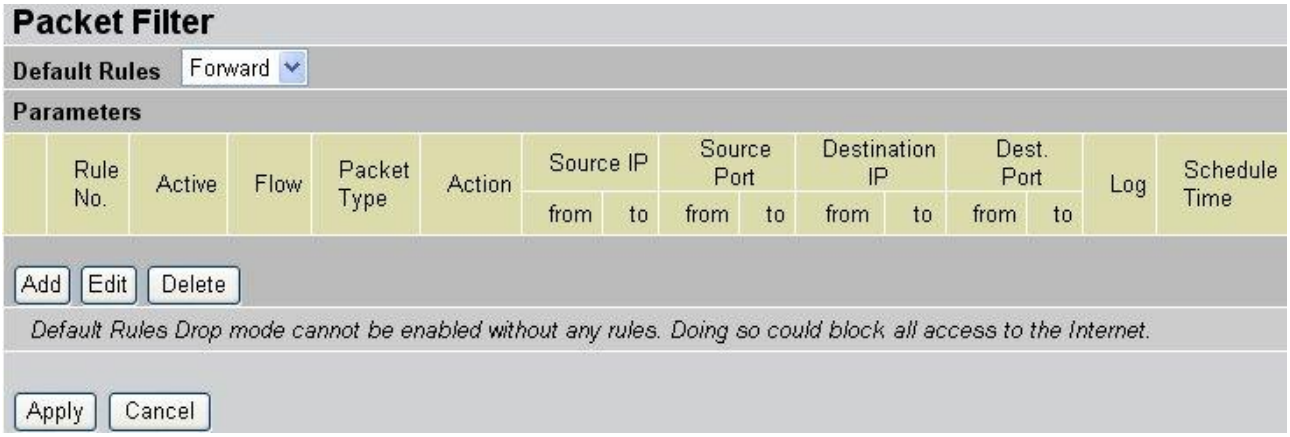
3.3.4. Firewall

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.

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

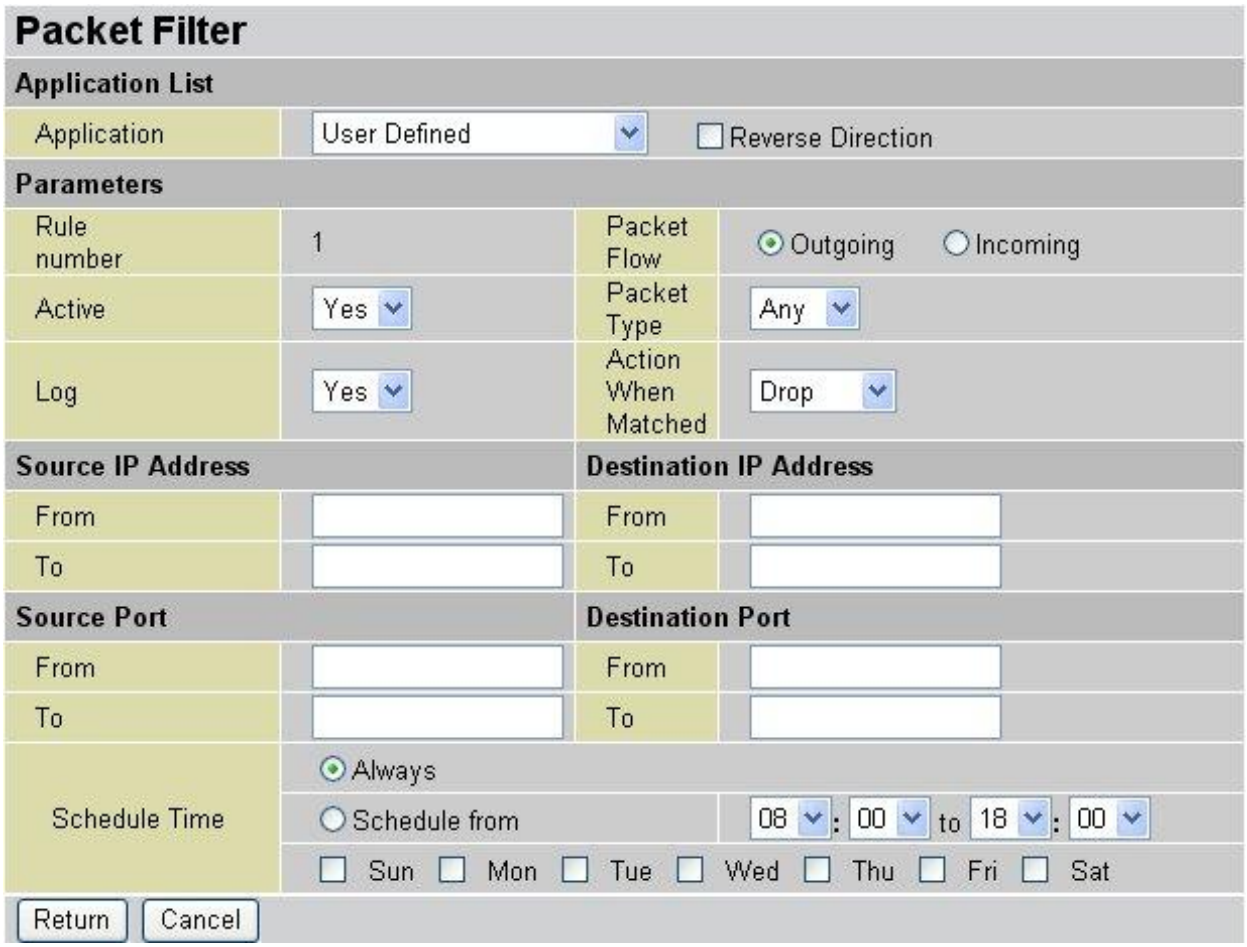
Packet Filter

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 is taken.



Add: Click this button to add a new packet filter rule and the next figure appears.
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”.

Apply: Click to save settings
Cancel: Click to discard changes



Application: User can choose **User Defined** and enter all information related to create your packet filter list, or just choose preset items from drop-down list. Click **Reverse Direction** check box to reverse flow direction

Rule number: Rule index
Packet Flow: Select **Outgoing** or **Incoming** Determine whether the rule is for outgoing packets or for incoming packets.
Active: Choose “Yes” to enable the rule, or choose “No” to disable the rule.
Packet Type: Specify the packet type (TCP, UDP, ICMP or any) 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.
Log: Choose “Yes” if you wish to generate logs when the filer rule is applied to a packet.
Action When Matched: If a packet matches this filter rule, Forward or Drop this packet.

Source IP Address: Enter the incoming or outgoing packet’s source IP address(es).
Source Port: Check the TCP or UDP packet’s source port number(s).

Destination IP Address: Enter the incoming or outgoing packet's destination IP address(es).
Destination Port: Check the TCP or UDP packet's destination port number(s).

Schedule time: User can setup the time to use the packet filter. Select either **Always** or **Schedule from**. For the Schedule from, user can set time range and week day.

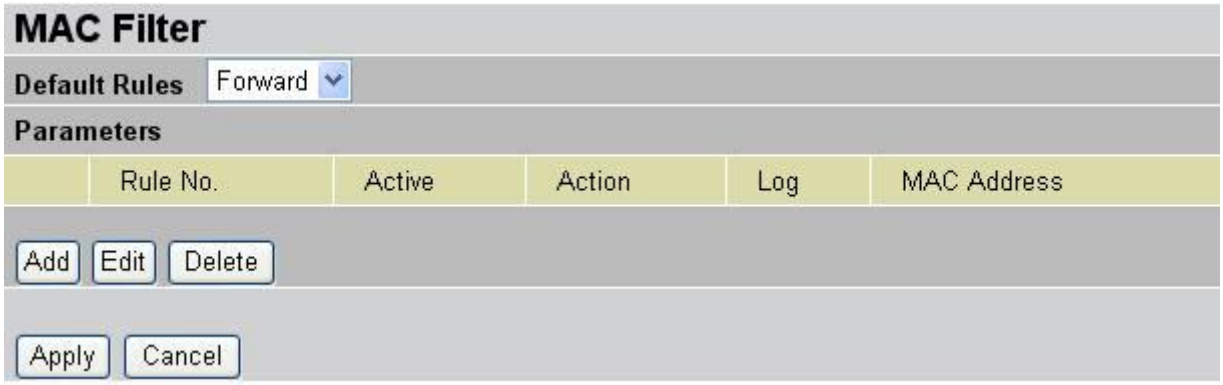
Return: Click to finish settings
Cancel: Click to discard changes

Note:

- For the IP address range, leave it blank or enter 0.0.0.0 to filter all IP addresses
- 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.

MAC Filter

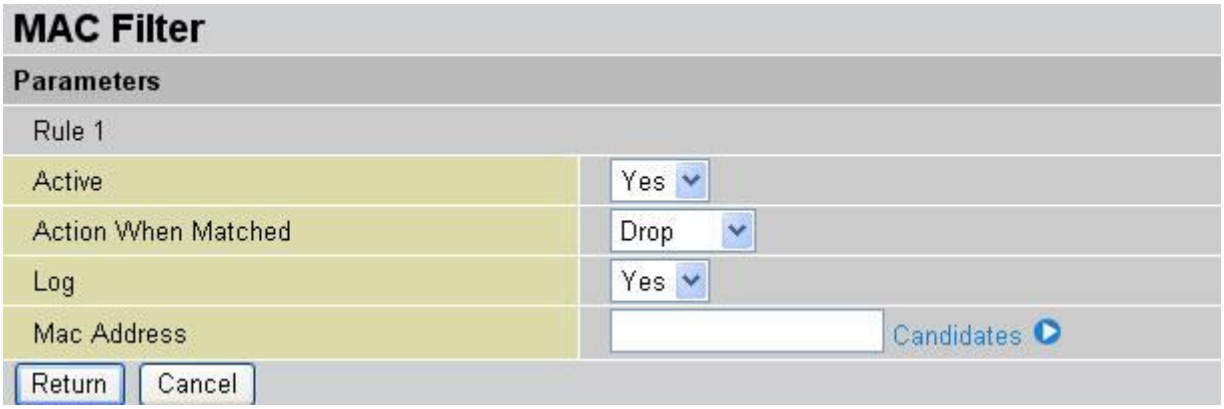
A Ethernet MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the switch to only accept traffic from specified machines, or else 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.



Click **Add** to add new MAC filter list.

Select Rule No. and click **Edit** to change settings

Select Rule No. and click **Delete** to delete it



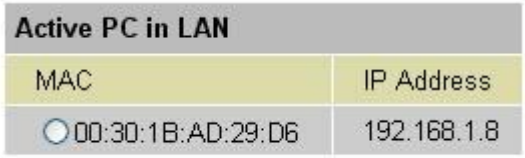
Active: Select Yes from the drop down list box to enable MAC address filtering.

Action When Matched: Select "Drop" or "Forward".

Log: Choose "Yes" if you wish to generate logs when the filer rule is applied to a packet.

MAC Address: Enter the MAC addresses you wish to manage.

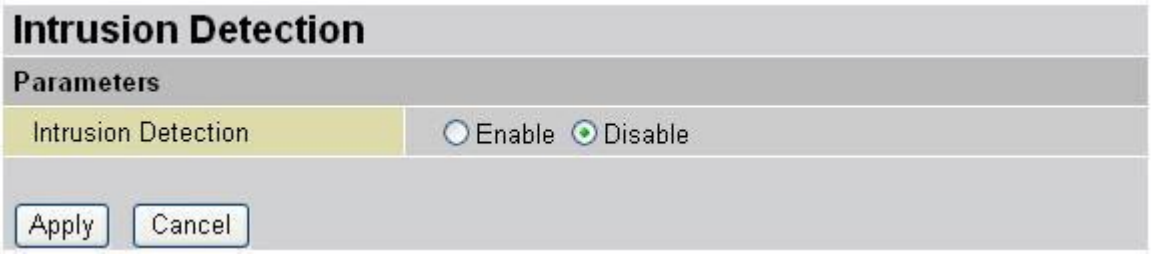
Candidates: It automatically detects devices connected to the router through the Ethernet. Click check box to add MAC Address automatically.



Return: Click to finish settings
Cancel: Click to discard changes

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 are not able to access network resources.



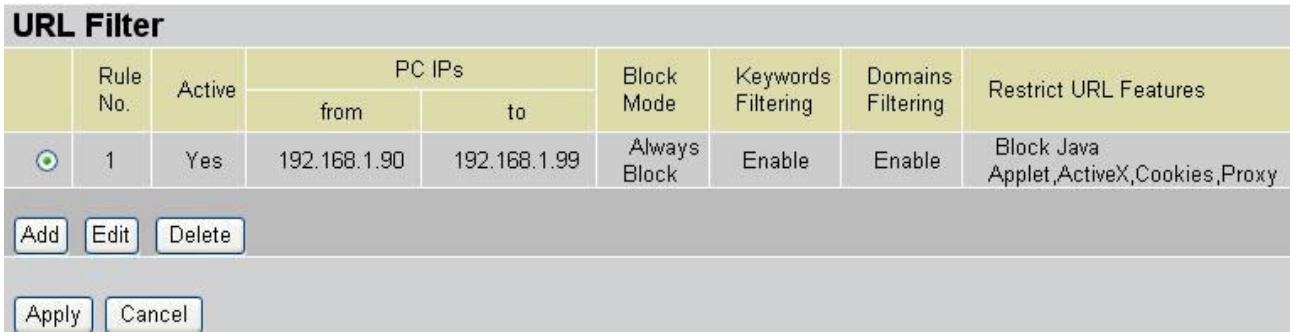
Intrusion Detection: Check “Enable” if you wish to detect intruders accessing your computer without permission. After enable this function, user needs to specify the e-mail account / SMTP server and notice message will send.

Block WAN Request

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

URL Filter

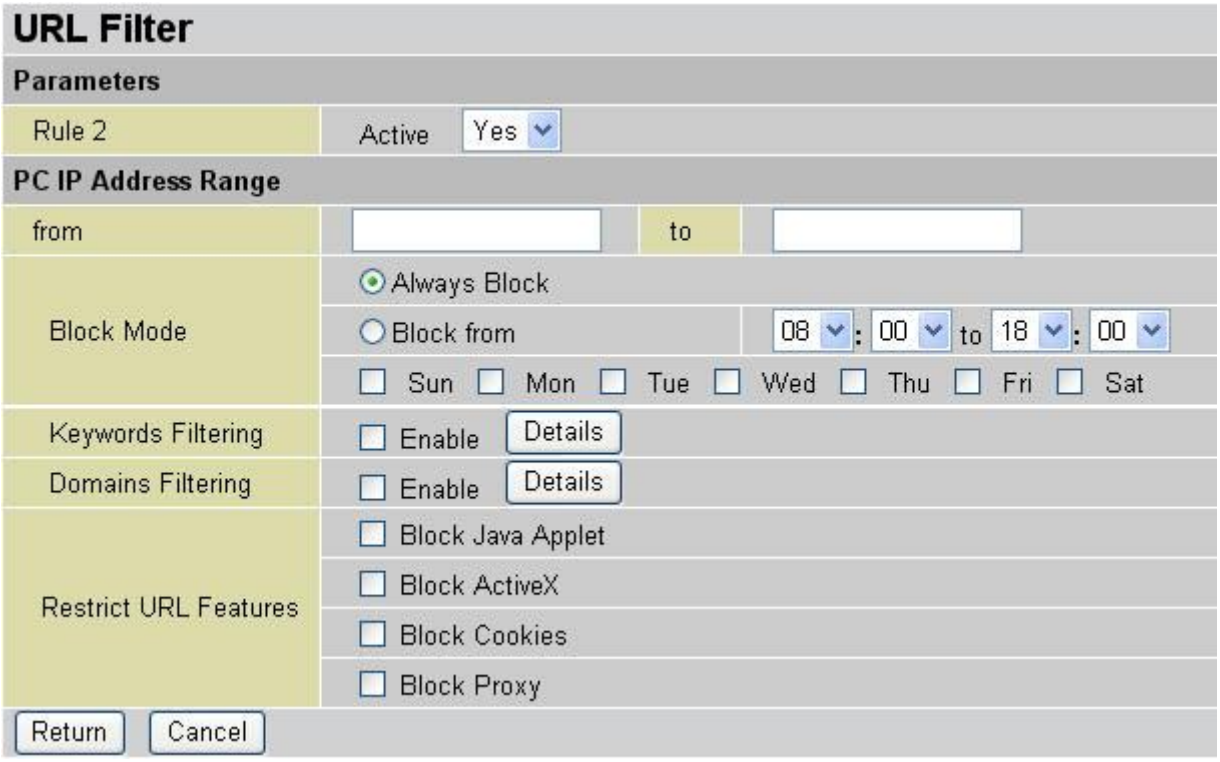
URL (Uniform Resource Locator – e.g. an address in the form of http://www.Level1.com or http://www.example.com) filter rules allow you to prevent users on your network from accessing particular websites from their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Click **Add** to add new MAC filter list.

Select Rule No. and click **Edit** to change settings

Select Rule No. and click **Delete** to delete it



Active: Select Yes from the drop down list box to enable or disable the URL Filter feature.

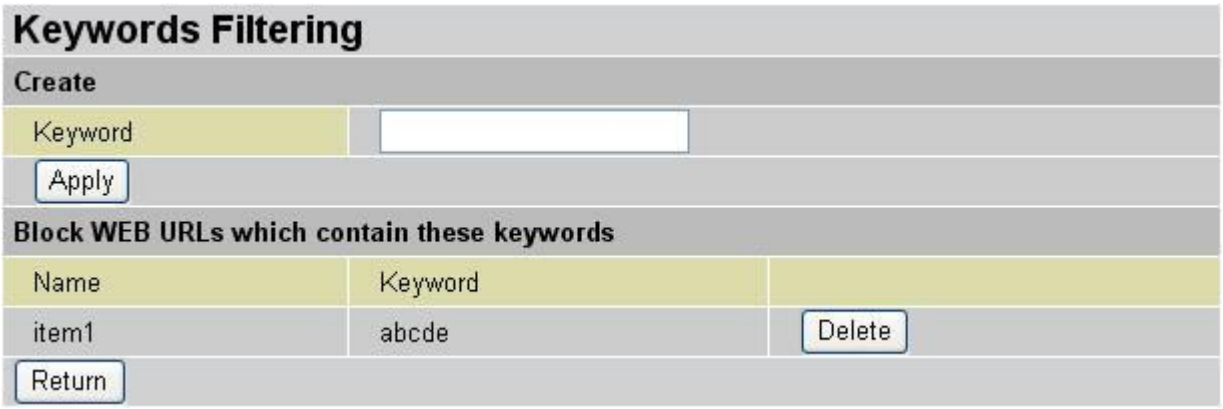
PC IP Address Range: Specify IP range

Block Mode

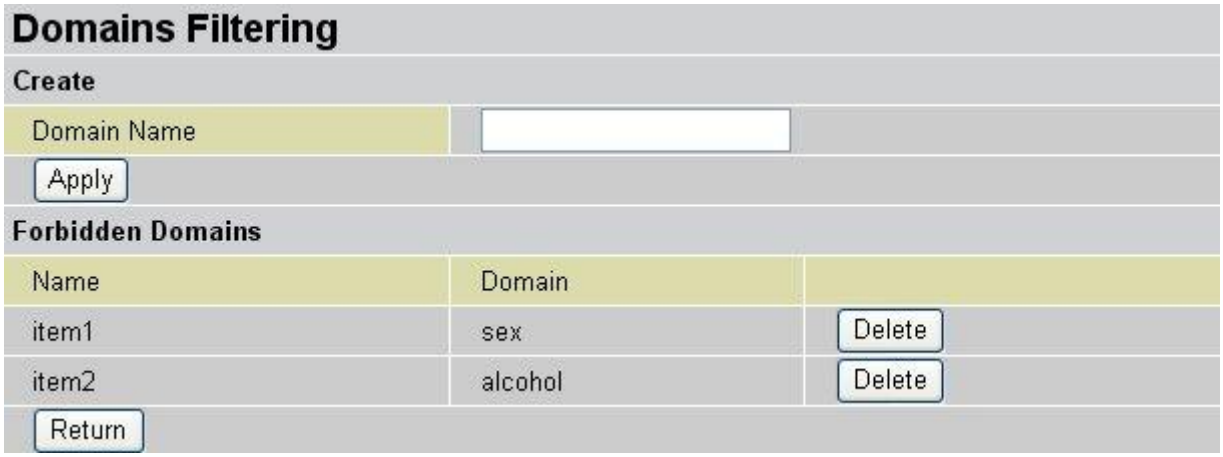
Always Block: Select to always check URL filter rules (i.e. at all hours of the day).

Block from: Specify the time period to check URL filter rules (e.g. during work hours).

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.



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:
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.
If not, it is checked with the forbidden list. If present, the connection attempt is dropped.
If the packet matches neither of the above, it is sent to the remote web server.
Please note that only the domain is specified, not the full URL. For example to block traffic to www.sex.com, enter “sex” or “sex.com” instead of “www.sex.com”. In the example below, the URL request for www.abc.com is sent to the remote web server because it is listed in the trusted list, while the URL request for www.sex or www.sex.com is dropped because sex.com is in the forbidden list.



Restrict URL Features

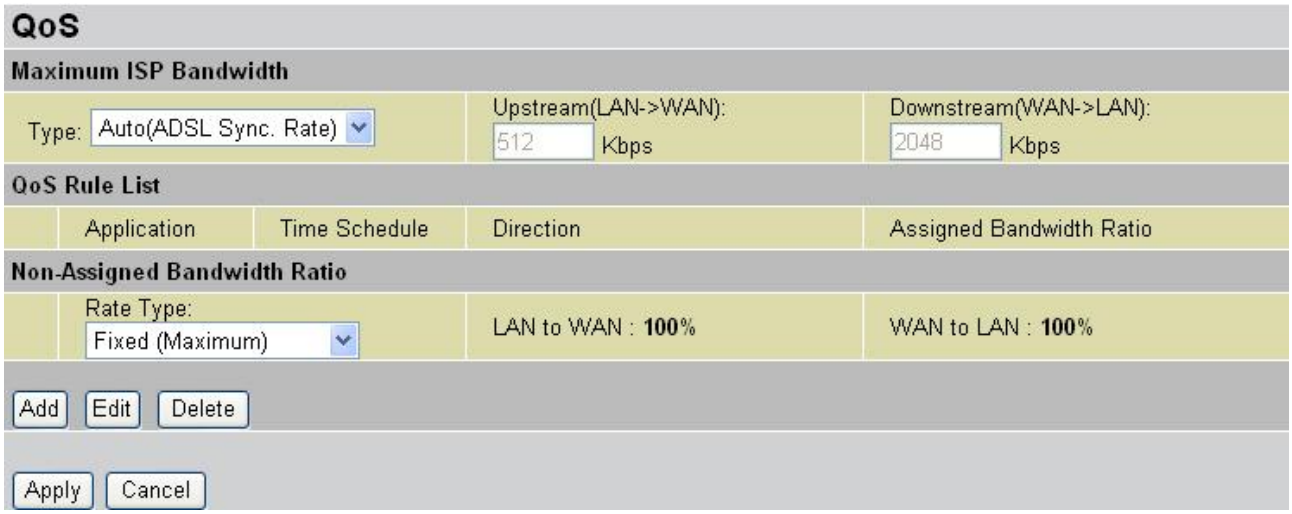
- Block Java Applet: Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.
- Block ActiveX: Blocks ActiveX
- Block Cookies: Blocks Cookies
- Block Proxy: Blocks Proxy

3.3.5. QoS (Quality of Service)

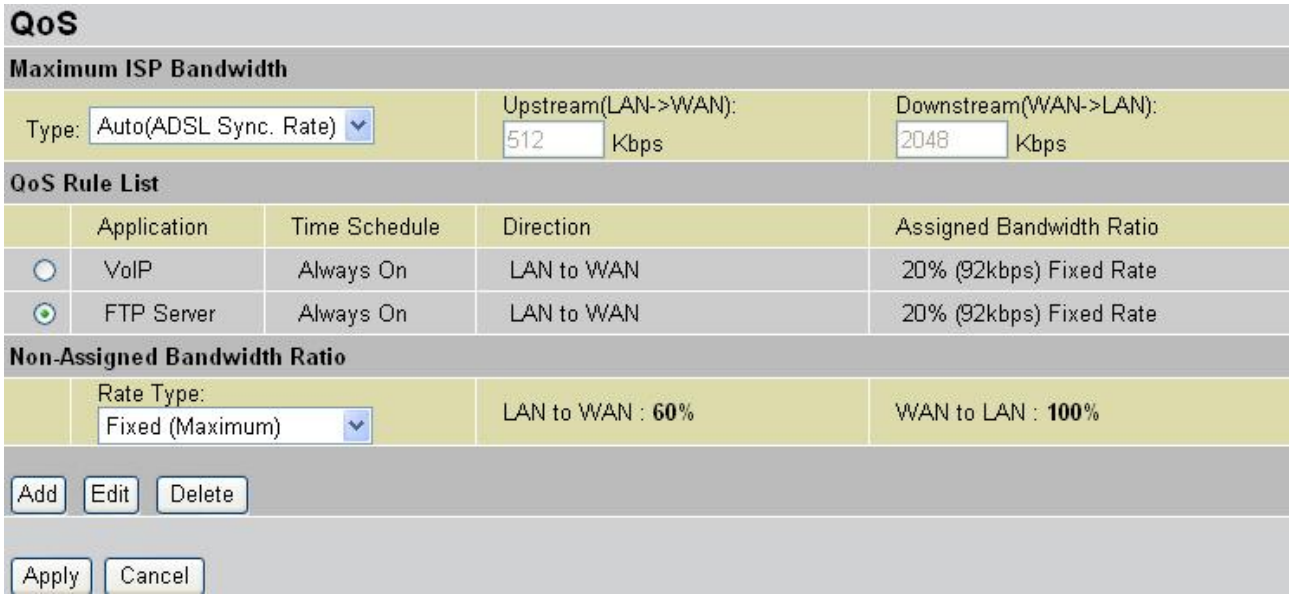
Quality of Service Introduction
If you've ever found your 'net' speed has slowed to a crawl because another family member is using a P2P file sharing program, you'll understand why the Quality of Service features in LevelOne's routers is such a breakthrough for home users and office users.

Configurable by source IP address, destination 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.



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.



Maximum ISP Bandwidth

It shows connection Upstream and Downstream rate.Auto type shows your DSL connection speed automatically, or select **Manual Input** to set Upstream and Downstream manually.

QoS Rule List

Application: A name that identifies an existing policy.

Time Schedule: Scheduling your QOS policy to be applied.

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.
- LAN to WAN: Control Traffic flow from the WAN to LAN. The connection maybe either issued from LAN to WAN or WAN to LAN.)

Assigned Bandwidth Ratio: This field shows the assigned bandwidth ratio in percentage for a QOS policy. If WAN connection to internet is established, the estimated transfer rate will be shown in kbps. You may specify a fixed transfer rate or Minimum Guaranteed Rate with priority for non-used bandwidth.

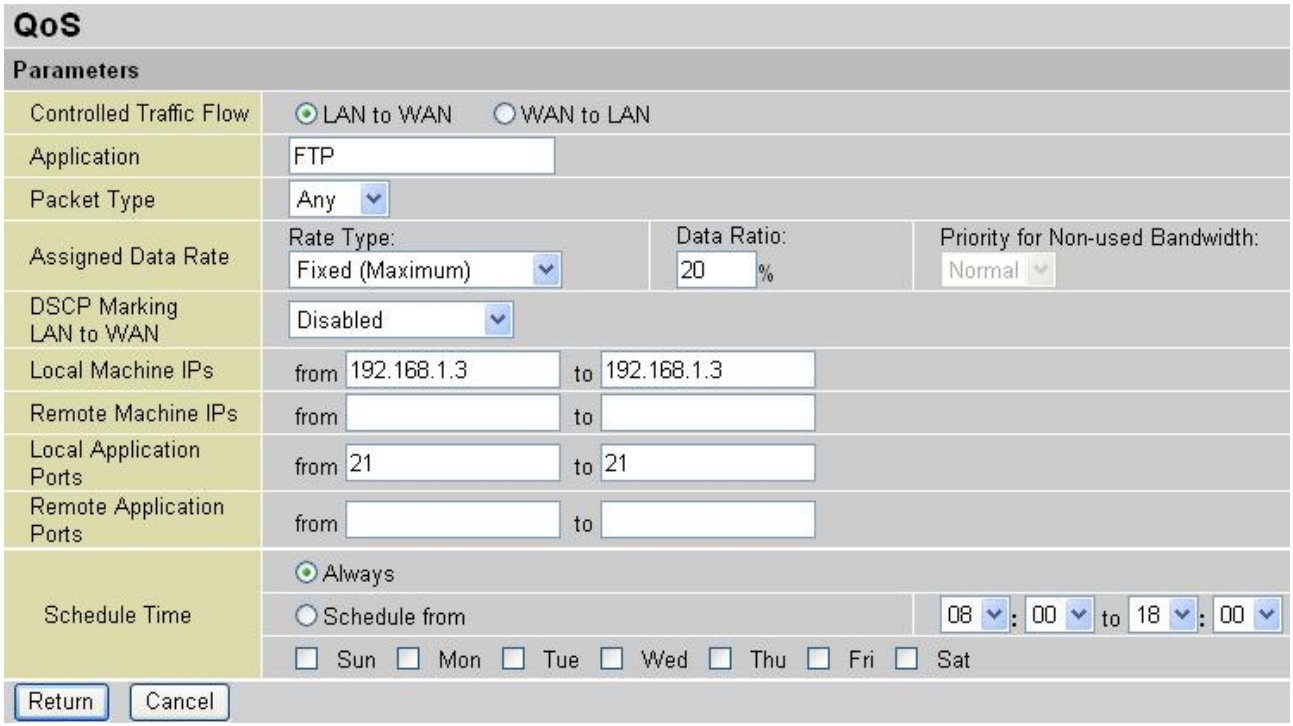
Non-Assigned Bandwidth Ratio: This field shows the available bandwidth ratio, for LAN to WAN and WAN to LAN, that has not yet assigned. Select Fixed or Guaranteed rate type depends on your requirement.

Add : Press this button to add a new QOS policy.

Edit Delete: Before using these buttons to edit or delete a policy, please select one policy you want to edit/delete from the radio option VoIP.

Apply:: After you have configured the policies, you can press this button to apply the configuration. If you want to make the change persistent in flash, choose **Save Config to Flash**: in the left windows to save it into flash.

When you press **Add** or **Edit** buttons described above, the following page will show up in your browser. You can use it to define a QOS policy.



Controlled Traffic Flow: Specify the traffic flow you want to control. Select direction whether from **LAN to WAN** or from **WAN To LAN**

Application: Specify application name

Packet type: The packet type 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 specified protocol type is specified.
- TCP
- UDP
- ICMP
- GRE: For PPTP VPN Connections.

Assigned Data rate: 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).

Rate Type:

- Fixed (Maximum): specify a fixed 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.

Data Ratio: percentage for the data rate to be controlled by this policy. As above FTP server examples, it is 20.

Priority for Non-used Bandwidth: You can set this function by **Guaranteed (Minimum)** selected, 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.

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.

DSCP Mapping Table	
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)

Local Machine IPs: 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.)

Remote Machine IPs: 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.)

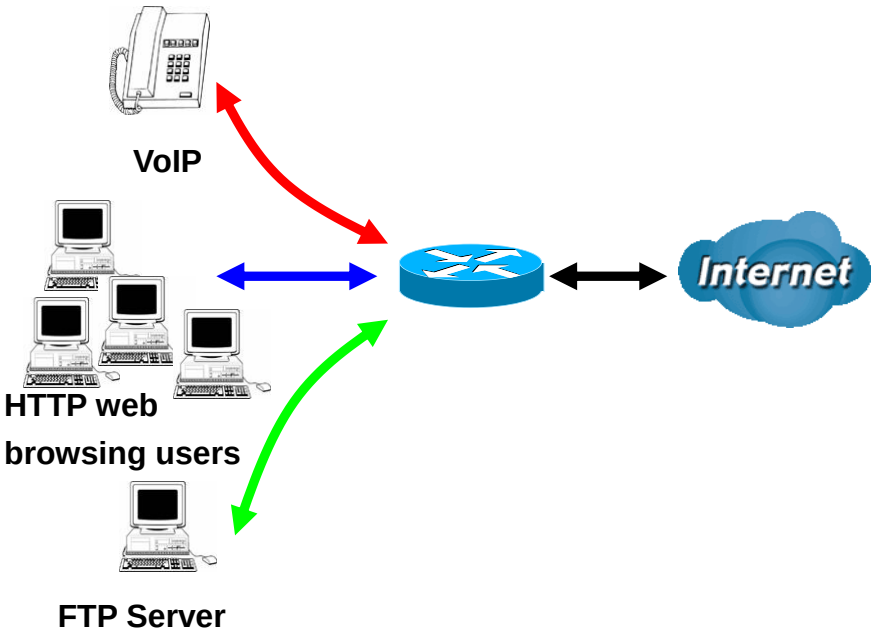
Local Application Ports: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

Remote Application 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.)

Schedule Time: Schedule your QOS policy. You can set this QoS policy always on or it can be set by schedule time, it depends on your usage

QOS Example

Connection Diagram



ADSL Subscription Rate

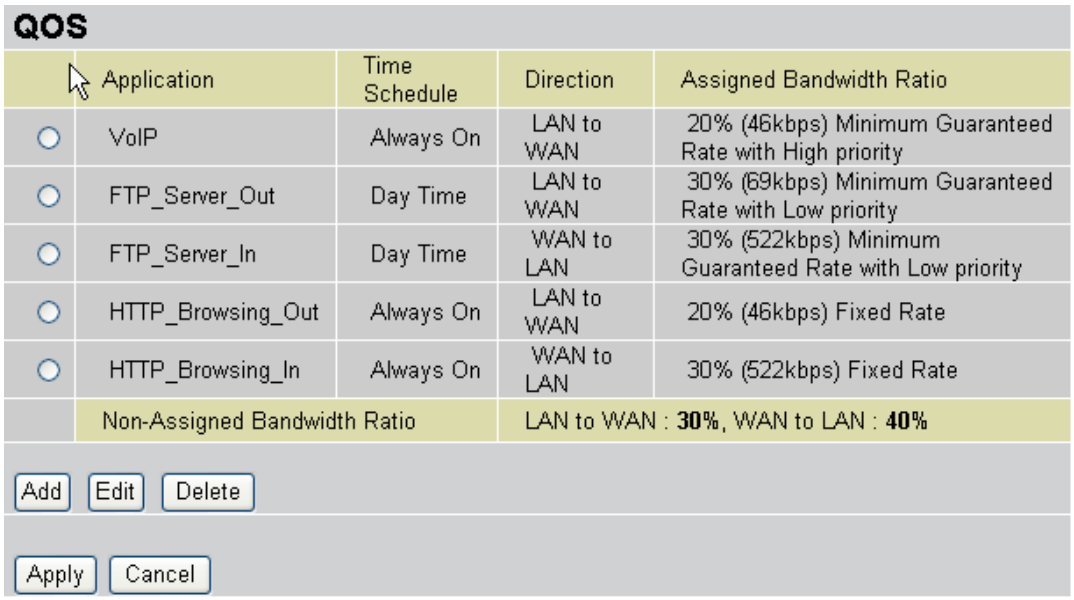
Upstream: 256 kbps

Downstream: 2048 Mbps

Example QOS Plan

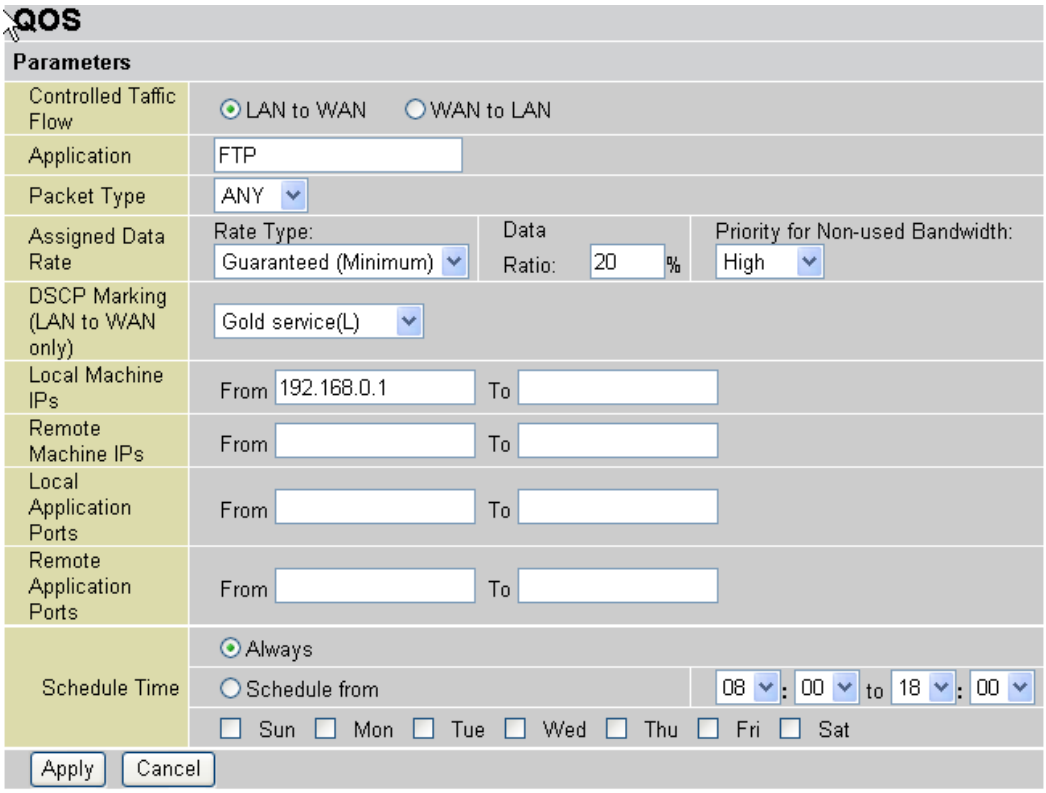
Application	IP or Ports	Control Flow	Data Rate	Time Schedule
VoIP User	192.168.0.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with SDCP marking Class 1 Gold Service	Always
FTP Sever	192.168.0.100	Incoming and Going	outgoing :minimal 30%. Data rate. incoming :minimal 30%. Data rate. 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 Going	outgoing : limited 20%. Data rate. incoming : limited 30%. Data rate.	Always

QOS Example Setup



VoIP application

Voice is latency-sensitive application. Most VoIP devices are use 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.

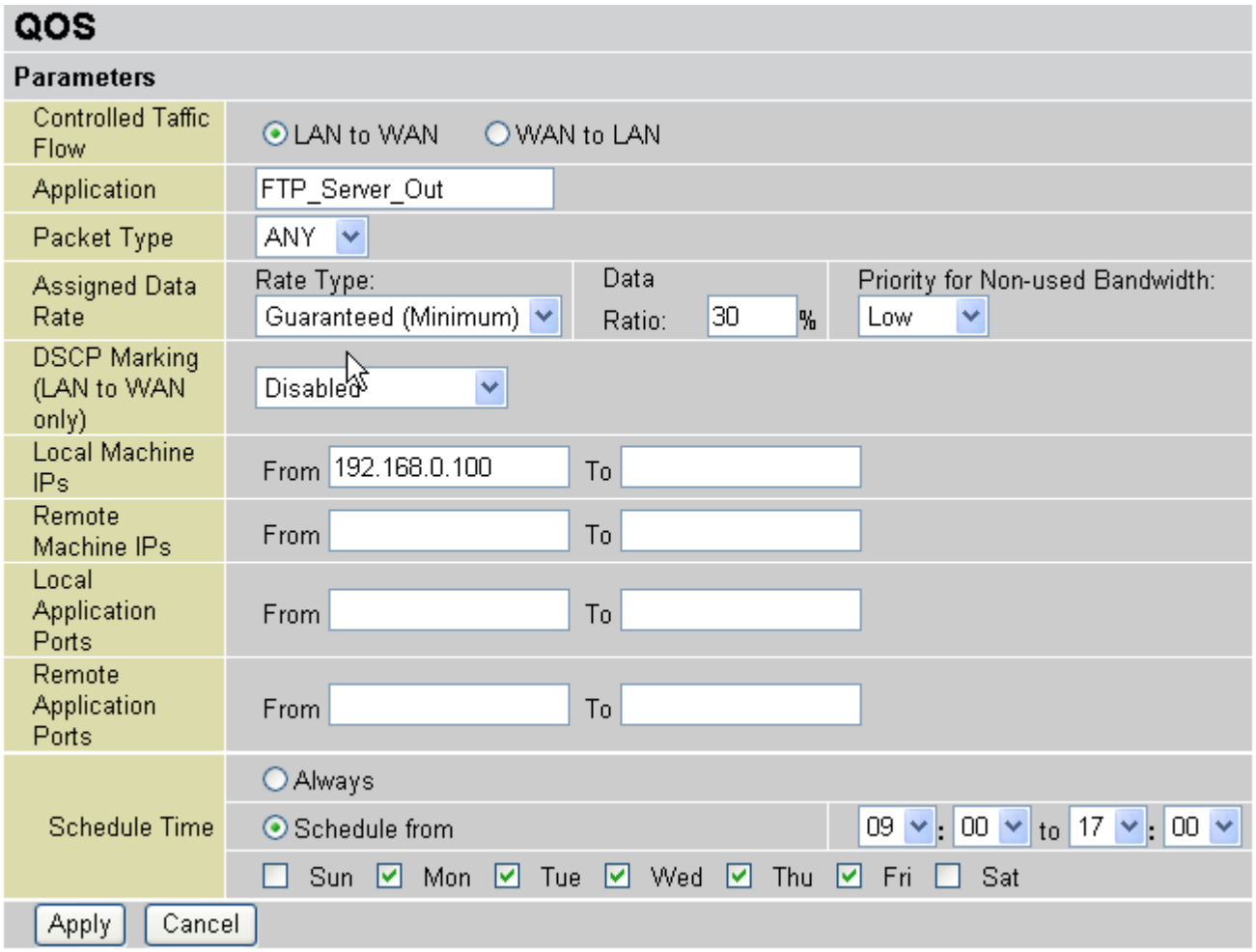


Above settings will help to improve quality of your VoIP service when traffic is full loading.

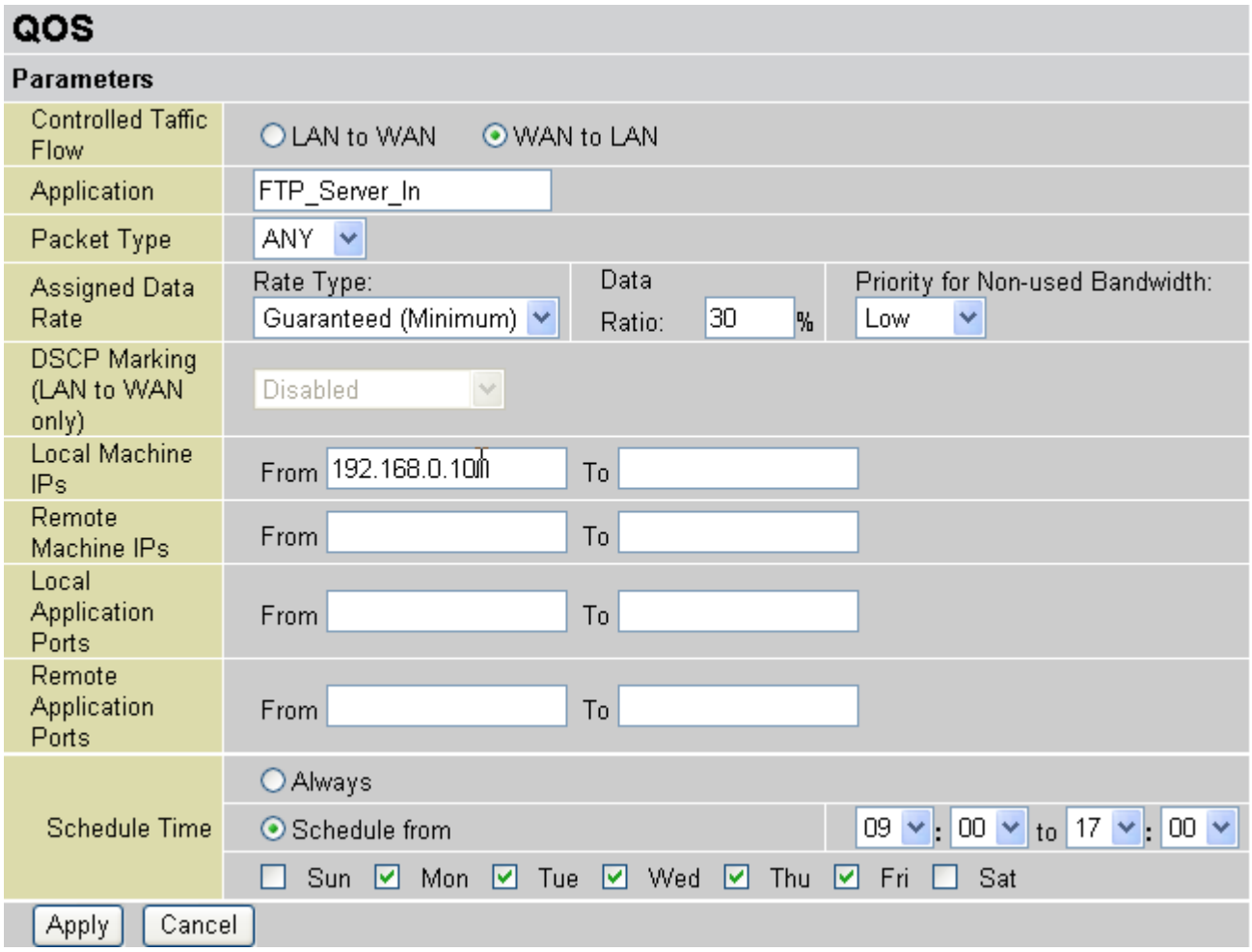
FTP Server Application

Some of companies will setup FTP server for customer downloading or home user sharing their files by using FTP.

LAN to WAN direction:



WAN to LAN direction:

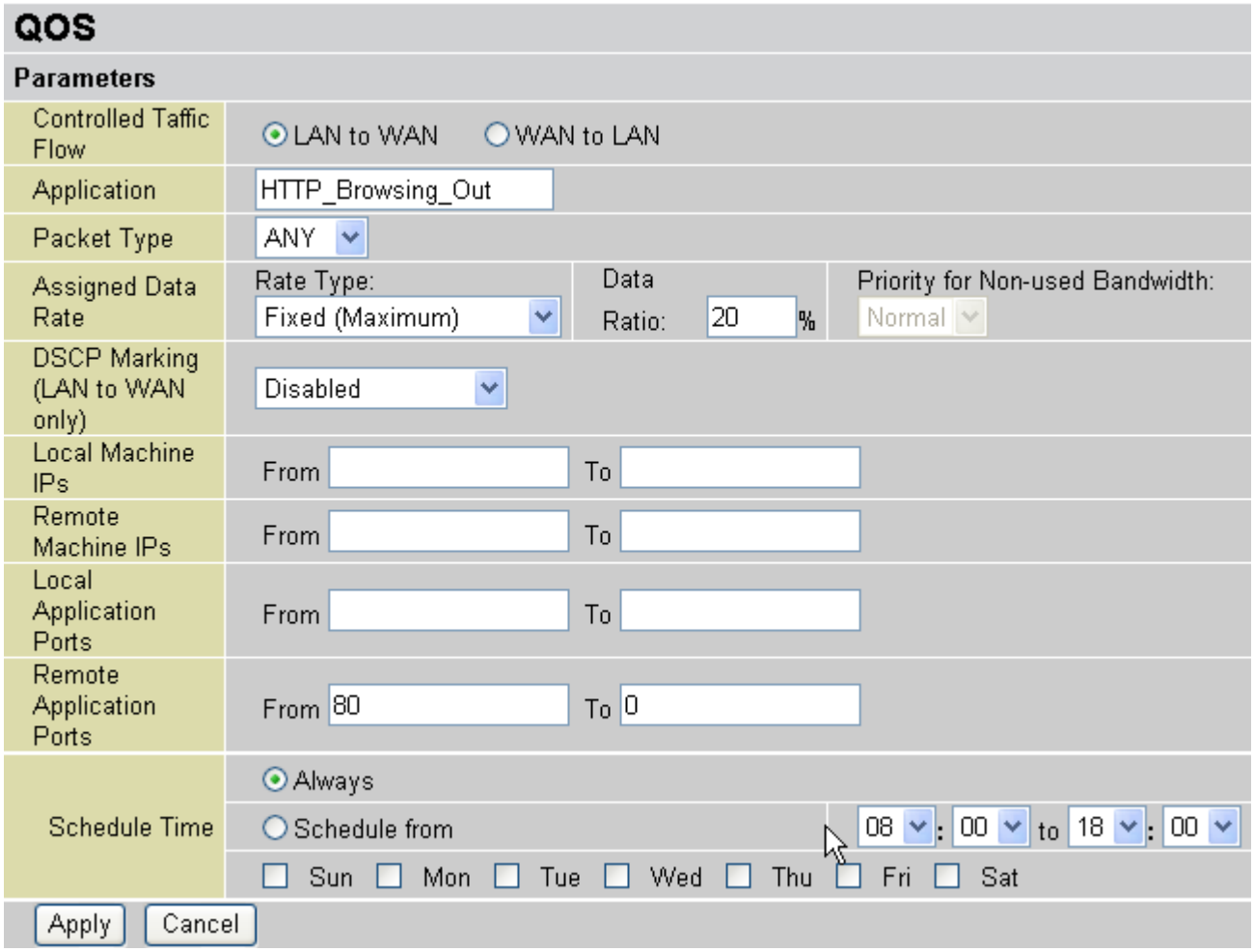


With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at day time.

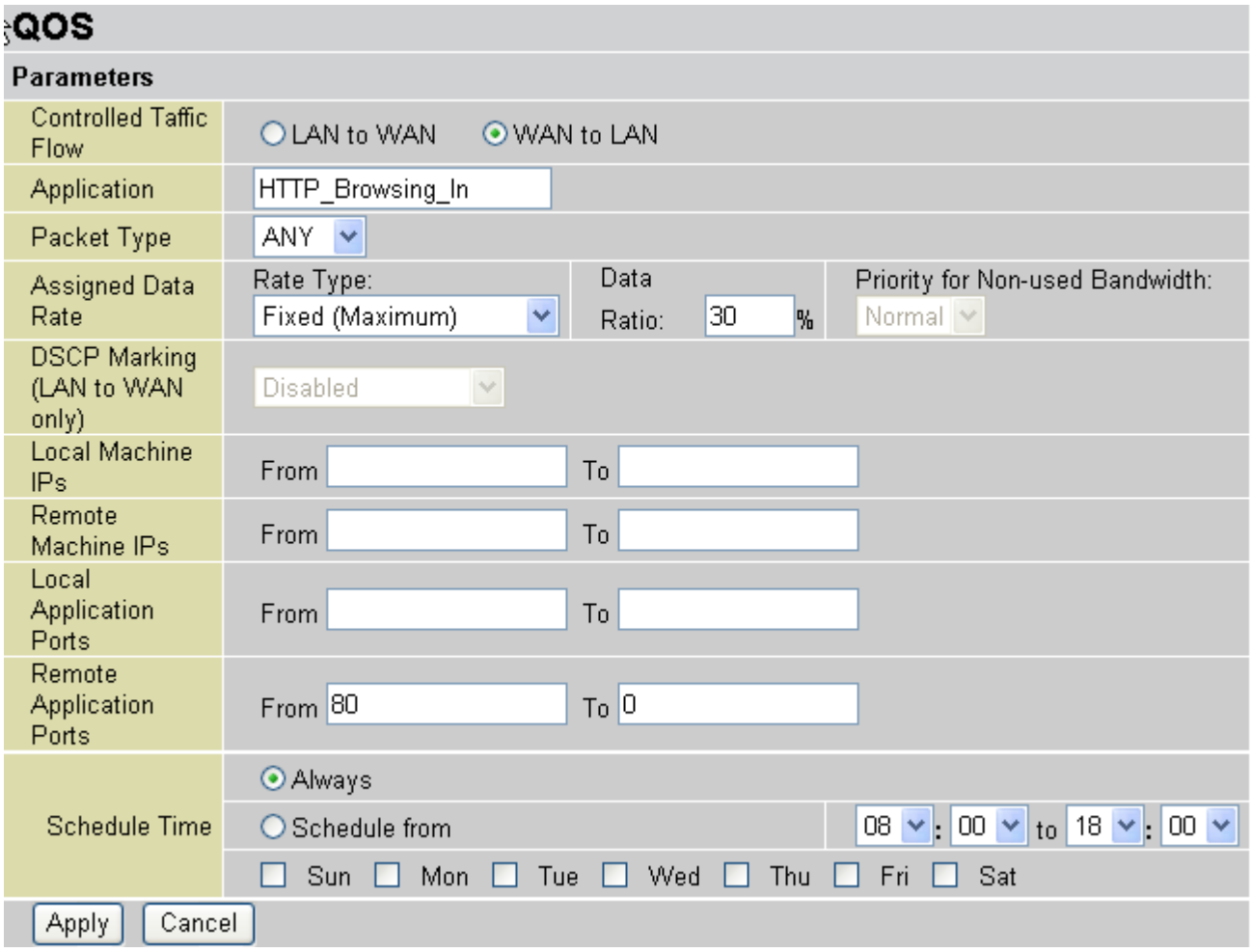
HTTP Web Browsing

You can control the internet web browsing by specify the HTTP 80 (8080 for some proxy server).

LAN to WAN direction:



WAN to LAN direction:



3.3.6. Virtual Server

In TCP/IP 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.

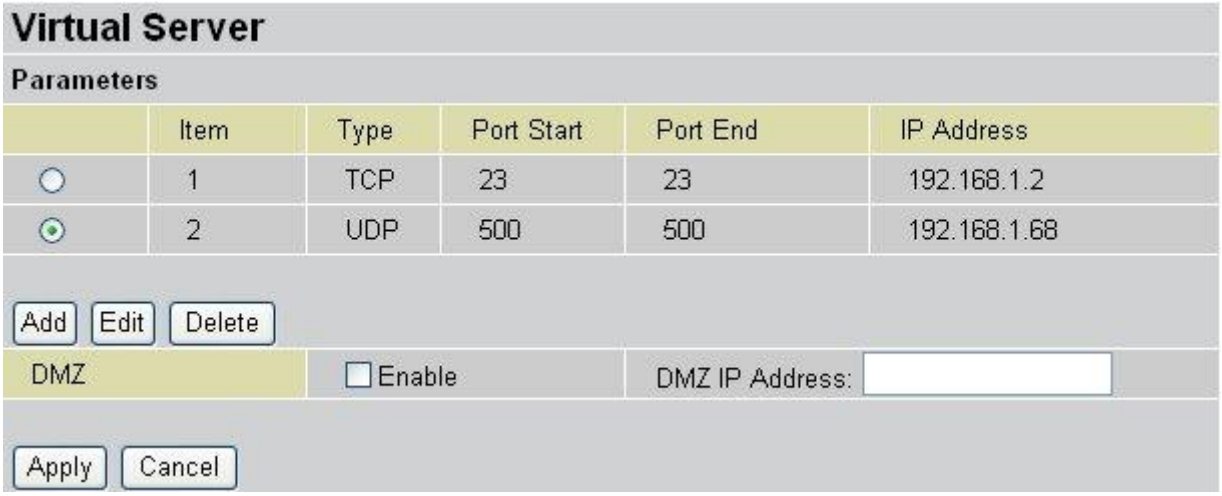
The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports”. The registered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

For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at: http://www.Level1.com

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



Item: Item number

Type: Select TCP if you wish to search for connection-based application services on the remote server using the port number.

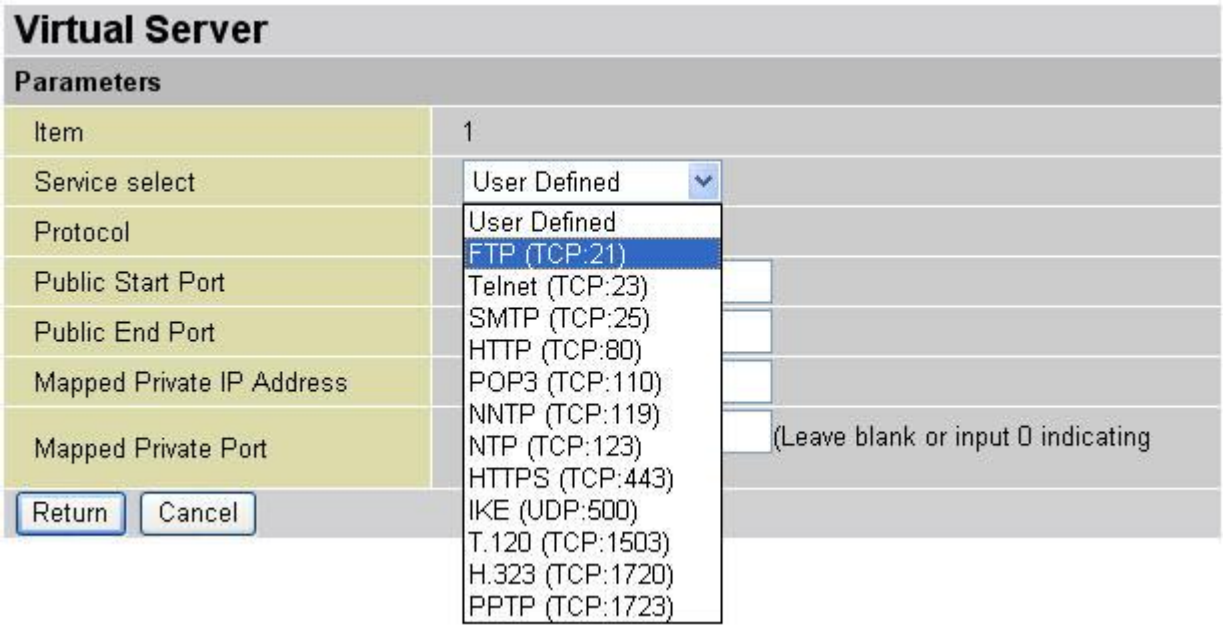
Port Start & Port End: Enter the public port number & range you wish to configure.

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”.

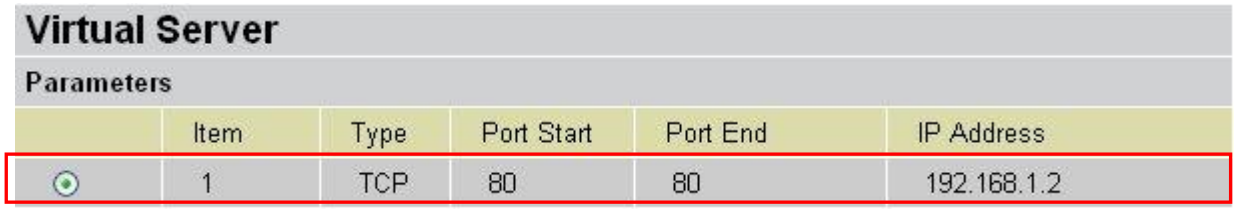
Delete: Check the Rule No. you wish to delete, then click “Delete”.



Item: Item number
Service select: Select the service you wish to configure
Protocol: Automatic when you choose Service select
Start Port & End Port: Enter the public port number & range you wish to configure.
IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Return: Click to finish settings
Cancel: Click to discard changes

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.



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.

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, then passed to the DMZ host when a packet received does not use a port number in use by any other Virtual Server entries.

Note:

Using port forwarding 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.

If you disable the NAT option in the WAN-ISP section, the Virtual Server function becomes invalid.

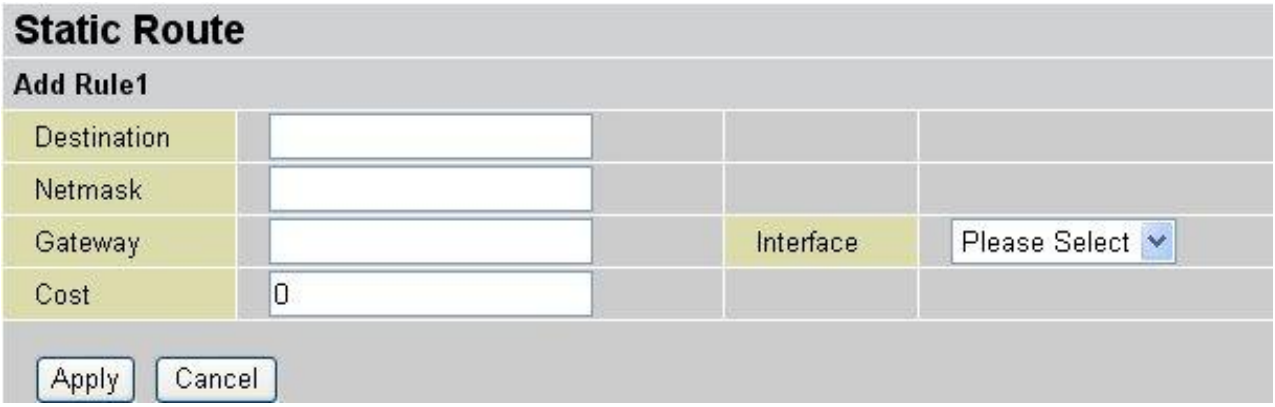
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign a static IP address to each virtual server PC, with an address that does not fall into 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.

3.3.7. 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 four items within the Advanced section: Static Route, Dynamic DNS, VLan Control and Device Management.

Static Route

Click on Routing Table and then choose Create Route to add a routing table.



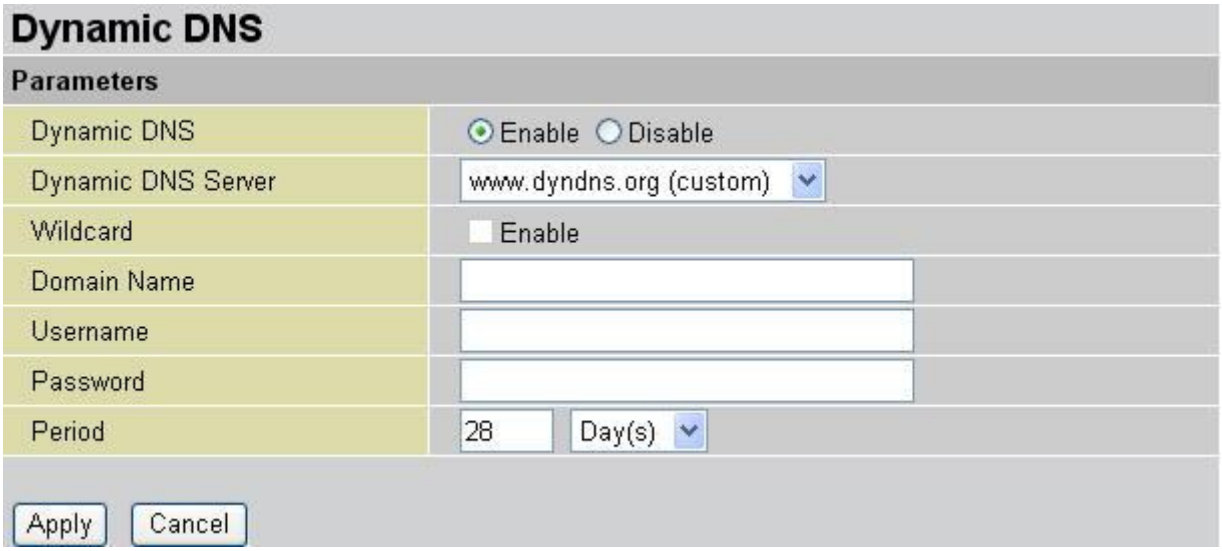
Destination: The destination subnet IP address.
Netmask: Subnet mask of the destination IP addresses based on above destination.
Gateway: The gateway IP address to which packets are forwarded.
Interface: Select the interface iplan or ipwan through which packets are forwarded.
Cost: Represents the cost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

Apply: Click to save settings
Cancel: Click to discard changes

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/



There are few DDNS services supported.

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 from drop-down list 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.

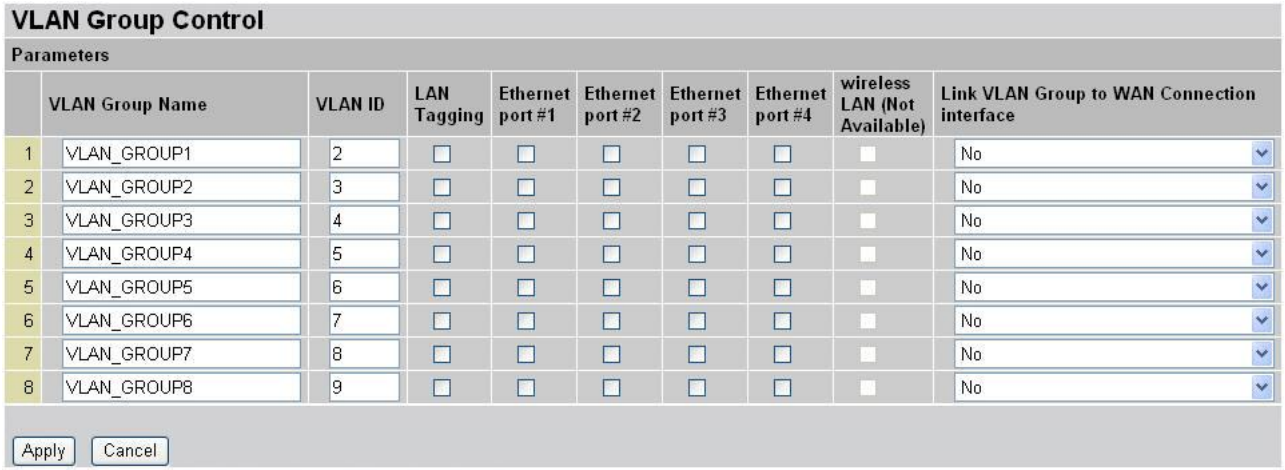
Period: Set the time period (Days/Hours) between updates, for the router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router performs an update when your dynamic IP address changes.

Apply: Click to save settings

Cancel: Click to discard changes

Vlan Control

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. While clients and servers may be located anywhere on a network, they are grouped together by VLAN technology, and broadcasts are sent to devices within the VLAN.

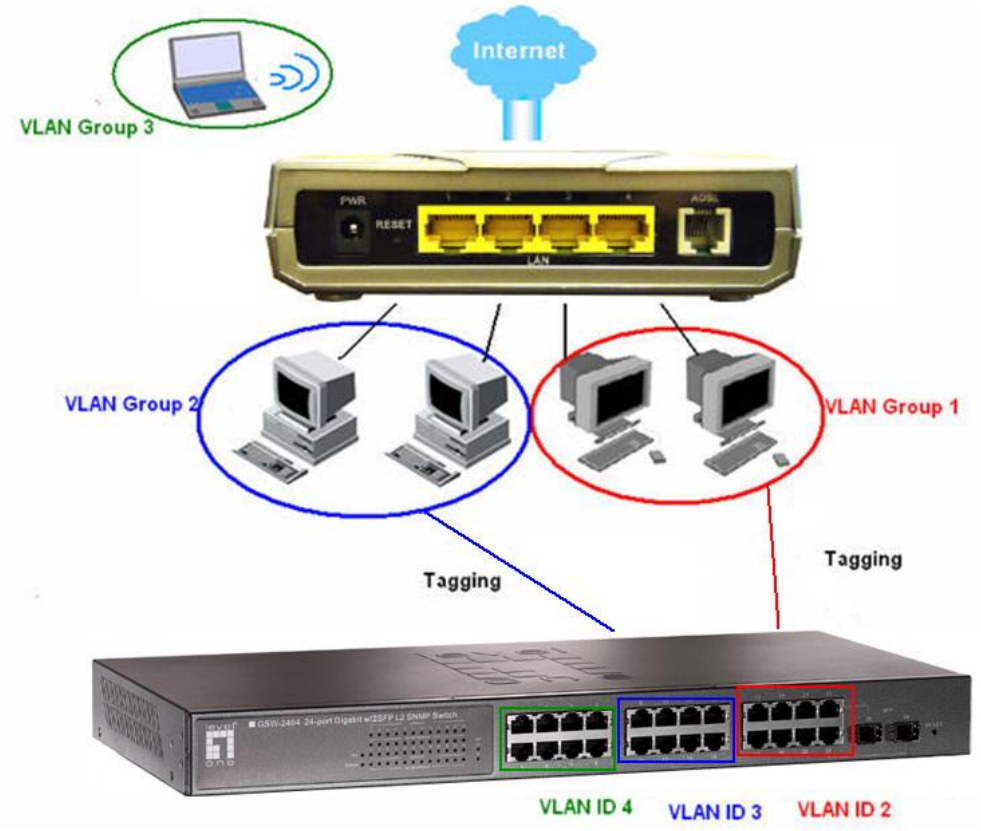


LAN Tagging: Tagging VLAN ID to the specific VLAN GROUP for ethernet interface

VLAN Group Name: There are eight groups that user can setup by themselves.
VLAN ID: Group name ID
LAN Tagging: Tagging VLAN ID to the specific VLAN group for Ethernet interface.
Ethernet port (1 ~ 4): Specify Port No of Router
Wireless LAN (Not Available)
Link VLAN Group to WAN connection Interface: Select the WAN connection interface that VLAN group link.

VLAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. Please refer to the following example.

1. If VLAN Group 1 is consisted of hosts linked to port1 and port2, VLAN Group 2 is consisted of hosts linked port3 and port4, and VLAN Group 3 is consisted wireless LAN.



2. After checking the box to enable VLAN function, you will check the table according to the needs as show below.

VLAN Group Control

Parameters

	VLAN Group Name	VLAN ID	LAN Tagging	Ethernet port #1	Ethernet port #2	Ethernet port #3	Ethernet port #4	wireless LAN	Link VLAN Group to interface
1	VLAN_GROUP1	2	☑	☑	☑	☐	☐	☐	Main WAN connect
2	VLAN_GROUP2	3	☑	☐	☐	☑	☑	☐	WAN Bridge Conne
3	VLAN_GROUP3	4	☐	☐	☐	☐	☐	☑	WAN Bridge Conne
4	VLAN_GROUP4	5	☐	☐	☐	☐	☐	☐	No
5	VLAN_GROUP5	6	☐	☐	☐	☐	☐	☐	No
6	VLAN_GROUP6	7	☐	☐	☐	☐	☐	☐	No
7	VLAN_GROUP7	8	☐	☐	☐	☐	☐	☐	No
8	VLAN_GROUP8	9	☐	☐	☐	☐	☐	☐	No

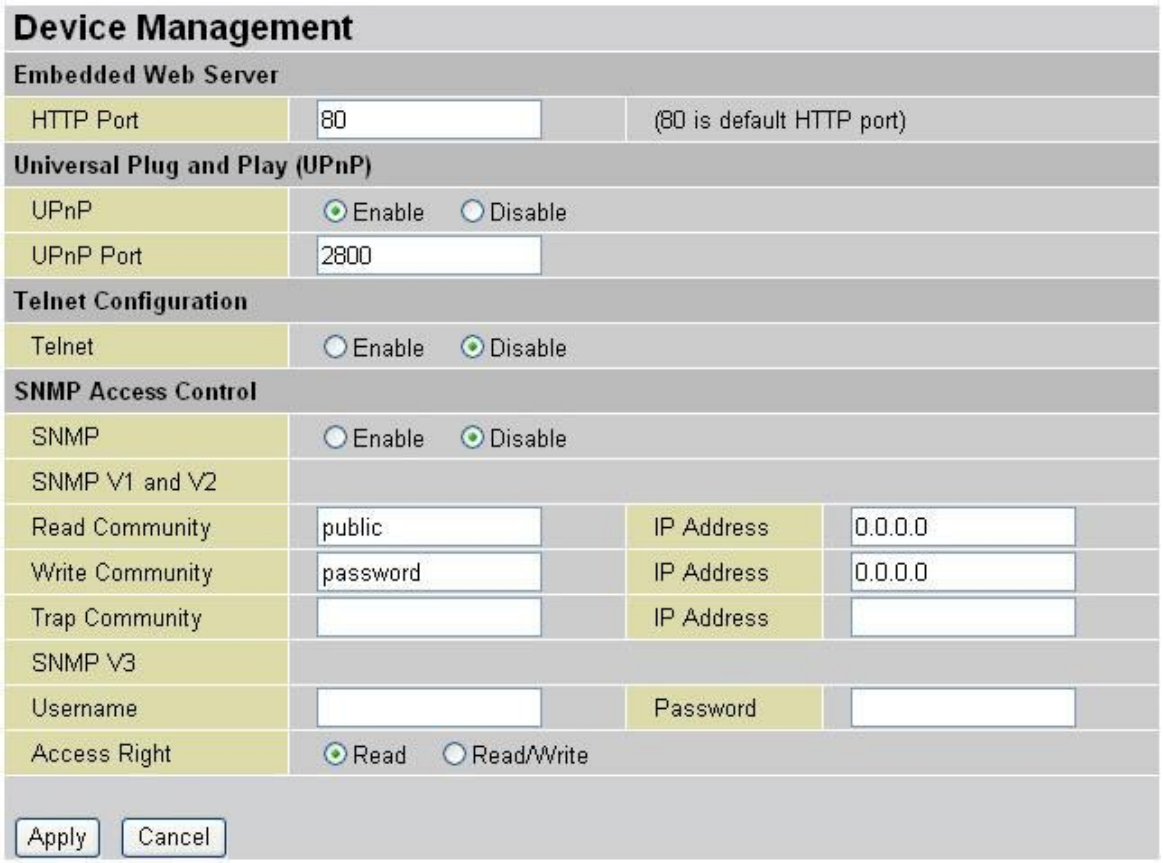
Apply Cancel

LAN Tagging: Tagging VLAN ID to the specific VLAN GROUP for ethernet interface

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.

Device Management

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



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 192.168.1.55, and sets the logout time to be 100 seconds. The router only allows User A access from the IP address 192.168.1.55 to logon to the Web GUI by typing: http://192.168.1.254:100 in their web browser. After 100 seconds, 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 that you use this port value. If the value conflicts with other ports already in use you may wish to change the port.

Telnet Configuration

Enable this function to use telnet

- Disable: Check to disable the router telnet functionality.
- Enable: Check to enable the router telnet functionality.

SNMP Access Control

Simple Network Management Protocol—software on a PC within the LAN is required to use this function. Enable this function to use telnet

- Disable: Check to disable the router SNMP functionality.
- Enable: Check to enable the router SNMP functionality.

SNMP V1 and V2:

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

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

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

SNMP V3:

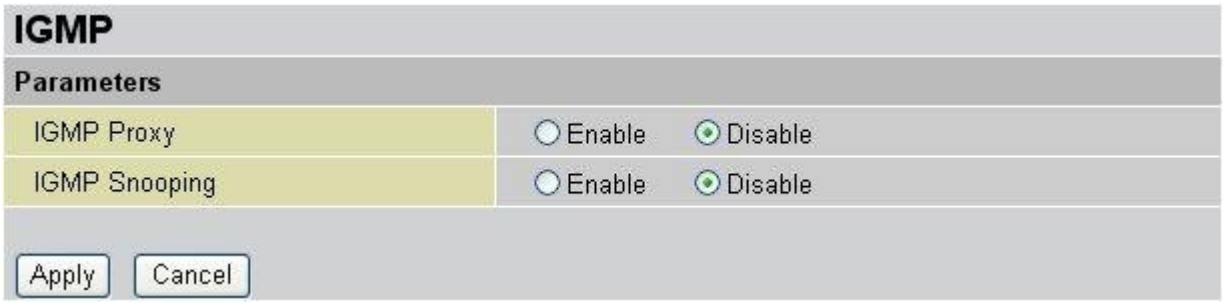
Specify a **User name** and **Password** for authentication, and define access rights to the Read or Read/Write. Once authentication has succeeded, users from this IP address are able to view and modify data. Specify **Access Right** to Read or Read/Write.

Apply: Click to save settings

Cancel: Click to discard changes

IGMP

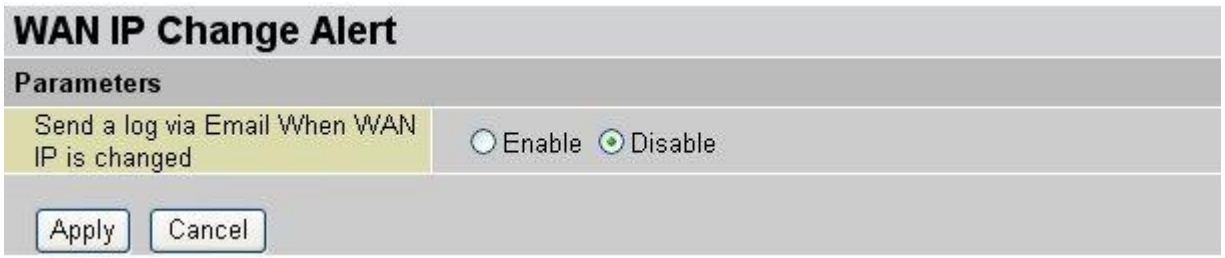
IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.



IGMP Proxy: Accepting multicast packet. Default is set to Disable.
IGMP Snooping: Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to Enable

Apply: Click to save settings
Cancel: Click to discard changes

WAN IP Change Alert



Send a log via Email When WAN IP is changed. Default is set to Disable. After enable this function, user needs to specify the e-mail account / SMTP server and notice message will send.

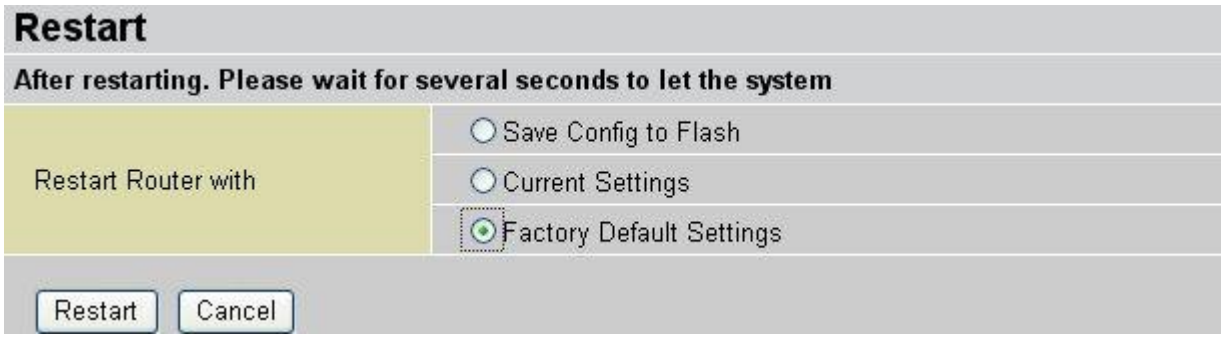
Apply: Click to save settings
Cancel: Click to discard changes

3.4. 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 to write your new configuration to FLASH. Click **Apply** to write setting to flash.

3.5. Restart

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



Select **Save Config to Flash** and click **Restart** to take all changes effect
Select **Current Settings** and click **Restart**, all changes will discard and restart with last saved settings.

Factory Default 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.
You may also reset your router to factory settings by holding in the small Reset pinhole button on the back of your router for 10-12 seconds while the router is turned on.

4. Troubleshooting

If your ADSL Router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider or LevelOne 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.
You have forgotten your router login and/or password.	Try the default login and password, please refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router for 6 seconds or more.

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 GE. 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.

5. Appendix

5.1. 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 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

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

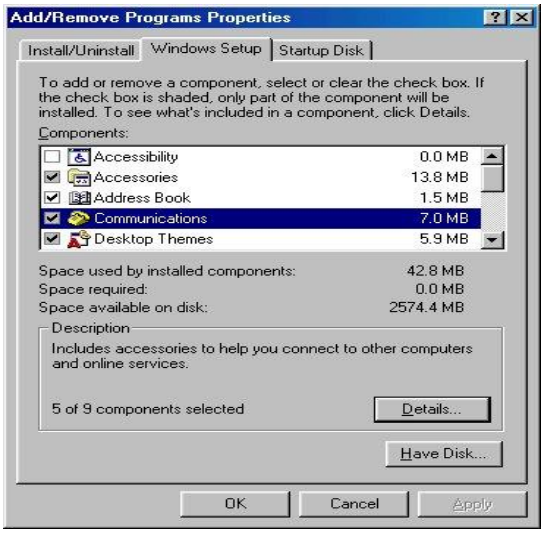
Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

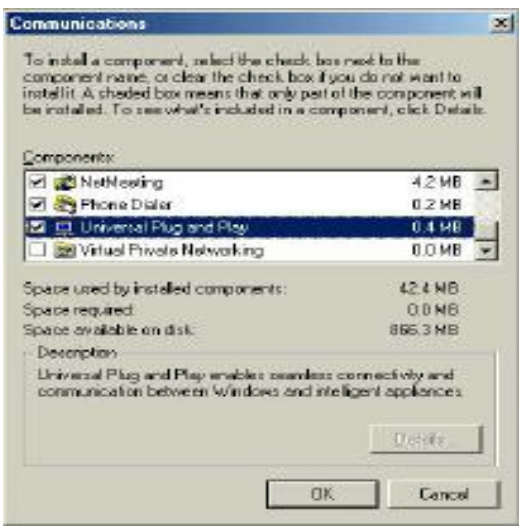
Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.

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

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

Step 5: Restart the computer when prompted.





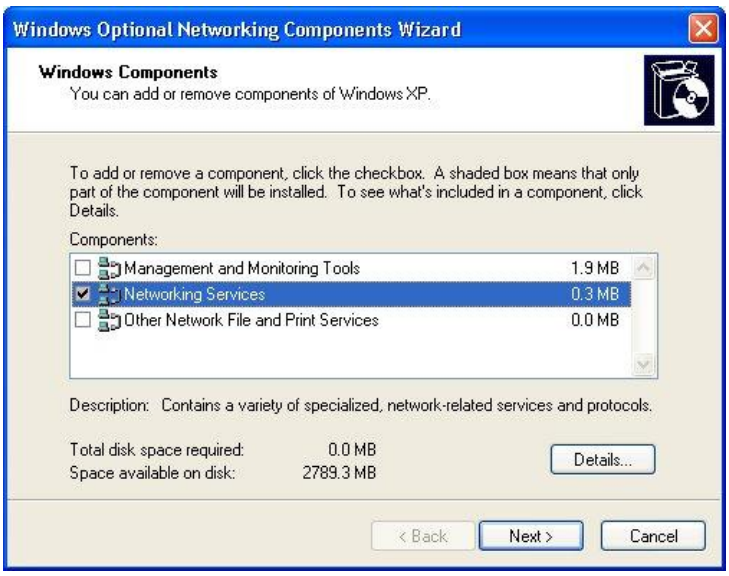
Follow the steps below to install the UPnP in Windows XP

Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

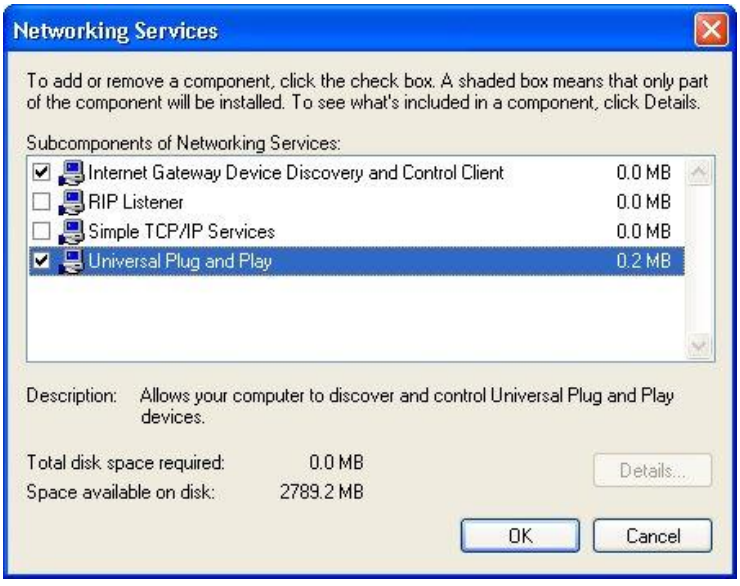
Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….
The Windows Optional Networking Components Wizard window displays.

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



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.

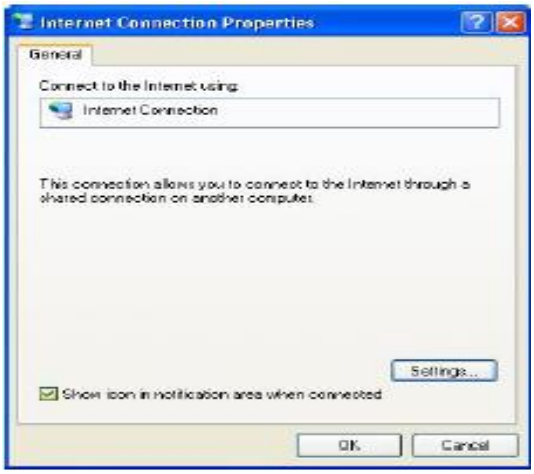


Auto-discover Your UPnP-enabled Network Device

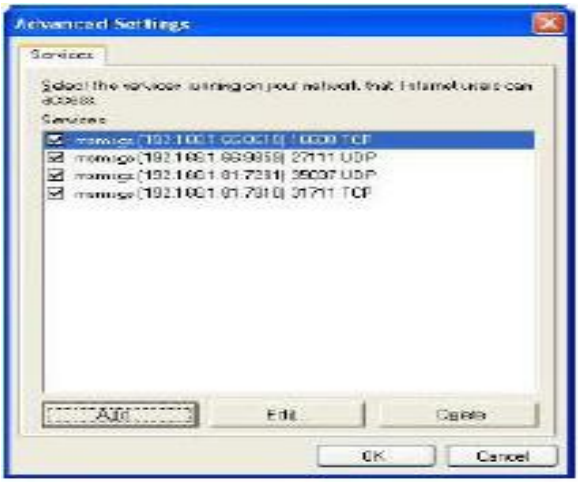
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

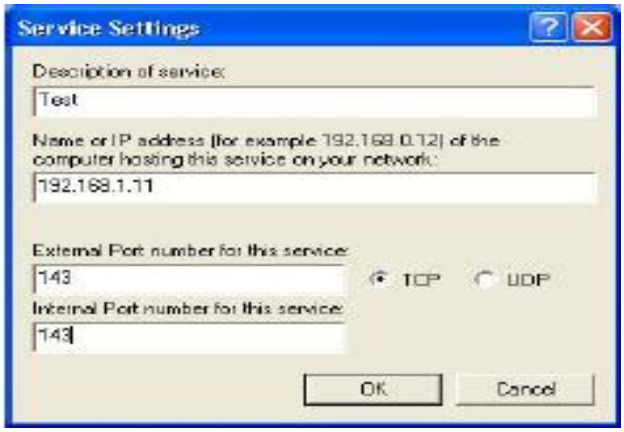
Step 2: Right-click the icon and select Properties.

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

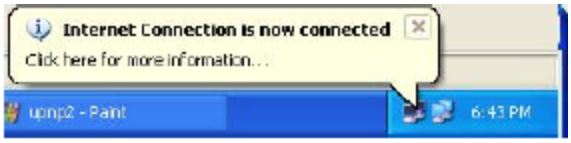


Step 4: You may edit or delete the port mappings or click Add to add it manually





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



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

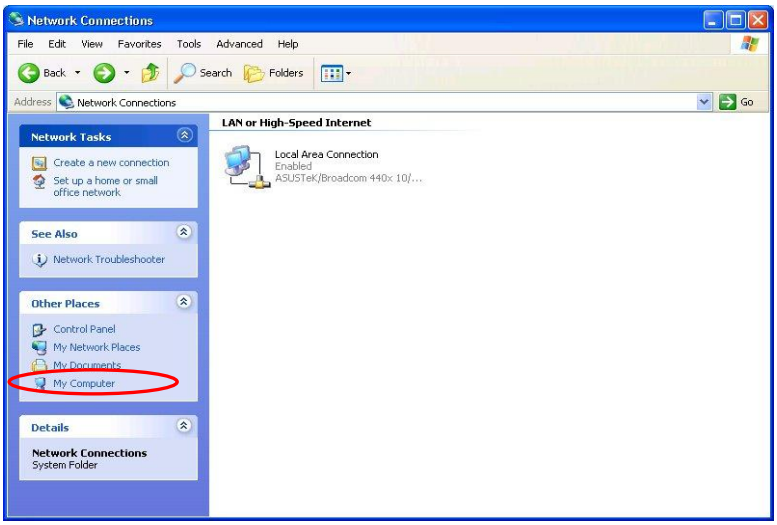
Web Configuration Easy Access

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. Regulatory Approvals

FCC Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

CE Approval

CE Standards

This product complies with the 99/5/EEC directives, including the following safety and EMC standards:

- EN300328-2
- EN301489-1/-17
- EN60950

CE Marking Warning

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

5.4. General Public License

This product incorporates open source code into the software and therefore falls under the guidelines governed by the General Public License (GPL) agreement.

Adhering to the GPL requirements, the open source code and open source license for the source code are available for free download at http://global.level1.com.

If you would like a copy of the GPL or other open source code in this software on a physical CD medium, LevelOne (Digital Data Communications) offers to mail this CD to you upon request, for a price of US$9.99 plus the cost of shipping.