BILLION™

BiPAC 7402GL *R4*

Wireless ADSL Firewall Router

User Manual

Version release 5.53.s5.wk

Last Revised Date 27-05-2009

Table of Contents

Chapter 1: Introduction

Introduction to your Router

Welcome to the wireless ADSL Firewall Router. The router is an “all-in-one” ADSL router, combining an ADSL modem, ADSL router and Ethernet network switch functionalities, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection. With features such as an ADSL Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users to the guru requiring advanced features and control over their Internet connection and network.

Features

- **Express Internet Access**

The router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis.plus (ITU G.992.5)).

- **802.11g Wireless AP with WPA Support**

With integrated 802.11g Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection with single device simplicity, and as a result, mobility to the users. In addition to 54 Mbps 802.11g data rate, it also interoperates backward with existing 802.11b equipment. The Wireless Protected Access (WPA-PSK and WPA2-PSK) and Wireless Encryption Protocol (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.

- **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. An Ethernet straight or crossover cable can be used directly for auto detection.

- **Multi-Protocol to Establish a Connection**

It supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation overATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard

It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf 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. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

Network Address Translation (NAT)

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

SOHO Firewall Security with DoS and SPI

Along with the built-in NAT natural firewall feature, the router also provides advanced hacker pattern-filtering protection. It can automatically detect and block Denial of Service (DoS) attacks. The router is built with Stateful Packet Inspection (SPI) to determine if a data packet is allowed through the firewall to the private LAN.

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo. com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in 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. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.

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 don’t saturate upload bandwidth, or office browsing doesn’t bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

Virtual Server (“port forwarding”)

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.

Rich Packet Filtering

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.

Dynamic Host Configuration Protocol (DHCP) Client and Server

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.

Static and RIP1/2 Routing

It has routing capability and supports easy static routing table or RIP1/2 routing protocol.

Simple Network Management Protocol (SNMP)

It is an easy way to remotely manage the router via SNMP.

Web based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

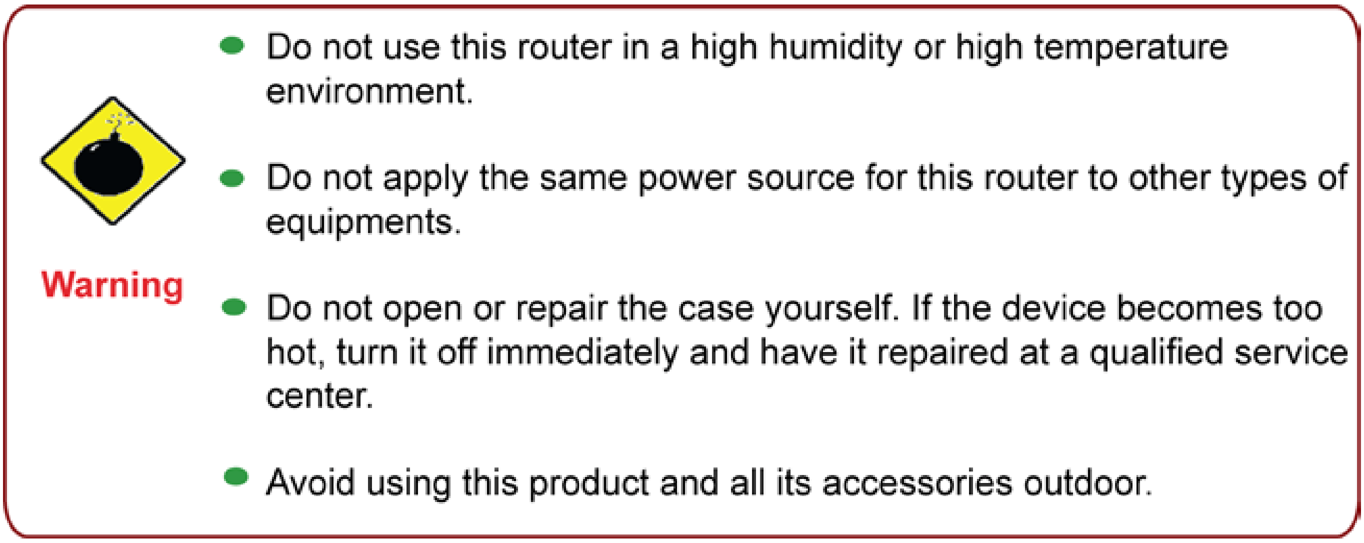
Device can be upgraded to the latest firmware through the WEB based GUI.

Rich Management Interfaces

It supports flexible management interfaces with LAN port, and WAN port. Users can use terminal applications through Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device.

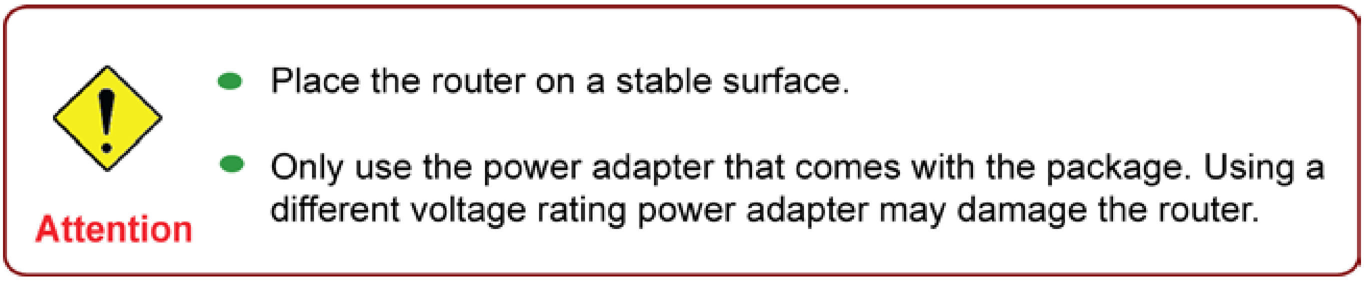
Chapter 2: Installing the Router

Important note for using this router



Warning

- Do not use this router in a high humidity or high temperature environment.
- Do not apply the same power source for this router to other types of equipments.
- Do not open or repair the case yourself. If the device becomes too hot, turn it off immediately and have it repaired at a qualified service center.
- Avoid using this product and all its accessories outdoor.



Attention

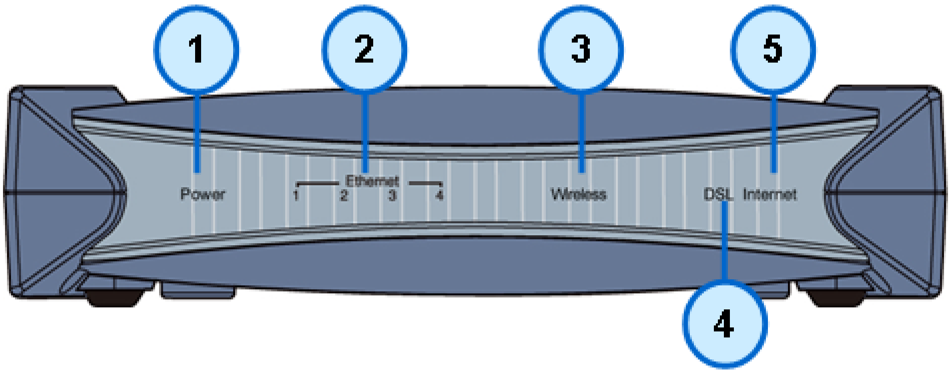
- Place the router on a stable surface.
- Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

Package Contents

- BiPAC 7402GL *R4* Wireless ADSL Firewall Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5) Cable
- Power adapter
- A detachable antenna
- Quick Start Guide

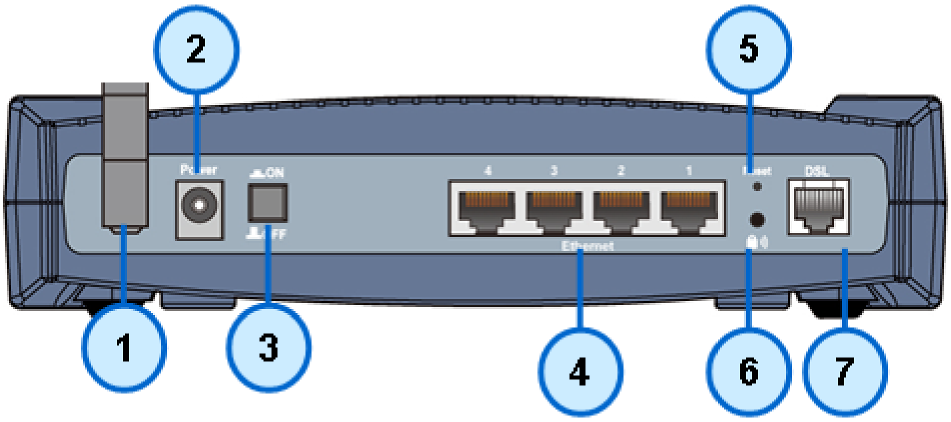
Device Description

The Front LEDs.



LED		Meaning
1	**Power**	Both red and green LEDs lit together when power is ON. Lit green when the device is ready. Lit red means system failure. Restart the device or contact Billion for support.
2	**Ethernet Port**	Lit green when Ethernet connection established Blink when data is being Transmitted / Received.
3	**Wireless**	Lit green when the wireless connection is established. Flashes when sending/receiving data.
4	**ADSL**	Lit Green when the device is successfully connected to an ADSL DSLAM.("line synch").
5	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when device in bridged mode or WAN connection not present.

The Rear Ports



NOTE: The Ethernet Port # 6 can be used as a console port. You need a special console tool which already includes in the package to connect with LAN.

Port		Meaning
1	**Antenna**	Connect the detachable antenna to this port.
2	**Power**	Connect it with the supplied power adapter.
3	**Power Switch**	Power ON/OFF switch.
4	**Ethernet**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
5	**RESET**	To be sure the device is being turned on press RESET button for: 1-3 seconds: quick reset the device. 6 seconds and above, power off, power on the device: restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). ***Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.***
6	**WPS**	Push WPS button to trigger Wi-Fi Protected Setup function.
7	**DSL**	Connect the supplied RJ-11 (“telephone”) cable on this port when connecting to the ADSL/telephone network.

Cabling

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

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, 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.

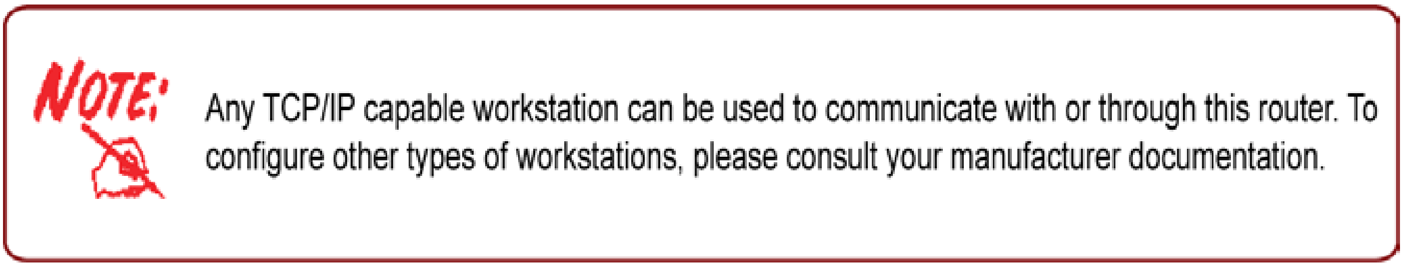
Chapter 3: Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please 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.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs 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 best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

Please follow the following steps to configure your PC network environment.

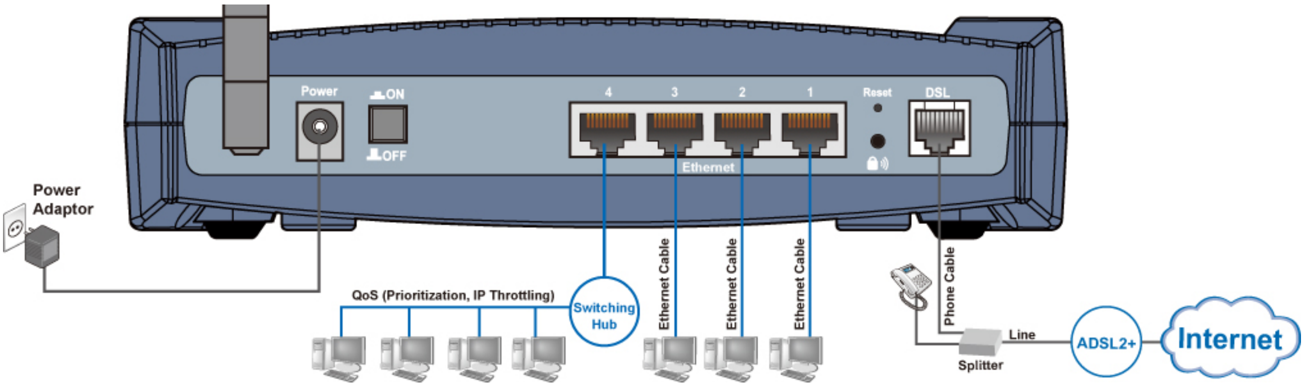


NOTE:

Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

Connecting Your Router

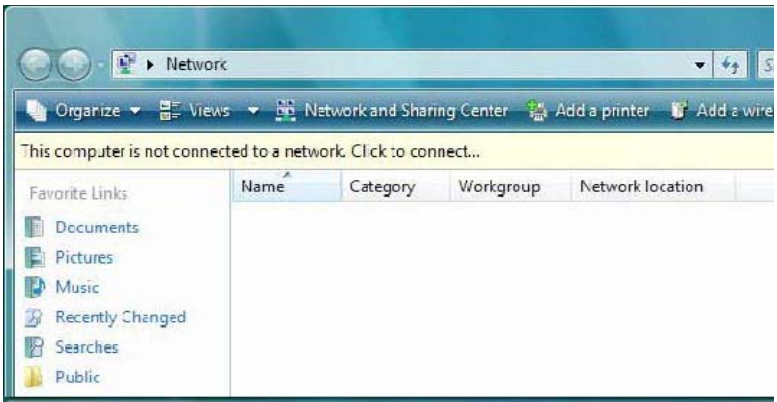
1. Connect this router to a LAN (Local Area Network) and the ADSL/telephone (ADSL) network.
2. Power on the device.
3. Make sure the **Power LED** lit steadily and that the **LAN** LED is lit.
4. Connect your router to the telephone jack on the wall with RJ-11 cable.



Network Configuration

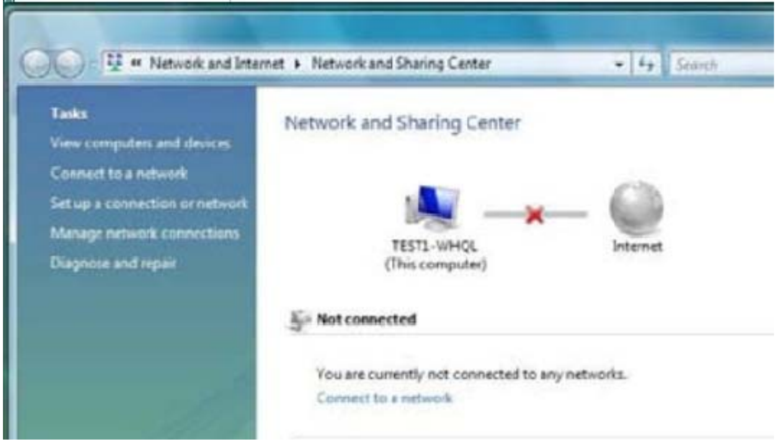
Configuring PC in Windows Vista

1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



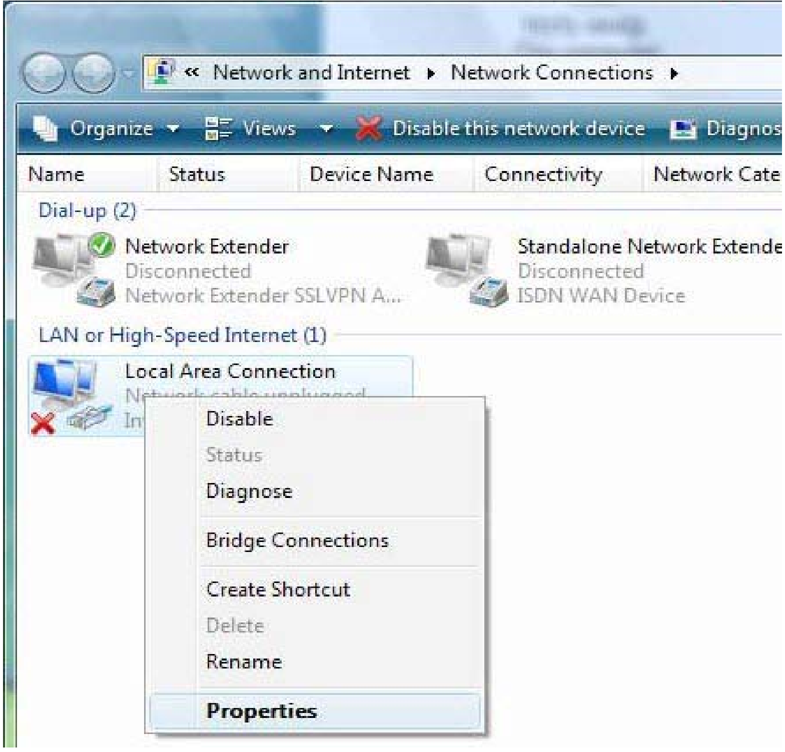
This computer is not connected to a network. Click to connect...

3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.

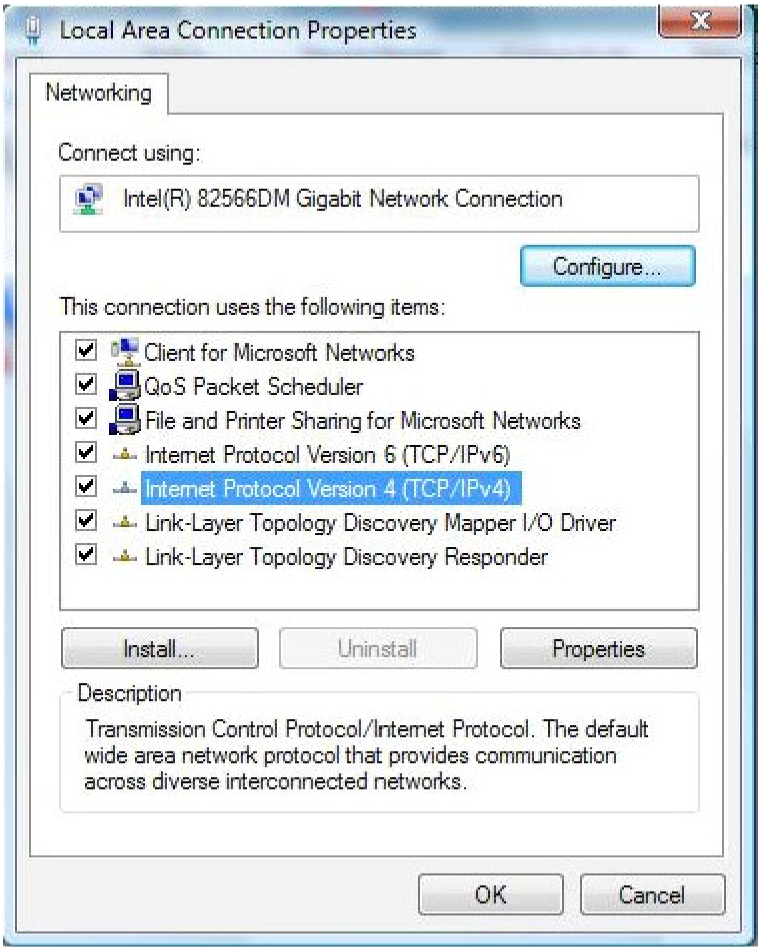


You are currently not connected to any networks.

4. Select the Local Area Connection, and right click the icon to select Properties.



5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82566DM Gigabit Network Connection

This connection uses the following items:

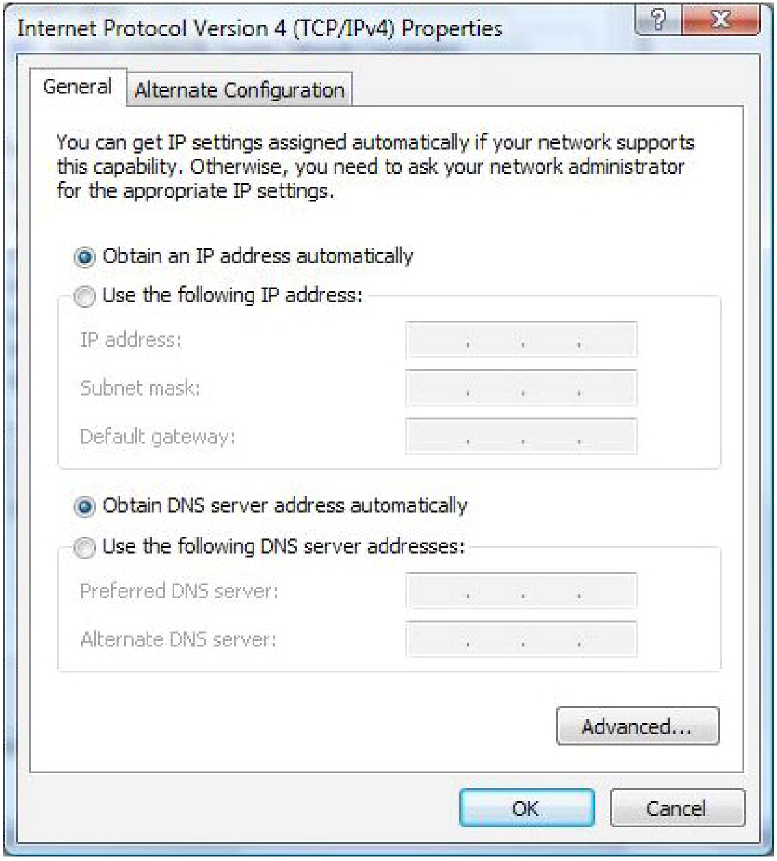
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

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

6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

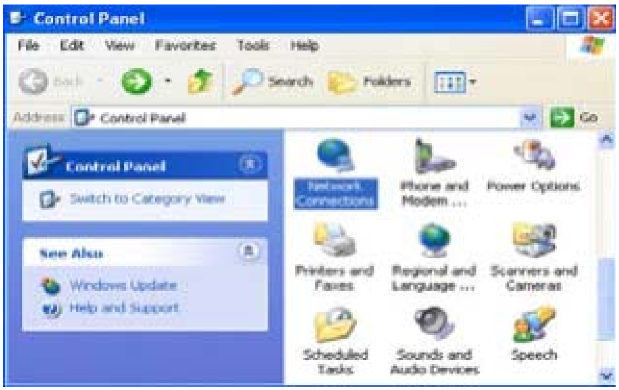
○ Use the following DNS server addresses:

Preferred DNS server: . . .

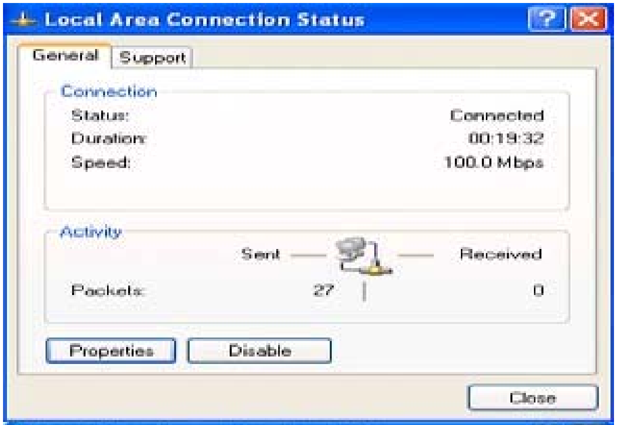
Alternate DNS server: . . .

Configuring PC in Windows XP

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



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


Local Area Connection Status

General | Support

Connection

Status: Connected

Duration: 00:19:32

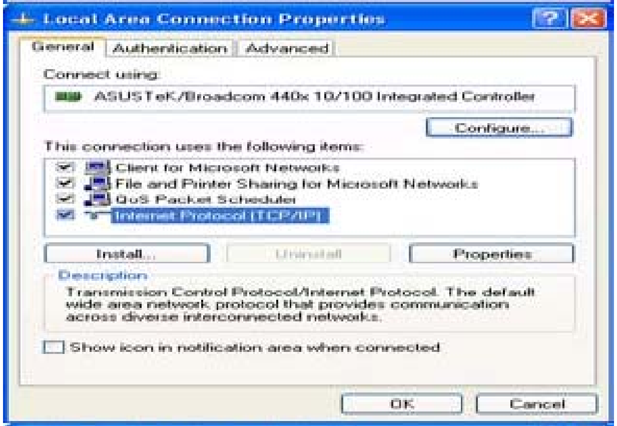
Speed: 100.0 Mbps

Activity

Sent — Received

Packets: 27 | 0

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


Local Area Connection Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

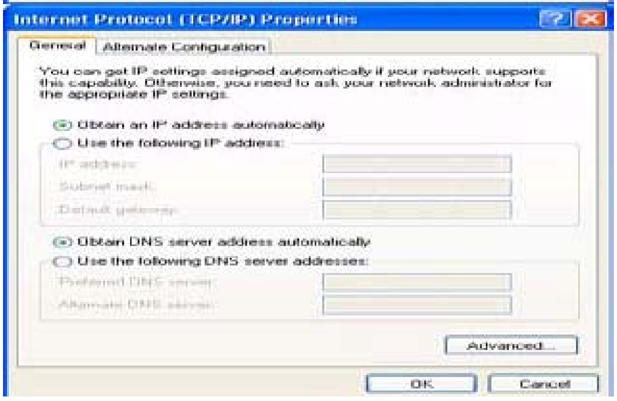
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

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

☐ Show icon in notification area when connected

5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.


Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

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

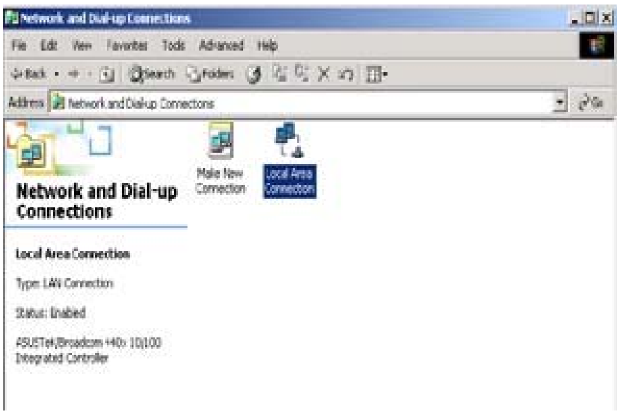
IP address:
Subnet mask:
Default gateway:

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

Preferred DNS server:
Alternate DNS server:

Configuring PC in Windows 2000

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



Network and Dial-up Connections

Address: Network and Dial-up Connections

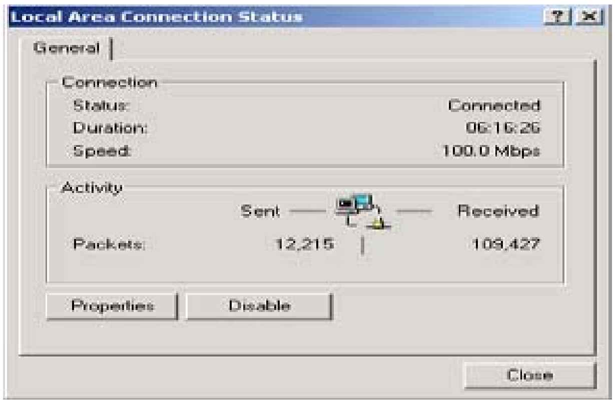
Local Area Connection

Type: LAN Connection

Status: Enabled

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

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



Local Area Connection Status

Connection

Status: Connected

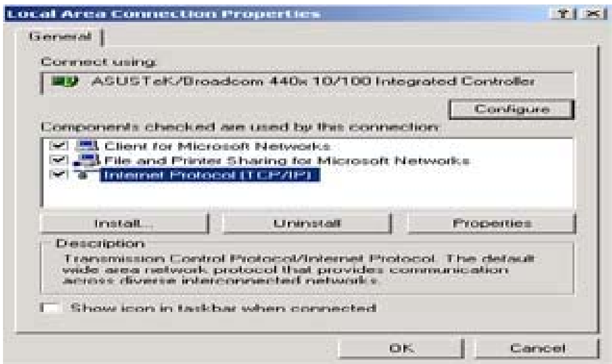
Duration: 06:16:26

Speed: 100.0 Mbps

Activity

	Sent	Received
Packets:	12,215	109,427

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



Local Area Connection Properties

Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

Components checked are used by this connection:

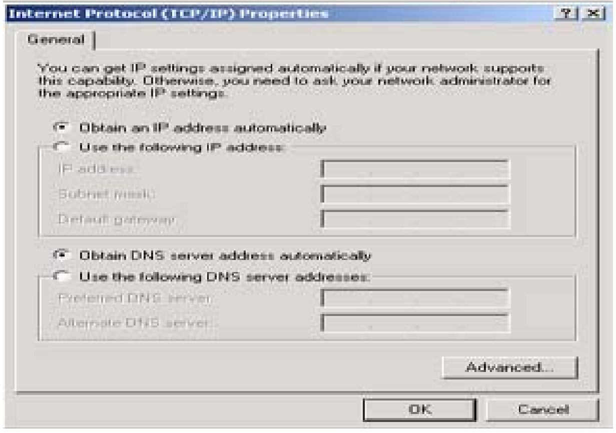
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

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

☐ Show icon in taskbar when connected

5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.



Internet Protocol (TCP/IP) Properties

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

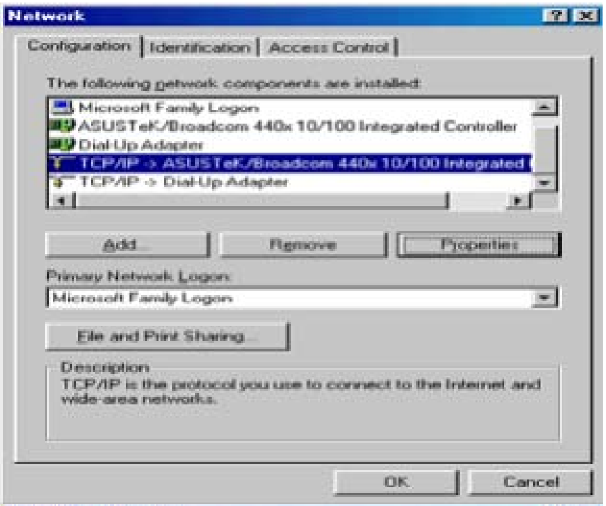
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Configuring PC in Windows 95/98/Me

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



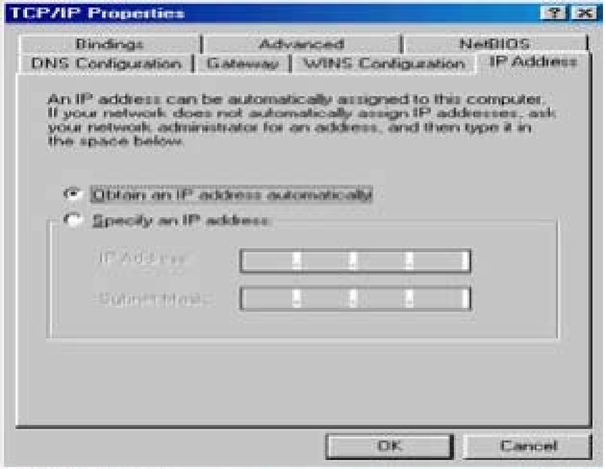
The following network components are installed:

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

Primary Network Logon: Microsoft Family Logon

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

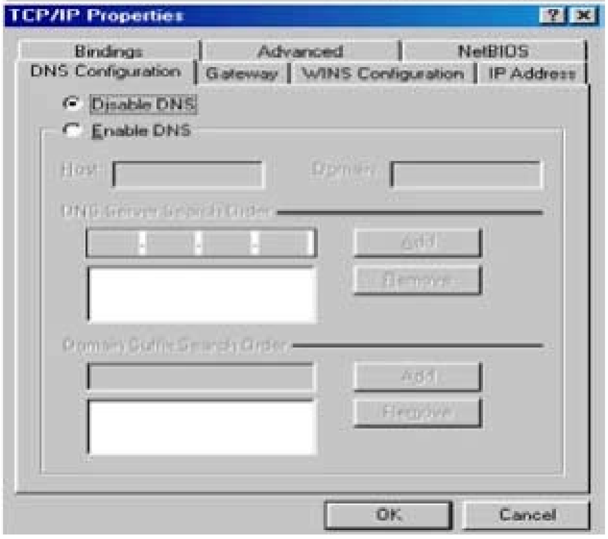
3. Select the Obtain an IP address automatically radio button.



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

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

4. Then select the DNS Configurationtab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

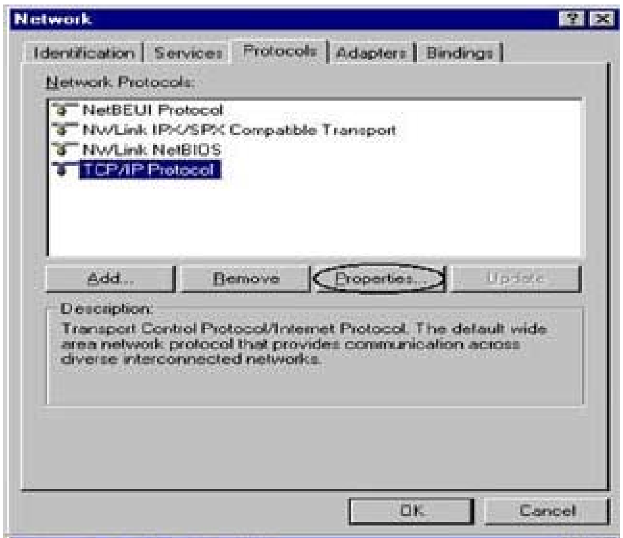


● Disable DNS
○ Enable DNS

Configuring PC in Windows NT4.0

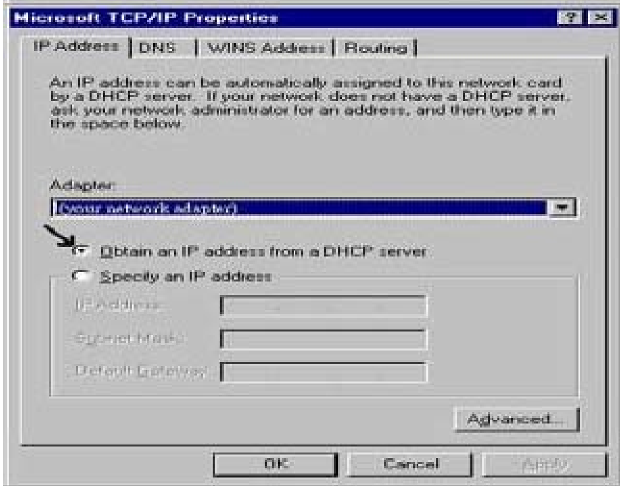
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.

2. Select TCP/IP Protocol and click Properties.



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

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



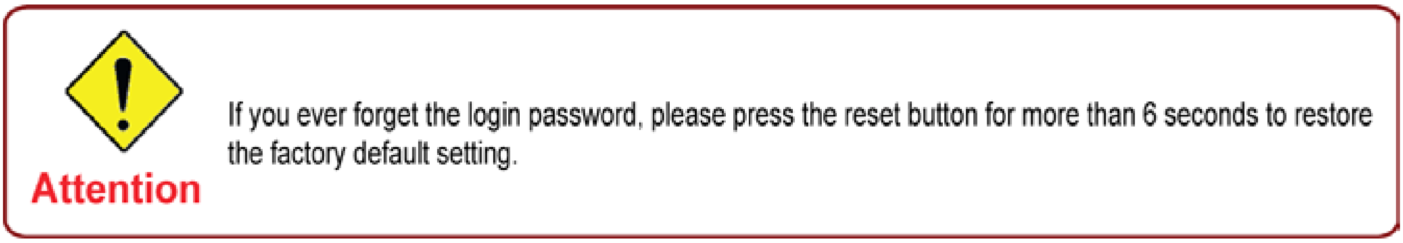
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Factory Default Settings

Before configuring your router, you need to know the following default settings.

Web Interface (Username and Password)

- Username: admin
- Password: admin



Attention

If you ever forget the login password, please press the reset button for more than 6 seconds to restore the factory default setting.

The default username and password are “**admin**” and “**admin**” respectively.

Device LAN 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

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown in the tale.

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 in ports 1, 2, 3 and 4	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

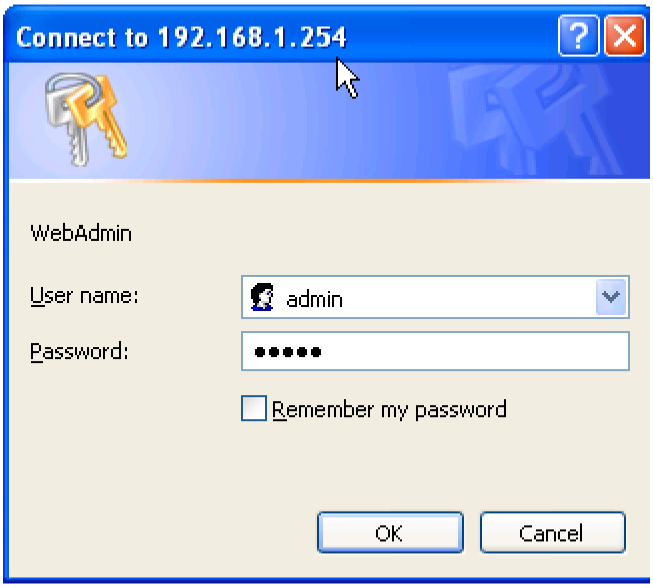
Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) or PPPoE.

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

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2684)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA(RFC1483/RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.
Multiple Session	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).

Configuring with your Web Browser

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 will appear. The default username and password are “admin” and “admin” respectively. (See Figure 3.14)



Connect to 192.168.1.254

WebAdmin

User name: admin

Password: ●●●●●

□ Remember my password

Figure 3.14: User name & Password Prompt Window

Congratulations! You are now successfully logon to the Router!

Chapter 4: Configuration

At the configuration homepage, the left navigation column provides you the link to each configuration page. The category of each configuration page is listed as below.

- **Status**

ADSL Status
ARP Table
DHCP Table
Routing Table
NAT Sessions
UPnP Portmap
Email Status
Event Log
Error Log
Diagnostic

- **Quick Start**

- **Configuration**

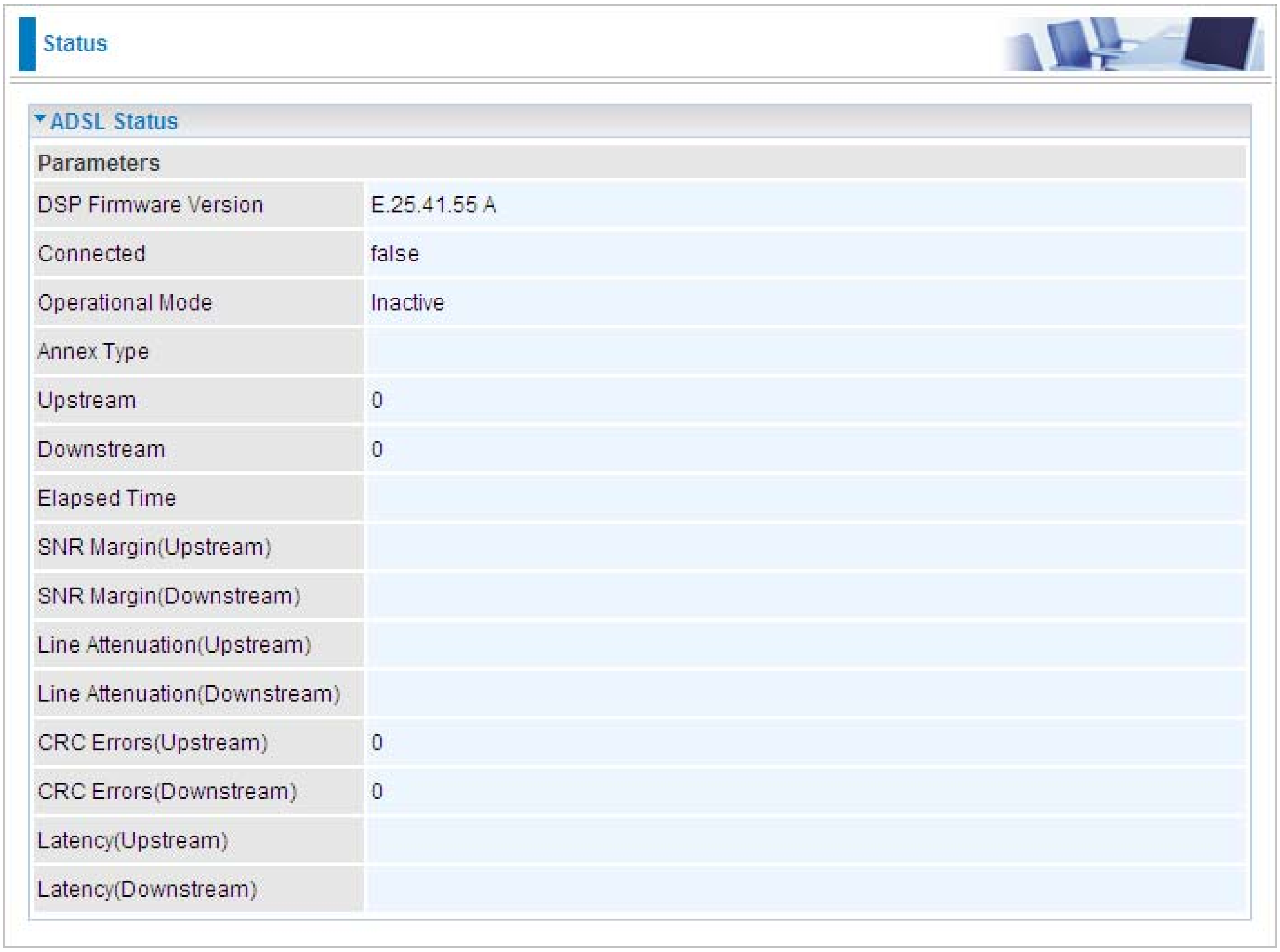
LAN
WAN
System
Firewall
QoS
Virtual Server
Wake on LAN
Time Schedule
Advanced

- **Language (provides user interface in English and French languages)**

Status

ADSL Status

This section displays the overall status of ADSL, such as DSP firmware version, Operational mode, Upstream/downstream rate, SNR margin, Line Attenuation, CRC Errors and Latency rate.



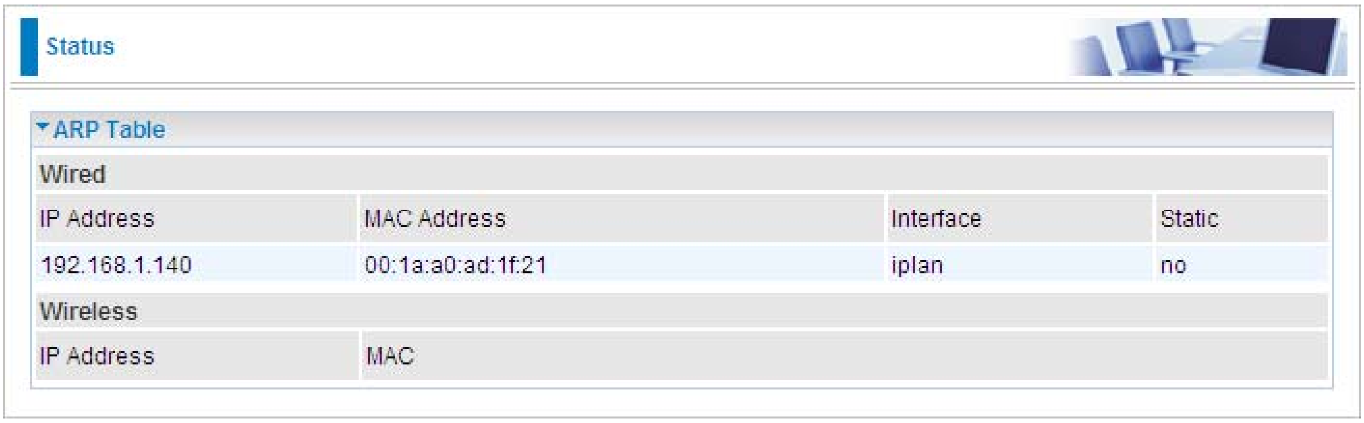
Status

▾ADSL Status

Parameters	
DSP Firmware Version	E.25.41.55 A
Connected	false
Operational Mode	Inactive
Annex Type	
Upstream	0
Downstream	0
Elapsed Time	
SNR Margin(Upstream)	
SNR Margin(Downstream)	
Line Attenuation(Upstream)	
Line Attenuation(Downstream)	
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	
Latency(Downstream)	

ARP Table

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



▾ARP Table

Wired

IP Address	MAC Address	Interface	Static
192.168.1.140	00:1a:a0:ad:1f:21	iplan	no

Wireless

IP Address	MAC

IP Address: Shows a list of IP addresses of devices on your LAN (Local Area Network).

MAC Address: Shows the MAC (Media Access Control) addresses of each device on your LAN.

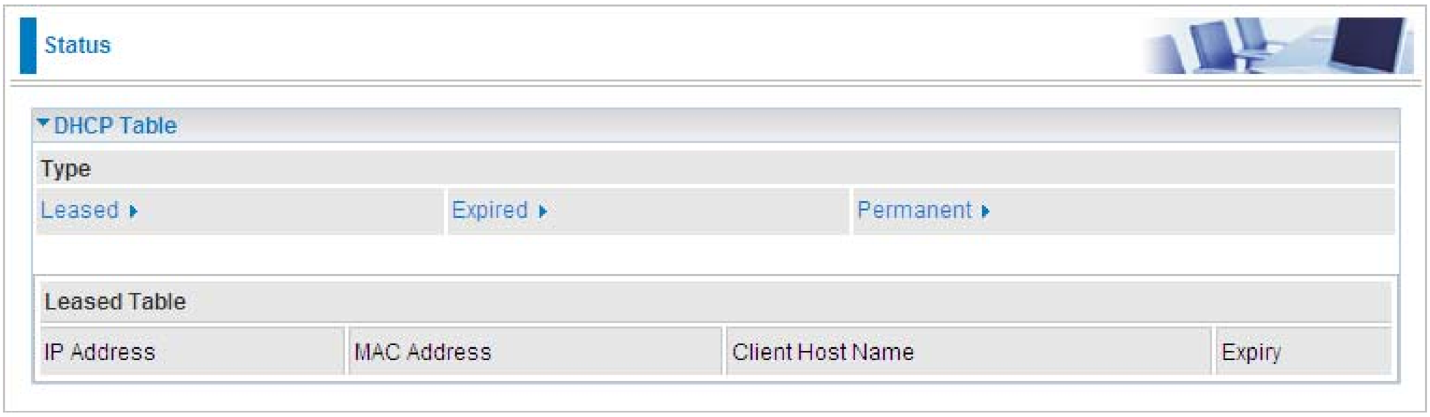
Interface: Shows the interface name (on the router) that this IP Address connects to.

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.

DHCP Table



Status

DHCP Table

Type		
Leased ▸	Expired ▸	Permanent ▸

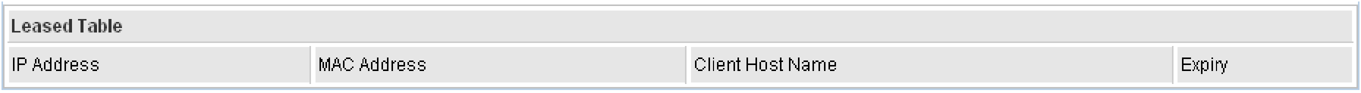
Leased Table			
IP Address	MAC Address	Client Host Name	Expiry

Leased: Shows the information of the DHCP assigned IP addresses.

Expired: Shows the information of all expired IP addresses.

Permanent: Shows the fixed host mapping information.

Leased Table



Leased Table			
IP Address	MAC Address	Client Host Name	Expiry

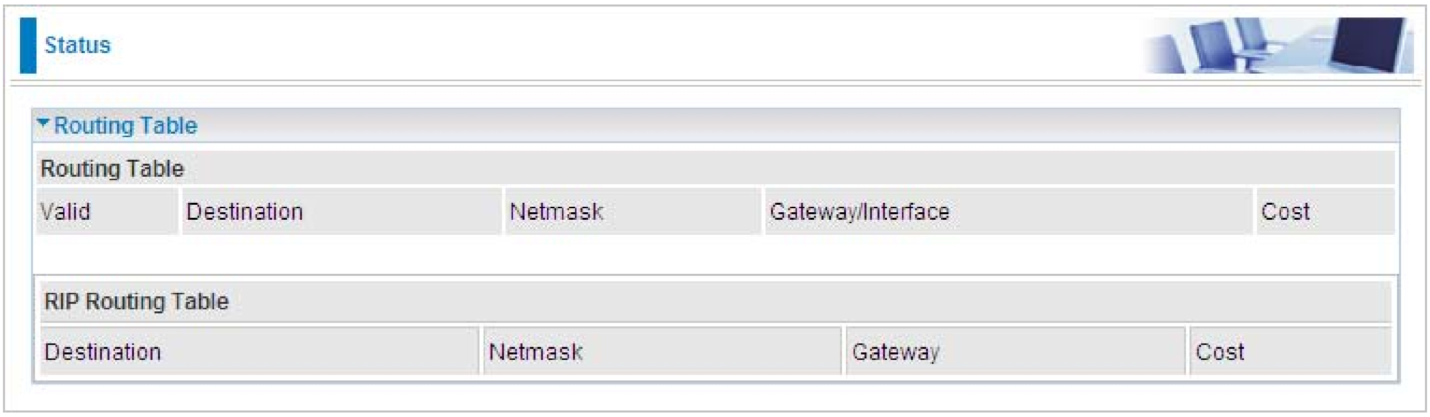
IP Address: Shows the IP address that is assigned to each client.

MAC Address: Shows the MAC address of each client.

Client Host Name: Shows the Host Name (Computer Name) of the client.

Expiry: Shows the current lease time of each client.

Routing Table



Status

Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost

RIP Routing Table

Destination	Netmask	Gateway	Cost

Routing Table

Valid: A check mark indicates a successful routing status.

Destination: Shows the IP address of the destination network.

Netmask: Shows the destination Netmask address.

Gateway/Interface: Shows the IP address of the gateway or the existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table

Destination: Shows the IP address of the destination network.

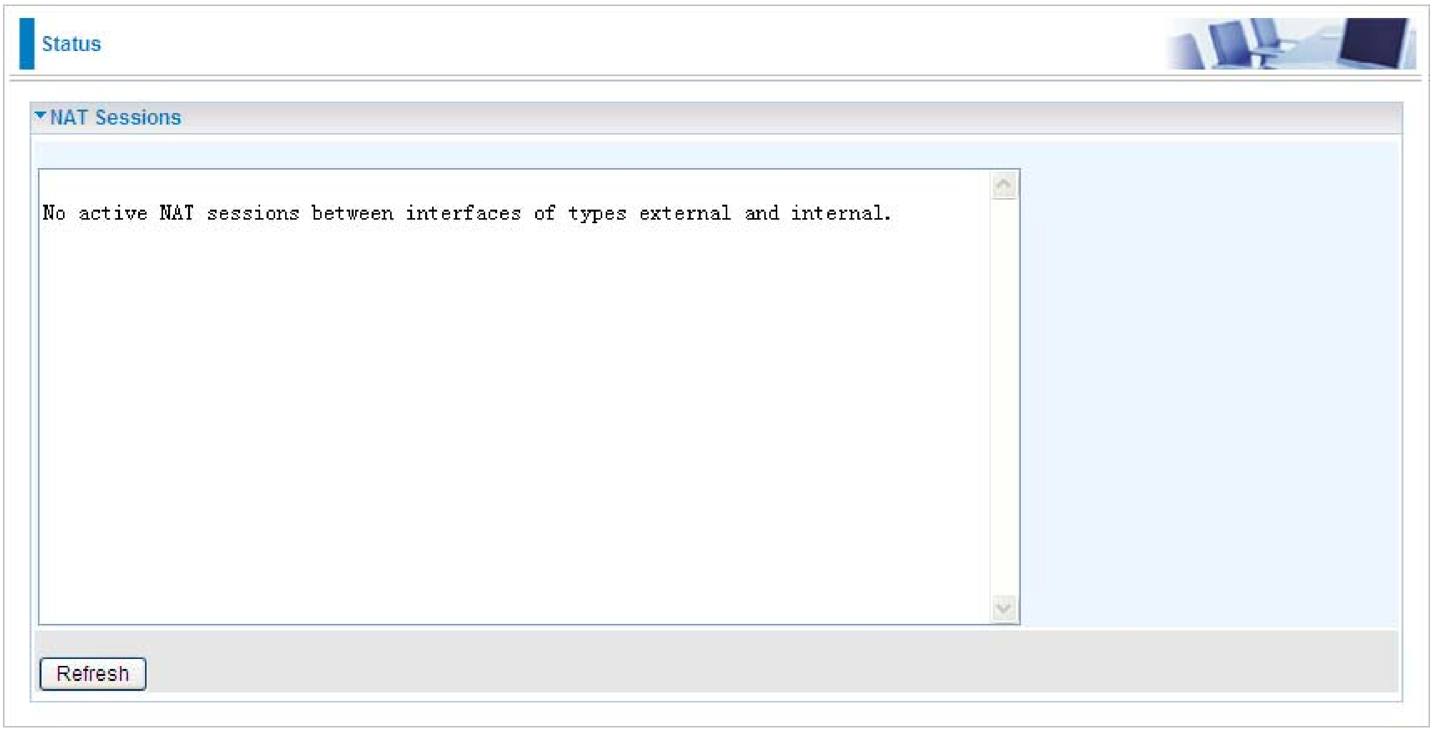
Netmask: Shows the destination Netmask address.

Gateway: Shows the IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

NAT Sessions

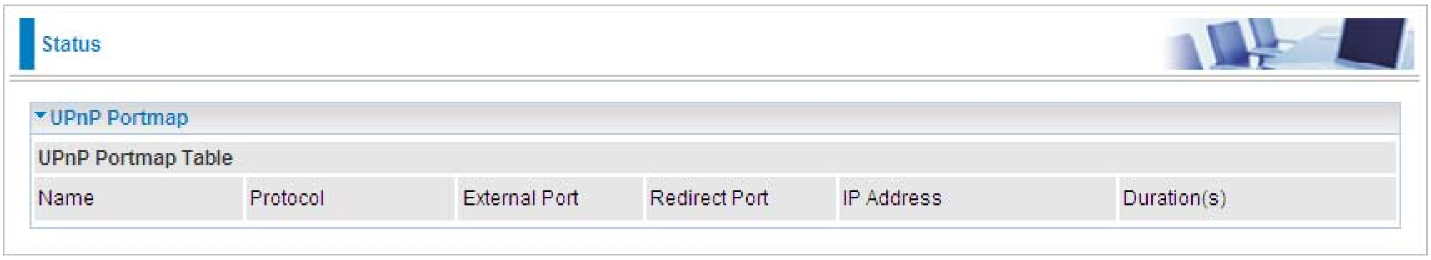
This section lists all the current NAT sessions between external (WAN) and internal (LAN) interface.



```
No active NAT sessions between interfaces of types external and internal.
```

UPnP Portmap

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

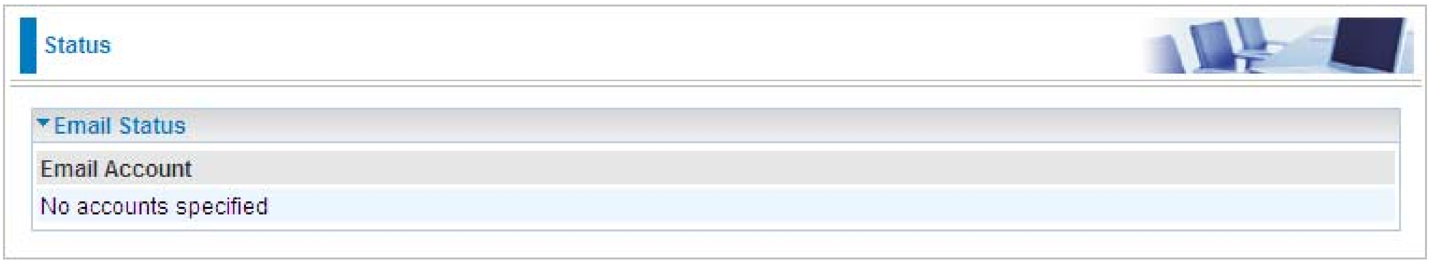


UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address	Duration(s)

Email Status

Details and status for the Email Account you have configured the router to check. Please see the **Advanced** section of this manual for details on this function.

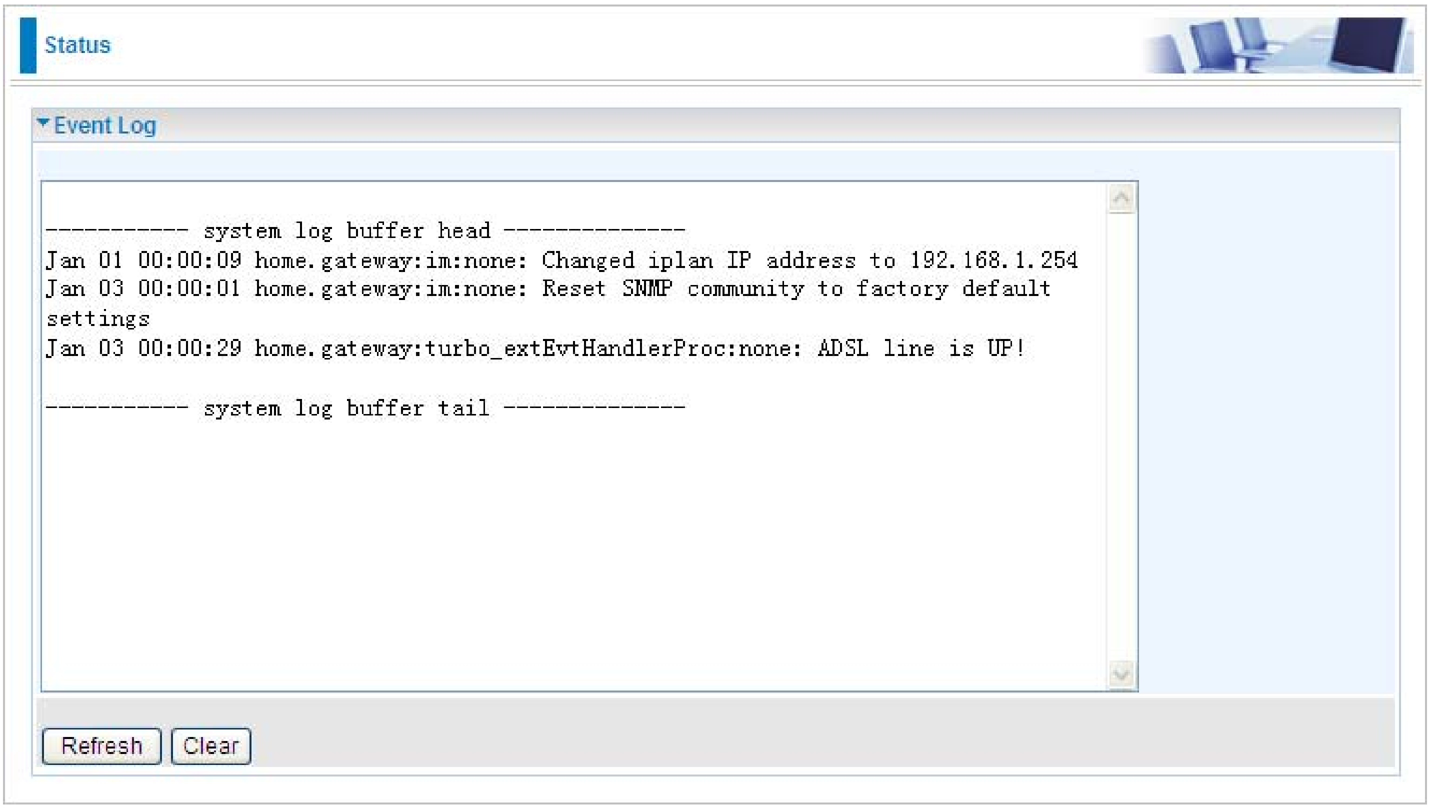


Email Account

No accounts specified

Event Log

This page displays all the event Log entries of the router such as when gets disconnected and during Firewall triggered events like Intrusion or Blocking Logging. Please see the Firewall section of this manual for more details on how to enable Firewall logging.

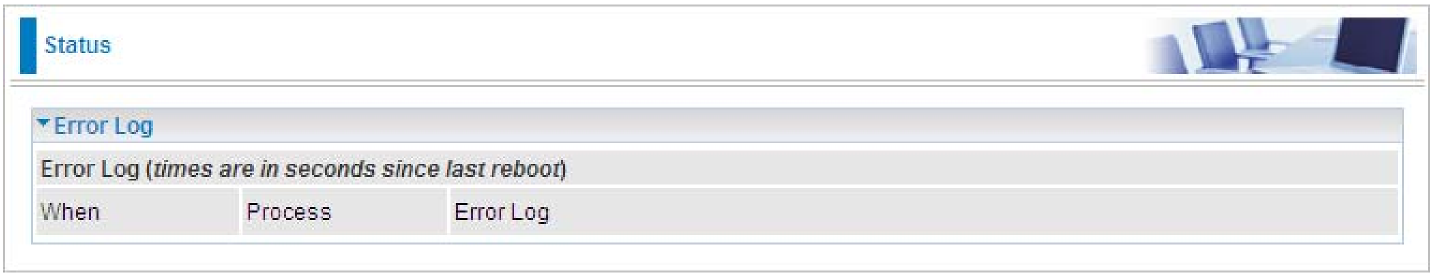


```
----------- system log buffer head --------------
Jan 01 00:00:09 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 03 00:00:01 home.gateway:im:none: Reset SNMP community to factory default
settings
Jan 03 00:00:29 home.gateway:turbo_extEvtHandlerProc:none: ADSL line is UP!

----------- system log buffer tail --------------
```

Error Log

Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.

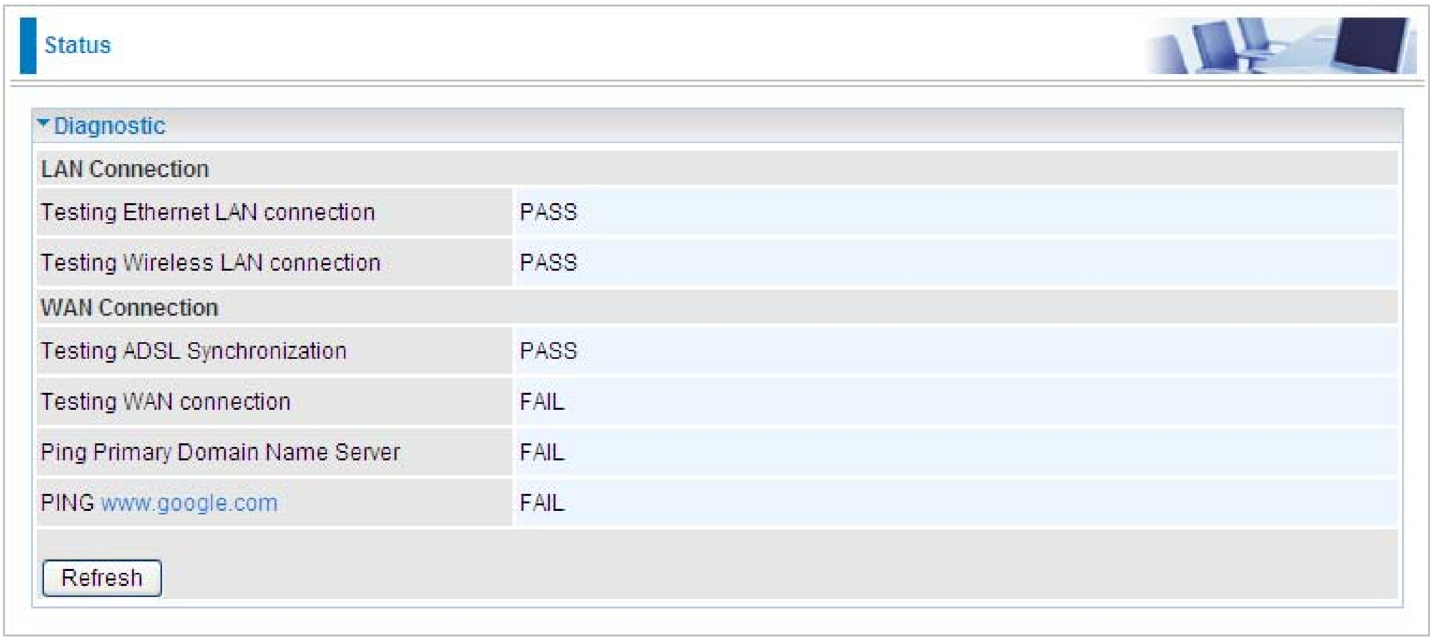


Error Log (*times are in seconds since last reboot*)

When	Process	Error Log

Diagnostic

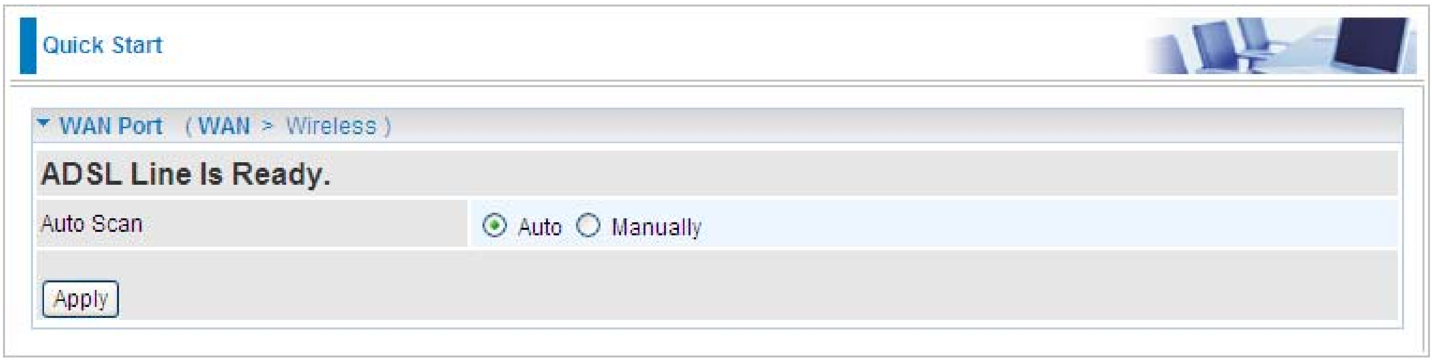
It tests the connection to computer(s) which is connected to the LAN ports and also the WAN Internet connection. If PING **www.google.com** is shown FAIL and the rest is PASS, you ought to check your PC's DNS setting is correct.



LAN Connection	
Testing Ethernet LAN connection	PASS
Testing Wireless LAN connection	PASS
WAN Connection	
Testing ADSL Synchronization	PASS
Testing WAN connection	FAIL
Ping Primary Domain Name Server	FAIL
PING www.google.com	FAIL

Quick Start

1. Click Quick Start.



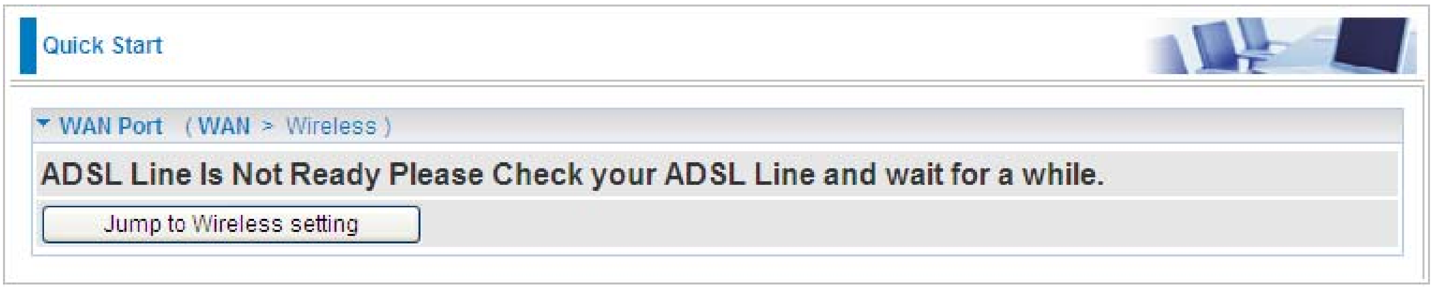
Quick Start

▾ WAN Port (WAN > Wireless)

ADSL Line Is Ready.

Auto Scan ● Auto ○ Manually

2. If your ADSL line is not ready, you need to check your ADSL line has been set or not.

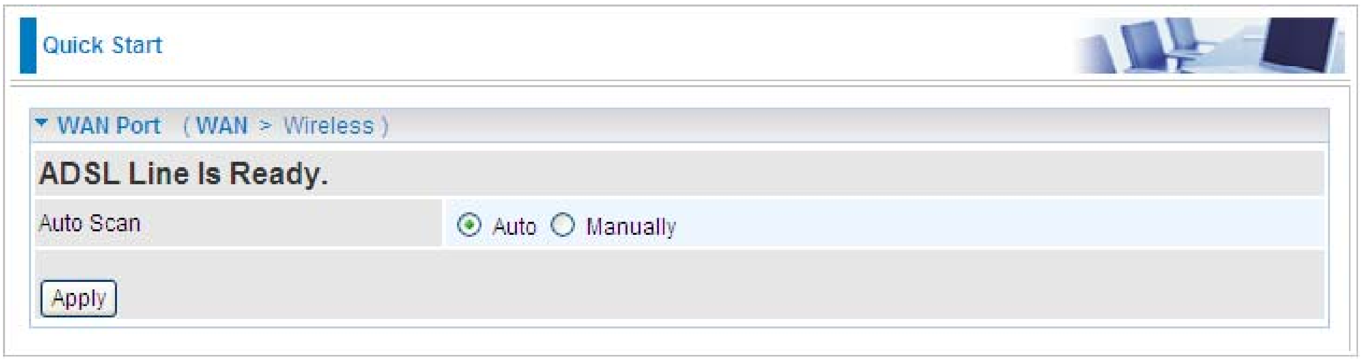


Quick Start

▾ WAN Port (WAN > Wireless)

ADSL Line Is Not Ready Please Check your ADSL Line and wait for a while.

3. If your ADSL line is ready, the screen appears ADSL Line is Ready. Choose **Auto** radio button and click **Apply.** It will automatically scan the recommended mode for you. Manually mode makes you to set the ADSL line by manual.



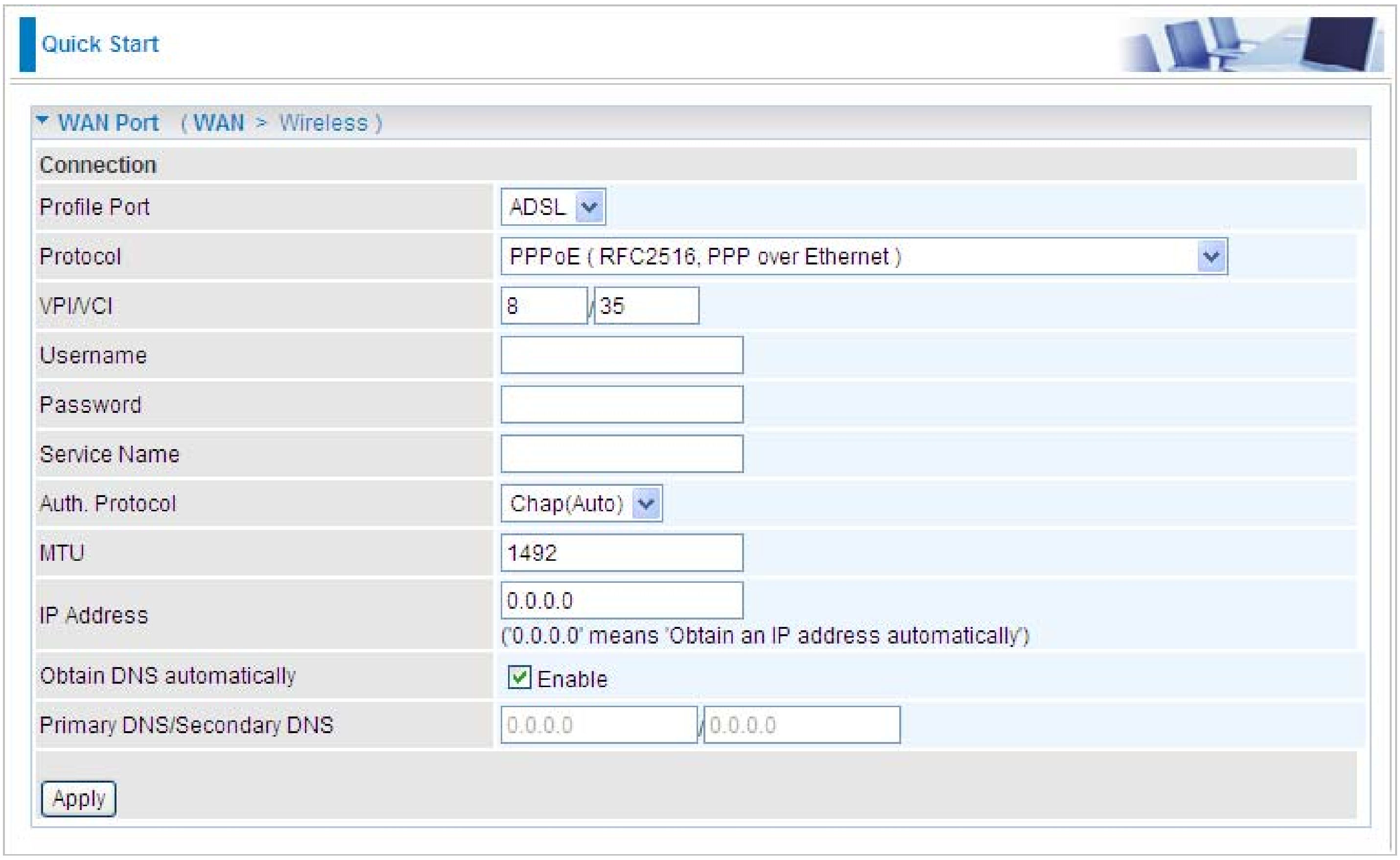
Quick Start

▾ WAN Port (WAN > Wireless)

ADSL Line Is Ready.

Auto Scan ● Auto ○ Manually

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



▾ WAN Port (WAN > Wireless)

Connection

Profile Port	ADSL
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI/VCI	8 / 35
Username	
Password	
Service Name	
Auth. Protocol	Chap(Auto)
MTU	1492
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

Profile Port: Select the connection mode. There is ADSL.

Protocol: Select the protocol;. The default is PPPoE.

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

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

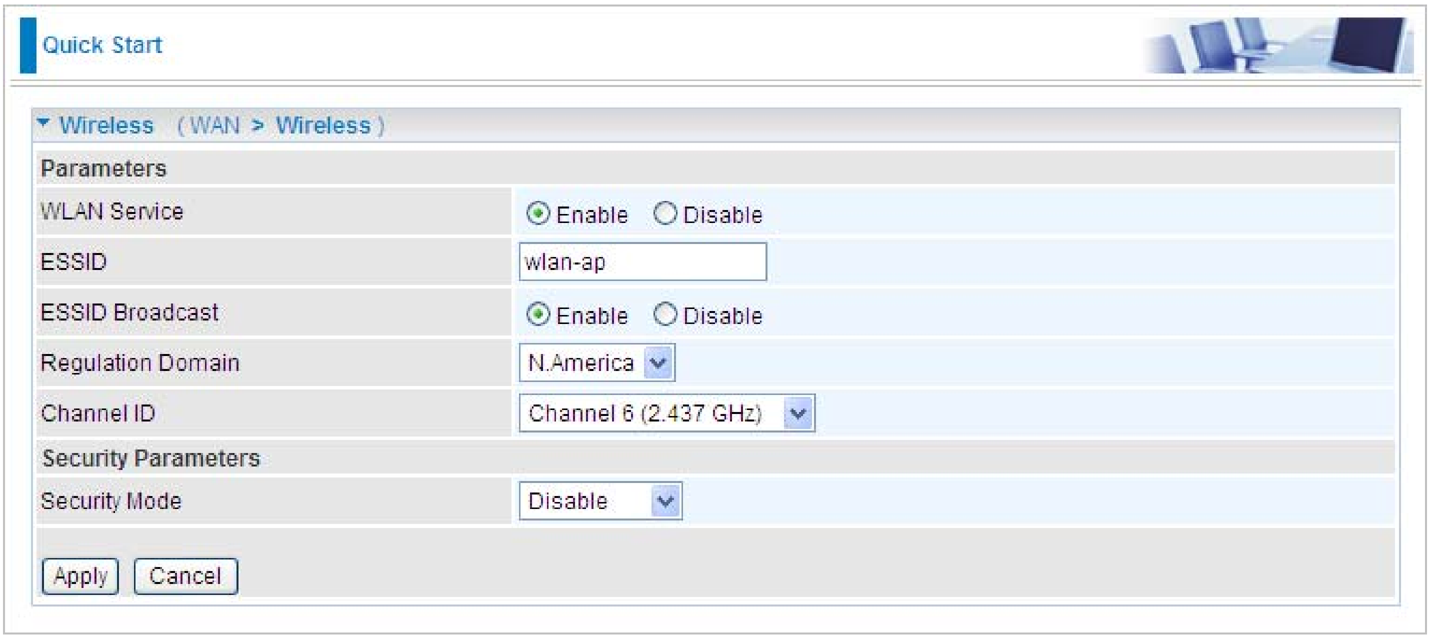
Service Name: This item is for identification purposes. If it is required, your ISP provides you the information.

Auth Protocol: Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**

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

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

5. Configure the Wireless LAN setting



Quick Start

▾ Wireless (WAN > Wireless)

Parameters	
WLAN Service	● Enable ○ Disable
ESSID	wlan-ap
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	N.America
Channel ID	Channel 6 (2.437 GHz)
Security Parameters	
Security Mode	Disable

WLAN Service: Default setting is set to **Enable**. If you want to use wireless, both 802.11g and 802.11b device in your network, you can select **Enable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

ESSID Broadcast: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Enable.**

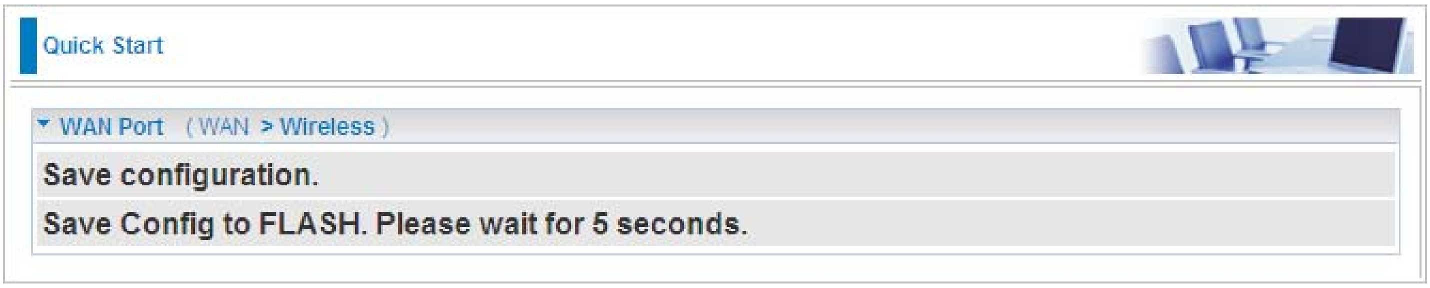
Enable: When Enable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Disable: Select Disable if you do not want broadcast your ESSID. When select Disable, no one will be able to locate the Access Point (AP) of your router.

Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

6. Wait for the configuration.

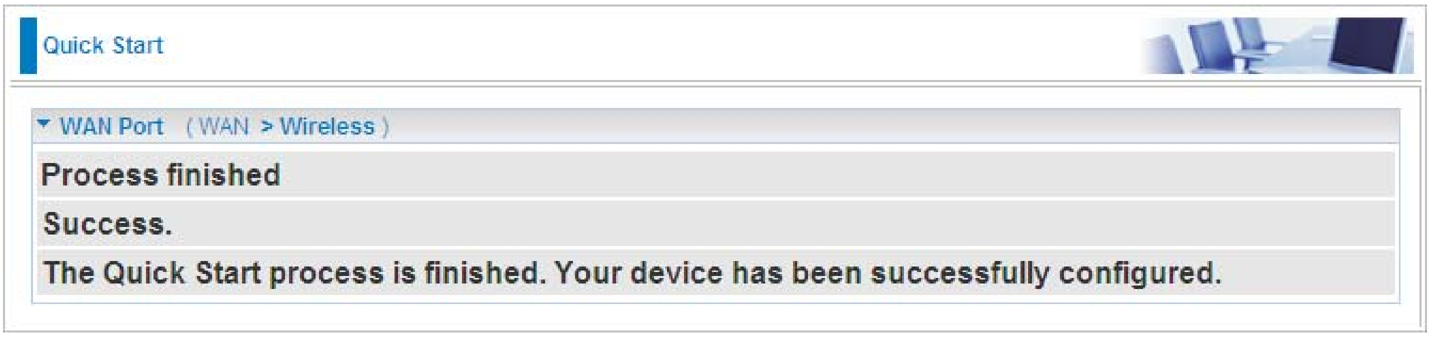


Quick Start

WAN Port (WAN > Wireless)

Save configuration.

Save Config to FLASH. Please wait for 5 seconds.



Quick Start

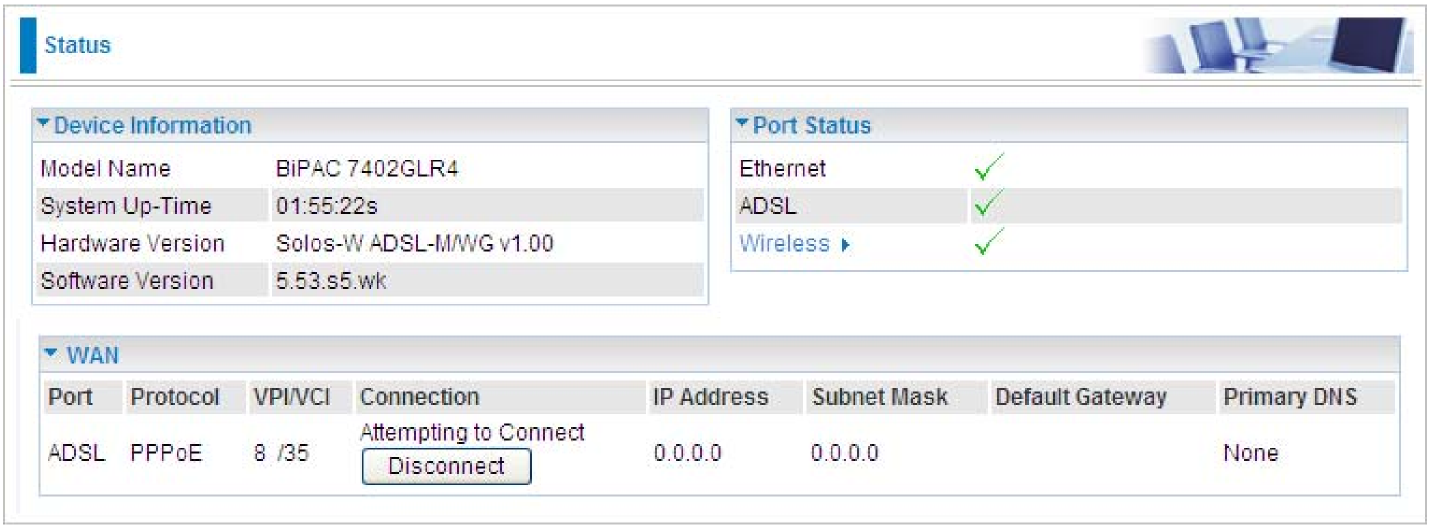
WAN Port (WAN > Wireless)

Process finished

Success.

The Quick Start process is finished. Your device has been successfully configured.

7. When ADSL is synchronic, it will appear “check”.



Status

Device Information

Model Name	BiPAC 7402GLR4
System Up-Time	01:55:22s
Hardware Version	Solos-W ADSL-M/WG v1.00
Software Version	5.53.s5.wk

Port Status

Ethernet	✓
ADSL	✓
Wireless ▸	✓

WAN

Port	Protocol	VPI/VCI	Connection	IP Address	Subnet Mask	Default Gateway	Primary DNS
ADSL	PPPoE	8 /35	Attempting to Connect Disconnect	0.0.0.0	0.0.0.0		None

Configuration

When you click this item, the column will expand to display the sub-items that will allow you to further configure your router.

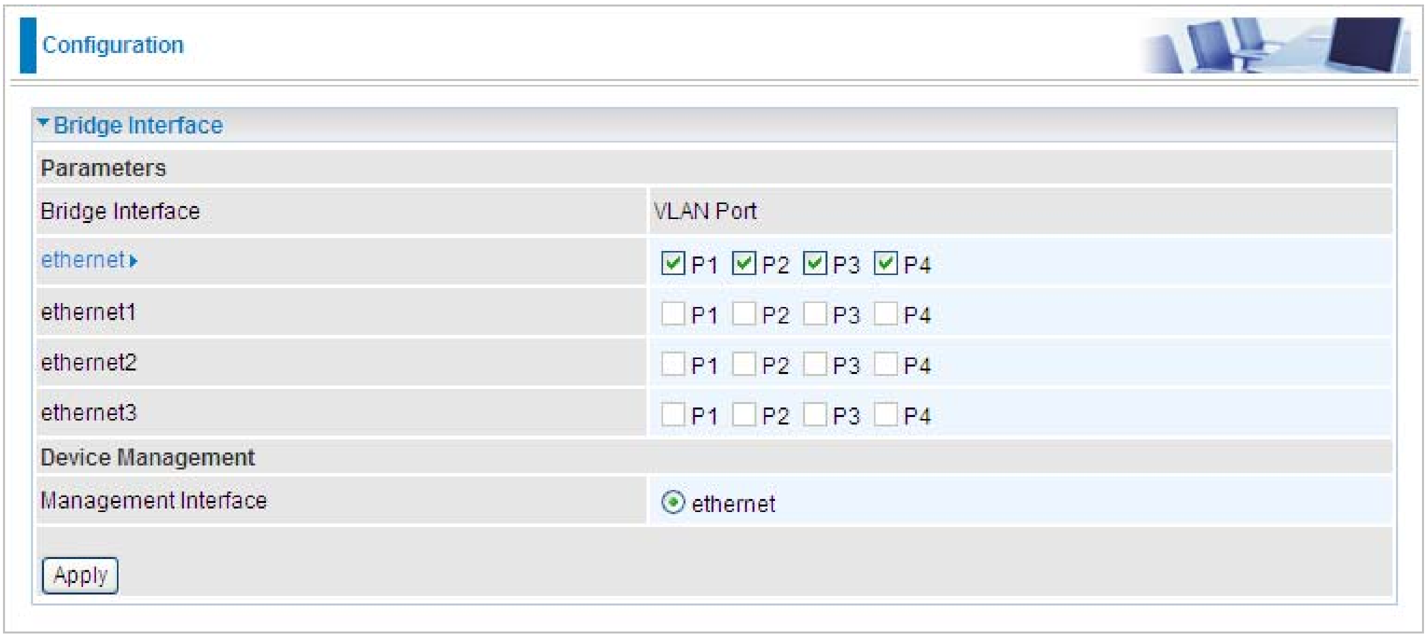
LAN, WAN, System, Firewall, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced

The function of each configuration sub-item is described in the following sections.

LAN - Local Area Network

Here are the items within the LAN section: **Ethernet, IP Alias, Ethernet Client Filter, Wireless, Wireless Security, Wireless Client Filter, WPS, Port Setting** and **DHCP Server.**

Bridge Interface



Configuration

▾Bridge Interface

Parameters

Bridge Interface	VLAN Port
ethernet▸	☑ P1 ☑ P2 ☑ P3 ☑ P4
ethernet1	□ P1 □ P2 □ P3 □ P4
ethernet2	□ P1 □ P2 □ P3 □ P4
ethernet3	□ P1 □ P2 □ P3 □ P4

Device Management

Management Interface	◉ ethernet

Apply

You can setup member ports for each VLAN group under Bridge Interface section. From the example, two VLAN groups need to be created.

Ethernet: P1 (Port 1)

Ethernet1: P2, P3 and P4 (Port 2, 3, 4). Uncheck P2, P3, P4 from Ethernet VLAN port first.

Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

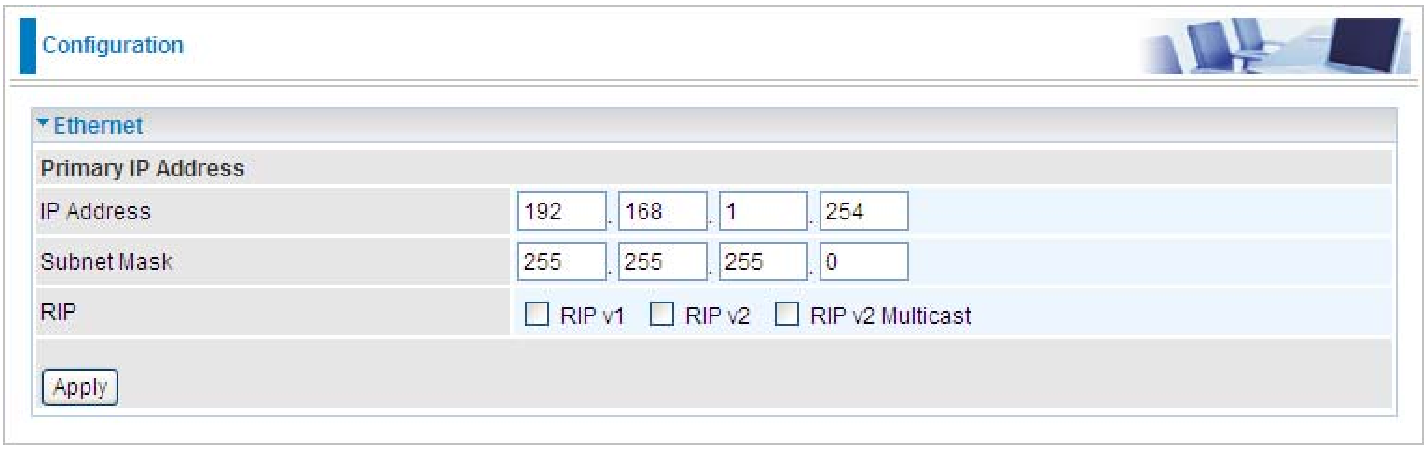
Bridge Interface	**VLAN Port (Always starts with)**
ethernet	P1 / P2 / P3 / P4
ethernet1	P2 / P3 / P4
ethernet2	P3 / P4
ethernet3	P4

Management Interface: To specify which VLAN group has possibility to do device management, like doing web management.

Note: NAT/NAPT can be applied to management interface only.

Ethernet

The router supports more than one Ethernet IP addresses in the LAN that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



Configuration

Ethernet

Primary IP Address	
IP Address	192 . 168 . 1 . 254
Subnet Mask	255 . 255 . 255 . 0
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast

Primary IP Address

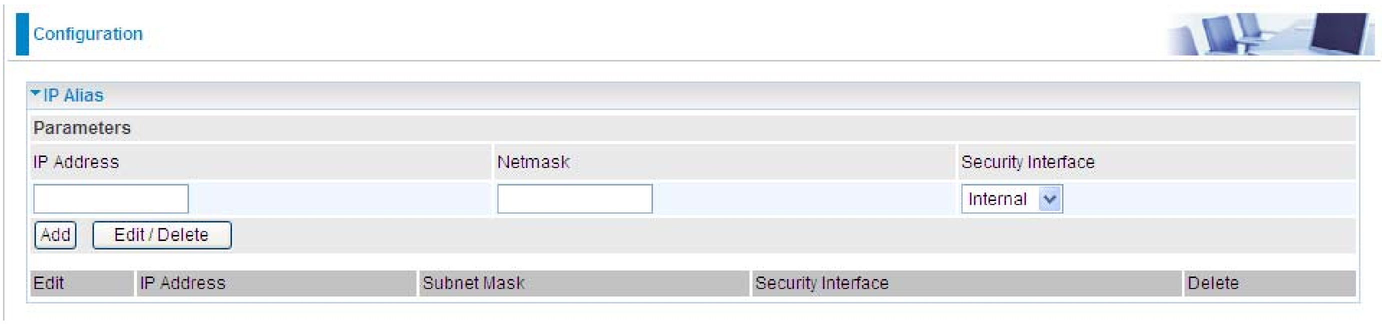
IP Address: The default IP on this router.

Subnet Mask: The default subnet mask on this router.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

IP Alias

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



Configuration

IP Alias

Parameters

IP Address	Netmask	Security Interface
		Internal

Edit	IP Address	Subnet Mask	Security Interface	Delete

IP Address: Specify an IP address for this virtual interface.

Netmask: Specify a subnet mask for this virtual interface.

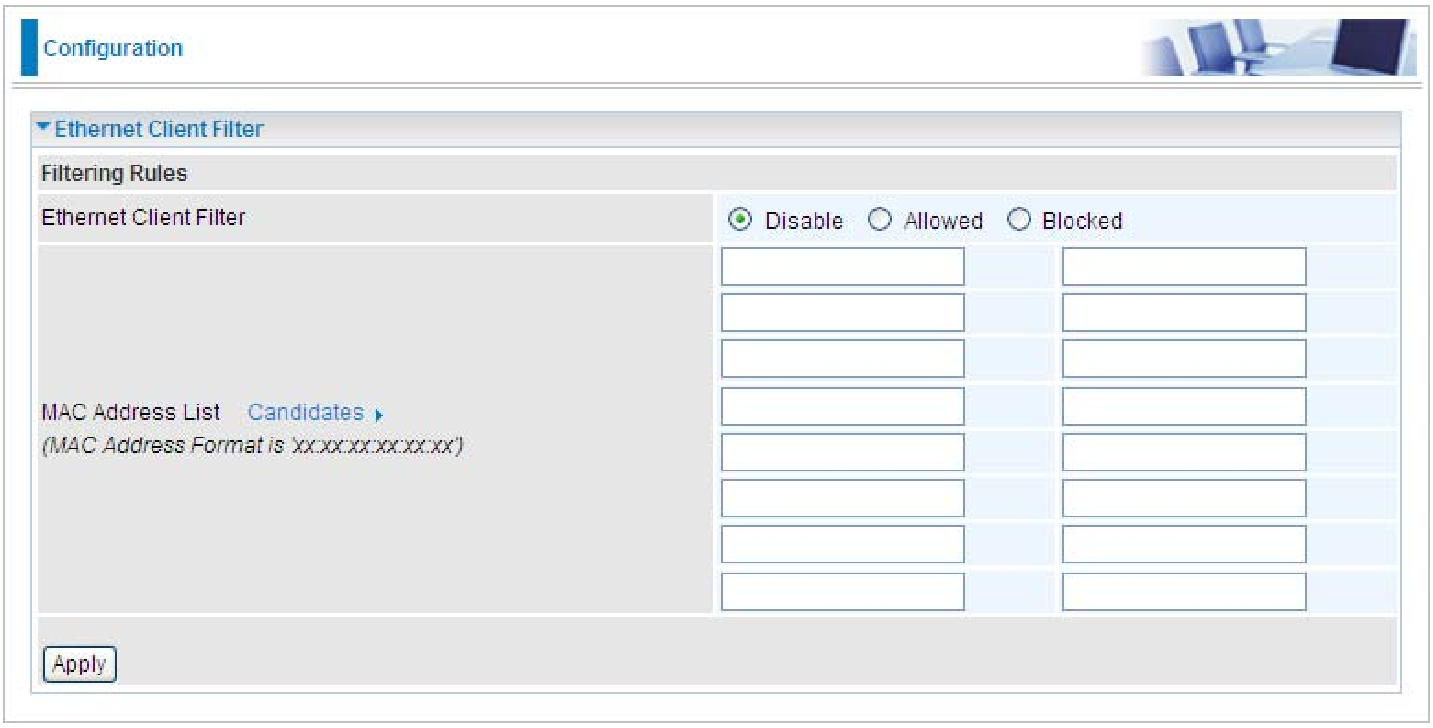
Security Interface: Specify the firewall setting for this virtual interface.

> **Internal:** This mean the network is behind NAT. All traffic will do network address translation when sending out data to the Internet if NAT is enabled.
>
> **External:** This means there is no NAT on this IP interface and it is connected directly to the Internet. This function is mostly used when you are provided with multiple public IP addresses by the ISP. In this case, you can use the public IP address in the local network whose gateway IP address points to the IP address on this interface.
>
> **DMZ:** Specify this network to a DMZ area. There is no NAT on this interface.

Ethernet Client Filter

The Ethernet Client Filter can support up to 16 Ethernet network computers. It enables you to accept traffic from specific authorized computers or can restrict unwanted computer(s) to access your LAN.

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



Configuration

Ethernet Client Filter

Filtering Rules

Ethernet Client Filter	● Disable ○ Allowed ○ Blocked
MAC Address List Candidates (MAC Address Format is 'xx:xx:xx:xx:xx:xx')	

Apply

Ethernet Client Filter: Default setting is set **Disable**.

Allowed: check to enable a specific PC to access your LAN by inserting the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.

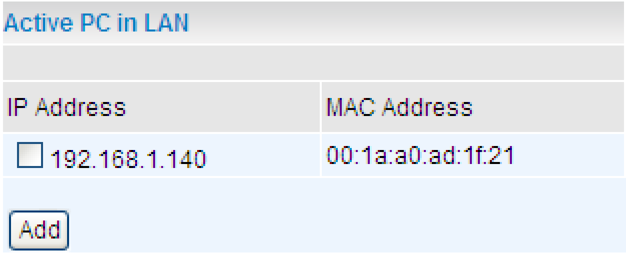
Blocked: check to prevent an unwanted PC from accessing your LAN by inserting the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is not listed.

The maximum number of client is 16. The MAC addresses should be 6 bytes long and are presented only in hexadecimal characters. Only numbers (0 - 9) and letters (a - f) are acceptable.

Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.

Candidates: automatically detects devices that are connected to the router through the Ethernet.

Click the Candidate button to access the **Active PC in LAN** window.



Active PC in LAN

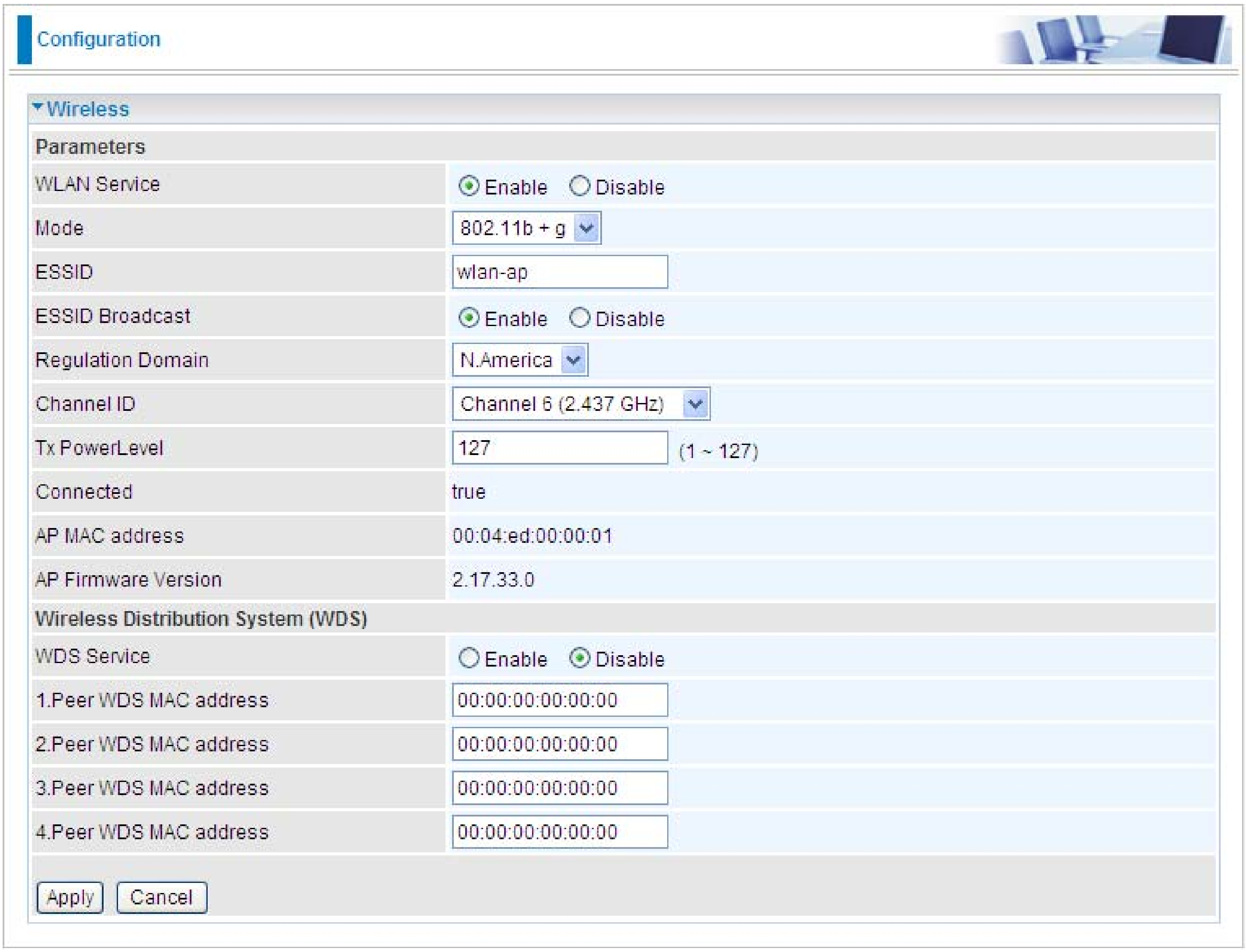
IP Address	MAC Address
□ 192.168.1.140	00:1a:a0:ad:1f:21

Add

Active PC in LAN: Active PC in LAN window displays a list of IP Address & MAC Address of each Ethernet device which connects to the router.

You can check the checkbox next to the IP address to block or to allow the PC from accessing the LAN. Then, click Add to insert the IP to the Ethernet Client Filter table. The maximum number of supported Ethernet client is 16.

Wireless



Configuration

Wireless

Parameters	
WLAN Service	● Enable ○ Disable
Mode	802.11b + g
ESSID	wlan-ap
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	N.America
Channel ID	Channel 6 (2.437 GHz)
Tx PowerLevel	127 (1 ~ 127)
Connected	true
AP MAC address	00:04:ed:00:00:01
AP Firmware Version	2.17.33.0
Wireless Distribution System (WDS)	
WDS Service	○ Enable ● Disable
1.Peer WDS MAC address	00:00:00:00:00:00
2.Peer WDS MAC address	00:00:00:00:00:00
3.Peer WDS MAC address	00:00:00:00:00:00
4.Peer WDS MAC address	00:00:00:00:00:00

Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

Mode: The default setting is 802.11b+g (Mixed mode). If you do not know or do not have both 11g and 11b devices on your network, then keep the setting in mixed mode. From the drop-down menu, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b.

ESSID: The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change the default wlan-ap to a unique ID name that is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Note: It is case sensitive and must not exceed 32 characters.

ESSID Broadcast: It is used to broadcast its ESSID on the network so that when a wireless client searches for a network, the router can be discovered and recognized. Default setting is **Enable.**

> **Enable:** When enabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.
>
> **Disable:** When disabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection ID channel that you would like to use.

Note: Wireless performance may degrade if the selected ID channel is already being occupied by other AP(s).

TX PowerLevel: It is a function that enhances the wireless transmission signal strength. User may adjust this power level from minimum 1 up to maximum 100 or 127 depending on the models used. Please refer to the note table for the appropriate power level range of your model.

Note: The Power Level maybe different in each access network user premises environment so choose the most suitable level for your network.

Connected: Display either as true or false. That it is the connection status between the system and the build-in wireless card.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantage of the cost saving and flexibility with no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

WDS Service: The default setting is **Disabled.** Check **Enable** radio button to activate this function.

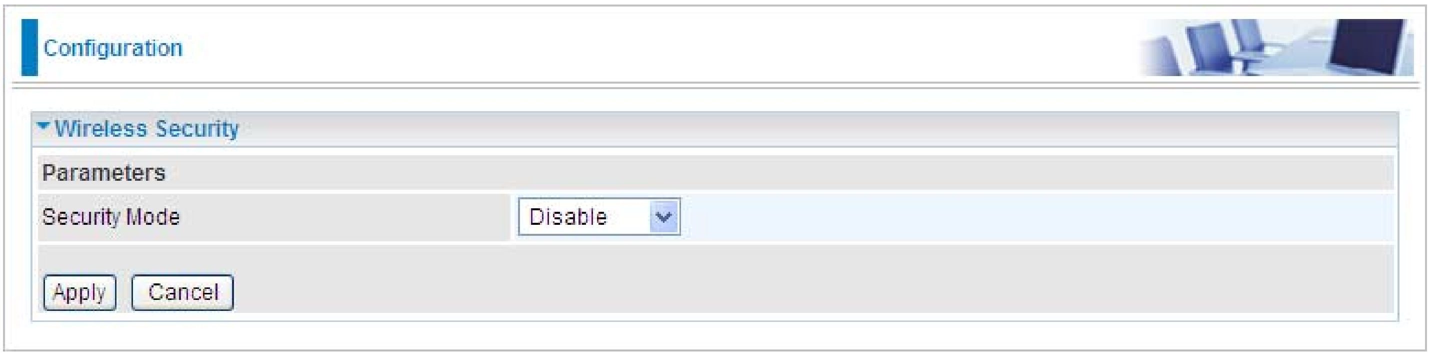
1. **Peer WDS MAC Address:** It is the associated AP MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.
2. **Peer WDS MAC Address:** It is the second associated AP MAC Address.
3. **Peer WDS MAC Address:** It is the third associated AP MAC Address.
4. **Peer WDS MAC Address:** It is the fourth associated AP MAC Address.

Note: For MAC Address, Semicolon (:) must be included.

Wireless Security

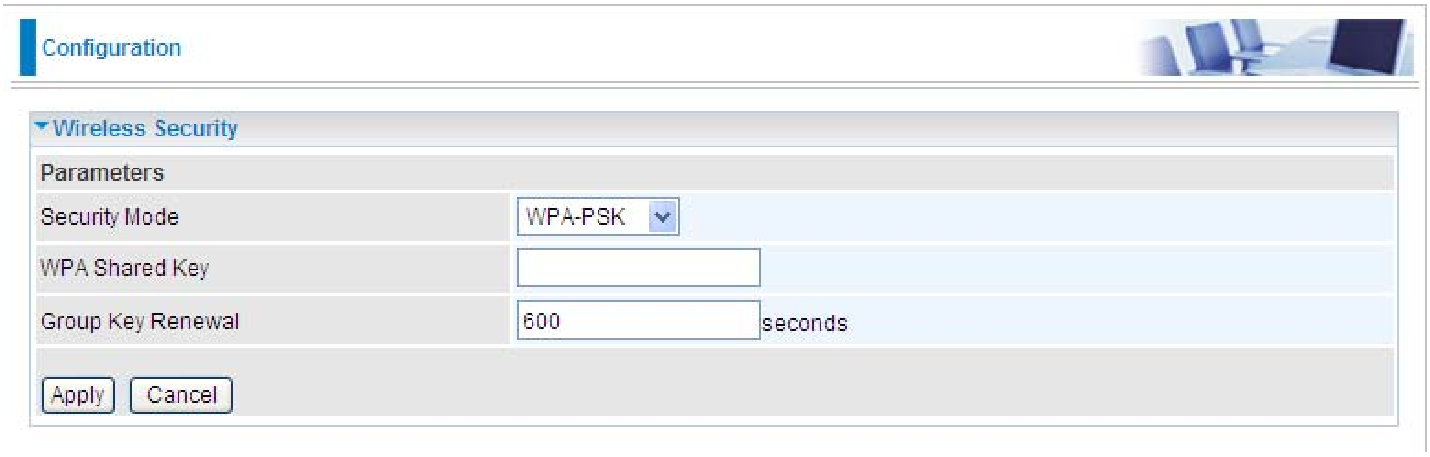
You can disable or enable the wireless security function using WPA or WEP for wireless network protection.

The default mode of wireless security is set to disabled.



Security Mode: Disable

WPA-PSK / WPA2-PSK



Security Mode: WPA-PSK

WPA Shared Key:

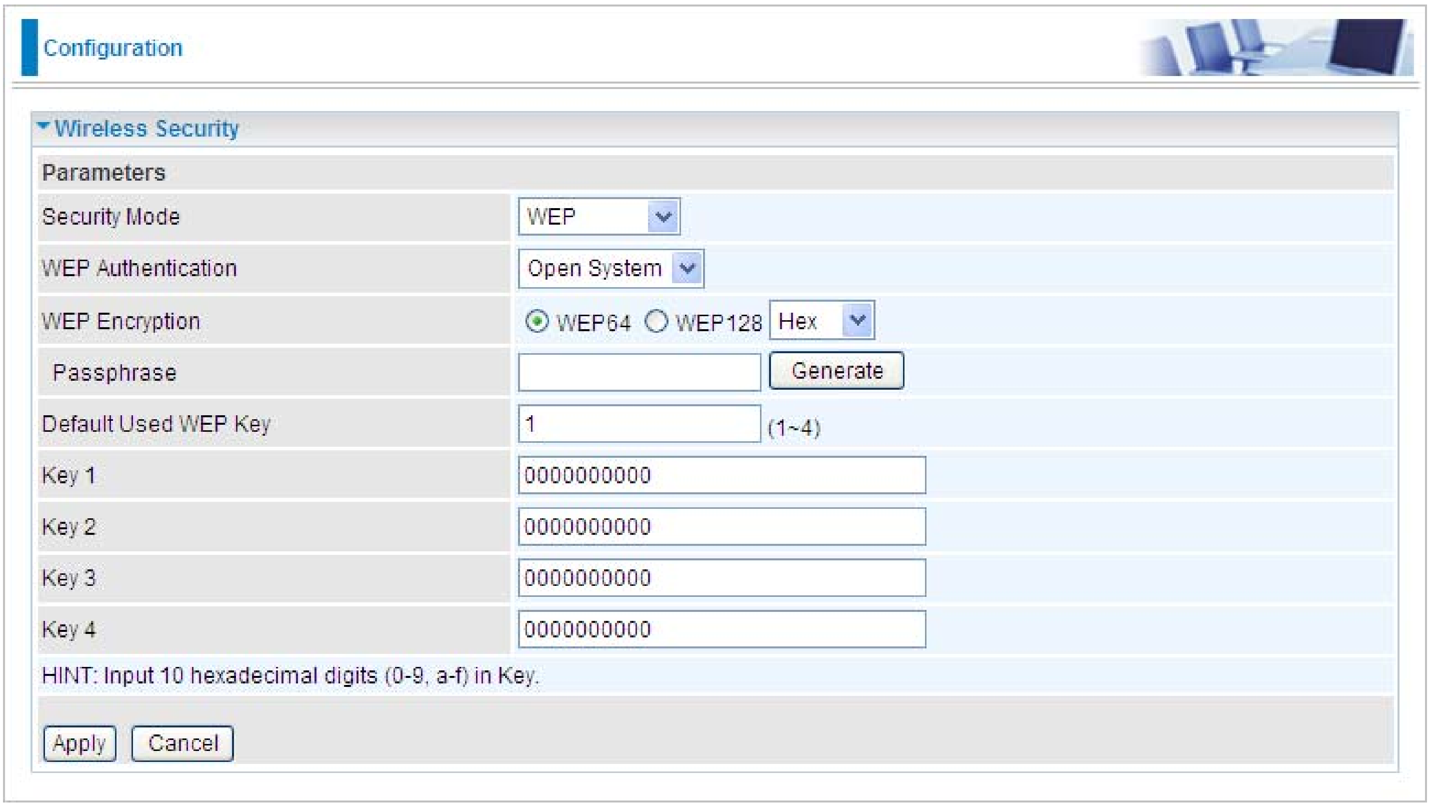
Group Key Renewal: 600 seconds

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is **600** seconds.

WEP



Configuration

▾Wireless Security

Parameters	
Security Mode	WEP
WEP Authentication	Open System
WEP Encryption	● WEP64 ○ WEP128 Hex
Passphrase	Generate
Default Used WEP Key	1 (1~4)
Key 1	0000000000
Key 2	0000000000
Key 3	0000000000
Key 4	0000000000

HINT: Input 10 hexadecimal digits (0-9, a-f) in Key.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are two options to select from: **Open System, Share key**.

WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

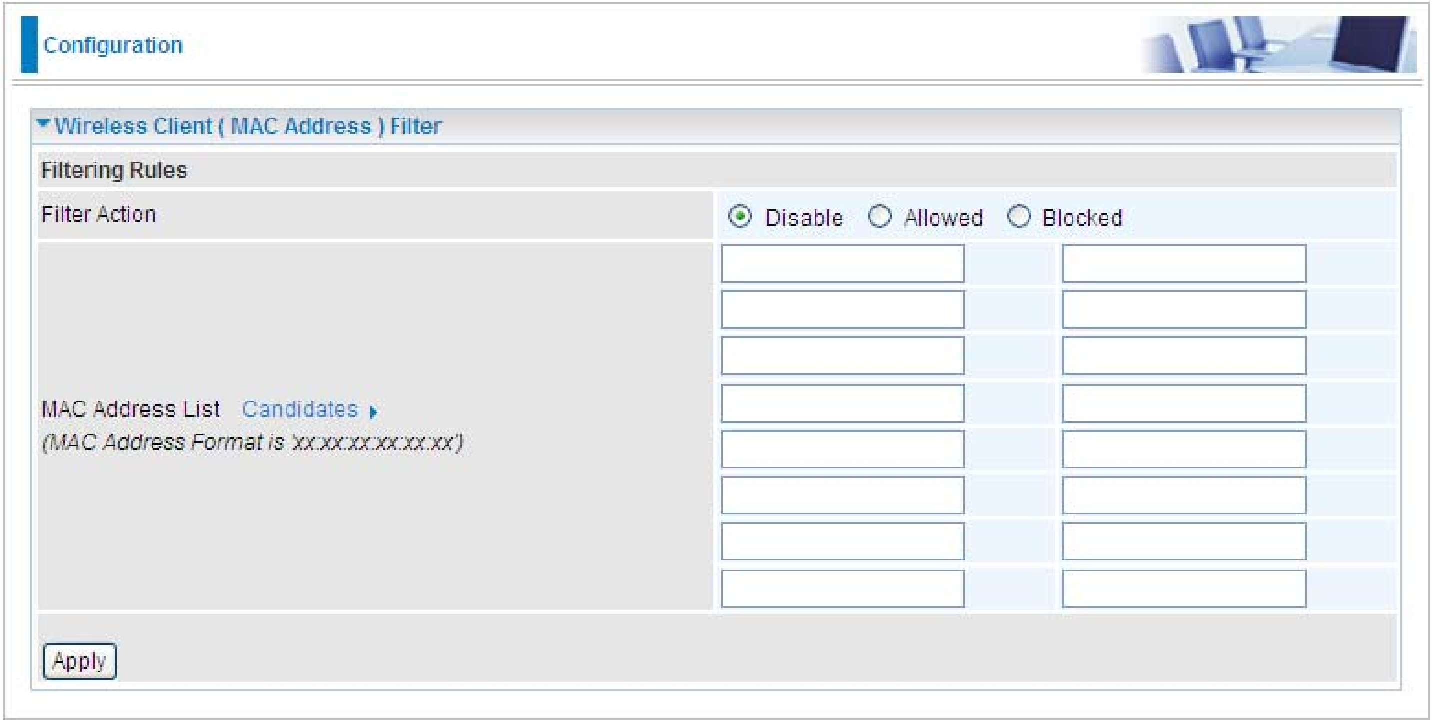
Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Wireless Client / MAC Address Filter

The MAC Address supports up to 16 wireless network PCs and helps you manage your network control to accept traffic from specific authorized PCs or to restrict unwanted PC(s) to access your LAN.

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



Configuration

▾Wireless Client (MAC Address) Filter

Filtering Rules

Filter Action	● Disable ○ Allowed ○ Blocked
MAC Address List Candidates ▸ (MAC Address Format is 'xx:xx:xx:xx:xx:xx')	

Filter Action: Default setting is set to **Disable**.

Allowed: To authorize specific device to access your LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.

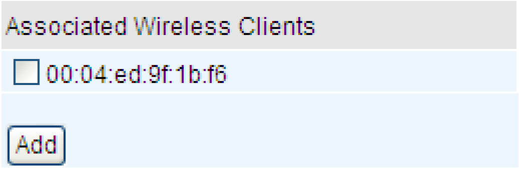
Blocked: To prevent unwanted device from accessing the LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is not listed.

The maximum client is 16. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number **0 - 9** and letters **a - f** are acceptable.

Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx. Semicolon (:) must be included.

Candidates: It automatically detects for devices that are connected to the router through the Wireless feature.

Click the Candidate button to access the **Associated Wireless Client** window.



Associated Wireless Clients

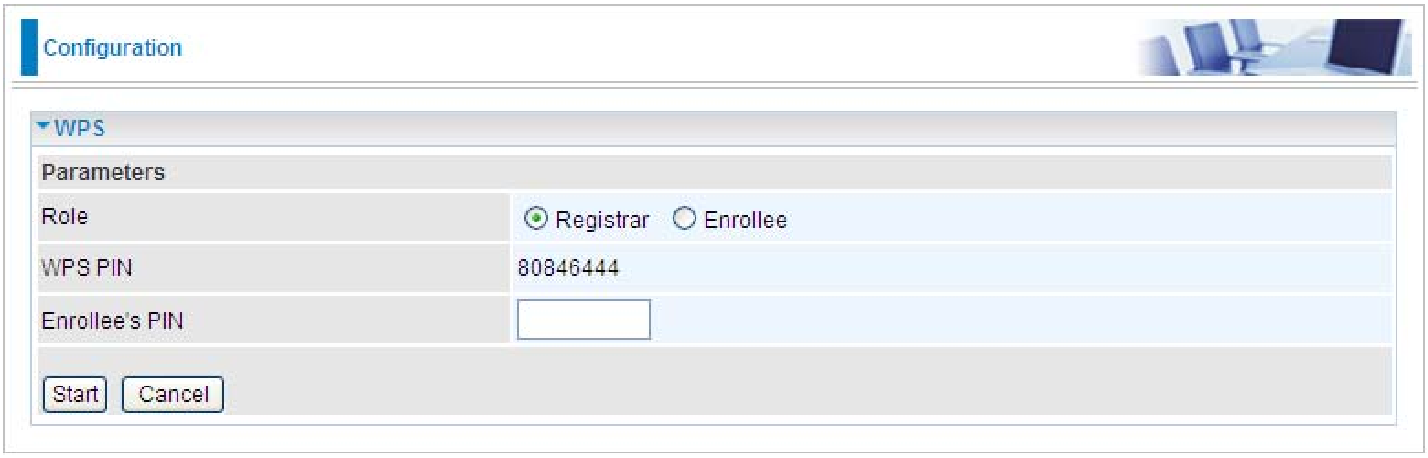
□ 00:04:ed:9f:1b:f6

Associate Wireless Client: Displays a list MAC addresses of all wireless devices that are currently connected to the router.

You can check the checkbox next to the MAC address to block or allow the wireless client to access the network. Then, Add to insert to the Wireless Client (MAC Address) Filter table. The maximum Wireless client is 16.

WPS

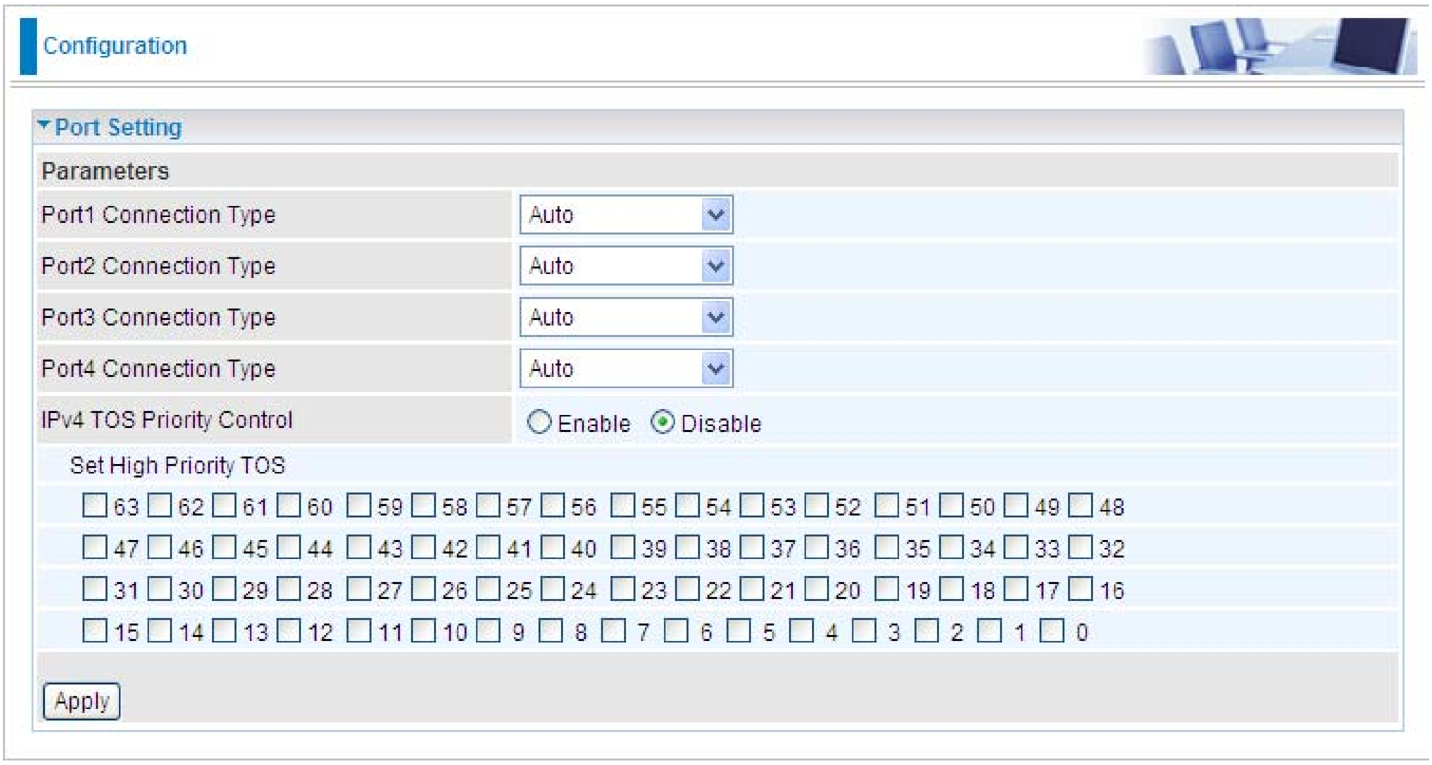
WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This protocol is used to build a Wi-Fi networks within a home / small office environment in an easy and secured manner. This feature thus provides a much simplified method to configure WiFi Protected Access to those who know very little about wireless security.



Parameters	
Role	● Registrar ○ Enrollee
WPS PIN	80846444
Enrollee's PIN	

Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



Configuration

▾Port Setting

Parameters	
Port1 Connection Type	Auto
Port2 Connection Type	Auto
Port3 Connection Type	Auto
Port4 Connection Type	Auto
IPv4 TOS Priority Control	○ Enable ● Disable

Set High Priority TOS

□ 63 □ 62 □ 61 □ 60 □ 59 □ 58 □ 57 □ 56 □ 55 □ 54 □ 53 □ 52 □ 51 □ 50 □ 49 □ 48

□ 47 □ 46 □ 45 □ 44 □ 43 □ 42 □ 41 □ 40 □ 39 □ 38 □ 37 □ 36 □ 35 □ 34 □ 33 □ 32

□ 31 □ 30 □ 29 □ 28 □ 27 □ 26 □ 25 □ 24 □ 23 □ 22 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16

□ 15 □ 14 □ 13 □ 12 □ 11 □ 10 □ 9 □ 8 □ 7 □ 6 □ 5 □ 4 □ 3 □ 2 □ 1 □ 0

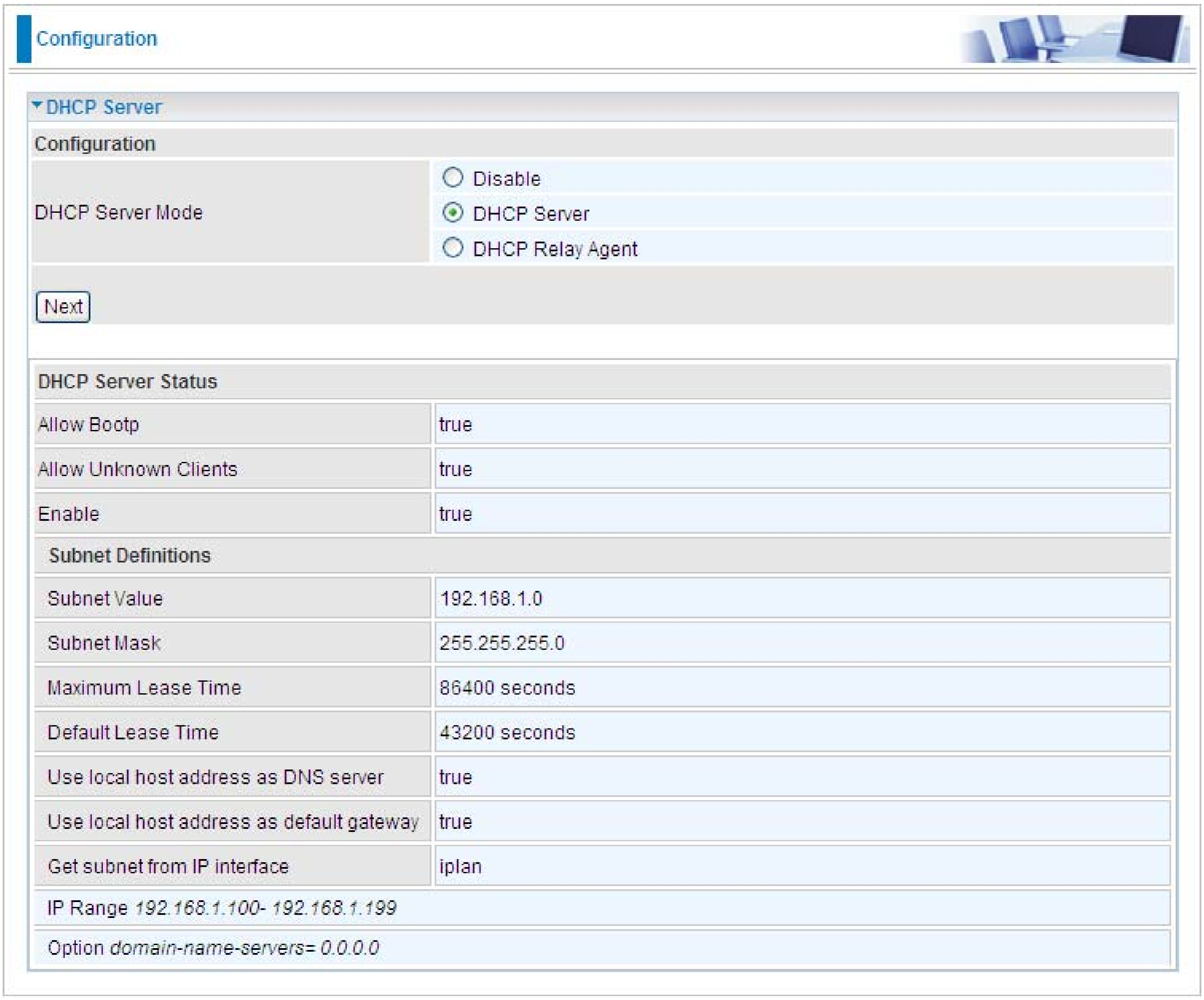
Port # Connection Type: There are Six options to choose from: Auto, disable, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility issues. The default is Auto, which users should keep unless there are specific problems with PCs not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

This feature uses bits 0-5 to classify the packet's priority. If the packet priority is set as high, its transmission will be given the first priority it will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will first check the 2nd octet of each IP packet. If the value in the TOS field matches the values checked in the table (0 to 63), this packet will be treated as high priority.

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 the PCs on your network if they are configured to obtain IP addresses automatically.



Configuration

DHCP Server Mode: ○ Disable ● DHCP Server ○ DHCP Relay Agent

Next

DHCP Server Status	
Allow Bootp	true
Allow Unknown Clients	true
Enable	true
Subnet Definitions	
Subnet Value	192.168.1.0
Subnet Mask	255.255.255.0
Maximum Lease Time	86400 seconds
Default Lease Time	43200 seconds
Use local host address as DNS server	true
Use local host address as default gateway	true
Get subnet from IP interface	iplan
IP Range *192.168.1.100- 192.168.1.199*	
Option *domain-name-servers= 0.0.0.0*	

To disable the router DHCP Server, check Disabled and click Next, then click Apply. When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (by default this is 192.168.1.254).

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

If you check DHCP Relay Agent and click Next, then you will have to enter the IP address of the DHCP server which will assign 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.

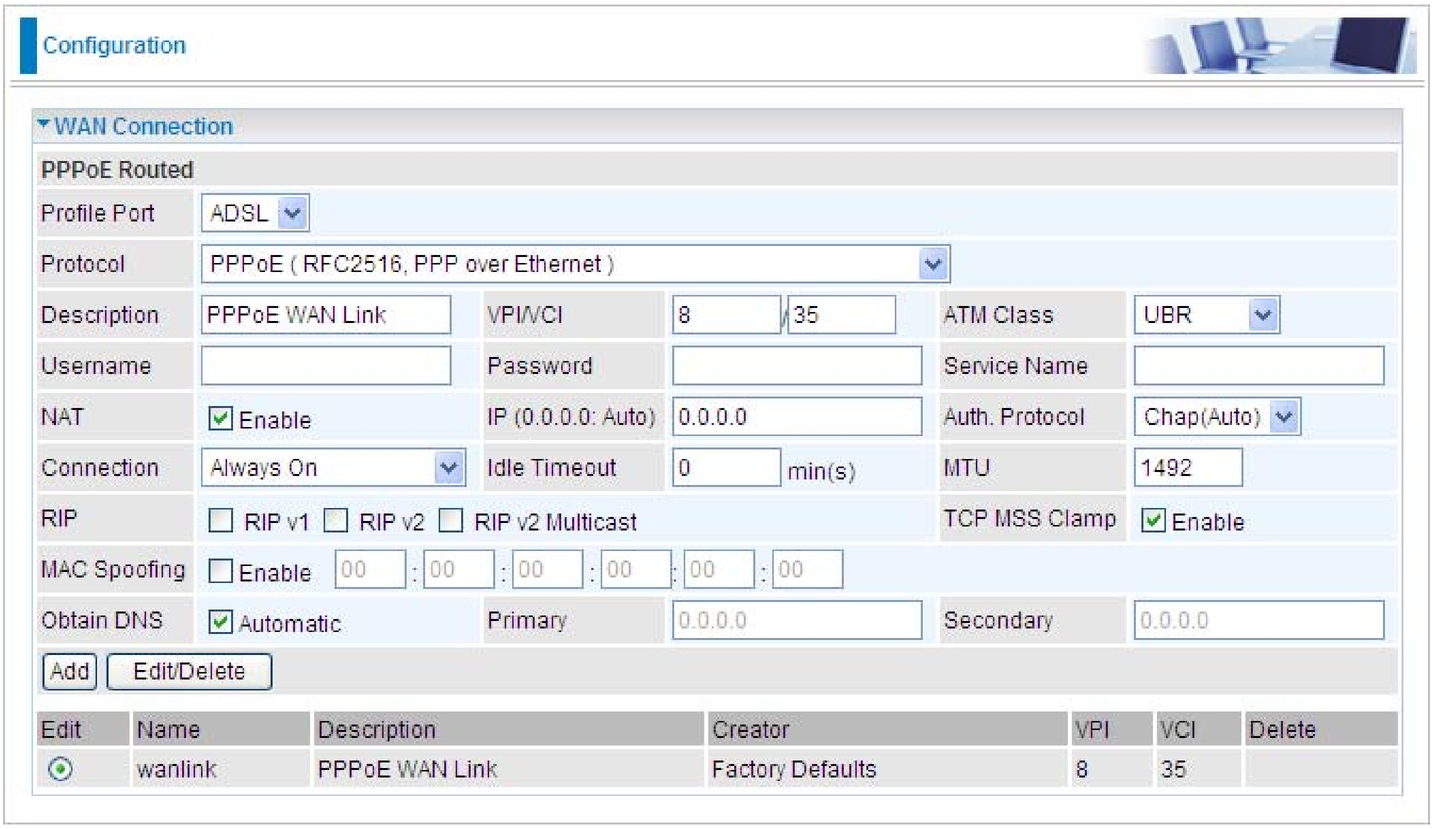
WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router’s connection to your ISP and the Internet. Here is the item within the WAN section: **WAN Profile.**

WAN Profile

PPPoE Connection

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



▾WAN Connection

PPPoE Routed					
Profile Port	ADSL				
Protocol	PPPoE (RFC2516, PPP over Ethernet)				
Description	PPPoE WAN Link	VPI/VCI	8 / 35	ATM Class	UBR
Username		Password		Service Name	
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Chap(Auto)
Connection	Always On	Idle Timeout	0 min(s)	MTU	1492
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
MAC Spoofing	□ Enable 00 : 00 : 00 : 00 : 00 : 00				
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

Add Edit/Delete

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoE WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive). This is the format of username “username@ispname” instead of “username”.

Password: Enter the password provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

Service Name: This item is for identification purpose. If it is required, your ISP will provide you the information. Maximum input is 15 alpha-numeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

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

Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

Connection:

> **Always on:** If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
>
> **Connect on Demand:** If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

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

> **Detail:** You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

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

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

MAC Spoofing: Some service providers require the configuring of this option. You must fill in the MAC address that is specified by the service provider when it is required. Default is disabled.

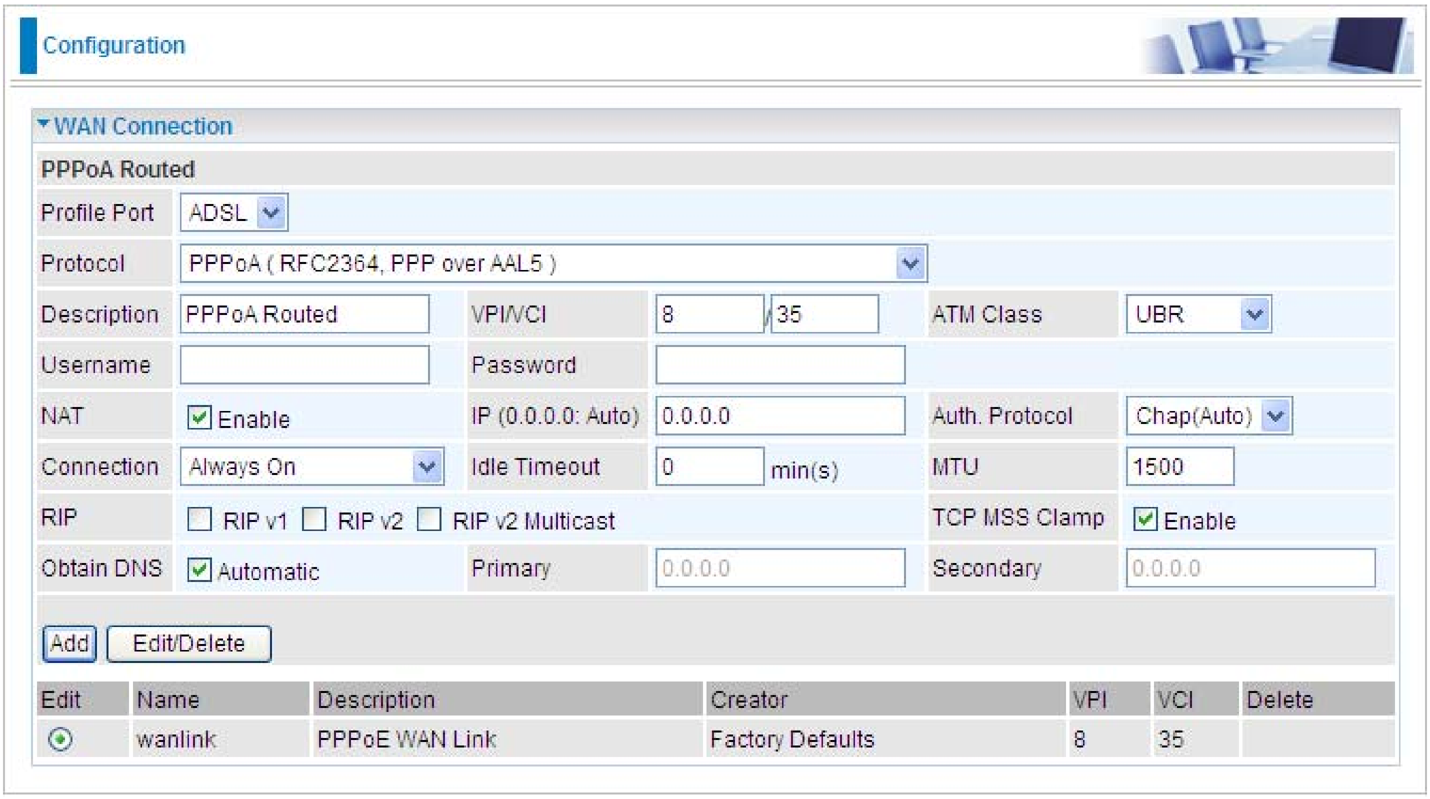
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

.

PPPoA Connection



Configuration

WAN Connection

PPPoA Routed

Profile Port	ADSL				
Protocol	PPPoA (RFC2364, PPP over AAL5)				
Description	PPPoA Routed	VPI/VCI	8 / 35	ATM Class	UBR
Username		Password			
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Chap(Auto)
Connection	Always On	Idle Timeout	0 min(s)	MTU	1500
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoE WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device..

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive). This is the format of username “username@ispname” instead of “username”.

Password: Enter the password provided by your ISP. You can input up to 128 alpha-numeric characters (case sensitive).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

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

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

Connection:

> **Always on:** If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
>
> **Connect on Demand:** If you want to establish a PPPoA session only when there is a packet

requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

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

Detail: You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

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

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

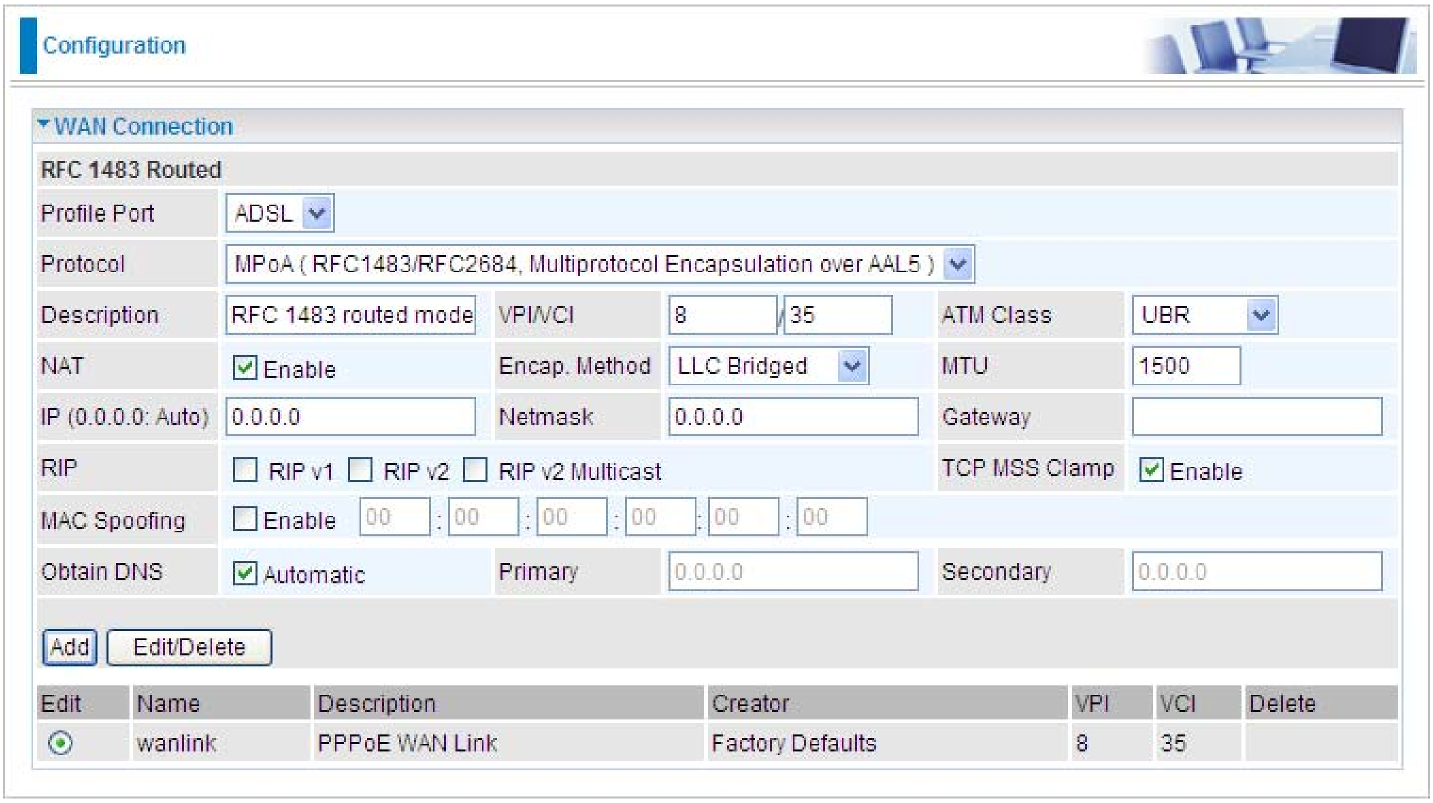
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

MPoA Connection

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



Configuration

▾WAN Connection

RFC 1483 Routed

Profile Port	ADSL				
Protocol	MPoA (RFC1483/RFC2684, Multiprotocol Encapsulation over AAL5)				
Description	RFC 1483 routed mode	VPI/VCI	8 / 35	ATM Class	UBR
NAT	☑ Enable	Encap. Method	LLC Bridged	MTU	1500
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	0.0.0.0	Gateway	
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
MAC Spoofing	□ Enable	00 : 00 : 00 : 00 : 00 : 00			
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoE WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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.

Encap. method: Choose whether you want the packets in WAN interface as bridged packet or routed packet.

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

IP (0.0.0.0:Auto): Specify an IP address allowed to logon and access the router’s web server.

Note: IP 0.0.0.0 indicates that all users who are connected to this router are allowed to logon the device and to modify data.

Netmask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway (if given).

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

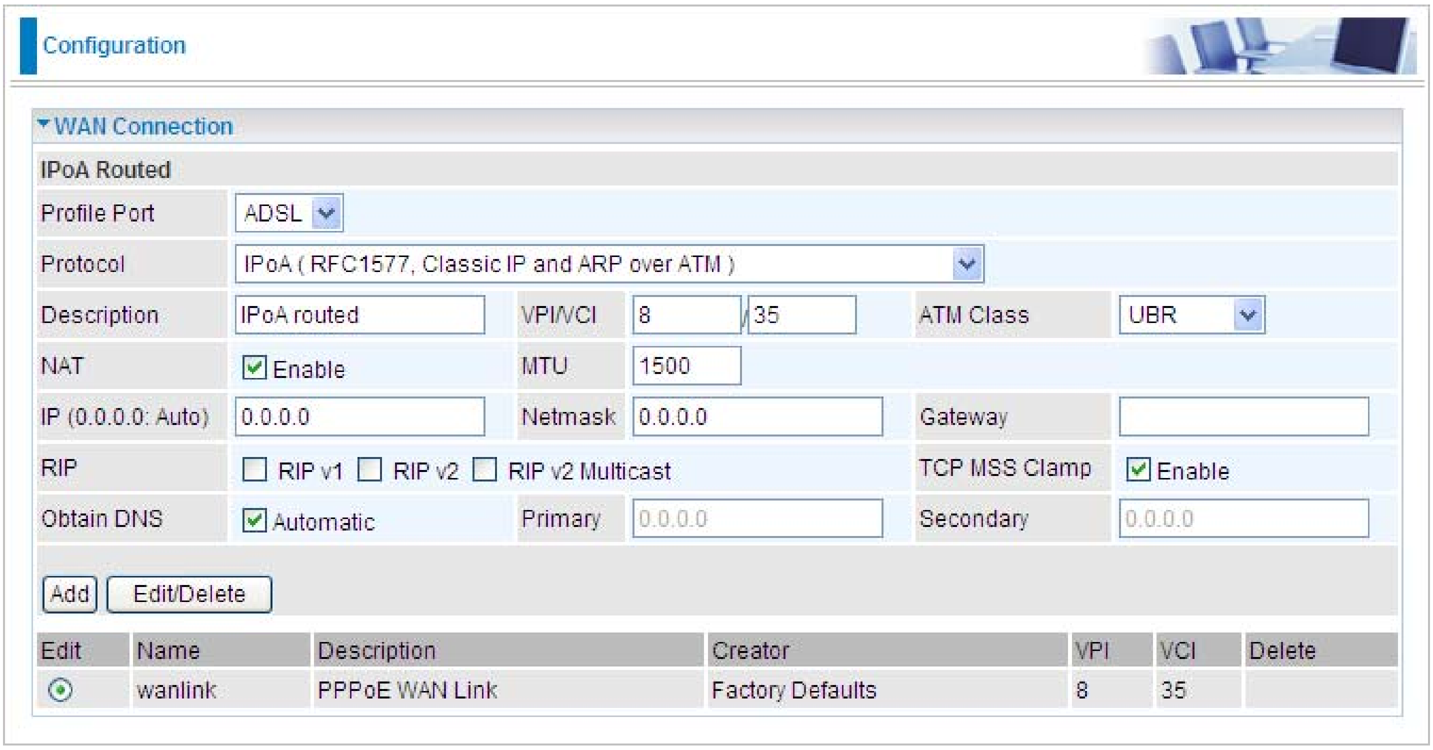
MAC Spoofing: Some service providers require the configuring of this option. You must fill in the MAC address that specify by service provider when it is required. Default is disabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

IPoA Routed Connection



IPoA Routed

Profile Port	ADSL				
Protocol	IPoA (RFC1577, Classic IP and ARP over ATM)				
Description	IPoA routed	VPI/VCI	8 / 35	ATM Class	UBR
NAT	☑ Enable	MTU	1500		
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	0.0.0.0	Gateway	
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoE WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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.

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

IP (0.0.0.0:Auto): Specify an IP address allowed to logon and access the router's web server.

Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.

Netmask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway (if given).

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

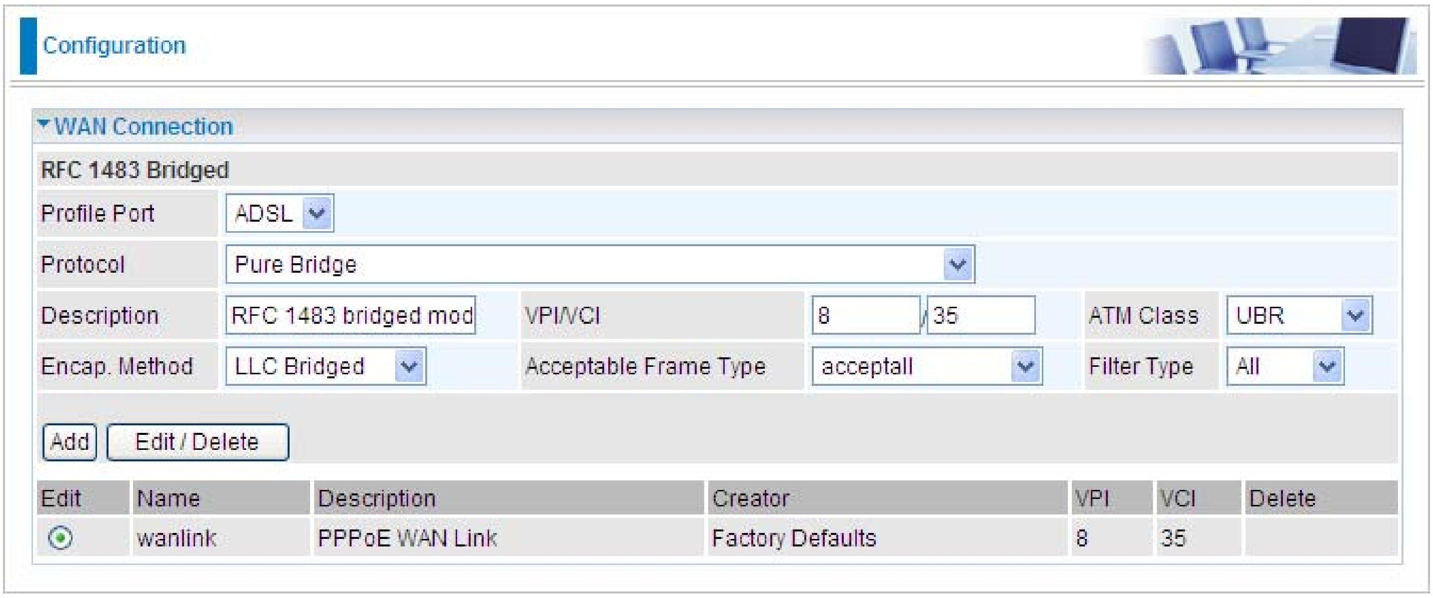
TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address of a specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS

Pure Bridge



Configuration

WAN Connection

RFC 1483 Bridged

Profile Port	ADSL				
Protocol	Pure Bridge				
Description	RFC 1483 bridged mod	VPI/VCI	8 / 35	ATM Class	UBR
Encap. Method	LLC Bridged	Acceptable Frame Type	acceptall	Filter Type	All

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoE WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for this connection.

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

ATM Class: The Quality of Service for ATM layer.

Encap. method: Choose whether you want the packets in WAN interface as bridged packet or routed packet.

Acceptable Frame Type: Specify which kind of traffic goes through this connection, all traffic or only VLAN tagged.

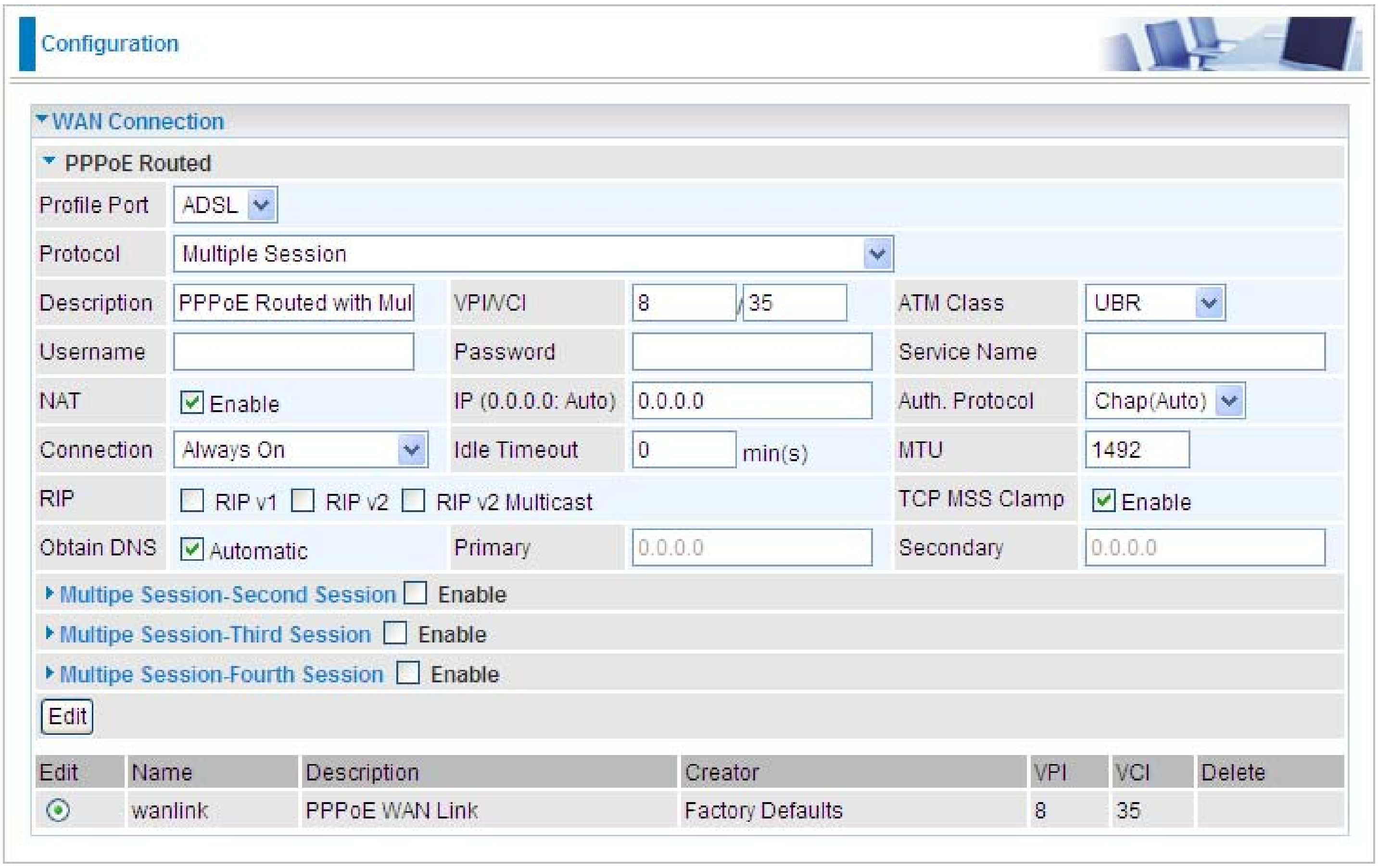
Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
IP	Allows only IP/ARP types of ethernet packets through the port.
PPPoE	Allows only PPPoE types of ethernet packets through the port.

Multiple Session

It allows user to have multiple PPPoE sessions on the same PVC. The device supports up to 4 sessions created at the same time. Also the user can still dial the PPPoE from the PC at the LAN network and no limitation of sessions.

Note: The maximum PPP session number is limited by ISP. And the device will use the first PPPoE sessions as default route, the user must create routing rules for other sessions manually.



Configuration

▼WAN Connection

▼ PPPoE Routed

Profile Port	ADSL				
Protocol	Multiple Session				
Description	PPPoE Routed with Mul	VPI/VCI	8 / 35	ATM Class	UBR
Username		Password		Service Name	
NAT	☑ Enable	IP (0.0.0.0: Auto)	0.0.0.0	Auth. Protocol	Chap(Auto)
Connection	Always On	Idle Timeout	0 min(s)	MTU	1492
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast			TCP MSS Clamp	☑ Enable
Obtain DNS	☑ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0

▸ Multipe Session-Second Session □ Enable

▸ Multipe Session-Third Session □ Enable

▸ Multipe Session-Fourth Session □ Enable

Edit

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoE WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

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

Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

Connection:

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

Connect on Demand: If you want to establish a multiple 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 broadband firewall gateway when there is no activity on the line for a predetermined period of time.

Detail: You can define the destination port and packet type (TCP/UDP) without checking by timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

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

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

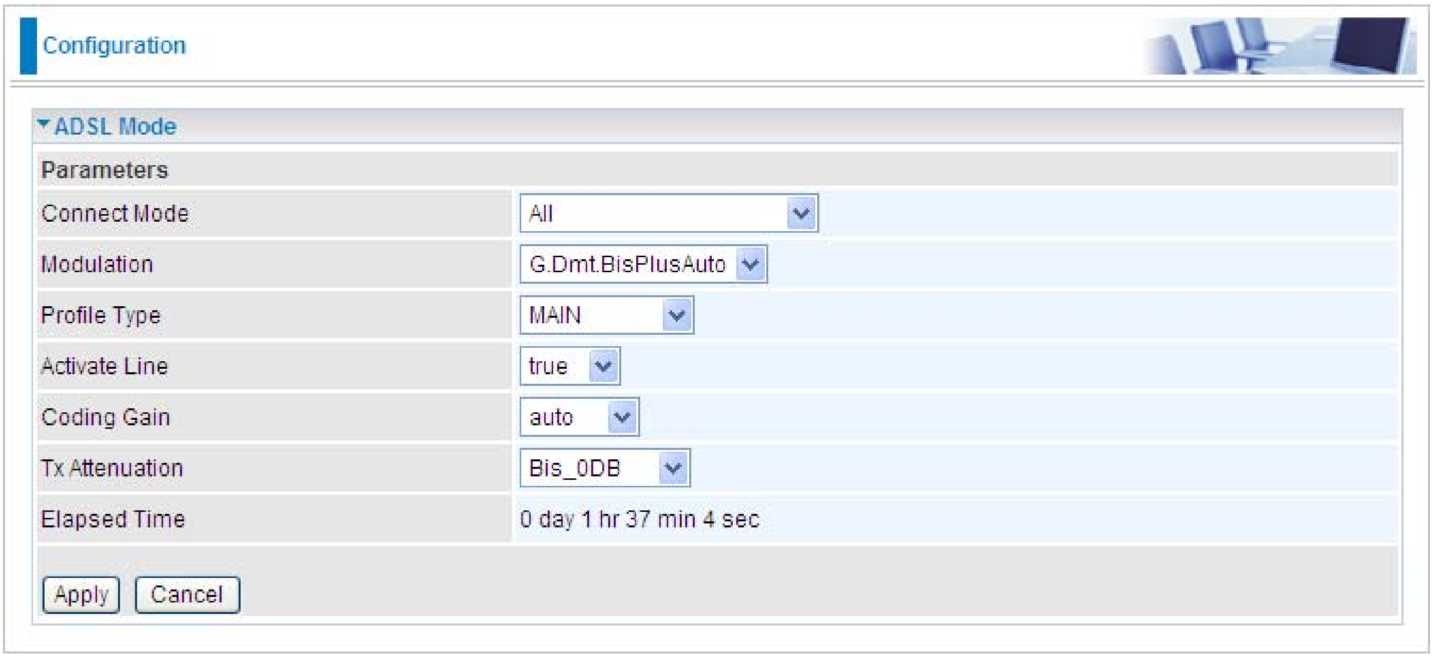
TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

ADSL Mode



Parameters	
Connect Mode	All
Modulation	G.Dmt.BisPlusAuto
Profile Type	MAIN
Activate Line	true
Coding Gain	auto
Tx Attenuation	Bis_0DB
Elapsed Time	0 day 1 hr 37 min 4 sec

Connect Mode: This mode will automatically detect your ADSL line code, ADSL2+, ADSL2, AnnexM2 and AnnexM2+, ADSL, All. Please keep the factory setting unless ADSL is detected as the symptom of synchronization problem.

Modulation: It will automatically detect capability of your ADSL line mode. Please keep the factory setting unless ADSL is detected as the symptom of synchronization problem.

Profile Type: Please keep the factory settings unless ADSL is detected as the symptom of low link rate or unstable problems. You may need to change the profile setting to reach the best ADSL line rate, it depends on the different DSLAM and location.

Activate Line: Aborting (false) your ADSL line and making it active (true) again for taking effect with setting of Connect Mode.

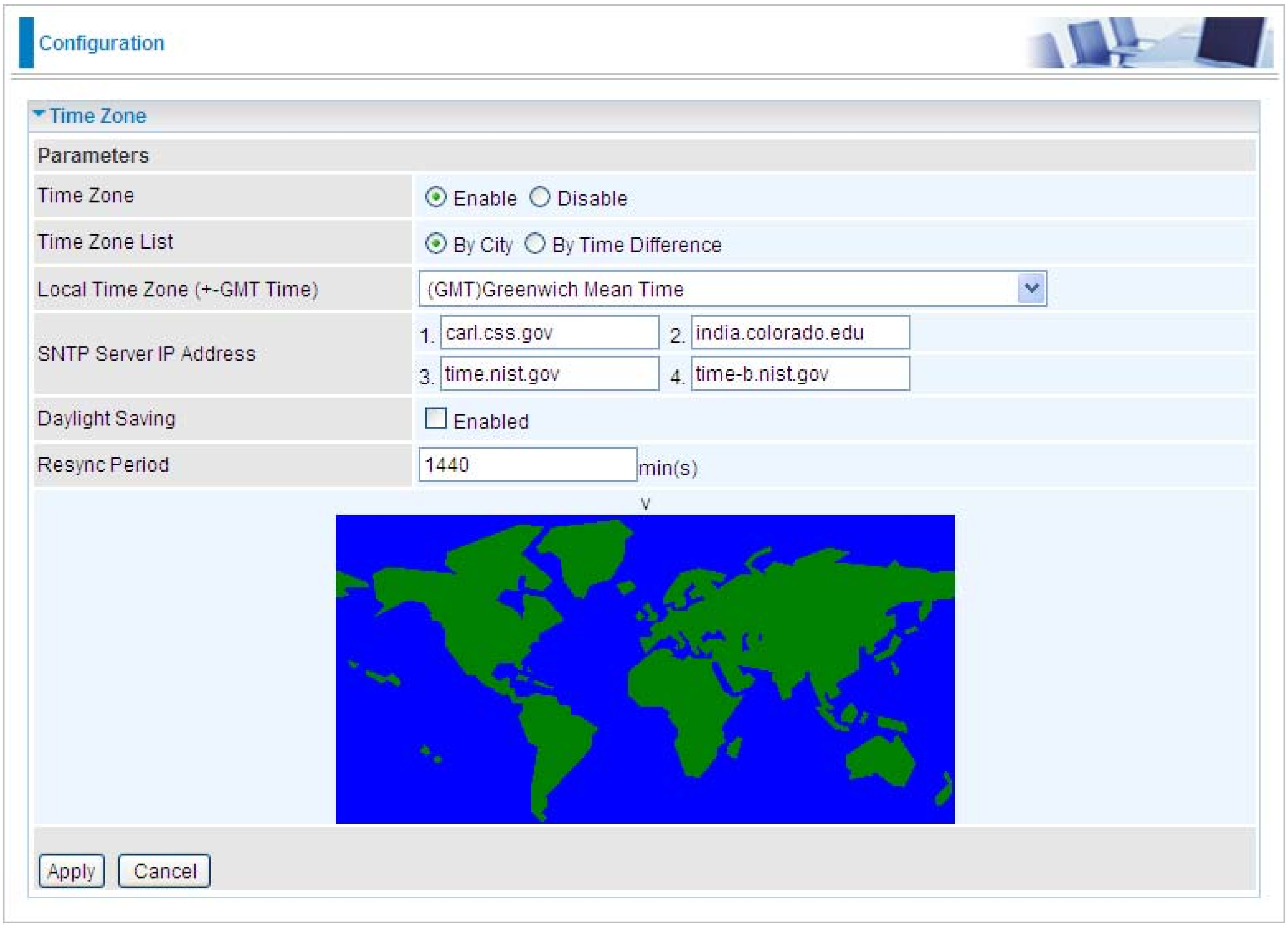
Coding Gain: It reduces router's transmit power which will effect to router's downstream performance. Higher the gain will increase the downstream rate but it sometimes causes unstable ADSL line. The configurable ADSL coding gain is from 0 dB to 7dB, or automatic.

Tx Attenuation: It is the amount of power that modem (upstream) or DSLAM (downstream) is using. The lower the power the better the performance will be in modem upstream.

System

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

Time Zone



Configuration

▾Time Zone

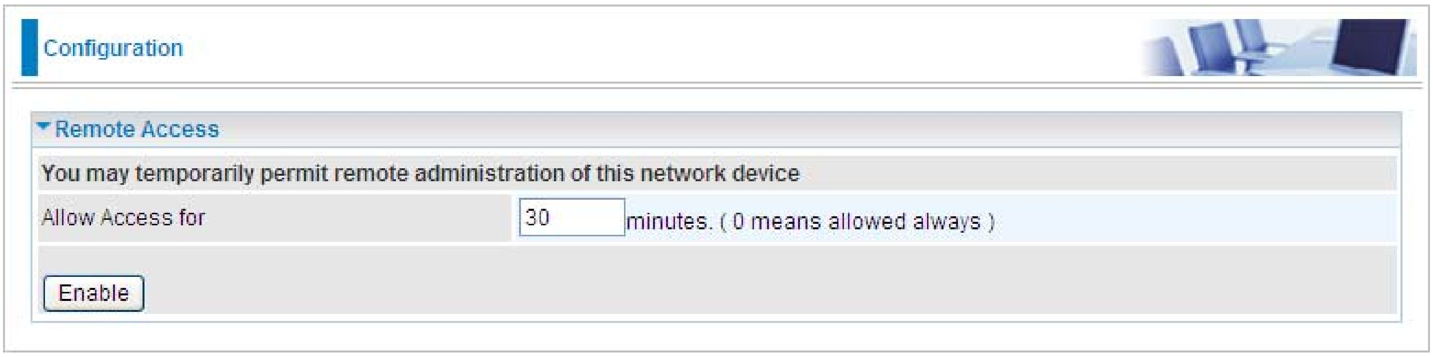
Parameters	
Time Zone	● Enable ○ Disable
Time Zone List	● By City ○ By Time Difference
Local Time Zone (+-GMT Time)	(GMT)Greenwich Mean Time
SNTP Server IP Address	1. carl.css.gov 2. india.colorado.edu 3. time.nist.gov 4. time-b.nist.gov
Daylight Saving	□ Enabled
Resync Period	1440 min(s)

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 will retrieve 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.

Daylight Saving is also known as Summer Time Period. Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check Enable checkbox to set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router’s time with that of the specified SNTP server. In order 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


Configuration

Remote Access

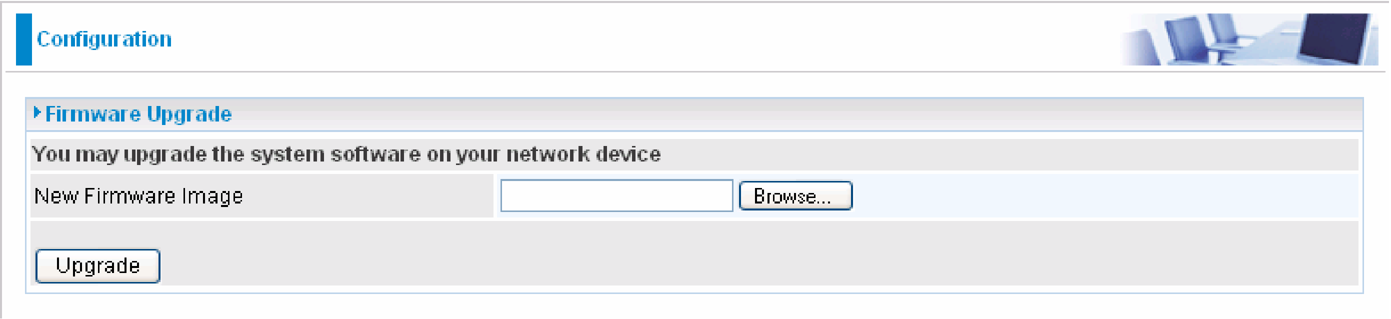
You may temporarily permit remote administration of this network device

Allow Access for: 30 minutes. (0 means allowed always)

This feature enables system administrator to set the time interval where the router can be accessed for administration purpose from a remote site (i.e. from outside your LAN).

If you wish to permanently enable remote access, set the time period to 0 minute.

Firmware Upgrade


Configuration

Firmware Upgrade

You may upgrade the system software on your network device

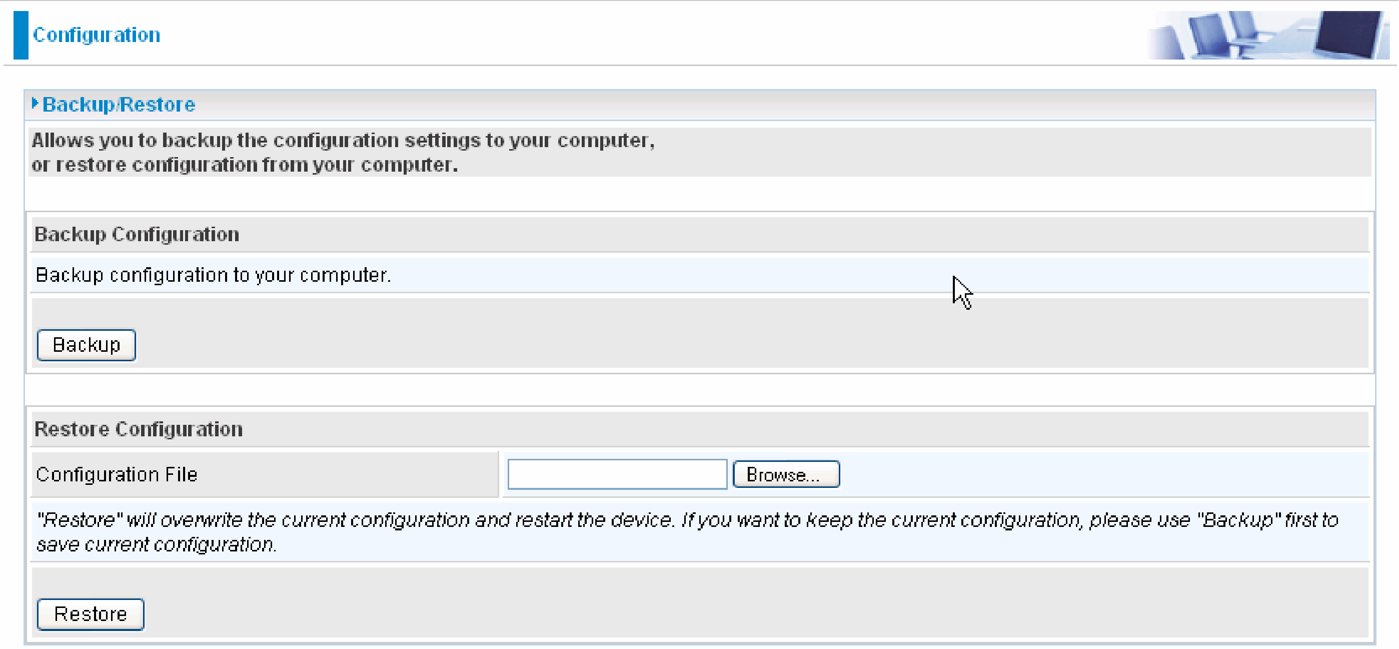
New Firmware Image:

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

Clicking on Browse will allow 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.

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Backup / Restore



Configuration

Backup/Restore

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

Backup Configuration

Backup configuration to your computer.

Restore Configuration

Configuration File

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

This function allows you to save a backup of the current configuration of your router to a file on your PC, or to restore a previously saved configuration. This is very useful if you wish to customize the setting of the router, knowing in advance that you can always restore the setting if any mistakes do occur. Therefore, It is advisable that you create a backup of the configuration of your router before customizing its configuration.

Create a Router Configuration Backup

To create a backup of the setting, simply press the Backup button and specify the location on where to save your configuration file. You may also change the name of the file if you wish to keep multiple backups.

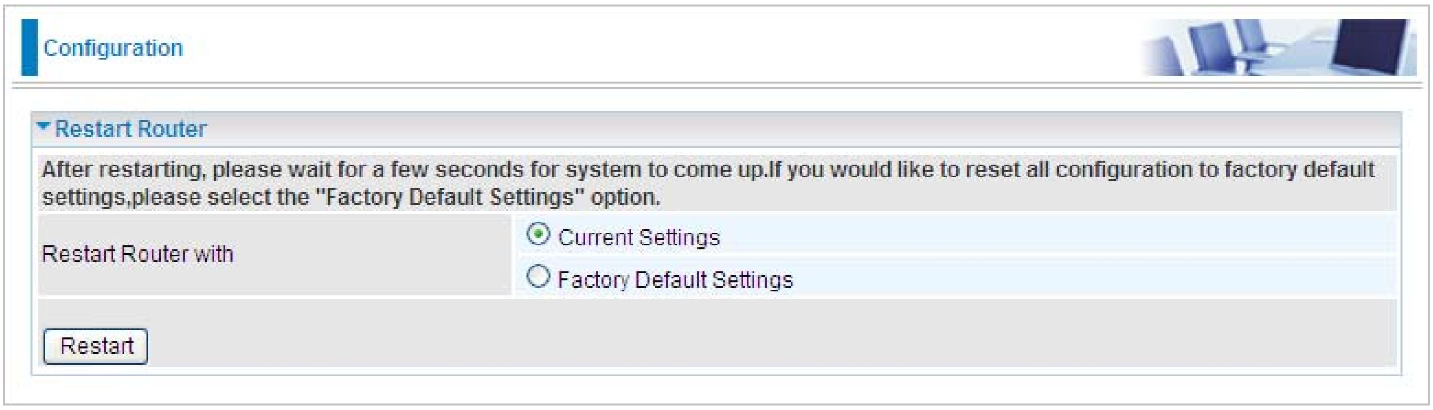
Restoring the Router Configuration

To restore the configuration of the router, press Browse to locate the configuration file from your PC. Once the file has been located, click on the file then click on the Restore button to load the setting.

Note: You should only restore the setting with the files that have been created using the Backup function with the most current firmware version. Settings files saved to your PC should not be manually edited in any way.

Restart Router

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



Restart Router

After restarting, please wait for a few seconds for system to come up.If you would like to reset all configuration to factory default settings,please select the "Factory Default Settings" option.

Restart Router with ● Current Settings ○ Factory Default Settings

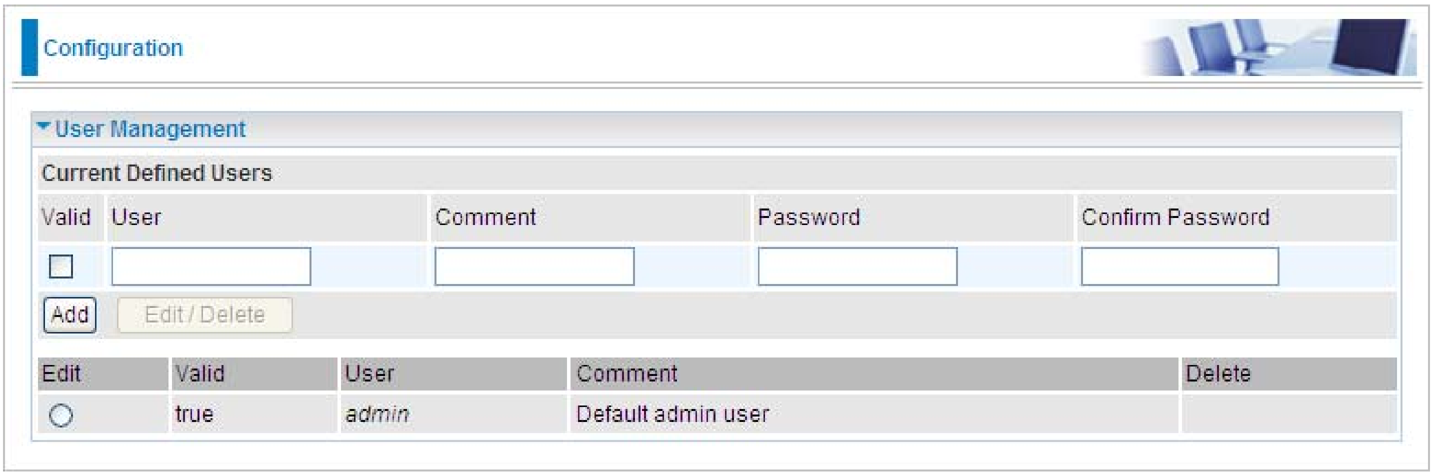
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

You may also reset your router to factory settings by holding the small Reset pinhole button more than 6 seconds on the back of your router.

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

User Management

In order to prevent unauthorized access to your router's configuration interface, it requires that all users are to login the GUI with a password. You can set up multiple user accounts, each with their own password. You can Edit any existing user accounts and Add new user account to grant access to the device configuration interface.



Configuration

User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
□				

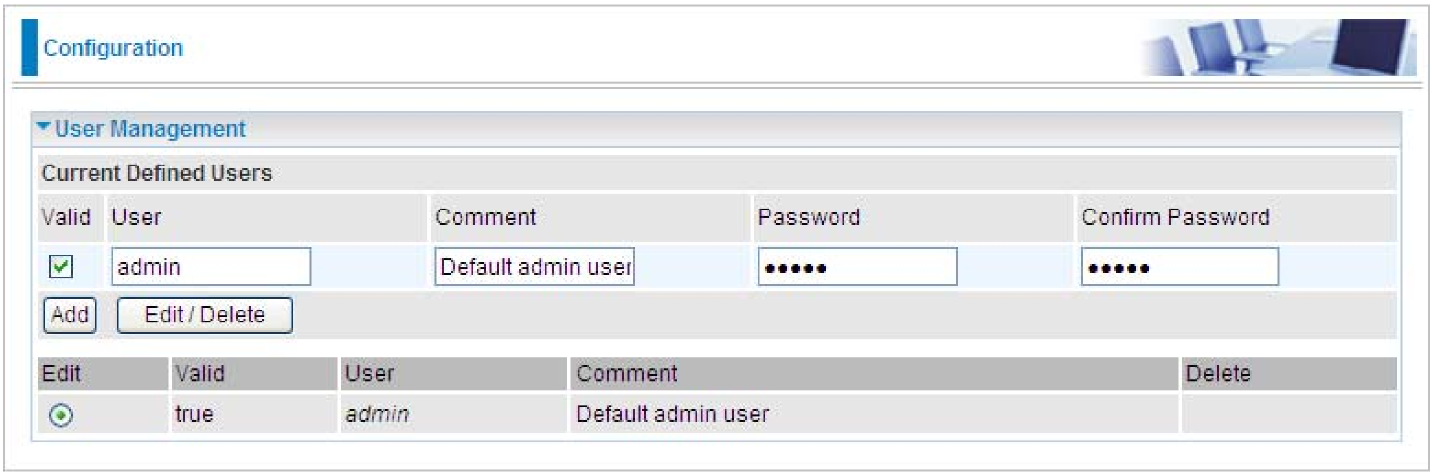
Edit	Valid	User	Comment	Delete
○	true	*admin*	Default admin user	

Edit Account Information

You can change the informations of any account whether the account is active or valid.

1. To edit an account, select the Edit radio button of the account to be edited. Once selected, all information of that account will be displayed.
2. Delete the information to be edited and replace it with the new one.
3. When it is done, simply click on the Edit/ Delete button to save your changes.

Note: It is recommended that you change the password immediately to prevent security breach to your GUI.



Configuration

User Management

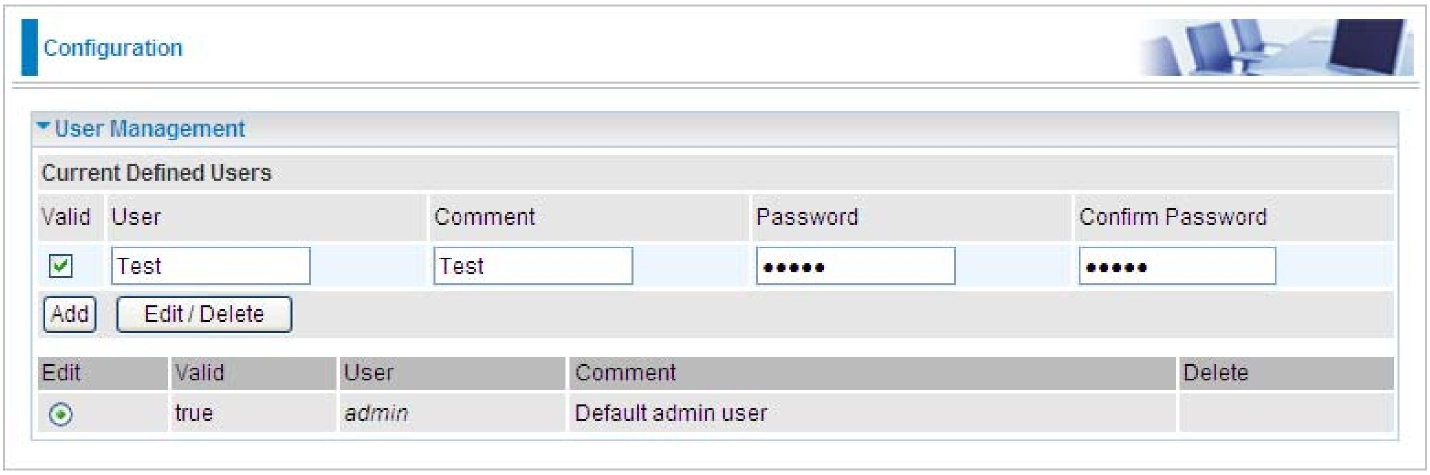
Current Defined Users

Valid	User	Comment	Password	Confirm Password
☑	admin	Default admin user	●●●●●	●●●●●

Edit	Valid	User	Comment	Delete
●	true	*admin*	Default admin user	

To Add an Account

1. Check the Valid checkbox, fill in all the information: User name, Comment (optional), Password, Confirm Password.
2. When it is done, click the Add button.



Configuration

User Management

Current Defined Users

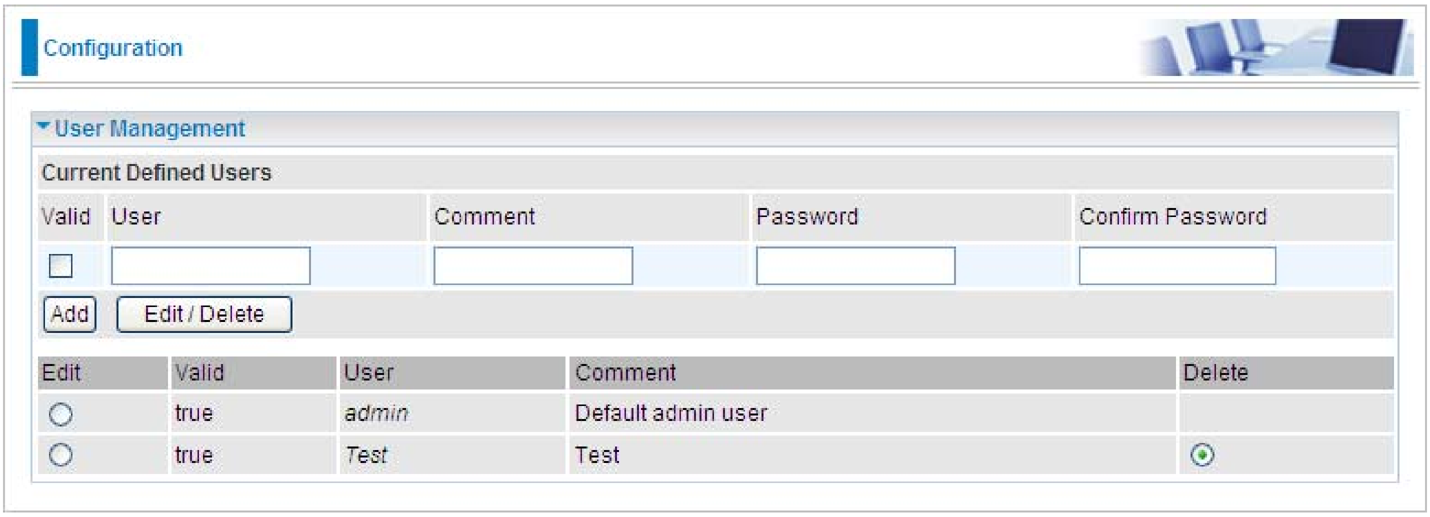
Valid	User	Comment	Password	Confirm Password
☑	Test	Test	●●●●●	●●●●●

Edit	Valid	User	Comment	Delete
●	true	*admin*	Default admin user	

To delete a user account:

1. Click on the Delete radio button of the account you want to delete.
2. Then click the Edit/Delete to confirm the deletion.

Note: You can delete any user account except for the default admin account. Thus there is no delete radio button available for this account.



Configuration

User Management

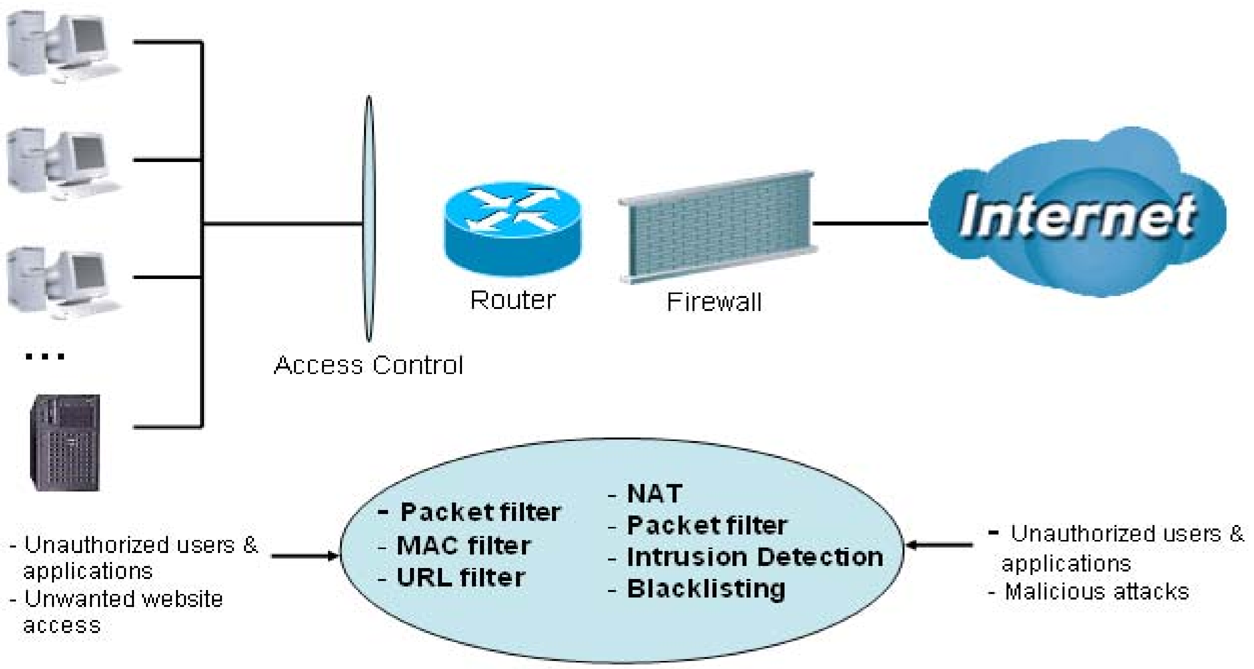
Current Defined Users

Valid	User	Comment	Password	Confirm Password
☐				

Edit	Valid	User	Comment	Delete
○	true	*admin*	Default admin user	
○	true	*Test*	Test	●

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for Internet access controlling from your LAN. This feature also protects your system from being attacked by hackers. When using NAT, the router acts as a “natural” Internet firewall, as all PCs on your LAN will have their own private IP addresses which is not directly accessible from the Internet. The router provides three levels of security support.



Firewall & Filter

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

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized computers or applications to access your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

Access Control: Prevent access from PCs on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized computers or applications from accessing the Internet.

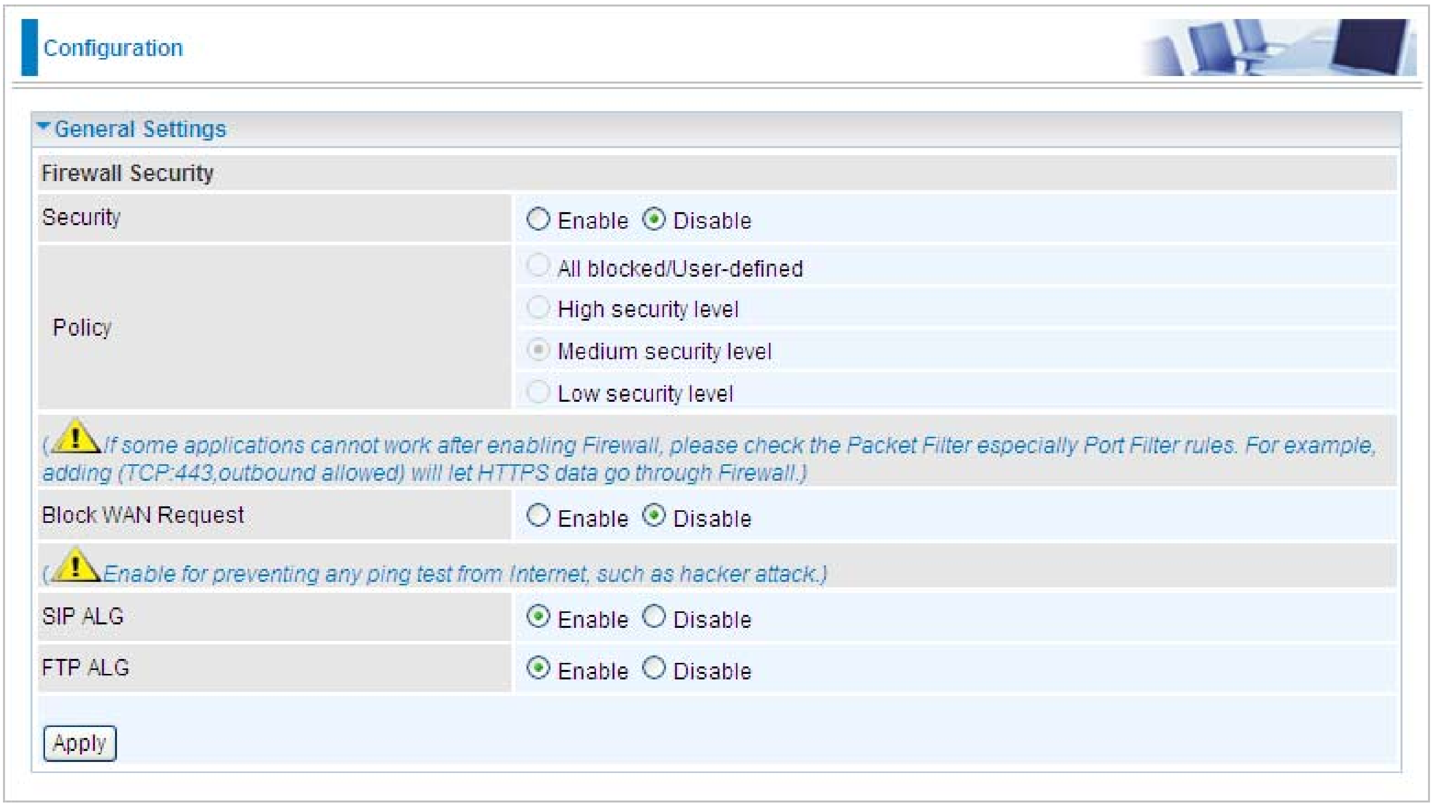
URL Filter: To block PCs on your local network from unwanted websites.

NOTE: When using Virtual Server, your PC will thus become exposed in a certain degree to unknown users if specific ports are set to open in the firewall packet filter setting. The degree of exposure depends on the parameter set in the Virtual Server Setting.

Listed are the items under the Firewall section: **General Settings, Packet Filter, Intrusion Detection, URL Filter, IM/P2P Blocking** and **Firewall Log.**

General Settings

You can choose to disable Firewall and still be able to access the URL Filter and IM/P2P Blocking or enable the Firewall using the preset filter rules and modify the port filter rules as required. The Packet Filter is used to filter packets based on Applications (Port) or IP addresses.



Configuration

General Settings

Firewall Security	
Security	○ Enable ● Disable
Policy	○ All blocked/User-defined ○ High security level ● Medium security level ○ Low security level
(⚠If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)	
Block WAN Request	○ Enable ● Disable
(⚠Enable for preventing any ping test from Internet, such as hacker attack.)	
SIP ALG	● Enable ○ Disable
FTP ALG	● Enable ○ Disable

There are four policy options to choose from:

> **All blocked/User-defined:** no predefined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules to access the Internet.
>
> **High/Medium/Low security level:** the predefined port filter rules for High, Medium and Low security are displayed in the Port Filters of the Packet Filter.

Select either High, Medium or Low security level to enable Firewall protection. The only difference between these three is the preset port filter rules in the Packet Filter. Firewall function is the same for all levels; it is only the list of preset port filters that changes between each setting. For more detail on level of preset port filter information, please refer to **Table 1: Predefined Port Filter**.

If you choose the preset security levels and add custom filters, the level of filter rules will be saved and you do not need to re-configure the rules again if you disable or switch to the other security level.

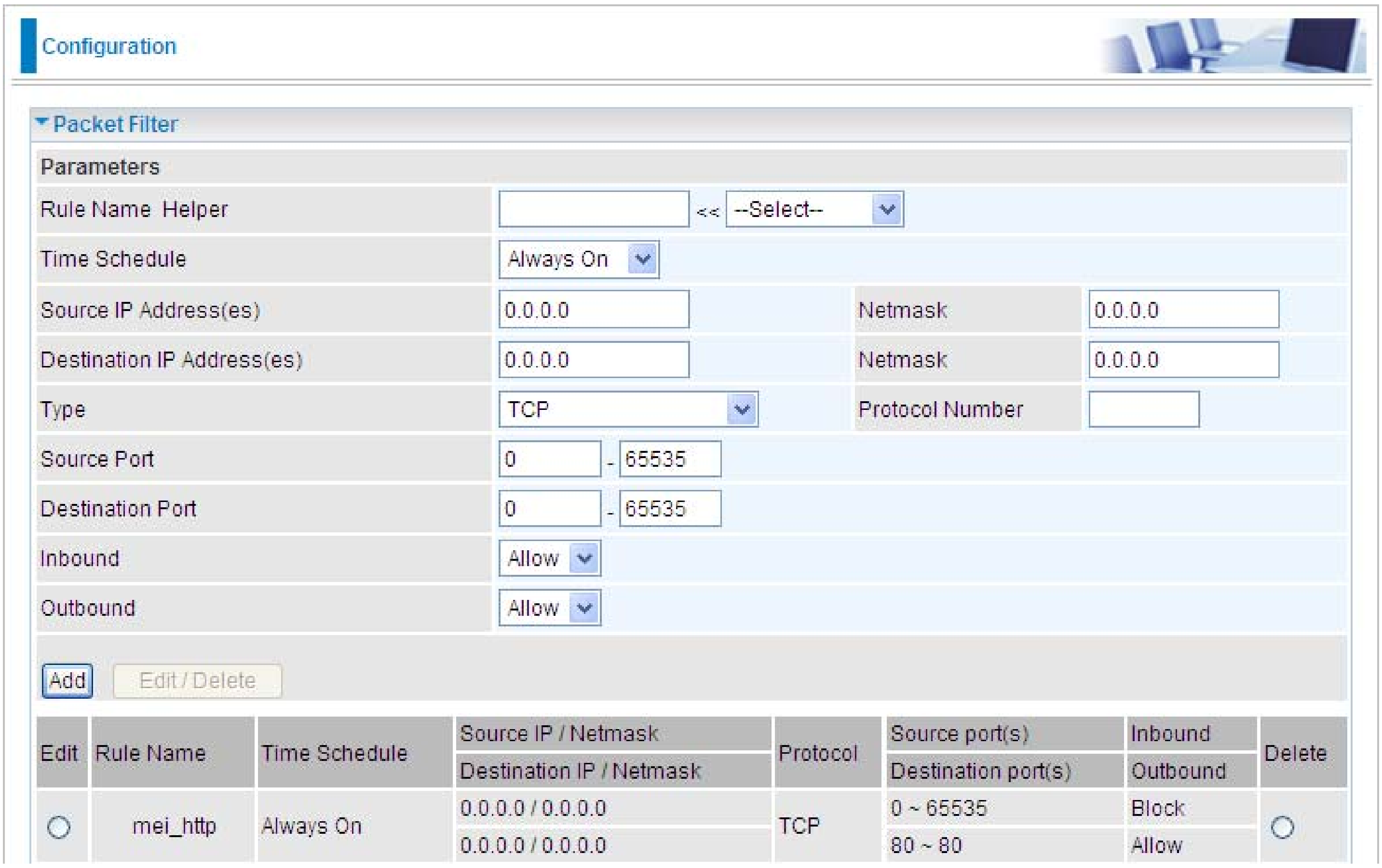
The “Block WAN Request” is a standalone function that is not affected by whether the security is enabled or disabled. This is used to prevent any scan tools that might be from hackers.

NOTE!

Any remote user attempting to perform this action may result in blocking all accesses to configure and manage the device from the Internet.

Packet Filter

This function is only available when Firewall is enabled with one of the four security levels selected (All blocked, High, Medium and Low). The preset port filter rules in the Packet Filter must be modified accordingly to the level of security selected. See Table1: Predefined Port Filter for more detail information.



Parameters

Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Edit	Rule Name	Time Schedule	Source IP / Netmask	Protocol	Source port(s)	Inbound	Delete
			Destination IP / Netmask		Destination port(s)	Outbound	
○	mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	○
			0.0.0.0 / 0.0.0.0		80 ~ 80	Allow	

Example: Predefined Port Filters Rules

The predefined port filter rules for High, Medium and Low security levels are listed. See Table 1.

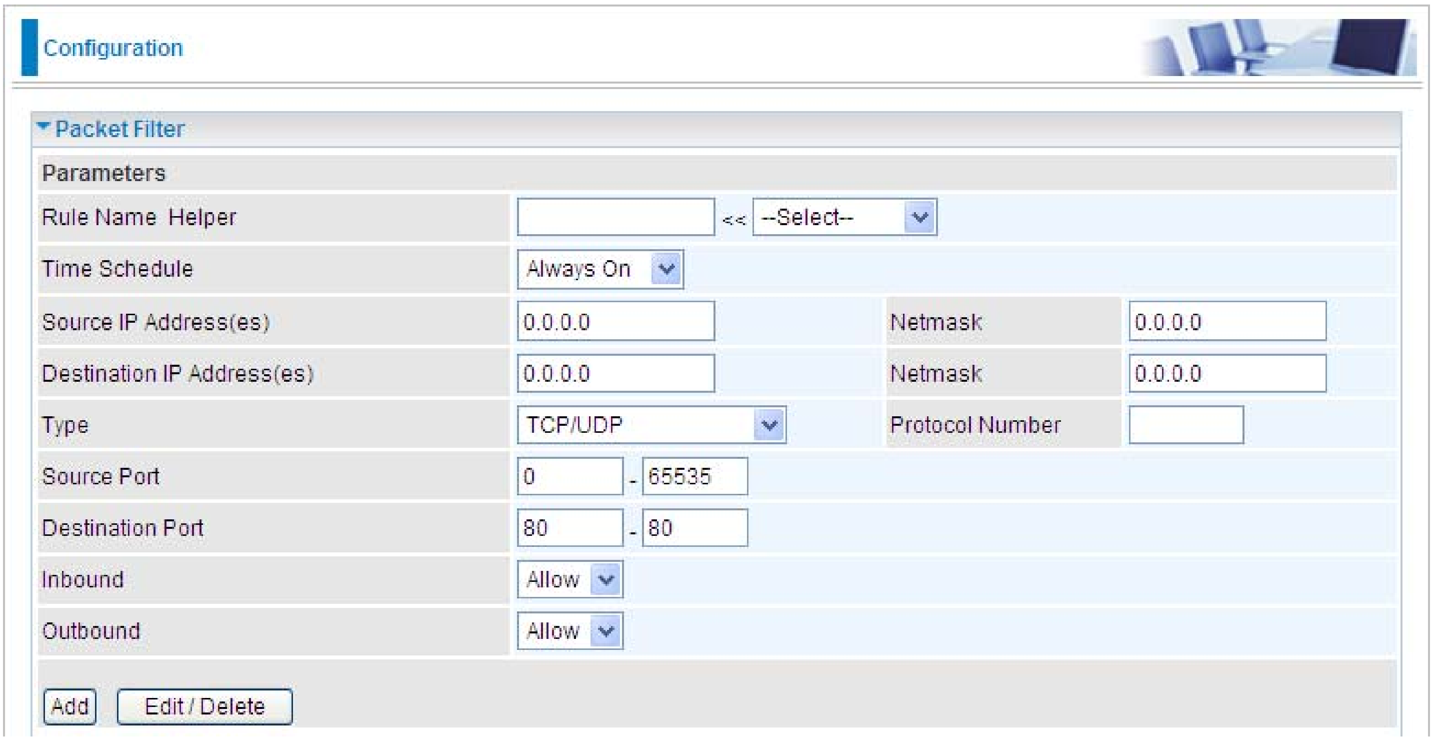
Note: Firewall – All Blocked/User-defined, you must define and create the port filter rules yourself. No predefined rule is being preconfigured.

Table 1: Predefined Port Filter

Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS(53)	UDP	53	53	NO	YES	NO	YES	NO	YES
DNS(53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMPT(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP/SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy(8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ(5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN(1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN(7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN
Outbound: LAN to Internet
YES: Allowed
NO: Blocked
N/A: Not Applicable

Packet Filter – Add TCP/UDP Filter



Parameters			
Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP/UDP	Protocol Number	
Source Port	0 - 65535		
Destination Port	80 - 80		
Inbound	Allow		
Outbound	Allow		

Rule Name Helper: User defined description for entry identification. You may also choose from the Select drop-down menu for an existing predefined rule. The maximum name length is 32 characters.

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

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Select the Subnet Mask of the IP address range you wish to allow/block the traffic to or form. Set the IP address and Subnet Mask to 0.0.0.0 to inactive the Address-Filter rule.

Tip: To block access, to/from a single IP address, enter that IP address as the Host IP Address and use a Host Subnet Mask of "255.255.255.255".

Type: It is the packet protocol type used by the application, select TCP, UDP or both TCP/UDP.

Protocol Number: Insert the port number.

Source Port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

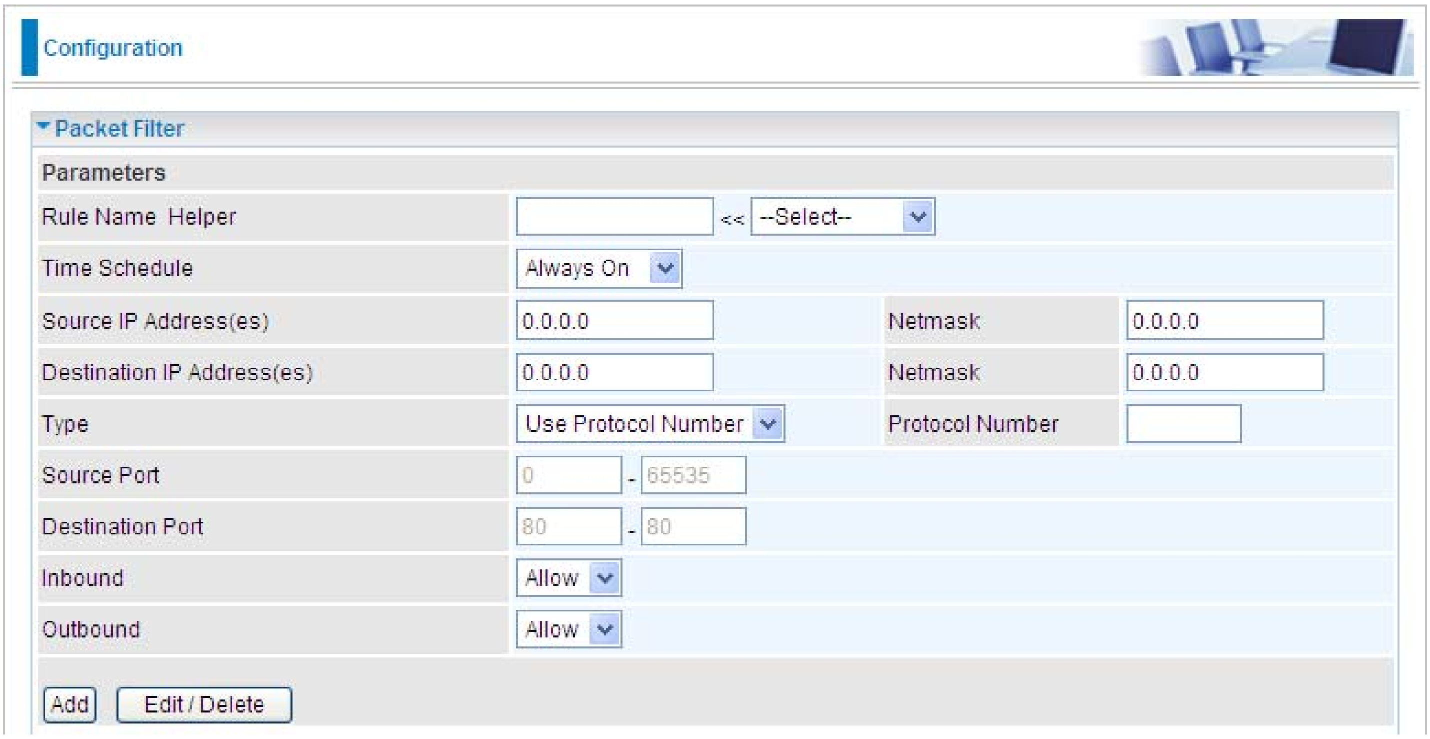
Destination Port: This is the Port or Port Ranges that defines the application.

Inbound / Outbound: Select Allow or Block the access to the Internet ("Outbound") or from the Internet ("Inbound").

When all changes is made, click Add button to apply your changes.

Packet Filter – Add Raw IP Filter

Go to “Type” drop-down menu, select “Use Protocol Number”.



Configuration

Packet Filter

Parameters			
Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	Use Protocol Number	Protocol Number	
Source Port	0 - 65535		
Destination Port	80 - 80		
Inbound	Allow		
Outbound	Allow		

Rule Name Helper: User defined description for entry identification. You may also choose from the Select drop-down menu for an existing predefined rule.

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

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Select the Subnet Mask of the IP address range you wish to allow/block the traffic to or form; set IP address and Subnet Mask to 0.0.0.0 to inactive the Address-Filter rule.

Tip: To block access to/from a single IP address, enter that IP address as the Host IP Address and use a Host Subnet Mask of “255.255.255.255”.

Type: It is the packet protocol type used by the application, select TCP, UDP or both TCP/UDP.

Protocol Number: Insert the port number, i.e. GRE 47.

Source Port: This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

Destination Port: This is the Port or Port Ranges that defines the application.

Inbound / Outbound: Select Allow or Block the access to the Internet (“Outbound”) or from the Internet (“Inbound”).

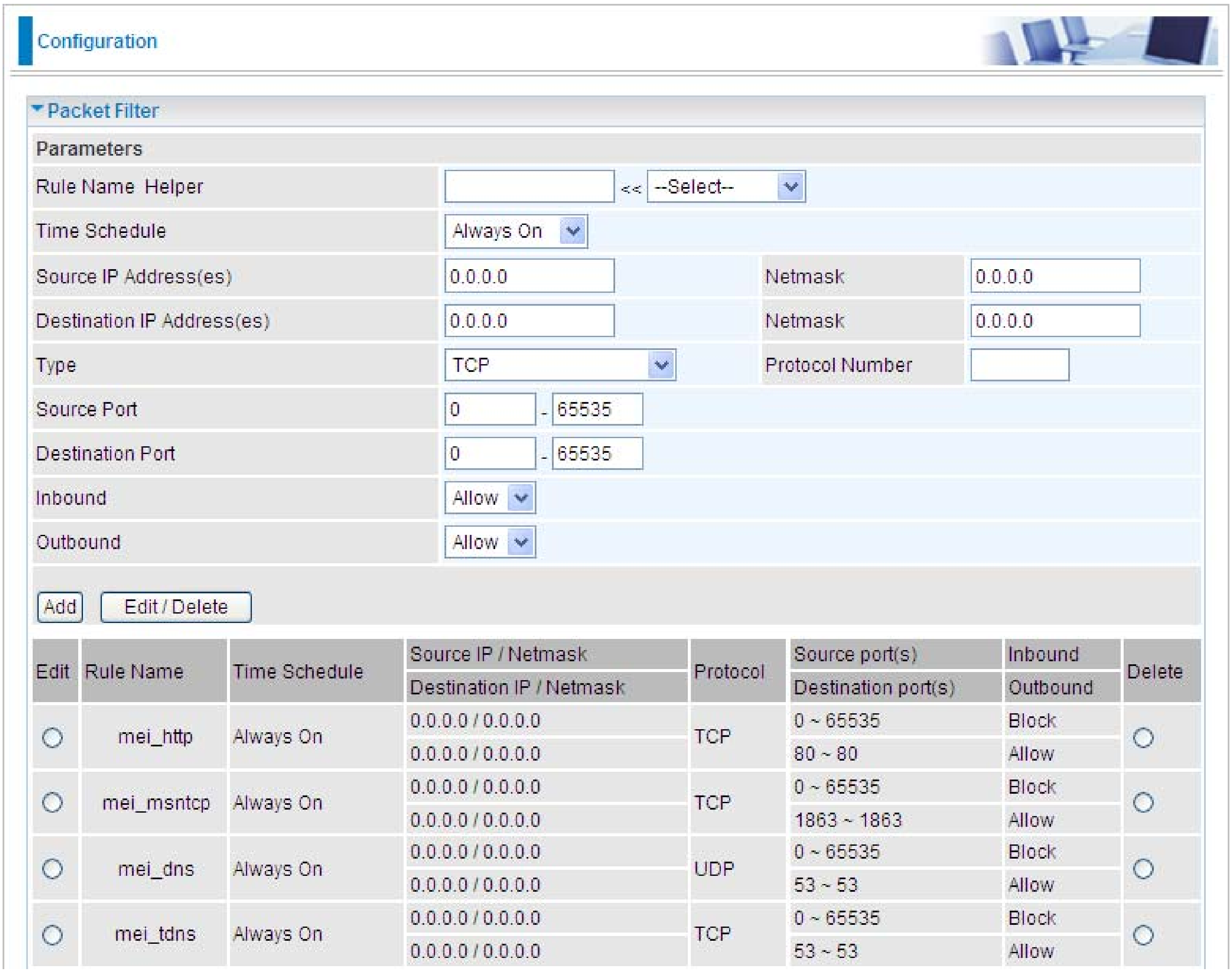
When all changes is made, click Add button to apply your changes.

Example: Configuring your firewall to allow a publicly accessible web server on your LAN

The predefined port filter rule for HTTP (TCP port 80) is the same whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

As you can see from the diagram below, when the firewall is enabled with one of the three presets (Low/Medium/High) security level selected, an inbound HTTP access is not allowed which means remote access through HTTP to your router is not allowed.

Note: Inbound indicates accessing from the Internet to LAN and Outbound is from LAN to the Internet.



Configuration

▾Packet Filter

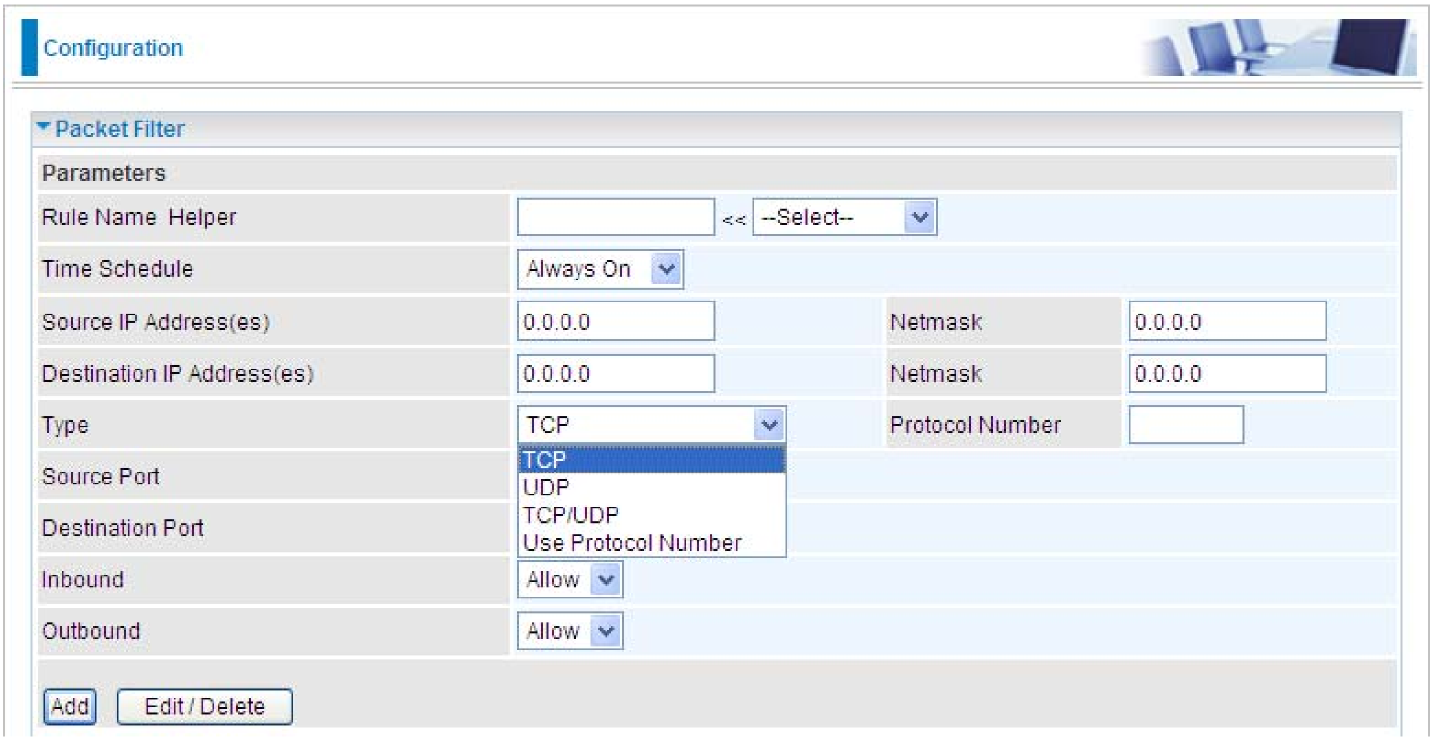
Parameters			
Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Edit	Rule Name	Time Schedule	Source IP / Netmask	Protocol	Source port(s)	Inbound	Delete
			Destination IP / Netmask		Destination port(s)	Outbound	
○	mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	○
			0.0.0.0 / 0.0.0.0		80 ~ 80	Allow	
○	mei_msntcp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	○
			0.0.0.0 / 0.0.0.0		1863 ~ 1863	Allow	
○	mei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	○
			0.0.0.0 / 0.0.0.0		53 ~ 53	Allow	
○	mei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	○
			0.0.0.0 / 0.0.0.0		53 ~ 53	Allow	

Configuring Packet Filter:

1. Click Packet Filters. You will then be presented with the predefined port filter rules screen (in this case for the low security level), shown below:

Note: You may click Edit the predefined rule instead of Delete it. This is an example to show to how you add a filter on your own.

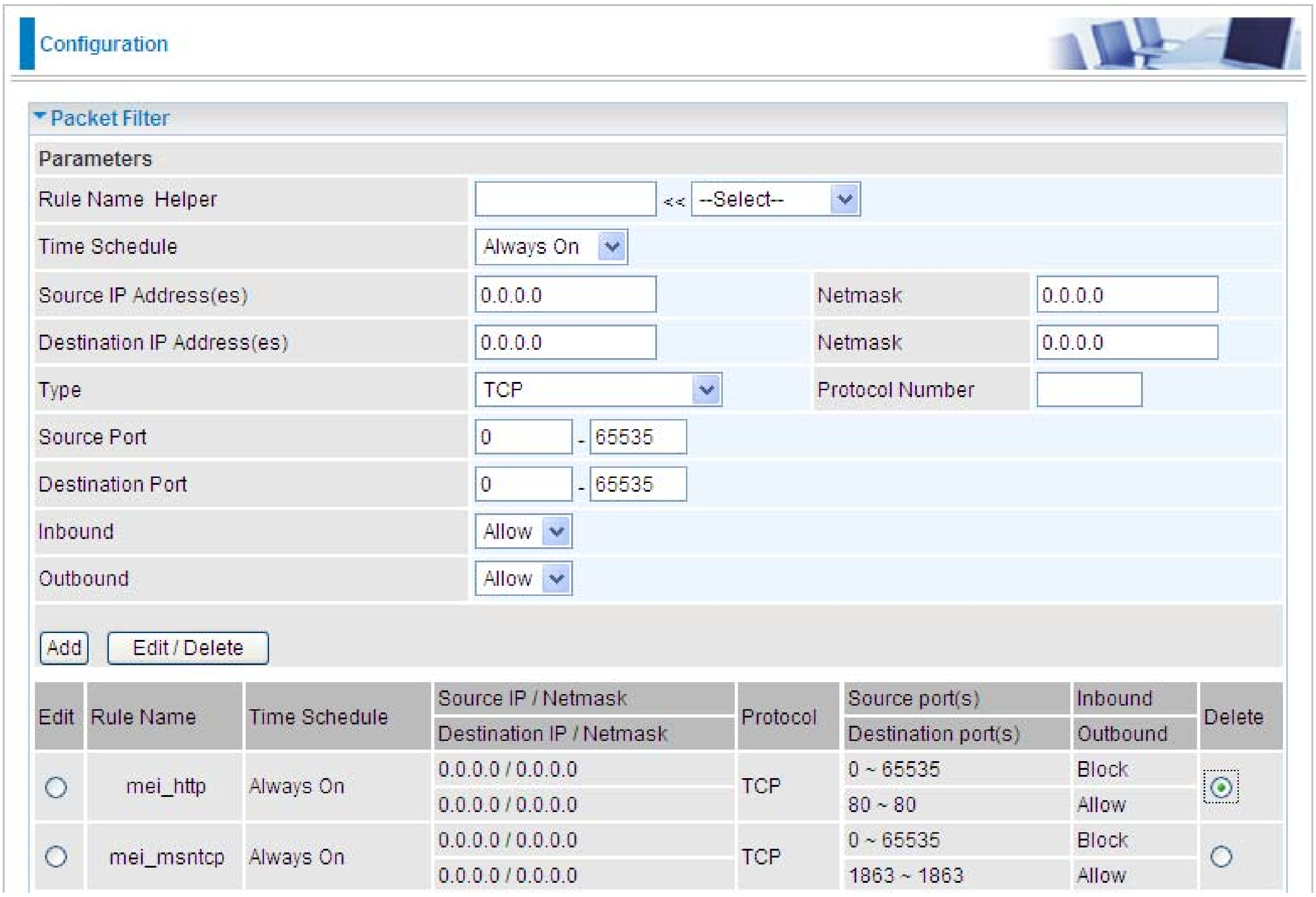


Configuration

Packet Filter

Parameters			
Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port			
Destination Port			
Inbound	Allow		
Outbound	Allow		

2. If you want to delete a filter rule, select the delete radio button of the HTTP rule you want to delete. Then click the Edit/Delete button to delete the rule.



Configuration

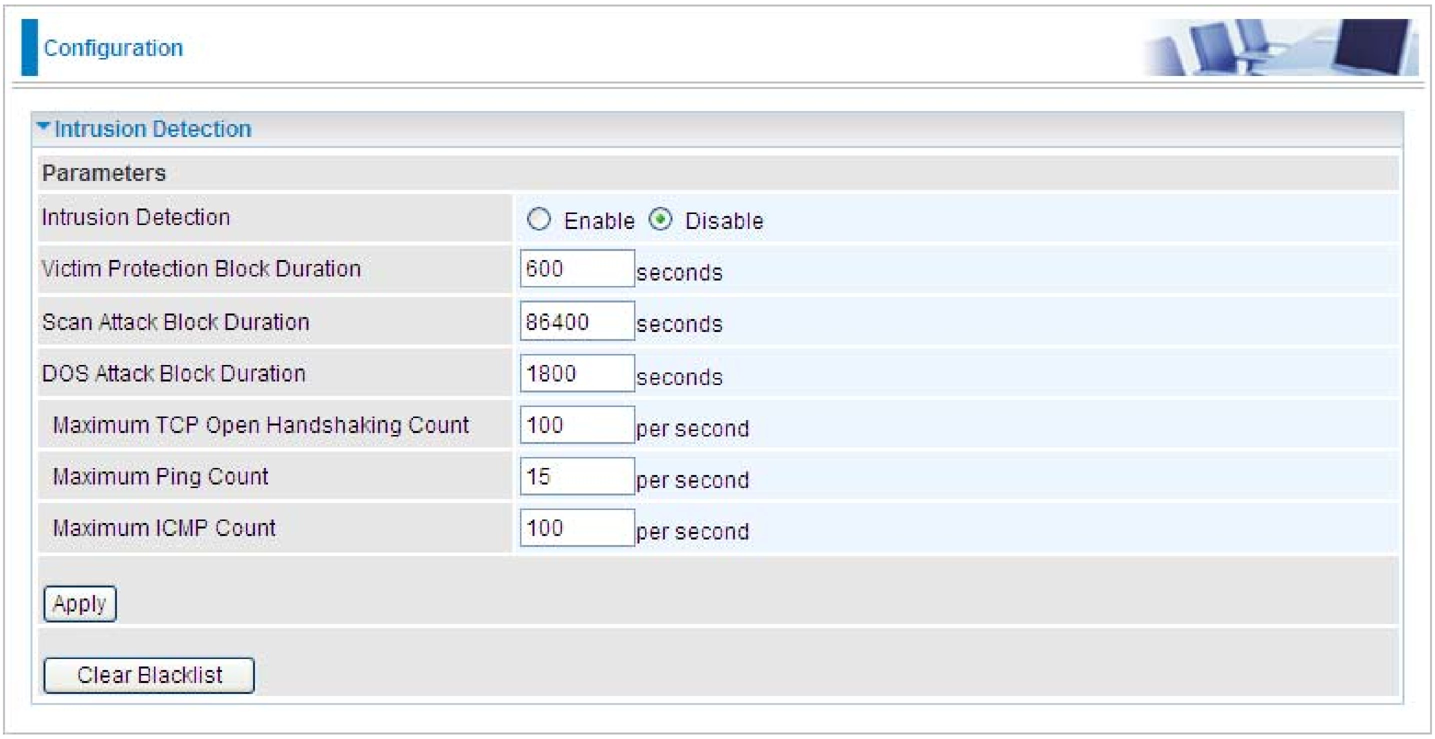
Packet Filter

Parameters			
Rule Name Helper	<< --Select--		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Edit	Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound	Delete
○	mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	●
○	mei_msntcp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 1863 ~ 1863	Block Allow	○

3. To add a new rule, Input the Rule Name, Time Schedule, Source/Destination IP, Type, Source/ Destination Port, Inbound and Outbound. Then click the Add button.

Intrusion Detection



Parameters	
Intrusion Detection	○ Enable ● Disable
Victim Protection Block Duration	600 seconds
Scan Attack Block Duration	86400 seconds
DOS Attack Block Duration	1800 seconds
Maximum TCP Open Handshaking Count	100 per second
Maximum Ping Count	15 per second
Maximum ICMP Count	100 per second

The router Intrusion Detection System (IDS) is used to detect hacker's attack and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified in the Block Duration. The default setting for this function is false (disabled). Some types of attack are denied immediately without using the Blacklist function, such as Land attack and Echo/CharGen scan.

Intrusion Detection: If enabled, IDS will block Smurf attack attempts. Default is false.

Block Duration:

Victim Protection Block Duration: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.

Scan Attack Block Duration: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.

DoS Attack Block Duration: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

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

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

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

For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

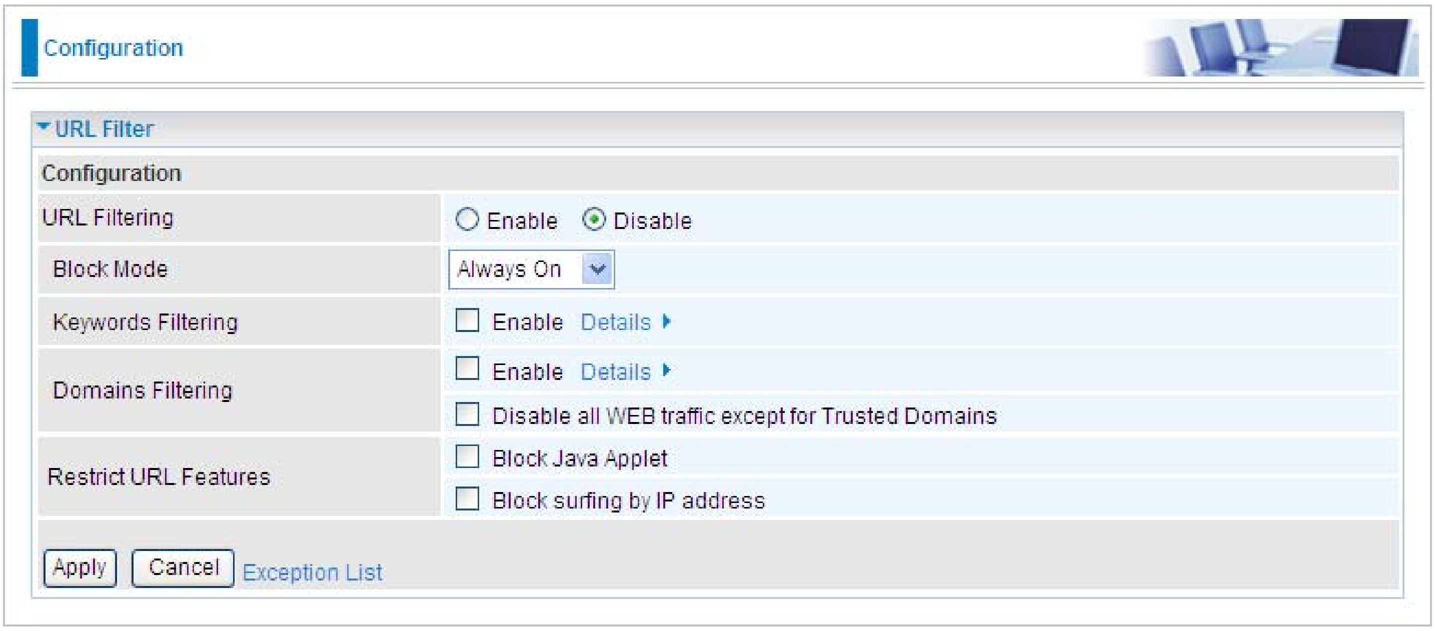
Table 2: Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Src Port: Source Port
Dst Port: Destination Port
Dst IP: Destination IP

URL Filter

URL (Uniform Resource Locator) (e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rule allows you to prevent users on your network from accessing specific websites defined by their URL. There are no predefined URL filter rules, therefore you can add filter rules to meet your requirements.



Configuration

▾URL Filter

Configuration	
URL Filtering	○ Enable ● Disable
Block Mode	Always On
Keywords Filtering	□ Enable Details ▸
Domains Filtering	□ Enable Details ▸ □ Disable all WEB traffic except for Trusted Domains
Restrict URL Features	□ Block Java Applet □ Block surfing by IP address

Enable/Disable: Select to enable or disable URL Filter feature.

Block Mode: A list of the modes that you can choose from to check the URL filter rules. The default is set to **Always On.**

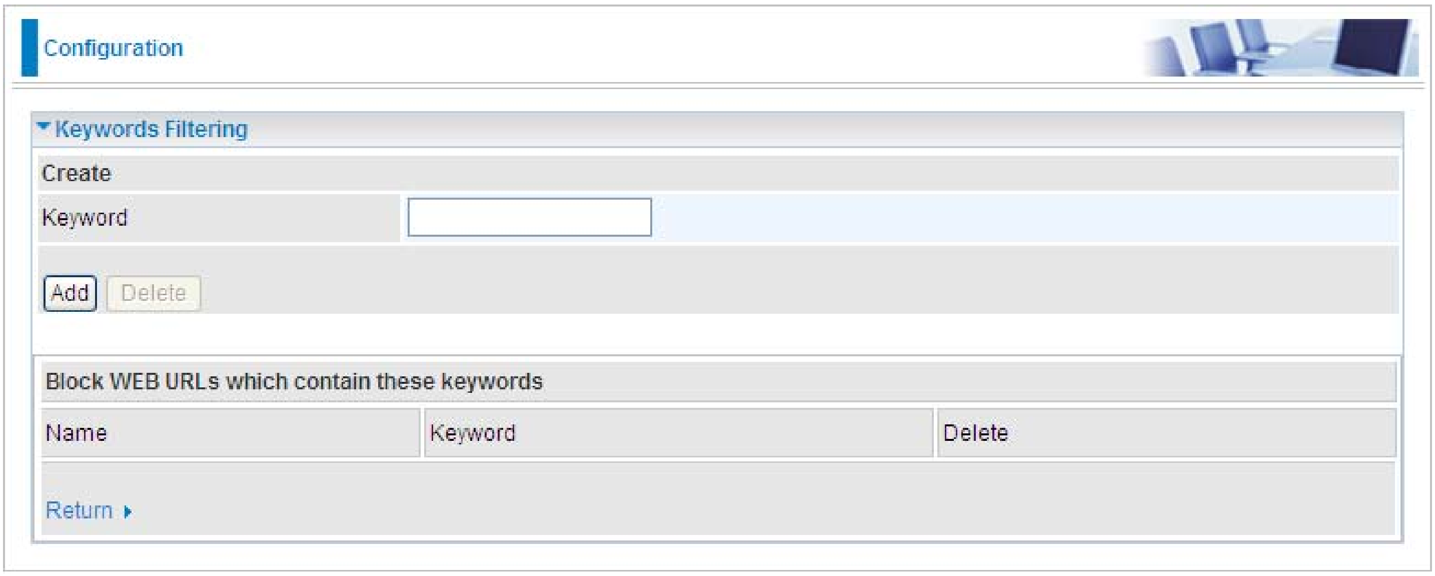
Disabled: No action will be performed by the Block Mode.

Always On: Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.

TimeSlot1 ~ TimeSlot16: It is a self defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Keywords Filtering: Allow blocking against 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 will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is http://www.abc.com/abcde.html, the connection will be dropped if the keyword "abcde" occurs in the URL.



Configuration

▾ Keywords Filtering

Create	
Keyword	

Add Delete

Block WEB URLs which contain these keywords

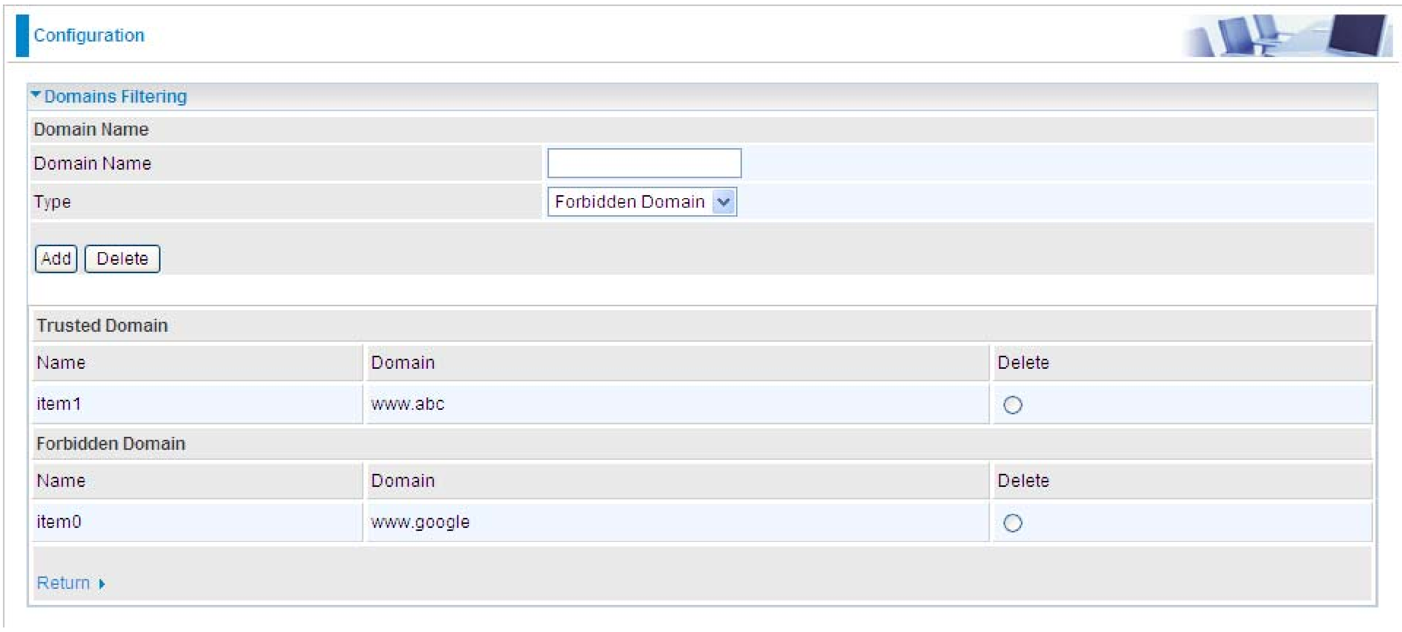
Name	Keyword	Delete

Return ▸

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden). For this function to be activated, both enable and disable checkboxes of Domain Filtering must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped.
3. If the packet does not match either of the above two conditions, it is sent to the remote web server.
4. Please be noted that the completed URL, "www" + domain name should be specific. e.g.: In order to block traffic to **www.google.com.au**, enter "**www.google**" or "**www.google.com**"

In the example below, the URL request for **www.abc.com** will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for **www.google** or **www.google.com** will be dropped, because **www.google** is in the forbidden list.



Configuration

▾ Domains Filtering

Domain Name	
Domain Name	
Type	Forbidden Domain

Add Delete

Trusted Domain

Name	Domain	Delete
item1	www.abc	○

Forbidden Domain

Name	Domain	Delete
item0	www.google	○

Return ▸

Example:

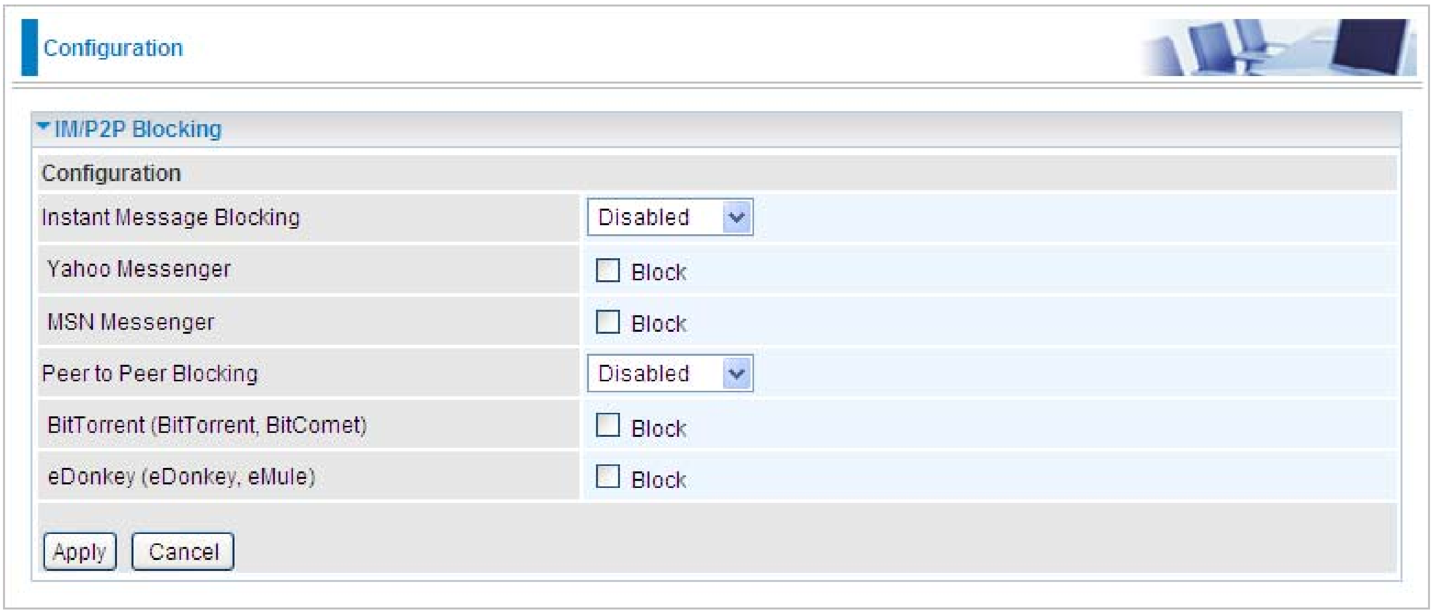
Andy wishes to disable all WEB traffic except for the ones listed in the trusted domain, which would prevent Bobby from accessing other websites. Andy selects both conditions in the Domain Filtering thinking that this will stop Bobby. But Bobby knows this function, Domain Filtering, ONLY disables all WEB traffic except for Trusted Domain, BUT not its IP address. If this is the situation, Block surfing by IP address function can become helpful. Now, Andy can successfully prevent Bobby from accessing other websites.

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

> **Block Java Applet:** This function can block Web content that includes Java Applets. It is to prevent someone who wants to damage your system via standard HTTP protocol.
>
> **Block surfing by IP address:** A further restriction against someone who uses IP address as URL to cheat around the Domains Filtering rule. Activates only if Domain Filtering is enabled.

IM / P2P Blocking

IM, short for Instant Message, is a client software that allows users to communicate & exchange text messages with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of users who share their files with each other within the network over the Internet across the globe. Both Instant Message and Peer-to-peer applications make communication faster and easier but your network can become increasingly insecure at the same time. Billion's IM and P2P blocking helps users to restrict LAN PCs to access the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.



Configuration	
Instant Message Blocking	Disabled
Yahoo Messenger	□ Block
MSN Messenger	□ Block
Peer to Peer Blocking	Disabled
BitTorrent (BitTorrent, BitComet)	□ Block
eDonkey (eDonkey, eMule)	□ Block

Instant Message Blocking: The default is set to Disabled.

Disabled: Instant Message blocking is not triggered. No action will be performed.

Always On: Action is enabled.

TimeSlot1 ~ TimeSlot16: This is the self defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

Yahoo/MSN Messenger: Check the checkbox to block either or both Yahoo or/and MSN Messenger. To be sure you enabled the *Instant Message Blocking* first.

Peer to Peer Blocking: The default is set to Disabled.

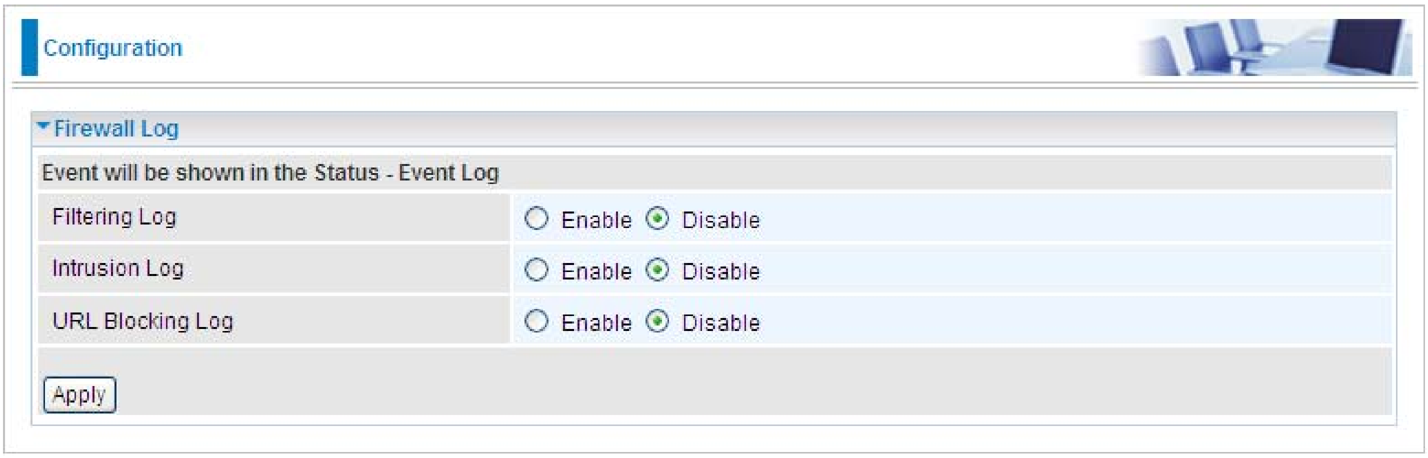
Disabled: Instant Message blocking is not triggered. No action will be performed.

Always On: Action is enabled.

TimeSlot1 ~ TimeSlot16: This is the self defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to Time Schedule section.

BitTorrent / eDonkey: Check the checkbox to block either or both Bit Torrent or/and eDonkey. To be sure you enabled the Peer to Peer Blocking first.

Firewall Log



Configuration

▾Firewall Log

Event will be shown in the Status - Event Log

Filtering Log	○ Enable ● Disable
Intrusion Log	○ Enable ● Disable
URL Blocking Log	○ Enable ● Disable

Firewall Log displays a log that contains information of any unexpected actions that occur to your firewall settings.

Check the Enable checkbox to activate event logging.

Log information can be seen in the Status – Event Log after the feature is enabled.

QoS - Quality of Service

QoS function helps you to control the network traffic of each application from LAN (Ethernet and/ or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.

These are the items within the QoS section: **Prioritization, Outbound IP Throttling & Inbound IP Throttling (bandwidth management).**

Prioritization

There are three priority settings to be provided in the Router:

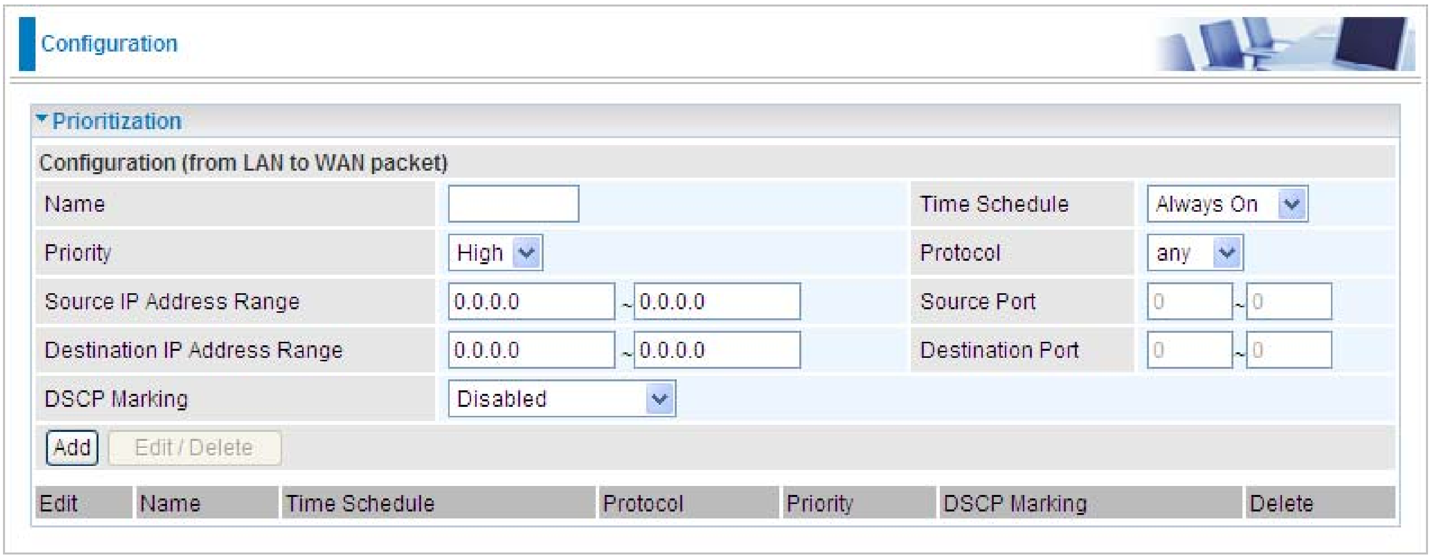
High

Normal (The default is normal priority for all of traffic without setting)

Low

The utilization percentage of each priority settings are High (60%), Normal (30%) and Low (10%).

To delete an application, you can click on the Delete radio button of the application and then click the Edit/Delete button.



Configuration

Prioritization

Configuration (from LAN to WAN packet)

Name		Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete

Name: User defined description to identify the new policy/application created.

Time Schedule: Schedule your prioritization policy.

Priority: The priority given to each policy/application. Its default setting is set to High. You may adjust this setting to fit your policy / application.

Protocol: The name of the supported protocol.

Source IP Address Range: The source IP address or the range of the packets to be monitored.

Source Port: The source port of the packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Destination Port: The destination port of the packets to be monitored.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value. See Table 4 for **DSCP Mapping Table**.

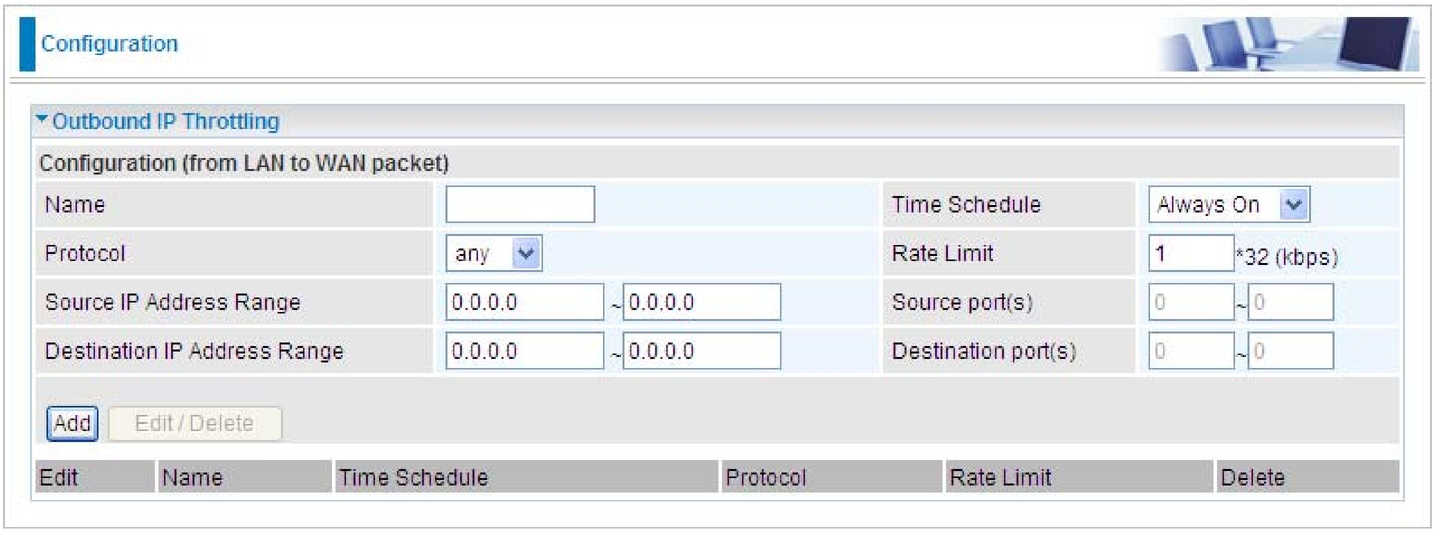
Note: Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.

Table 4: DSCP Mapping Table

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

Outbound IP Throttling (LAN to WAN)

IP Throttling allows you to limit the speed of the IP traffic. The value entered in the Rate Limit blank will set the speed limitation of the application.



Configuration (from LAN to WAN packet)

Name		Time Schedule	Always On
Protocol	any	Rate Limit	1 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete

Name: User defined description to identify the new policy/name created.

Time Schedule: Schedule your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of the supported protocol.

Rate Limit: To limit the speed of the outbound traffic.

Source IP Address Range: The source IP address or the range of packets to be monitored.

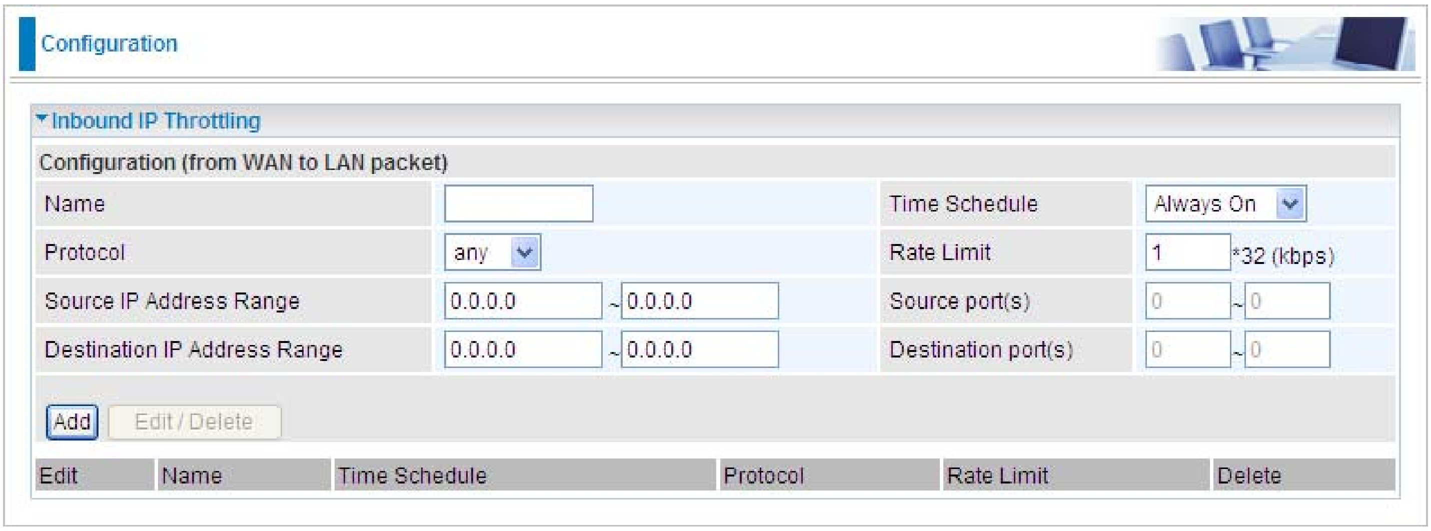
Source Port(s): The source port of the packets to be monitored.

Destination IP Address Range: The destination IP address or the range of packets to be monitored.

Destination Port(s): The destination port of the packets to be monitored.

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of the IP traffic. The value entered in the Rate Limit blank will set the speed limitation of the application.



Configuration (from WAN to LAN packet)

Name		Time Schedule	Always On
Protocol	any	Rate Limit	1 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete

Name: User defined description to identify the new policy/application created.

Time Schedule: Schedule your prioritization policy. Refer to **Time Schedule** for more information.

Protocol: The name of the supported protocol.

Rate Limit: To limit the speed of the inbound traffic.

Source IP Address Range: The source IP address or the range of the packets to be monitored.

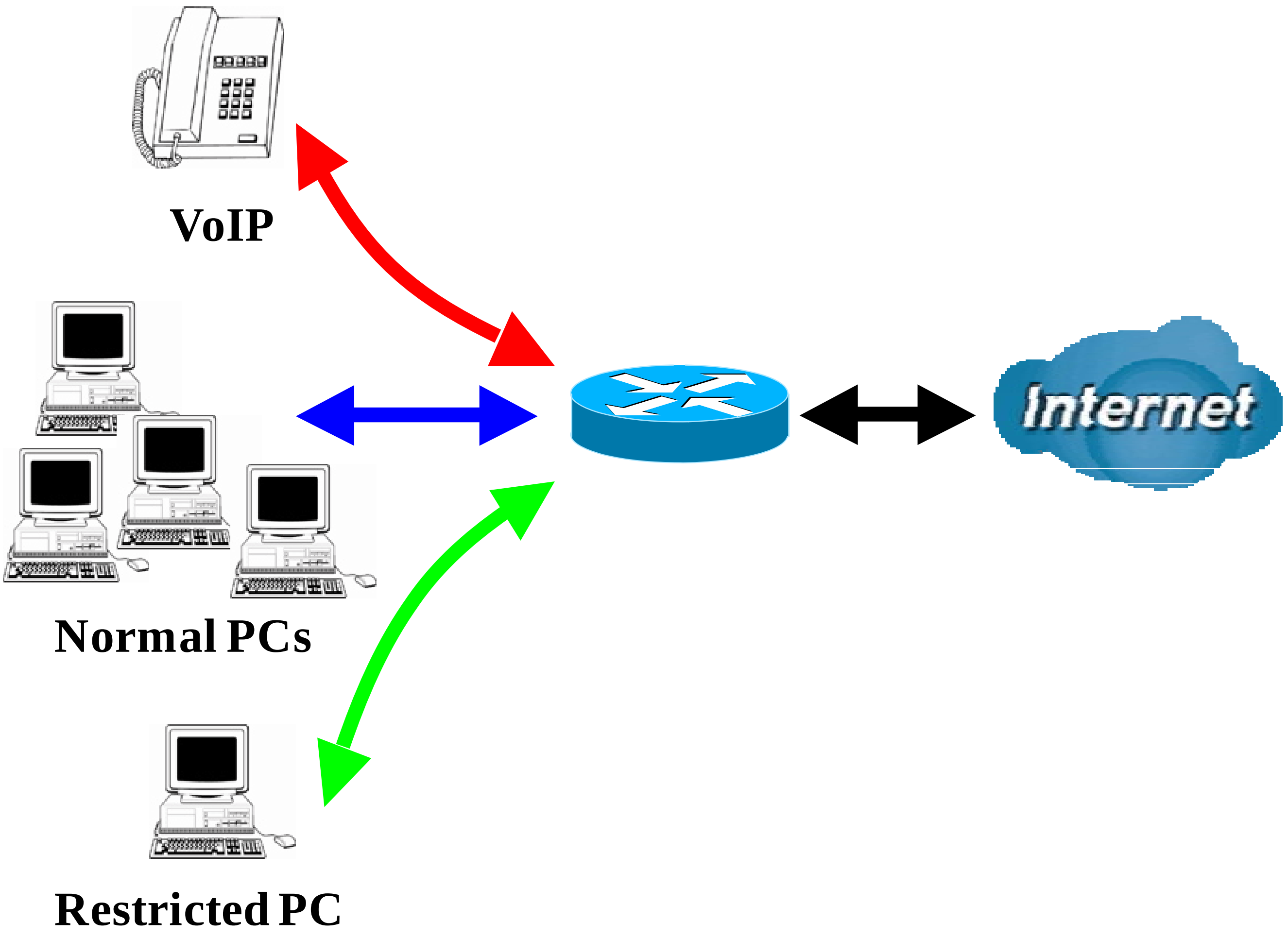
Source Port(s): The source port of the packets to be monitored.

Destination IP Address Range: The destination IP address or the range of the packets to be monitored.

Destination Port(s): The destination port of the packets to be monitored.

Example: QoS for your Network

Connection Diagram



Information and Settings

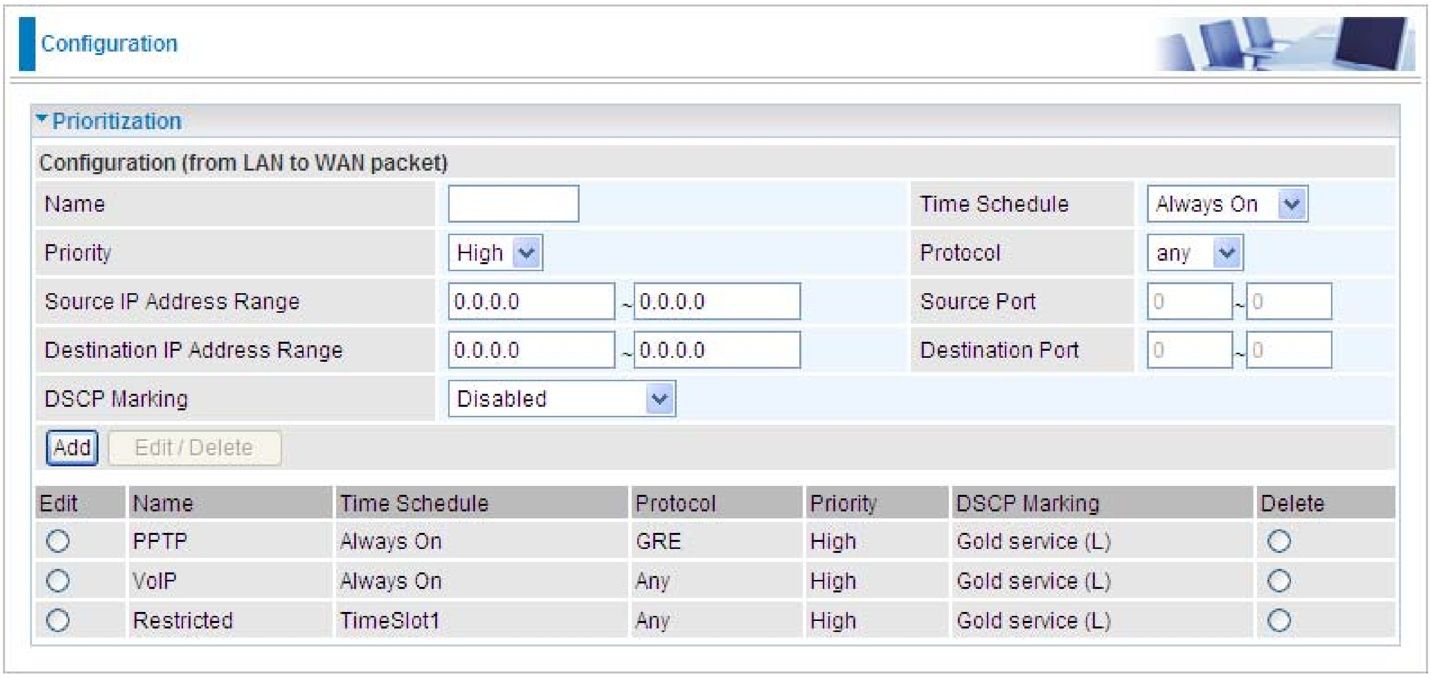
Upstream: 928 kbps

Downstream: 8 Mbps

VoIP User : 192.168.1.1

Normal Users : 192.168.1.2~192.168.1.5

Restricted User: 192.168.1.100



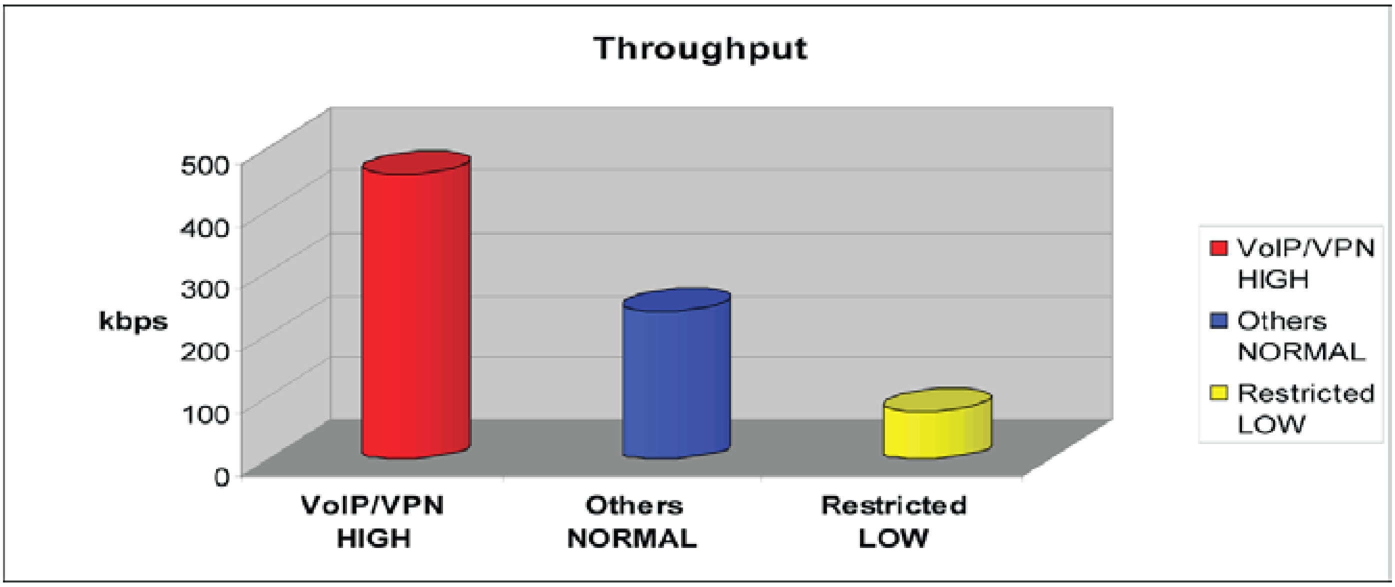
Configuration

▾ Prioritization

Configuration (from LAN to WAN packet)

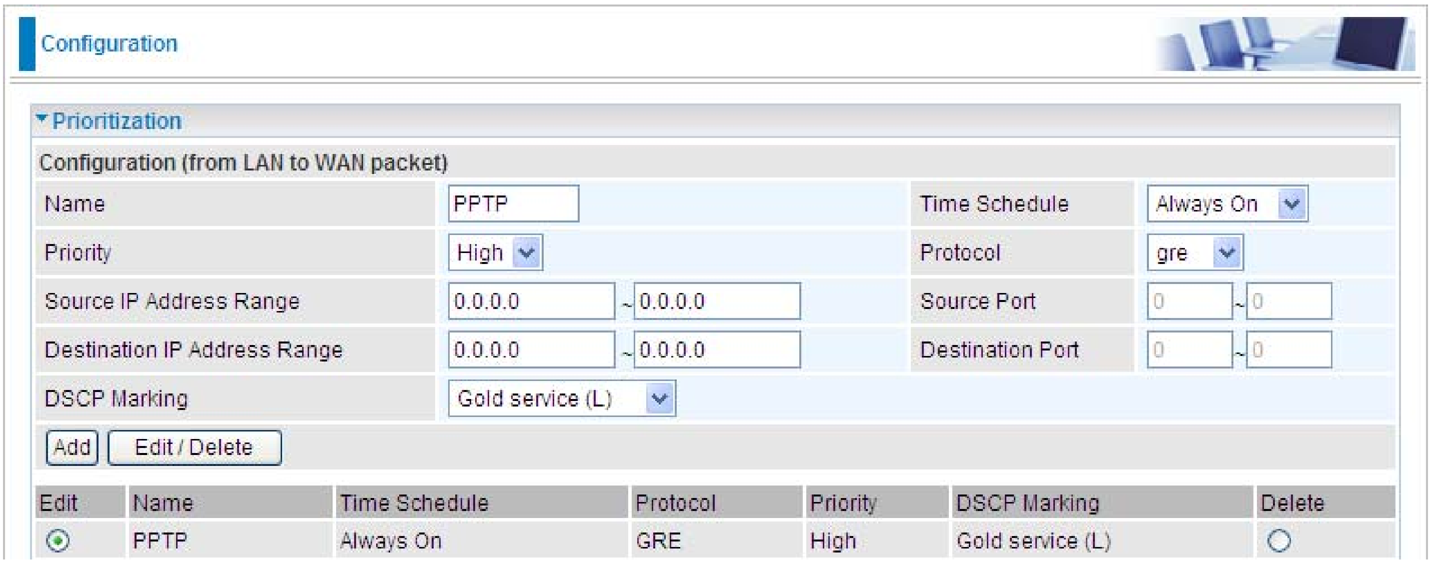
Name		Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
○	PPTP	Always On	GRE	High	Gold service (L)	○
○	VoIP	Always On	Any	High	Gold service (L)	○
○	Restricted	TimeSlot1	Any	High	Gold service (L)	○



Mission-critical application

Mostly the VPN connection is mission-critical application for doing data exchange between head and branch office.



Configuration

▾Prioritization

Configuration (from LAN to WAN packet)

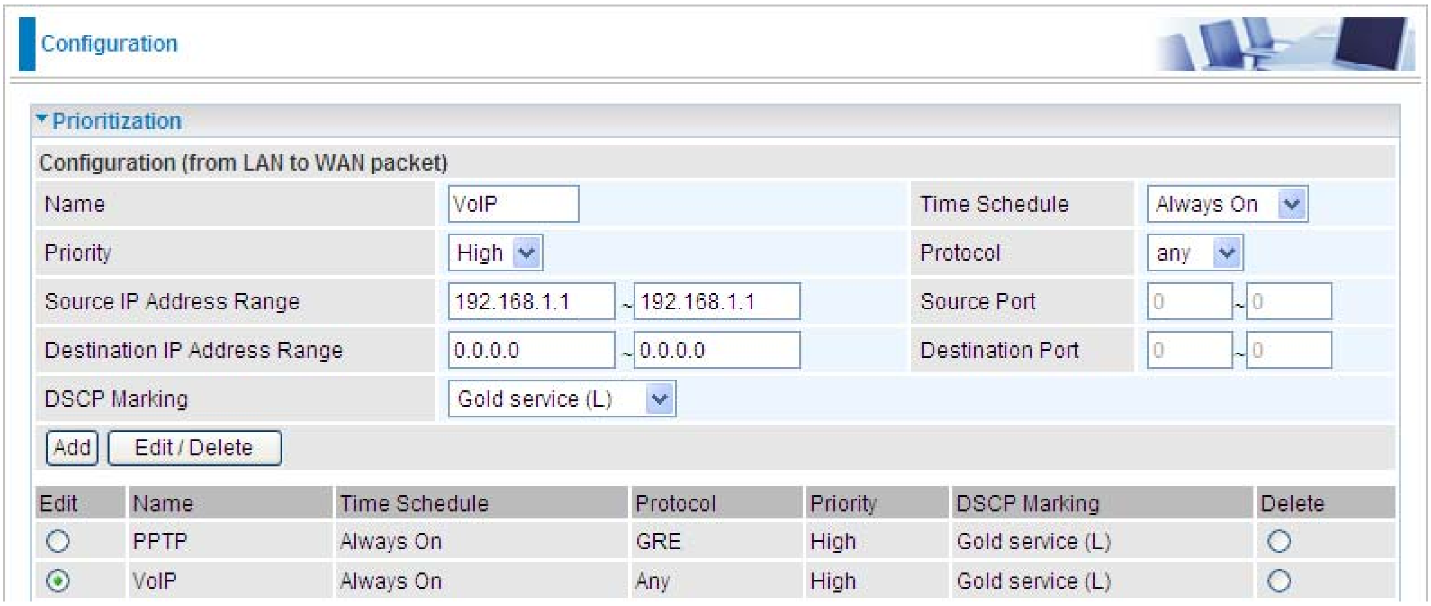
Name	PPTP	Time Schedule	Always On
Priority	High	Protocol	gre
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
●	PPTP	Always On	GRE	High	Gold service (L)	○

The mission-critical application must be sent out smoothly without any drop out. Set the level of priority as high to prevent other applications from saturating the bandwidth.

Voice 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.



Configuration

▾Prioritization

Configuration (from LAN to WAN packet)

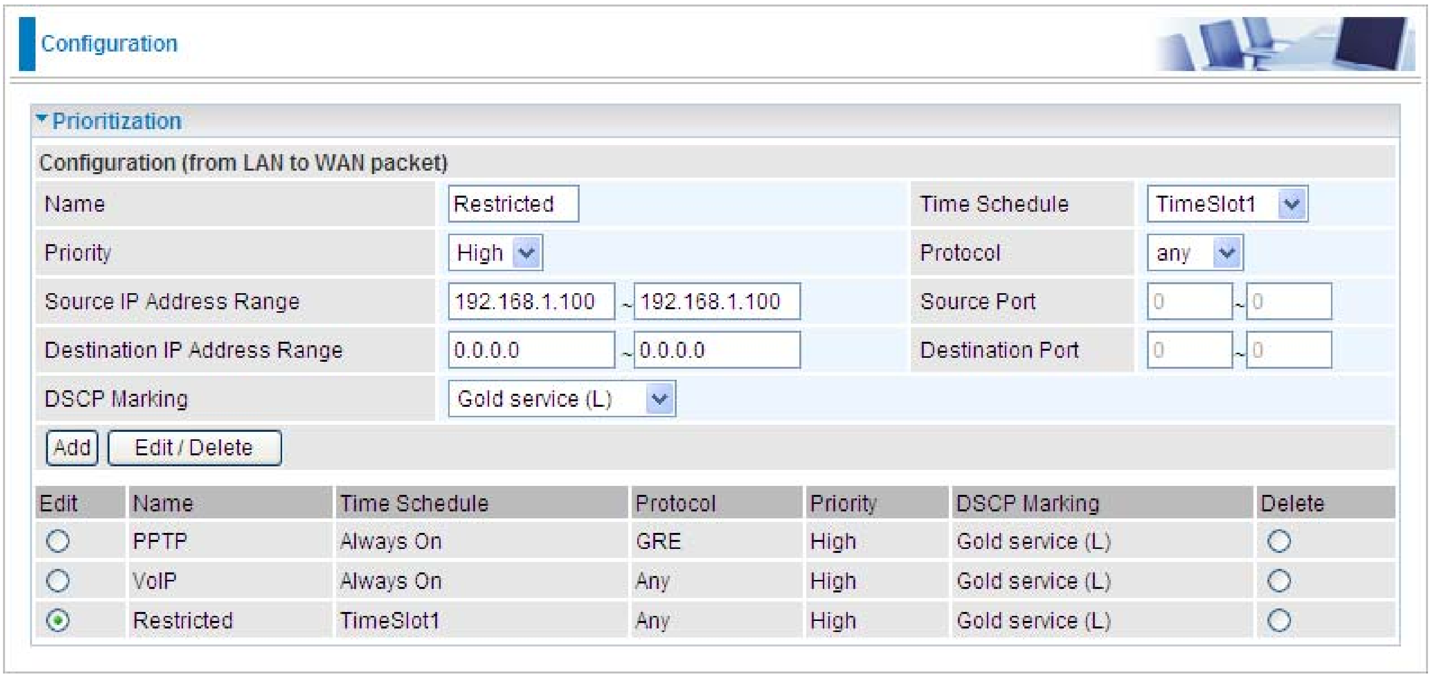
Name	VoIP	Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	192.168.1.1 ~ 192.168.1.1	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
○	PPTP	Always On	GRE	High	Gold service (L)	○
●	VoIP	Always On	Any	High	Gold service (L)	○

The setting above will help to improve the quality of your VoIP service when the the traffic is fully loaded.

Restricted Application

Some companies will setup their FTP servers for data download while others may use FTP for file sharing.



Configuration (from LAN to WAN packet)

Name	Restricted	Time Schedule	TimeSlot1
Priority	High	Protocol	any
Source IP Address Range	192.168.1.100 ~ 192.168.1.100	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
○	PPTP	Always On	GRE	High	Gold service (L)	○
○	VoIP	Always On	Any	High	Gold service (L)	○
●	Restricted	TimeSlot1	Any	High	Gold service (L)	○

The setting above helps to limit the utilization of the FTP upstream rate. Time schedule also helps to limit its utilization only during daytime.

Advanced setting by using IP throttling

IP throttling enables you to set parameters for bandwidth allocation, although the applications maybe located on the same level.

Upstream: 928kbps (29*32kbps)

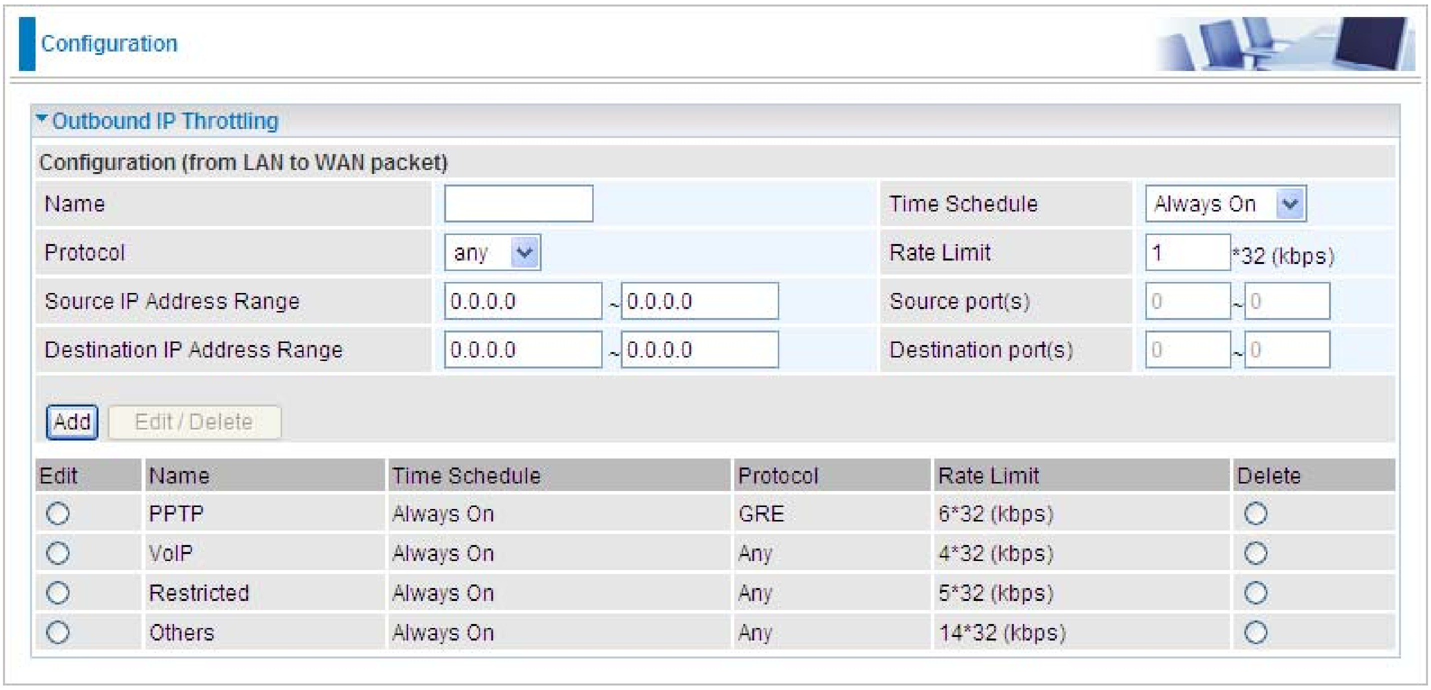
Mission-critical Application: 192kbps (6*32kbps)

Voice Application: 128kbps (4*32kbps)

Restricted Application: 160kbps (5*32kbps)

Other Applications: 448kbps (14*32kbps)

6+4+14+5=29, 29*32kbps=928kbps


Configuration

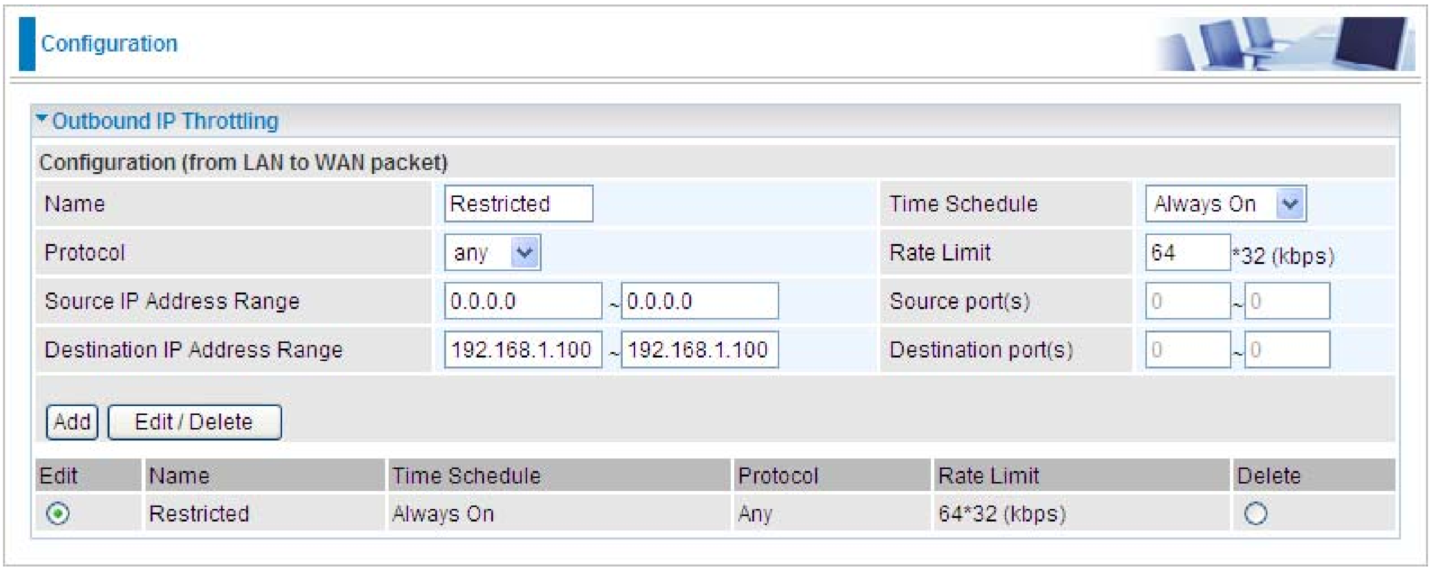
▾ Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name		Time Schedule	Always On
Protocol	any	Rate Limit	1 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
○	PPTP	Always On	GRE	6*32 (kbps)	○
○	VoIP	Always On	Any	4*32 (kbps)	○
○	Restricted	Always On	Any	5*32 (kbps)	○
○	Others	Always On	Any	14*32 (kbps)	○

Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below help you to limit bandwidth for the restricted application.


Configuration

▾ Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name	Restricted	Time Schedule	Always On
Protocol	any	Rate Limit	64 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	192.168.1.100 ~ 192.168.1.100	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
●	Restricted	Always On	Any	64*32 (kbps)	○

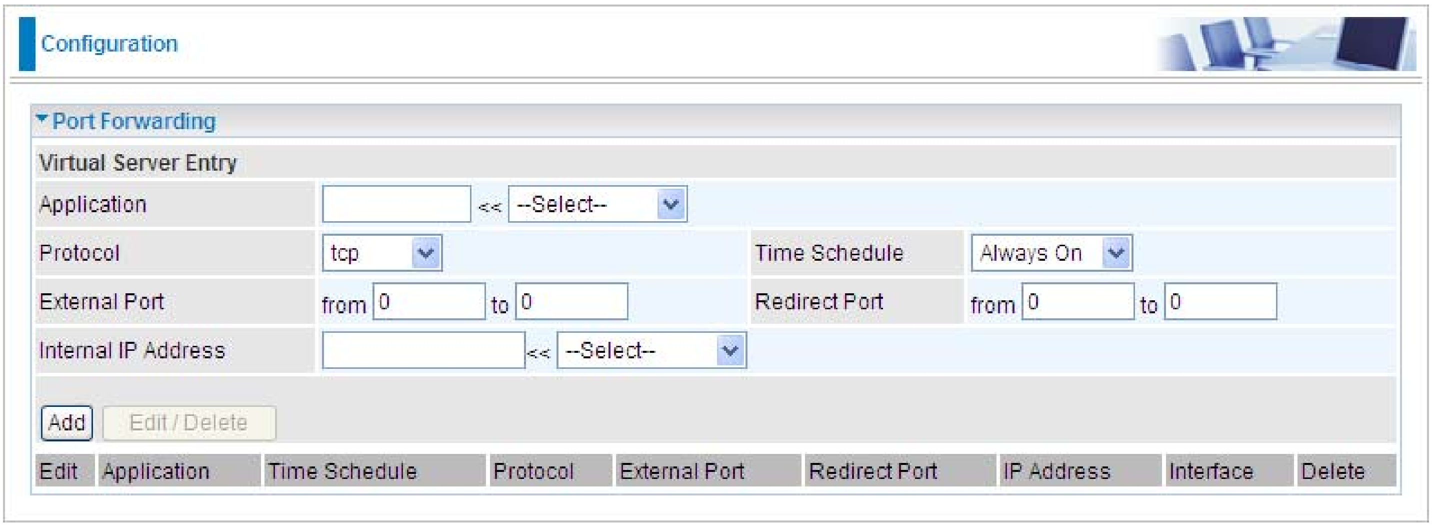
Virtual Server (known as Port Forwarding)

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 will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

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

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.



Virtual Server Entry

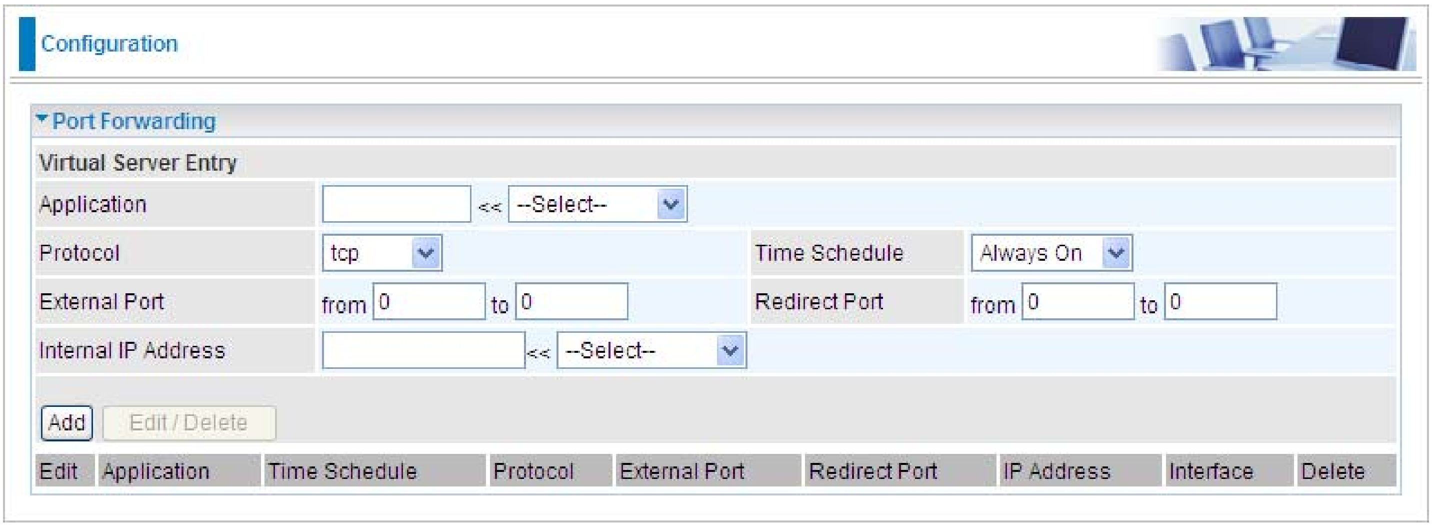
Application	<< --Select--		
Protocol	tcp	Time Schedule	Always On
External Port	from 0 to 0	Redirect Port	from 0 to 0
Internal IP Address	<< --Select--		

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete

Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will 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 an outside user to access the internal server, 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 this service, 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 will be forwarded to the corresponding internal server.



Virtual Server Entry

Application	<< --Select--		
Protocol	tcp	Time Schedule	Always On
External Port	from 0 to 0	Redirect Port	from 0 to 0
Internal IP Address	<< --Select--		

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete

Application: User defined description to identify this entry or click the Application drop-down menu to select an existing predefined rules.

--Select--: 20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by a particular application. Most applications will use TCP or UDP.

Time Schedule: User defined time period to enable your virtual server. You may specify a time schedule or select “Always on” for this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

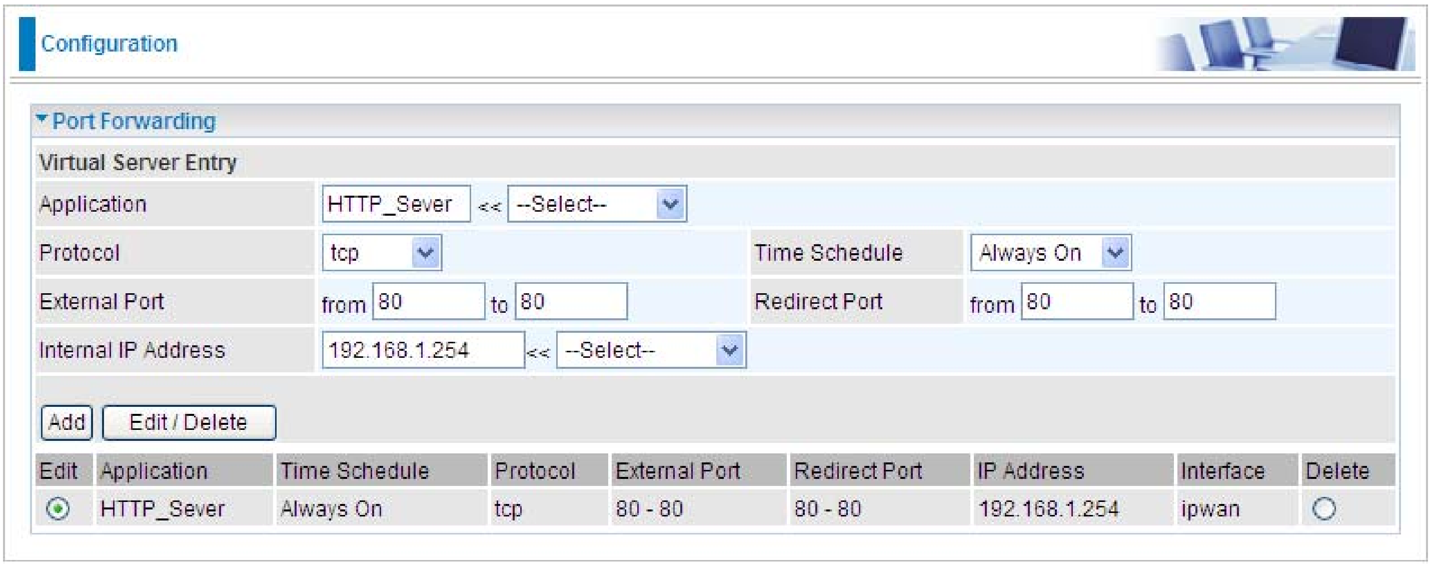
Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. --Select-- List all existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

Example:

If you like to remotely access your Router through the Web/HTTP all the time, you will need to enable port number 80 (Web/HTTP) and map to the Router’s IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with an IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the Application click Helper. A window with a list of predefined rules will pop, you can then select HTTP_Sever.

Application: *HTTP_Sever*
Time Schedule: *Always On*
Protocol: *tcp*
External Port: *80-80*
Redirect Port: *80-80*
IP Address: *192.168.1.254*



Configuration

Port Forwarding

Virtual Server Entry

Application	HTTP_Sever << --Select--		
Protocol	tcp	Time Schedule	Always On
External Port	from 80 to 80	Redirect Port	from 80 to 80
Internal IP Address	192.168.1.254 << --Select--		

Add   Edit / Delete

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
●	HTTP_Sever	Always On	tcp	80 - 80	80 - 80	192.168.1.254	ipwan	○

Add: Click it to apply your settings.

Edit/Delete: Click it to edit or delete this virtual server application.

NOTE:

Using Port Forwarding does have implications, as outside users will be able to connect to the PCs on your network. For this reason, you are adviced to use specific Virtual Server entries just for the port your application requires instead of using DMZ. Doing so will result in all connections from WAN to attempt to access the public IP your DMZ specifies.

Attention

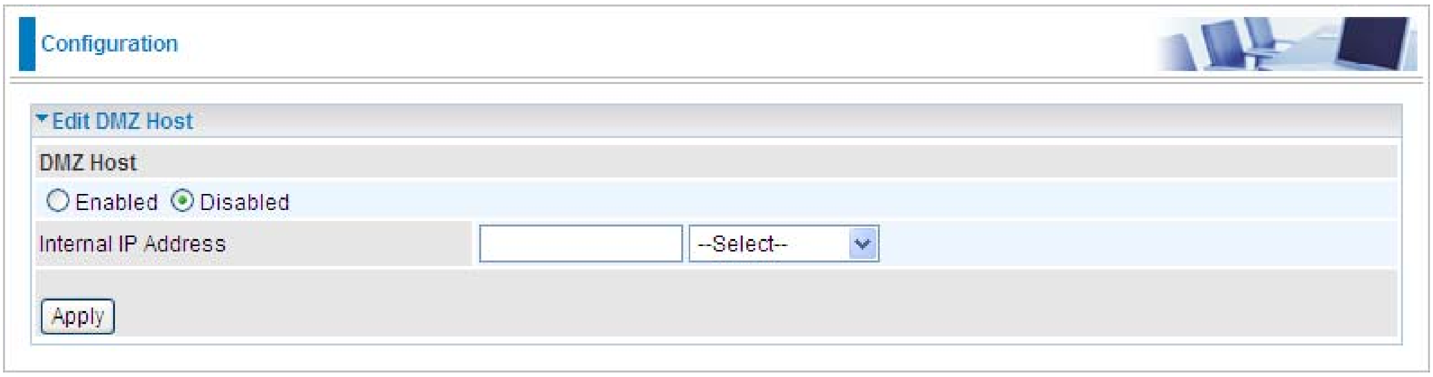
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be 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.

Edit DMZ Host

DMZ Host is a local computer that is exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets especially those that do not use the port number that is being used by any other Virtual Server entries will be checked by the Firewall and NAT algorithms before being passed to the DMZ host.

Cautious: The local computer that is exposed to the Internet may face various security risks.

Go to Configuration > Virtual Server > Edit DMZ Host



DMZ Host

○ Enabled ● Disabled

Internal IP Address [ ] --Select--

Enabled: It activates your DMZ function.

Disabled: As set in default setting, it disables the DMZ function.

Internal IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

--Select-- List all the existing PCs connected to the network. You may assign a PC with an IP address from this list.

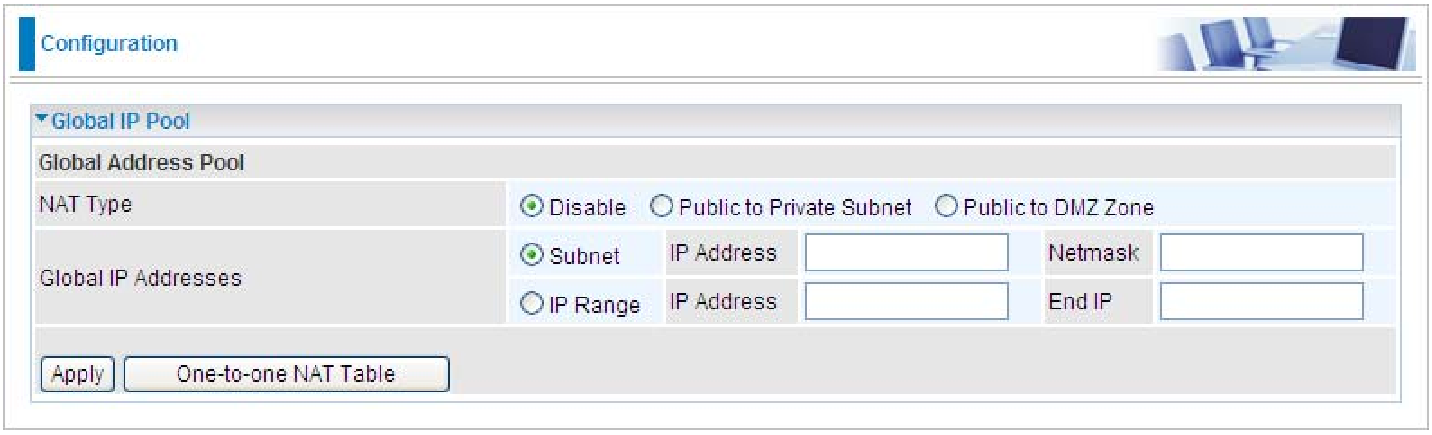
Select the Apply button to apply your changes.

Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private / local IP address to a global / public IP address.

If you have multiple public / WAN IP addresses from your ISP, you are eligible to use these IP addresses in One-to-One NAT .

Go to Configuration > Virtual Server > Edit One-to-one NAT



Configuration

▼Global IP Pool

Global Address Pool				
NAT Type	● Disable ○ Public to Private Subnet ○ Public to DMZ Zone			
Global IP Addresses	● Subnet	IP Address		Netmask
	○ IP Range	IP Address		End IP

Apply | One-to-one NAT Table

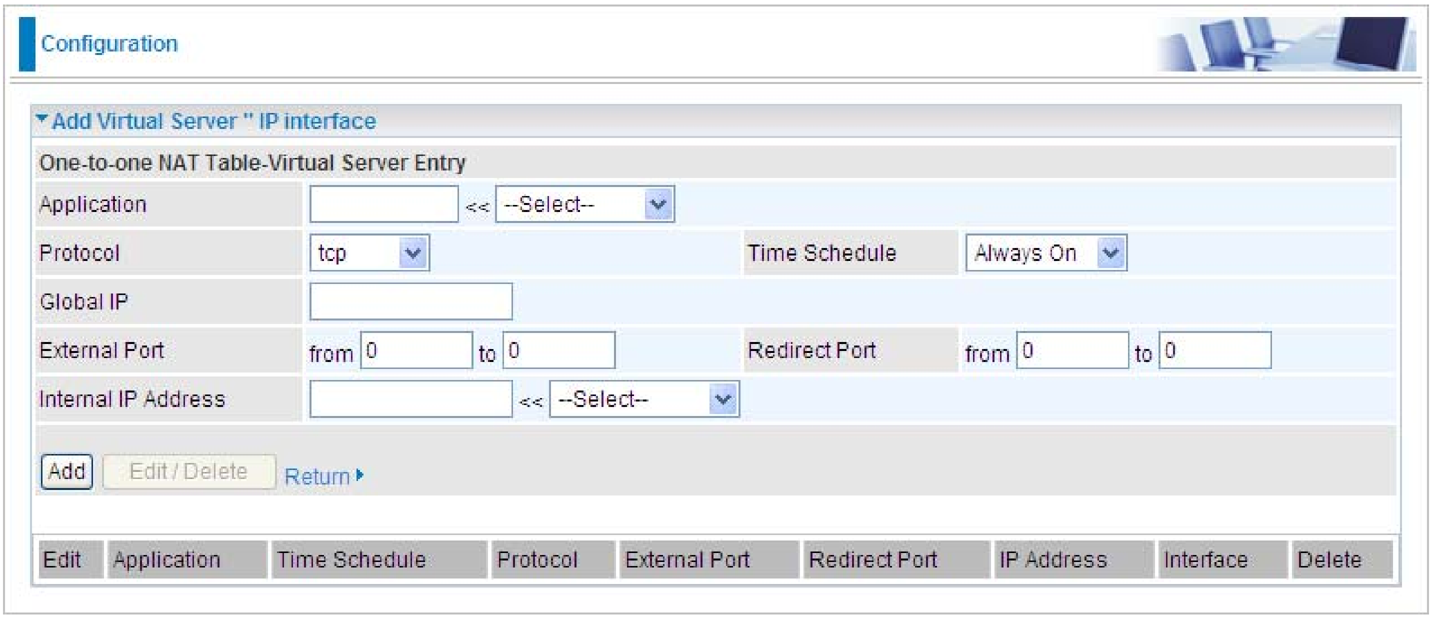
NAT Type: Select the desired NAT type. One-to-One NAT function is set to Disabled by default.

Global IP Address:

> **Subnet:** The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.
>
> **IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 1.1.1.1, end IP: 1.1.1.10

Select the **Apply** button to apply your changes.

Check One-to-one NAT Table to create a new One-to-One NAT rule:



Configuration

▼Add Virtual Server " IP interface

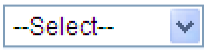
One-to-one NAT Table-Virtual Server Entry			
Application	<< --Select--		
Protocol	tcp	Time Schedule	Always On
Global IP			
External Port	from 0 to 0	Redirect Port	from 0 to 0
Internal IP Address	<< --Select--		

Add | Edit / Delete | Return ▸

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete

Application: User defined description to identify this entry or click the

drop-down menu to select an existing predefined rule.



:20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

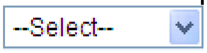
Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

Time Schedule: User defined time period to enable your virtual server. You may specify a time schedule or select "Always on" for this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section.

Global IP: Define a public / WAN IP address for this Application. This Global IP address must be defined in the Global IP Address blank.

External Port: The Port number on the Remote / WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network which provides the virtual server application. 

List all the existing PCs connecting to the network. You may assign a PC with an IP address from this list.

Select the **Add** button to apply your changes.

Example: List of some well-known and registered port numbers.

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 ports numbers 0 to 1023 are reserved for privileged services and are designated as "well-known ports" (Please refer to Table 5). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

For further information, please see IANA's website at **http://www.iana.org/assignments/port-numbers**

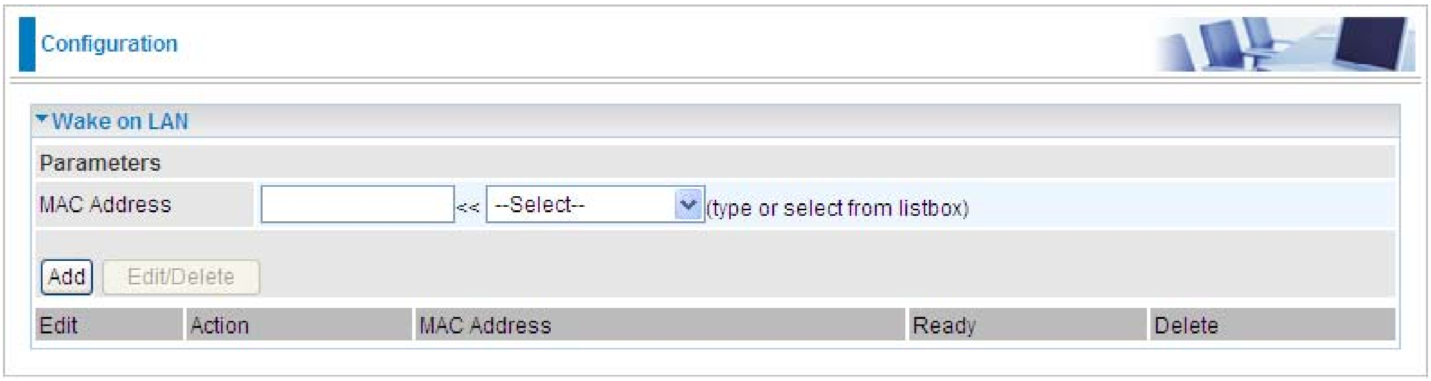
For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at **http://www.billion.com**

Table 5: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Contro
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) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Wake on LAN

This feature provides greater flexibility for users to turn on / boot the computer of the network from a remotely site.



Configuration

Wake on LAN

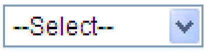
Parameters

MAC Address [ ] << --Select-- (type or select from listbox)

Add Edit/Delete

Edit	Action	MAC Address	Ready	Delete

MAC Address: Enter the MAC address of the target computer or you can select the MAC address directly from the Select drop down menu on the right.

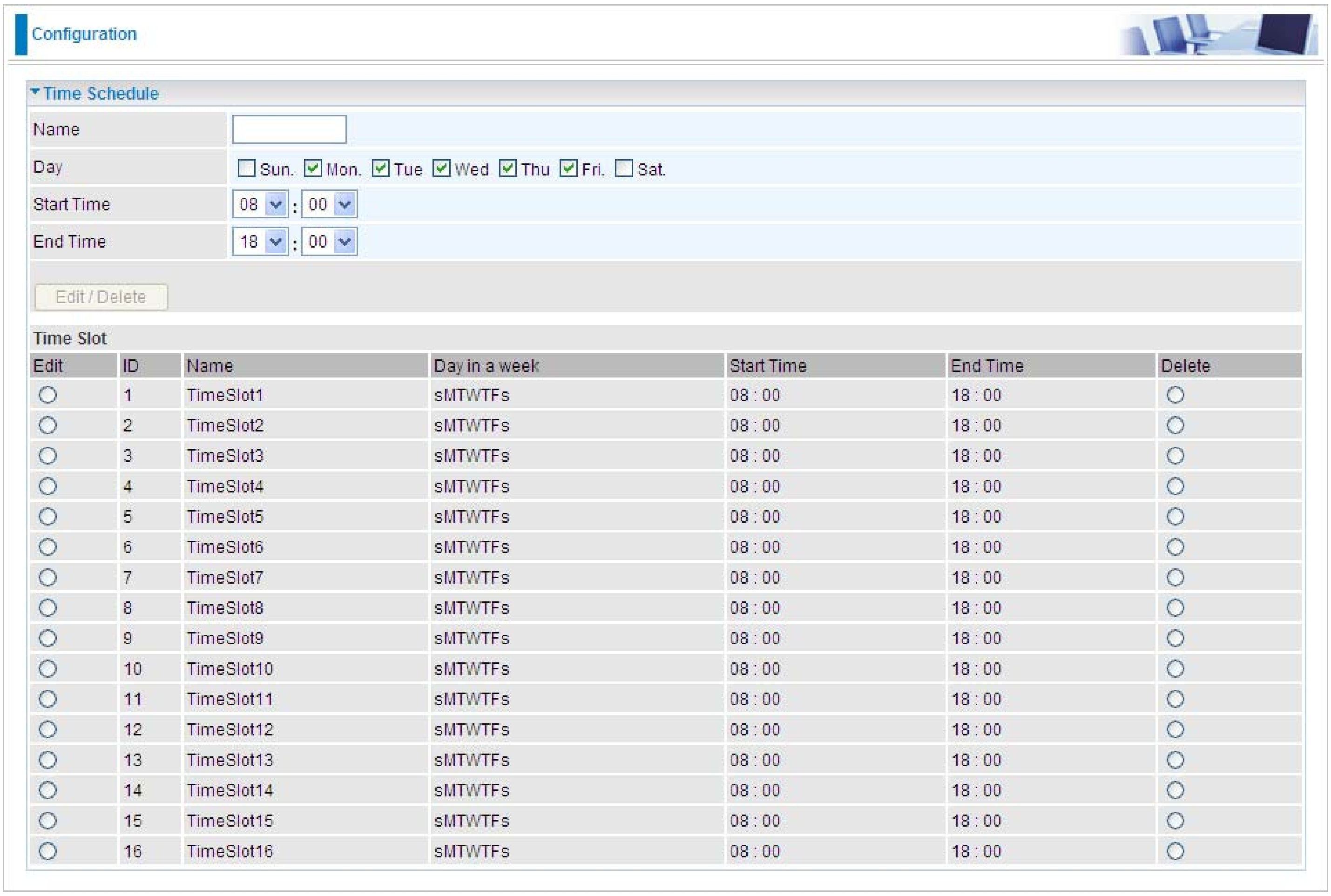


: You can select the MAC from this list.

Time Schedule

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

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



Name	
Day	☐ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. ☐ Sat.
Start Time	08 : 00
End Time	18 : 00

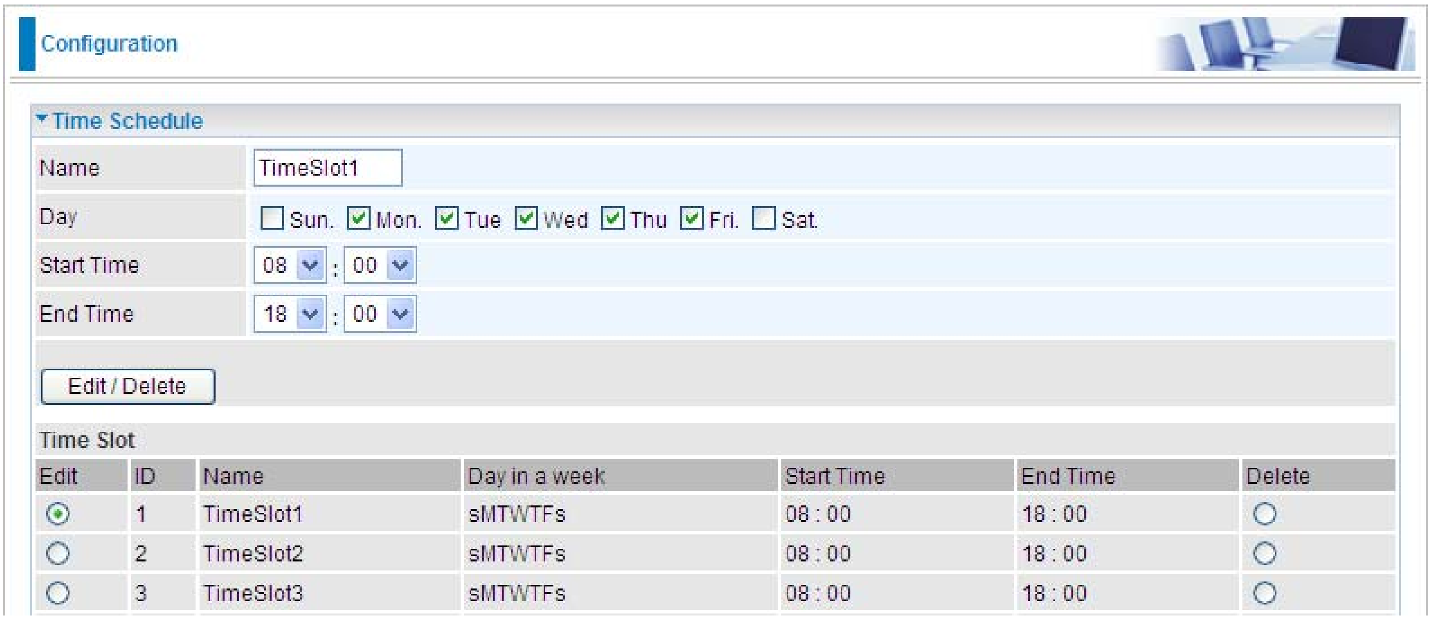
Time Slot

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
○	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	○
○	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	○
○	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	○
○	4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	○
○	5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	○
○	6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	○
○	7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	○
○	8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	○
○	9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	○
○	10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	○
○	11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	○
○	12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	○
○	13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	○
○	14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	○
○	15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	○
○	16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	○

Configuration of Time Schedule

Edit a Time Slot

1. Choose any Time Slot (ID 1 to ID 16) to edit, click Edit radio button.



Configuration

Time Schedule

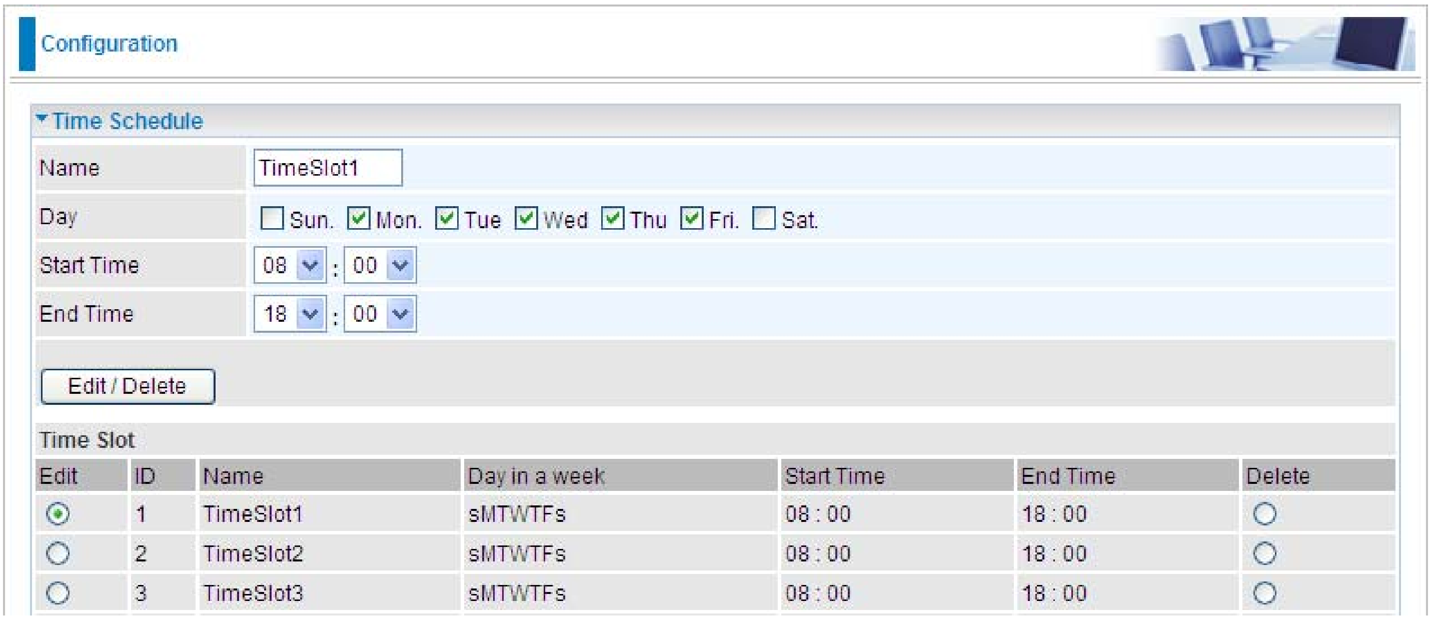
Name	TimeSlot1
Day	☐ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. ☐ Sat.
Start Time	08 : 00
End Time	18 : 00

Time Slot

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
●	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	○
○	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	○
○	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	○

Note: Watch it carefully, the days you have selected will present in capital letter. Lower case letter shows the day(s) is not selected, and no rule will apply on this day(s).

2. A detailed setting of this Time Slot will be shown.



Configuration

Time Schedule

Name	TimeSlot1
Day	☐ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. ☐ Sat.
Start Time	08 : 00
End Time	18 : 00

Edit / Delete

Time Slot

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
●	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	○
○	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	○
○	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	○

ID: This is the index of the time slot.

Name: A user defined description to identify this time portfolio.

Day in a week: The default is set from Monday through Friday. You may also specify the days for the schedule to be applied to.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

Choose Edit radio button and click Edit/Delete button to apply your changes.

Delete a Time Slot

Click on the Delete radio button of the Time Slot you wish to delete under the Time Slot section, and then click the Edit/Delete button to confirm the deletion of the selected Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

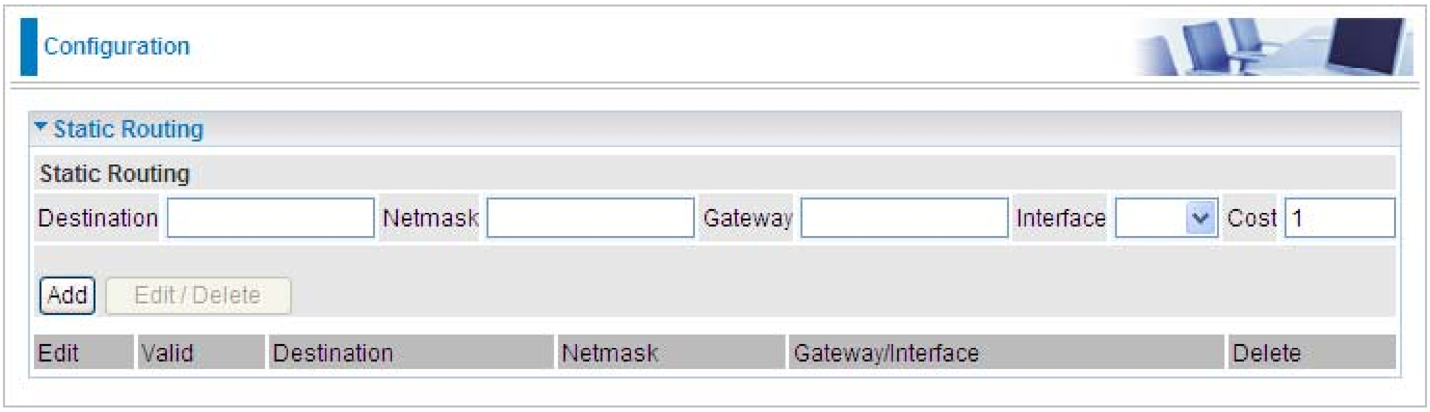
Advanced

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.

These are the items within the Advanced section: **Static Route, Static ARP, Dynamic DNS, Check Email, Device Management** and **IGMP.**

Static Route

Go to Configuration > Advanced > Static Route.



Configuration

▾ Static Routing

Static Routing

Destination		Netmask		Gateway		Interface		Cost	1

Edit	Valid	Destination	Netmask	Gateway/Interface	Delete

Destination: This is the destination subnet IP address.

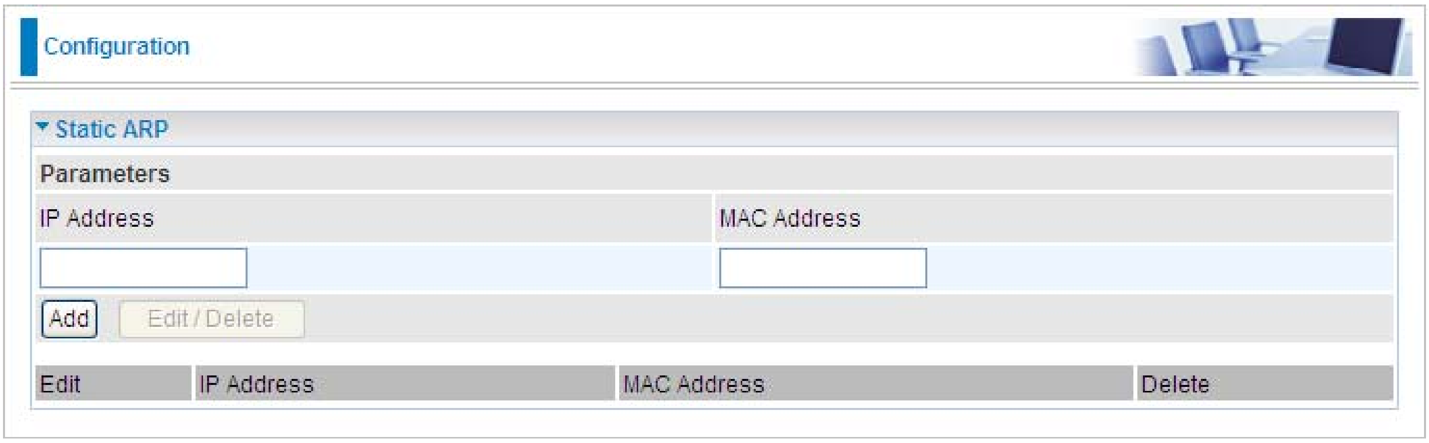
Netmask: Subnet mask of the destination IP addresses based on the above destination subnet IP.

Gateway: This is the gateway IP address to which packets are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1.

Static ARP



IP Address: Fill in the IP address of the host computer that is sending the data packet.

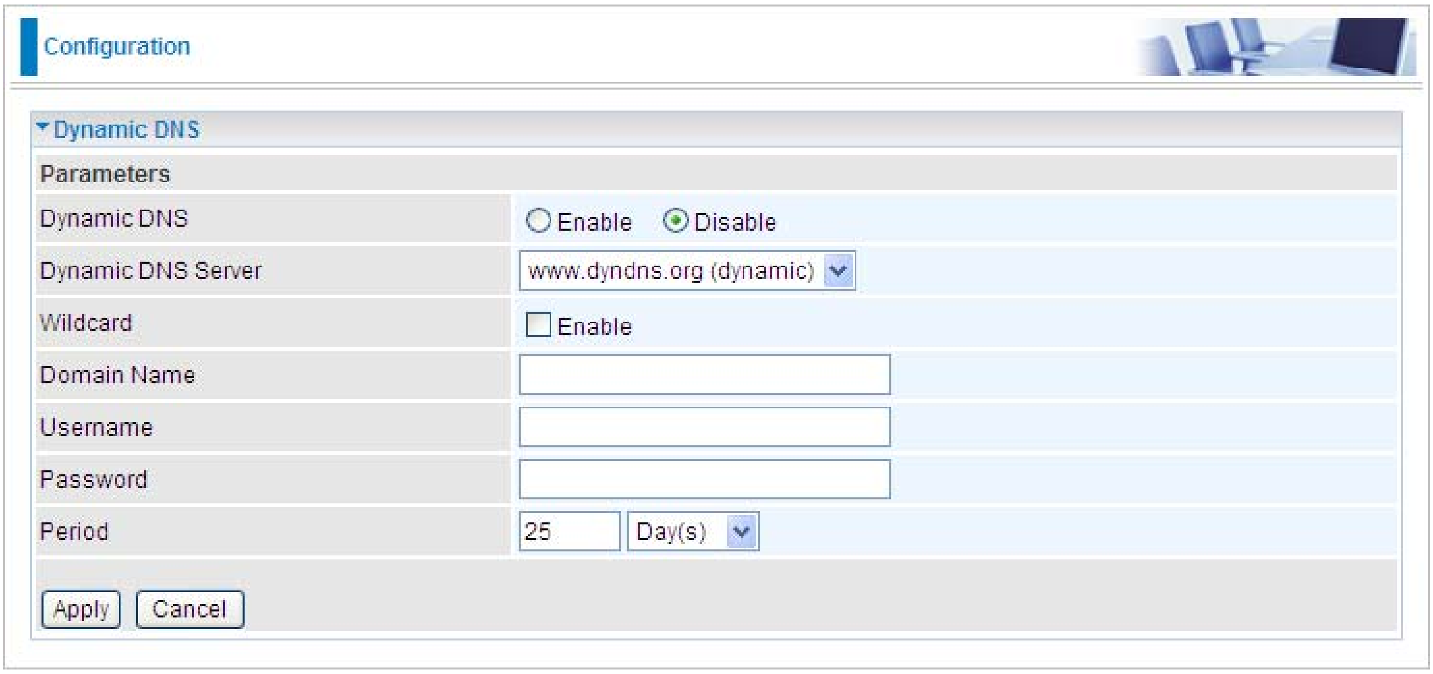
MAC Address: Fill in the MAC address of the computer that the incoming data packets are to be forwarded.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your 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 will first need to register and establish an account with the Dynamic DNS provider using their website, for example **http://www.dyndns.org/**

There are more than 5 DDNS services supported.



Configuration

Dynamic DNS

Parameters	
Dynamic DNS	○ Enable ● Disable
Dynamic DNS Server	www.dyndns.org (dynamic)
Wildcard	□ Enable
Domain Name	
Username	
Password	
Period	25 Day(s)

Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The following fields will be activated and required.

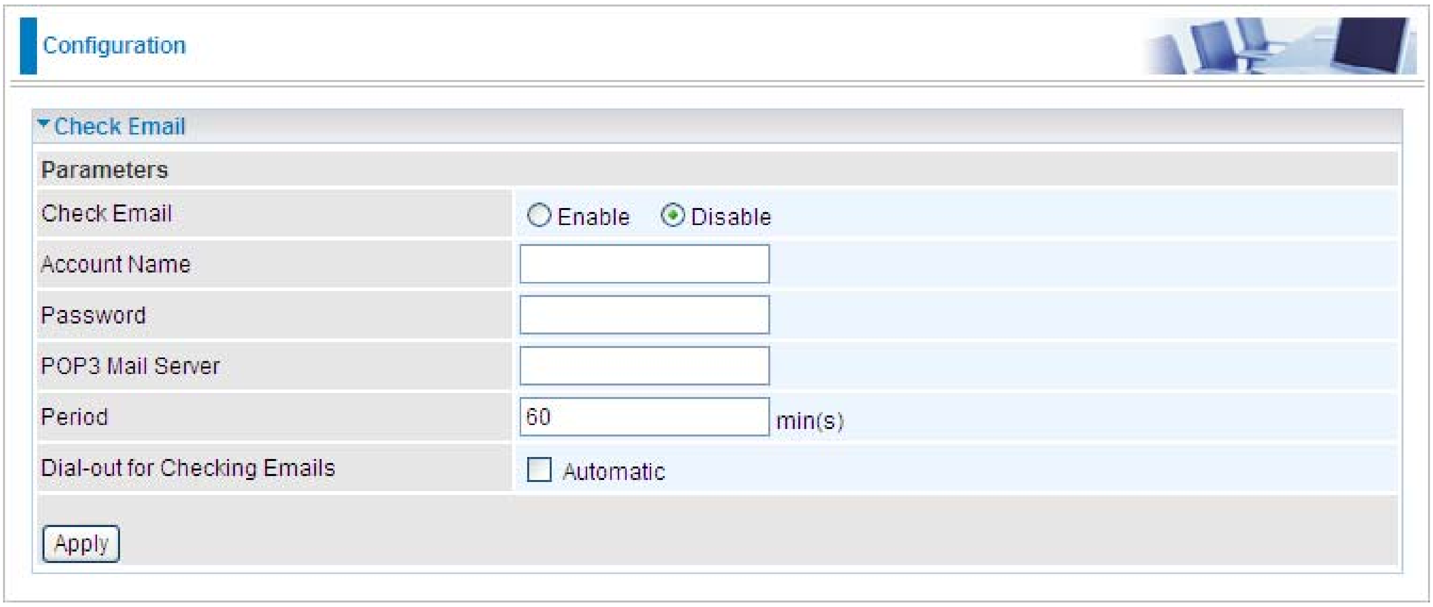
Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain Name, Username and Password: Enter your registered domain name and your username and password for this service.

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Check Email

This function allows you to have the router check your POP3 mailbox for new Email messages. The Mail LED on your router will light when it detects new messages waiting for download. You may also view the status of this function using the Status – Email Checking section of the web interface, which also provides details on the number of new messages waiting. See the Status section of this manual for more information.



Configuration

▾Check Email

Parameters	
Check Email	○ Enable ● Disable
Account Name	
Password	
POP3 Mail Server	
Period	60 min(s)
Dial-out for Checking Emails	□ Automatic

Check Email:

Disable: Check to disable the Email checking function.

Enable: Check to enable the Email checking function. The following fields will be activated and required.

Account Name: Enter the name (login) of the POP3 account you wish to check. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account's password.

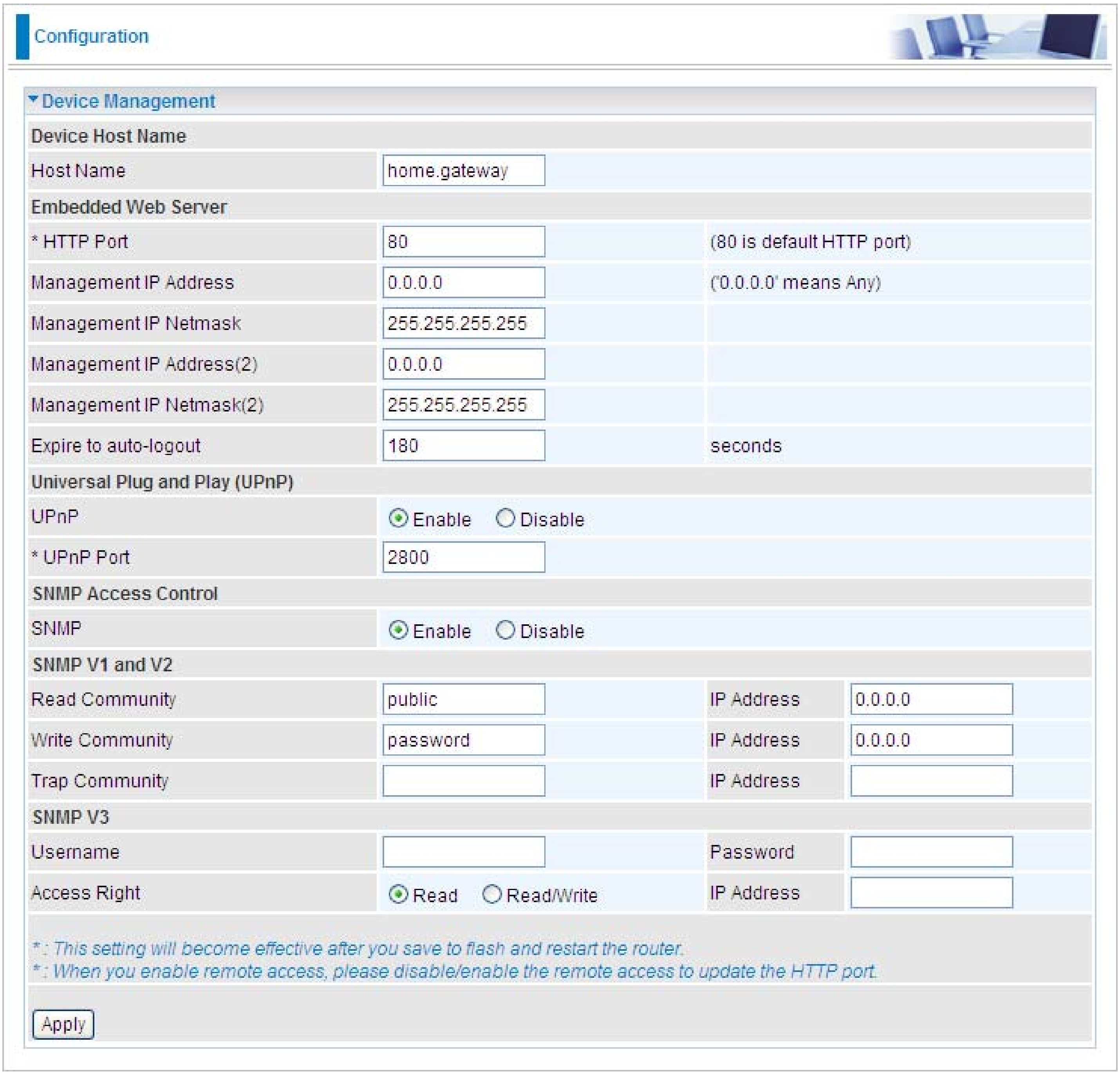
POP3 Mail Server: Enter your (POP) mail server name. You Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Period: Enter the value in minutes between periodic mail checks.

Dial-out for checking Emails: When the function is enabled, your ADSL router will connect to your ISP automatically to check emails if your Internet connection dropped. Please be careful when using this feature if your ADSL service is charged by time online.

Device Management

The Device Management advanced configuration setting allows you to control your router security option and device monitoring features.



Configuration

▾ Device Management

Device Host Name			
Host Name	home.gateway		
Embedded Web Server			
* HTTP Port	80	(80 is default HTTP port)	
Management IP Address	0.0.0.0	('0.0.0.0' means Any)	
Management IP Netmask	255.255.255.255		
Management IP Address(2)	0.0.0.0		
Management IP Netmask(2)	255.255.255.255		
Expire to auto-logout	180	seconds	
Universal Plug and Play (UPnP)			
UPnP	● Enable ○ Disable		
* UPnP Port	2800		
SNMP Access Control			
SNMP	● Enable ○ Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	● Read ○ Read/Write	IP Address	

*: This setting will become effective after you save to flash and restart the router.
*: When you enable remote access, please disable/enable the remote access to update the HTTP port.

Device Host Name

Host Name: Assign it a name.

Note: The Host Name must have more than a word. These two words should be connected with a '.' period inbetween.

Example:
Host Name: homegateway ==> Incorrect
Host Name: home.gateway or my.home.gateway ==> Correct)

Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number that the router embedded web server (for web-based configuration) will use. The default value is the standard HTTP port 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify an IP address for logon and access the router web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a duration for the system to log the user out of the configuration session automatically.

For Example:

User A changes the HTTP port number to 100, specifies their own IP address as 192.168.1.55 and sets the logout time as 100 seconds. The router will only allow User A to access the Web GUI from the IP address 192.168.1.55 by typing **http://192.168.1.254:100** in their web browser. Nevertheless, after 100 seconds the device will automatically log User A out of the system.

Universal Plug and Play (UPnP)

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

Both 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) while Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to gain support for UPnP. Nevertheless 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: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used, you may wish to change the port.

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

SNMP V1 and V2:

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

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

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

SNMP V3:

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

SNMP Version: SNMPv2c and SNMPv3

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

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

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II) System group

System group

Interface group

Address Translation group

IP group

ICMP Group

TCP group

UDP group

EGP (not applicable)

Transmission

SNMP group

From RFC 1650 (EtherLike-MIB)

dot3stats

From RFC 1493 (Bridge MIB)

dot1 dBase group

dot1 dTp group

dot1 dStp group (if configured as spanning tree)

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 RFC 1573 (IfMIB)

ifMIBObjects group

From RFC 1695 (atmMIB)

atmMIBObjects

From RFC 1907 (SNMPv2)

only snmpSetSerialNo OID

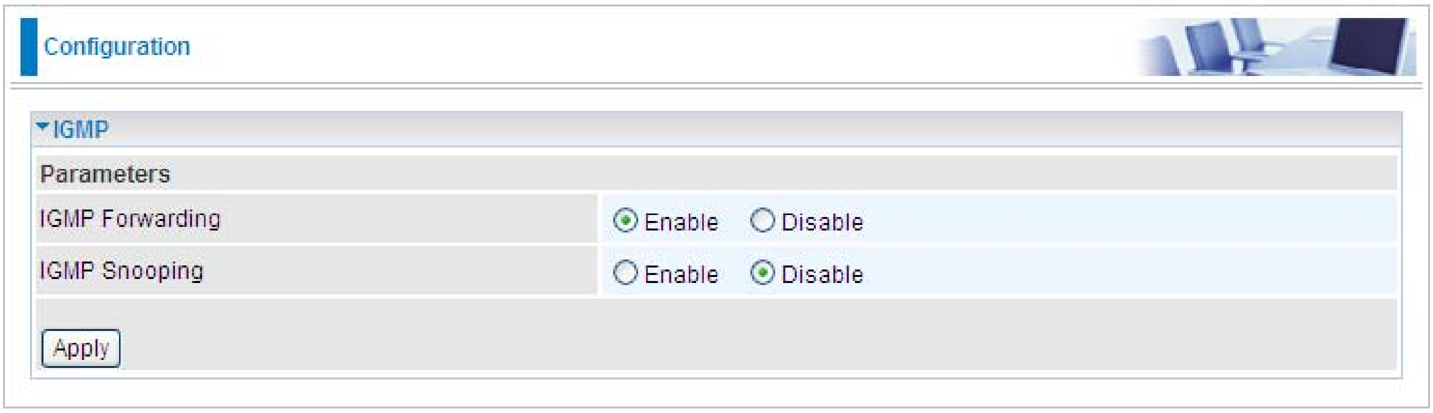
From RFC 1471 (PPP/LCP MIB)

pppLink group

pppLgr group (not applicable)

IGMP

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



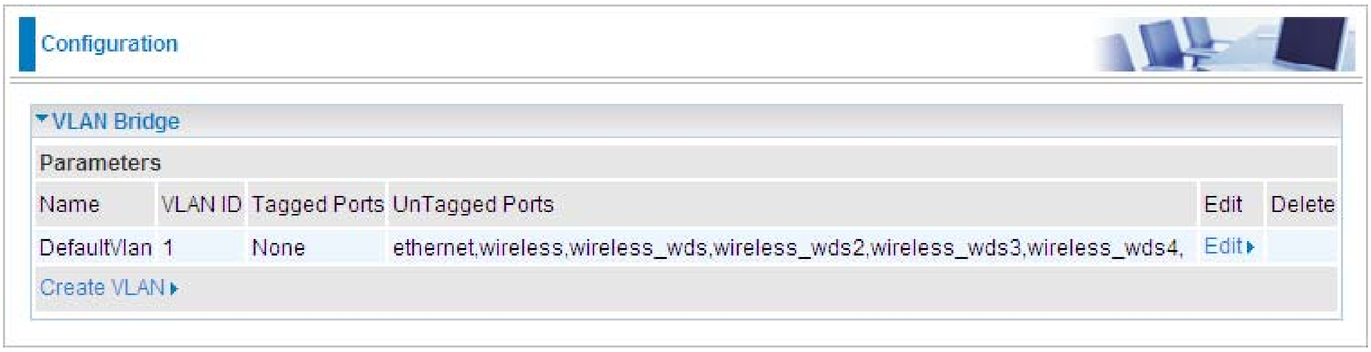
IGMP Forwarding	● Enable ○ Disable
IGMP Snooping	○ Enable ● Disable

IGMP Forwarding: Accepting multicast packet. Default is set to Enable.

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

VLAN Bridge

This section allows you to create VLAN group and specify the members of each group.



Name	VLAN ID	Tagged Ports	UnTagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,wireless_wds2,wireless_wds3,wireless_wds4,	Edit ▸	

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

To exit the router web interface, choose **Logout**. Please save your configuration setting before logging out of the system.

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the Advanced section of this manual for more information.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on.	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the reset button for more than 6 seconds.

Problems with WAN interface

Problem	Suggested Action
Initialization of PVC connection (line-sync)fail	Make sure that the telephone cable is properly connected between the ADSL port and the wall jack. The ADSL LED on the front panel should lit. 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 problem, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnection)	Make sure that all devices (e.g telephone, fax machine, analogue modems) that are connected to the telephone line as your router have a line filter connected between them and the wall outlet (unless your are using a Central Splitter or Central Filter installed by a qualified and licensed electrician). Make sure that alll line filters are correctly installed as missing line filters or incorrect installation of line filters can cause ADSL connection problem, including frequent disconnections.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

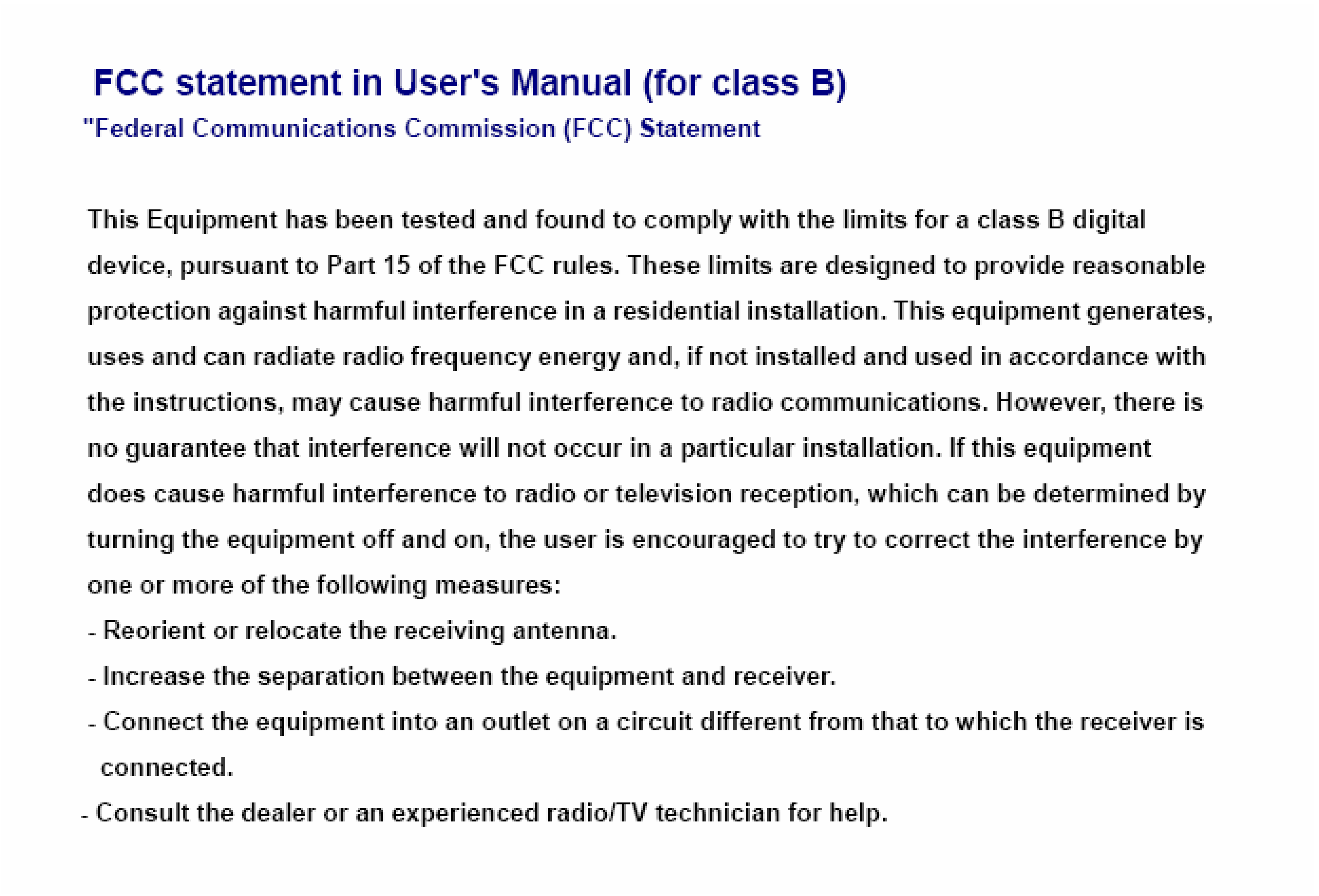
Appendix: Product Support & Contact

Following the suggestions listed in the Troubleshooting section of the user manual can help you solve most of your problems. However if your problems persist or you come across other technical issues that are not listed in the Troubleshooting section, please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

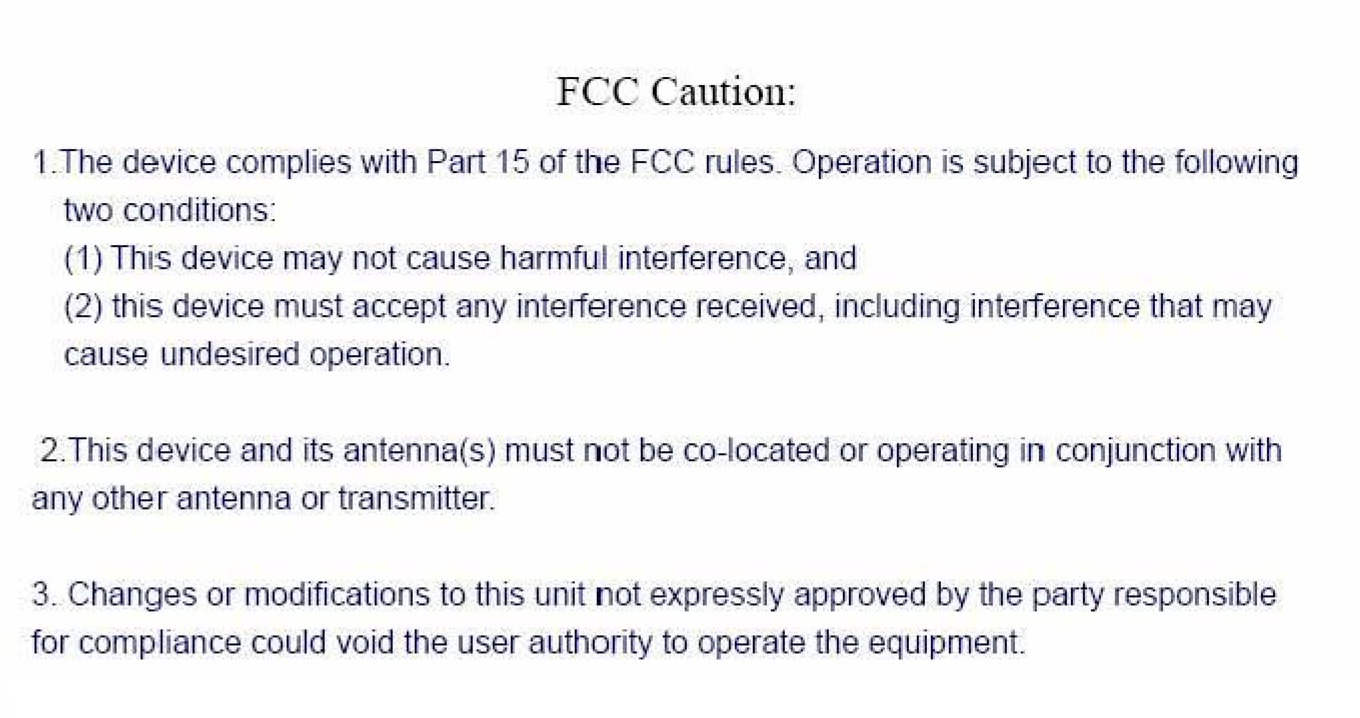


FCC statement in User's Manual (for class B)

"Federal Communications Commission (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 or more 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.



FCC Caution:

1.The 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.

2.This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.