BiPAC 7402NX(L)

802.11n 3G/ADSL2+ (VPN) Firewall Router

User Manual

Version released: 6.24b.dm2

Last Revision Date: 9-30-2010

Table of Contents

Chapter 1: Introduction

Introduction to your Router

Welcome to the BiPAC 7402NX(L) 802.11n 3G/ ADSL2+ (VPN) 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**
  This router complies with worldwide ADSL standards. It supports downstream rates of up to 12/24 Mbps with ADSL2/2+, 8 Mbps with ADSL, and upstream rates of up to 1 Mbps. With this technology, users enjoy not only high-speed ADSL service but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much more quickly and easily than ever. In particular, by doubling the upstream data rate, the Annex M standard included in the BiPAC 7402NX model supports the latest ADSL2/2+ for higher upload speeds.

- **Virtual Private Network (VPN) (VPN model only)**
  It allows user to make a tunnel with a remote site directly to secure the data transmission among the connection. User can use embedded PPTP and L2TP client/server, IKE and IPSec which are supported by this router to make a VPN connection or users can run the PPTP client in PC and the router already provides IPSec and PPTP pass through function to establish a VPN connection if the user likes to run the PPTP client in his local computer.

- **3G**

  With 3G-based Internet connection (requires an additional 3G USB modem), user can access internet through 3G - whether you're seated at your desk or taking a cross-country train trip.

- **EWAN**
  Besides using 3G/ADSL to get connected to the Internet, the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online.

- **Dual WAN**
  Dual WAN is a new way of getting connected to the internet which is to use each two of the 3G/ADSL/EWAN to deal with the unexpected case and balance traffic load. That is a way of improving greatly the robustness.

- **802.11n Wireless AP with WPA Support**
  With an integrated 802.11n Wireless Access Point in the router, the device delivers up to 6 times faster speeds and 3 times farther range than an 802.11b/g wireless network. It offers a quick yet easily accessible and mobile to the users among wired network, wireless network, broadband connection (ADSL). In addition to having a 300Mbps. data rate, it is also backward compatible with existing 802.11b/11g equipments. The supported features of Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) enhance the security level of data protection and access control via Wireless LAN.

- **Fast Ethernet Switch**
  A 4-port 10/100/1000Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T, 100Base-TX and 1000Base-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 over ATM (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.

- **IPv6 supported**

  Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4.

  IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2128 (about 3.4×1038) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

  IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).

  Network security is integrated into the design of the IPv6 architecture. Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread optional deployment first in IPv4 (into which it was back-engineered). The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

- **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 local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or 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 the router in high humidity or high temperatures.
- Do not use the same power source for the router as other equipment.
- Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Avoid using this product and all accessories outdoors.

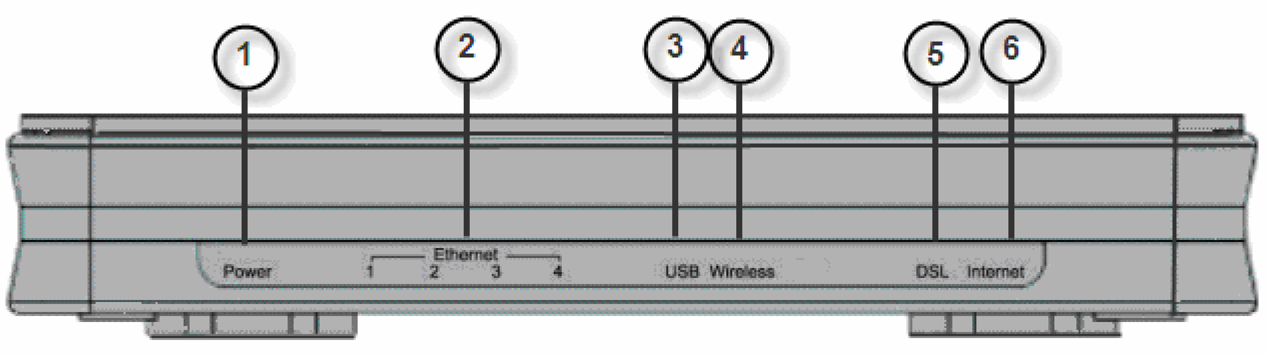
Attention

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

Package Contents

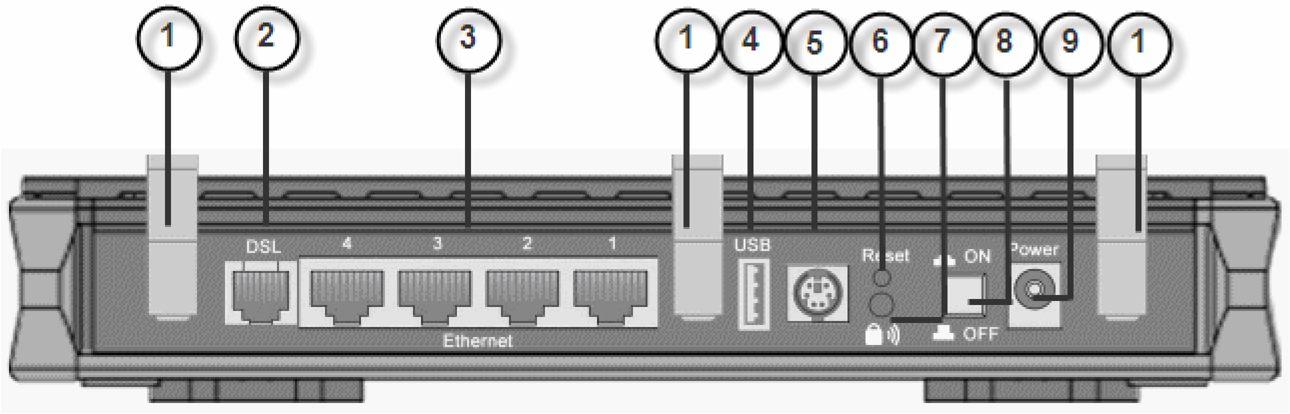
- **BiPAC 7402NX(L) 802.11n 3G/ ADSL2+ (VPN) Firewall Router**
- **CD containing the on-line manual**
- **RJ-11 ADSL/ telephone cable**
- **Ethernet (CAT-5 LAN) cable**
- **Three 2dbi detachable antennas**
- **Power adapter**
- **PS2-RS 232 console cable**
- **Quick Start Guide**
- **Splitter/ Micro-filter (Optional)**

The Front LEDs



LED		Meaning
1	**Power**	Both red and green LEDs lit together when power is ON. Lit red means system failure. Restart the device or contact support. Lit green when the device is ready.
2	**Ethernet Port 1X - 4X** (RJ-45 connector)	Lit when one of LAN ports are connected to Ethernet devices. If the speed of transmission hits 1000Mbps light will appear Green; If the speed of transmission hits 100Mbps light will appear Orange. If the speed of transmission hits 10Mbps, light will not shine. Blinking when data is Transmitted / Received.
3	**USB**	Lit green when the device is connected to a USB device and ready. Flashing when the device is sending/receiving data.
4	**Wireless**	Lit green when the wireless connection is established. Flashing when the device is sending/receiving data. Flash once per second while wi-fi protected setup is in progress.
5	**DSL**	Lit Green when the device is successfully connected to an ADSL DSLAM ("line sync").
6	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when the device is in bridge mode or when WAN connection is absent.

The Rear Ports



Port		Meaning
1	**Antenna**	Connect the detachable antenna to this port.
2	**DSL**	Connect the supplied RJ-11 ("telephone") cable on this port when connecting to the ADSL/telephone network.
3	**Ethernet** **1X - 4X** (RJ-45 connector)	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, 100Mbps or 1000Mbps.
4	**USB**	Connect the USB cable on this port.
5	**Console**	Console port. 3G/ HSDPA USB modem backup for Internet access.
6	**RESET**	To be sure the device is being turned on → press RESET button for: **1-3 seconds**: quick reset the device. **6 seconds above, and 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.
7	**WPS**	Push WPS button for less than 5 sec to trigger Wi-Fi Protected Setup function; push WPS button for more than 5 sec to enable/disable WLAN Service.
8	**Power**	Power ON/OFF switch
9	**Power Switch**	Connect the supplied power adapter to this jack.

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 with your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 7/98/NT/2000/XP/Me, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect with the router, either through an external repeater hub to the router or directly connecting with PCs. However, to be sure PCs have an Ethernet interface installed properly prior to connecting to 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's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

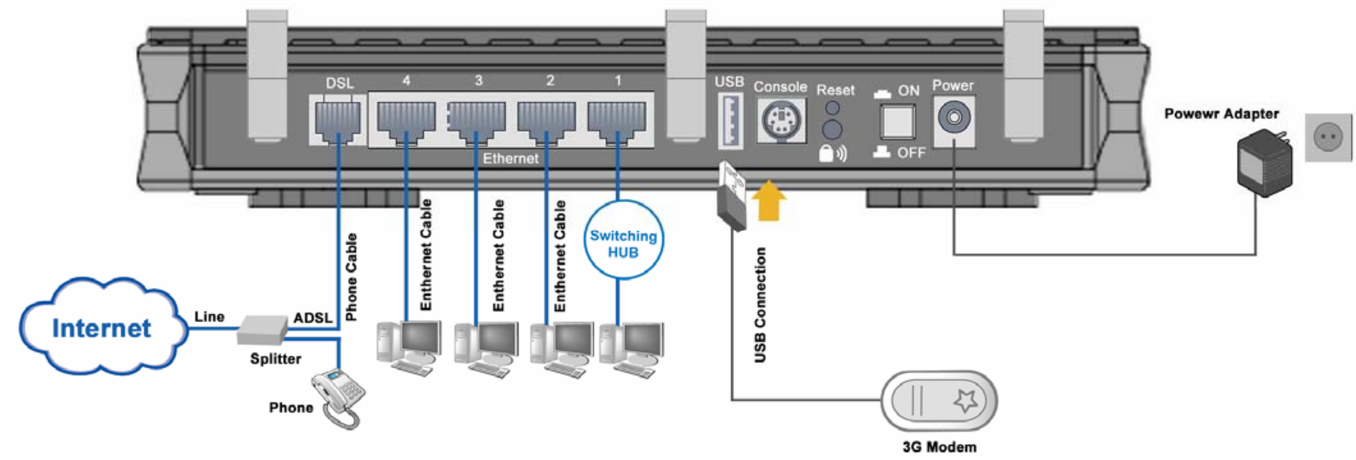
Please follow the steps below for your PC's network environment installation.

NOTE:

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

Connecting Your Router

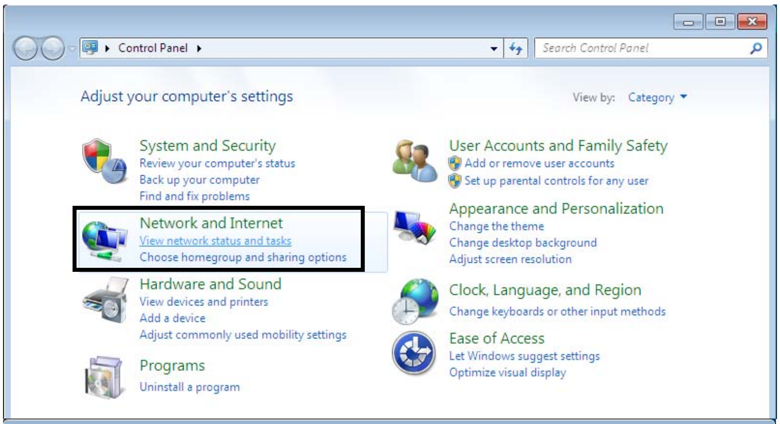
1. Connect this router to a **LAN** (Local Area Network) and the ADSL/telephone (**ADSL**) network.
2. Power on the device.
3. Make sure the **Power** is lit steadily and that the **LAN** LED is lit.
4. Connect RJ-11 cable to LINE Port when connecting to the telephone wall jack.
5. Connect USB 2.0 cable.



Configuring PCs in Windows 7

1. Go to **Start**. Click on **Control Panel**.

Then click on **Network and Internet**.



Control Panel ▸

Search Control Panel

Adjust your computer's settings

View by: Category ▾

System and Security
Review your computer's status
Back up your computer
Find and fix problems

User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user

Network and Internet
View network status and tasks
Choose homegroup and sharing options

Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

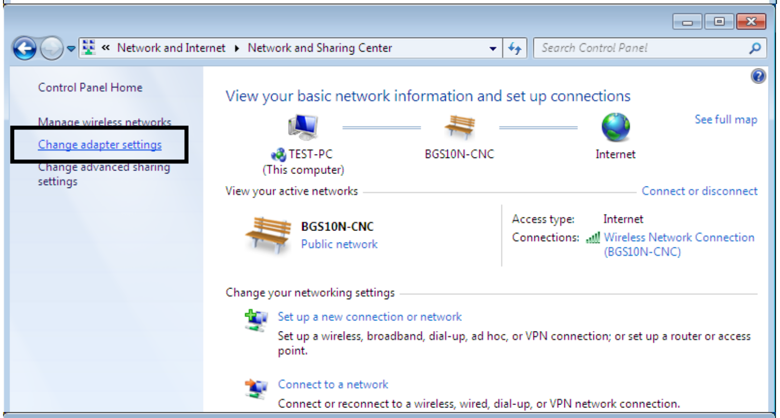
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Clock, Language, and Region
Change keyboards or other input methods

Ease of Access
Let Windows suggest settings
Optimize visual display

Programs
Uninstall a program

2. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



« Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

TEST-PC (This computer) — BGS10N-CNC — Internet

See full map

View your active networks

Connect or disconnect

BGS10N-CNC
Public network

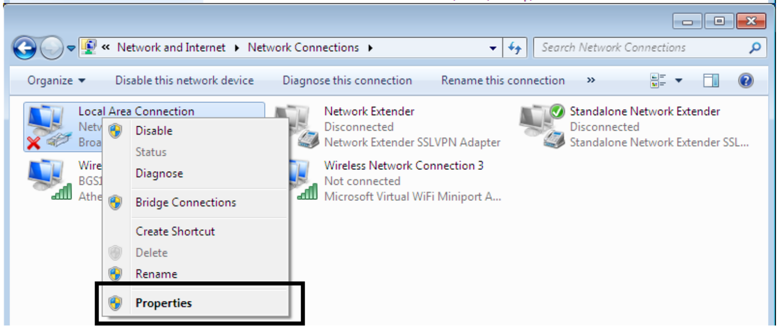
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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



« Network and Internet ▸ Network Connections ▸

Search Network Connections

Organize ▾ Disable this network device Diagnose this connection Rename this connection »

Local Area Connection
Netw
Broa

Wire
BGS1
Athe

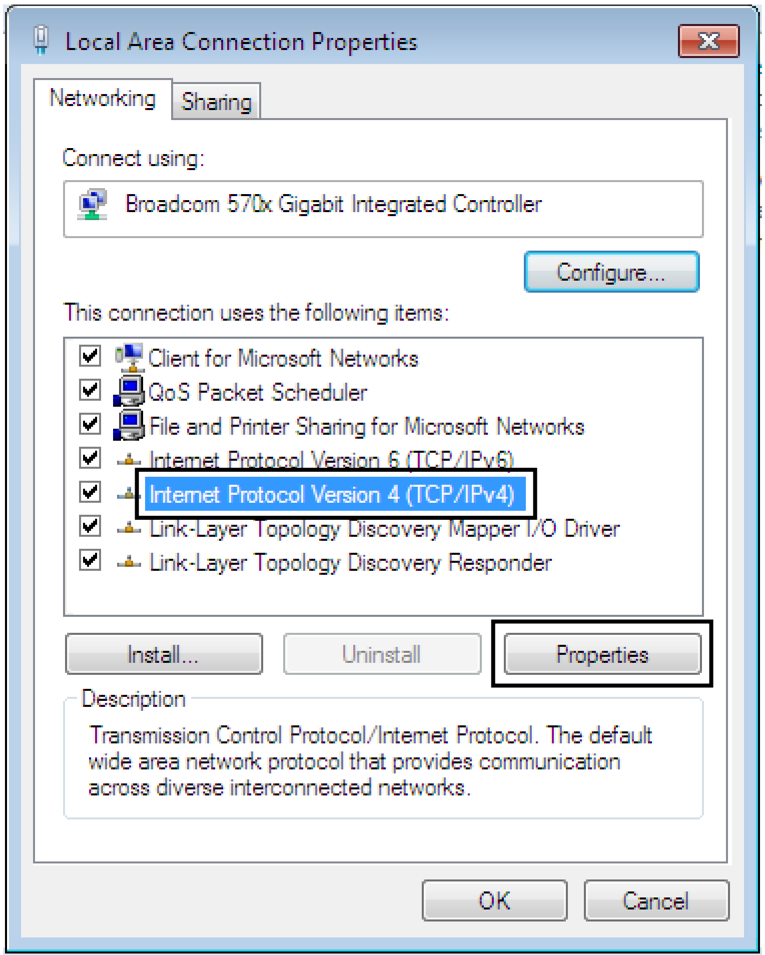
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

Network Extender
Disconnected
Network Extender SSLVPN Adapter

Standalone Network Extender
Disconnected
Standalone Network Extender SSL...

Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...

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



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

Configure...

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

Install... | Uninstall | Properties

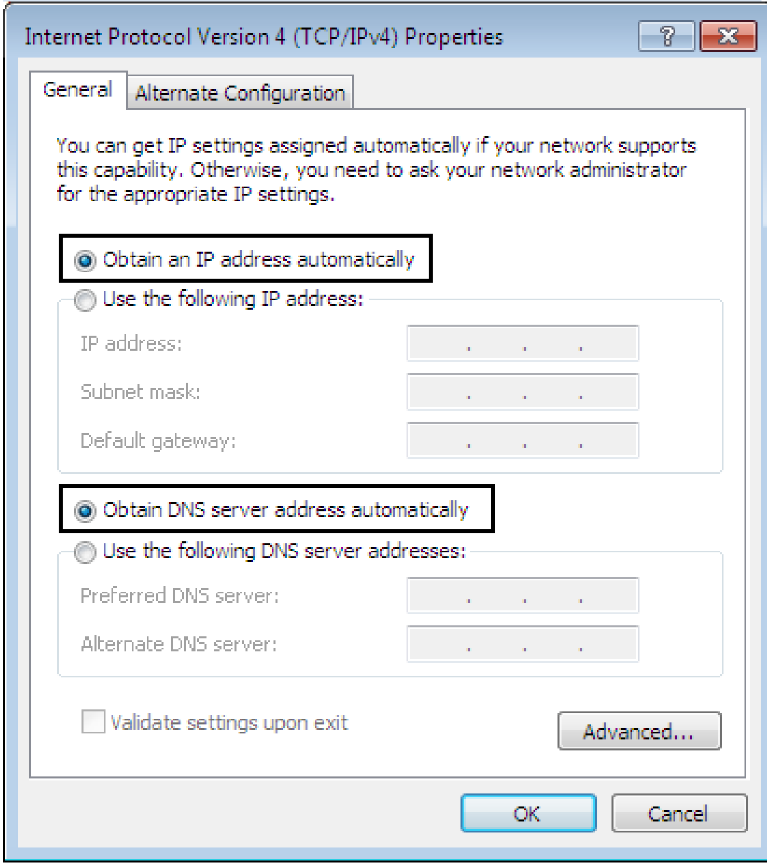
Description

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

OK | Cancel

5. 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.

6. 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: . . .

□ Validate settings upon exit

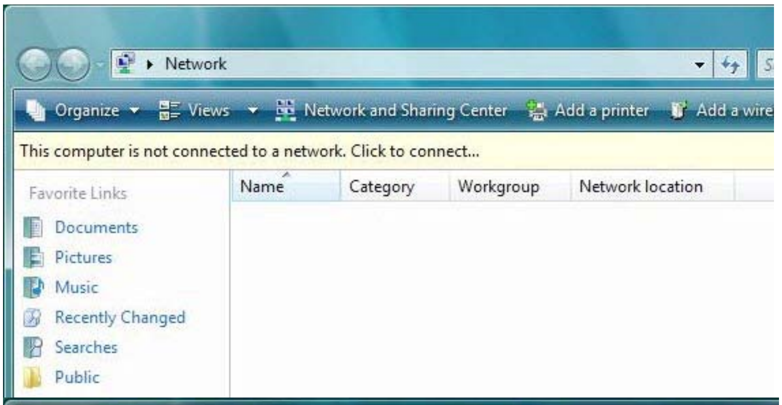
Advanced...

OK | Cancel

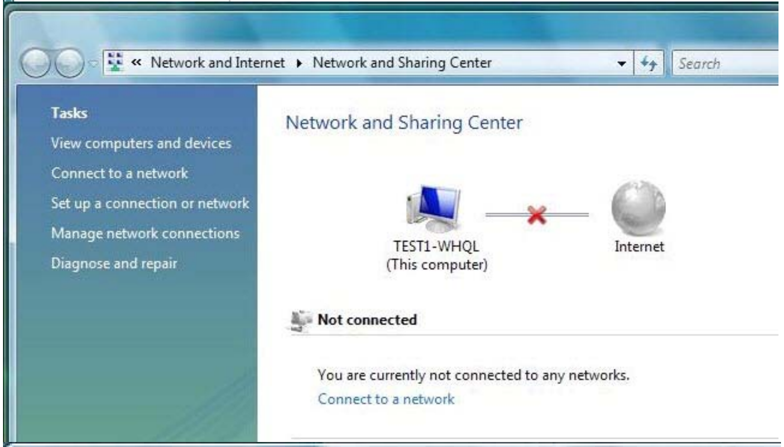
Configuring PCs in Windows Vista

1. Go to **Start**. Click on Network.

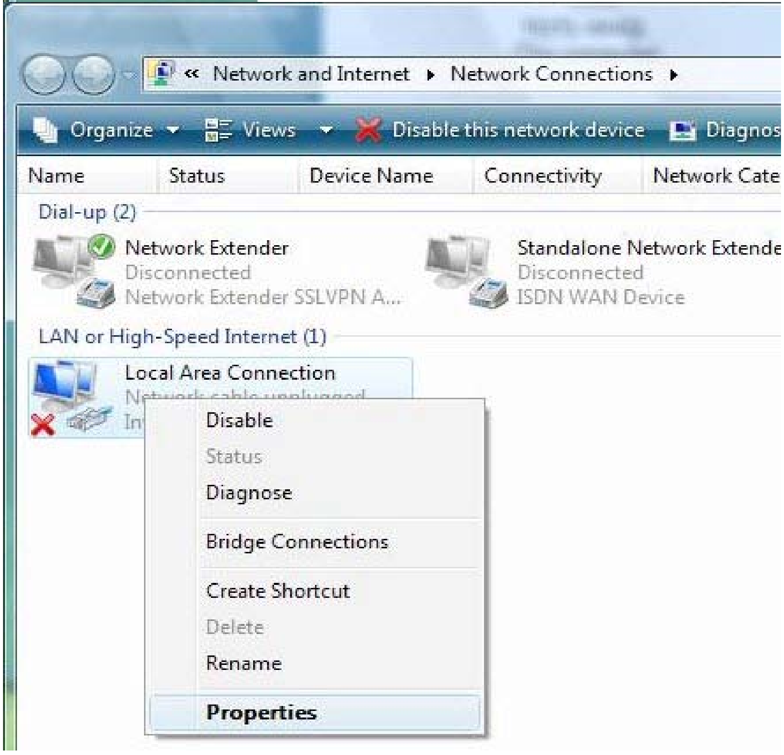
2. Then click on Network and Sharing Center at the top bar



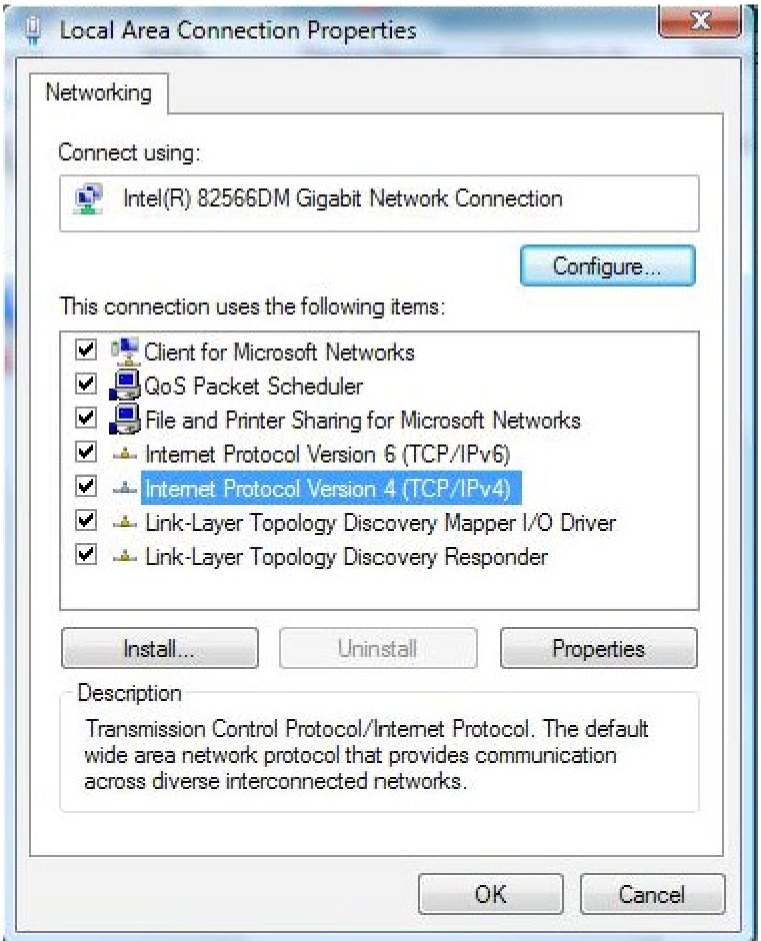
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.


« Network and Internet ▸ Network and Sharing Center
Search
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
TEST1-WHQL
(This computer)
Internet
Not connected
You are currently not connected to any networks.
Connect to a network

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

Configure...

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

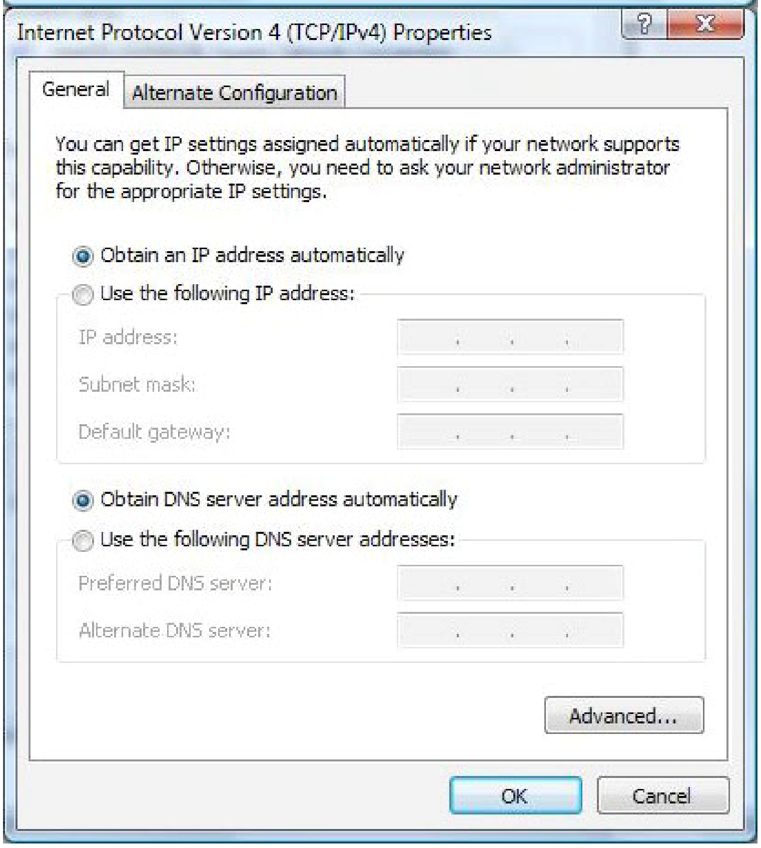
Install... Uninstall Properties

Description

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

OK Cancel

6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio but- tons. Then click OK to exit the set- ting.
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: . . .

Advanced...

OK Cancel

Configuring PCs in Windows in Window XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click **Network Connections**.
2. Double-click **Local Area Connection**. **(See Figure 3.1)**

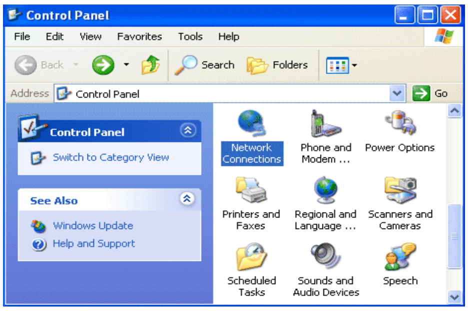
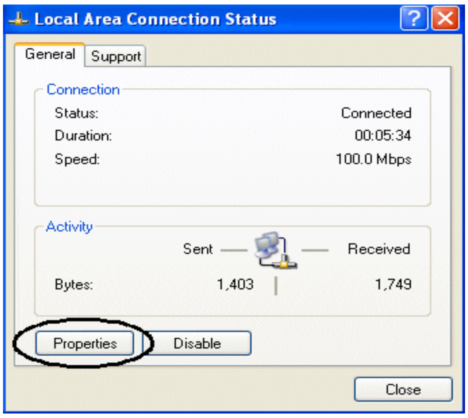


Figure 3.1: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. (**See Figure 3.2)**



Status: Connected

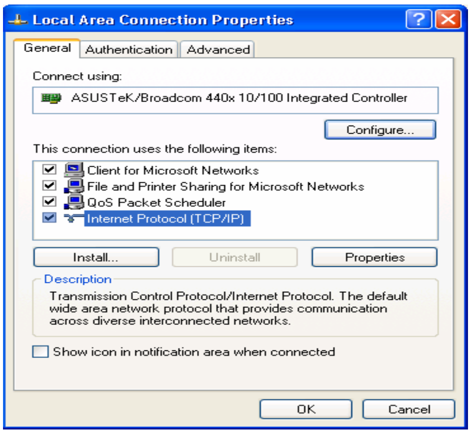
Duration: 00:05:34

Speed: 100.0 Mbps

	Sent	Received
Bytes:	1,403	1,749

Figure 3.2: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. (**See Figure 3.3)**



Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

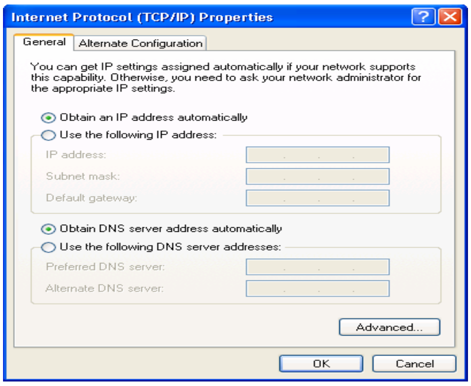
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

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

Figure 3.3: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (**See Figure 3.4**)
6. Click **OK** to finish the configuration.



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

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

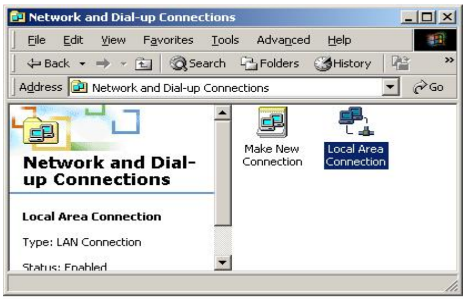
Preferred DNS server:

Alternate DNS server:

Figure 3.4: IP Address & DNS Configuration

Configuring PCs in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network and Dial-up Connections**.
2. Double-click **Local Area ("LAN") Connection**. **(See Figure 3.5)**



Network and Dial-up Connections

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

Network and Dial-up Connections

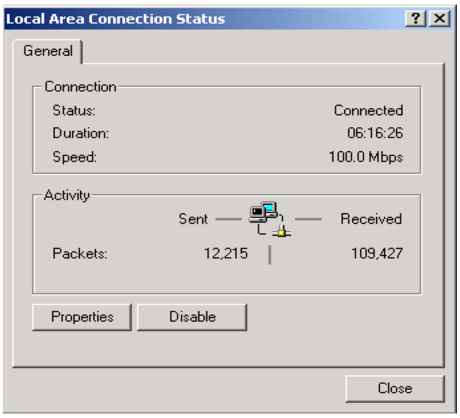
Local Area Connection

Type: LAN Connection

Status: Enabled

Figure 3.5: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. **(See Figure 3.6)**



Local Area Connection Status

General

Connection

Status: Connected

Duration: 06:16:26

Speed: 100.0 Mbps

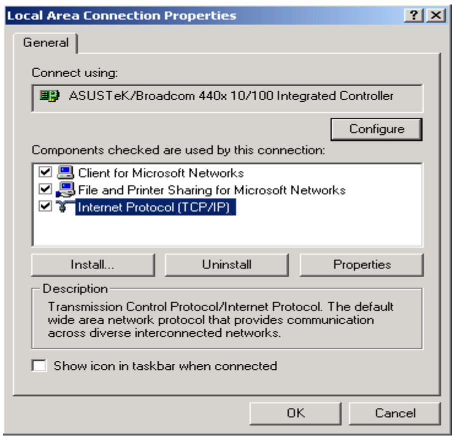
Activity

Sent — — Received

Packets: 12,215 | 109,427

Figure 3.6: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. **(See Figure 3.7)**



Local Area Connection Properties

General

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)

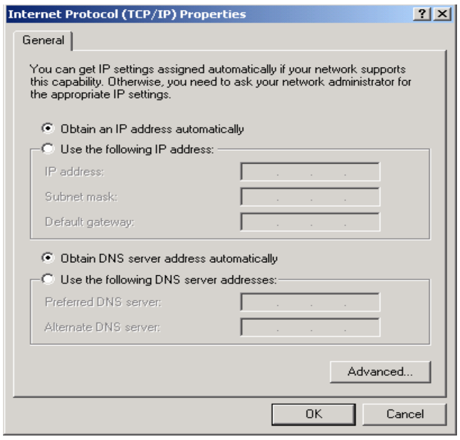
Description

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

□ Show icon in taskbar when connected

Figure 3.7: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. **(See Figure 3.8)**
6. Click **OK** to finish the configuration.



Internet Protocol (TCP/IP) Properties

General

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:

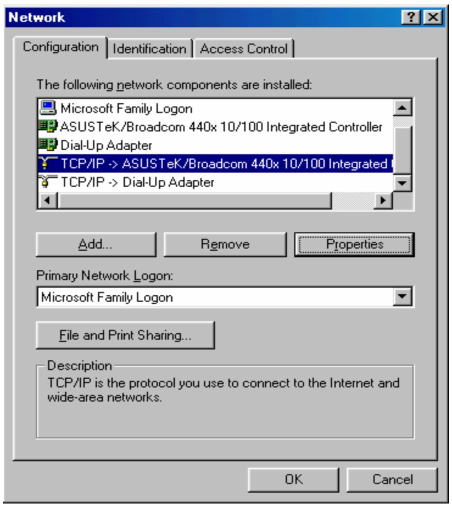
Preferred DNS server:

Alternate DNS server:

Figure 3.8: IP Address & DNS Configuration

Configuring PC in Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC. (**See Figure 3.9)**
3. Click **Properties**.



The following network components are installed:

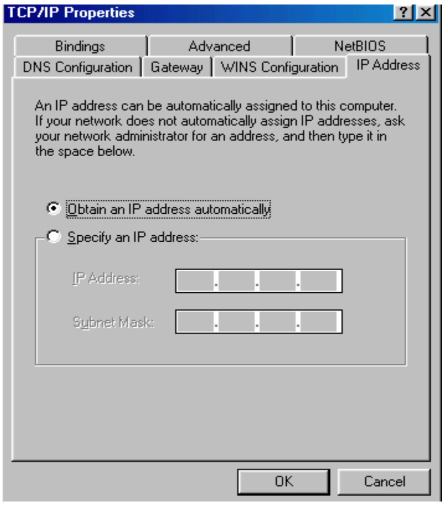
- Microsoft Family Logon
- ASUSTeK/Broadcom 440x 10/100 Integrated Controller
- Dial-Up Adapter
- TCP/IP -> ASUSTeK/Broadcom 440x 10/100 Integrated
- TCP/IP -> Dial-Up Adapter

Primary Network Logon: Microsoft Family Logon

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

Figure 3.9: TCP / IP

4. Select the **IP Address** tab. In this page, click the Obtain an IP address automatically radio button. (**See Figure 3.10)**



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

● Obtain an IP address automatically

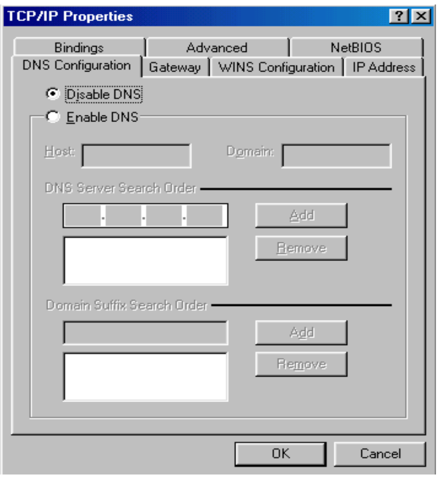
○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Figure 3.10: IP Address

5. Then select the **DNS Configuration** tab. **(See Figure 3.11)**
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



● Disable DNS

○ Enable DNS

Host: Domain:

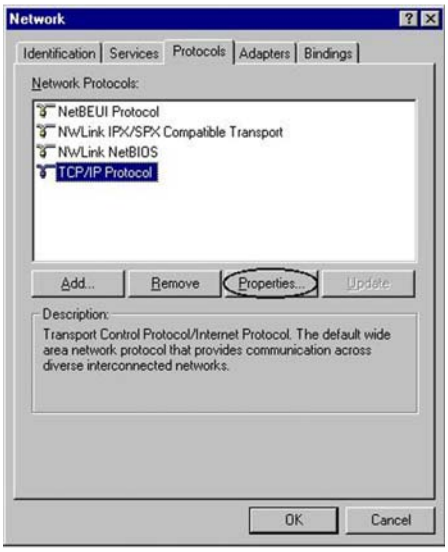
DNS Server Search Order

Domain Suffix Search Order

Figure 3.11: DNS Configuration

Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**. (**See Figure 3.12)**



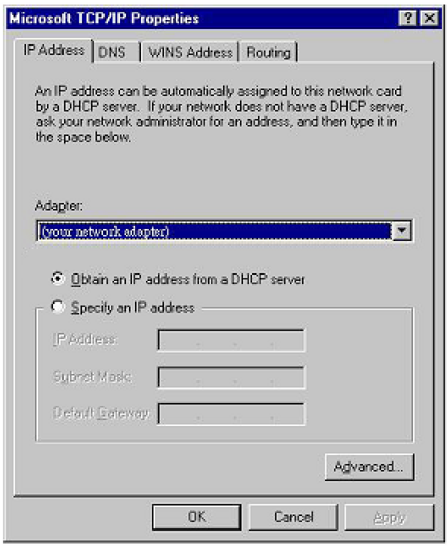
Network Protocols:

- NetBEUI Protocol
- NWLink IPX/SPX Compatible Transport
- NWLink NetBIOS
- TCP/IP Protocol

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

Figure 3.12: TCP / IP

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**. (**See Figure 3.13)**



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.

Adapter: (your network adapter)

● Obtain an IP address from a DHCP server
○ Specify an IP address

IP Address: . . .
Subnet Mask: . . .
Default Gateway: . . .

Figure 3.13: IP Address

Factory Default Settings

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

Web Interface (Username and Password)

- Username: admin
- Password: admin

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

Attention

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

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

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 below.

LAN Port		**WAN Port**
IP address	192.168.1.254	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

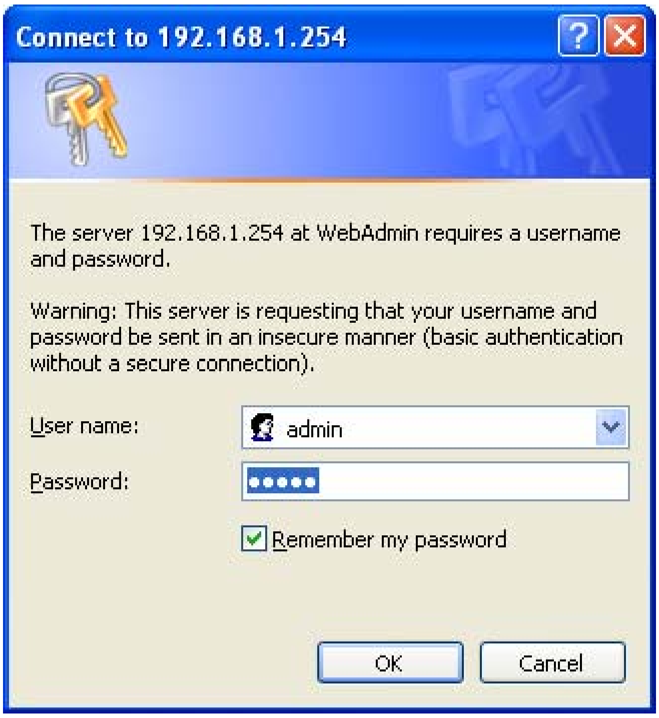
Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP (Obtain an IP Address Automatically, Static IP (Fixed IP Address) and PPPoE.

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(RFC2364)	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.

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

The server 192.168.1.254 at WebAdmin requires a username and password.

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

User name: admin

Password: •••••

☑ Remember my password

Figure 3.14: User name & Password Prompt Window

Congratulations! You are now successfully logon to the Router!

Chapter 4: Configuration

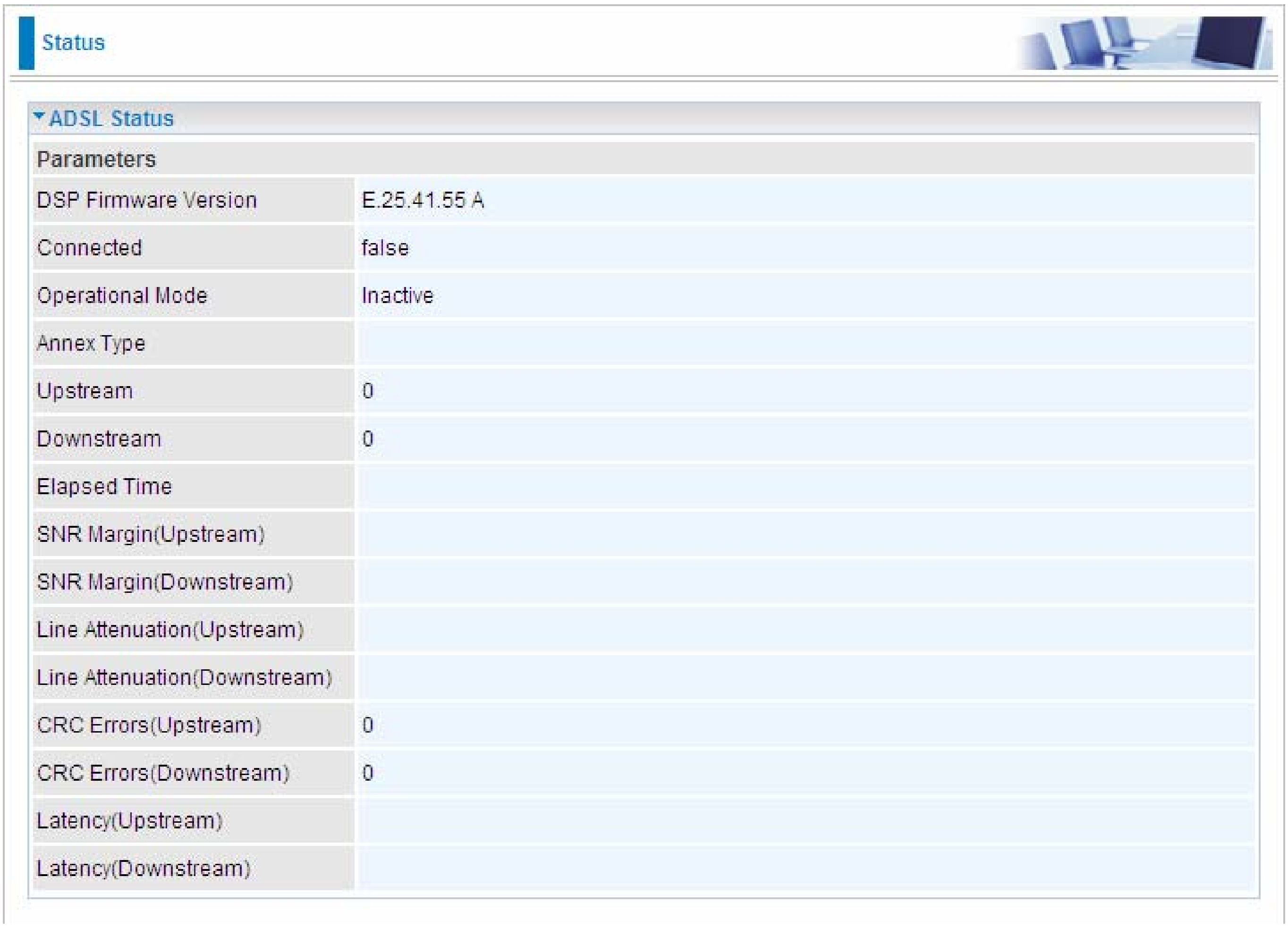
At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status**
  - ADSL Status
  - 3G Status
  - EWAN Status
  - IBurst Status
  - ARP Table
  - DHCP Table
  - Routing Table
  - NAT Sessions
  - UPnP Portmap
  - PPTP Status
  - IPSec Status
  - L2TP Status
  - Event Log
  - Error Log
  - IDS Log
  - Diagnostic
- **Quick Start**
- **Configuration**
  - LAN
  - WAN
  - System
  - Firewall
  - VPN
  - 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 ADSL overall status, which shows a number of helpful information such as DSP firmware version.

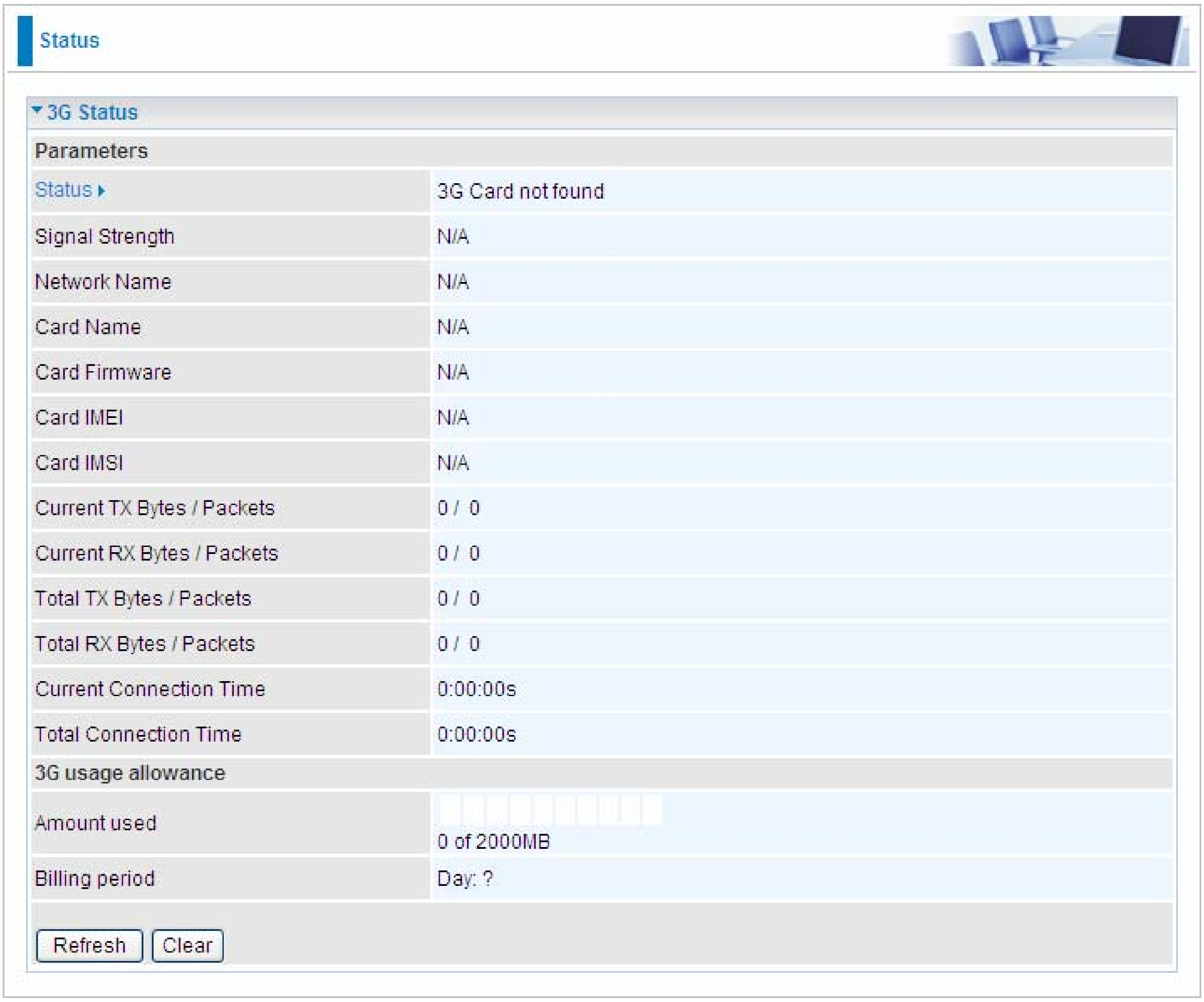


▾ADSL Status

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)	

3G Status

This section displays the 3G Card's overall status, which shows you a number of helpful information such as the current signal strength and statistics on current and total bytes transferred and received **(Note: 3G card/modem does not come with the router)**.



3G Status

Parameters	
Status	3G Card not found
Signal Strength	N/A
Network Name	N/A
Card Name	N/A
Card Firmware	N/A
Card IMEI	N/A
Card IMSI	N/A
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0
Current Connection Time	0:00:00s
Total Connection Time	0:00:00s
3G usage allowance	
Amount used	0 of 2000MB
Billing period	Day: ?

Status: The current status of the 3G card.

Signal Strength: The signal strength bar indicates current 3G signal strength.

Network Name: The network name that the device is connected to.

Card Name: The name of the 3G card.

Card Firmware: The current firmware for the 3G card.

Card IMEI: the IMEI (International Mobile Equipment Identity) of the 3G card.

Card IMSI: International Mobile Subscriber Identification Number.

Current TX Bytes / Packets: The statistics of transmission, count for this call.

Current RX Bytes / Packets: The statistics of receive, count for this call.

Total TX Bytes / Packets: The statistics of transmission, count from system ready.

Total RX Bytes / Packets: The statistics of receive, count from system ready.

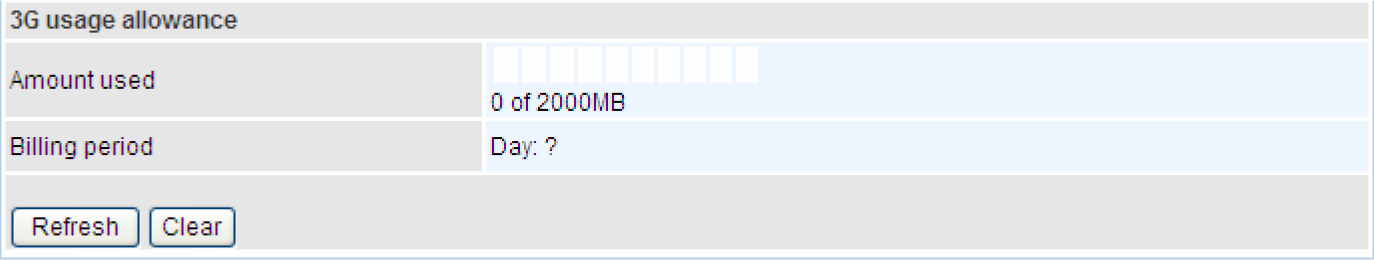
Current Connection Time: The duration for the current connection.

Total Connection Time: The cumulative connection time.

Amount used: Show the traffic or hours has been used.

Billing period: The day from which the fee is charged.

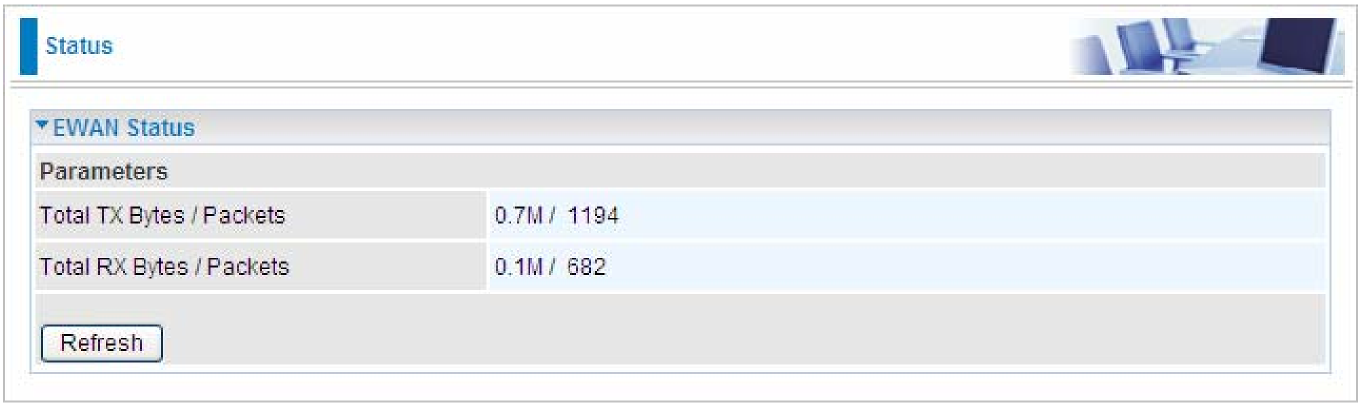
Note: Only after you have checked to enable Usage Allowance ▸ , the following information will be shown.



3G usage allowance	
Amount used	0 of 2000MB
Billing period	Day: ?

EWAN Status

Besides using 3G/ADSL to get connected to the Internet, the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online.



▾EWAN Status

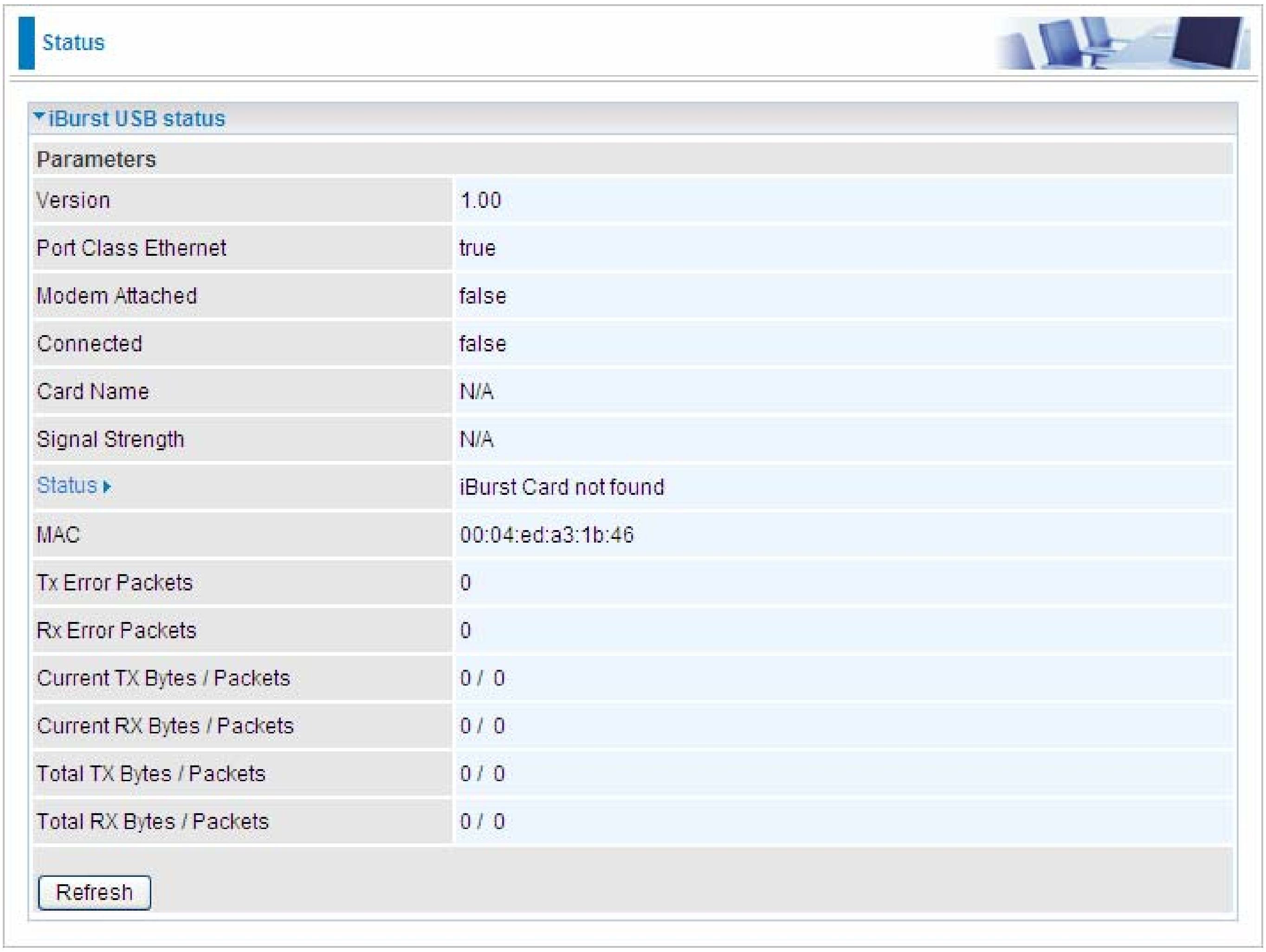
Parameters	
Total TX Bytes / Packets	0.7M / 1194
Total RX Bytes / Packets	0.1M / 682

Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

iBurst Status

Displays additional information of the 3G status when iBurst function is enabled in the 3G configuration such as its signal strength, card name, connection status and port class Ethernet.



Parameters	
Version	1.00
Port Class Ethernet	true
Modem Attached	false
Connected	false
Card Name	N/A
Signal Strength	N/A
Status ▸	iBurst Card not found
MAC	00:04:ed:a3:1b:46
Tx Error Packets	0
Rx Error Packets	0
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0

Card Name: The name of the card.

Signal Strength: The signal strength bar indicates the current signal strength.

Current TX Bytes / Packets: The statistics of data transmission in bytes / packets during a call.

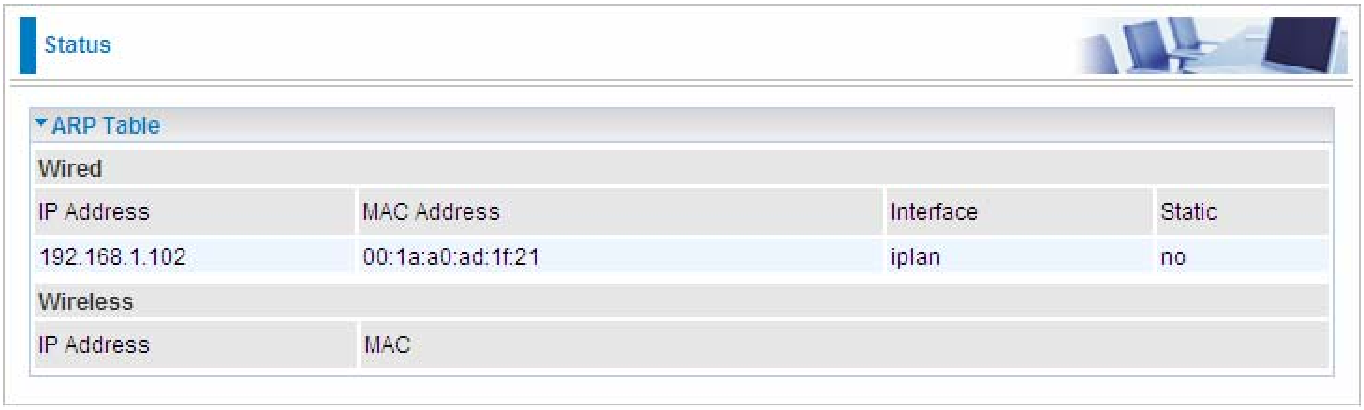
Current RX Bytes / Packets: The statistics of data received in bytes / packets during a call.

Total TX Bytes / Packets: The statistics of total data transmission in bytes / packets since system ready.

Total RX Bytes / Packets: The statistics of total data received in bytes / packets since system ready.

ARP Table

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



Status

▾ARP Table

Wired

IP Address	MAC Address	Interface	Static
192.168.1.102	00:1a:a0:ad:1f:21	iplan	no

Wireless

IP Address	MAC

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

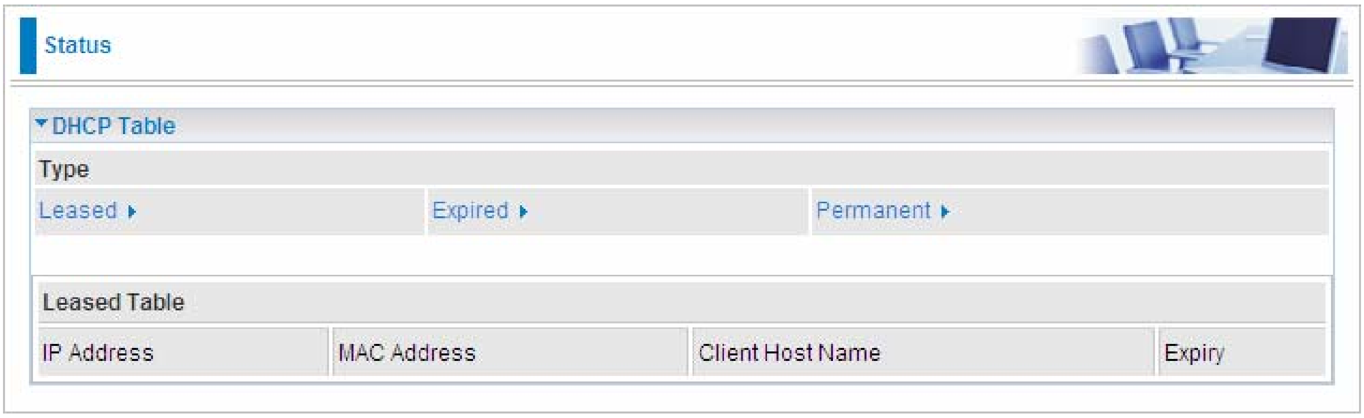
MAC Address: The MAC (Media Access Control) addresses for each device on your LAN.

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

Static: Static status of the ARP table entry:

- “**no**” for dynamically-generated ARP table entries.
- “**yes**” for static ARP table entries added by the user.

DHCP Table



Status

▾DHCP Table

Type

Leased ▸ Expired ▸ Permanent ▸

Leased Table

IP Address	MAC Address	Client Host Name	Expiry

Leased: The DHCP assigned IP addresses information.

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

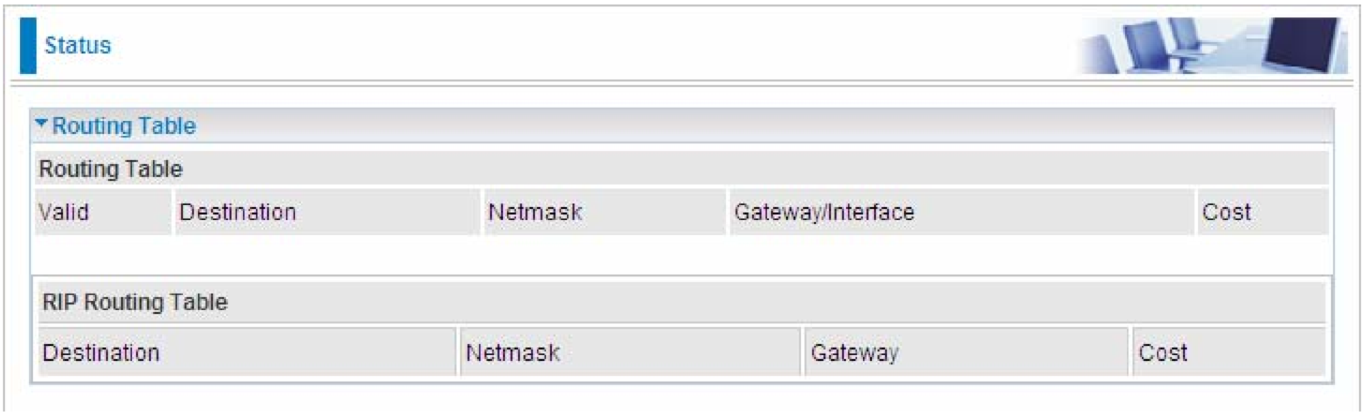
IP Address: The IP address that assigned to client.

MAC Address: The MAC address of client.

Client Host Name: The Host Name (Computer Name) of client.

Expiry: The current lease time of client.

Routing Table



Status

▾ Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost

RIP Routing Table

Destination	Netmask	Gateway	Cost

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination Netmask address.

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

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

RIP Routing Table

Destination: The IP address of the destination network.

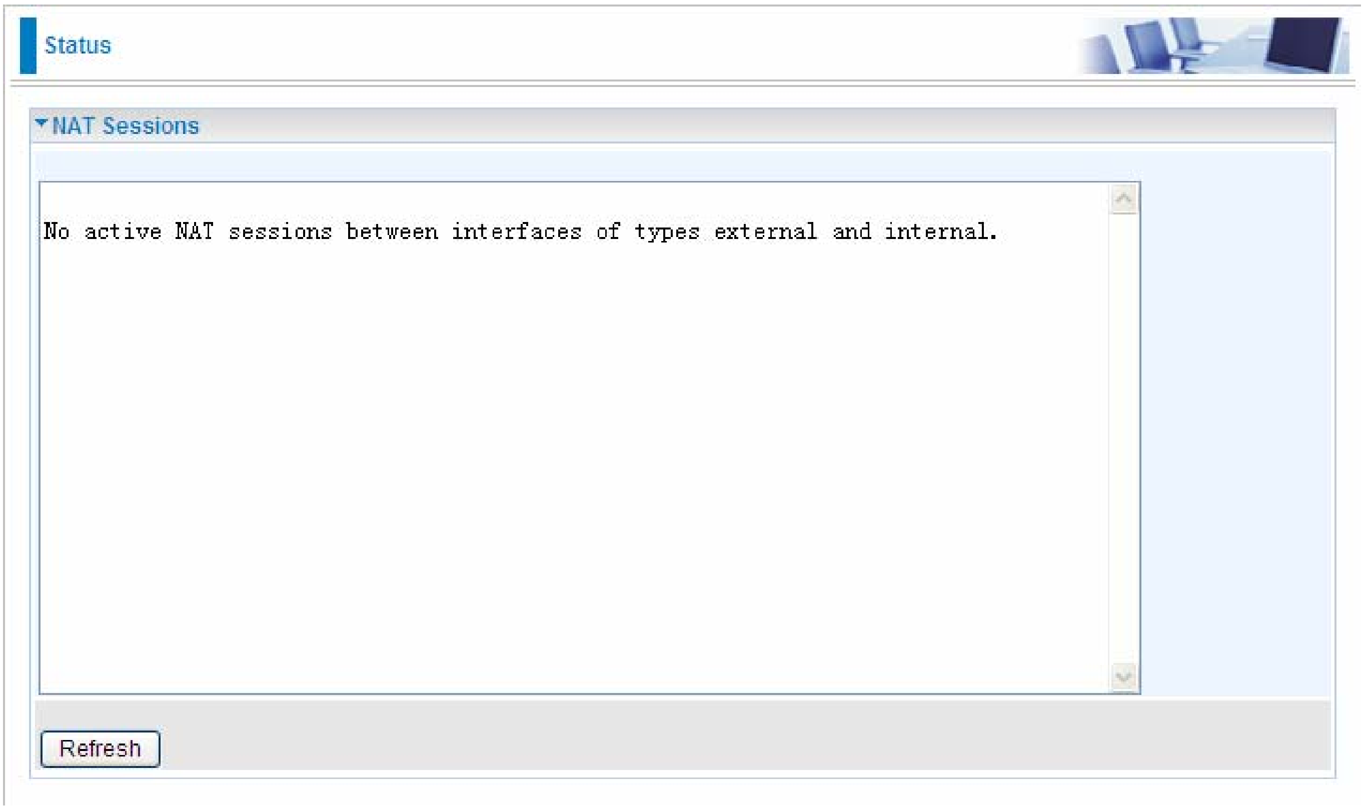
Netmask: The destination Netmask address.

Gateway: 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

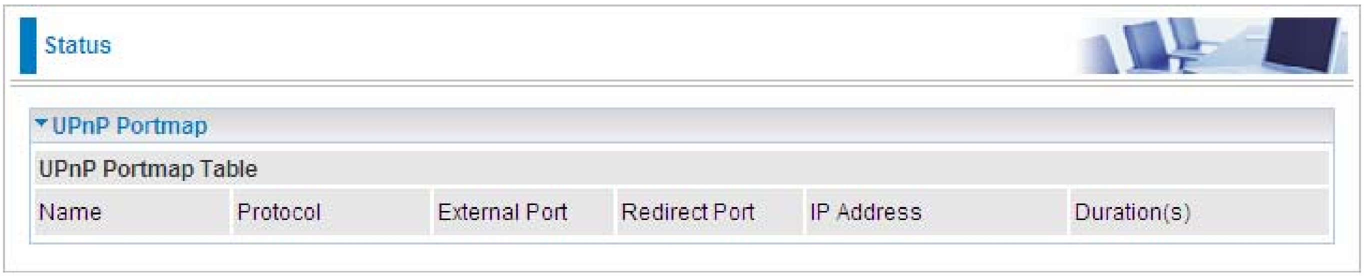
This section lists all current NAT sessions between interface of types external (WAN) and internal (LAN).



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

UPnP Portmap

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

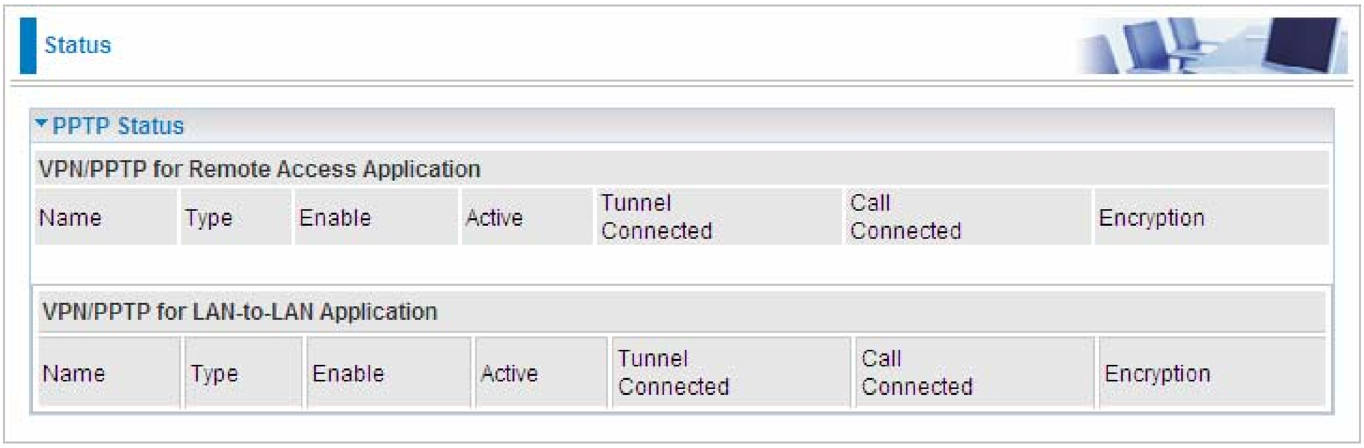


UPnP Portmap Table

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

PPTP Status

This shows details of your configured PPTP VPN Connections.



Status

▾ PPTP Status

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/PPTP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular PPTP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

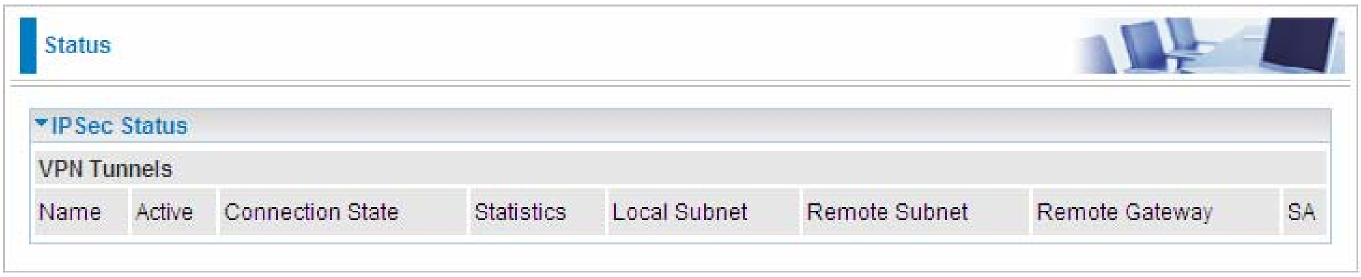
Tunnel Connected: Whether the VPN Tunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

IPSec Status

This shows details of your configured IPSec VPN Connections.



Status

▾ IPSec Status

VPN Tunnels

Name	Active	Connection State	Statistics	Local Subnet	Remote Subnet	Remote Gateway	SA

Name: The name you assigned to the particular VPN entry.

Active: Whether the VPN Connection is currently Active.

Connection State: Whether the VPN is Connected or Disconnected.

Statistics: Statistics for this VPN Connection.

Local Subnet: The local IP Address or Subnet used.

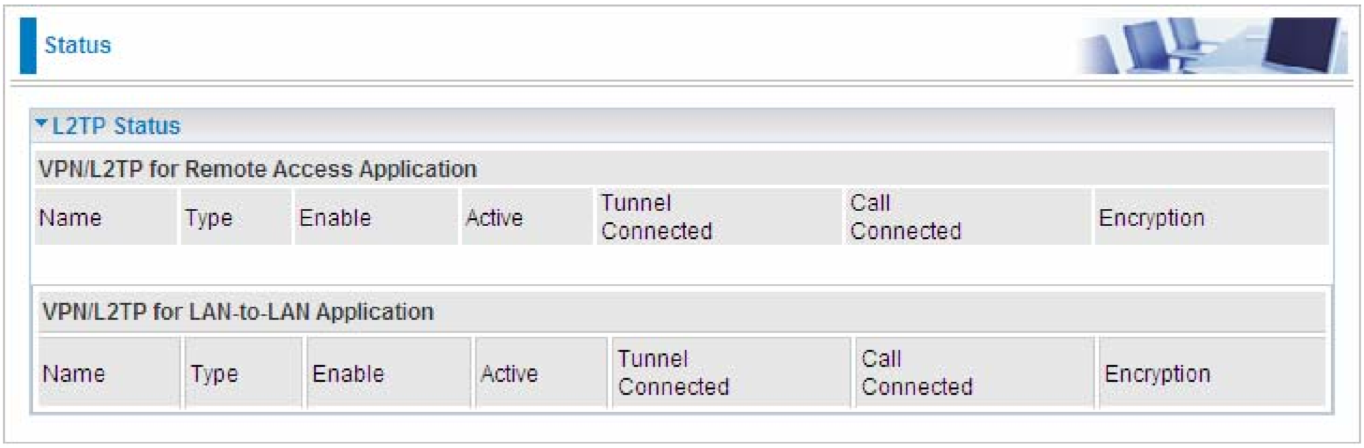
Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

L2TP Status

This shows details of your configured L2TP VPN Connections.



Status

▾L2TP Status

VPN/L2TP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/L2TP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: The name you assigned to the particular L2TP connection in your VPN configuration.

Type: The type of connection (dial-in/dial-out).

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

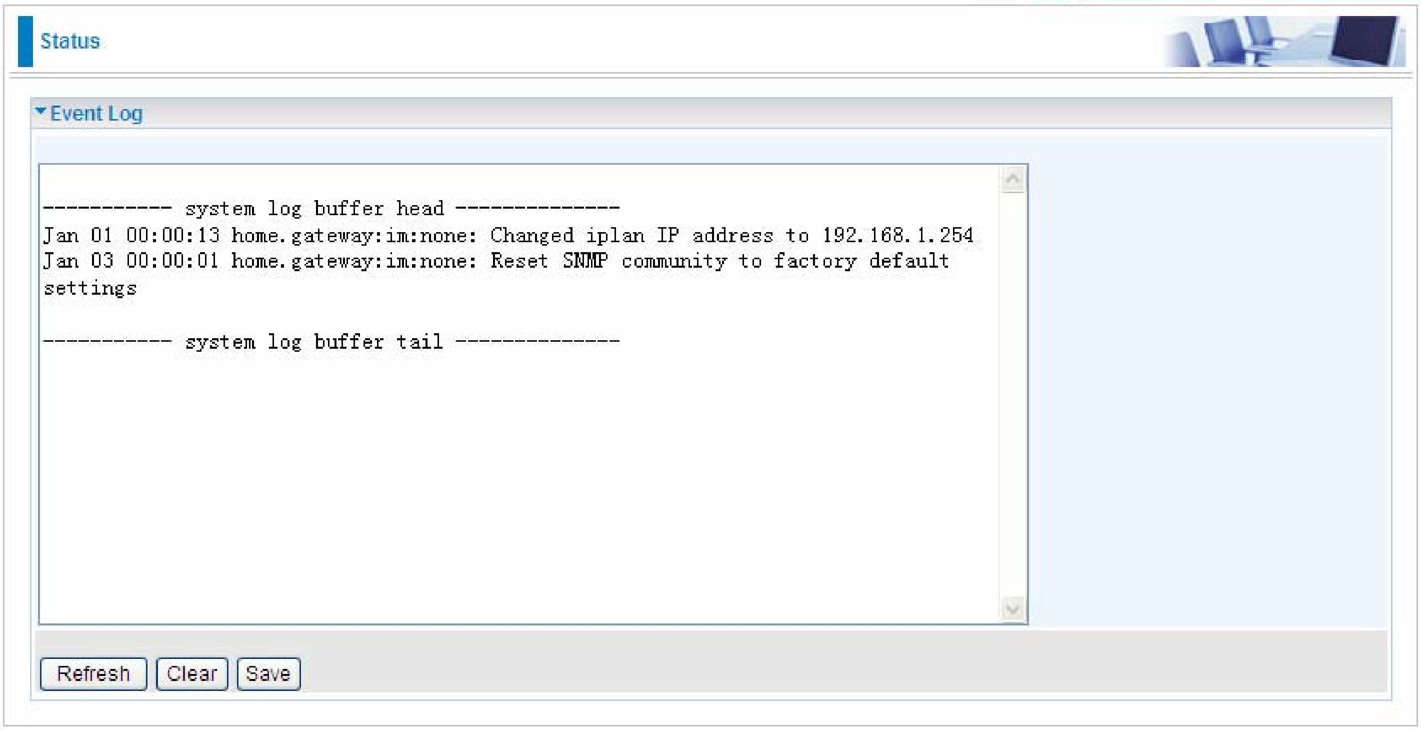
Tunnel Connected: Whether the VPN Tunnel is currently connected.

Call Connected: If the Call for this VPN entry is currently connected.

Encryption: The encryption type used for this VPN connection.

Event Log

This page displays the router's Event Log entries. Major events are logged to this window, such as when the router's ADSL connection is disconnected, as well as Firewall events when you have enabled Intrusion or Blocking Logging in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.



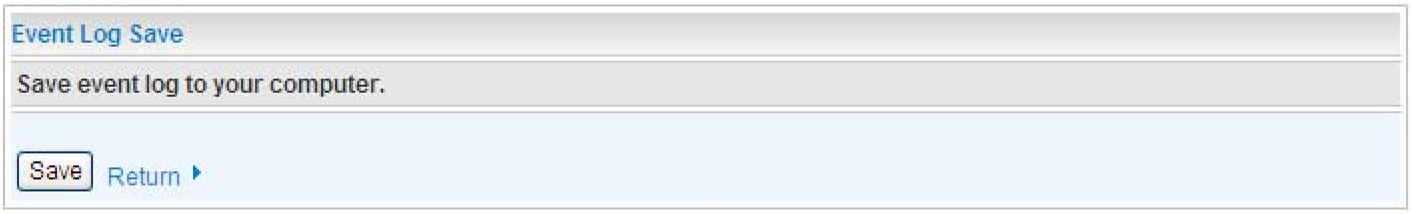
```
----------- system log buffer head --------------
Jan 01 00:00:13 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 03 00:00:01 home.gateway:im:none: Reset SNMP community to factory default
settings

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

Click **Refresh** button to get the latest event log information.

Click **Clear** button to clear the log information.

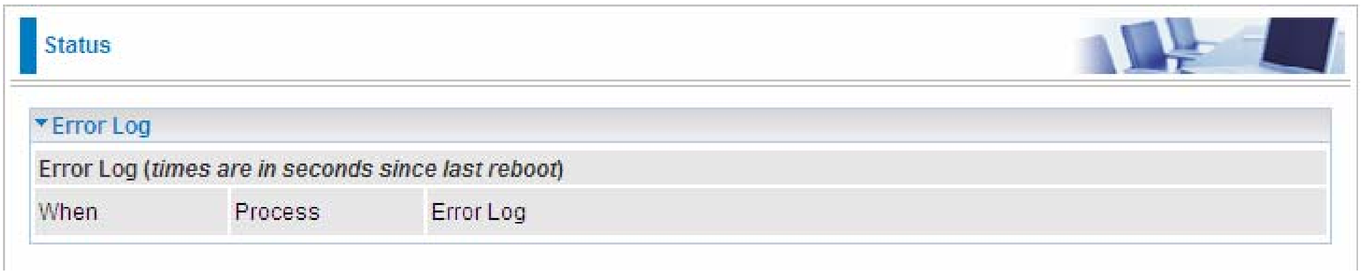
Click **Save** button to backup the event log information to your computer. Click Save button, you will enter page as follows to save the backup to your computer.



Save event log to your computer.

Error Log

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



Status

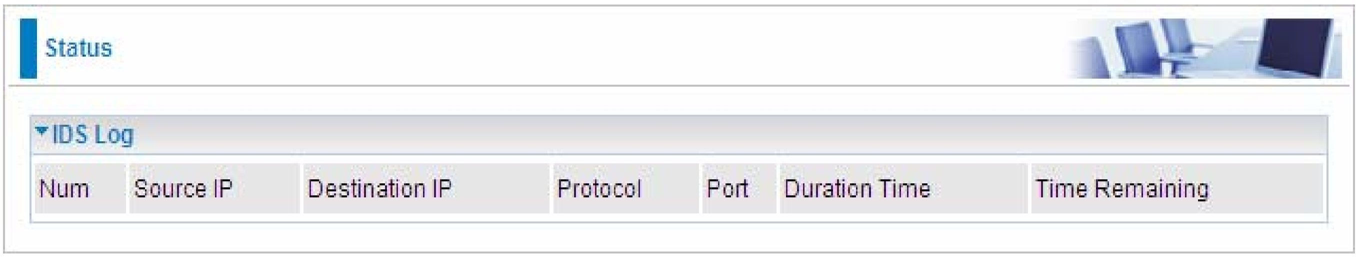
▾Error Log

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

When	Process	Error Log

IDS Log

Any records about hacker attacks and intrusion attempts from the Internet are logged to this window.



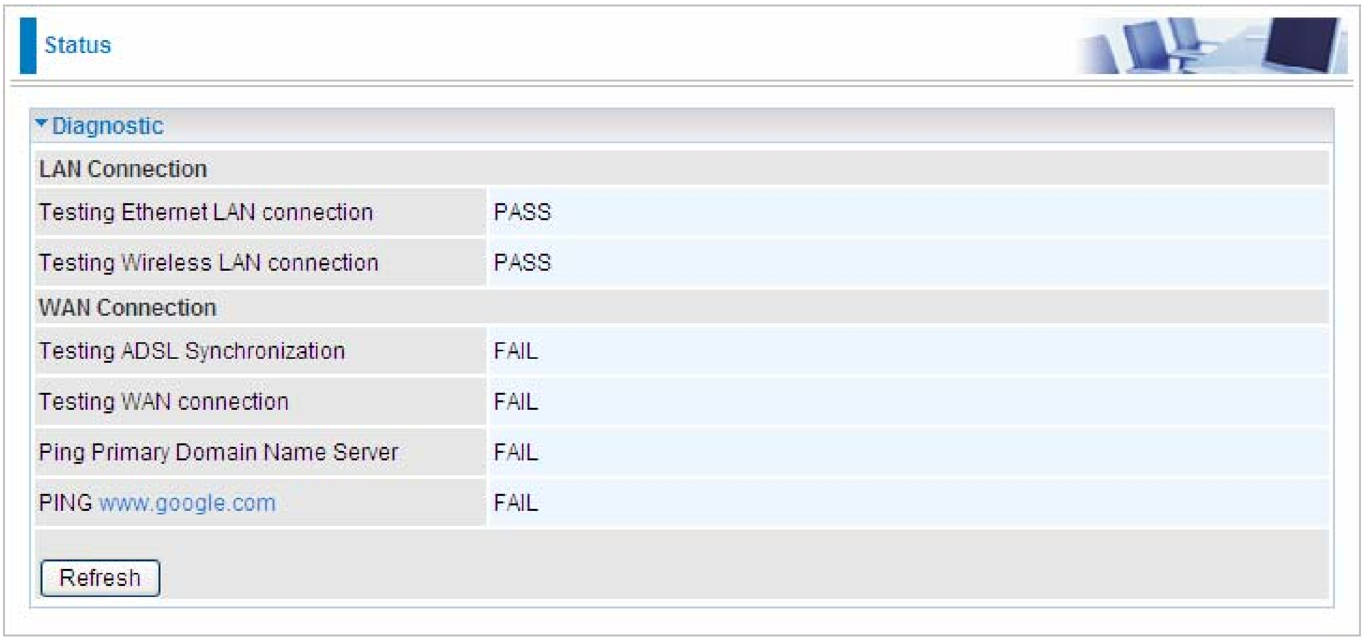
Status

▾IDS Log

Num	Source IP	Destination IP	Protocol	Port	Duration Time	Time Remaining

Diagnostic

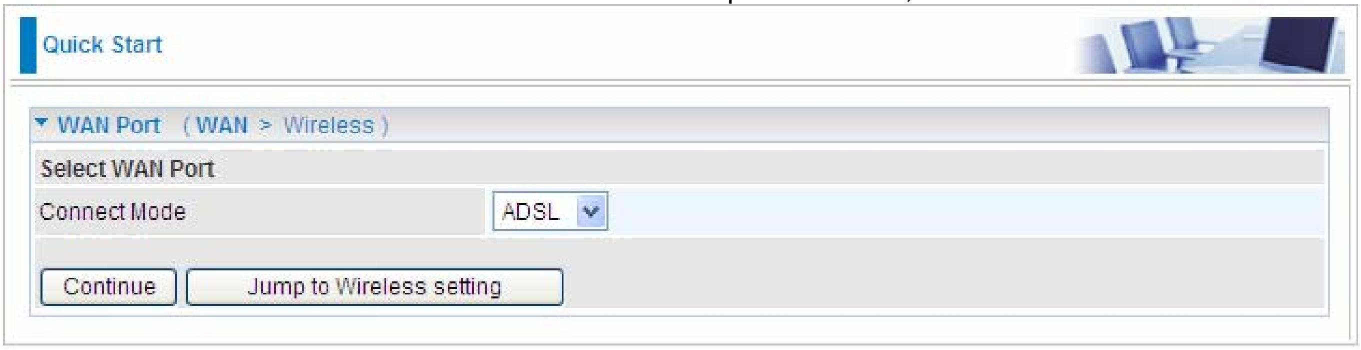
It tests the connection to computer(s) which is connected to LAN ports and also the WAN Internet connection. If **PING** www.google.com is shown FAIL and the rest is PASS, you ought to check your PC's DNS settings is set correctly.



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

Quick Start

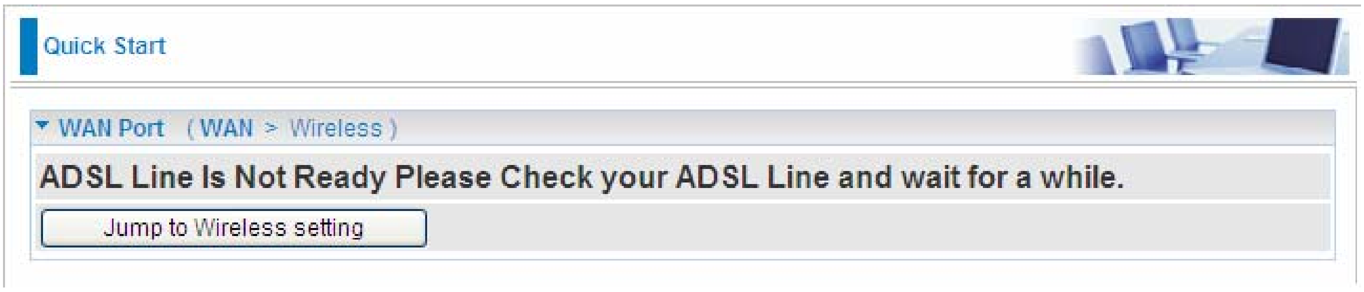
1. Click Quick Start. Select the connect mode you want. There are two options you can choose, **ADSL, EWAN** and **3G**. Select **ADSL** from Connect Mode drop-down menu, and click **Continue**.



Select WAN Port

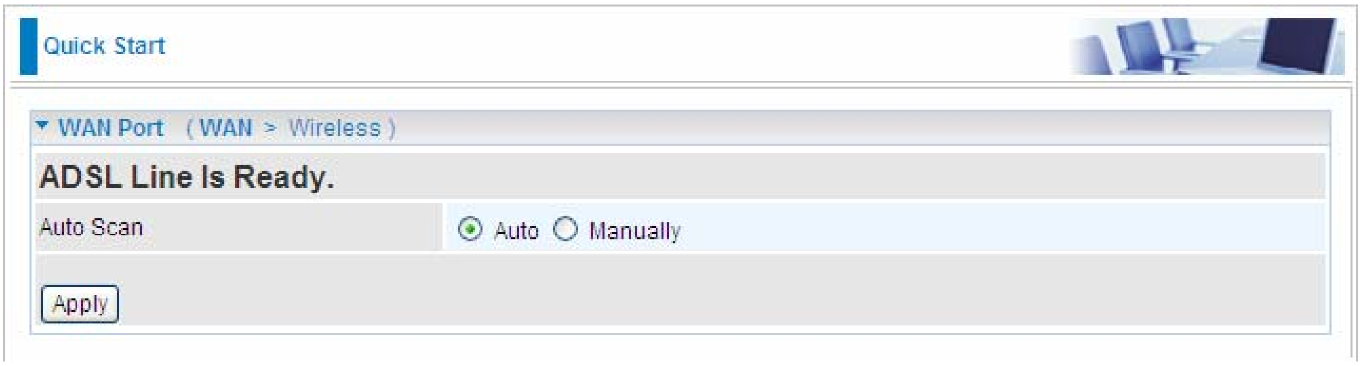
Connect Mode: ADSL

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



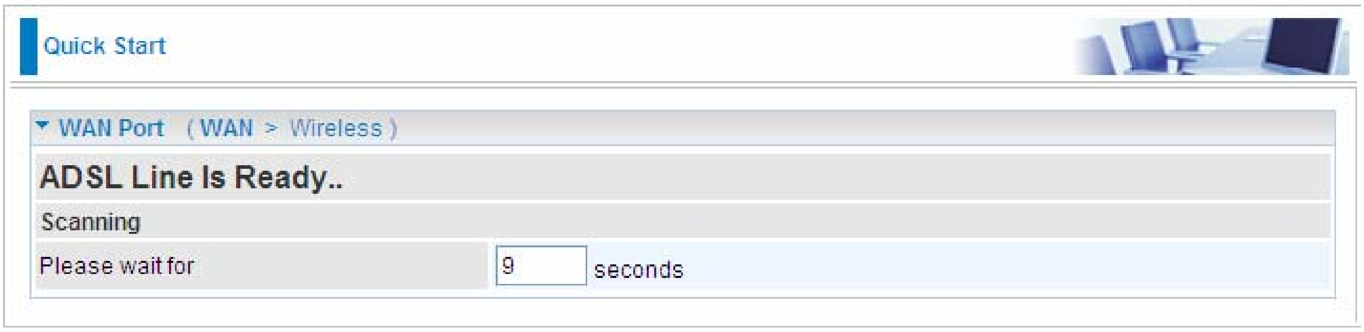
ADSL Line Is Not Ready Please Check your ADSL Line and wait for a while.

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. (If you choose **Manually**, you will directly go to step 5.)



ADSL Line Is Ready.

Auto Scan: ● Auto ○ Manually

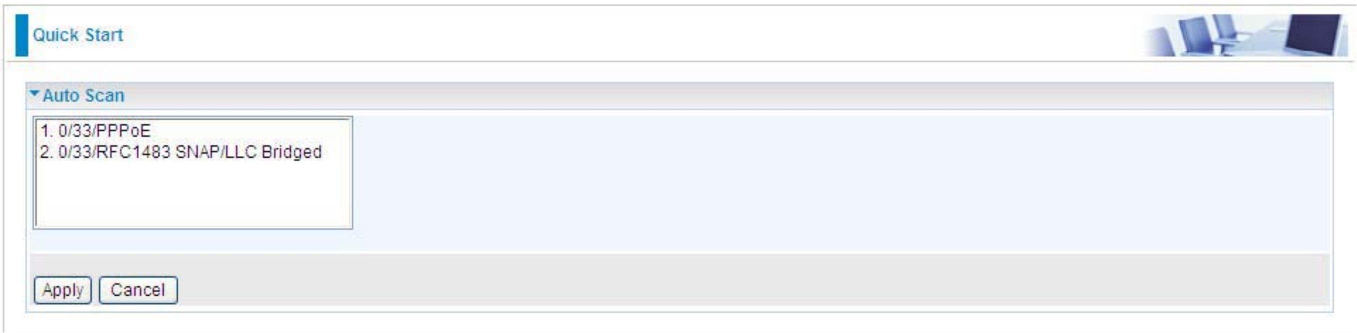


ADSL Line Is Ready..

Scanning

Please wait for 9 seconds

4. The list below has different mode applied for your choice. Choose **0/33/PPPoE (Recommended)** and click **Apply**.

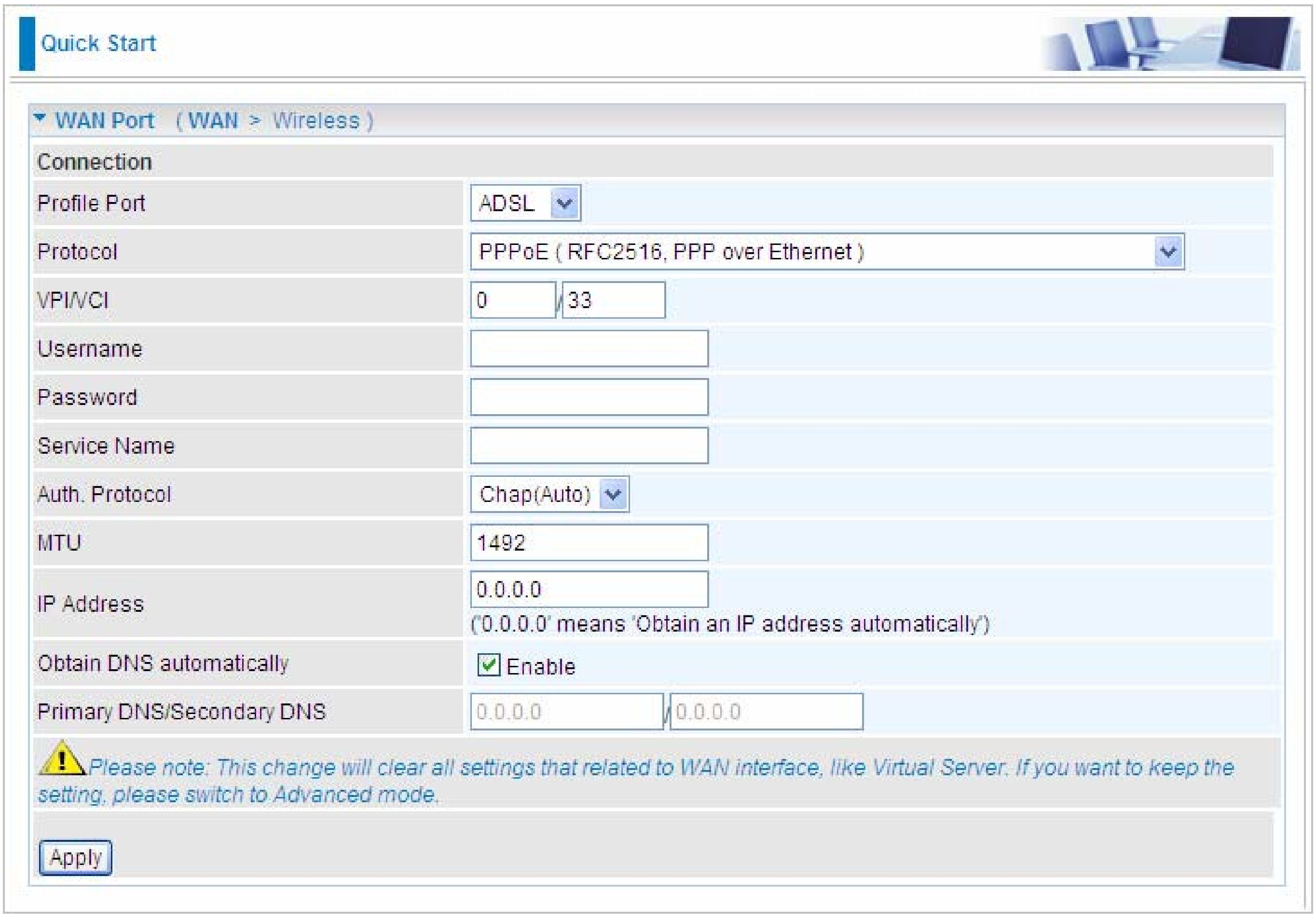


Quick Start

▾Auto Scan

1. 0/33/PPPoE
2. 0/33/RFC1483 SNAP/LLC Bridged

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



Quick Start

▾ WAN Port (WAN > Wireless)

Connection	
Profile Port	ADSL
Protocol	PPPoE (RFC2516, PPP over Ethernet)
VPI/VCI	0 / 33
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

Please note: This change will clear all settings that related to WAN interface, like Virtual Server. If you want to keep the setting, please switch to Advanced mode.

Profile Port: Select the connection mode. There are ADSL and 3G**.**

Encapsulation: Select the encapsulation mode. The default mode is PPPoE.

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

Username: Enter the username provided by your ISP.

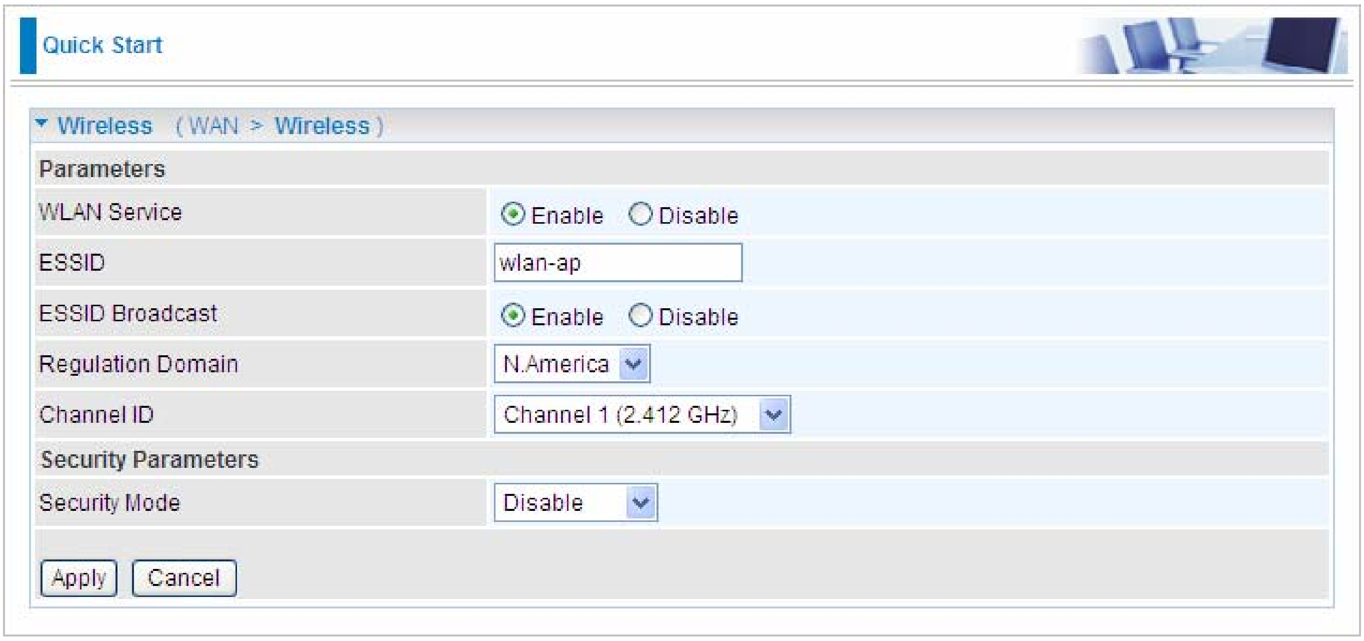
Password: Enter the password provided by your ISP.

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

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

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

6. 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 1 (2.412 GHz)
Security Parameters	
Security Mode	Disable

WLAN Service: Default setting is set to **Enable**. If you want to use wireless, 802.11n, 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.

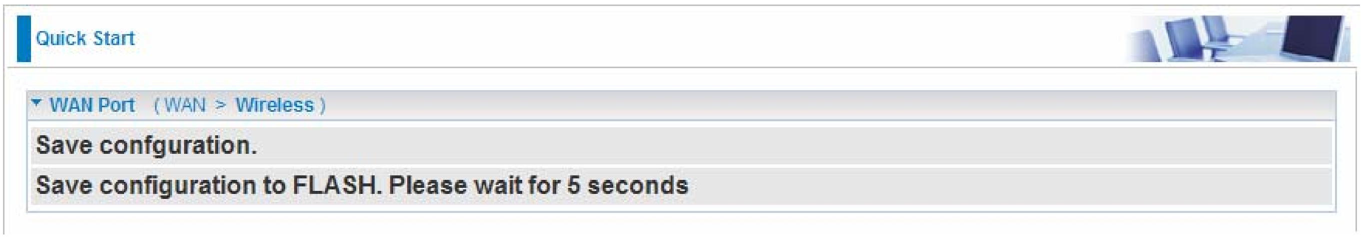
ESSID Broadcast: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Enable.**

- ⊙ **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**.

7. Wait for the configuration.



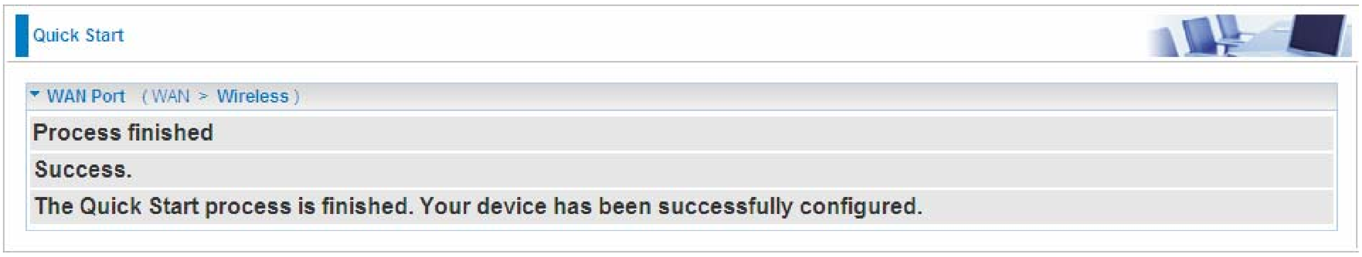
Quick Start

▼ WAN Port (WAN > Wireless)

Save confguration.

Save configuration to FLASH. Please wait for 5 seconds

8. If connection is successful the following image will be shown.



Quick Start

▼ WAN Port (WAN > Wireless)

Process finished

Success.

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

Configuration

When you click this item, you get following sub-items to configure the ADSL router.

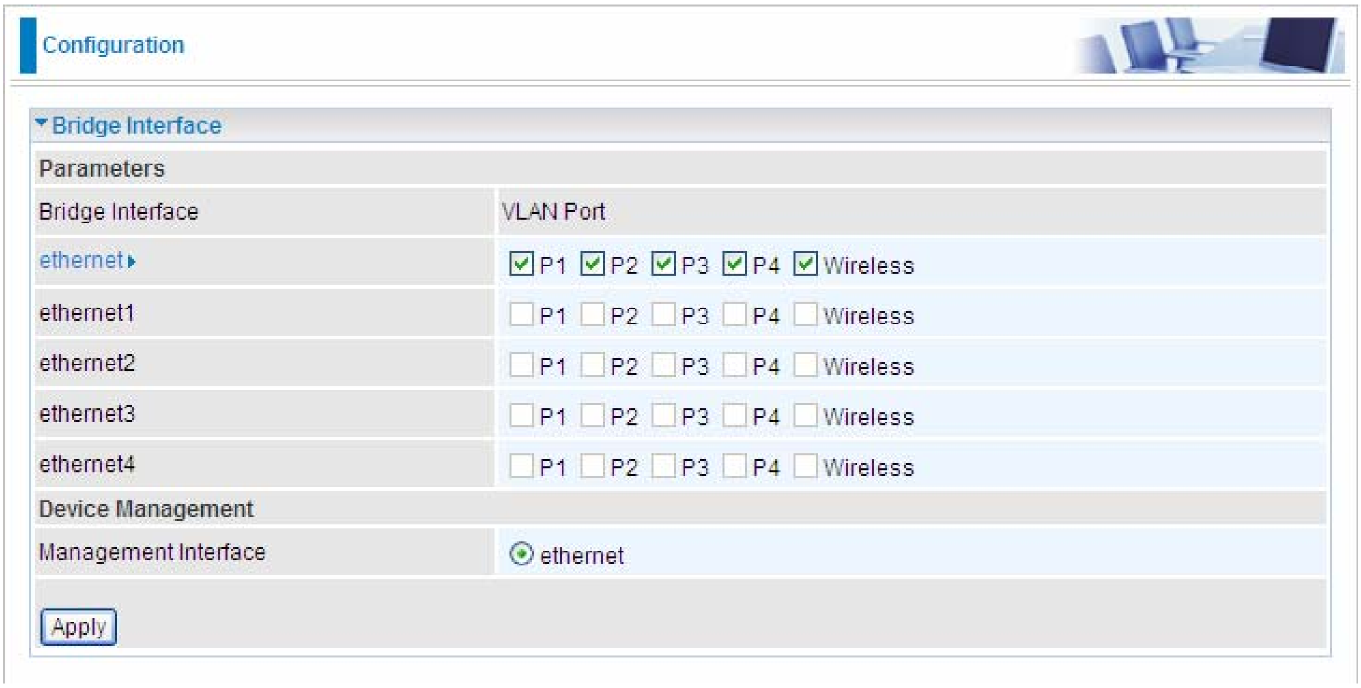
- LAN, WAN, System, Firewall, VPN, QoS, Virtual Server, Wake on LAN, Time Schedule and **Advanced**

These functions are described below in the following sections.

LAN - Local Area Network

Here are the items within the LAN section: **Bridge Interface, Ethernet, IP Alias, IPv6 Autoconfig, 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 ☑ Wireless
ethernet1	□ P1 □ P2 □ P3 □ P4 □ Wireless
ethernet2	□ P1 □ P2 □ P3 □ P4 □ Wireless
ethernet3	□ P1 □ P2 □ P3 □ P4 □ Wireless
ethernet4	□ P1 □ P2 □ P3 □ P4 □ Wireless
Device Management	
Management Interface	● ethernet

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 and P2 (Port 1, 2).

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

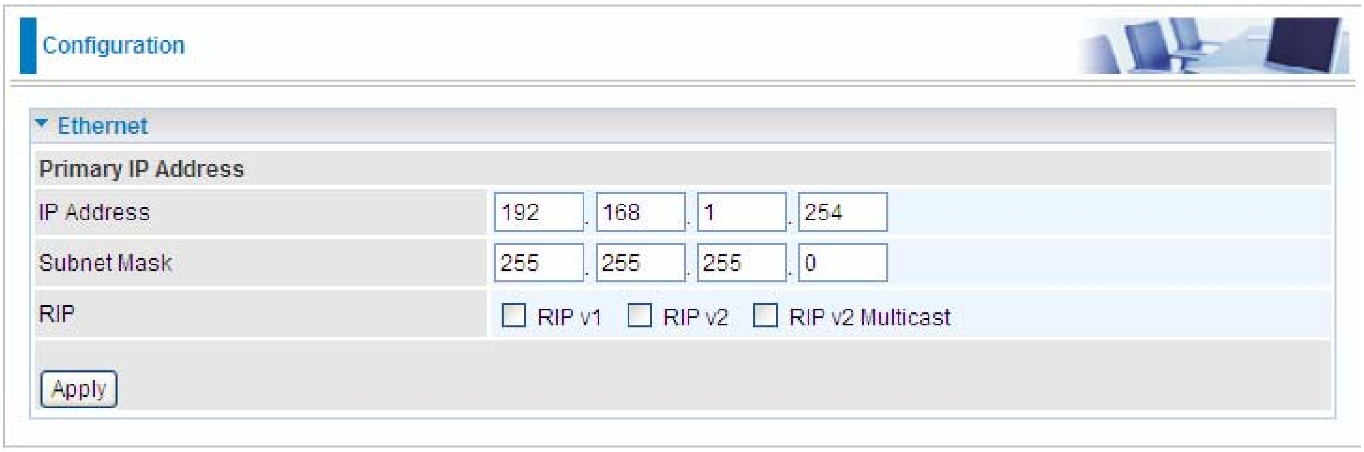
Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
ethernet	P1 / P2 / P3 / P4 / Wireless
ethernet1	P2 / P3 / P4 / Wireless
ethernet2	P3 / P4 / Wireless
ethernet3	P4 / Wireless
ethernet4	Wireless

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



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

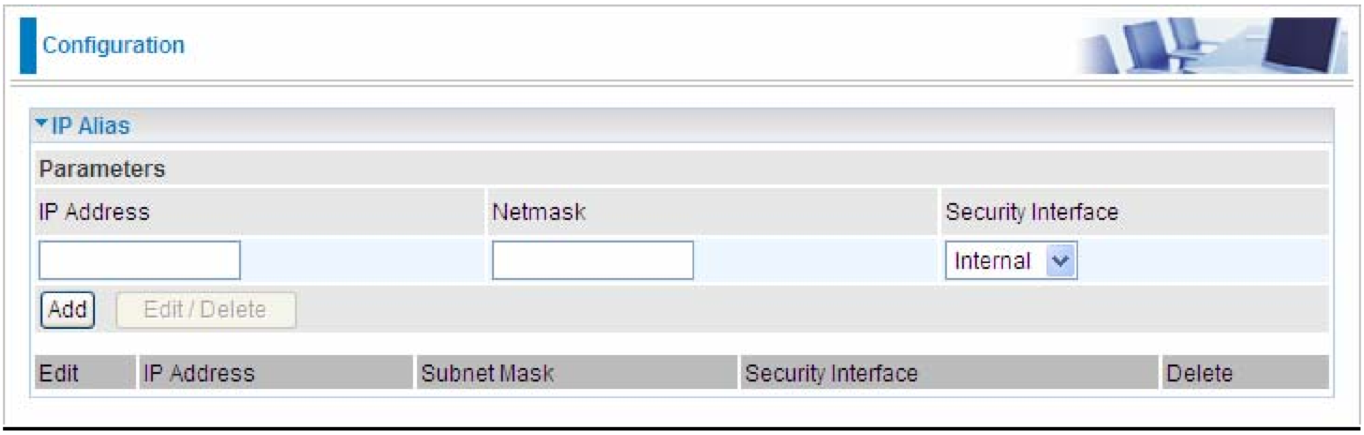
IP Address: The default IP on this router.

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



Configuration

IP Alias

Parameters

IP Address	Netmask	Security Interface
		Internal

Edit	IP Address	Subnet Mask	Security Interface	Delete

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

Netmask: Specify a subnet mask on this virtual interface.

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

Internal: The network is behind NAT. All traffic will do network address translation when sending out to Internet if NAT is enabled.

External: There is no NAT on this IP interface and connected to the Internet directly. Mostly it will be used when providing multiple public IP addresses by ISP. In this case, you can use public IP address in local network which gateway IP address point to the IP address on this interface.

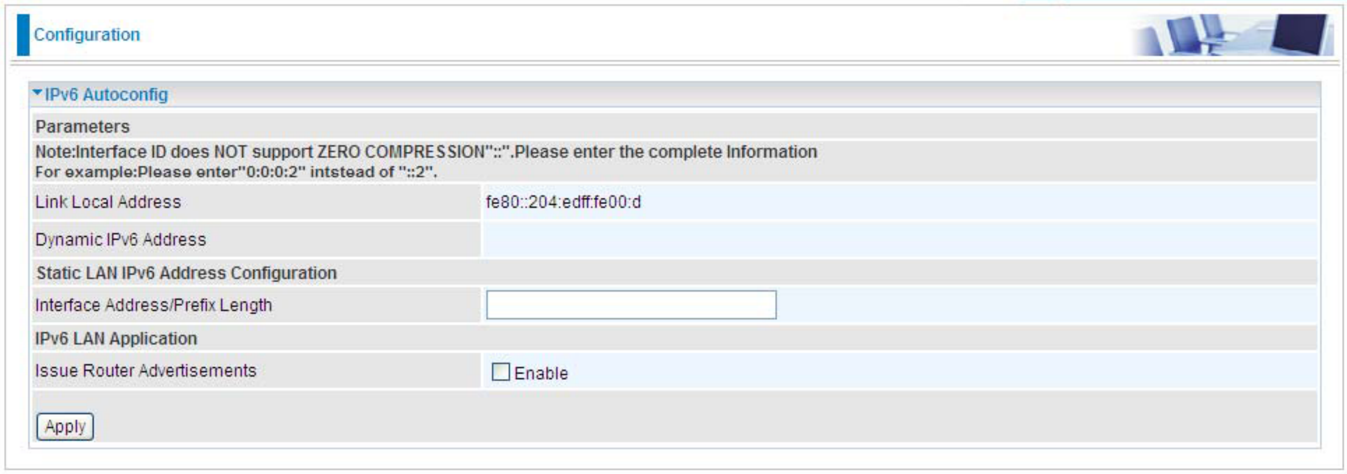
DMZ: Specify this network to DMZ area. There is no NAT on this interface.

IPv6 Autoconfig

The IPv6 address composes of two parts, thus, the prefix and the interface ID.

BiPAC 7402NX(L) dynamically configure IPv6 address on host with Stateless auto-configuration mode.

Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information(prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.



Configuration

▾IPv6 Autoconfig

Parameters

Note:Interface ID does NOT support ZERO COMPRESSION"::".Please enter the complete Information
For example:Please enter"0:0:0:2" intstead of "::2".

Link Local Address	fe80::204:edff:fe00:d
Dynamic IPv6 Address	
Static LAN IPv6 Address Configuration	
Interface Address/Prefix Length	
IPv6 LAN Application	
Issue Router Advertisements	□ Enable

Link Local Address: the Link local address for this device.

Dynamic IPv6 Address: this field displays the dynamic obtained IPv6 address if you haven't set static IPv6 address.

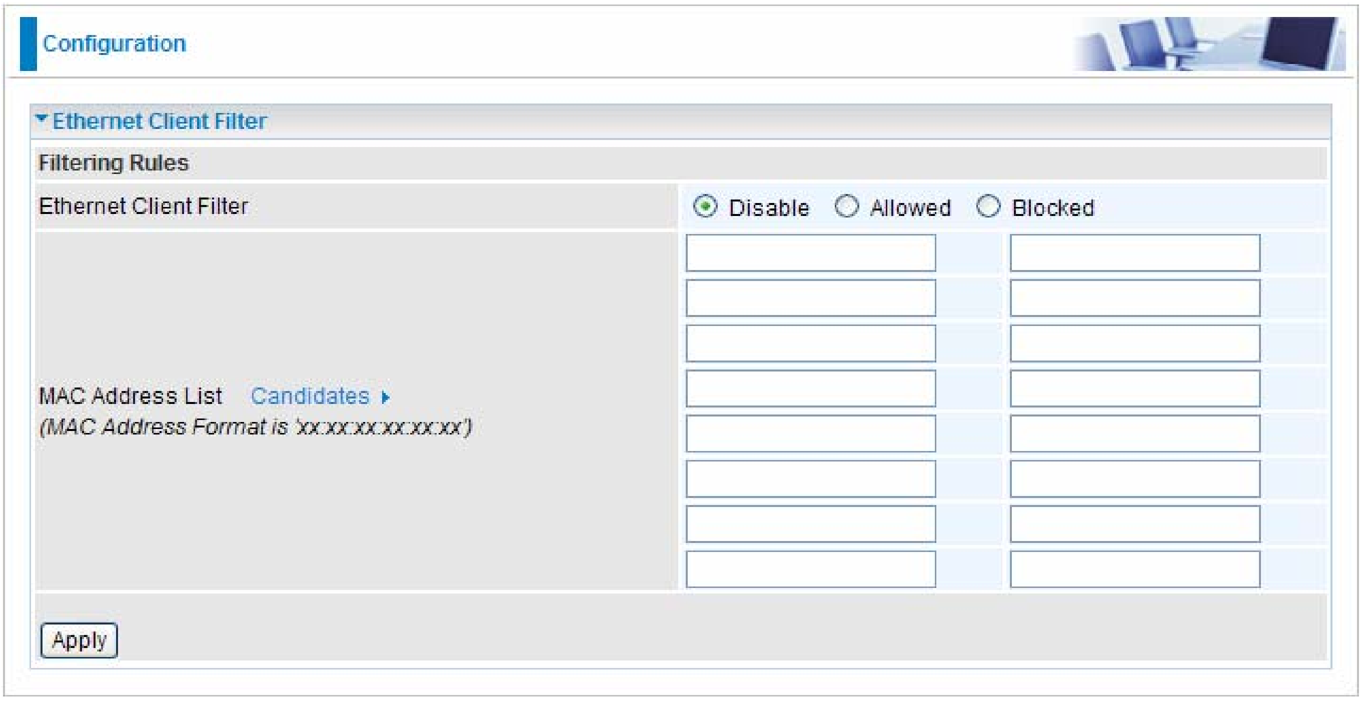
Interface Address/Prefix length: enter the static LAN IPv6 address.

Issue Router Advertisements: check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

Ethernet Client Filter

The Ethernet Client Filter supports up to 16 Ethernet network machines that helps you to manage your network control to accept traffic from specific authorized machines or can restrict unwanted machine(s) to access your LAN.

There are no pre-define 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')*	

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

⊙ **Allowed:** check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is listed.

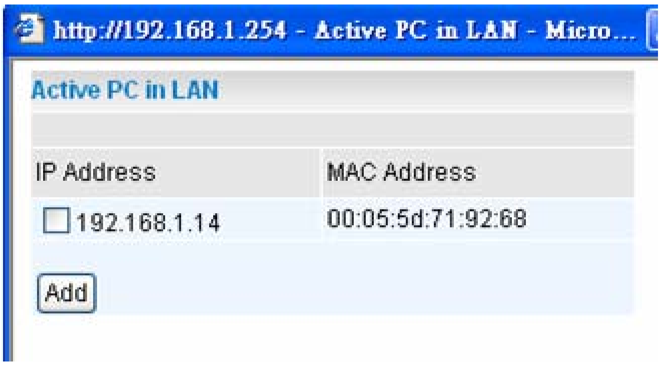
⊙ **Blocked:** check to prevent unwanted device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is not listed.

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: automatically detects devices connected to the router through the Ethernet.

Candidates ▸ → **Active PC in LAN**



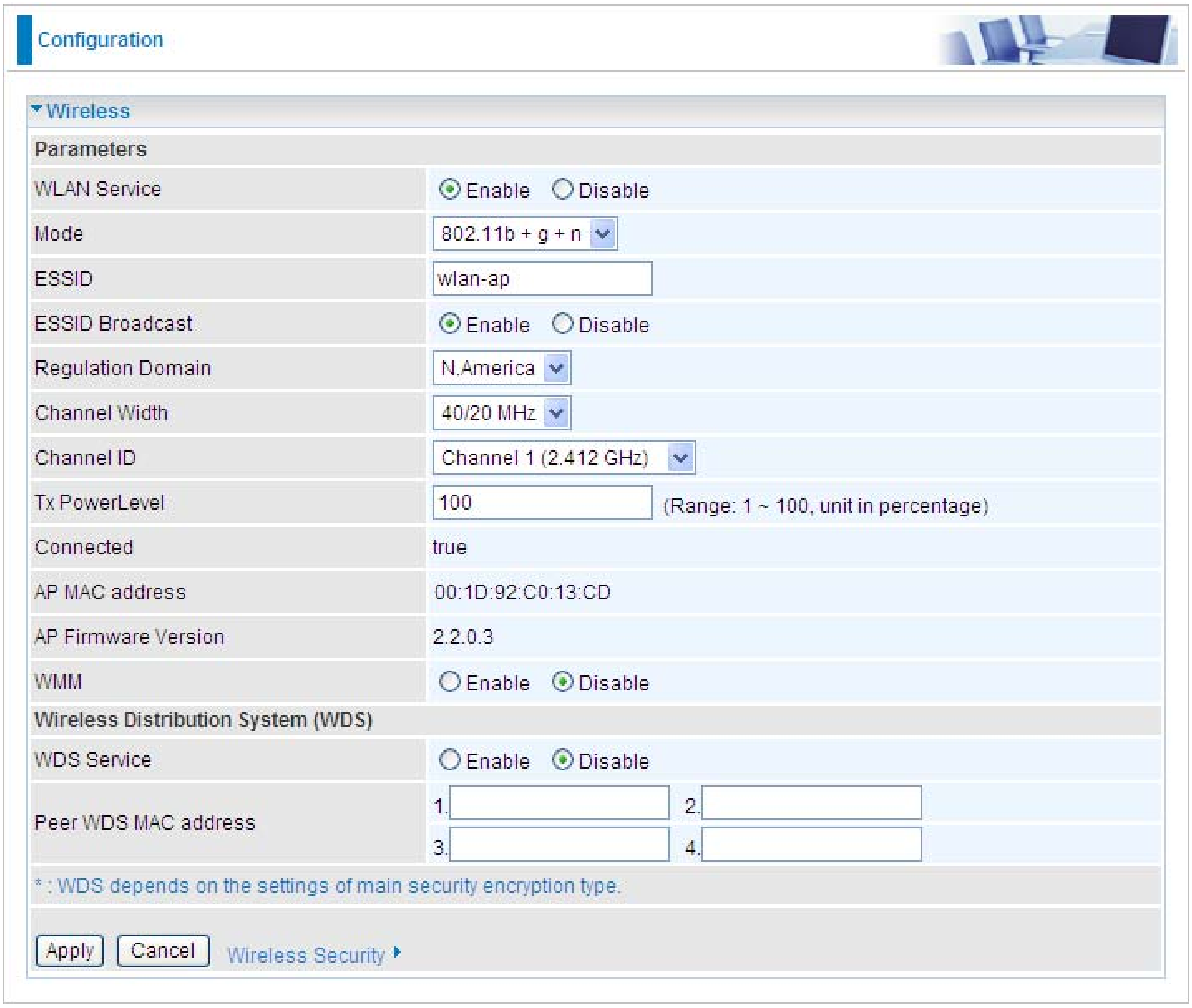
Active PC in LAN

IP Address	MAC Address
□ 192.168.1.14	00:05:5d:71:92:68

Active PC in LAN displays a list of individual Ethernet device's IP Address & MAC Address which connecting to the router.

You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table. The maximum Ethernet client is 16.

Wireless



Configuration

▾ Wireless

Parameters	
WLAN Service	● Enable ○ Disable
Mode	802.11b + g + n
ESSID	wlan-ap
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	N.America
Channel Width	40/20 MHz
Channel ID	Channel 1 (2.412 GHz)
Tx PowerLevel	100 (Range: 1 ~ 100, unit in percentage)
Connected	true
AP MAC address	00:1D:92:C0:13:CD
AP Firmware Version	2.2.0.3
WMM	○ Enable ● Disable
Wireless Distribution System (WDS)	
WDS Service	○ Enable ● Disable
Peer WDS MAC address	1. 2. 3. 4.

* : WDS depends on the settings of main security encryption type.

Parameters

WLAN Service: Choose Disabled/Enable/TimeSlot from the drop-down list.

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

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default **wlan-ap** 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.
Note: It is case sensitive and must not excess 32 characters.

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 **Enabled.**

⊙ **Disable:** If you do not want broadcast your ESSID. Any client uses "any" wireless setting cannot discover the Access Point (AP) of your router.

⊙ **Enable:** Any client that using the "any" setting can discover the Access Point (AP).

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 Wdith: Select either **20 MHz** or **20/40 MHz** for the channel bandwidth. The higher the bandwidth the better the performance will be.

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

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

TX PowerLevel: It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 1 up to maximum 100.

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

Connected: Representing in **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.

WMM: This feature works concurrently with QoS that enables the system to prioritize the flow of data packets according to 4 categories: Voice, Video, Best Efforts and Background.

- **Enable:** Click to activate WMM feature.
- **Disable:** Click to deactivate WMM feature.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed simply to define peer's MAC address of the connected AP. WDS takes advantages of cost saving and flexibility which 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 enhances its link connection security in WEP mode, WEP key encryption 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's 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's MAC Address.

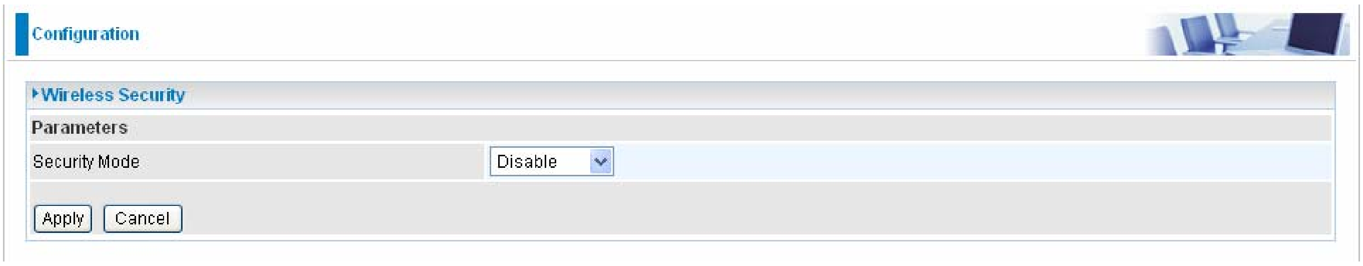
3. Peer WDS MAC Address: It is the third associated AP's MAC Address.

4. Peer WDS MAC Address: It is the fourth associated AP's MAC Address.

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

Wireless Security

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

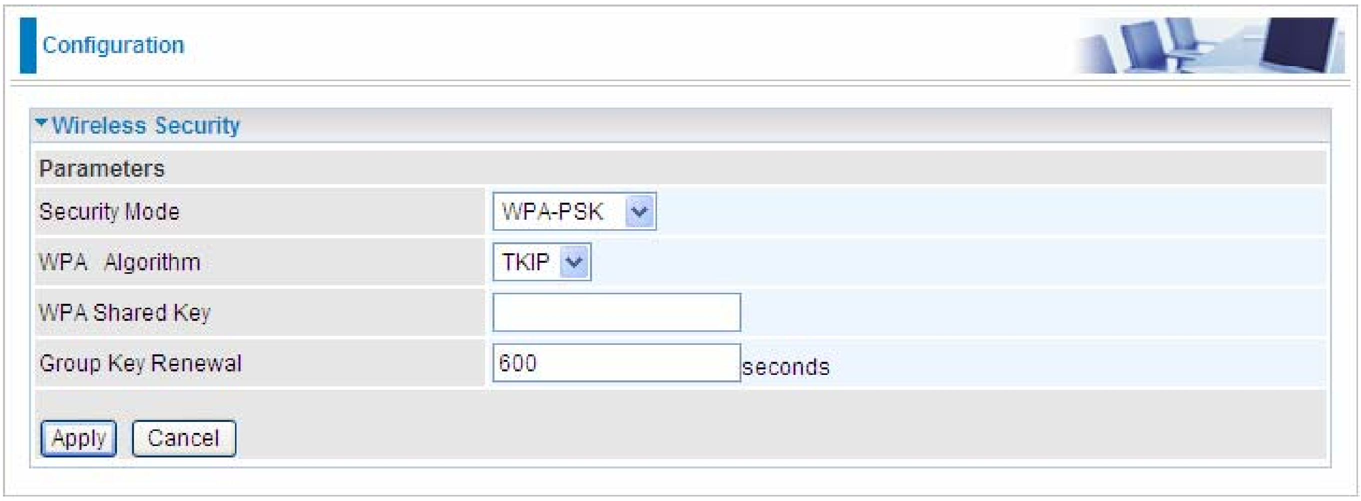


Configuration

Wireless Security

Parameters	
Security Mode	Disable

WPA-PSK / WPA2-PSK



Configuration

Wireless Security

Parameters	
Security Mode	WPA-PSK
WPA Algorithm	TKIP
WPA Shared Key	
Group Key Renewal	600 seconds

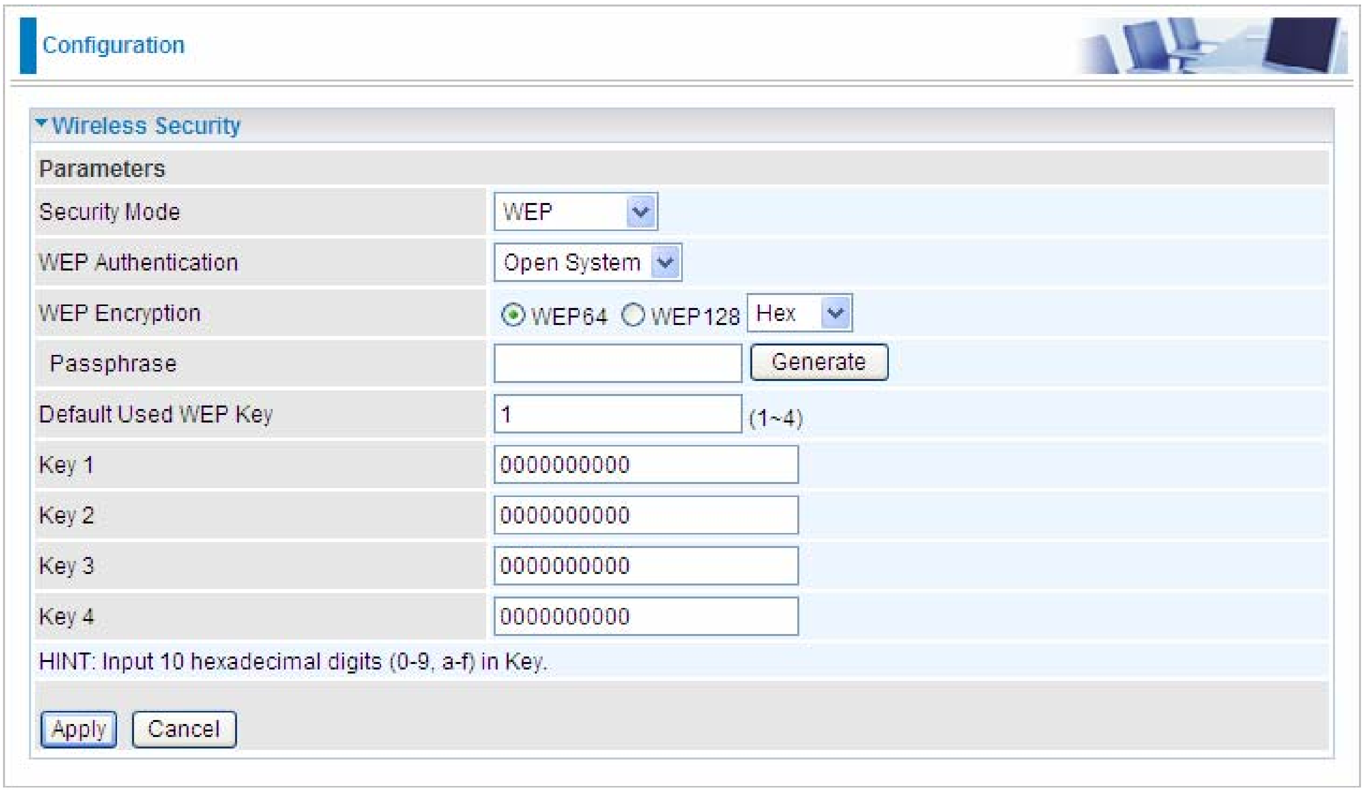
Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

WPA Algorithms: There are two types of the WPA-PSK, and WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

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. The encryption can either be HEX or ASCII.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. You can input the same string in both the AP and Client card settings to generate the same WEP keys. Please note that you do not have to enter **Key (1-4)** as below when the **Passphrase** is enabled. Passphrase will convert an inputted string into the HEX format which will automatically fill the input space for Key 1 to Key 4.

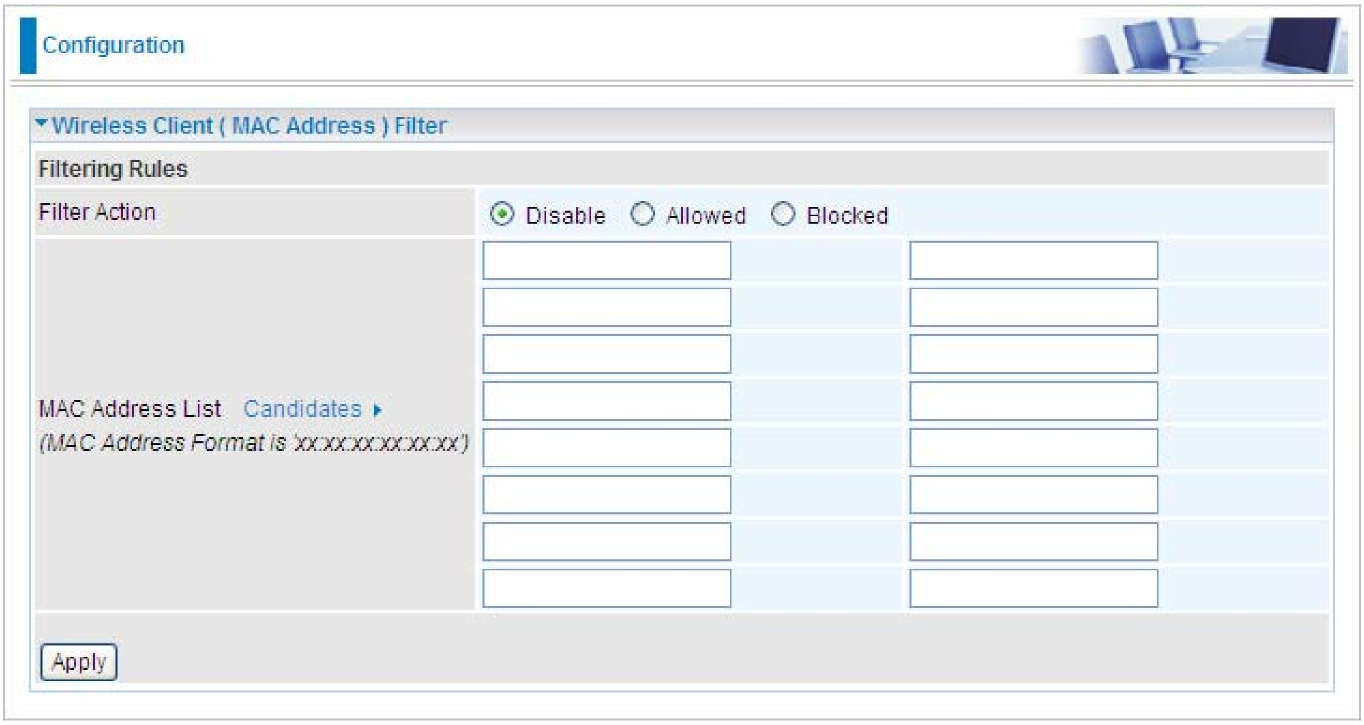
Default Used WEP Key: Select the encryption key ID. There are 4 keys to choose from so that you will not have to re-create a key every time you decide to have it as something different. You can just have 4 sets of keys to rotate instead of jus having 1 key. Please refer to **Key (1~4)** below.

Key (1-4): Enter the key to encrypt wireless data this can be in ASCII or HEX depending on the WEP Encryption that you have selected above. 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 (10 and 26 HEX codes) or ASCII style (5 and 13 ASCII codes) are required for WEP64 and WEP128 respectively-no any separator is included.

Wireless Client / MAC Address Filter

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

There are no pre-define 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')	

Apply

Wireless Client Filter: Default setting is set to **Disable**.

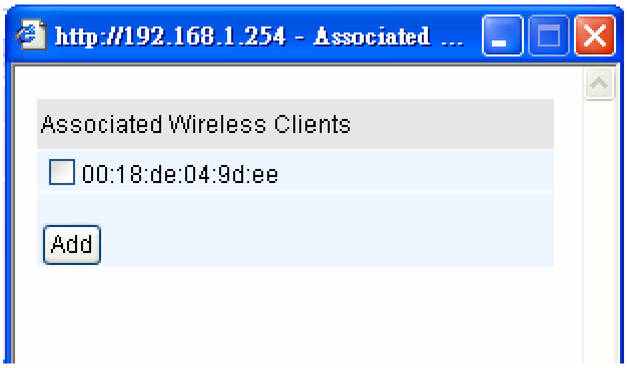
- ⊙ **Allowed:** To authorize specific device accessing your LAN by insert the MAC Address in the space provided or click Candidates ▸. Make sure your PC's MAC is listed.
- ⊙ **Blocked:** To prevent unwanted device accessing the LAN by insert the MAC Address in the space provided or click Candidates ▸. 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 devices connected to the router through the Wireless.

Candidates ▸ →**Associated Wireless Clients**



http://192.168.1.254 - Associated ...

Associated Wireless Clients

□ 00:18:de:04:9d:ee

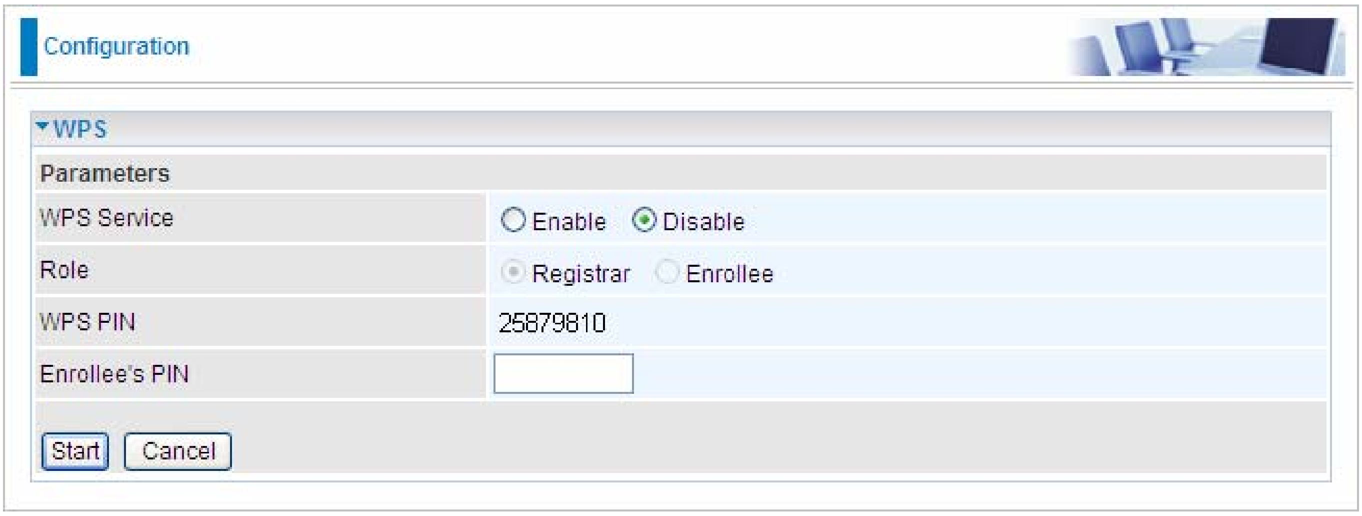
Add

Associate Wireless Client displays a list of individual wireless device's MAC Address that currently connects to the router.

You can easily by checking the box next to the MAC address to be blocked or allowed. 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 feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.



Configuration

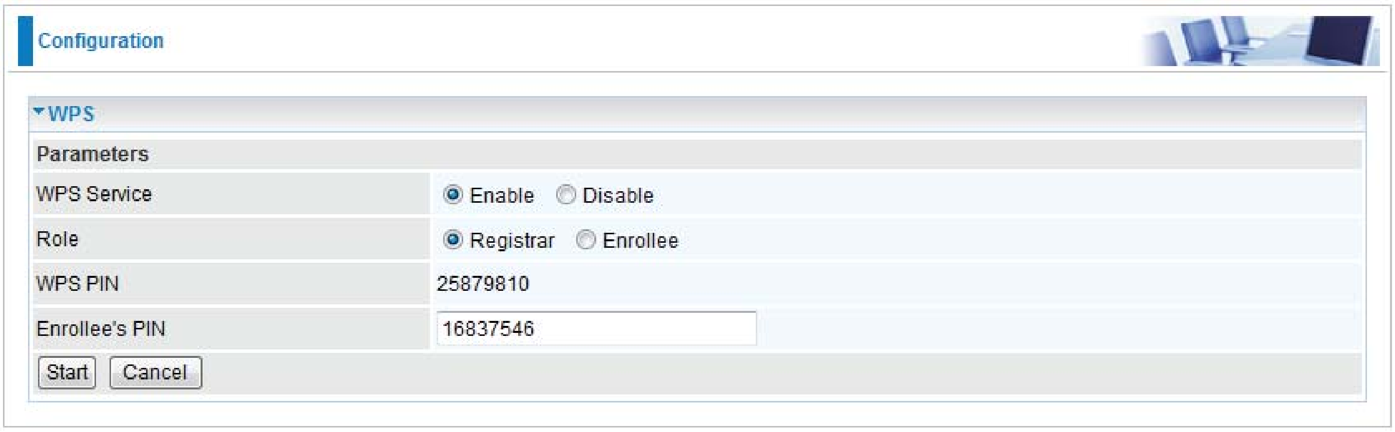
▾WPS

Parameters	
WPS Service	○ Enable ● Disable
Role	● Registrar ○ Enrollee
WPS PIN	25879810
Enrollee's PIN	

Wi-Fi Network Setup

PIN Method: Configure AP as Registrar

1. Jot down the client's Pin (e.g. 16837546).



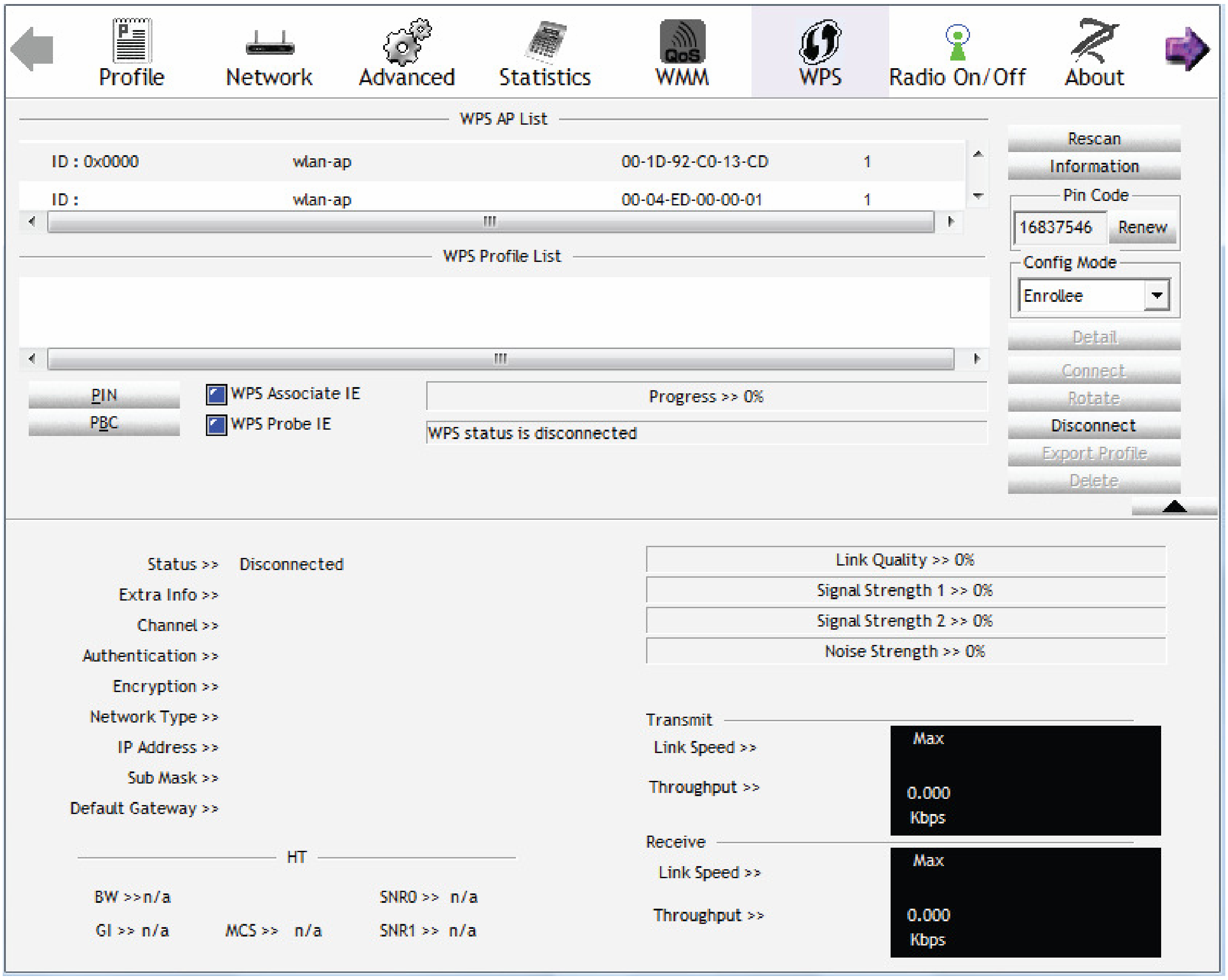
Configuration

▾WPS

Parameters	
WPS Service	● Enable ○ Disable
Role	● Registrar ○ Enrollee
WPS PIN	25879810
Enrollee's PIN	16837546

2. Enter the Enrollee's PIN number and then press Start.

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Configure Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column.Then press the PIN button located on the middle left of the page to run the scan.



WPS AP List

ID : 0x0000	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-00-00-01	1

WPS Profile List

☑ WPS Associate IE
☑ WPS Probe IE

Progress >> 0%

WPS status is disconnected

Pin Code: 16837546

Config Mode: Enrollee

Status >> Disconnected
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

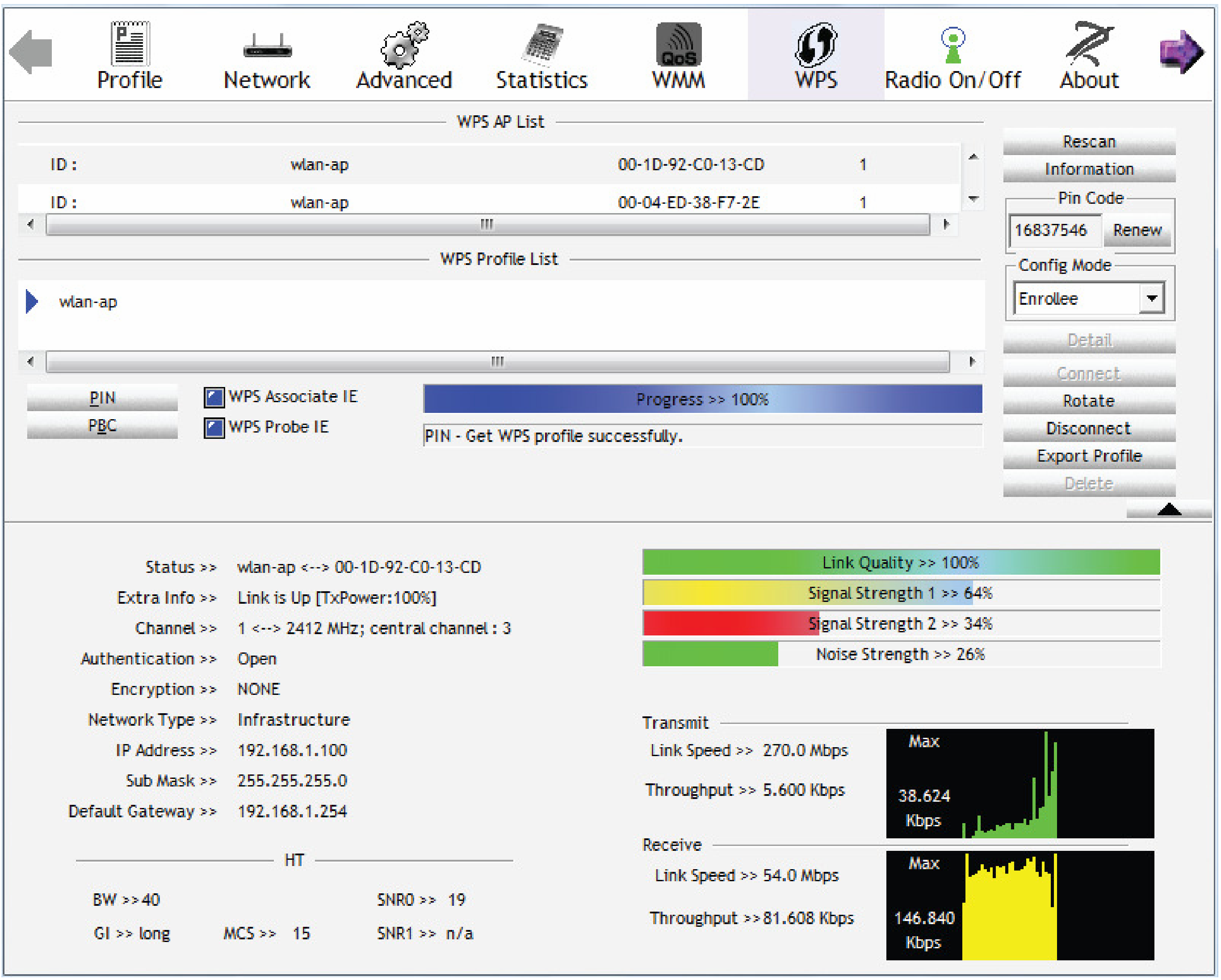
Link Quality >> 0%
Signal Strength 1 >> 0%
Signal Strength 2 >> 0%
Noise Strength >> 0%

HT
BW >>n/a
GI >> n/a MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Transmit
Link Speed >>
Throughput >>
Max
0.000 Kbps

Receive
Link Speed >>
Throughput >>
Max
0.000 Kbps

4. The client’ s SSID and security setting will now be configured to match the SSID and security setting of the registrar.



WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

Pin Code: 16837546

Config Mode: Enrollee

WPS Profile List

wlan-ap

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Status >> wlan-ap <--> 00-1D-92-C0-13-CD
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 3
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.1.100
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.254

HT

BW >> 40 SNR0 >> 19
GI >> long MCS >> 15 SNR1 >> n/a

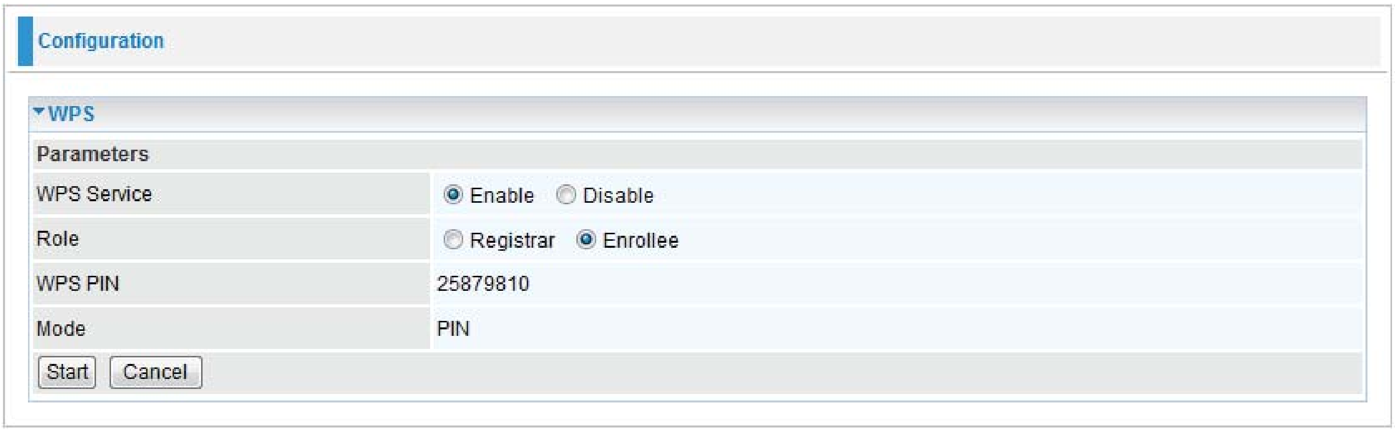
Link Quality >> 100%
Signal Strength 1 >> 64%
Signal Strength 2 >> 34%
Noise Strength >> 26%

Transmit
Link Speed >> 270.0 Mbps
Throughput >> 5.600 Kbps
38.624 Kbps

Receive
Link Speed >> 54.0 Mbps
Throughput >> 81.608 Kbps
146.840 Kbps

PIN Method: Configure AP as Enrollee

1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (e.g. 25879810).



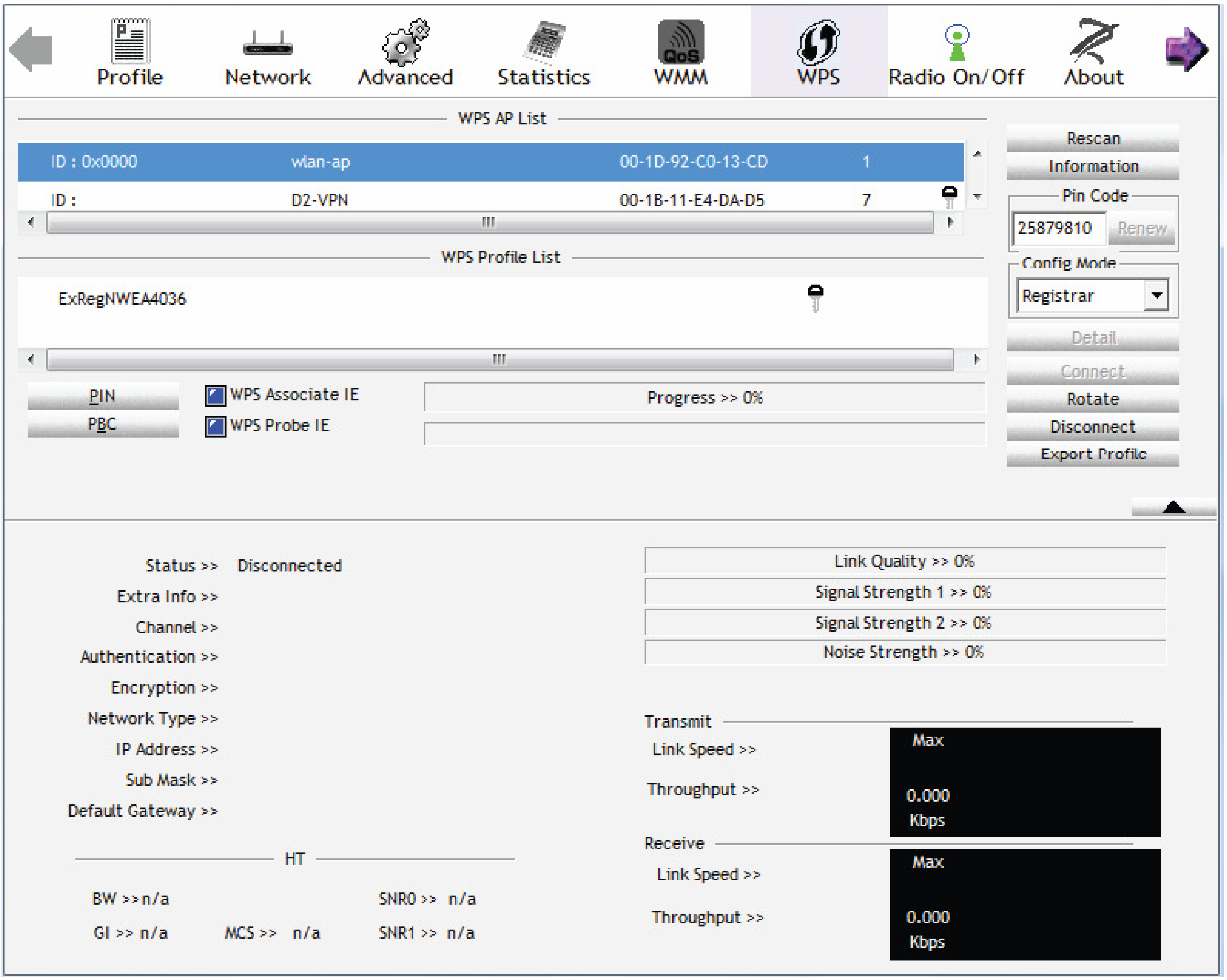
Configuration

▾WPS

Parameters	
WPS Service	● Enable ○ Disable
Role	○ Registrar ● Enrollee
WPS PIN	25879810
Mode	PIN

Start Cancel

3. Launch the wireless client’s WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.



WPS AP List

ID : 0x0000	wlan-ap	00-1D-92-C0-13-CD	1
ID :	D2-VPN	00-1B-11-E4-DA-D5	7

WPS Profile List

ExRegNWEA4036

Pin Code: 25879810

Config Mode: Registrar

☑ WPS Associate IE
☑ WPS Probe IE

Progress >> 0%

Status >> Disconnected
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

Link Quality >> 0%
Signal Strength 1 >> 0%
Signal Strength 2 >> 0%
Noise Strength >> 0%

HT

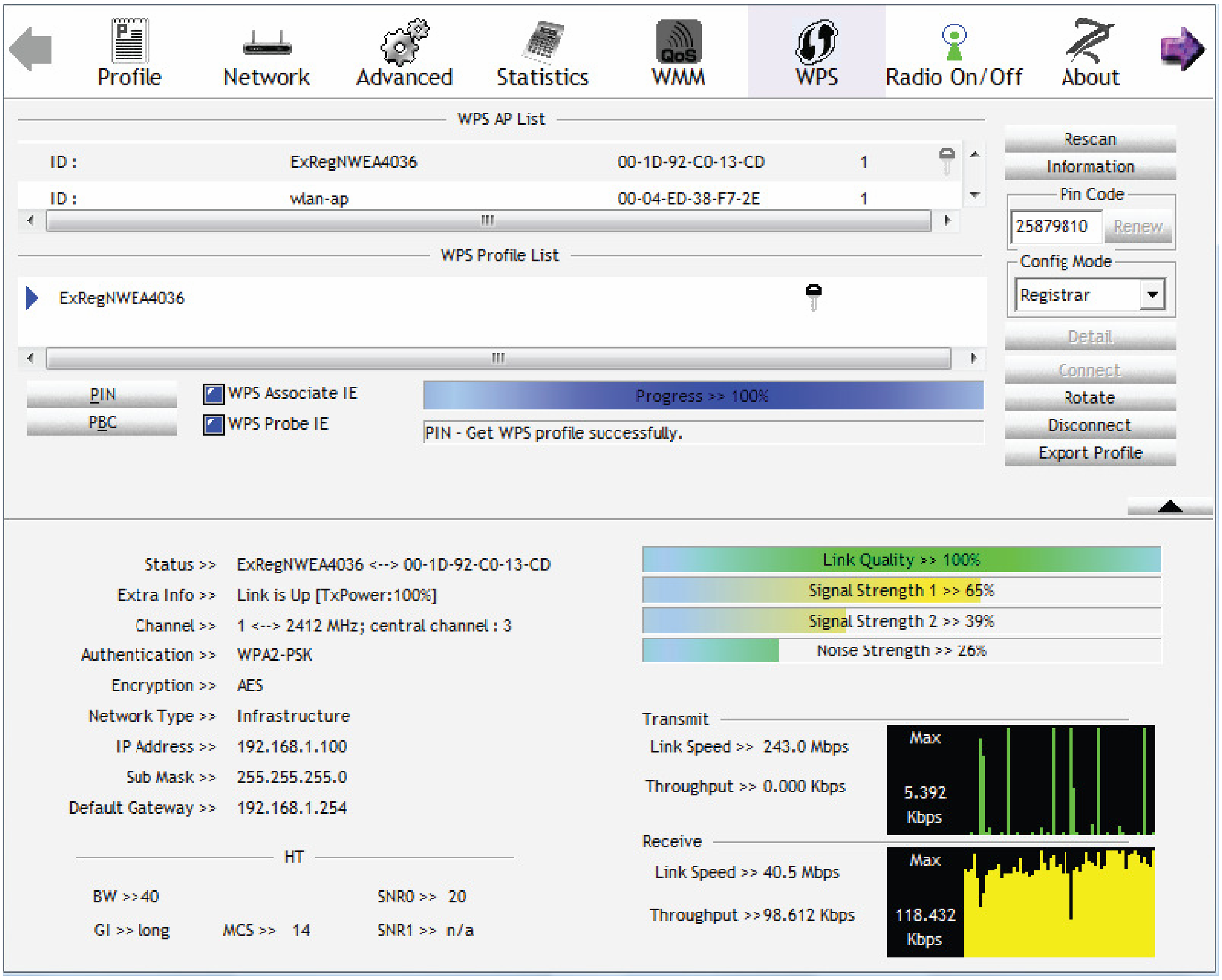
BW >> n/a
GI >> n/a MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Transmit
Link Speed >>
Throughput >>
Max
0.000
Kbps

Receive
Link Speed >>
Throughput >>
Max
0.000
Kbps

4. The router’s (AP’s) SSID and security setting will now be configured to match the SSID and security

setting of the registrar.



WPS AP List

ID :	ExRegNWEA4036	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

Pin Code: 25879810

Config Mode: Registrar

WPS Profile List

ExRegNWEA4036

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Status >> ExRegNWEA4036 <--> 00-1D-92-C0-13-CD

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel : 3

Authentication >> WPA2-PSK

Encryption >> AES

Network Type >> Infrastructure

IP Address >> 192.168.1.100

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1.254

HT

BW >>40

GI >> long

MCS >> 14

SNR0 >> 20

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 65%

Signal Strength 2 >> 39%

Noise Strength >> 26%

Transmit

Link Speed >> 243.0 Mbps

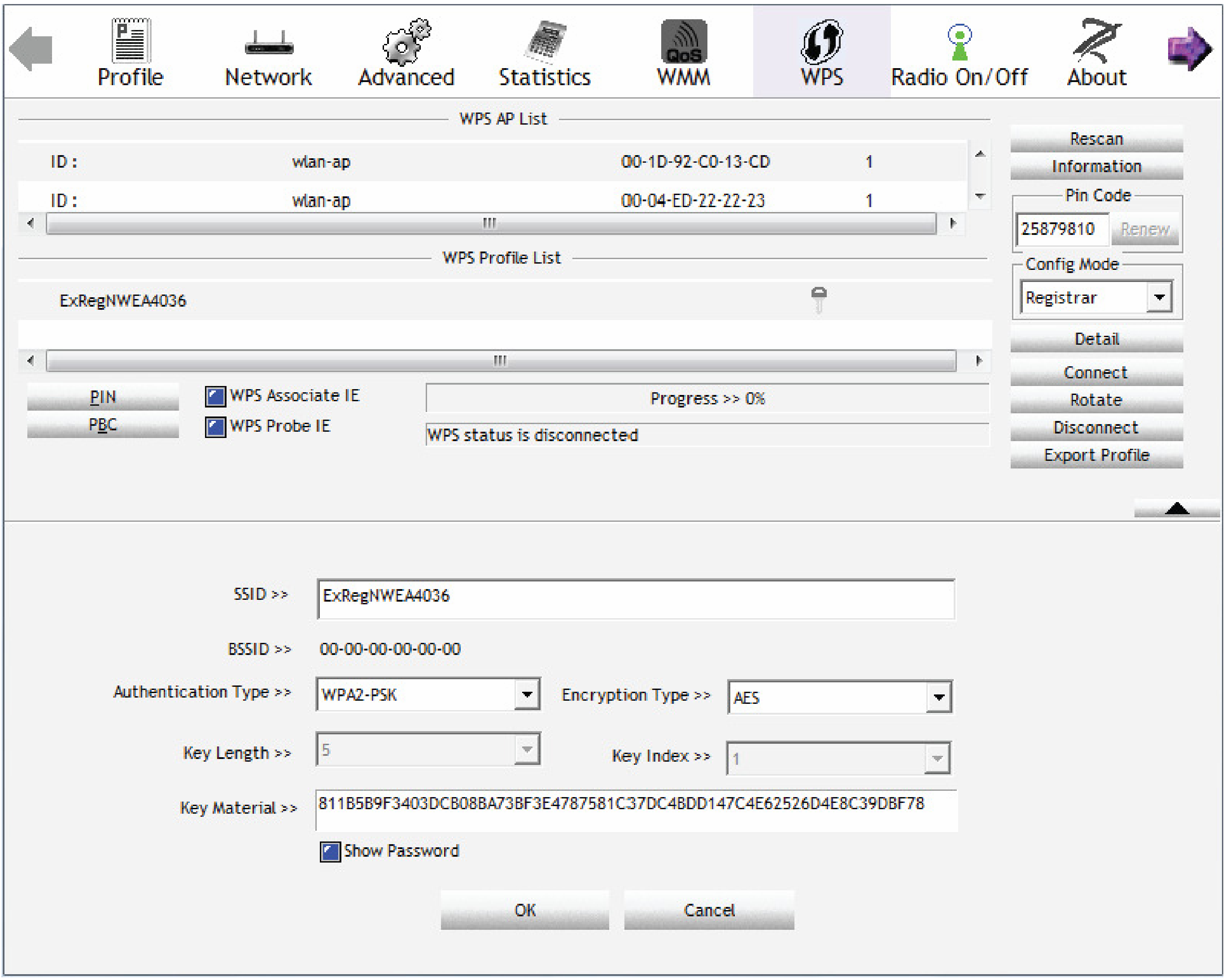
Throughput >> 0.000 Kbps

Receive

Link Speed >> 40.5 Mbps

Throughput >>98.612 Kbps

5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.



WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-22-22-23	1

WPS Profile List

ExRegNWEA4036

Pin Code: 25879810

Config Mode: Registrar

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

WPS status is disconnected

SSID >> ExRegNWEA4036

BSSID >> 00-00-00-00-00-00

Authentication Type >> WPA2-PSK

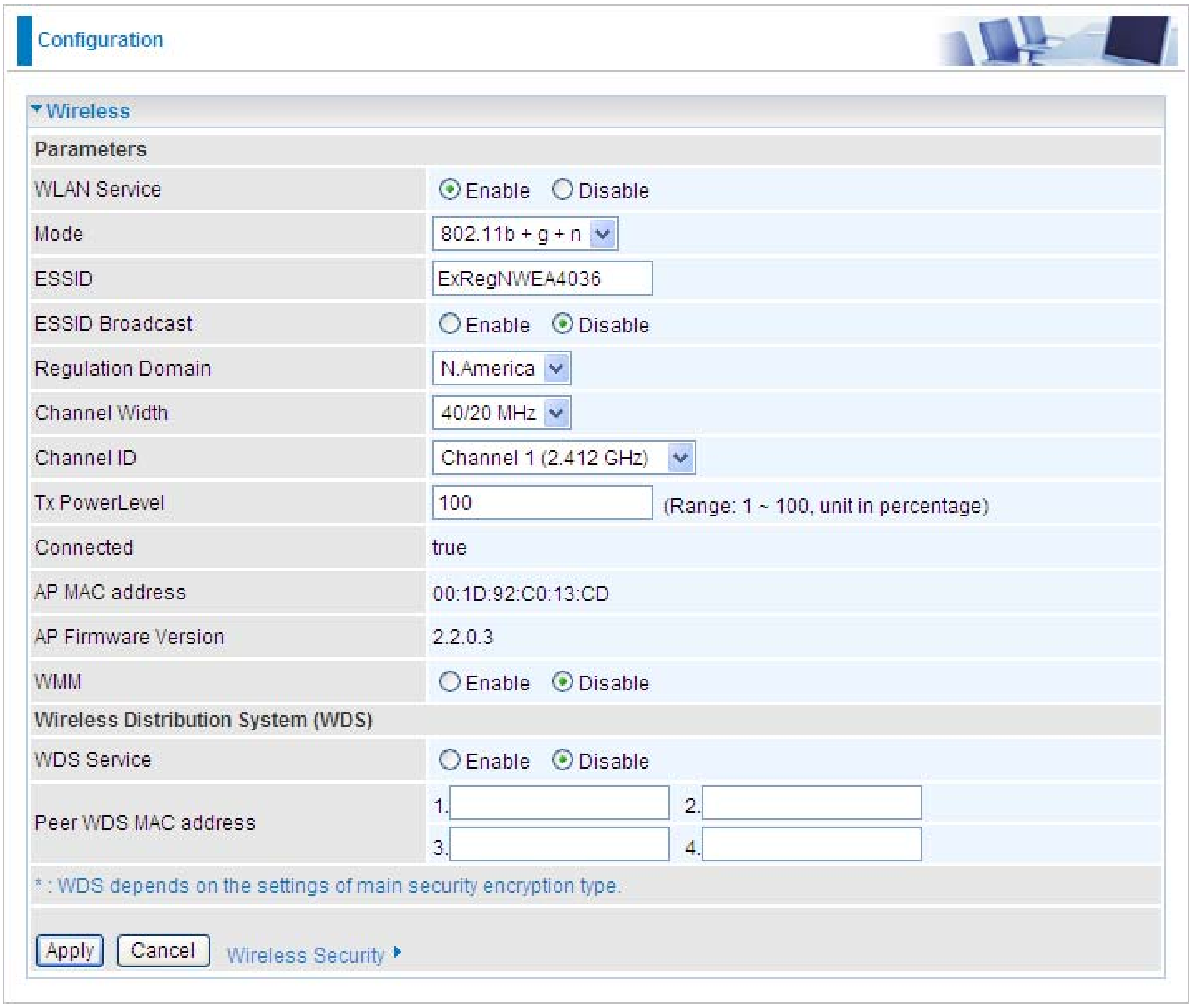
Encryption Type >> AES

Key Length >> 5

Key Index >> 1

Key Material >> 811B5B9F3403DCB08BA73BF3E4787581C37DC4BDD147C4E62526D4E8C39DBF78

☑ Show Password

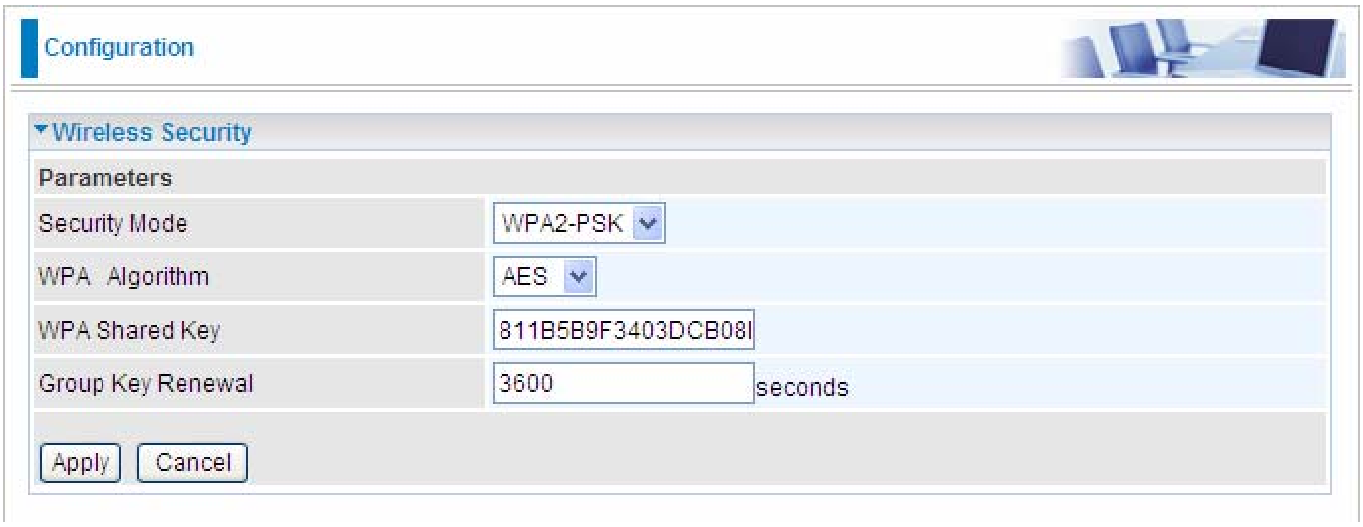


Configuration

▾ Wireless

Parameters	
WLAN Service	● Enable ○ Disable
Mode	802.11b + g + n
ESSID	ExRegNWEA4036
ESSID Broadcast	○ Enable ● Disable
Regulation Domain	N.America
Channel Width	40/20 MHz
Channel ID	Channel 1 (2.412 GHz)
Tx PowerLevel	100 (Range: 1 ~ 100, unit in percentage)
Connected	true
AP MAC address	00:1D:92:C0:13:CD
AP Firmware Version	2.2.0.3
WMM	○ Enable ● Disable
Wireless Distribution System (WDS)	
WDS Service	○ Enable ● Disable
Peer WDS MAC address	1. 2. 3. 4.

* : WDS depends on the settings of main security encryption type.



Configuration

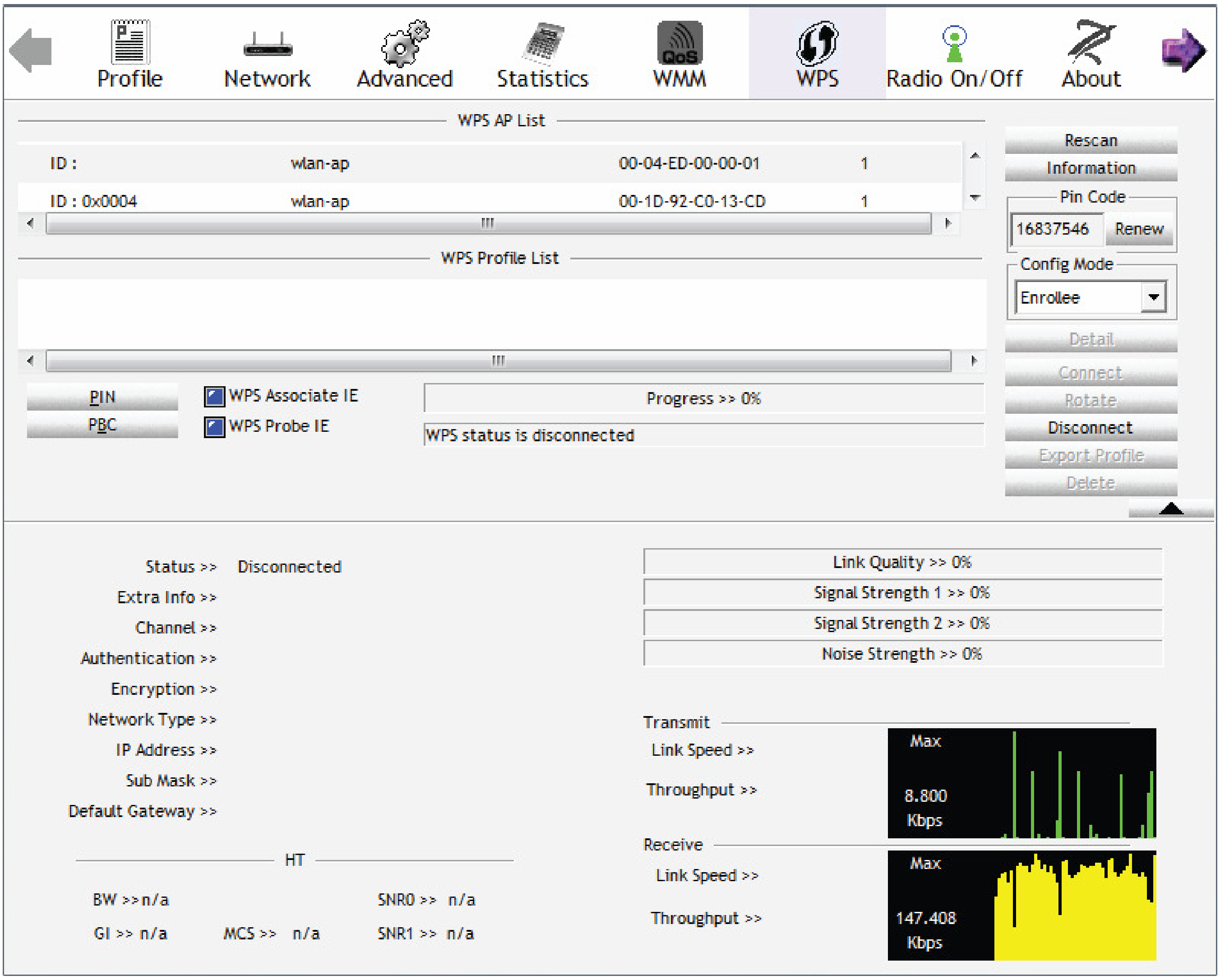
▾ Wireless Security

Parameters	
Security Mode	WPA2-PSK
WPA Algorithm	AES
WPA Shared Key	811B5B9F3403DCB08I
Group Key Renewal	3600 seconds

PBC Method:

1. Press the PBC button of the AP.

2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.



WPS AP List

ID :	wlan-ap	00-04-ED-00-00-01	1
ID : 0x0004	wlan-ap	00-1D-92-C0-13-CD	1

WPS Profile List

Pin Code: 16837546

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

WPS status is disconnected

Status >> Disconnected
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

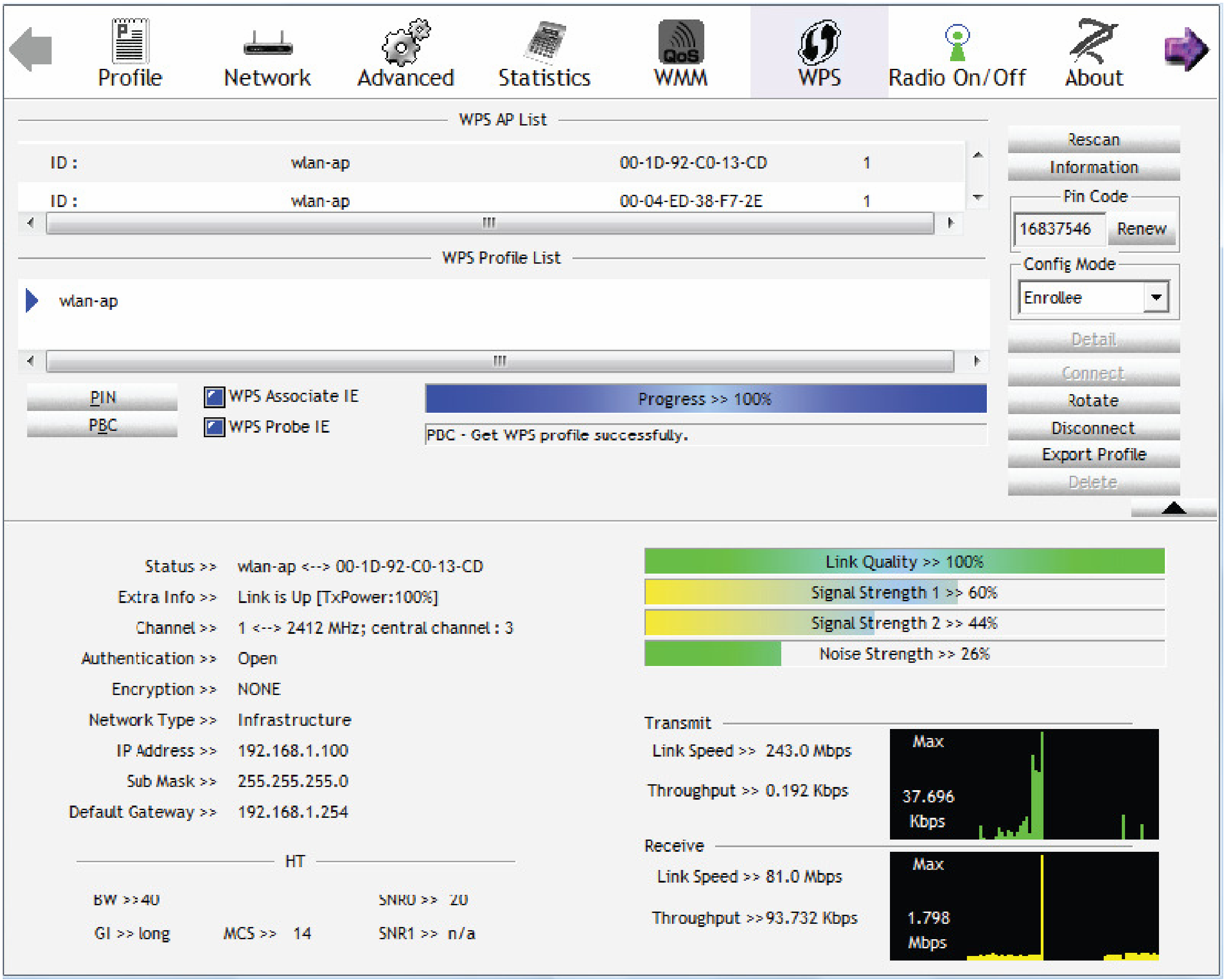
Link Quality >> 0%
Signal Strength 1 >> 0%
Signal Strength 2 >> 0%
Noise Strength >> 0%

HT
BW >> n/a
GI >> n/a MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Transmit
Link Speed >>
Throughput >>
Max
8.800 Kbps

Receive
Link Speed >>
Throughput >>
Max
147.408 Kbps

3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



WPS AP List

ID :	wlan-ap	00-1D-92-C0-13-CD	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

Pin Code: 16837546

Config Mode: Enrollee

WPS Profile List

wlan-ap

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

PBC - Get WPS profile successfully.

Status >> wlan-ap <--> 00-1D-92-C0-13-CD
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 3
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.1.100
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.254

HT

BW >>40 SNR0 >> 20
GI >> long MCS >> 14 SNR1 >> n/a

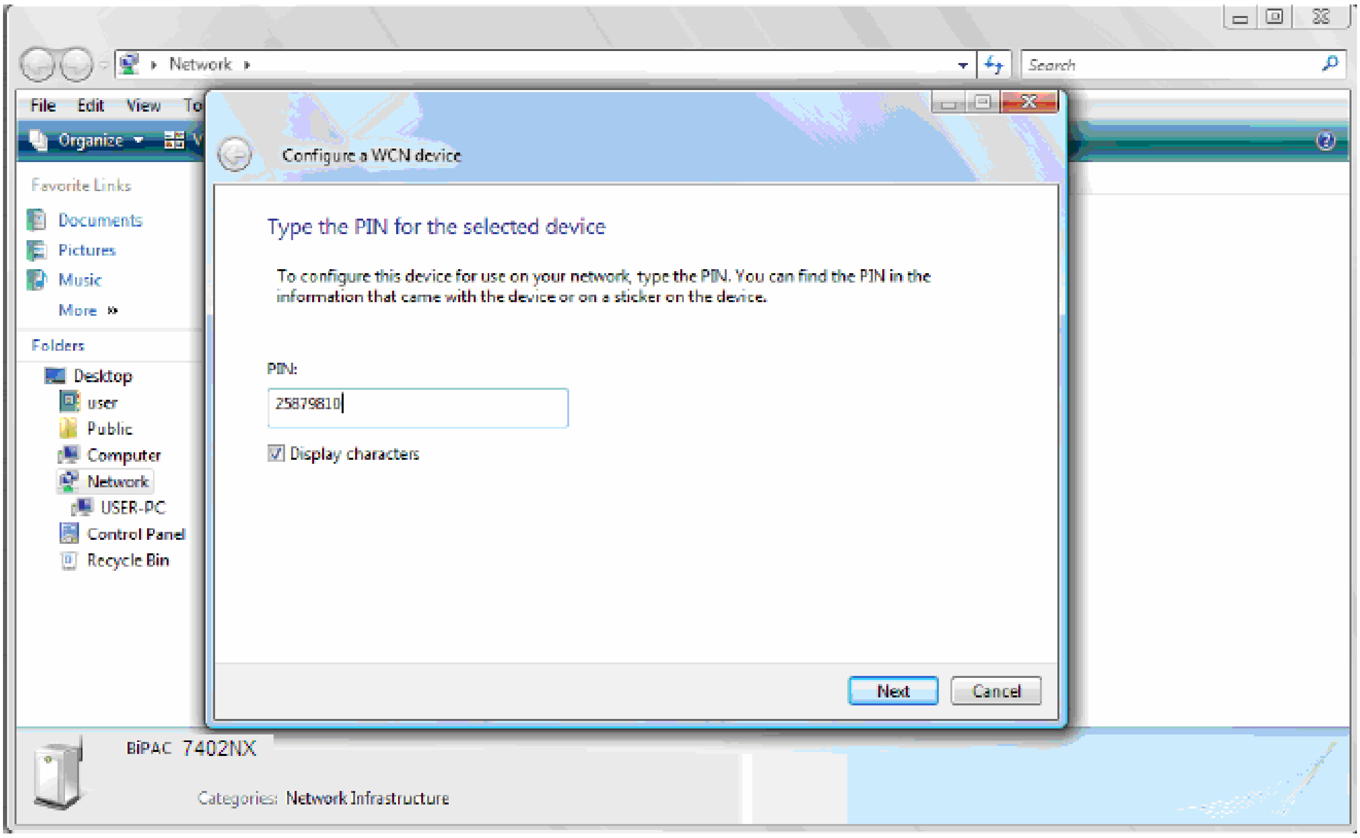
Link Quality >> 100%
Signal Strength 1 >> 60%
Signal Strength 2 >> 44%
Noise Strength >> 26%

Transmit
Link Speed >> 243.0 Mbps
Throughput >> 0.192 Kbps
Max 37.696 Kbps

Receive
Link Speed >> 81.0 Mbps
Throughput >>93.732 Kbps
Max 1.798 Mbps

Wi-Fi Network Setup with Windows Vista WCN:

1. Jot down the AP PIN from the Web (eg. 25879810).
2. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the router icon and enter the AP PIN in the column provided then press Next.



Configure a WCN device

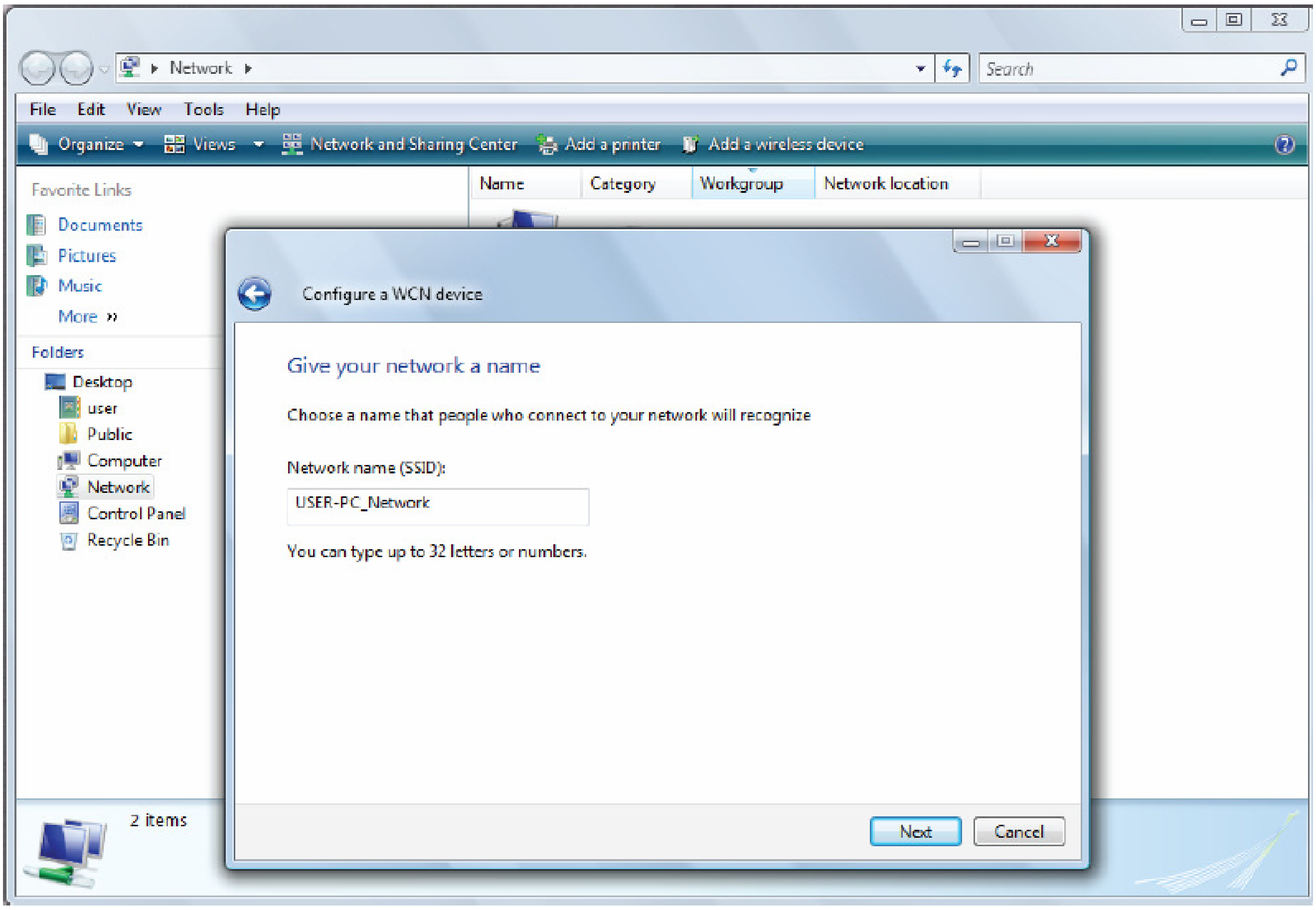
Type the PIN for the selected device

To configure this device for use on your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

PIN: 25879810

☑ Display characters

3. Enter the AP SSID then click Next.


Network
Search
File Edit View Tools Help
Organize Views Network and Sharing Center Add a printer Add a wireless device
Favorite Links
Documents
Pictures
Music
More »
Folders
Desktop
user
Public
Computer
Network
Control Panel
Recycle Bin
Name Category Workgroup Network location
2 items
Next
Cancel

Configure a WCN device

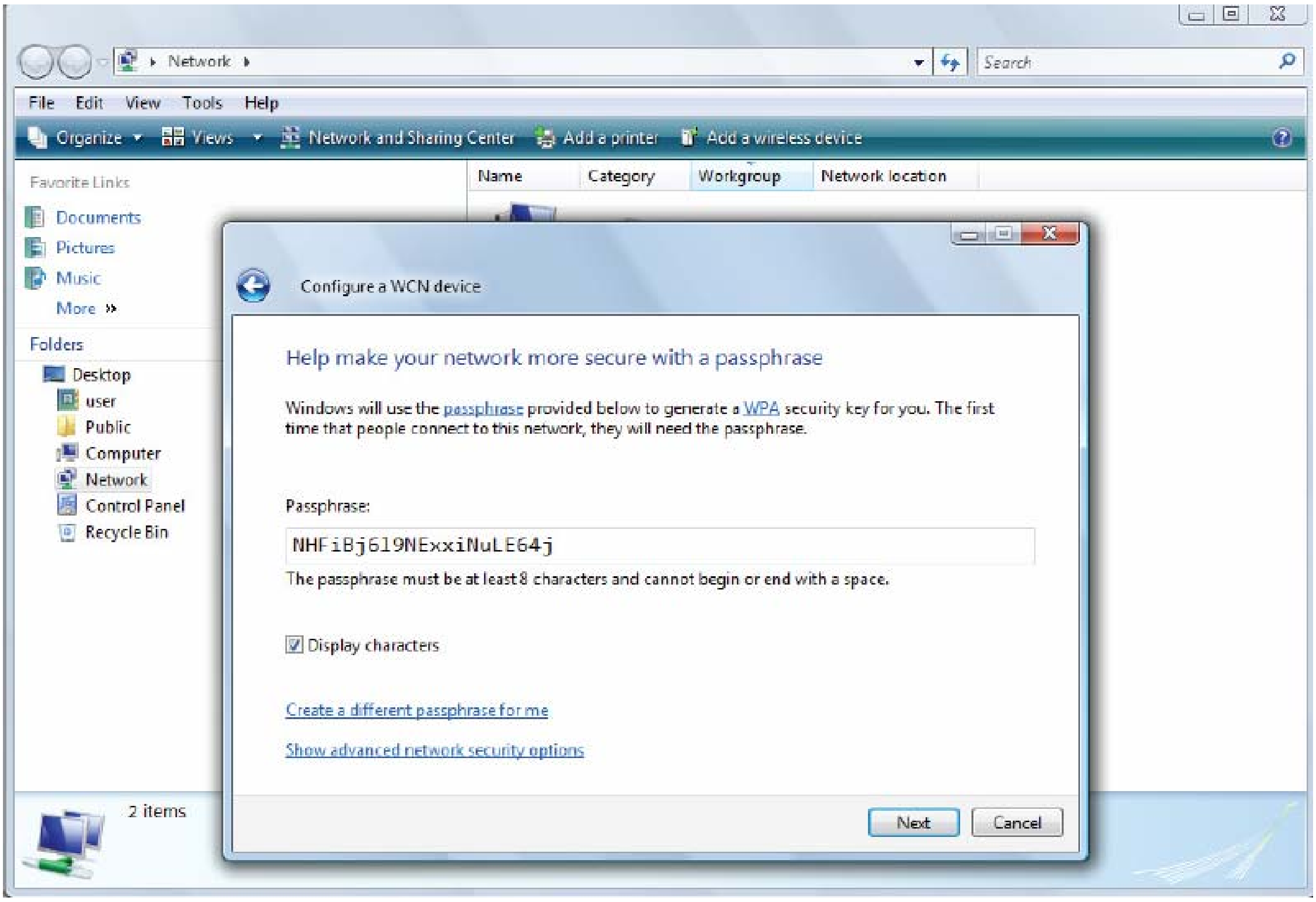
Give your network a name

Choose a name that people who connect to your network will recognize

Network name (SSID): USER-PC_Network

You can type up to 32 letters or numbers.

4. Enter the passphrase then click Next.


Network
Search
File Edit View Tools Help
Organize Views Network and Sharing Center Add a printer Add a wireless device
Favorite Links
Documents
Pictures
Music
More »
Folders
Desktop
user
Public
Computer
Network
Control Panel
Recycle Bin
Name Category Workgroup Network location
2 items
Next
Cancel

Configure a WCN device

Help make your network more secure with a passphrase

Windows will use the passphrase provided below to generate a WPA security key for you. The first time that people connect to this network, they will need the passphrase.

Passphrase: NHFiBj619NExxiNuLE64j

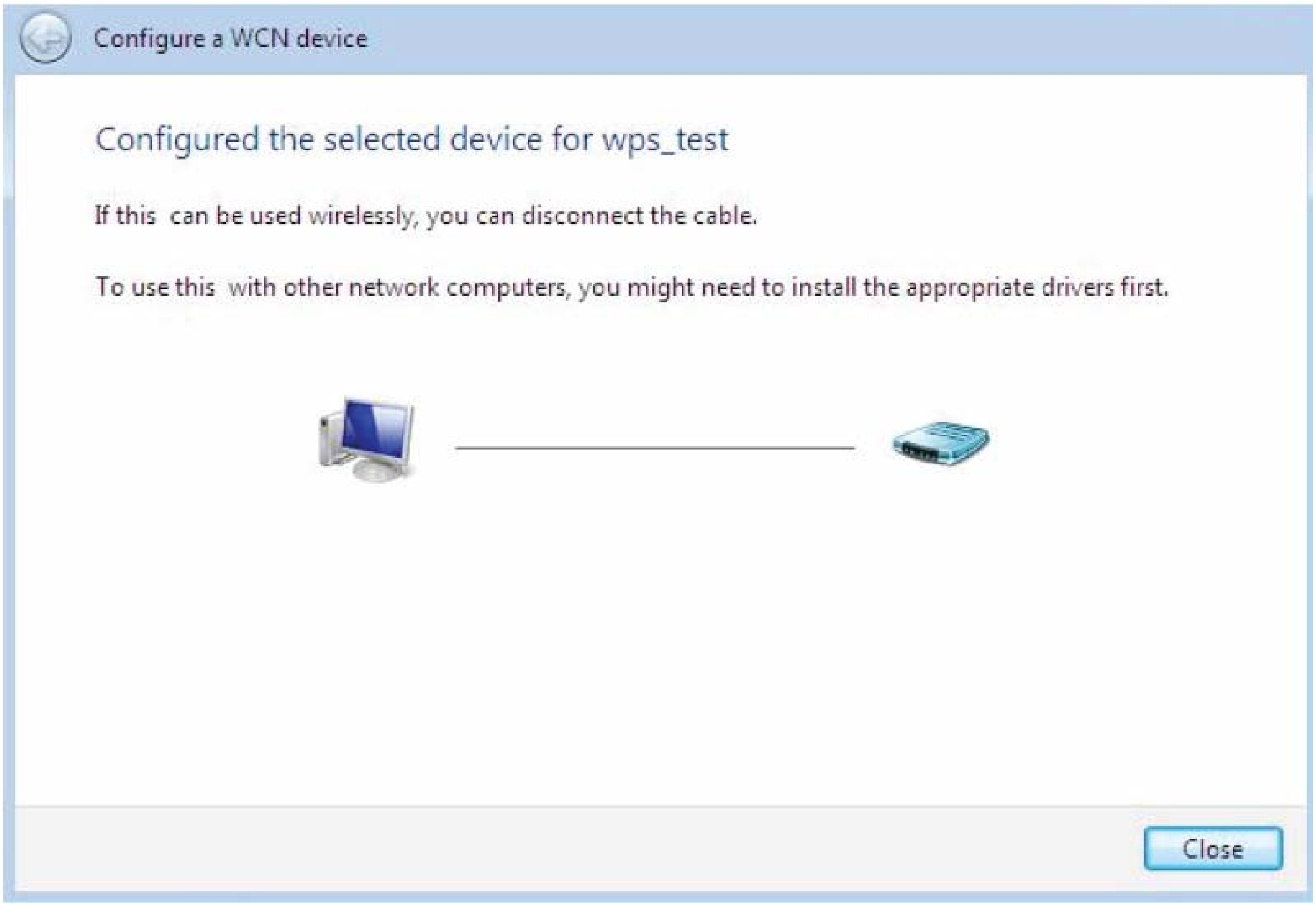
The passphrase must be at least 8 characters and cannot begin or end with a space.

☑ Display characters

Create a different passphrase for me

Show advanced network security options

5. When you have come to this step, you will have completed the Wi-Fi network setup using the built-in WCN feature in Windows Vista.



Configure a WCN device

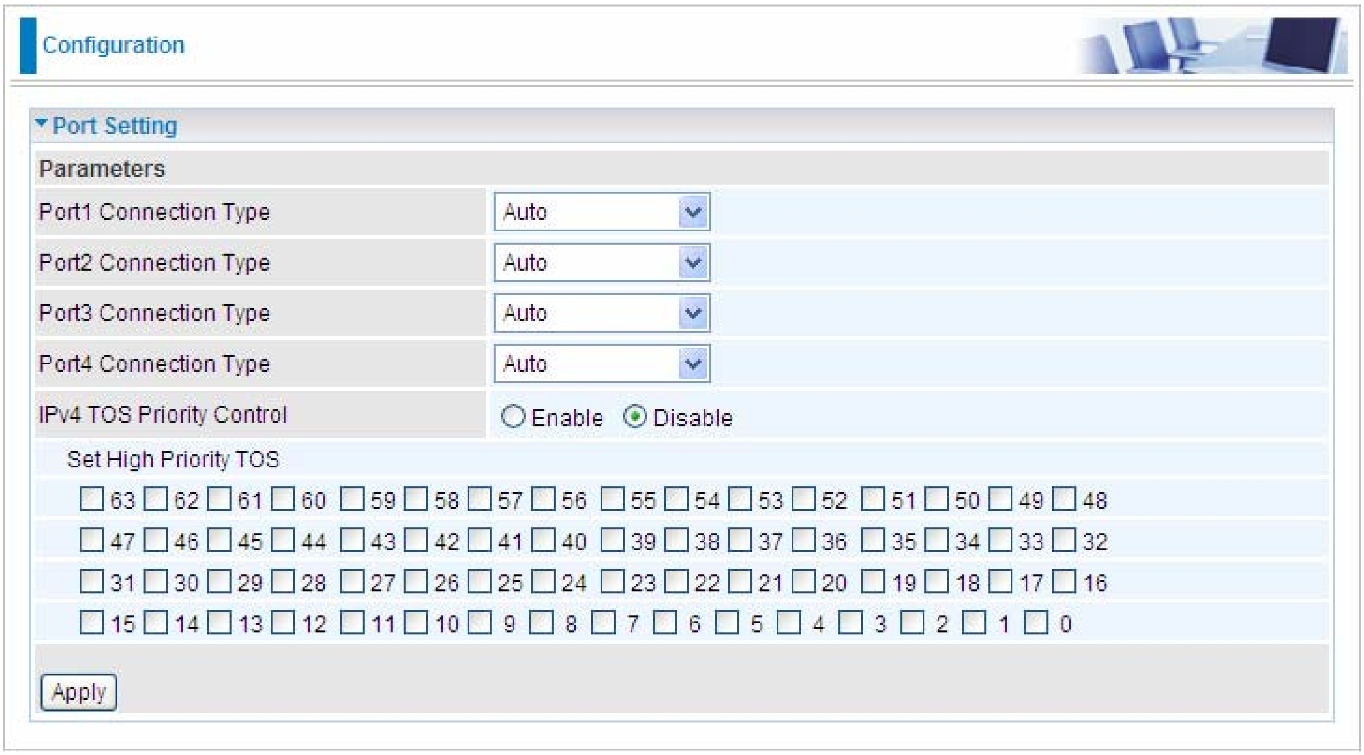
Configured the selected device for wps_test

If this can be used wirelessly, you can disconnect the cable.

To use this with other network computers, you might need to install the appropriate drivers first.

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.



▾ 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

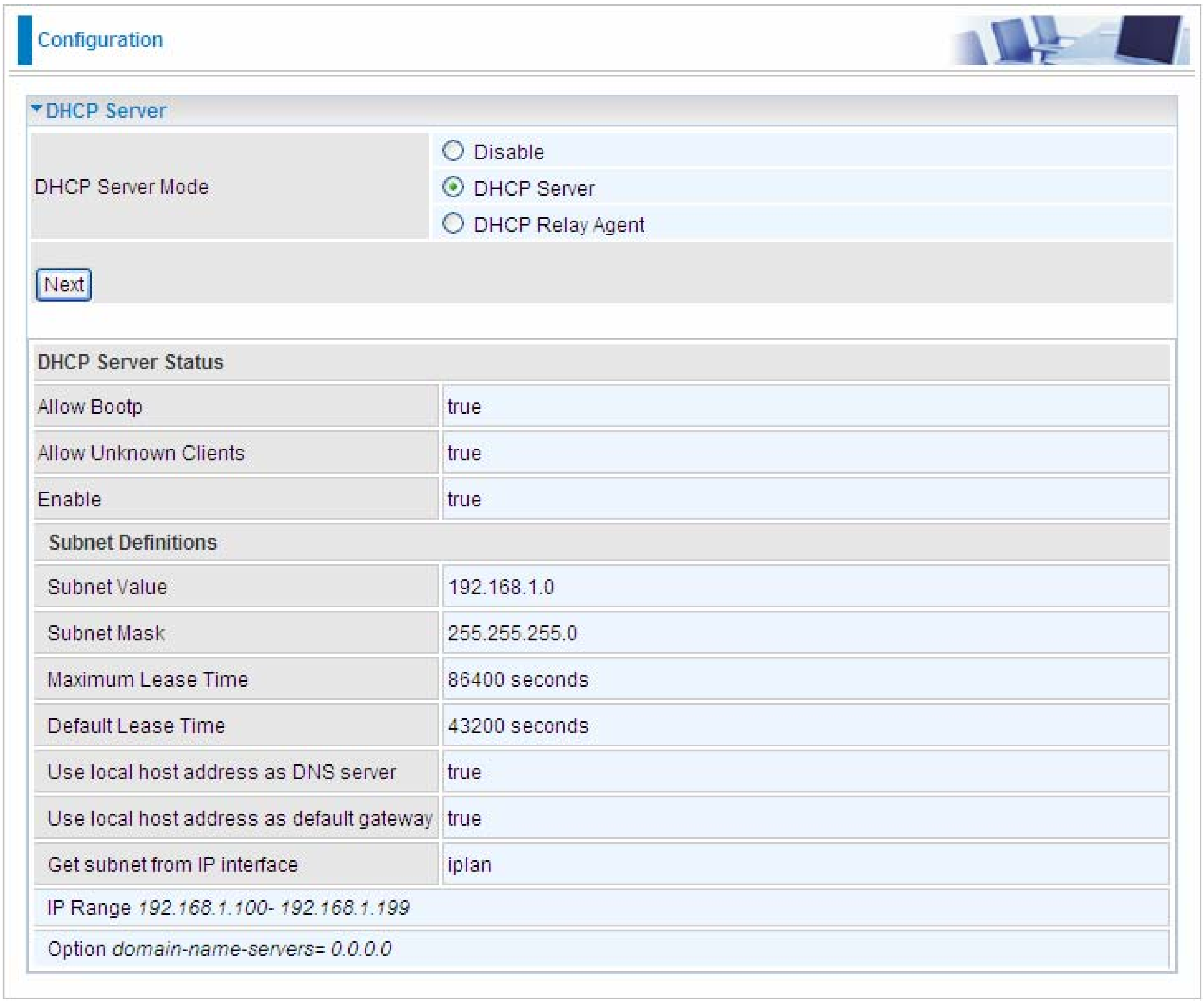
Port # Connection Type: There are Six options to choose from: Auto, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex, 1000M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility 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 is high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the TOS field matches the checked values 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 PCs on your network if they are configured to obtain IP addresses automatically.



Configuration

▾DHCP Server

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's 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 PCs on your network, and set the default gateway for each PCs to the IP address of the router (by default this is 192.168.1.254).

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

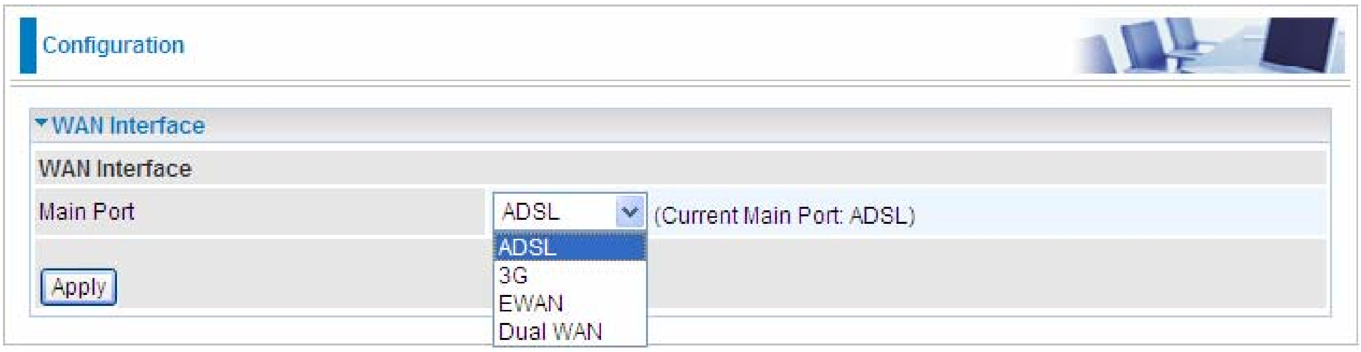
Click **Apply** to enable this function.

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 are the items within the **WAN** section: **WAN Interface**, **WAN Profile** and **ADSL Mode**.

WAN Interface

The factory default has the Connection Mode as ADSL and the Protocol as PPPoE.



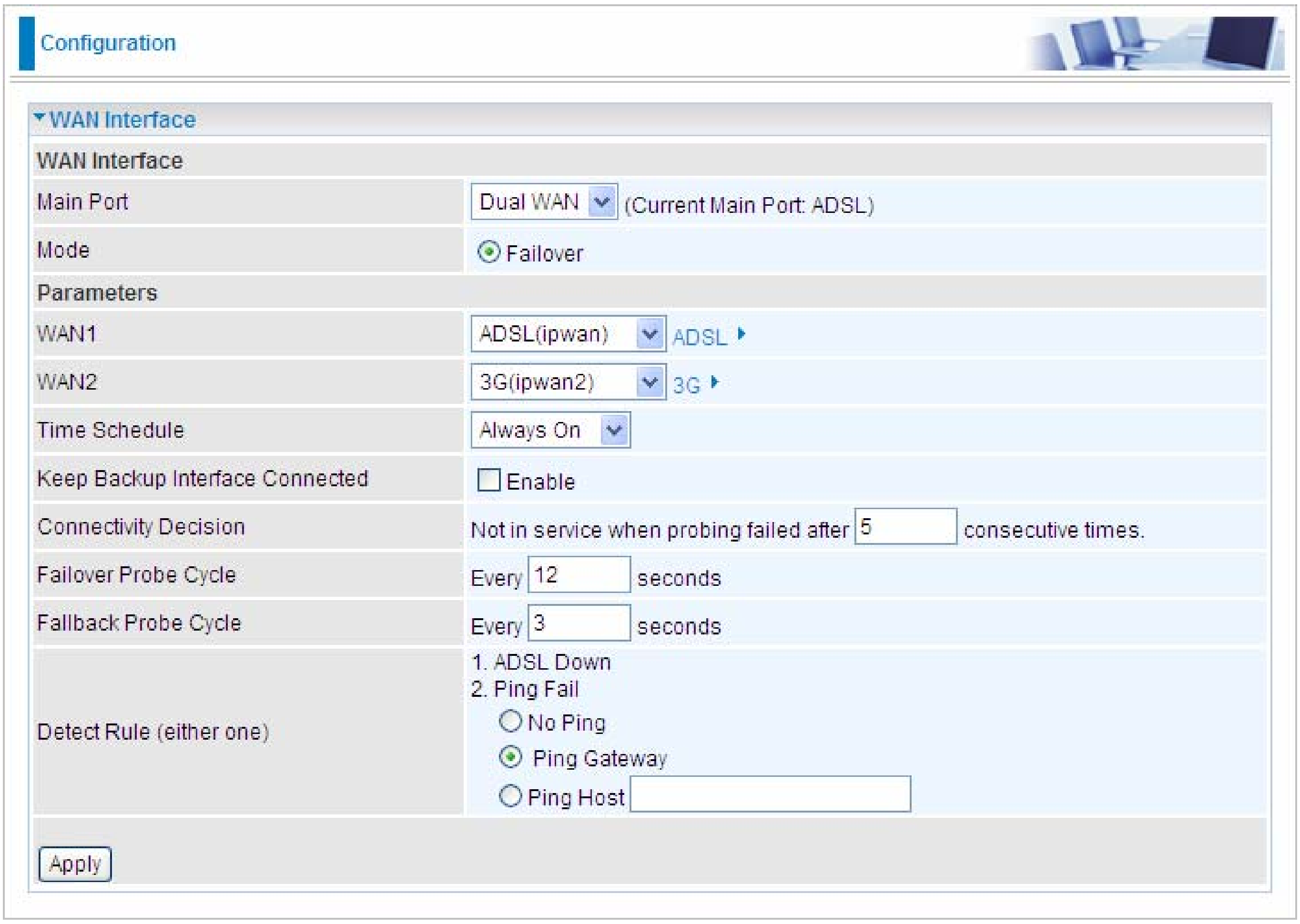
Configuration

▾WAN Interface

WAN Interface	
Main Port	ADSL (Current Main Port: ADSL)

Main Port—Dual WAN

In dual wan mode, it supports failover function. When WAN1 fails, it will switch to WAN2, and when WAN1 is OK, it will switch to WAN1 again.



Configuration

▾WAN Interface

WAN Interface	
Main Port	Dual WAN (Current Main Port: ADSL)
Mode	● Failover
Parameters	
WAN1	ADSL(ipwan) ADSL ▸
WAN2	3G(ipwan2) 3G ▸
Time Schedule	Always On
Keep Backup Interface Connected	□ Enable
Connectivity Decision	Not in service when probing failed after 5 consecutive times.
Failover Probe Cycle	Every 12 seconds
Fallback Probe Cycle	Every 3 seconds
Detect Rule (either one)	1. ADSL Down 2. Ping Fail ○ No Ping ● Ping Gateway ○ Ping Host

Main Port: Select **Dual WAN**.

Mode Failover: Set to trigger ADSL / 3G failover function ready.

WAN1: Select "ADSL" "EWAN" or "3G" mode for WAN1.

WAN2: Select the left WAN mode for WAN2 as backup port. For example, if 3G is set for main port, then there can be no option for failover/failback.

Time Schedule: A self defined time period. You may specify a time schedule for failover/failback functioning. For setup and detail, refer to Time Schedule section.

Keep Backup Interface Connected: Select Enable this function, the backup WAN port will connect always.

Connectivity Decision: Set how many times of probing failed to switch backup port.

Failover Probe Cycle: Set the time duration for the **Failover Probe Cycle** to determine when the router will switch to the backup connection (backup port) once the main connection (main port) fails.

Note: The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle duration** multiplied by **connection Decision amount** (e.g. From the image above it will be 60 seconds multiplied by 5 consecutive fails).

Failback Probe Cycle: Set the time duration for the **Failback Probe Cycle** to determine when the router will switch back to the main connection (main port) from the backup connection (backup port) once the main connection is communicating again.

Note: The time set is for each probe cycle, but the decision to change to the backup port is determined by **Probe Cycle duration** multiplied by **Connection Decision amount** (e.g. From the image above it will be 60 seconds multiplied by 5 consecutive fails).

Detect Rule:

Rule 1. ADSL Down

Rule 2. Ping Fail

⊙ **No Ping:** It will not send any ping packet to determine the connection. It means to disable the ping fail detection.

⊙ **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every "Probe Cycle".

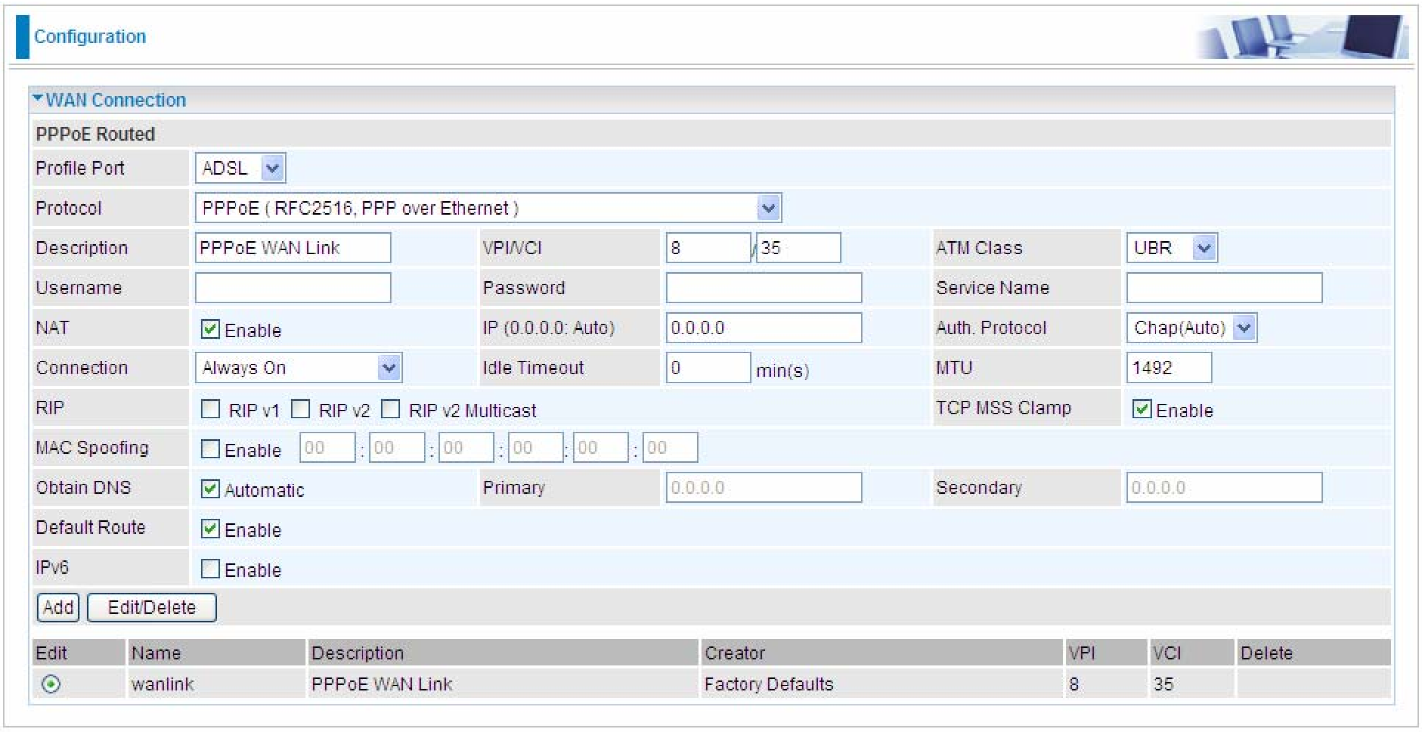
⊙ **Ping Host:** It will send ping packet to specific host and wait response in every "Probe Cycle". The host must be an IP address.

WAN Profile

ADSL

PPPoE Connection

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



Configuration

▾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
Default Route	☑ Enable				
IPv6	□ Enable				

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** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).
Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single 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 PPP session when starting up and to automatically re-establish the PPP session when disconnected by the ISP.
- ⊙ **Connect on Demand:** If you want to establish a PPP 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.

MAC Spoofing: This option is required by some service providers. You must fill in the MAC address that specify by service provider when it is required. Default is disabled.

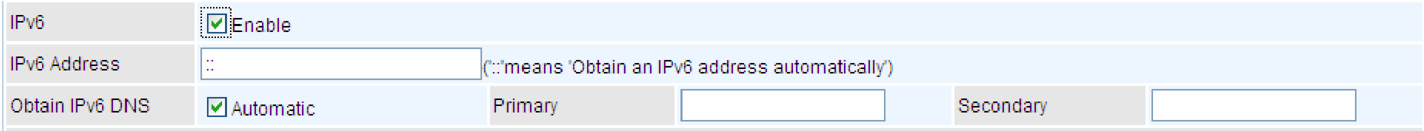
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.

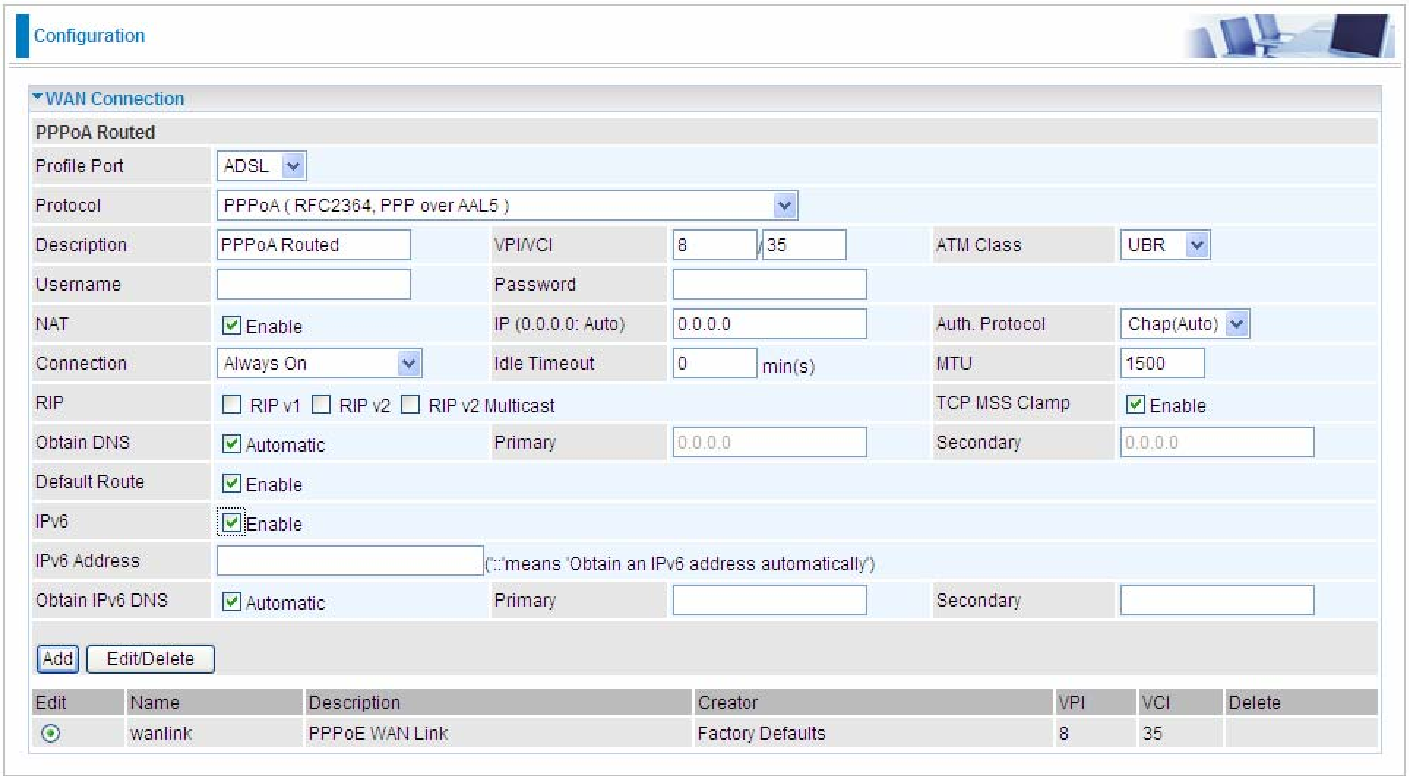


IPv6	☑ Enable				
IPv6 Address	:: ('::'means 'Obtain an IPv6 address automatically')				
Obtain IPv6 DNS	☑ Automatic	Primary		Secondary	

IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ”::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the exact one in the Primary field.

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
Default Route	☑ Enable				
IPv6	☑ Enable				
IPv6 Address	('::'means 'Obtain an IPv6 address automatically')				
Obtain IPv6 DNS	☑ Automatic	Primary		Secondary	

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** alphanumeric characters (case sensitive). This is in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).
Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single 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 PPP session when starting up and to automatically re-establish the PPP session when disconnected by the ISP.
- ⊙ **Connect on Demand:** If you want to establish a PPP 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.

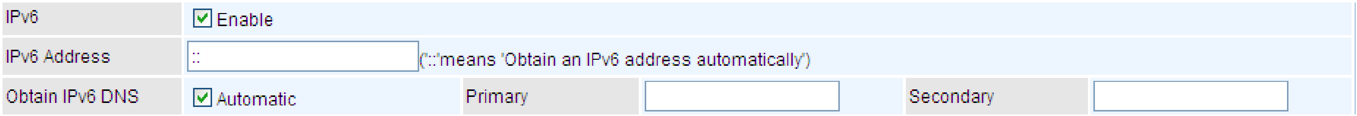
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



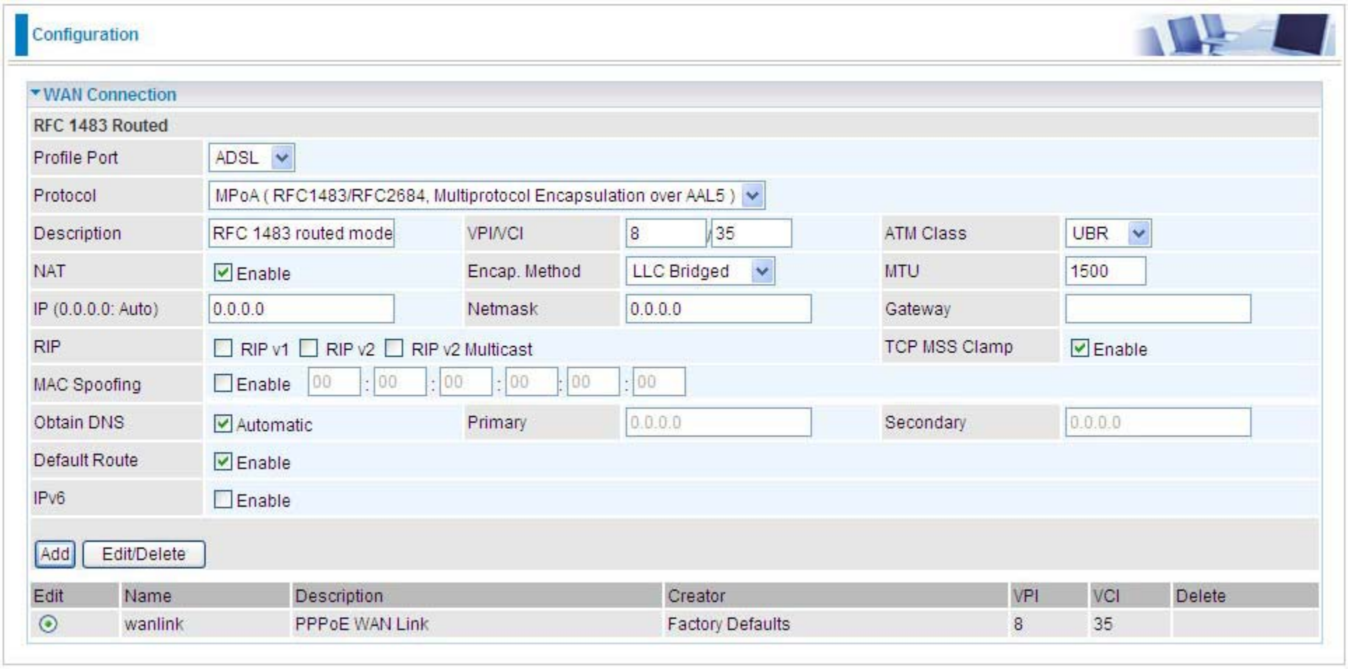
IPv6	☑ Enable				
IPv6 Address	:: ('::'means 'Obtain an IPv6 address automatically')				
Obtain IPv6 DNS	☑ Automatic	Primary		Secondary	

IPv6 Address: type the IPv6 address from your ISP, or get it automatically. ” ::” means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

.

MPoA Connection



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
Default Route	☑ Enable				
IPv6	□ Enable				

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

Netmask: The default is 0.0.0.0. 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: This option is required by some service providers. You must fill in the MAC address that specify by service provider when it is required. Default is disabled.

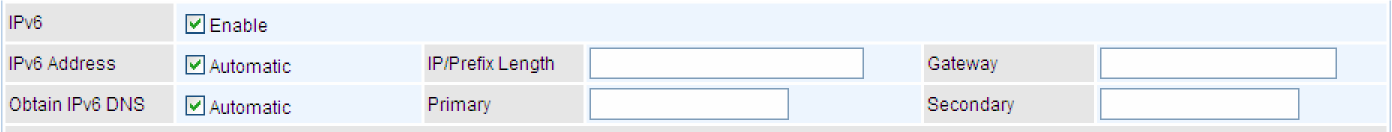
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

IPv6: check to enable IPv6 service. If enabled, please set the IPv6 Address, Ipv6 DNS, similar as IPv4.



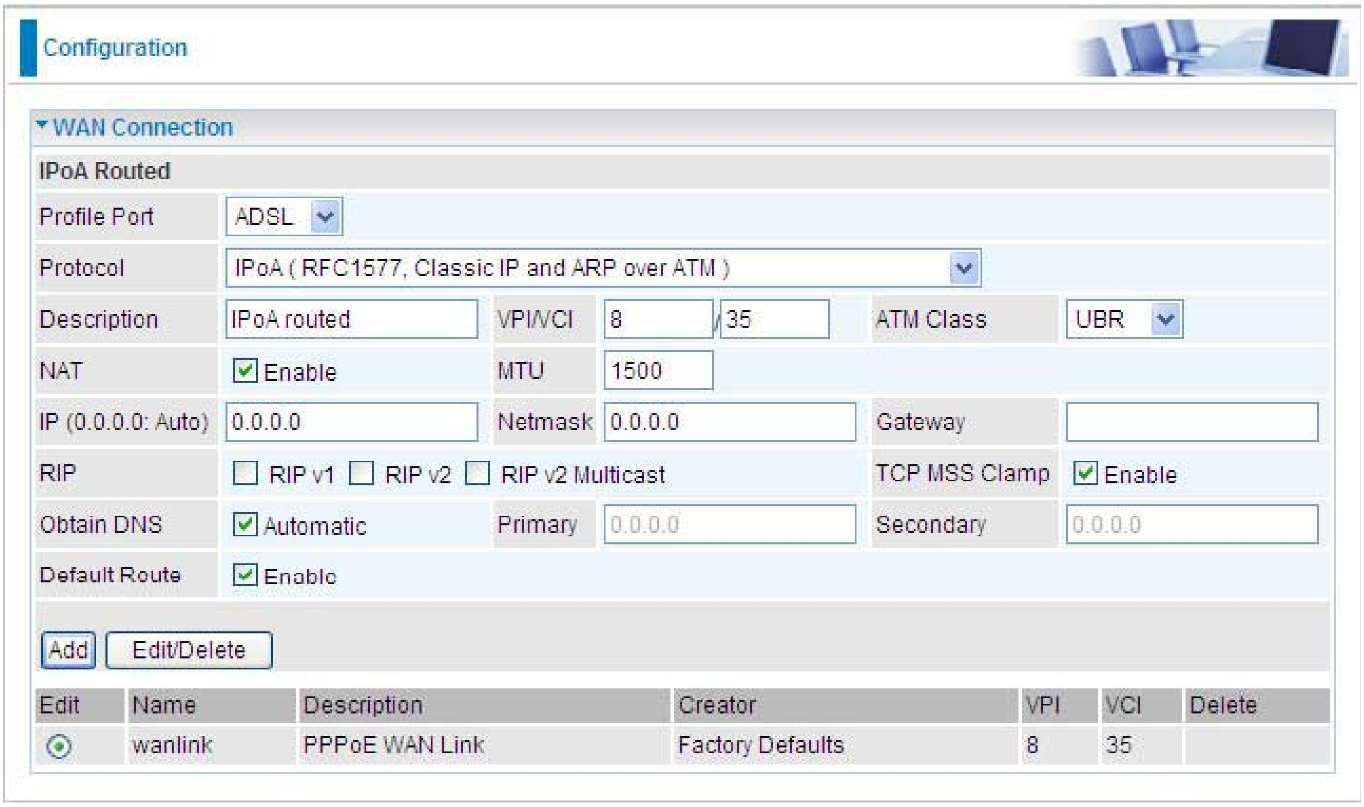
IPv6	☑ Enable				
IPv6 Address	☑ Automatic	IP/Prefix Length		Gateway	
Obtain IPv6 DNS	☑ Automatic	Primary		Secondary	

IPv6 Address: Check **Automatic** to obtain IPv6 address automatically. If not, please type the IP and the prefix length for the IPv6 address from your ISP.

Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary and Secondary fields.

IPoA Routed Connection



Configuration

▾ WAN 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
Default Route	☑ Enable				

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

Netmask: The default is 0.0.0.0. User can change it to other such as 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.

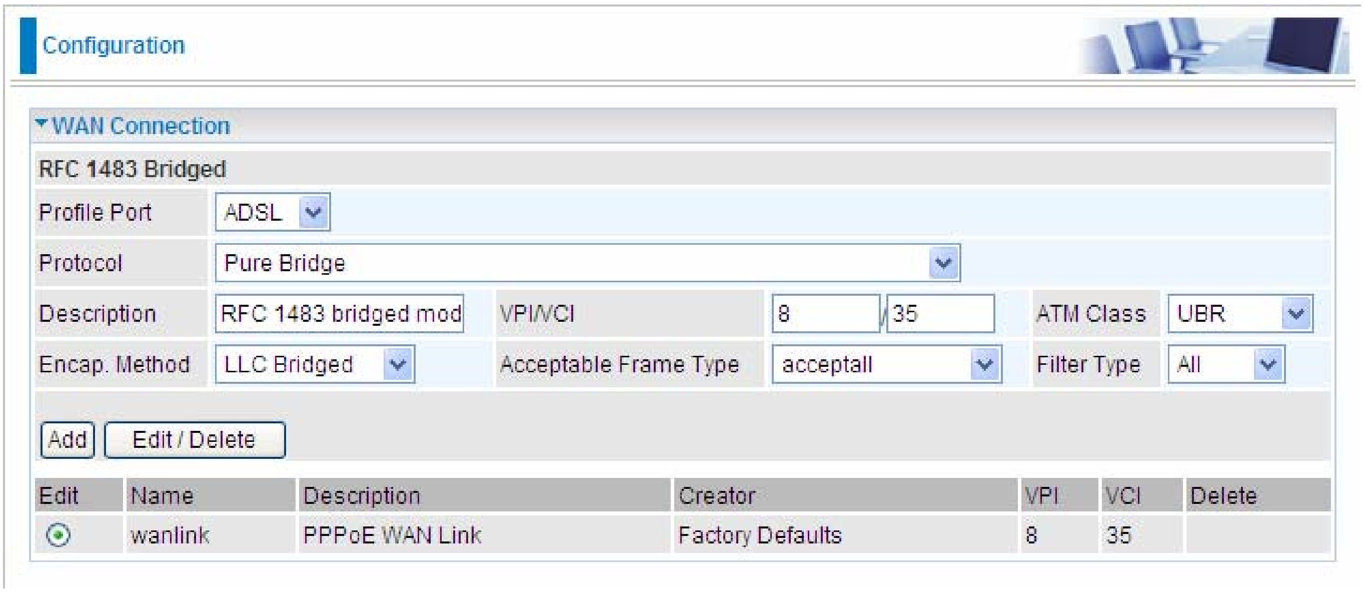
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Default Route: Check to enable default route.

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 either ADSL or 3G.

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. mode: Choose whether you want the packets in WAN interface as LLC bridged packet or VcMux bridged 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.

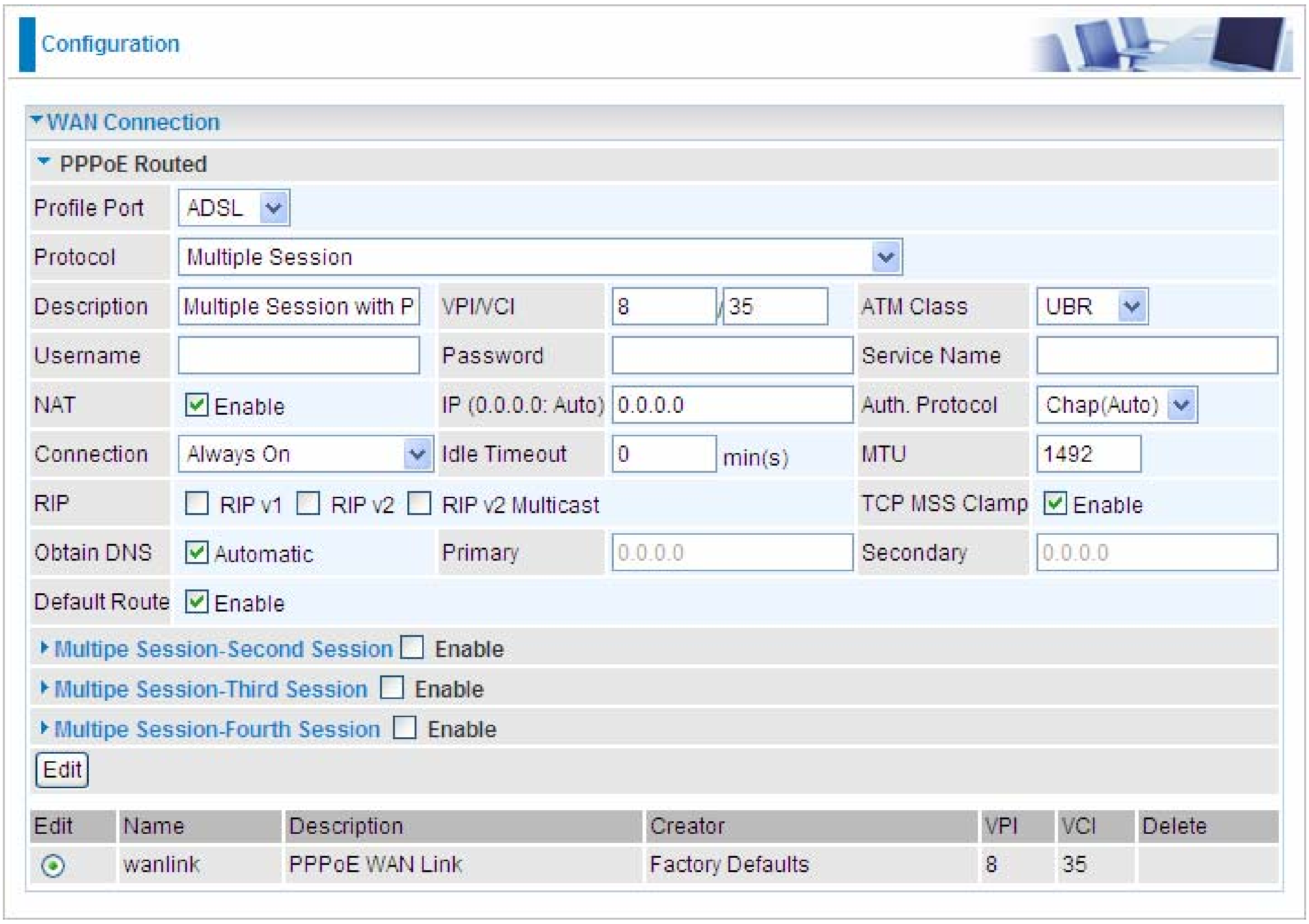
All	Allows all types of ethernet packets through the port.
Ip	Allows only IP/ARP types of ethernet packets through the port.
Pppoe	Allows only PPPoE types of ethernet packets through the port.

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.

Multiple Session



WAN Connection

PPPoE Routed

Profile Port	ADSL				
Protocol	Multiple Session				
Description	Multiple Session with P	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
Default Route	☑ Enable				

Multipe Session-Second Session □ Enable

Multipe Session-Third Session □ Enable

Multipe Session-Fourth Session □ Enable

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 Multiple Session 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.

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

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 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.

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.

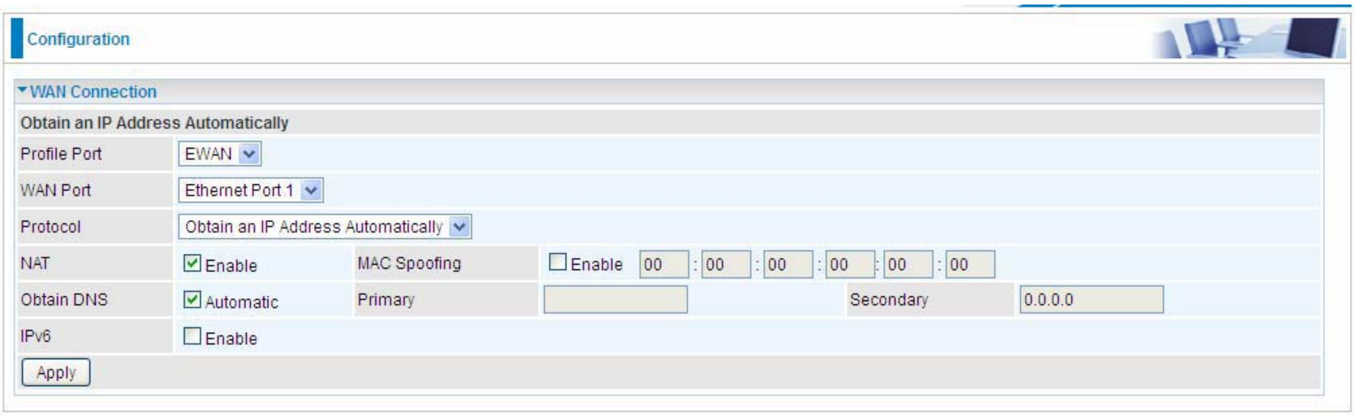
Default Route: Check to enable default route.

Multiple Session Second Session / Multiple Session Third Session / Multiple Session Forth Session: Check Enable to activate the second/third/forth session.

EWAN

Obtain an IP Address Automatically

When connecting to the ISP, This router also functions as a DHCP client. It can automatically obtain an IP address, netmask, gateway address, and DNS server addresses if the ISP assigns this information via DHCP.



Configuration

WAN Connection

Obtain an IP Address Automatically

Profile Port	EWAN				
WAN Port	Ethernet Port 1				
Protocol	Obtain an IP Address Automatically				
NAT	☑ Enable	MAC Spoofing	□ Enable 00 : 00 : 00 : 00 : 00 : 00		
Obtain DNS	☑ Automatic	Primary		Secondary	0.0.0.0
IPv6	□ Enable				

Apply

Profile Port: Select the profile port as EWAN.

WAN Port: the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems and fiber optic lines.

Protocol: Select **Obtain an IP Address Automatically**.

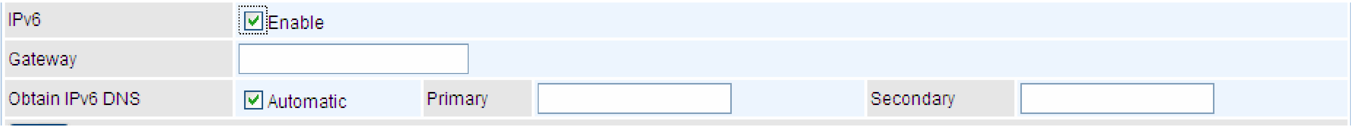
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If PCs in LAN should share the WAN IP for WAN access, please enable NAT. If users on your LAN have public IP addresses and can access the Internet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

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: Select Automatic to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers.

The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.



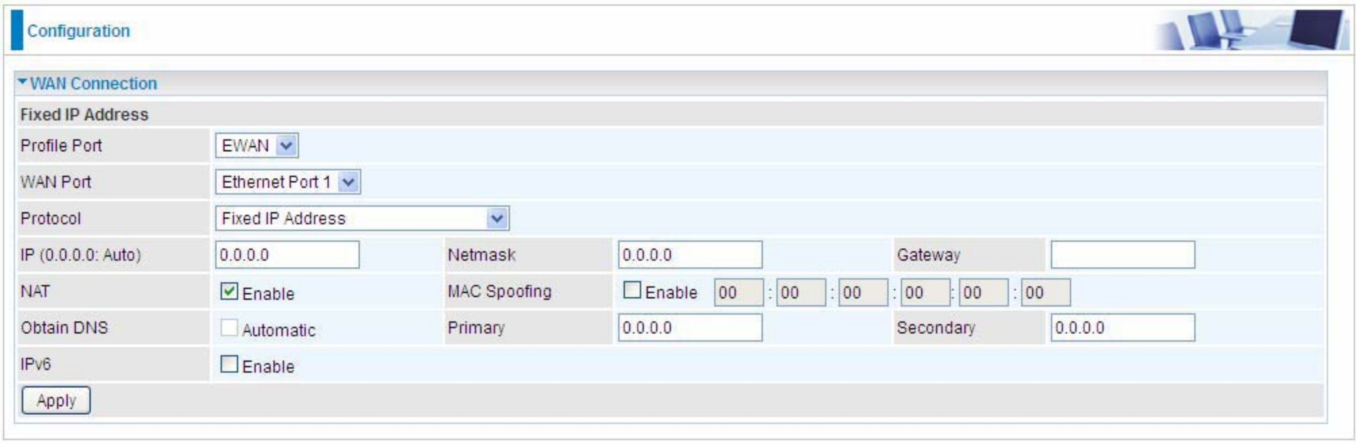
IPv6	☑ Enable				
Gateway					
Obtain IPv6 DNS	☑ Automatic	Primary		Secondary	

Gateway: type the gateway address to which WAN packets are forwarded.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically.   If not, please type the concrete ones in the Primary and Secondary fields.

Fixed IP Address

Select this option to set static IP information. You will need to enter in the Connection type, IP address, netmask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



Configuration

WAN Connection

Fixed IP Address

Profile Port	EWAN				
WAN Port	Ethernet Port 1				
Protocol	Fixed IP Address				
IP (0.0.0.0: Auto)	0.0.0.0	Netmask	0.0.0.0	Gateway	
NAT	☑ Enable	MAC Spoofing	□ Enable 00 : 00 : 00 : 00 : 00 : 00		
Obtain DNS	□ Automatic	Primary	0.0.0.0	Secondary	0.0.0.0
IPv6	□ Enable				

Profile Port: Select the profile port as EWAN.

WAN Port: the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems and fiber optic lines.

Protocol: Select **Fixed IP Address**.

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

Netmask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the netmask assigned to you by your ISP (if given).

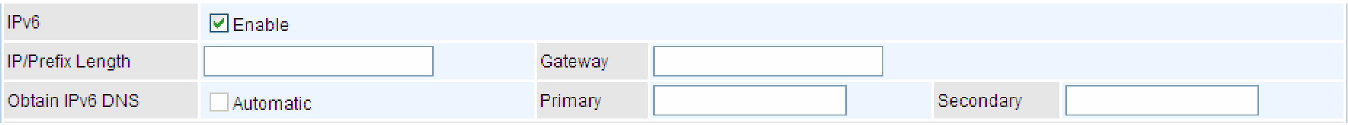
Gateway: You must specify a gateway IP address (supplied by your ISP).

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

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: Select Automatic to use DNS.
Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.



IPv6	☑ Enable				
IP/Prefix Length		Gateway			
Obtain IPv6 DNS	□ Automatic	Primary		Secondary	

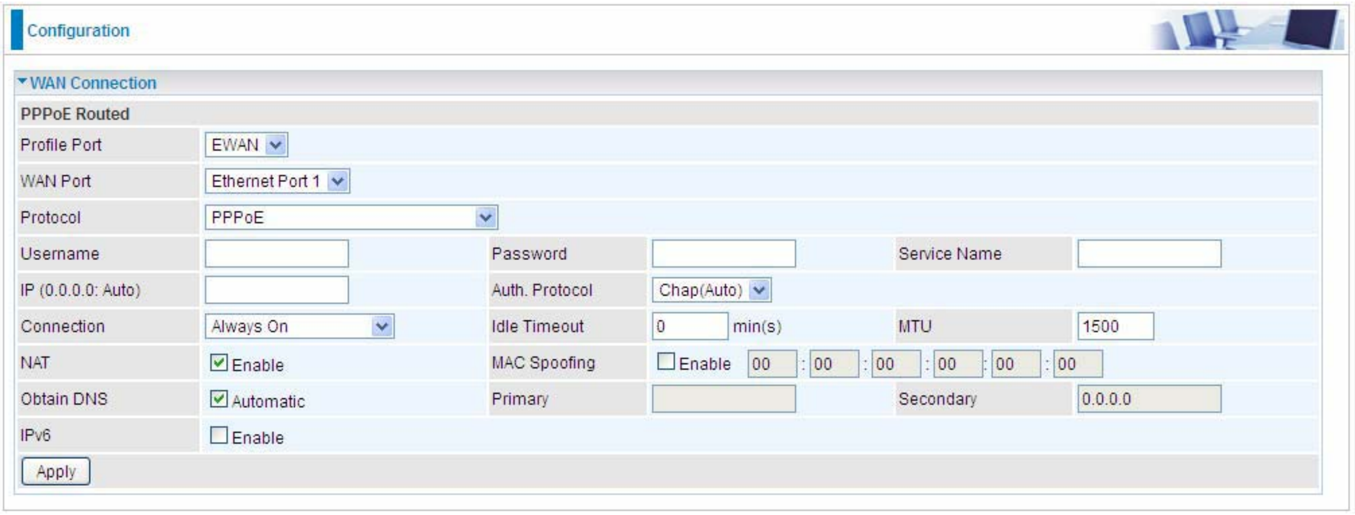
IP/Prefix Length: Please specify the IP and the prefix length for the IPv6 address from your ISP.

Gateway: Type the gateway to which the WAN packets are forwarded.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete ones in the Primary and Secondary fields.

PPPoE

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



Configuration

▾WAN Connection

PPPoE Routed

Profile Port	EWAN				
WAN Port	Ethernet Port 1				
Protocol	PPPoE				
Username		Password		Service Name	
IP (0.0.0.0: Auto)		Auth. Protocol	Chap(Auto)		
Connection	Always On	Idle Timeout	0 min(s)	MTU	1500
NAT	☑ Enable	MAC Spoofing	□ Enable 00 : 00 : 00 : 00 : 00 : 00		
Obtain DNS	☑ Automatic	Primary		Secondary	0.0.0.0
IPv6	□ Enable				

Apply

Profile Port: Select the profile port as EWAN.

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

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

Service Name: Enter a name for this connection.

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

Connection:

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

Connect on Demand: If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

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

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

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 PCs in LAN should share the WAN IP for WAN access, please enable NAT. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

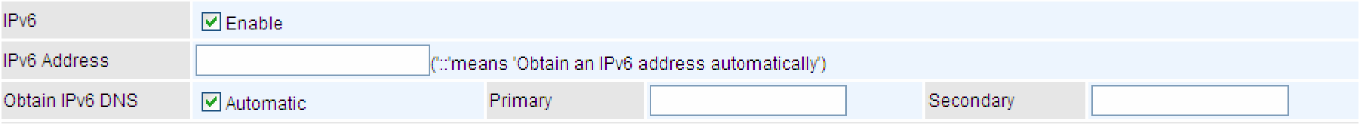
Auth. Protocol: Default is Auto. Your ISP advises on using Chap or Pap.

MAC Spoofing: Select Enable and enter a MAC address that will temporarily change your router’s MAC address to the one you have specified in this field. Leave it as Disabled if you do not wish to change the MAC address of your router.

Obtain DNS: Select Automatic to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask

IPv6: check to enable IPv6 service. Enter IPv6 Gateway address and set IPv6 DNS as same in IPv4 mode.

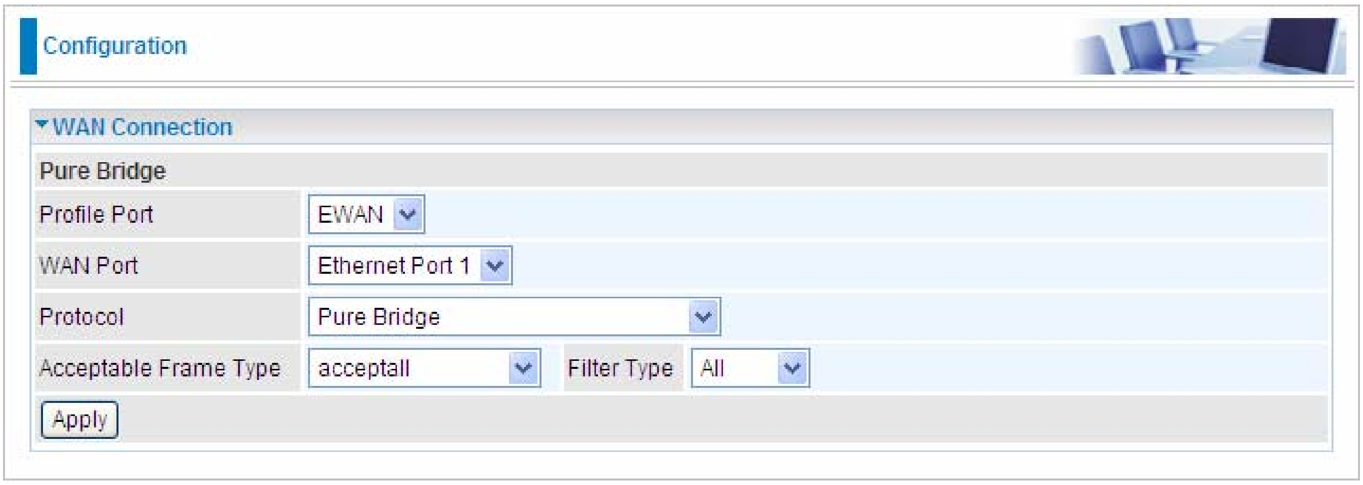


IPv6	☑ Enable				
IPv6 Address	('::'means 'Obtain an IPv6 address automatically')				
Obtain IPv6 DNS	☑ Automatic	Primary		Secondary	

IPv6 Address: type the IPv6 address from your ISP, or get it automatically. " ::" means to obtain IPv6 address automatically.

Obtain IPv6 DNS: check **Automatic** to obtain DNS automatically. If not, please type the concrete one in the Primary and Secondary fields.

Pure Bridge



Configuration

▾WAN Connection

Pure Bridge			
Profile Port	EWAN		
WAN Port	Ethernet Port 1		
Protocol	Pure Bridge		
Acceptable Frame Type	acceptall	Filter Type	All

Profile Port: Select the profile port as EWAN.

Protocol: Select **Pure Bridge**.

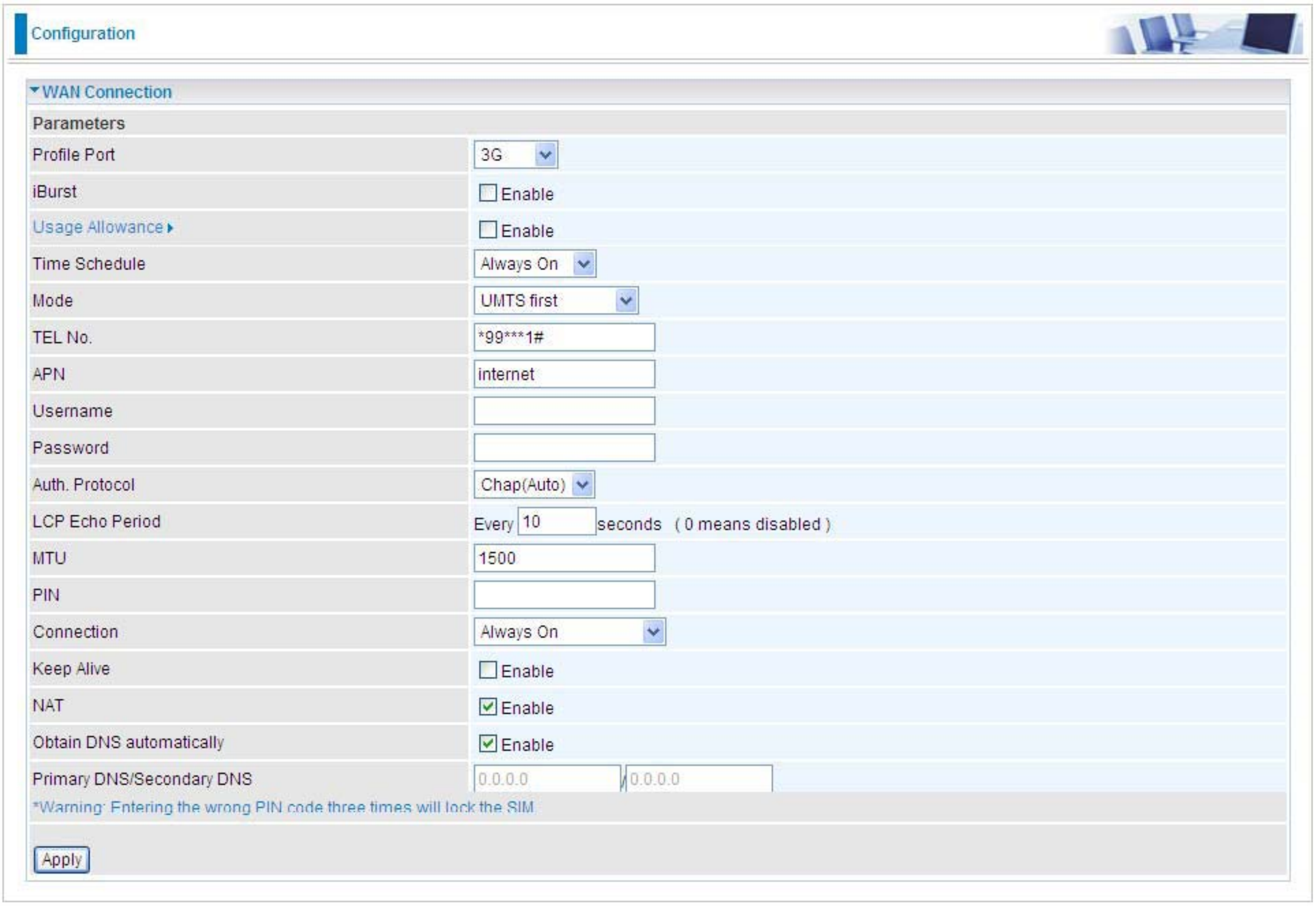
Acceptable Frame Type: Specify which kind of traffic goes through this connection, all traffic or only VLAN tagged.

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.

3G

The router allows you to insert a 3G/HSDPA card to its USB slot, enabling you to use a 3G/HSDPA, UMTS, EDGE, GPRS, or GSM Internet connection, makes downstream rates of to 14.4 Mbps*.



Configuration

▾WAN Connection

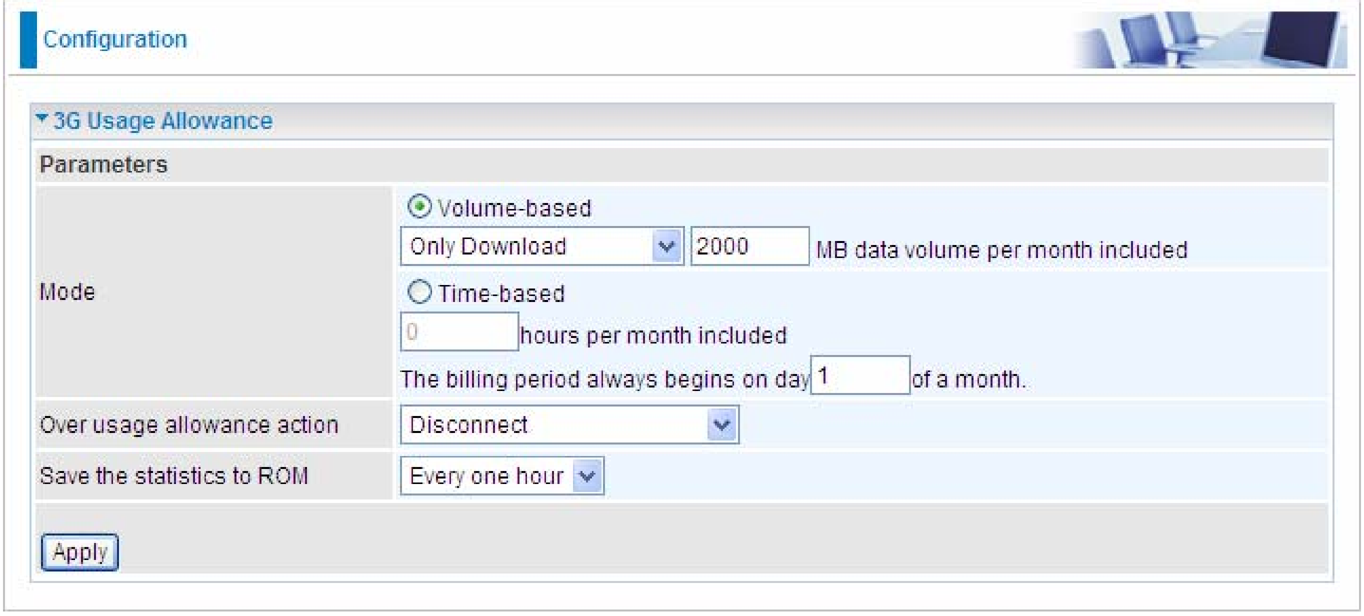
Parameters	
Profile Port	3G
iBurst	□ Enable
Usage Allowance ▸	□ Enable
Time Schedule	Always On
Mode	UMTS first
TEL No.	*99***1#
APN	internet
Username	
Password	
Auth. Protocol	Chap(Auto)
LCP Echo Period	Every 10 seconds (0 means disabled)
MTU	1500
PIN	
Connection	Always On
Keep Alive	□ Enable
NAT	☑ Enable
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

*Warning: Entering the wrong PIN code three times will lock the SIM.

Profile Port: Select the profile port as 3G.

iBurst: Enable or Disable the router's iBurst functionality.

Usage Allowance: Check to enable usage allowance function.
Click Usage Allowance ▸ to continue the detailed configuration.



Configuration

▾3G Usage Allowance

Parameters	
Mode	● Volume-based Only Download 2000 MB data volume per month included ○ Time-based 0 hours per month included The billing period always begins on day 1 of a month.
Over usage allowance action	Disconnect
Save the statistics to ROM	Every one hour

In order to query online time or volume used, you can set the following options.

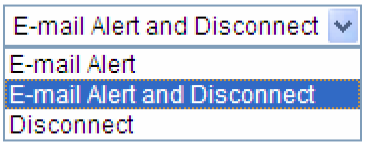
Mode: Two methods are provided, that is, **Volume-based** and **Time-based**.

Volume-based: The volume amount you can use per month.

Only Download: Only make statistics of Download Traffic.
Only Upload: Only make statistics of Upload Traffic.
Download and Upload: Make statistics of both Download and Upload Traffic.

Time-based: The hours you can use per month.

Over usage allowance action: If the online time or traffic you have used exceeds the usage allowance you set. The system will do the followings operations.



Save the statistics to ROM: Choose the time interval for saving statistics. You can choose to save for **Every one hour** or **Disable** the function**.**
Time Schedule: Specify time duration for your 3G WAN connection.
Mode: select your wanted mode of 3G operation from the drop-down menu.

TEL No.: The dial string to make a GPRS / 3G user internetworking call. It may be provided by your mobile service provider.

APN: An APN is similar to a URL on the WWW, it is what the unit makes a GPRS / UMTS call. The service provider is able to attach anything to an APN to create a data connection. Requirements for APN assignment varies between different service providers. Most service providers have an internet portal which they connect a DHCP Server to, giving you access to the internet i.e. Some 3G operators use the APN 'internet' for their portal. The default value of APN is "internet".

Username: Enter the username provided by your service provider.

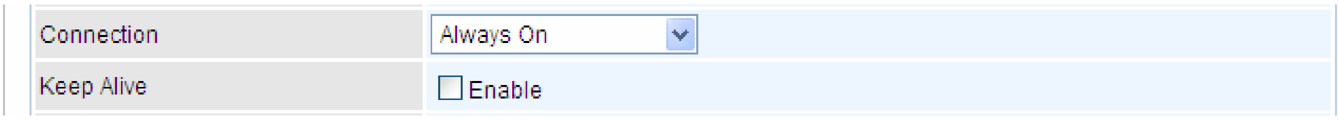
Password: Enter the password provided by your service provider.

Auth. Protocol: Manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which authentication type the server is using (when acting as a client), or the authentication type you want the clients to use when they are connecting to you (when acting as a server). When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

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

PIN: PIN stands for Personal Identification Number. A PIN code is a numeric value used in certain systems as a password to gain access, and authentication. In mobile phones a PIN code locks the SIM card until you enter the correct code. If you enter the PIN code incorrectly into the phone 3 times in a row, then the SIM card will be blocked and a PUK code will be required from your network / service provider to unlock it.

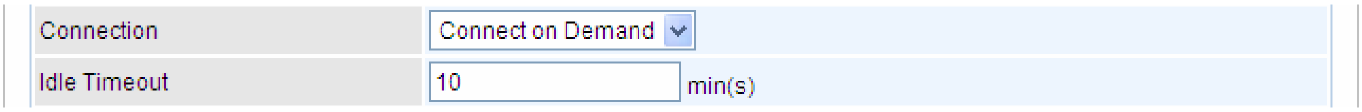
Connection:



Connection	Always On
Keep Alive	☐ Enable

Always On: The router will make UMTS/GPRS call when starting up. Enabling Always On, will give you an option of Keep Alive.

Keep Alive: Set Enable to keep the router on line and prevent to be disconnected by the ISP when they think there is no activity on the line.



Connection	Connect on Demand
Idle Timeout	10 min(s)

Connect to Demand: If you want to make UMTS/GPRS call only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet). In this mode, you must set Idle Timeout value at same time. Enabling Connect on Demand will give you an option of Idle Timeout.

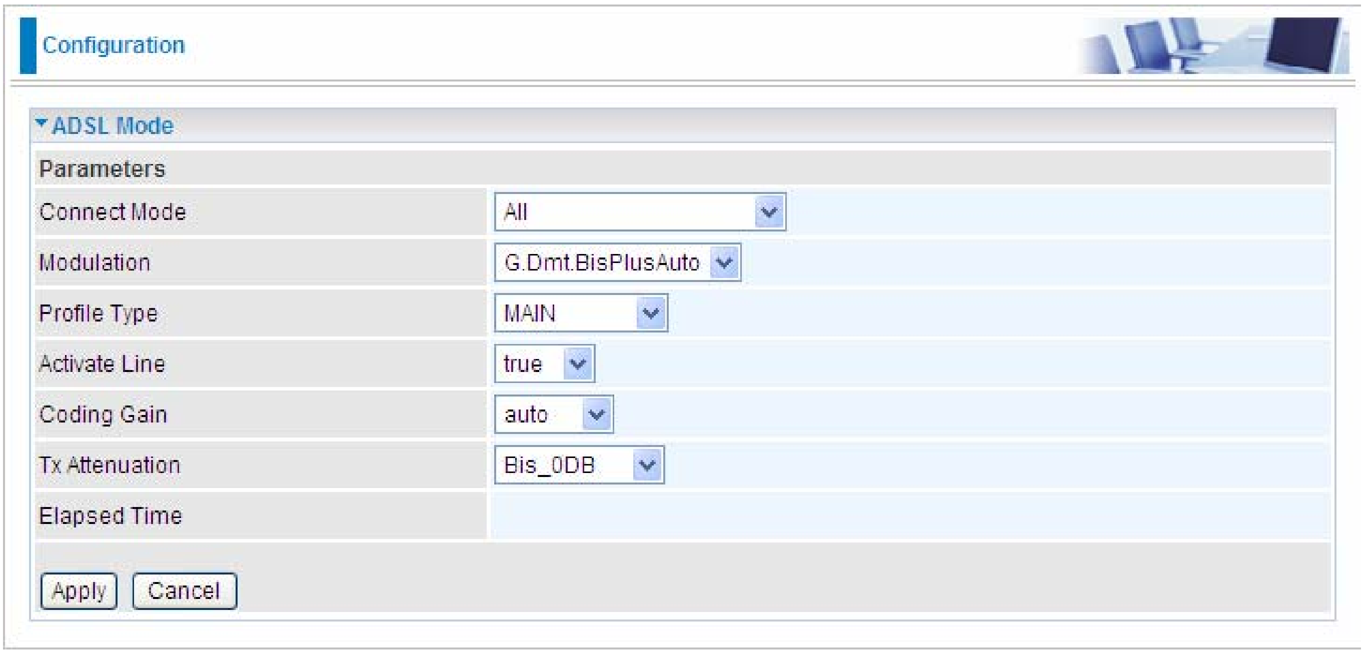
Idle Timeout: Auto-disconnect the connection when there is no activity on this call for a predetermined period of time. The default value is 10 min(s).

Obtain DNS Automatically: Select this checkbox to use DNS.

Primary DNS/ Secondary DNS: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Note: If you don't know how to set these values and please keep them untouched.

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	

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.

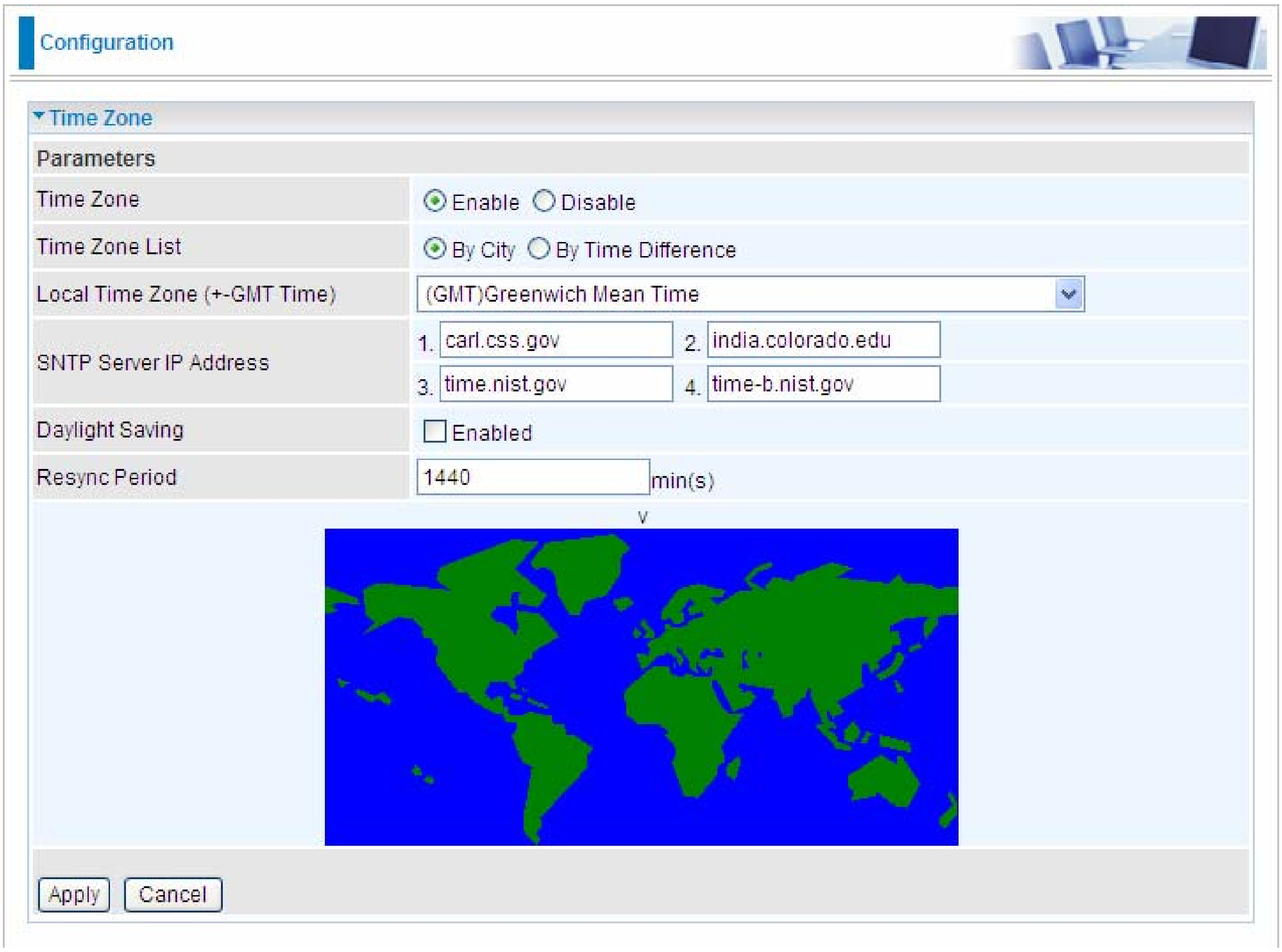
Activate Line: Aborting (false) your ADSL line and making it active (true) again for taking effect with setting of **Connect Mode**.

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.

System

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

Time Zone



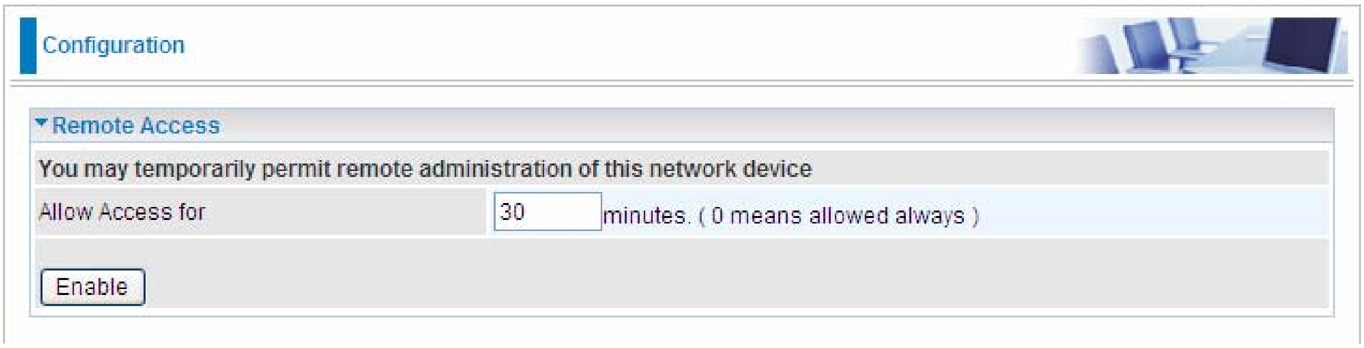
Parameters	
Time Zone	● Enable ○ Disable
Time Zone List	● By City ○ By Time Difference
Local Time Zone (+-GMT Time)	(GMT)Greenwich Mean Time
SNTP Server IP Address	1. carl.css.gov 2. india.colorado.edu 3. time.nist.gov 4. time-b.nist.gov
Daylight Saving	□ Enabled
Resync Period	1440 min(s)

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 **Automatic** box to auto 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



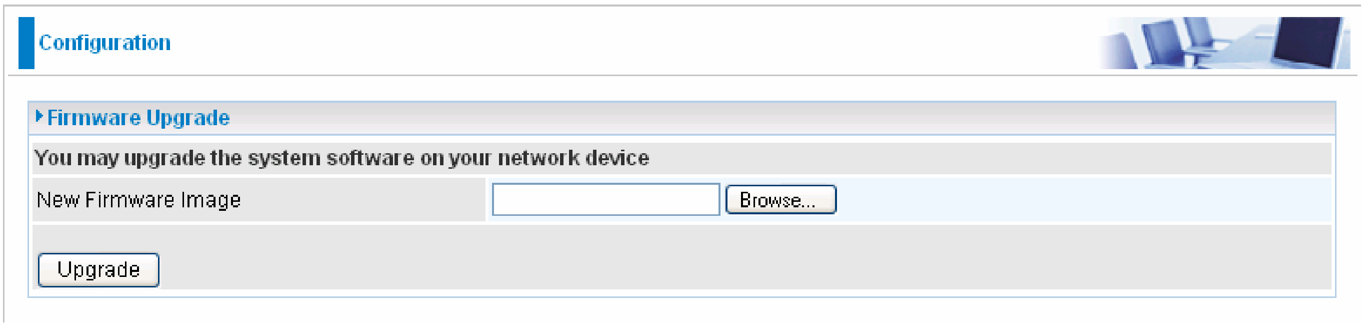
You may temporarily permit remote administration of this network device

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

To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router will permit remote access for and click **Enable.** You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

If you wish to permanently enable remote access, choose a time period of **0** minute.

Firmware Upgrade



You may upgrade the system software on your network device

New Firmware Image

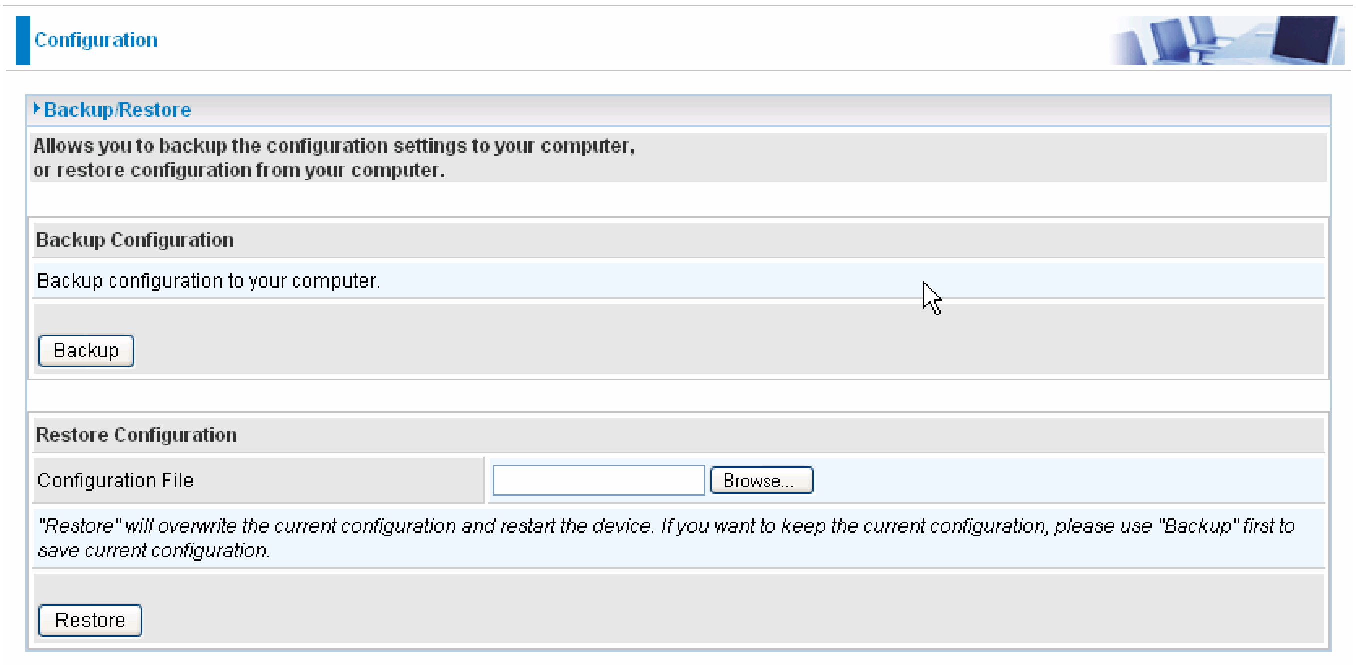
Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs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

Don't power down the router or interrupt the firmware while it is still in process.Improper opteration could damage the router.

Warning

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.

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

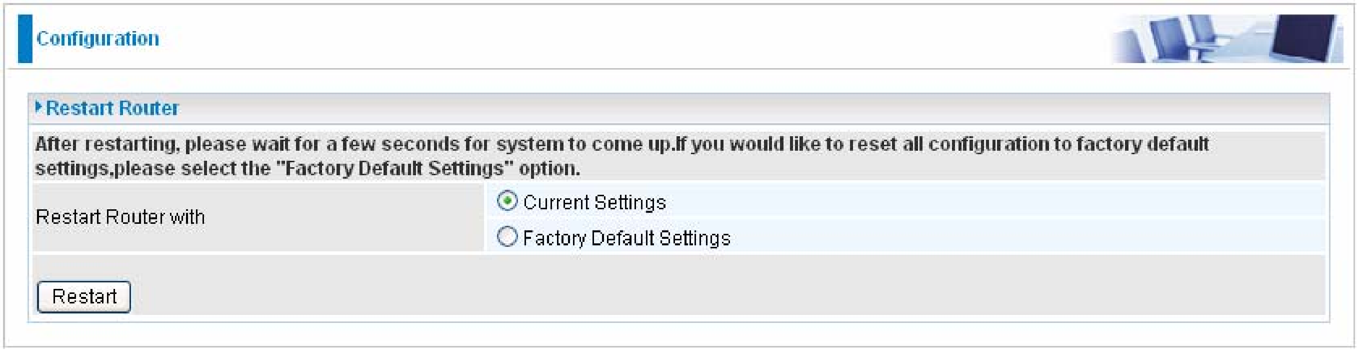
Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

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

After selecting the settings file you wish to use, pressing **Restore** will load those settings into the router.

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.

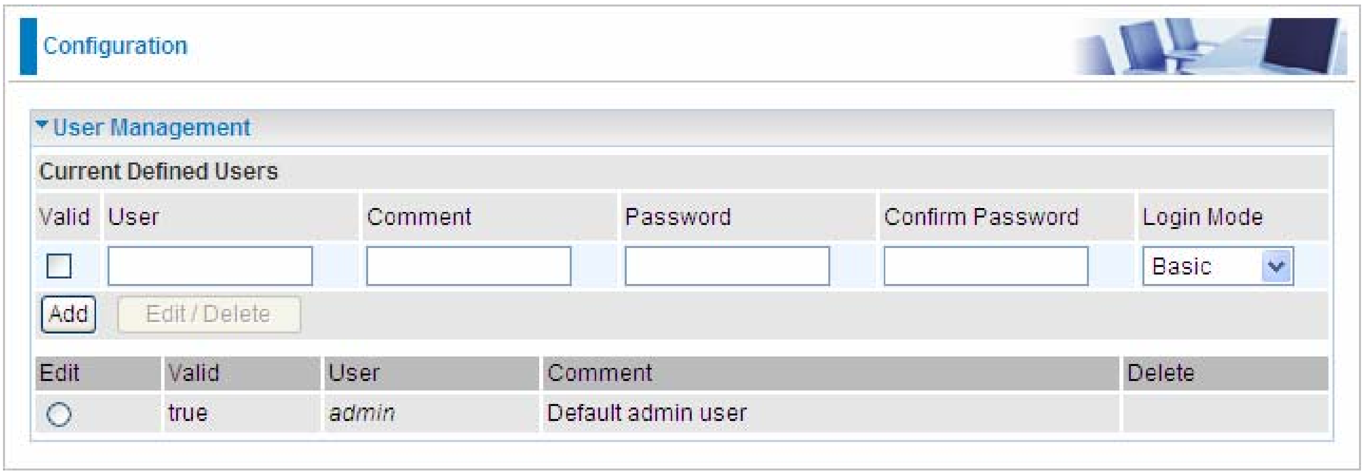
Restart Router with	● Current Settings ○ Factory Default Settings

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



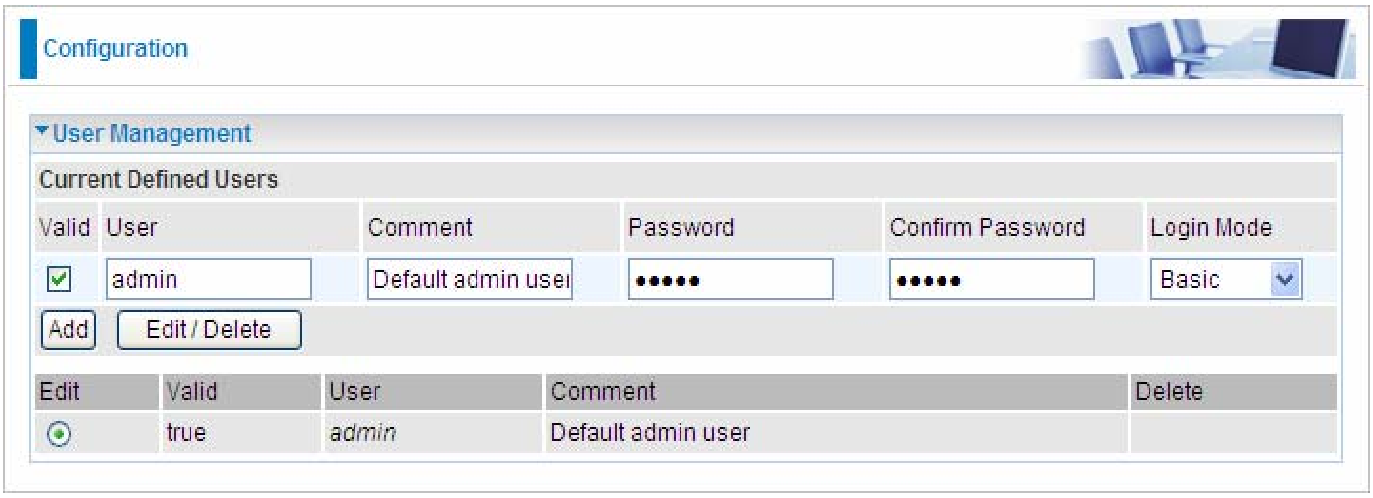
Current Defined Users

Valid	User	Comment	Password	Confirm Password	Login Mode
□					Basic

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

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

You are able to **Edit** existing users and **Add** new users who are able to access the device's configuration interface. Once you have clicked on **Edit,** you are shown the following options:

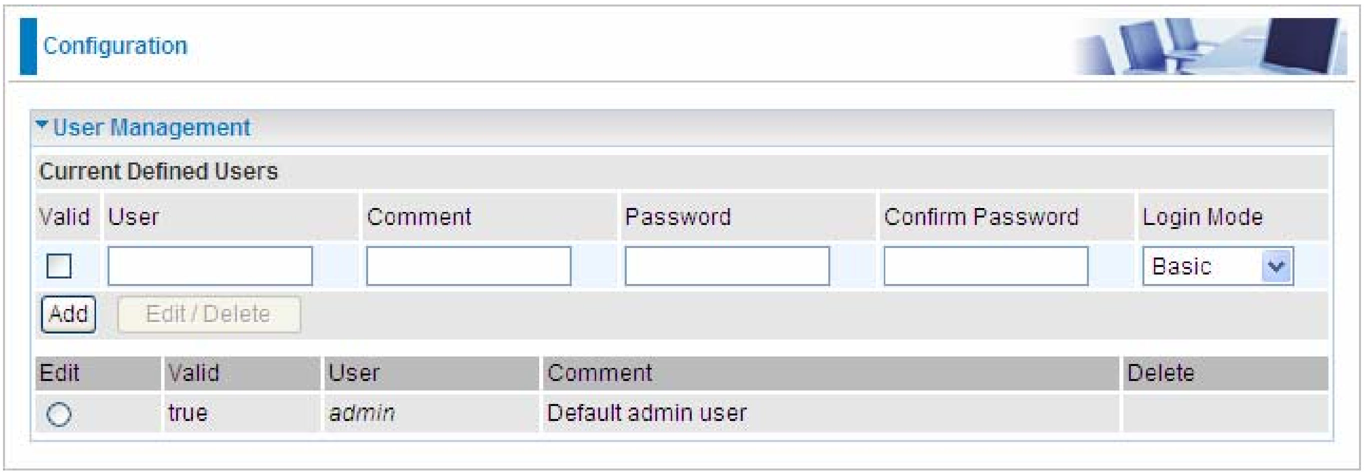


Current Defined Users

Valid	User	Comment	Password	Confirm Password	Login Mode
☑	admin	Default admin usei	•••••	•••••	Basic

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

You can change the user's **password**, whether their account is active and **valid**, as well as add a comment to each user account. Click Edit/Delete button to save your revise. You cannot delete the default admin account, if you do you will be log out. However, you can delete any other created accounts by clicking **Delete** when editing the user. You are strongly advised to change the password on the default "**admin**" account when you receive your router, and any time you reset your configuration to Factory Defaults.

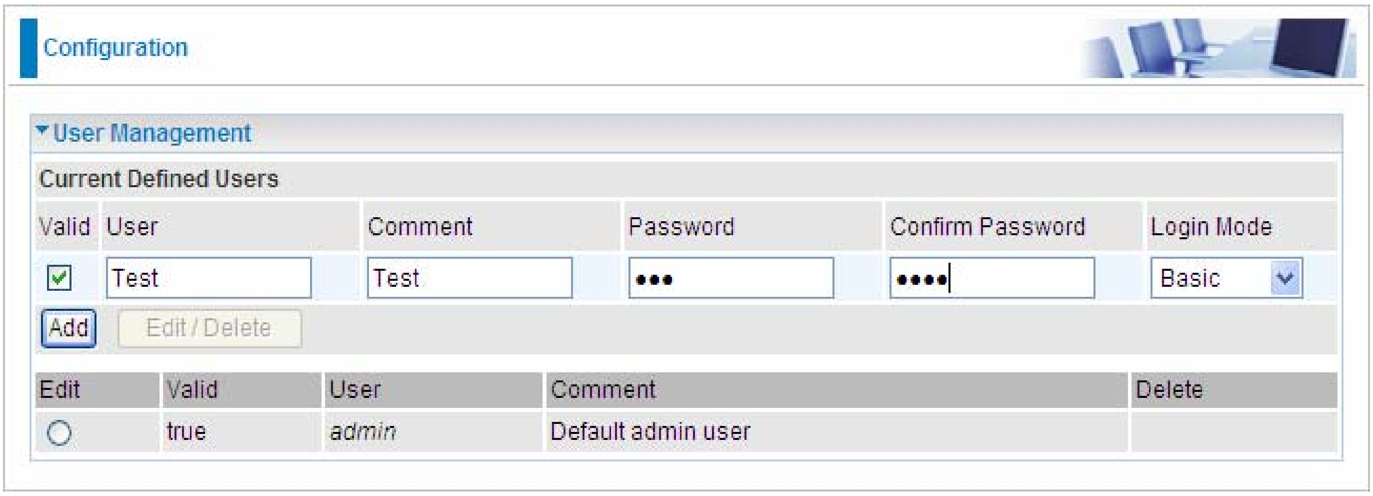


Current Defined Users

Valid	User	Comment	Password	Confirm Password	Login Mode
□					Basic

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

When you create a user account, you check Valid to fill in the blank with User, Comment, Password and Confirm Password. Later, click **Add** button to add your new user account.



Configuration

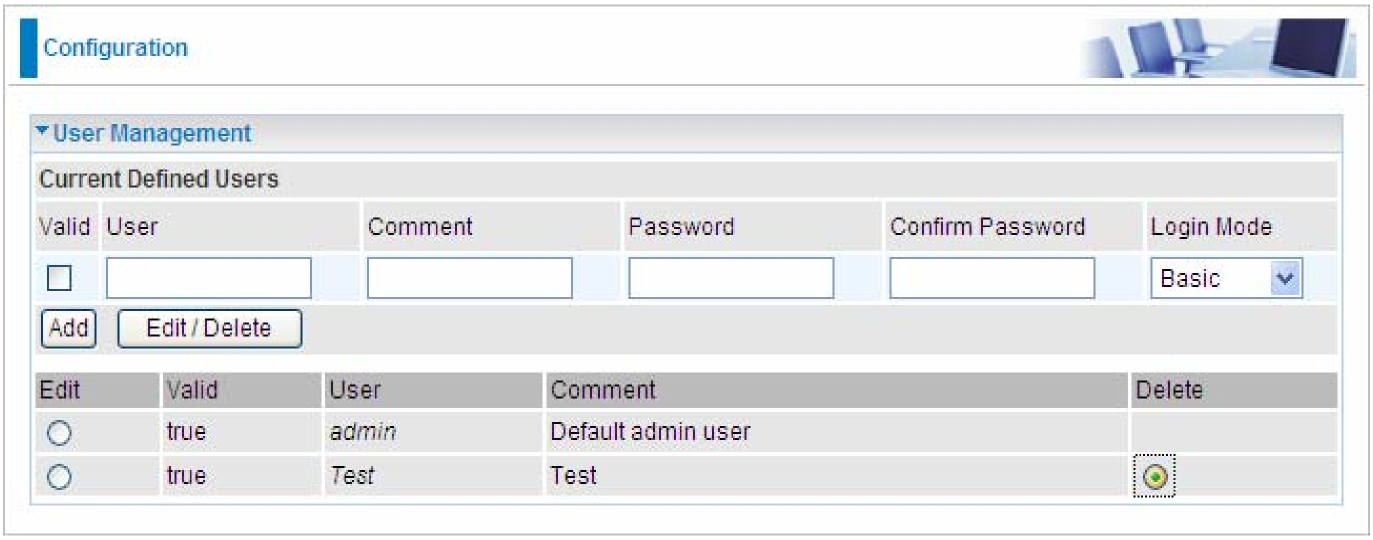
User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password	Login Mode
☑	Test	Test	•••	••••	Basic

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

For deleting the user account, you choose Delete option. In the end, you click **Edit/Delete** button to delete the chosen user account.



Configuration

User Management

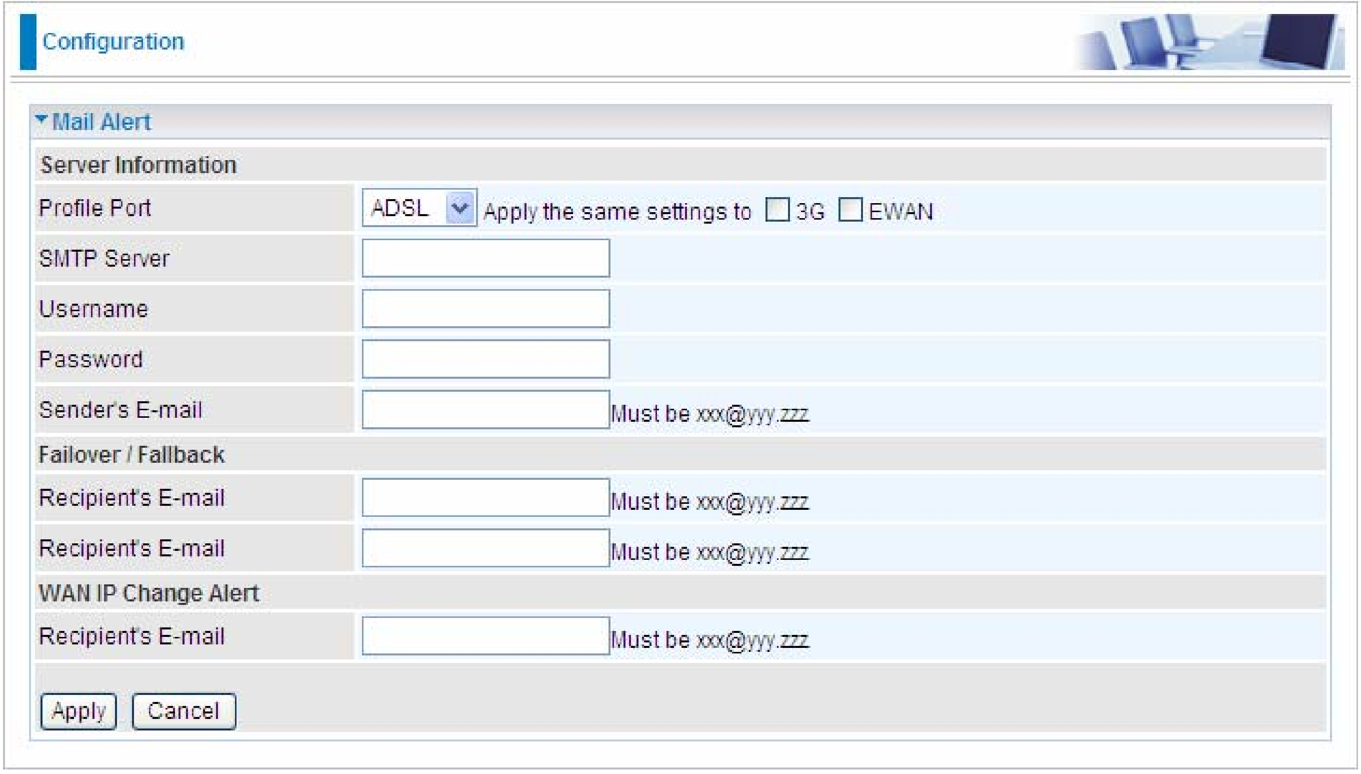
Current Defined Users

Valid	User	Comment	Password	Confirm Password	Login Mode
□					Basic

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

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnels alerted of any unexpected events that might have occured to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



Server Information	
Profile Port	ADSL ▾ Apply the same settings to □ 3G □ EWAN
SMTP Server	
Username	
Password	
Sender's E-mail	Must be xxx@yyy.zzz
Failover / Fallback	
Recipient's E-mail	Must be xxx@yyy.zzz
Recipient's E-mail	Must be xxx@yyy.zzz
WAN IP Change Alert	
Recipient's E-mail	Must be xxx@yyy.zzz

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

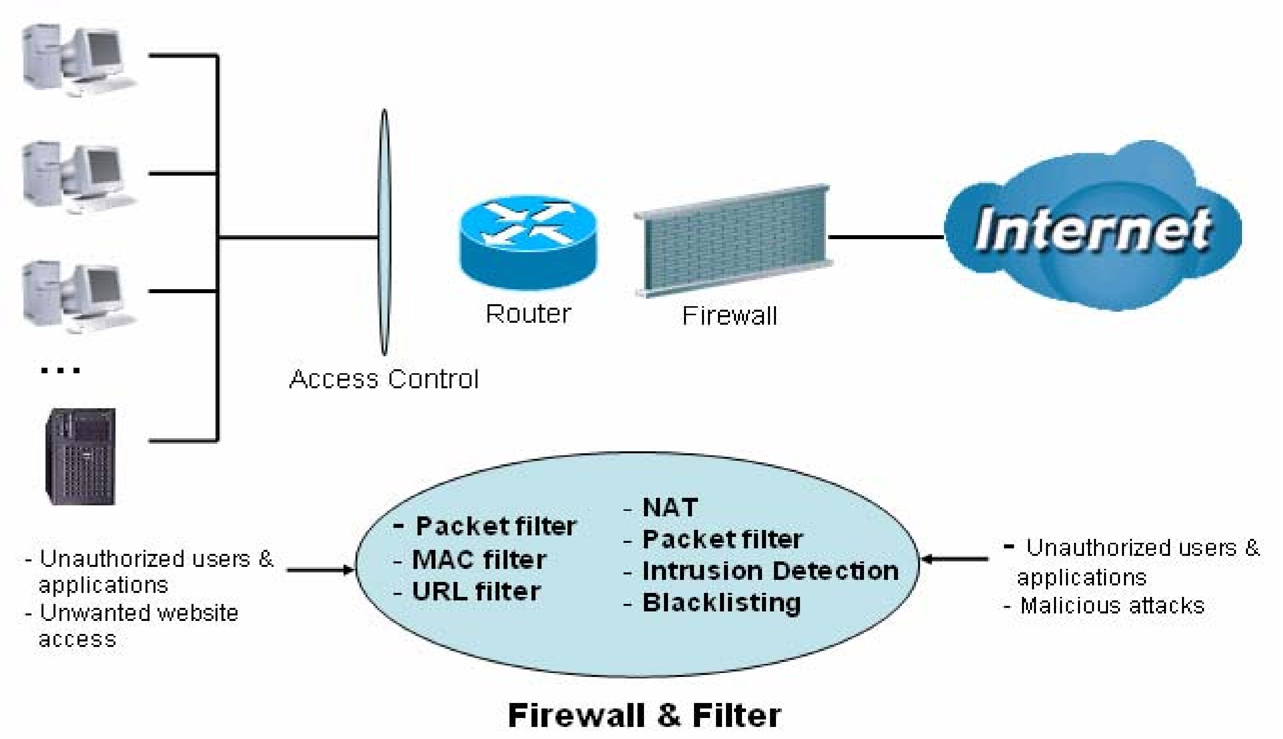
Sender's Email: Enter your email address.

Recipient's Email (Failover / Failback): Enter the email address that will receive the alert message once a computer / network server failover occurs.

Recipient's Email (WAN IP Change Alert): Enter the email address that will receive the alert message once an WAN IP change has been detected.

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. Besides, when using NAT, the router acts as a "natural" Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.



Firewall: Prevents access from outside your network. The router provides three levels of security support:

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

NOTE:

When using Virtual Servers your PCs will be exposed to the degree specified in your Virtual Server settings provided the ports specified are opened in your firewall packet filter settings.

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

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

Access Control: Prevents 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 accessing the Internet.

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

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

General Settings

You can choose not to enable Firewall and still able to access to URL Filter, Intrusion Detection and IM/P2P Blocking or enable the Firewall using 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.

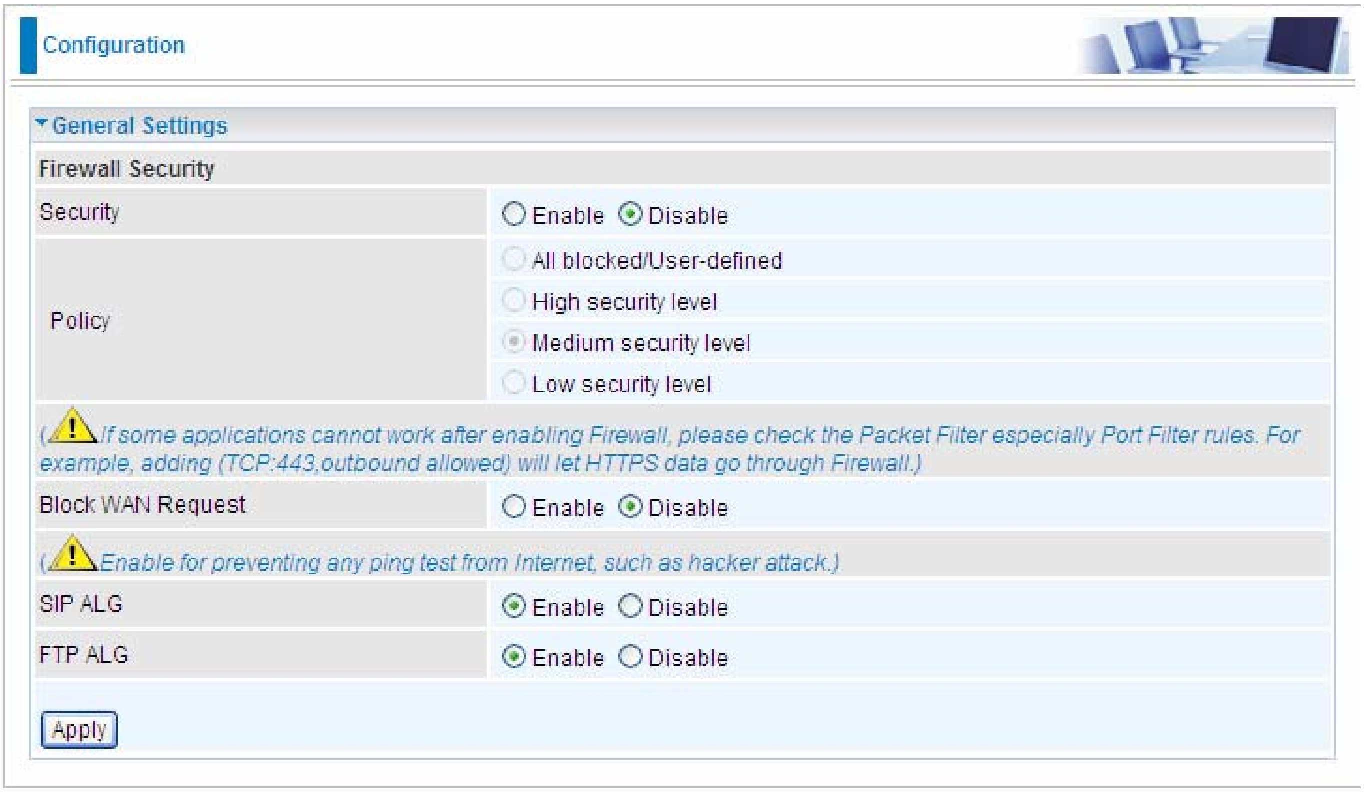
There are four options when you enable the Firewall, they are:

- ⊙ **All blocked/User-defined**: no pre-defined 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 for further access to the Internet.
- ⊙ **High/Medium/Low security level:** the predefined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

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

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

The "**Block WAN Request**" is a stand-alone function and not relate to whether security enable or disable. Mostly it is for preventing any scan tools from WAN site by hacker.



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.)

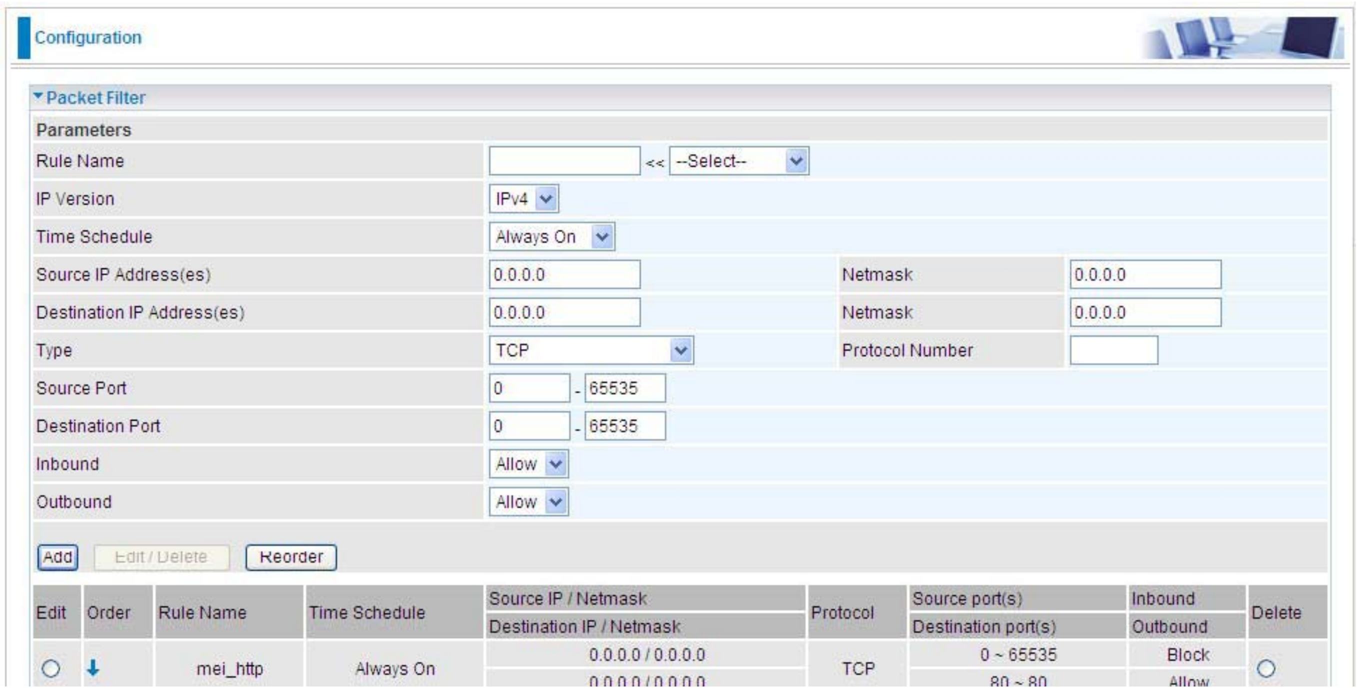
SIP ALG	● Enable ○ Disable
FTP ALG	● Enable ○ Disable

NOTE:

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

Packet Filter

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



Configuration

▾ Packet Filter

Parameters			
Rule Name	<< --Select--		
IP Version	IPv4		
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	Order	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	○

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.

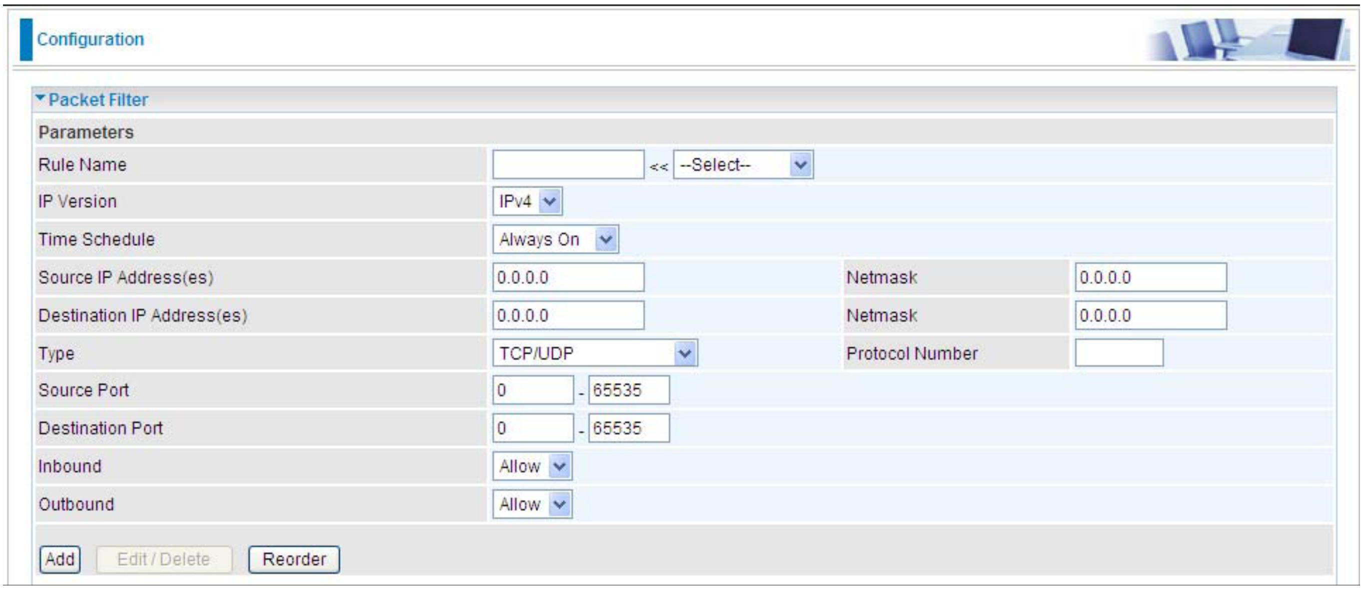
Table 1: Predefined Port Filter

Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	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
SMTP(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) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	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 (9000)	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



Configuration

Packet Filter

Parameters

Rule Name	<< --Select--		
IP Version	IPv4		
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	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Rule Name: Users-define description to identify this entry or click "**Select" drop-down menu** to select existing predefined rules. The maximum name length is 32 characters.

IP version: select IPv4 or IPv6.

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

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). Selecting 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".

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.

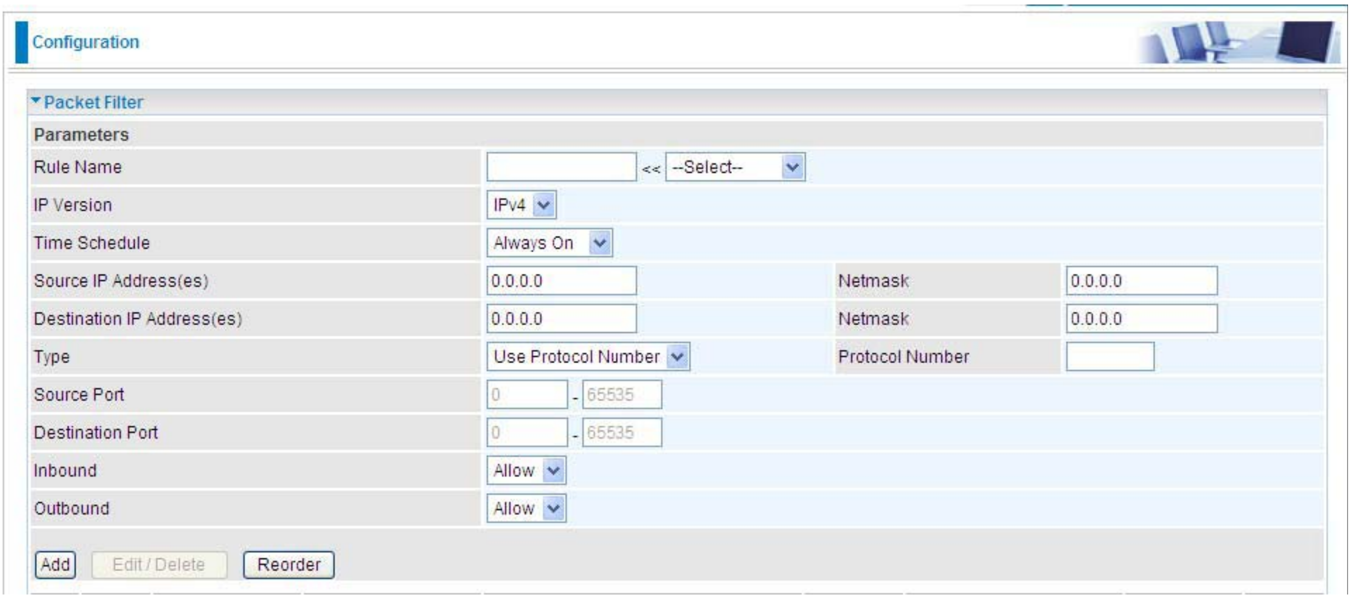
Type: It is the packet protocol type used by the application, select **TCP**, **UDP** or both **TCP/UDP**. **Protocol Number:** Insert the port number.

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

Click **Add** button to apply your changes.

Packet Filter – Add Raw IP Filter

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



Parameters			
Rule Name	<< --Select--		
IP Version	IPv4		
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	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Rule Name Helper: Users-define description to identify this entry or choosing “Select” drop-down menu to select existing predefined rules.

IP version: select IPv4 or IPv6.

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

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

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

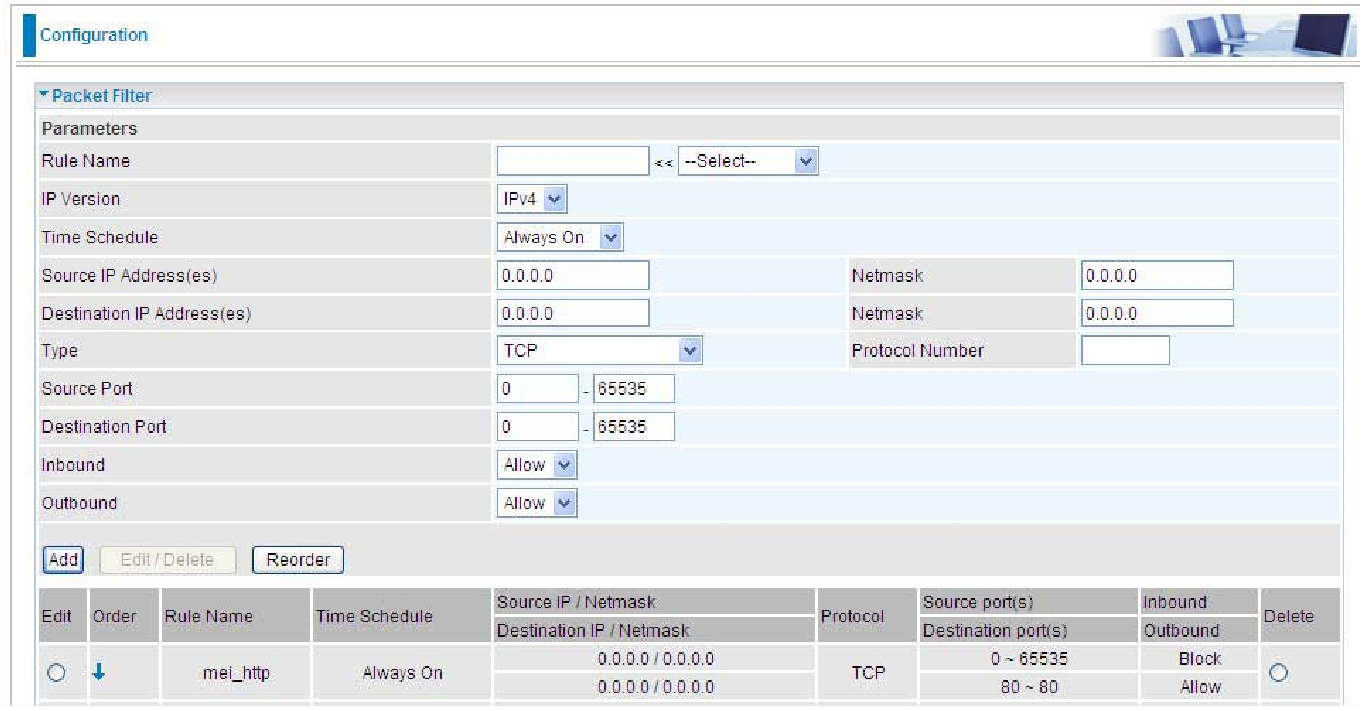
Click **Add** button to apply your changes.

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 no matter 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), inbound HTTP access is not allowed which means remote access through HTTP to your router is not allowed.

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



Configuration

Packet Filter

Parameters

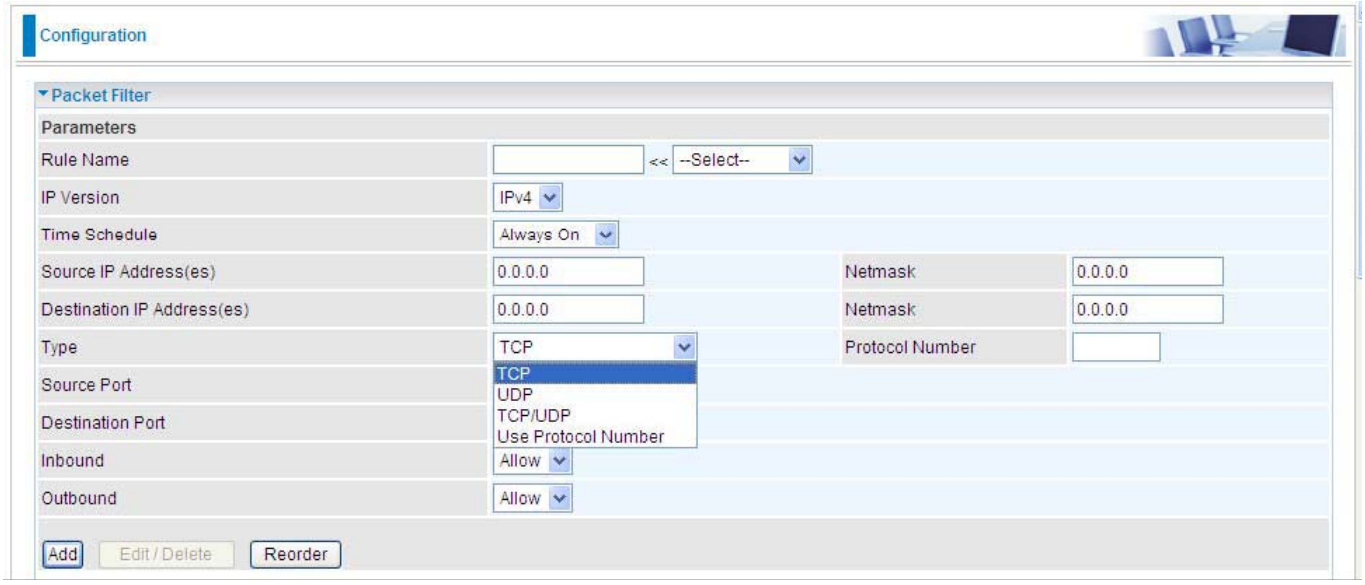
Rule Name	<< --Select--		
IP Version	IPv4		
Time Schedule	Always On		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP	Protocol Number	
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow		
Outbound	Allow		

Edit	Order	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	○

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.

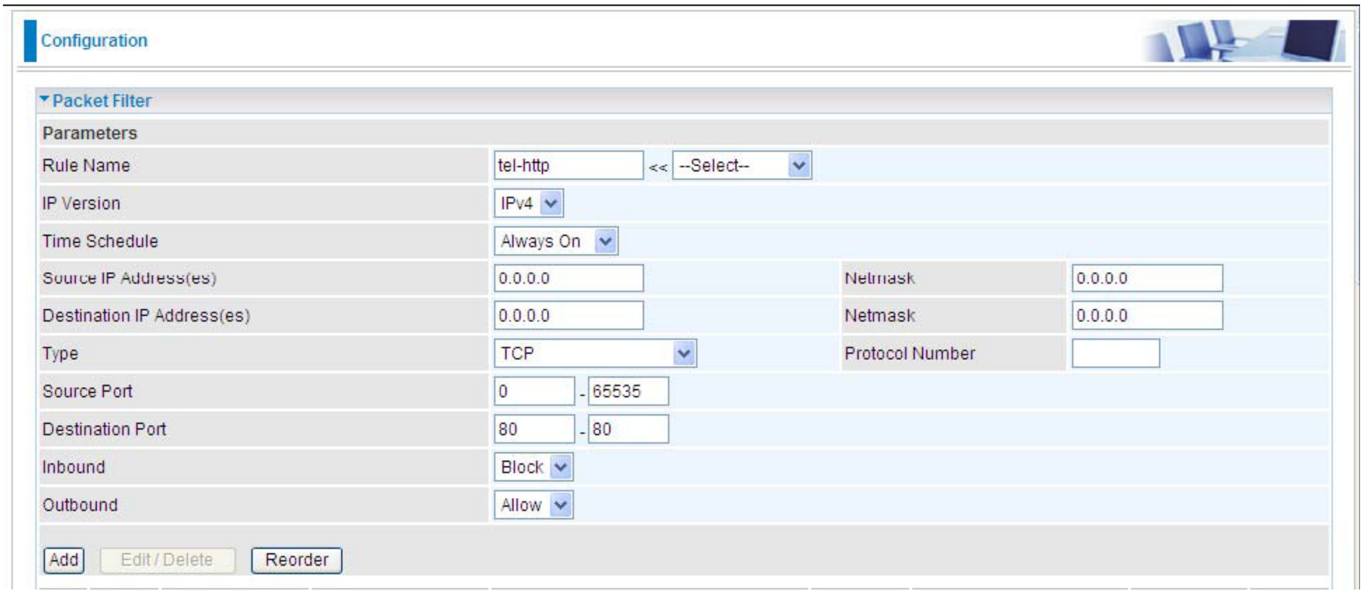


Configuration

▾Packet Filter

Parameters			
Rule Name	<< --Select--		
IP Version	IPv4		
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. Choose the radio button you want to delete the existing HTTP rule. Click **Edit/Delete** button to delete the existing HTTP rule.



Configuration

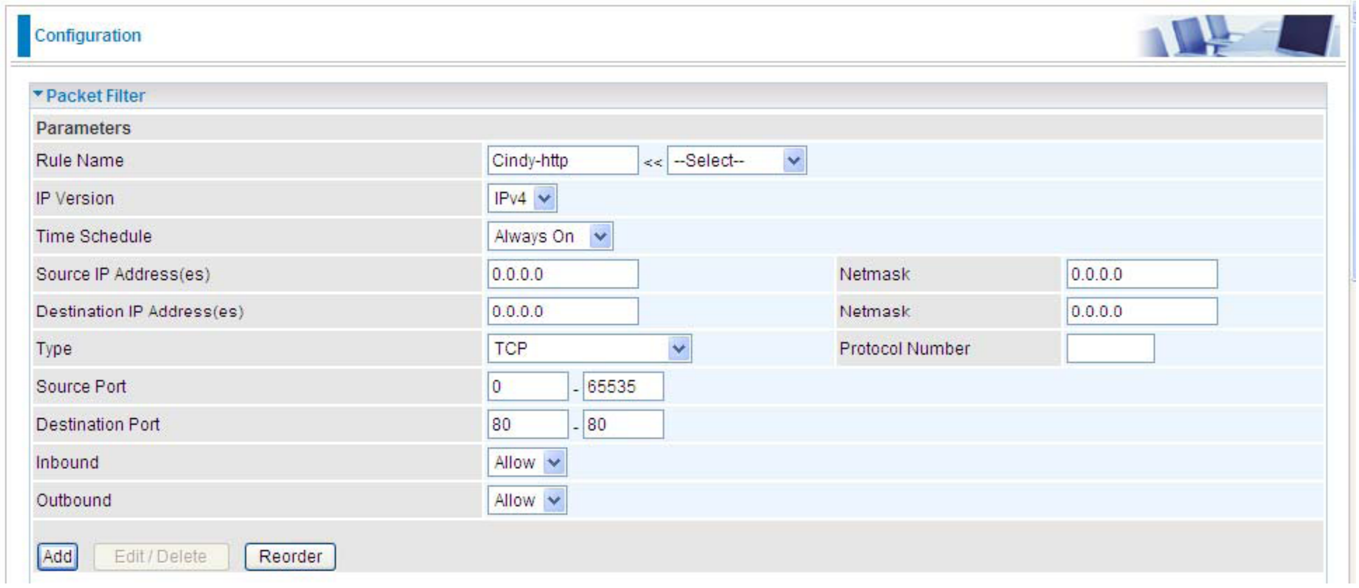
▾Packet Filter

Parameters			
Rule Name	tel-http << --Select--		
IP Version	IPv4		
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	80 - 80		
Inbound	Block		
Outbound	Allow		

3. Input the Rule Name, Time Schedule, Source/Destination IP, Type, Source/Destination Port, Inbound and Outbound.

Example:

Application: *Cindy_HTTP*
Time Schedule: *Always On*
Source / Destination IP Address(es): *0.0.0.0* ***(I do not wish to active the address-filter, instead I use the port-filter)***
Type: *TCP (Please refer to Table1: Predefined Port Filter)*
Source Port: *0-65535* ***(I allow all ports to connect with the application))***
Redirect Port: *80-80* ***(This is Port defined for HTTP)***
Inbound / Outbound: *Allow*

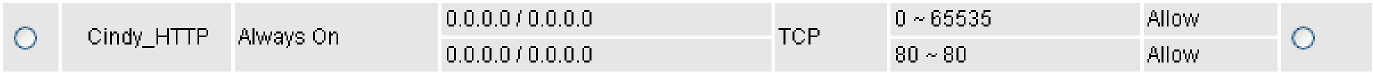


Configuration

Packet Filter

Parameters			
Rule Name	Cindy-http << --Select--		
IP Version	IPv4		
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	80 - 80		
Inbound	Allow		
Outbound	Allow		

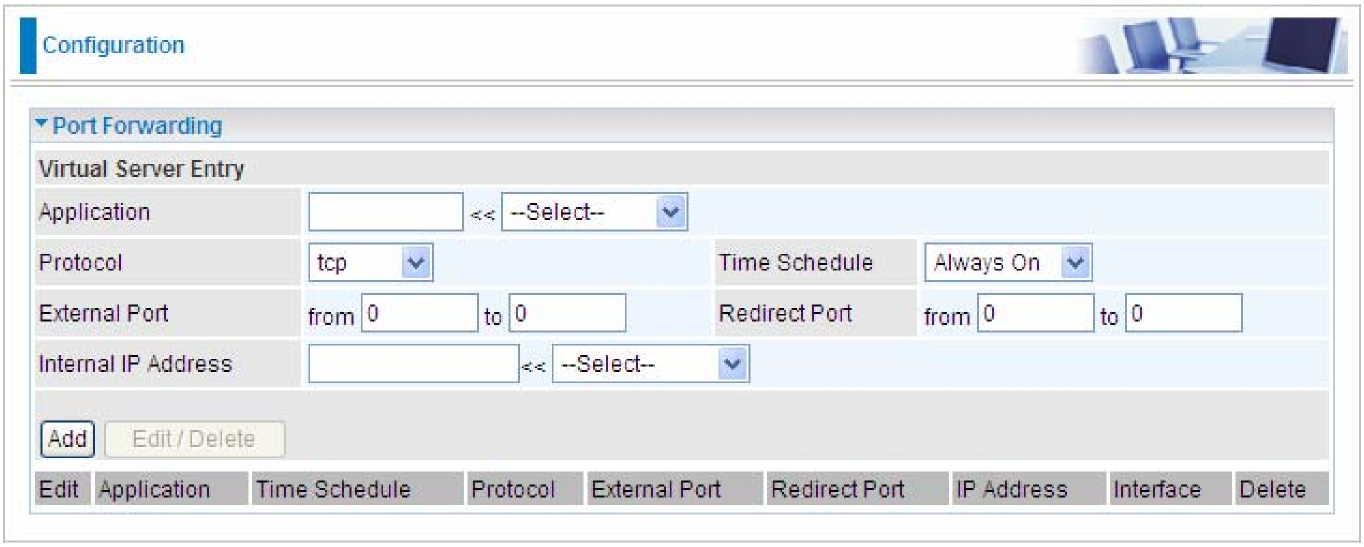
4. The new port filter rule for HTTP is shown below:



○	Cindy_HTTP	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Allow	○
			0.0.0.0 / 0.0.0.0		80 ~ 80	Allow	

5. Configure your Virtual Server ("port forwarding") settings so that incoming HTTP requests on port 80 will be forwarded to the PC running your web server:

Note: For how to configure the HTTP in Virtual Server, go to Add Virtual Server in Virtual Server section for more details.



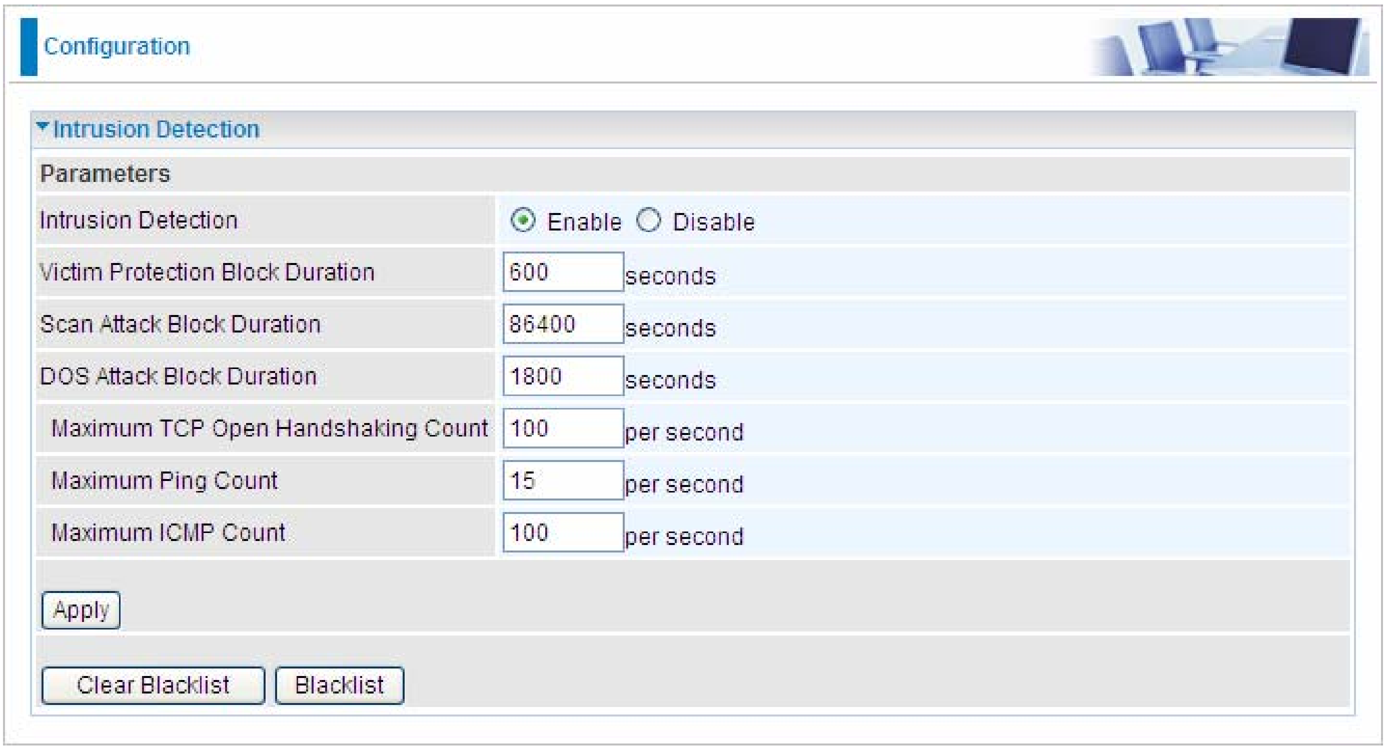
Configuration

Port Forwarding

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

Intrusion Detection



▾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's *Intrusion Detection System* (IDS) is used to detect hacker attacks 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 as the **Block Duration**. The default setting for this function is false (disabled). Some attack types 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).

Clear Blacklist: Clear the current blacklist.
Blacklist: Show the blacklist information.

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

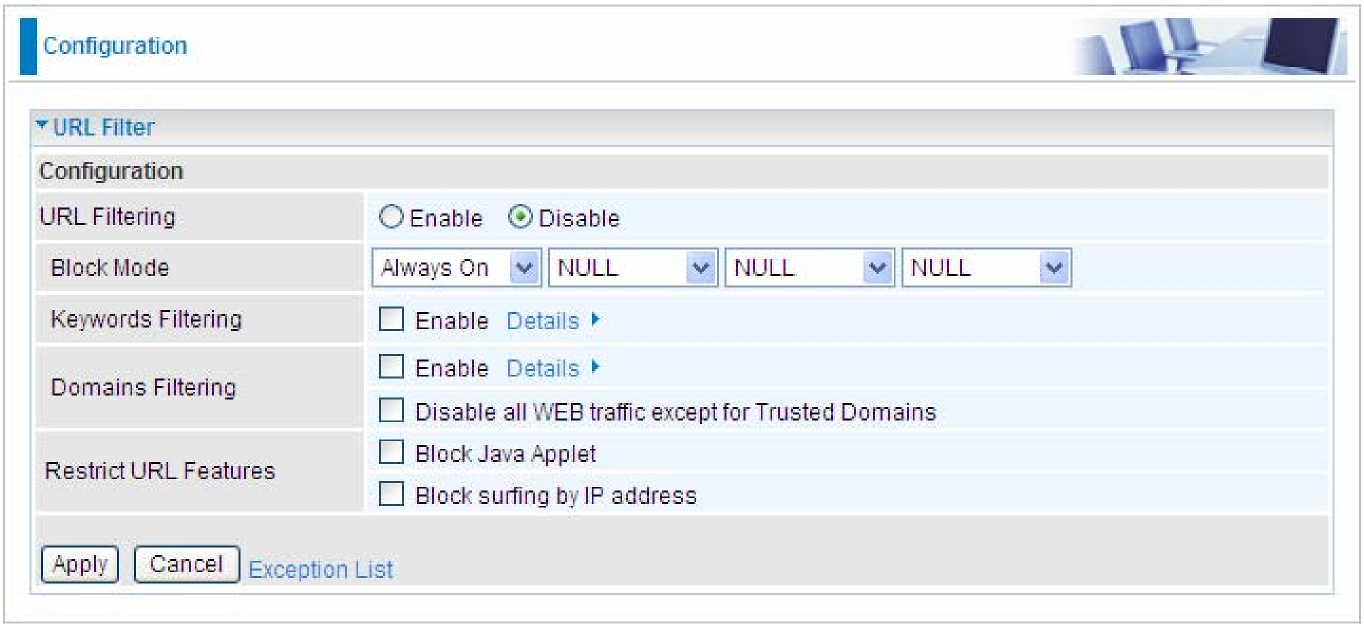
Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
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
Dst Port: Destination Port

Src Port: Source 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 rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Configuration

▾ URL Filter

Configuration	
URL Filtering	○ Enable ● Disable
Block Mode	Always On ▾ NULL ▾ NULL ▾ NULL ▾
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

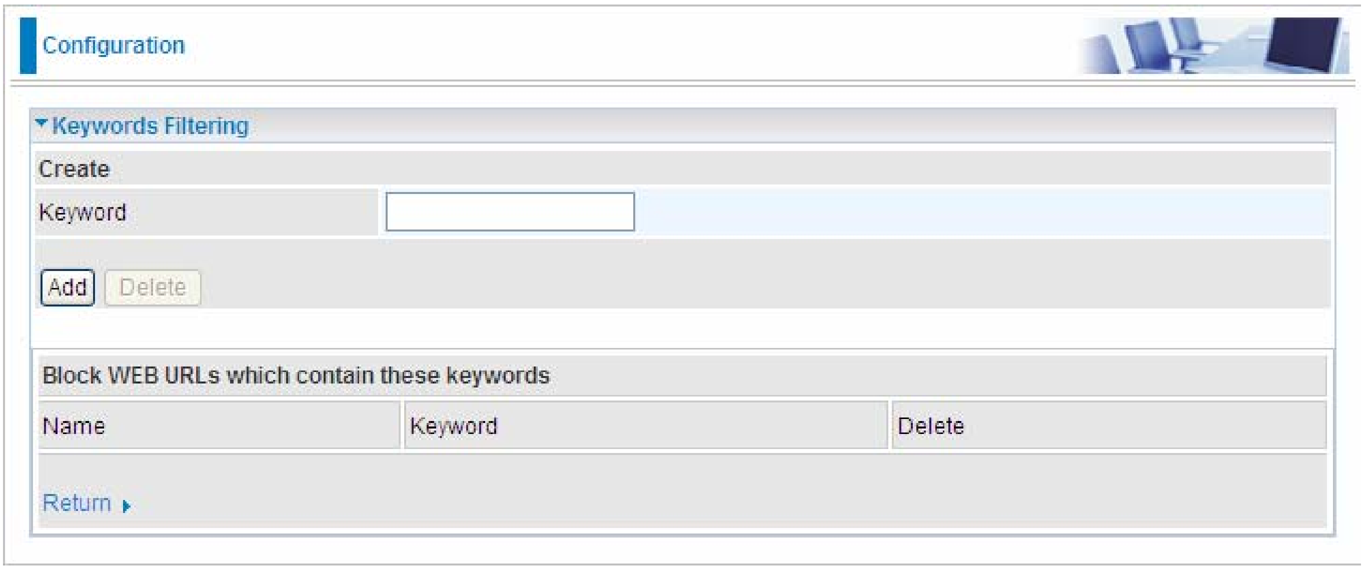
Enable/Disable: To enable or disable URL Filter feature.

Block Mode: It can support up to 4 timeslots.

- **Disabled:** No action will be performed by the Block Mode.
- **Always On:** Action is enabled. URL filter rules will be monitoring and checking all hours of the day.
- **TimeSlot1 ~ TimeSlot16:** It is 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: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called "advertisement.gif"). When enabled, your specified keywords list 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, it will be dropped as the keyword "abcde" occurs in the URL.



Configuration

▾ Keywords Filtering

Create

Keyword

Add Delete

Block WEB URLs which contain these keywords

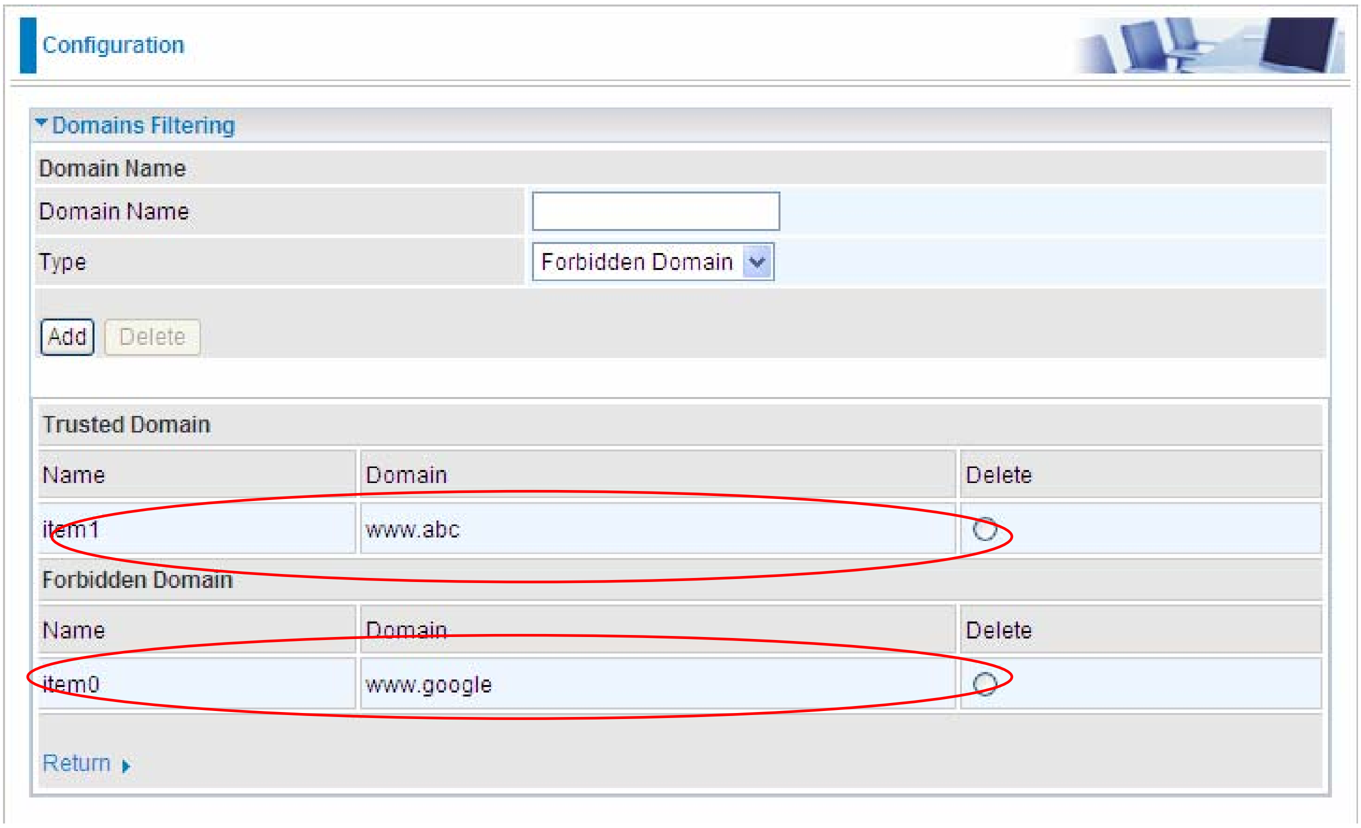
Name	Keyword	Delete

Return ▸

Domains Filtering: This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes 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 items, it is sent to the remote web server.
4. Please be note that the completed URL, "www" + domain name shall be specified. For example to block traffic to www.google.com.au, enter "www.google" or "www.google.com"

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

Trusted Domain

Name	Domain	Delete
item1	www.abc	○

Forbidden Domain

Name	Domain	Delete
item0	www.google	○

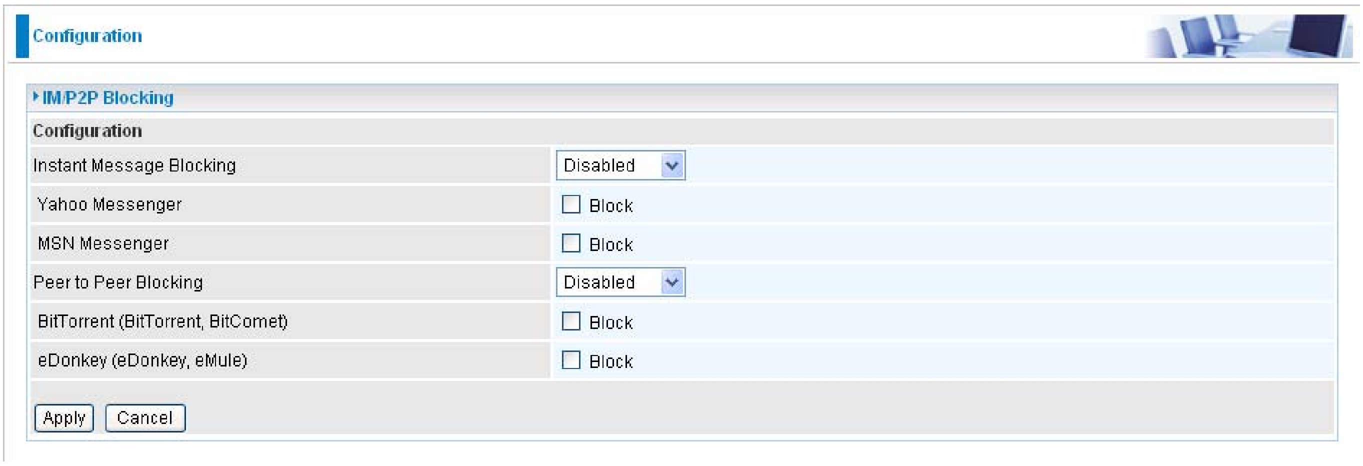
Example: Andy wishes to disable all WEB traffic except for ones listed in the trusted domain, which would prevent Bobby from accessing other web sites. Andy selects both functions in the *Domain Filtering* and thinks that it will stop Bobby. But Bobby knows this function, *Domain Filtering*, ONLY disables all WEB traffic except for **Trusted Domain,** BUT not its **IP address.** If this is the situation, **Block surfing by IP address** function can be handy and helpful to Andy. Now, Andy can prevent Bobby from accessing other sites.

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

- **Block Java Applet:** This function can block Web content that includes the Java Applet. It is to prevent someone who wants to damage your system via standard HTTP protocol.
- **Block surfing by IP address:** Preventing someone who uses the IP address as URL for skipping Domains Filtering function. Activates only and if Domain Filtering enabled.

IM / P2P Blocking

IM, short for Instant Message, is required to use client program software that allows users to communicate, in exchanging text message, with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of computer users who share file to specific groups of people across the Internet. 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 to 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.

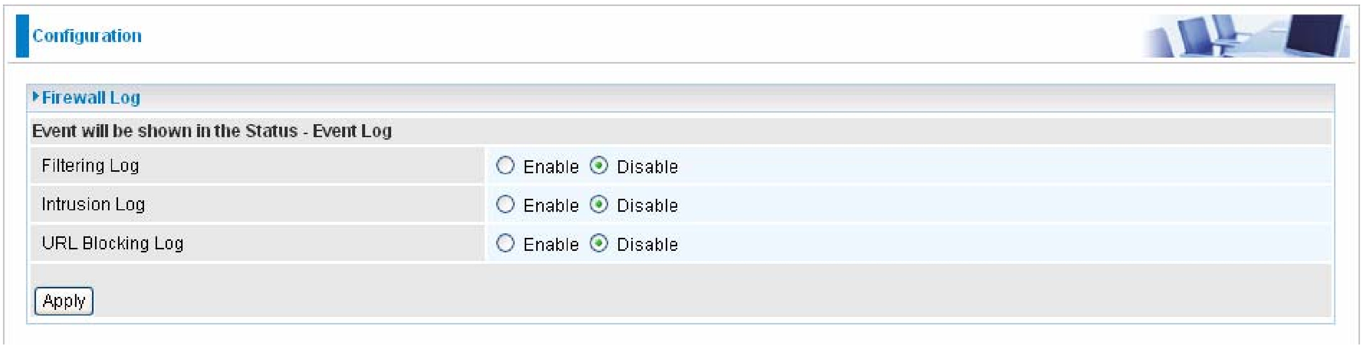
Yahoo/MSN Messenger: Check the box to block either or both Yahoo or/and MSN Messenger. To be sure you enabled the *Instant Message Blocking* first.

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 box to block either or both Bit Torrent or/and eDonkey. To be sure you enabled the *Peer to Peer Blocking* first.

Firewall Log



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 display log information of any unexpected action with your firewall settings.

Check the **Enable** box to activate the logs.

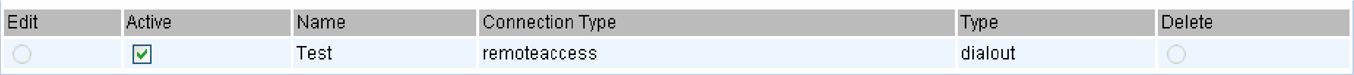
Log information can be seen in the **Status – Event Log** after enabling.

VPN - Virtual Private Networks (BiPAC 7402NX only)

Virtual Private Networks is ways to establish secured communication tunnels to an organization's network via the Internet. Your router supports three main types of VPN (Virtual Private Network), PPTP, IPSec and L2TP.

PPTP (Point-to-Point Tunneling Protocol)

There are two types of PPTP VPN supported; **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click Configuration/VPN/PPTP.



Edit	Active	Name	Connection Type	Type	Delete
○	☑	Test	remoteaccess	dialout	○

Name: A given name for the connection.

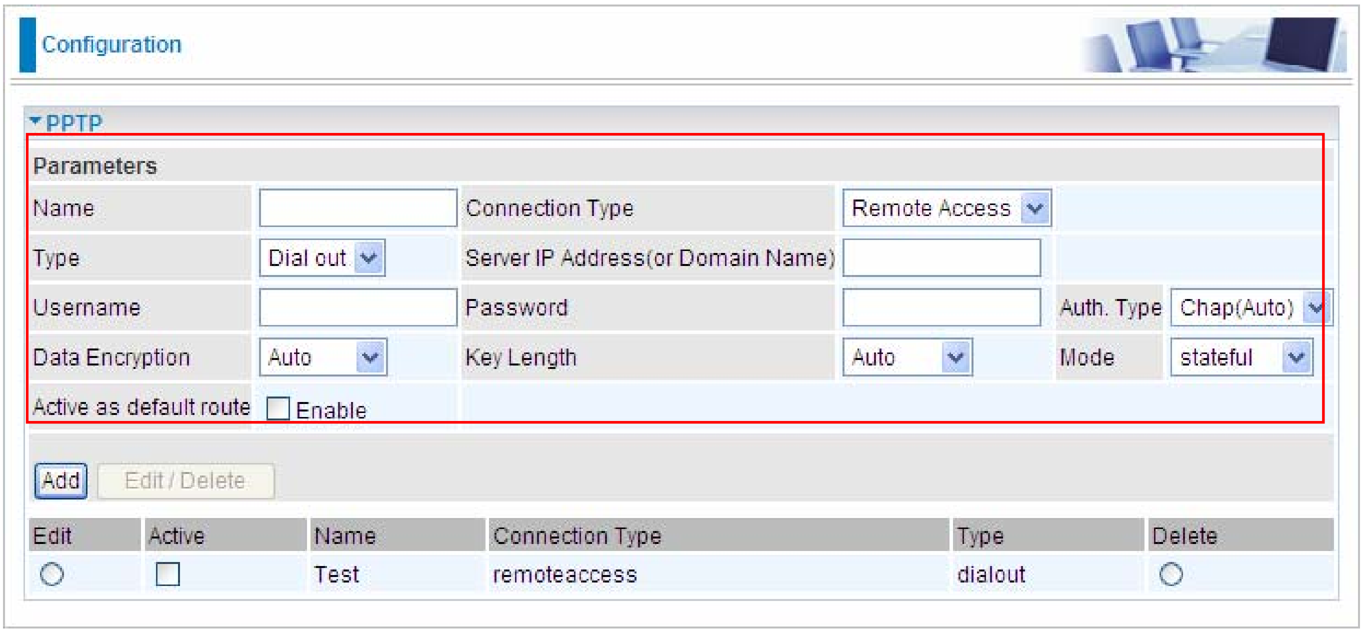
Active: This function activates or deactivates the PPTP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Connection Type: It informs your PPTP tunnel connection condition.

Type: This refers to your router operates as a client or a server, **Dialout** or **Dialin** respectively.

PPTP Connection - Remote Access



Configuration

PPTP

Parameters

Name		Connection Type	Remote Access		
Type	Dial out	Server IP Address(or Domain Name)			
Username		Password		Auth. Type	Chap(Auto)
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Active as default route	□ Enable				

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Name: A given name for the connection (e.g. "connection to office").

Connection Type: Remote Access or **LAN to LAN**

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Domain Name)** you wish to connect to.

a) When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

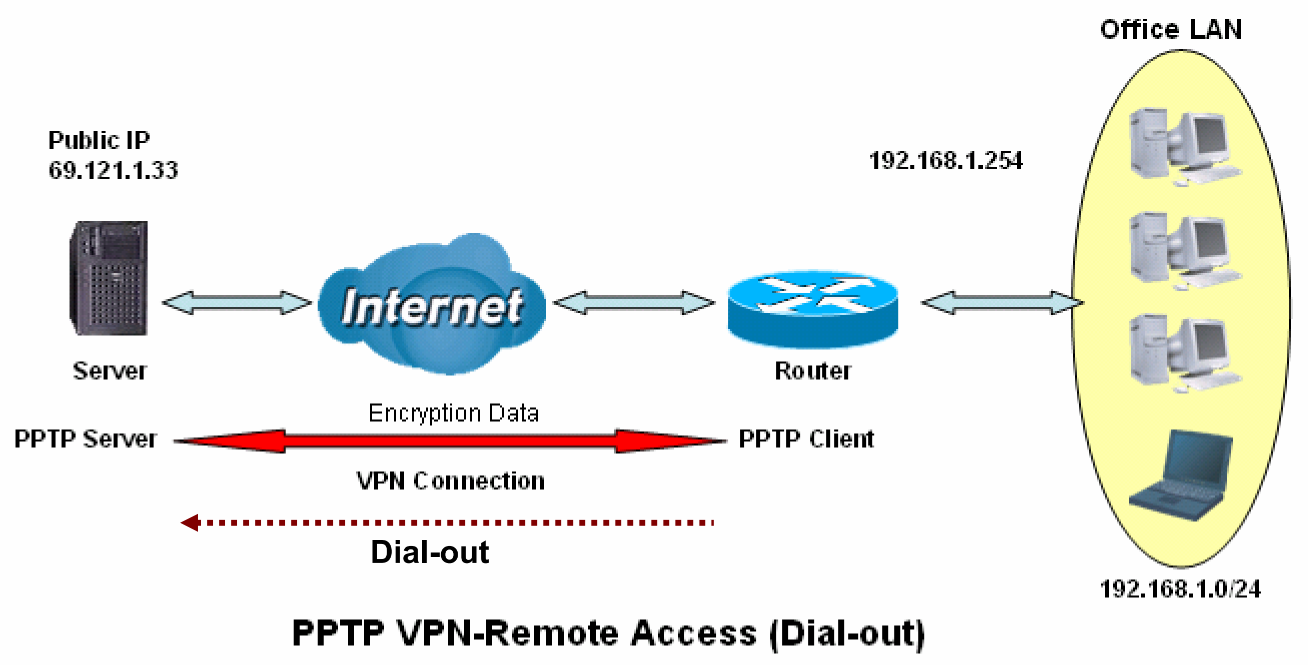
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Click **Edit/Delete** button to save your changes.

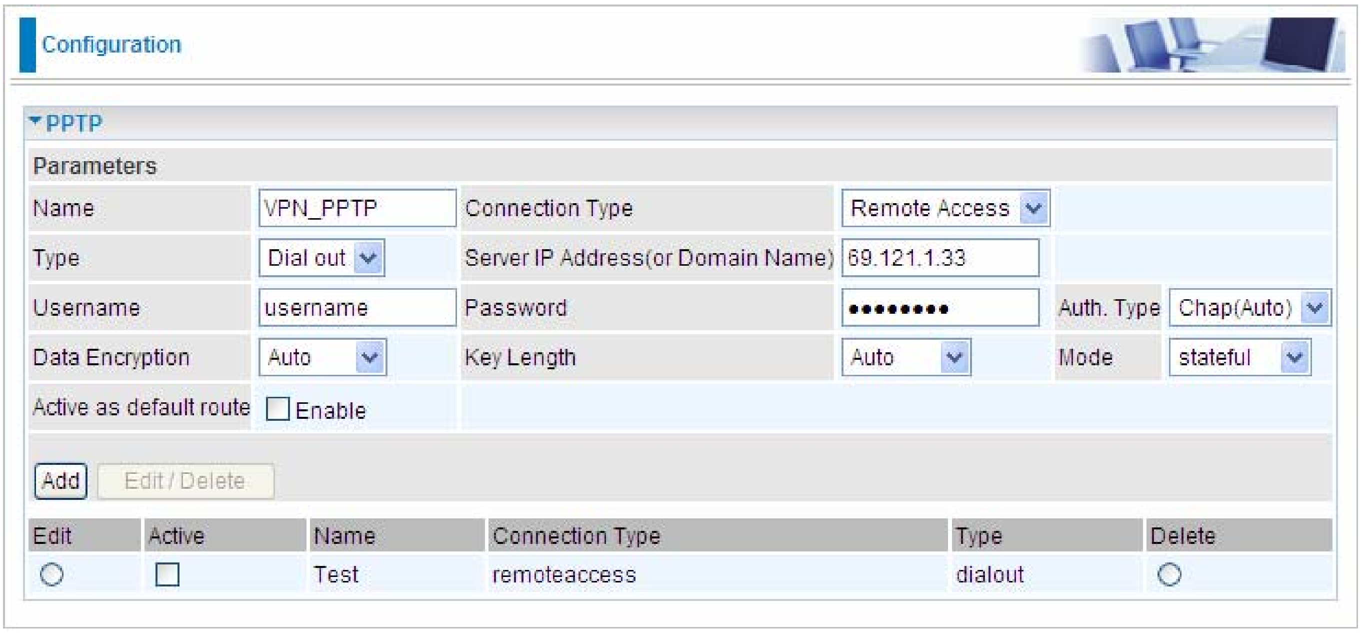
Example: Configuring a Remote Access PPTP VPN Dial-out Connection

A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



Configuring the PPTP VPN in the Office

Click **Configuration/VPN/PPTP**. Choose **Remote Access** from **Connect Type** drop-down menu. You can either input the IP address (69.121.1.33 in this case) or hostname to reach the server.



Configuration

▾PPTP

Parameters

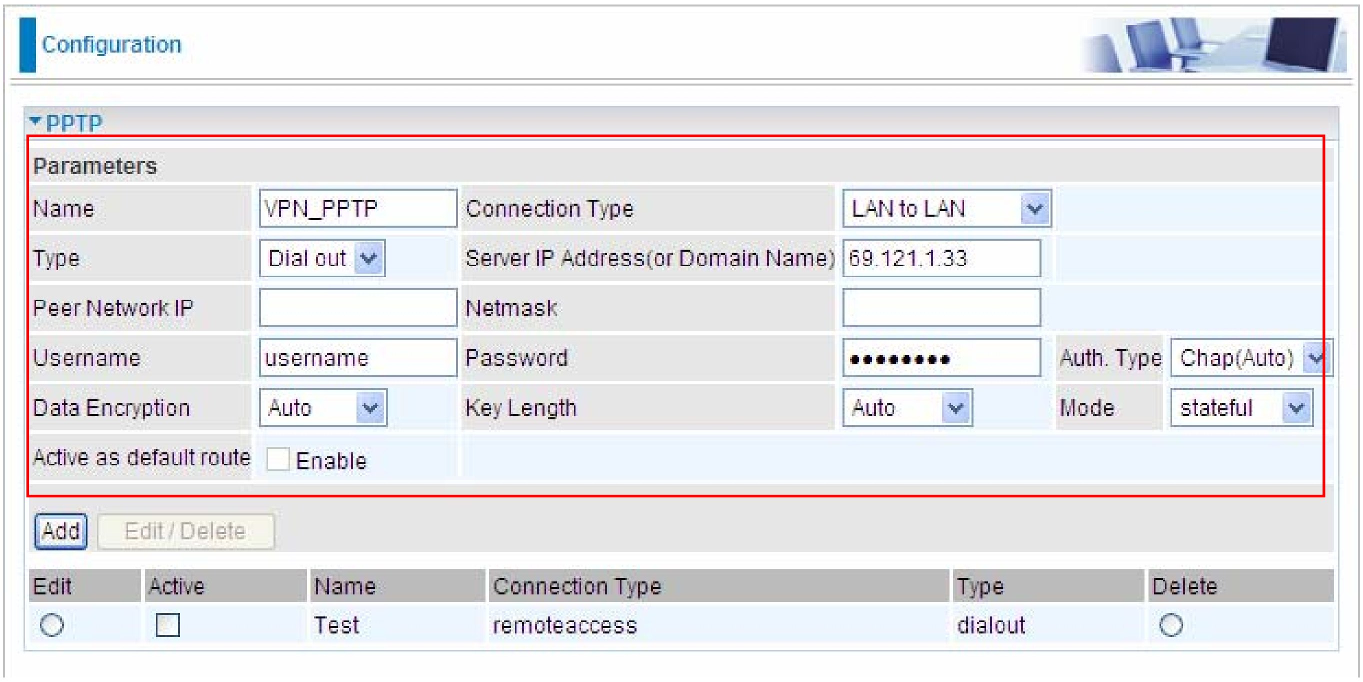
Name	VPN_PPTP	Connection Type	Remote Access		
Type	Dial out	Server IP Address(or Domain Name)	69.121.1.33		
Username	username	Password	●●●●●●●●	Auth. Type	Chap(Auto)
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Active as default route	□ Enable				

Add | Edit / Delete

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Item	Function		Description
1	Name	VPN_PPTP	Given name of PPTP connection
2	Connection Type	Remote Access	Select Remote Access from Connection Type drop-down menu
3	Type	Dial out	Select Dial out from Type drop-down menu
	IP Address (or Domain name)	69.121.1.33	An Dialed server IP
4	Username	username	A given username & password
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	

PPTP Connection - LAN to LAN



Name	VPN_PPTP	Connection Type	LAN to LAN		
Type	Dial out	Server IP Address(or Domain Name)	69.121.1.33		
Peer Network IP		Netmask			
Username	username	Password	●●●●●●●●	Auth. Type	Chap(Auto)
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Active as default route	□ Enable				

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Name: A given name of the connection.

Connection Type: Remote Access or **LAN to LAN.**

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

- When configuring your router as a Client, enter the remote **Server IP Address (or Domain name)** you wish to connect to.
- When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Data Encryption: Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default is **Auto,** so that this setting is negotiated when establishing a connection, or else you can manually **Enable** or **Disable** encryption.

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is **Auto**, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

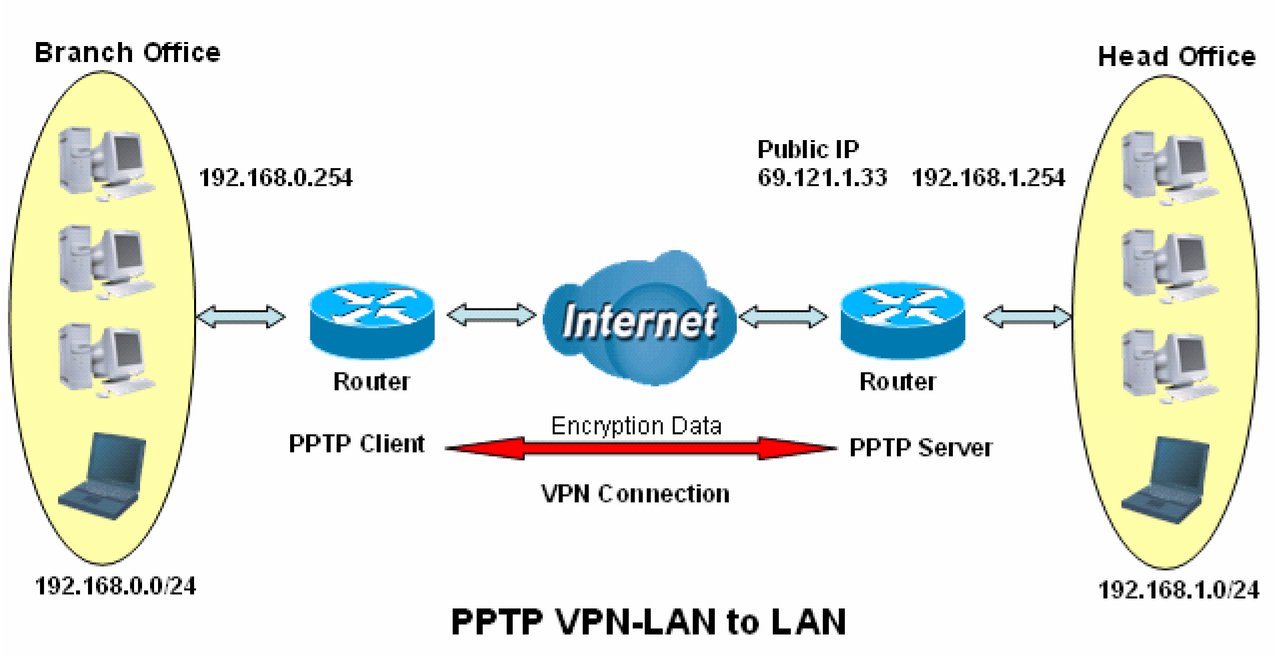
Mode: You may select **Stateful** or **Stateless** mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Active as default route: As the connection type is LAN to LAN, this function will become to disable.

Click **Edit/Delete** button to save your changes.

Example: Configuring a PPTP LAN-to-LAN VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.

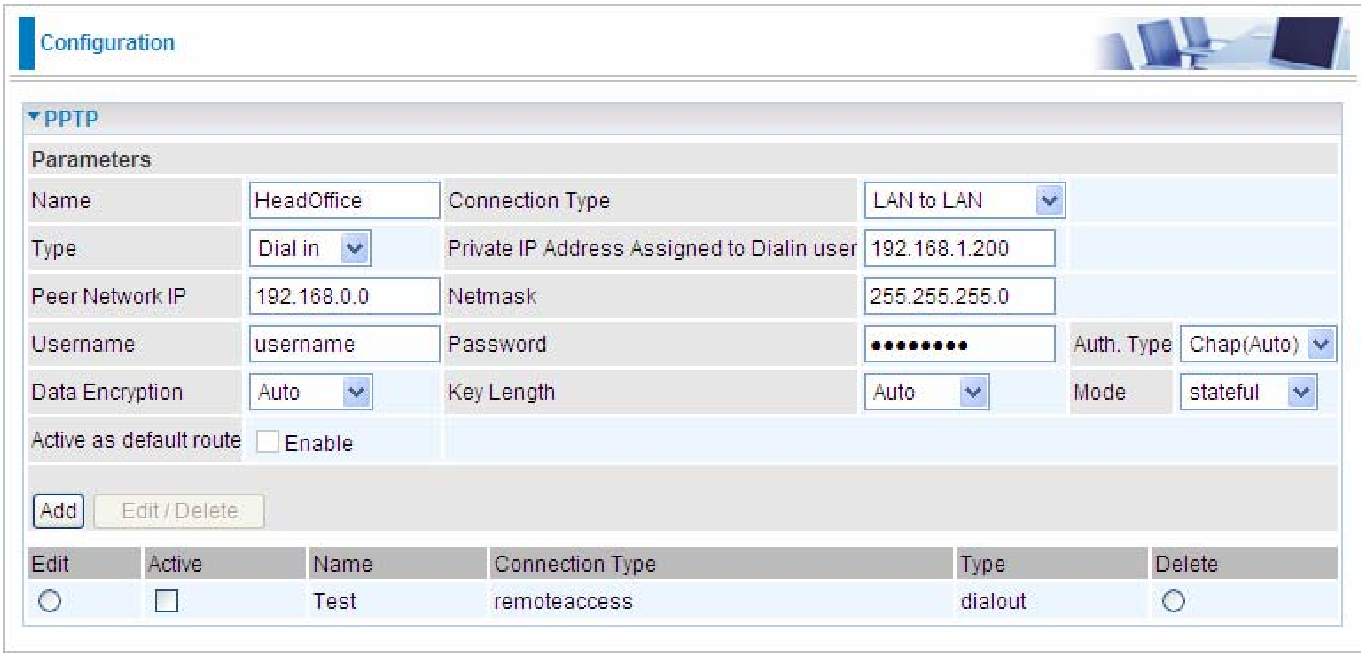


Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Configuring PPTP VPN in the Head Office

The IP address 192.168.1.201 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



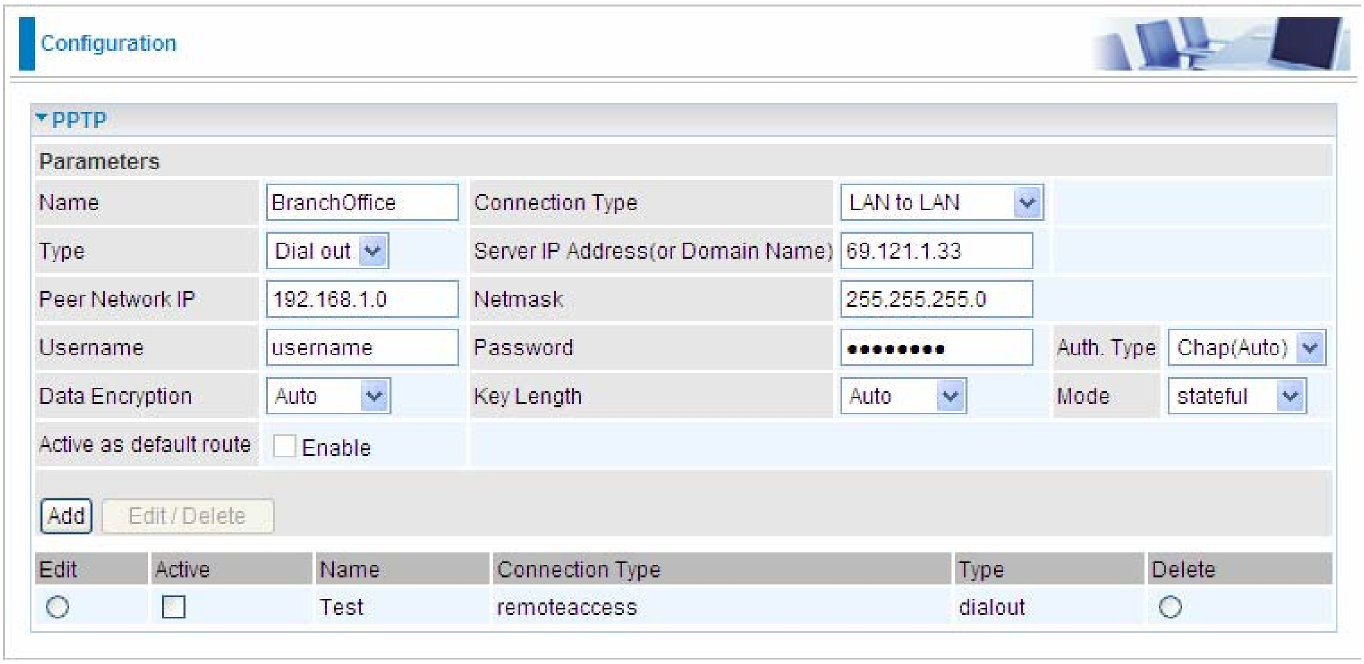
Name	HeadOffice	Connection Type	LAN to LAN		
Type	Dial in	Private IP Address Assigned to Dialin user	192.168.1.200		
Peer Network IP	192.168.0.0	Netmask	255.255.255.0		
Username	username	Password	••••••••	Auth. Type	Chap(Auto)
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Active as default route	□ Enable				

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Item	Function		Description
1	Name	HeadOffice	Given a name of PPTP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from Connection Type drop-down menu
3	Type	Dial in	Select Dial in from Type drop-down menu
	IP Address	192.168.1.200	IP address assigned to branch office network
4	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate branch office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	

Configuring PPTP VPN in the Branch Office

The IP address 69.121.1.33 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.



Configuration

PPTP

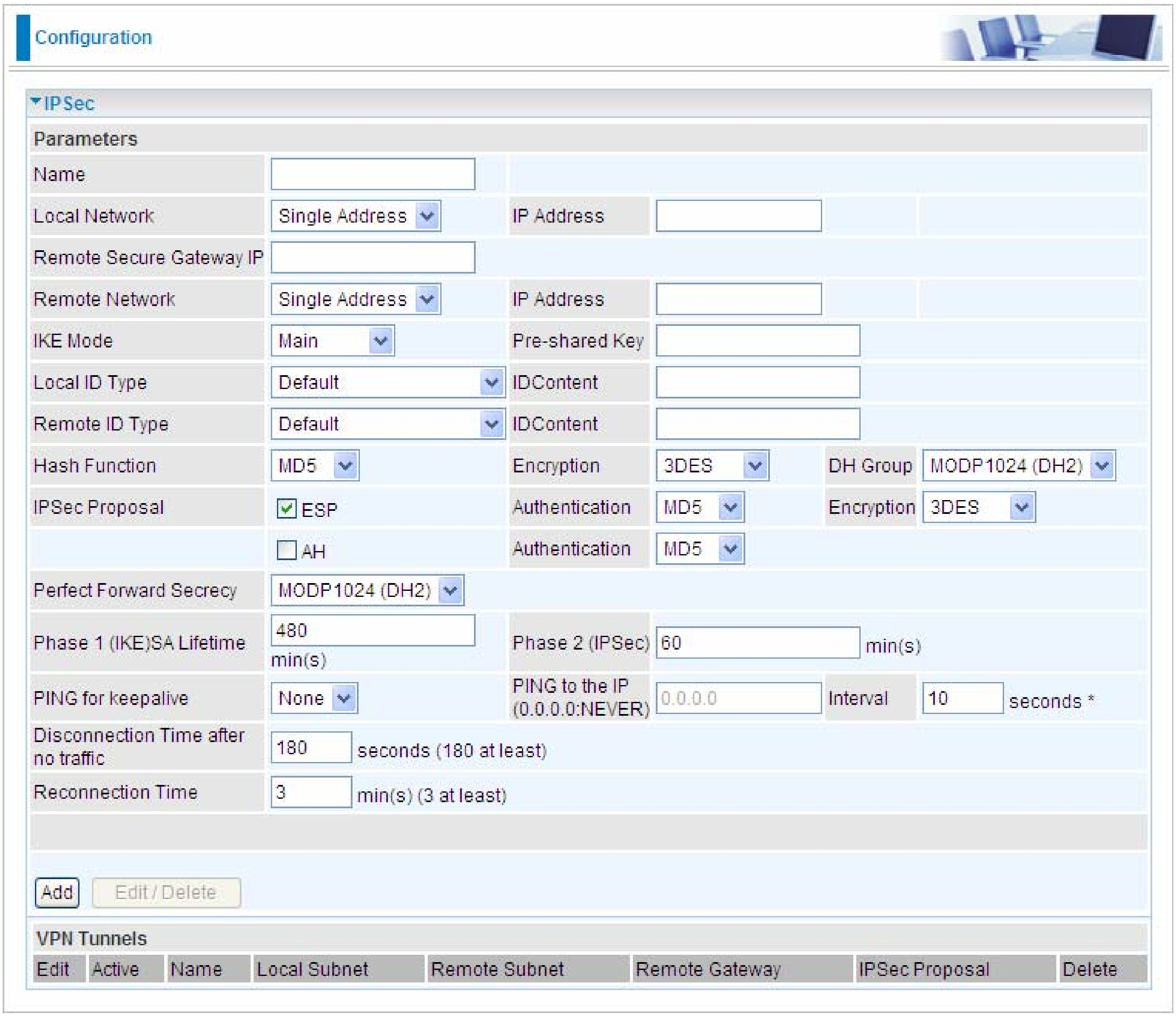
Parameters

Name	BranchOffice	Connection Type	LAN to LAN		
Type	Dial out	Server IP Address(or Domain Name)	69.121.1.33		
Peer Network IP	192.168.1.0	Netmask	255.255.255.0		
Username	username	Password	●●●●●●●●	Auth. Type	Chap(Auto)
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Active as default route	□ Enable				

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Item	Function		Description
1	Name	BranchOffice	Given a name of PPTP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from Connection Type drop-down menu
3	Type	Dial out	Select Dial out from Type drop-down menu
	IP Address (or Domain name)	69.121.1.33	IP address of the head office router (in WAN side)
4	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate head office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	

IPSec (IP Security Protocol)



Configuration

IPSec

Parameters

Name					
Local Network	Single Address	IP Address			
Remote Secure Gateway IP					
Remote Network	Single Address	IP Address			
IKE Mode	Main	Pre-shared Key			
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	□ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

Edit	Active	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Delete

Active: This function activates or deactivates the IPSec connection.   Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Name: This is a given name of the connection.

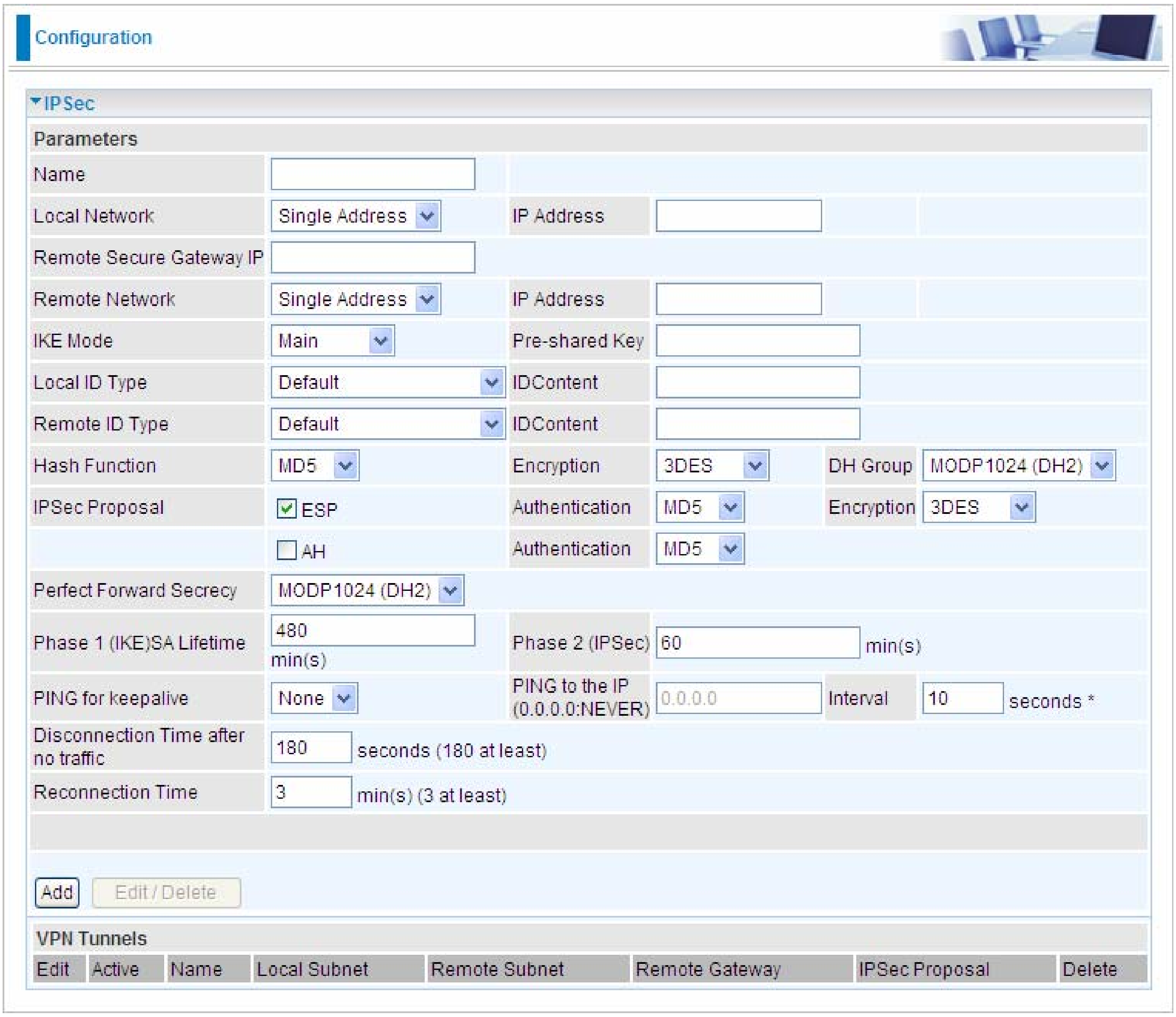
Local Subnet: Displays IP address and subnet of the local network.

Remote Subnet: Displays IP address and subnet of the remote network.

Remote Gateway: This is the IP address or Domain Name of the remote VPN device that is connected and established a VPN tunnel.

IPSec Proposal: This is selected IPSec security method.

IPSec VPN Connection



Parameters

Name					
Local Network	Single Address	IP Address			
Remote Secure Gateway IP					
Remote Network	Single Address	IP Address			
IKE Mode	Main	Pre-shared Key			
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	☐ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

Edit	Active	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Delete

Name: A given name for the connection (e.g. "connection to office").

Local Network: Set the IP address, subnet or address range of the local network.

- **Single Address:** The IP address of the local host.
- **Subnet:** The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).
- **IP Range:** The IP address range of the local network. For example, IP: 192.168.1.1, end IP: 192.168.1.10.

Remote Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

Remote Network: Set the IP address, subnet or address range of the remote network.

IKE (Internet key Exchange) Mode: Select IKE mode to Main mode or Aggressive mode. This IKE provides secured key generation and key management.

Local ID:

- **Content:** Input ID's information, like domain name www.ipsectest.com.

Remote ID:

b) **Identifier:** Input remote ID's information, like domain name www.ipsectest.com.

Hash Function: It is a Message Digest algorithm which coverts any length of a message into a unique set of bits. It is widely used MD5 (Message Digest) and SHA-1 (Secure Hash Algorithm) algorithms. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

⊙ **MD5:** A one-way hashing algorithm that produces a 128−bit hash.

⊙ **SHA1:** A one-way hashing algorithm that produces a 160−bit hash

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES** and **AES (128, 192 and 256)**. 3DES and AES are more powerful but increase latency.

c) **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

d) **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

⊙ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

DH (Diffie-Hellman) Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

IPSec Proposal: Select the IPSec security method. There are two methods of checking the authentication information, AH (authentication header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. Using AH data will be authenticated but not encrypted.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

e) **MD5:** A one-way hashing algorithm that produces a 128−bit hash.

f) **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are several options, **DES**, **3DES**, **AES (128, 192 and 256)** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

g) **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

h) **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

i) **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

⊙ **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.

⊙ **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

PING for Keep Alive:

⊙**None:** The default setting is **None**. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of **Disconnection time after no traffic**, which the remote IPSec will be disconnected after the time you set in this function.

⊙**PING:** This mode will detect the remote IPSec peer has lost or not by pinging specify IP address.

⊙**DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Re-establish of this connection is required. Default setting is 0.0.0.0 which disables the function.

Interval: This sets the time interval between ***Pings to the IP*** function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

Ping to the IP	**Interval (sec)**	***Ping to the IP* Action**
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the **Reconnection Time** set. **180 seconds** is minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. **3 minutes** is minimum time interval for this function.

Click **Edit/Delete** to save your changes.

Example: Configuring a IPSec LAN-to-LAN VPN Connection

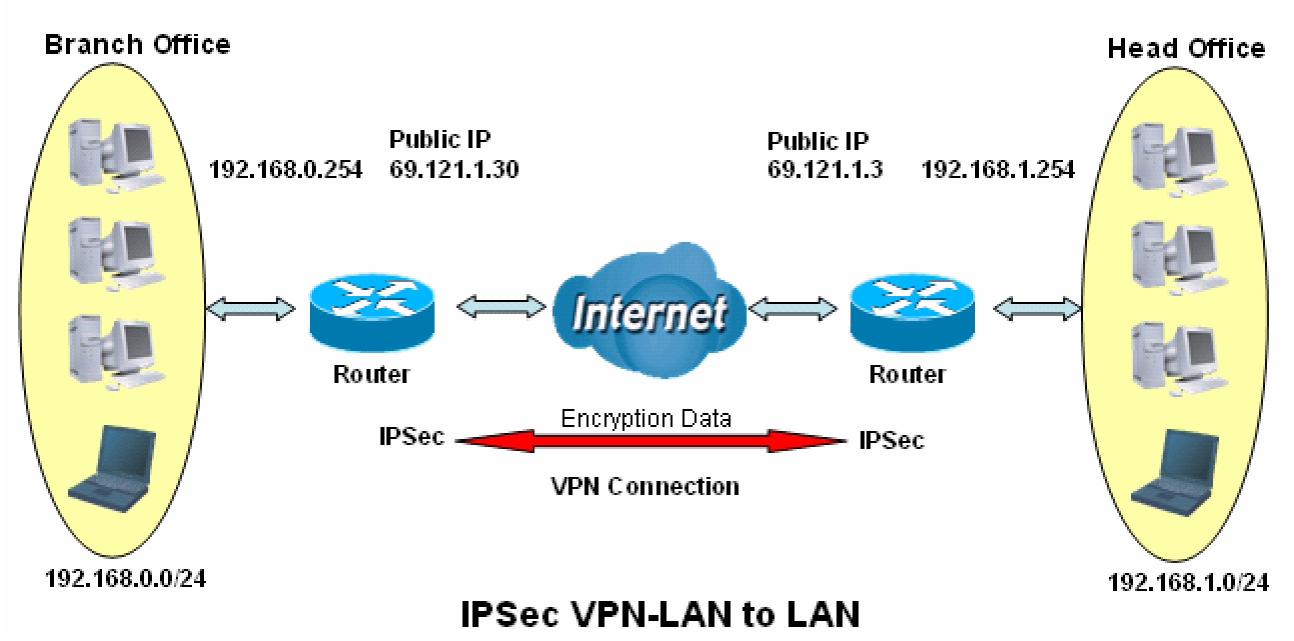


Table 3: Network Configuration and Security Plan

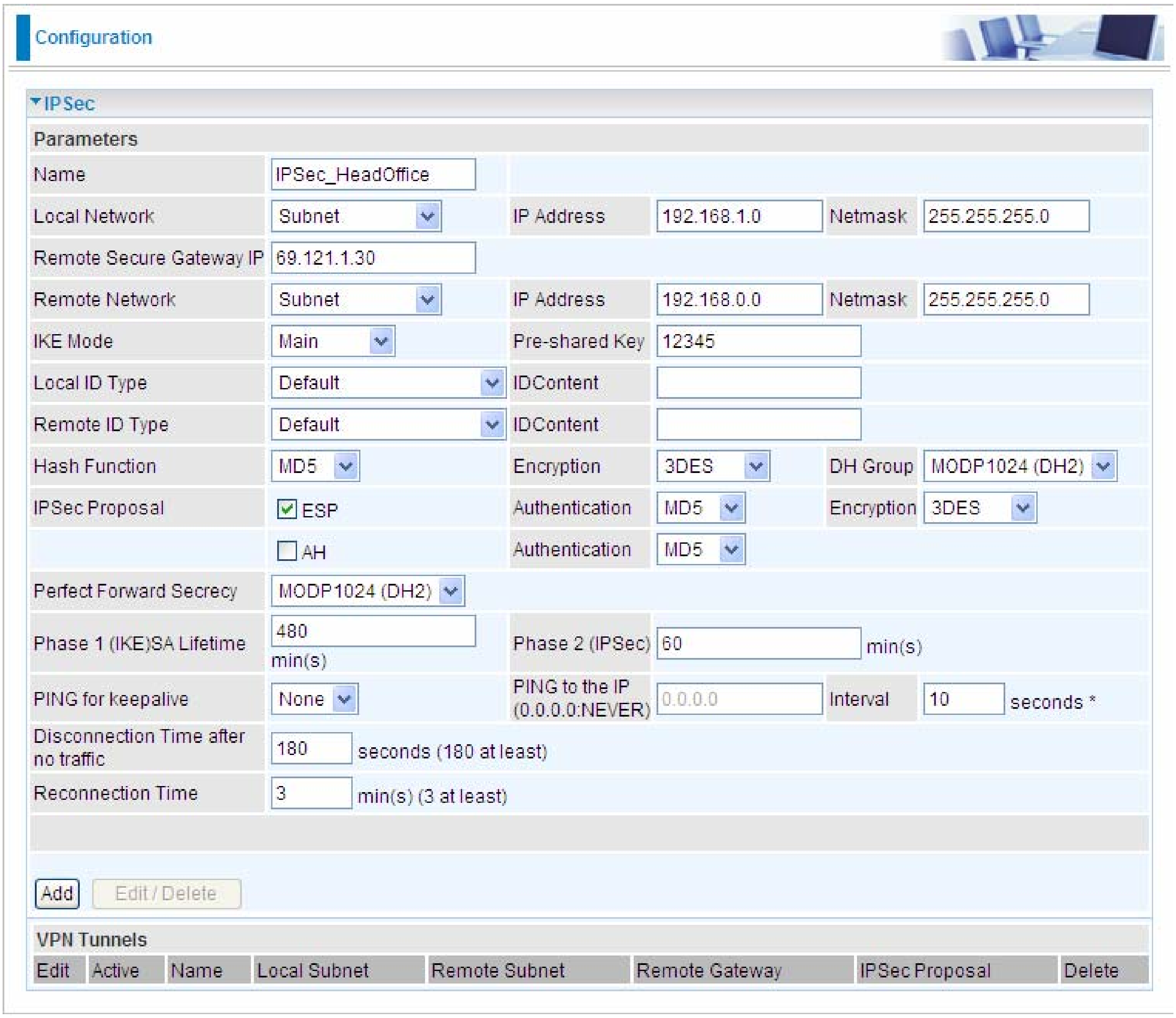
	Branch Office	Head Office
Local Network ID	192.168.0.0/24	192.168.1.0/24
Local Router IP	69.121.1.30	69.121.1.3
Remote Network ID	192.168.1.0/24	192.168.0.0/24
Remote Router IP	69.1.121.3	69.1.121.30
IKE Pre-shared Key	12345678	12345678
VPN Connection Type	Tunnel mode	Tunnel mode
Security Algorithm	ESP:MD5 with AES	ESP:MD5 with AES

Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring IPSec VPN in the Head Office



Parameters

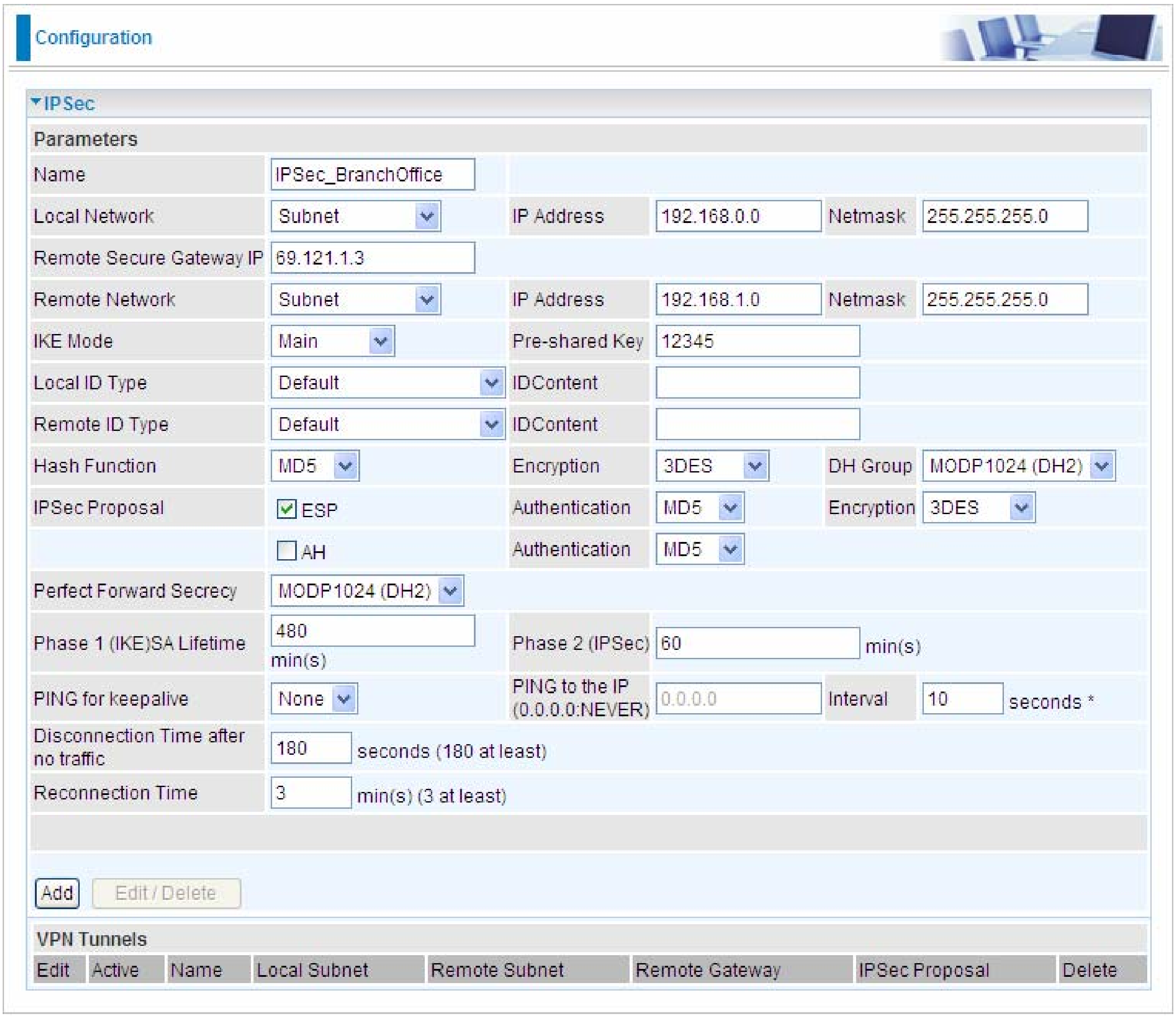
Name	IPSec_HeadOffice				
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Secure Gateway IP	69.121.1.30				
Remote Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
IKE Mode	Main	Pre-shared Key	12345		
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	☐ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

Edit	Active	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Delete

Item	Function		Description
1	Name	IPSec_HeadOffice	Given a name of IPSec connection
2	Local Network	Subnet	Select Subnet from Local Network drop-down menu.
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway IP (or Hostname)	69.121.1.30	IP address of the branch office router (in WAN side)
4	Remote Network	Subnet	Select Subnet from Remote Network drop-down menu
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345	

Configuring IPSec VPN in the Branch Office



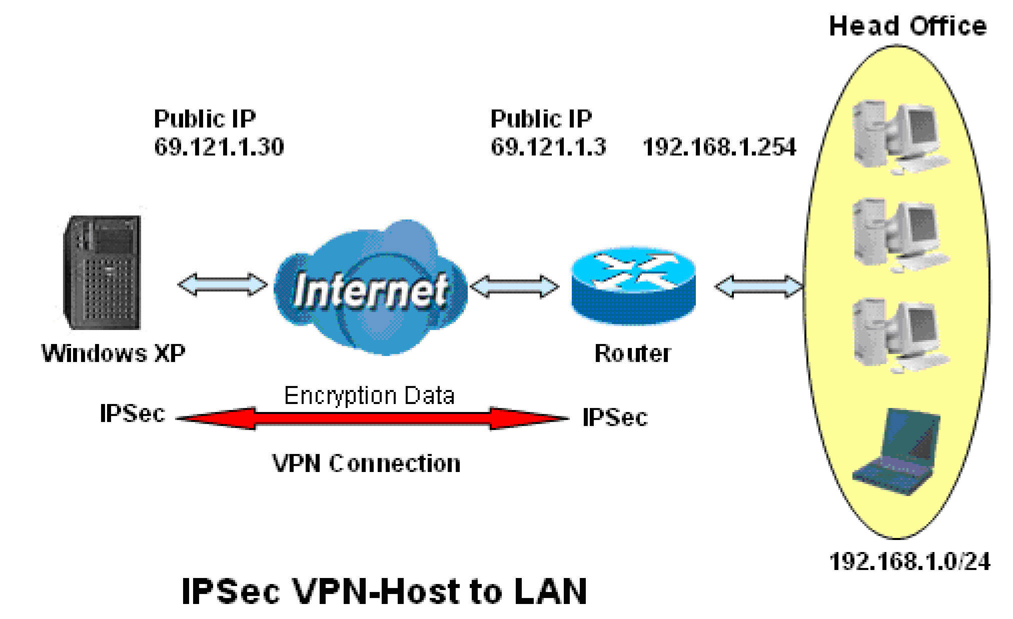
Parameters					
Name	IPSec_BranchOffice				
Local Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Remote Secure Gateway IP	69.121.1.3				
Remote Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
IKE Mode	Main	Pre-shared Key	12345		
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	☐ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

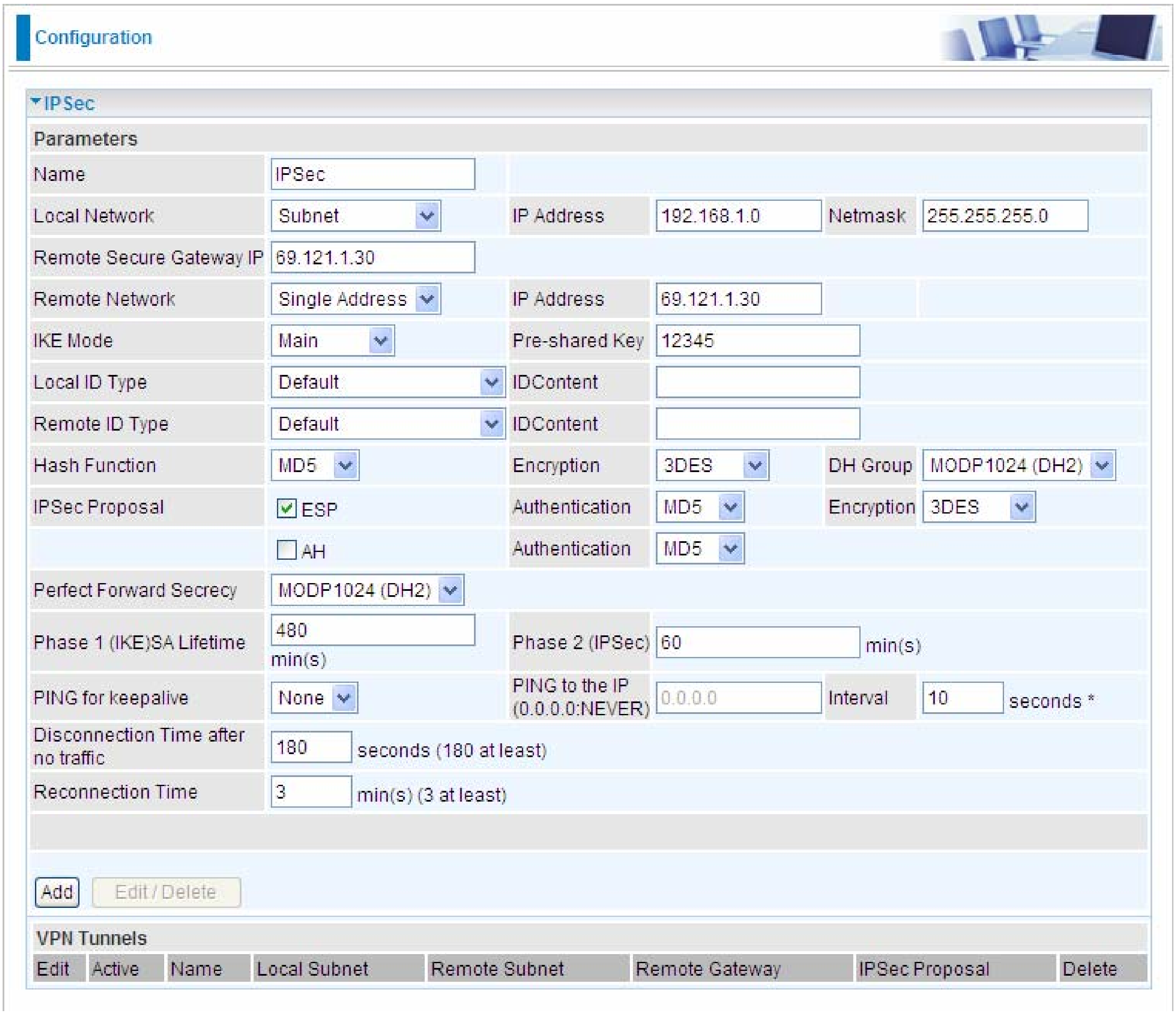
Edit	Active	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Delete

Item	Function		Description
1	Name	IPSec_Branch Office	Given a name of IPSec connection
2	Local Network	Subnet	Select Subnet from Local Network drop-down menu.
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway IP (or Hostname)	69.121.1.3	IP address of the head office router (in WAN side)
4	Remote Network	Subnet	Select Subnet from Remote Network drop-down menu
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345	

Example: Configuring a IPSec Host-to-LAN VPN Connection



Configuring IPSec VPN in the Office



Parameters

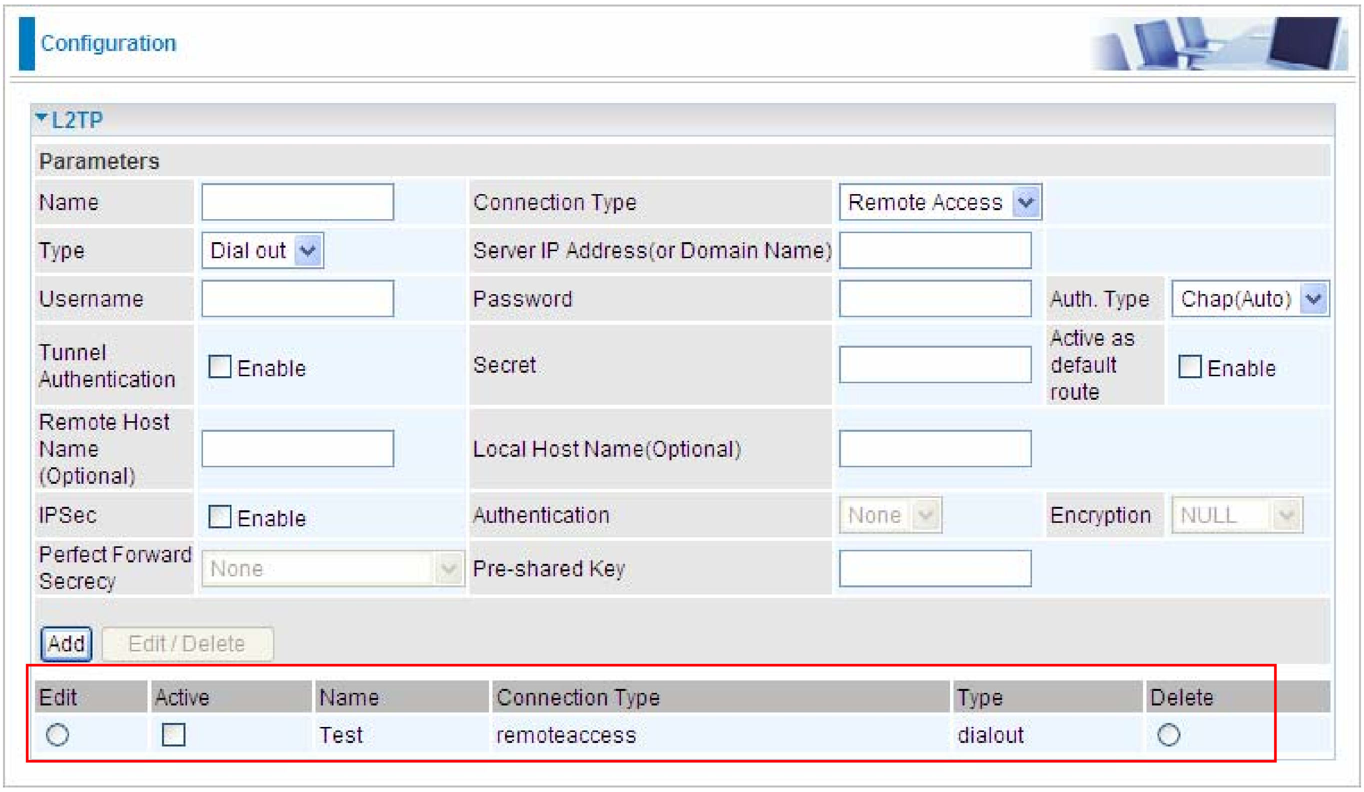
Name	IPSec				
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Secure Gateway IP	69.121.1.30				
Remote Network	Single Address	IP Address	69.121.1.30		
IKE Mode	Main	Pre-shared Key	12345		
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	☐ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

Edit	Active	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Delete

Item	Function		Description
1	Name	IPSec	Given a name of IPSec connection
2	Local Network	Subnet	Select Subnet from Network drop-down menu
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway IP (or Hostname)	69.121.1.30	Remote worker's IP address
4	Remote Network	Single Address	Select Single Address from Remote Network drop-down menu
	IP Address	69.121.1.30	Remote worker's IP address
5	Authentication	MD5	Security plan
	Encryption	3DES	
	Prefer Forward Security	None	
	Pre-shared Key	12345	

L2TP (Layer Two Tunneling Protocol)



Configuration

L2TP

Parameters

Name		Connection Type	Remote Access		
Type	Dial out	Server IP Address(or Domain Name)			
Username		Password		Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name (Optional)		Local Host Name(Optional)			
IPSec	□ Enable	Authentication	None	Encryption	NULL
Perfect Forward Secrecy	None	Pre-shared Key			

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Two types of L2TP VPN are supported **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Fill in the blank with information you need and click **Add** to create a new VPN connection account.

Active: This function activates or deactivates the L2TP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

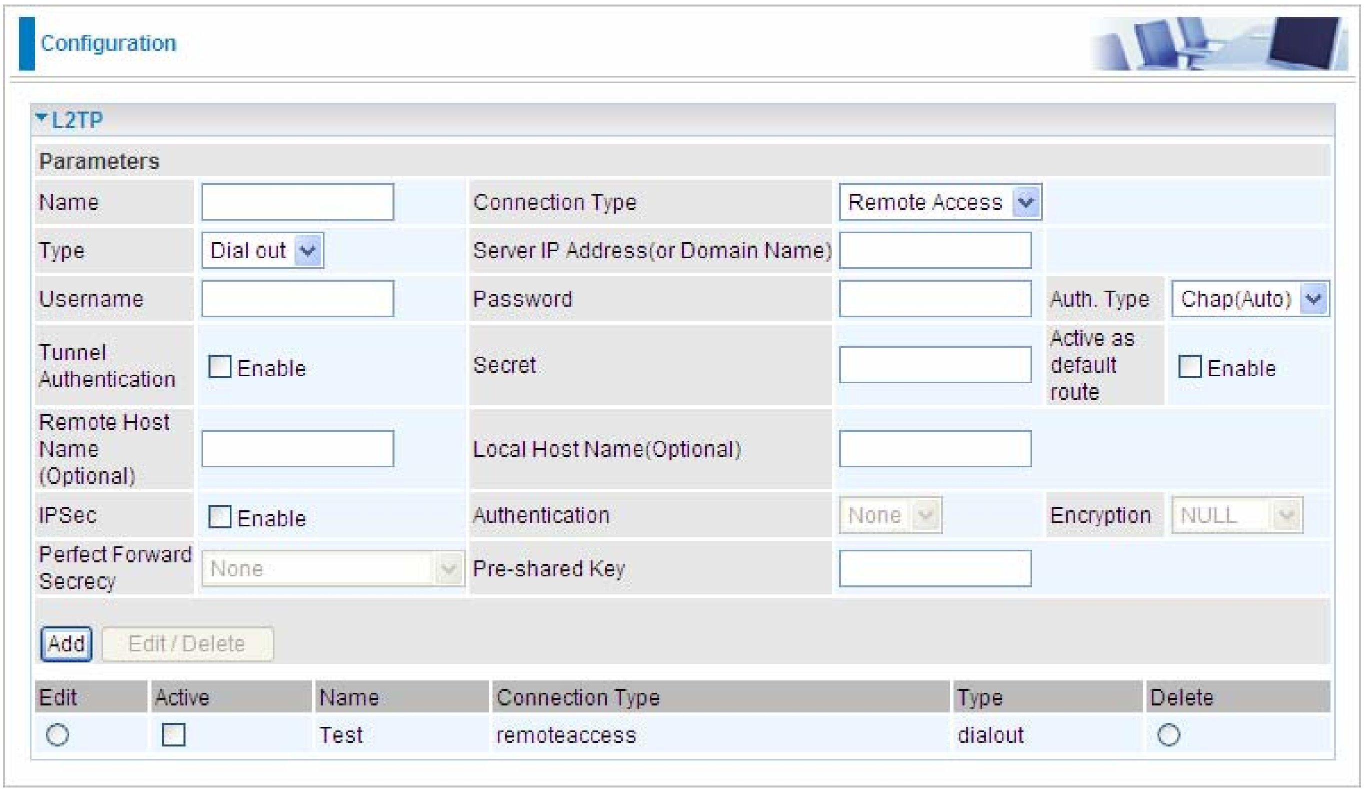
Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Name: This is a given name of the connection.

Connection Type: It informs your L2TP tunnel connection condition.

Type: This refers to your router operates as a client or a server, **Dialout** or **Dialin** in respectively.

L2TP Connection - Remote Access



Configuration

▾L2TP

Parameters

Name		Connection Type	Remote Access		
Type	Dial out	Server IP Address(or Domain Name)			
Username		Password		Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name (Optional)		Local Host Name(Optional)			
IPSec	□ Enable	Authentication	None	Encryption	NULL
Perfect Forward Secrecy	None	Pre-shared Key			

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

<u>**Connection Type: Remote Access** or **LAN to LAN**</u>

Name: A given name for the connection (e.g. "connection to office").

Active: This function activates or deactivates the L2TP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

When configuring your router as a Client, enter the remote **Server IP Address (or Hostname)** you wish to connection to.

When configuring your router as a server, enter the **Private IP Address Assigned to Dial in User** address.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Remote Host Name (Optional): Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Cautious: This is only when the router performs as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. As default, Router's default Hostname is **home.gateway.**

IPSec: Enable for enhancing your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

- ⊙ **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- ⊙ **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

- ⊙ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- ⊙ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ⊙ **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

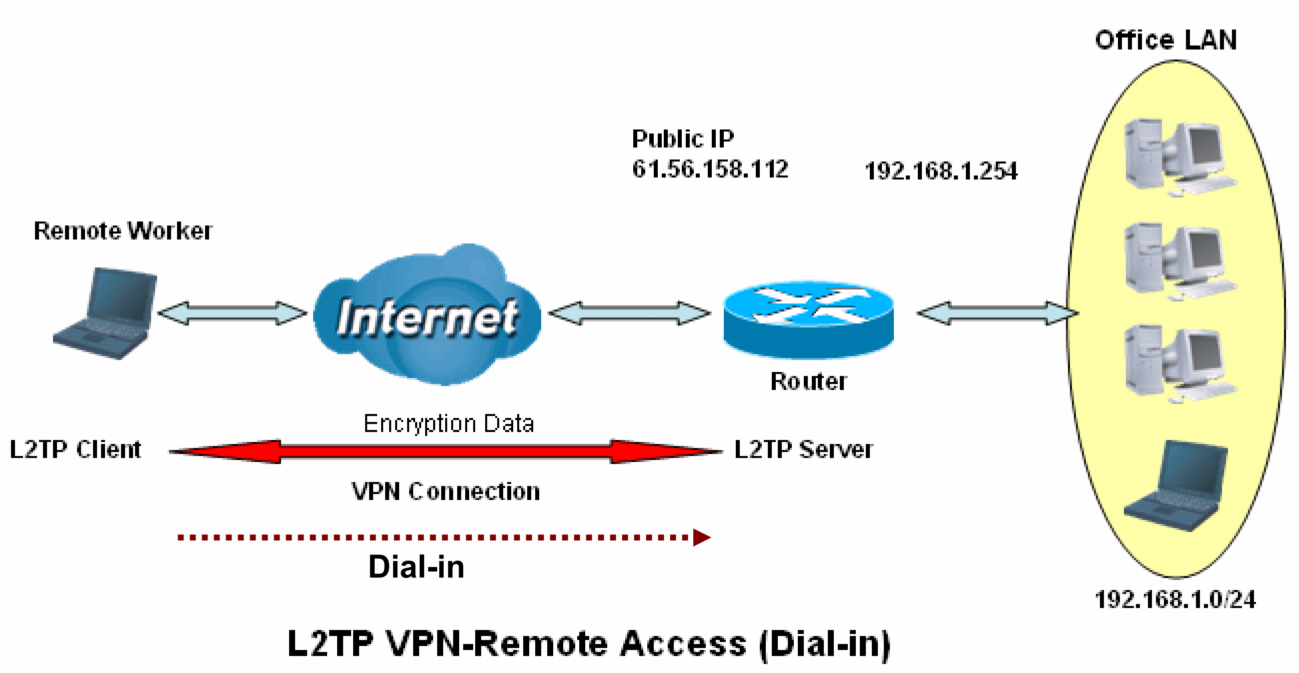
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Click **Edit/Delete** to save your changes**.**

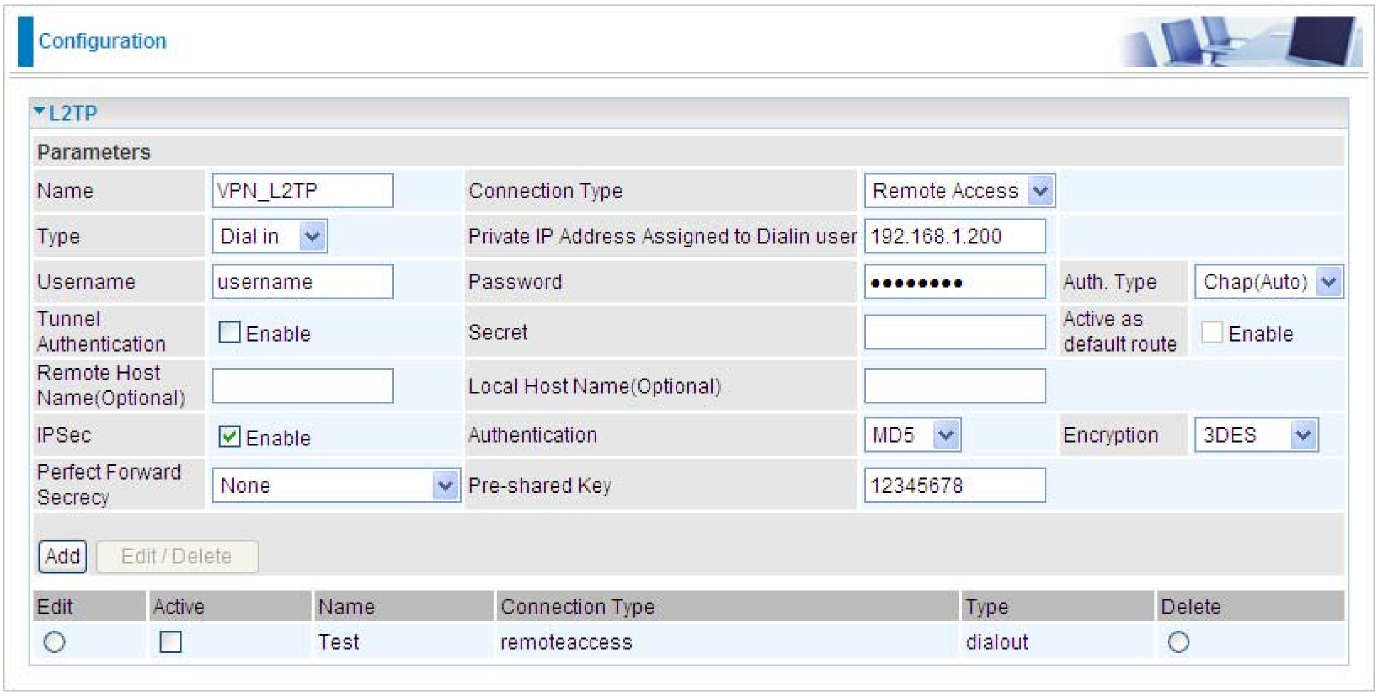
Example: Configuring a L2TP VPN - Remote Access Dial-in Connection

A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office, connected to a couple of PCs and Servers.



Configuring L2TP VPN in the Office

The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.



Parameters

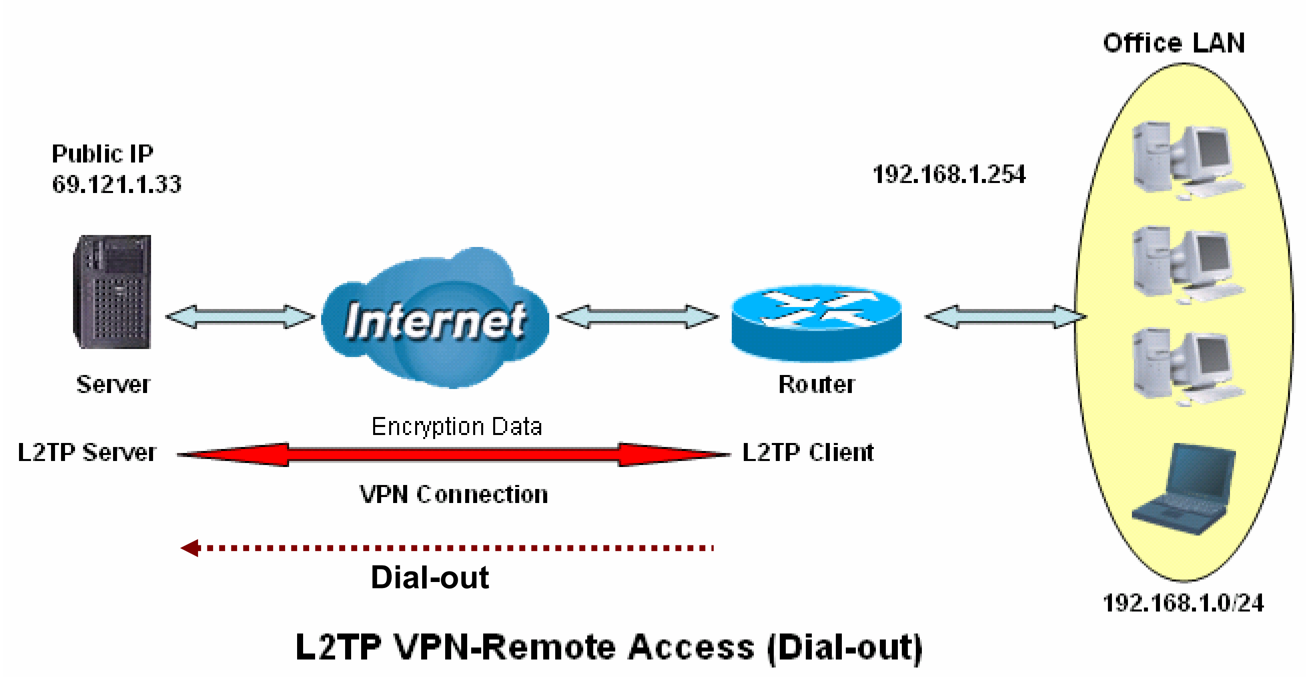
Name	VPN_L2TP	Connection Type	Remote Access		
Type	Dial in	Private IP Address Assigned to Dialin user	192.168.1.200		
Username	username	Password	••••••••	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name(Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

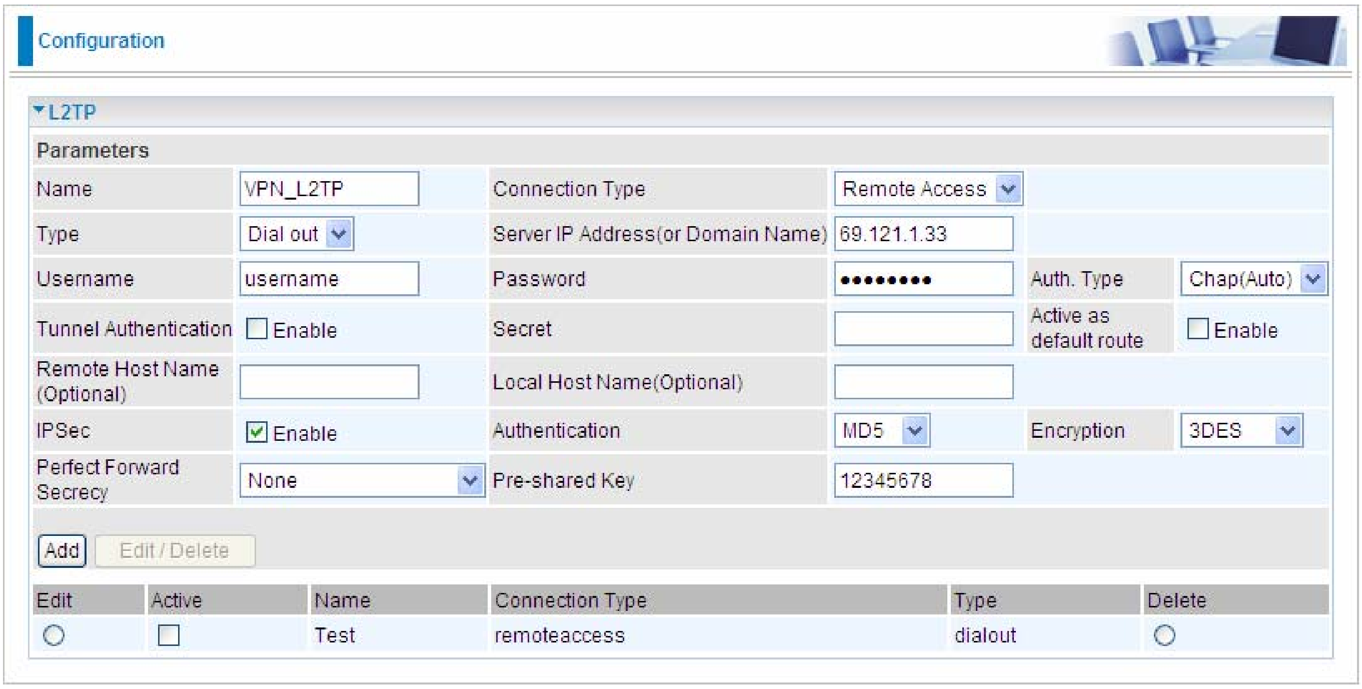
Item	Function		Description
1	Name	VPN_L2TP	Given a name of L2TP connection
2	Connection Type	Remote Access	Select Remote Access from Connection Type drop-down menu
3	Type	Dial in	Select Dial in from Type drop-down menu
	IP Address	192.168.1.200	An assigned IP address for the remote worker
4	Username	username	Input username & password to authenticate remote worker
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring a Remote Access L2TP VPN Dial-out Connection

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



Configuring the L2TP VPN in the Office



Configuration

▾L2TP

Parameters

Name	VPN_L2TP	Connection Type	Remote Access		
Type	Dial out	Server IP Address(or Domain Name)	69.121.1.33		
Username	username	Password	••••••••	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name (Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

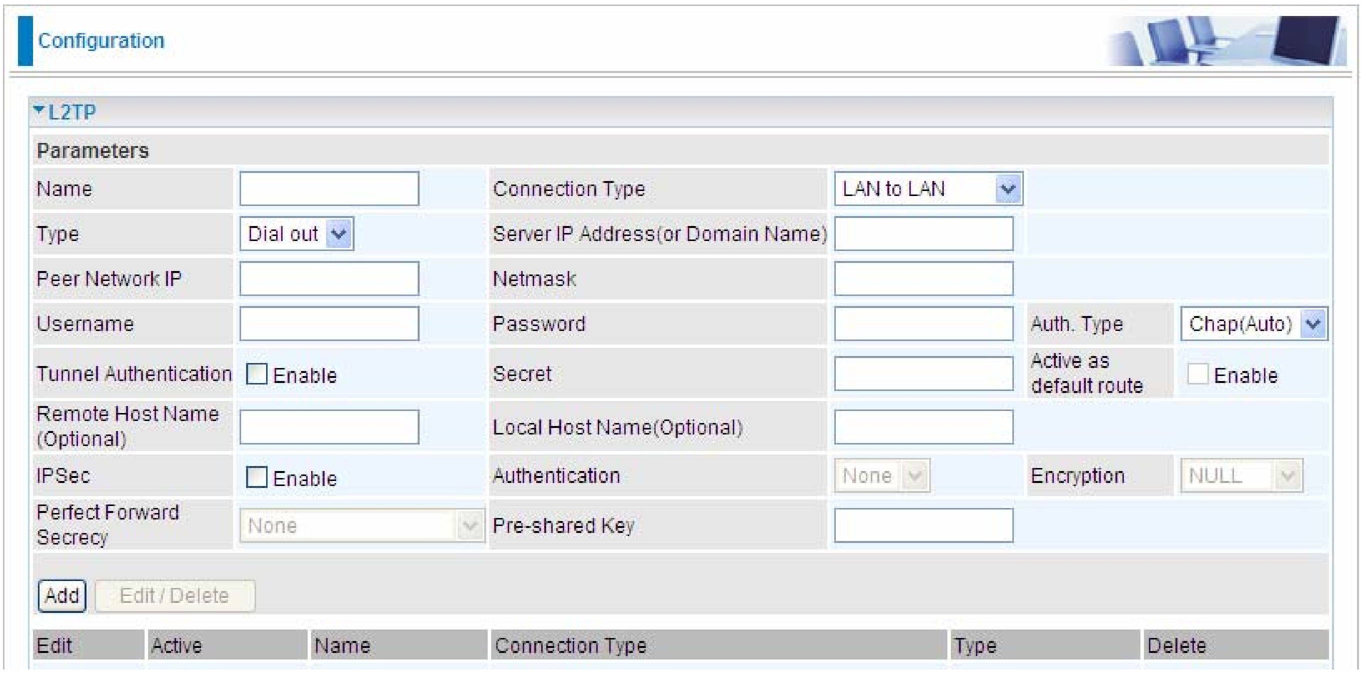
Edit	Active	Name	Connection Type	Type	Delete
○	□	Test	remoteaccess	dialout	○

Item	Function		Description
1	Name	VPN_L2TP	Given name of L2TP connection
2	Connection Type	Remote Access	Select Remote Access from Connection Type drop-down menu
3	Type	Dial out	Select Dial out from Type drop-down menu
	IP Address (or Hostname)	69.121.1.33	An Dialed server IP
4	Username	username	A given username & password
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Example: Configuring your Router to Dial-in to the Server

Currently, Microsoft Windows operation system does not support L2TP incoming service. Additional software may be required to set up your L2TP incoming service.

L2TP Connection - LAN to LAN



Configuration

▾L2TP

Parameters

Name		Connection Type	LAN to LAN		
Type	Dial out	Server IP Address(or Domain Name)			
Peer Network IP		Netmask			
Username		Password		Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name (Optional)		Local Host Name(Optional)			
IPSec	□ Enable	Authentication	None	Encryption	NULL
Perfect Forward Secrecy	None	Pre-shared Key			

Add Edit / Delete

Edit	Active	Name	Connection Type	Type	Delete

L2TP VPN Connection

Name: A given name of the connection.

Connection Type: Remote Access or **LAN to LAN.**

Active: This function activates or deactivates the L2TP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

Note: When the Active checkbox is checked, the function of Edit and Delete will not be available.

Type: Check **Dial Out** if you want your router to operate as a client (connecting to a remote VPN server, e.g. your office server), check **Dial In** operates as a VPN server.

j) When configuring your router establish the connection to a remote LAN, enter the remote **Server IP Address (or Hostname)** you wish to connection to.

k) When configuring your router as a server to accept incoming connections, enter the **Private IP Address Assigned to Dial in User** address.

Peer Network IP: Enter Peer network IP address.

Netmask: Enter the subnet mask of peer network based on the Peer Network IP setting.

Username: If you are a Dial-Out user (client), enter the username provided by your Host. If you are a Dial-In user (server), enter your own username.

Password: If you are a Dial-Out user (client), enter the password provided by your Host. If you are a Dial-In user (server), enter your own password.

Authentication Type: Default is **Auto** if you want the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that the client has not been replaced by an intruder.

Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Active as default route: As the connection type is LAN to LAN, this function will become to disable.

Remote Host Name (Optional): Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Cautious: This is only when the router performs as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. As default, Router's default Hostname is **home.gateway.**

IPSec: Enable for enhancing your L2TP VPN security.

Authentication: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA-1 is more resistant to brute-force attacks than MD5, however it is slower.

- ⊙ **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- ⊙ **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NULL**. NULL means it is a tunnel only with no encryption. 3DES and AES are more powerful but increase latency.

l) **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.

m) **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

n) **AES:** Stands for Advanced Encryption Standards, it uses 128 bits as an encryption method.

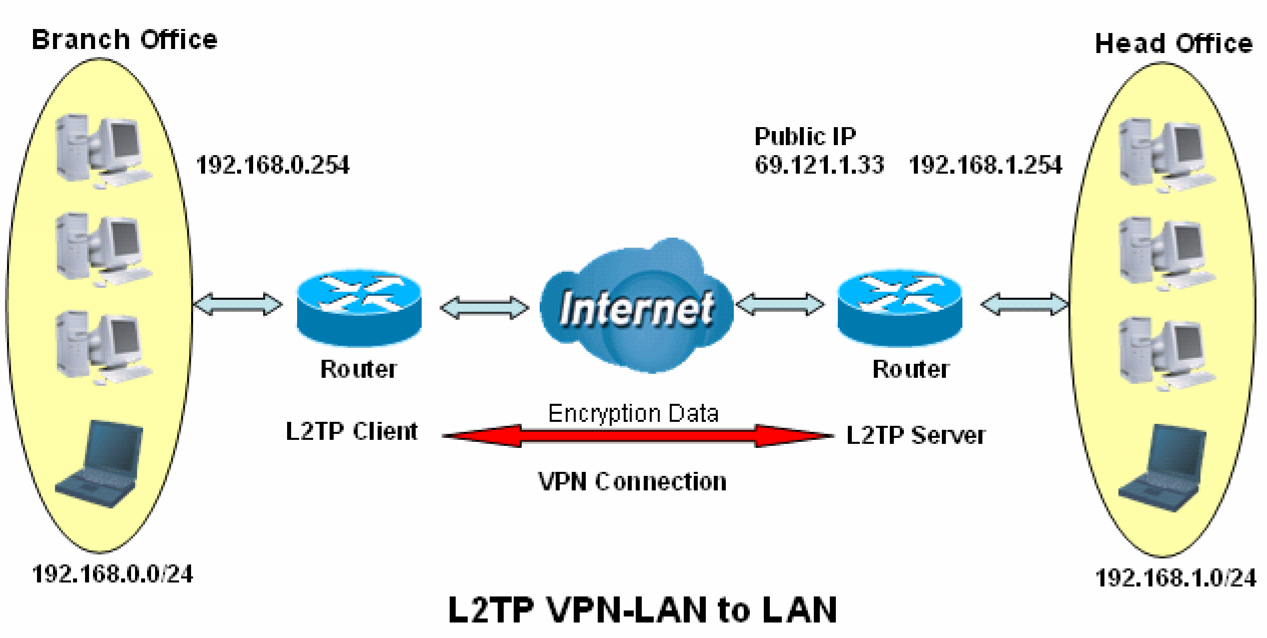
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). There are three modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Pre-shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Click **Edit/Delete** to save your changes.

Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.



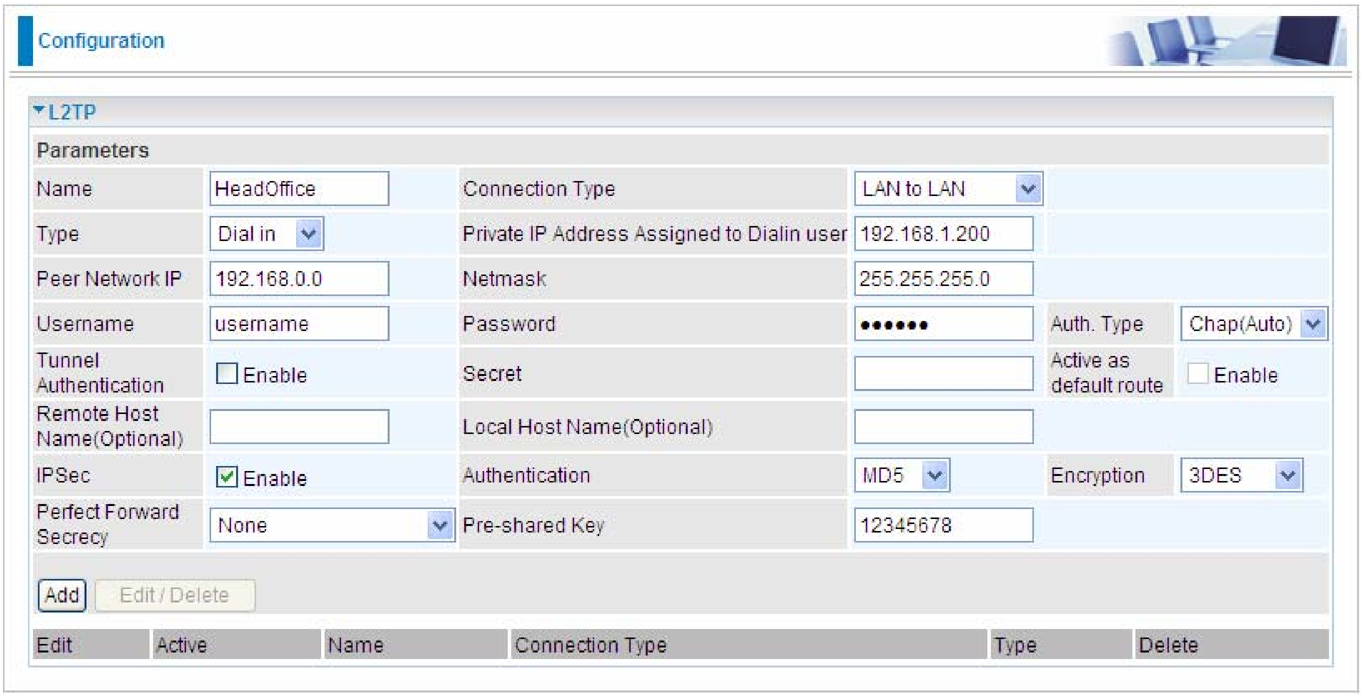
Attention

Both office LAN networks **MUST in different subnet** with LAN to LAN application.

Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.

Configuring L2TP VPN in the Head Office

The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.



Configuration

▾L2TP

Parameters

Name	HeadOffice	Connection Type	LAN to LAN		
Type	Dial in	Private IP Address Assigned to Dialin user	192.168.1.200		
Peer Network IP	192.168.0.0	Netmask	255.255.255.0		
Username	username	Password	••••••	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name(Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

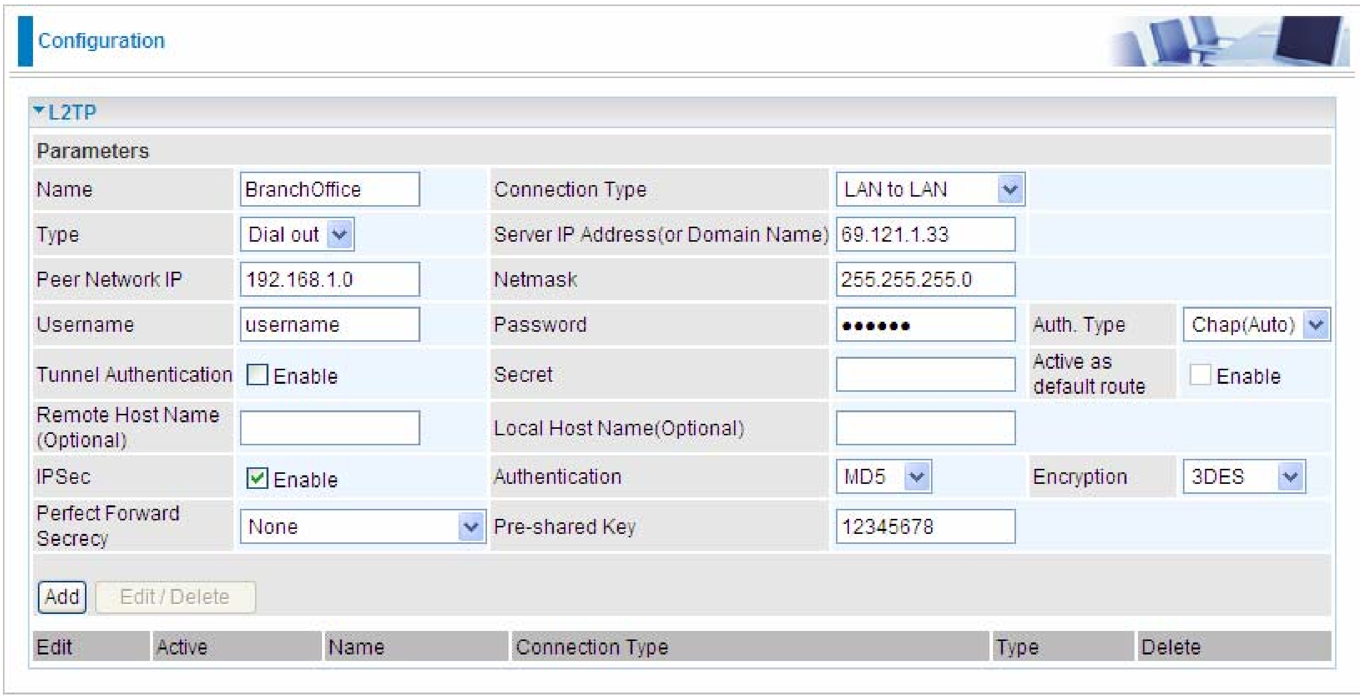
Add | Edit / Delete

Edit	Active	Name	Connection Type	Type	Delete

Item	Function		Description
1	Name	HeadOffice	Given a name of L2TP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from Connection Type drop-down menu
3	Type	Dial in	Select Dial in from Type drop-down menu
	IP Address	192.168.1.200	IP address assigned to branch office network
4	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate branch office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
7	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

Configuring L2TP VPN in the Branch Office

The IP address 69.121.1.33 is the **Public IP** address of the router located in head office. If you registered the DDNS (please refer to the **DDNS** section of this manual), you can also use the domain name instead of the IP address to reach the router.



Configuration

▾L2TP

Parameters

Name	BranchOffice	Connection Type	LAN to LAN		
Type	Dial out	Server IP Address(or Domain Name)	69.121.1.33		
Peer Network IP	192.168.1.0	Netmask	255.255.255.0		
Username	username	Password	••••••	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name (Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

Edit	Active	Name	Connection Type	Type	Delete

Item	Function		Description
1	Name	BranchOffice	Given a name of L2TP connection
2	Connection Type	LAN to LAN	Select LAN to LAN from drop-down menu
3	Type	Dial out	Select Dial out from drop-down menu
	IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
4	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Username	username	Input username & password to authenticate head office network
	Password	123456	
6	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
7	IPSec	Enable	Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

QoS - Quality of Service

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

Here are the items within the **QoS** section: **Prioritization** and **Outbound / Inbound IP Throttling** (bandwidth management).

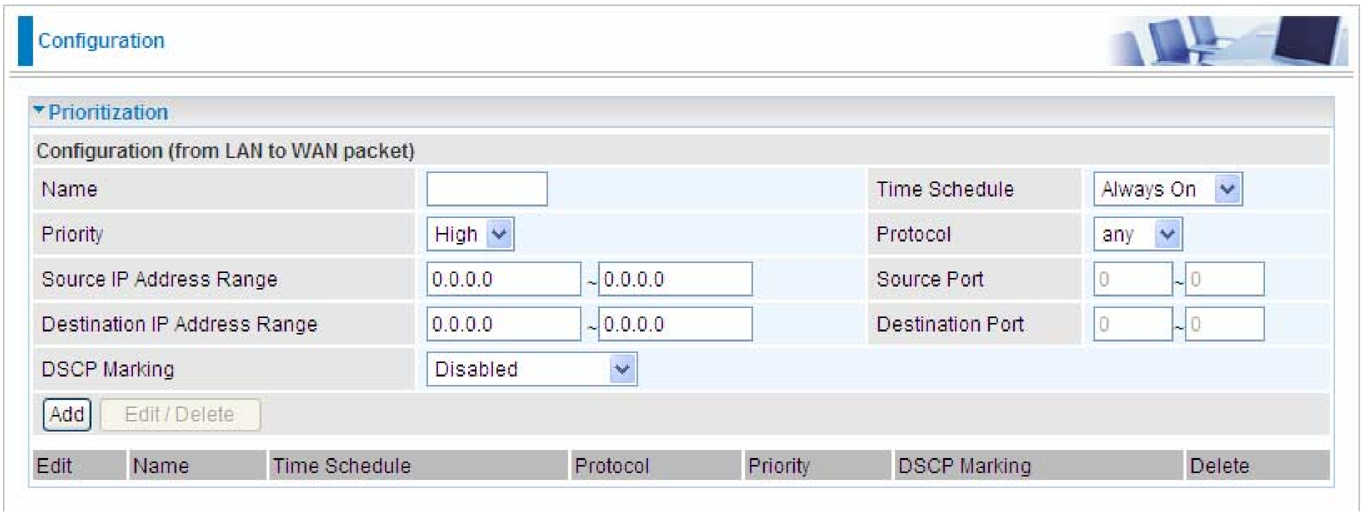
Prioritization

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**

And the balances of utilization for each priority are High (60%), Normal (30%) and Low (10%).

To delete the application, you can choose Delete option and then click Edit/Delete.



▾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-define description to identify this new policy/application.

Time Schedule: Scheduling 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 supported protocol.

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

Source Port: The source port of 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 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 assign specific application traffic to be executed in priority by the next Router based on the DSCP value. See Table 4. The DSCP Mapping Table:

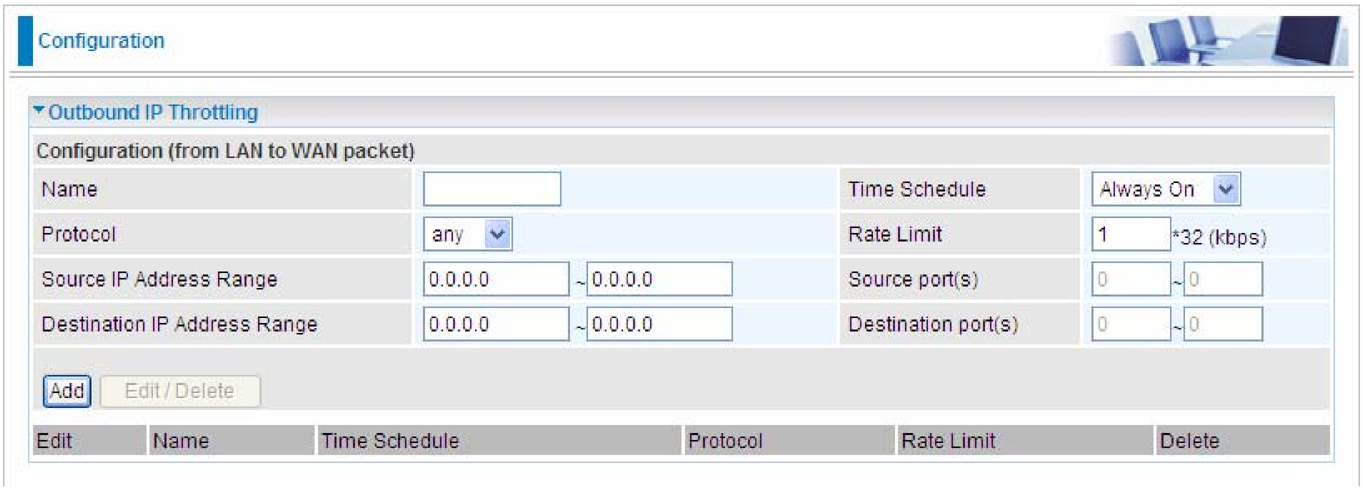
Note: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

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 IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.



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

Name: User-define description to identify this new policy/name.

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

Protocol: The name of supported protocol.

Rate Limit: To limit the speed of outbound traffic

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

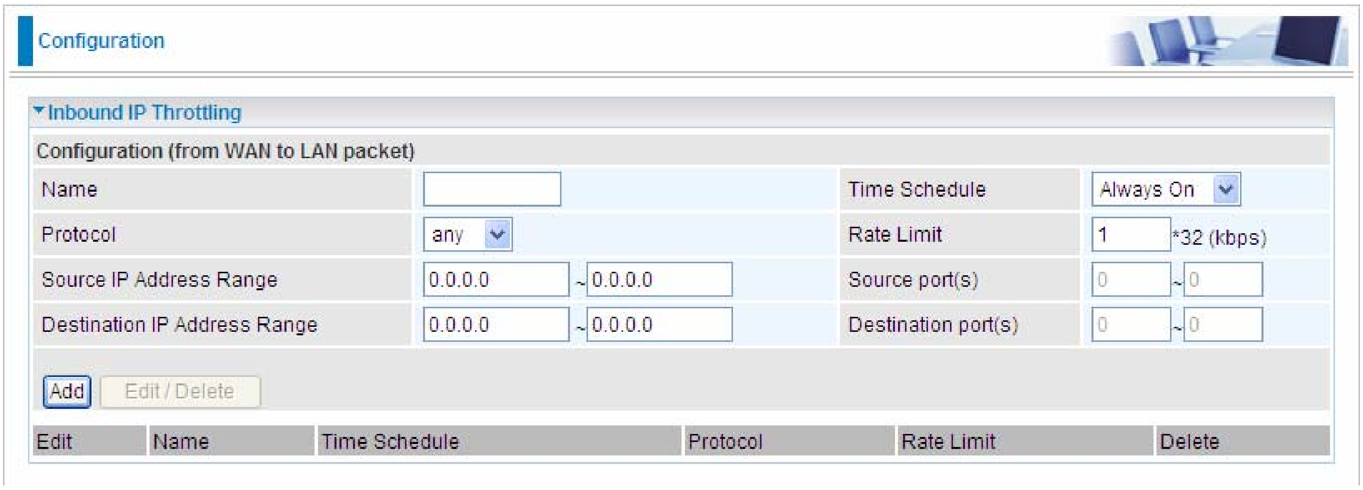
Source Port(s): The source port of packets to be monitored.

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

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

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the application that you set to the specified value's multiple of 32kbps.



Configuration

▾Inbound IP Throttling

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-define description to identify this new policy/application.

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

Protocol: The name of supported protocol.

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

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

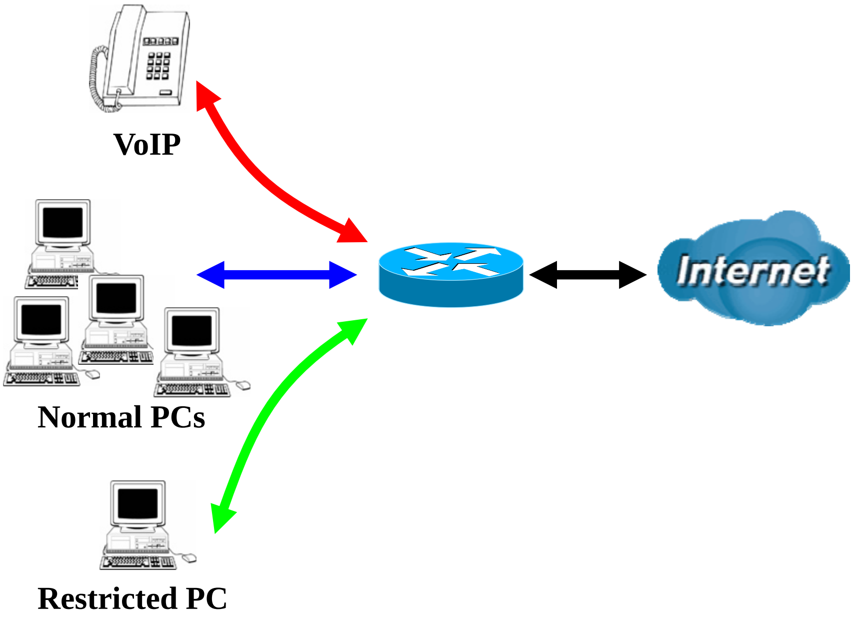
Source Port(s): The source port of packets to be monitored.

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

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

Example: QoS for your Network

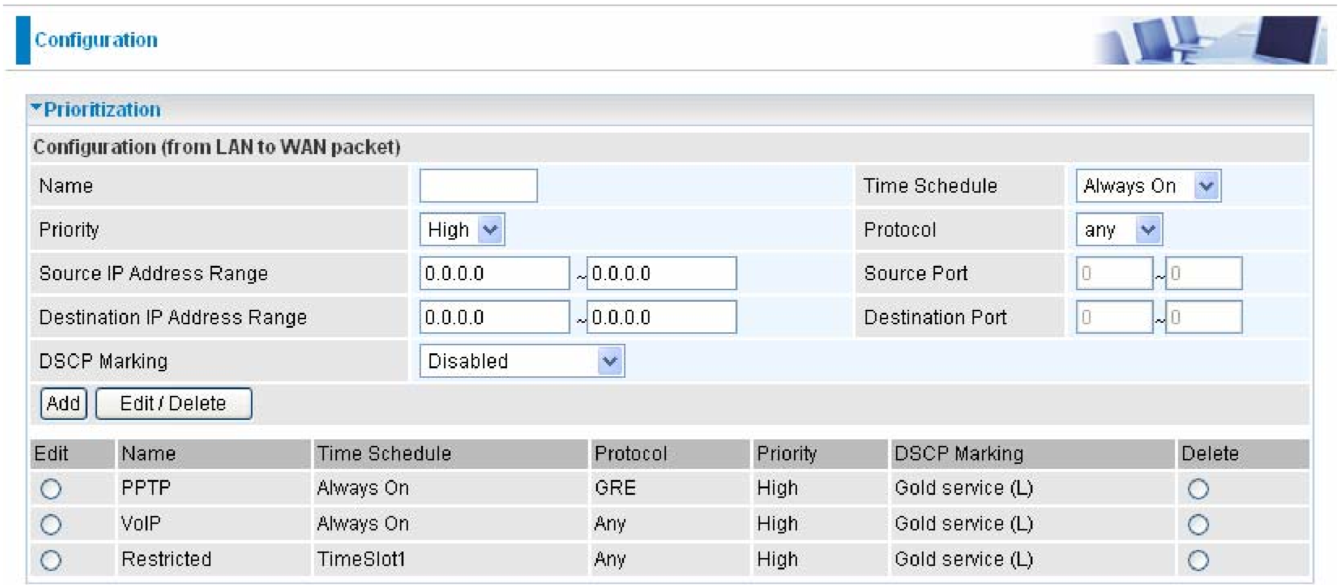
Connection Diagram



Information and Settings

Upstream: 928 kbps
Downstream: 8 Mbps

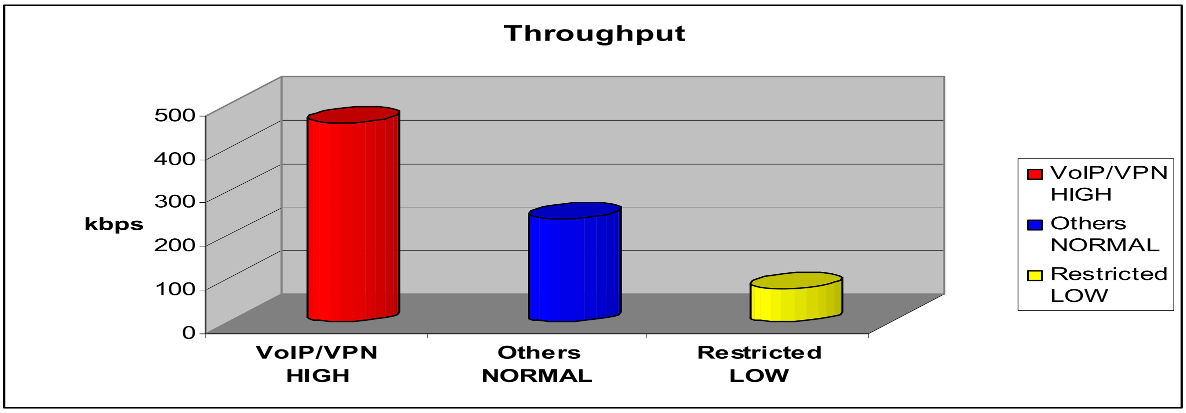
VoIP User : 192.168.1.1
Normal Users : 192.168.1.2~192.168.1.5
Restricted User: 192.168.1.100



Configuration (from LAN to WAN packet)

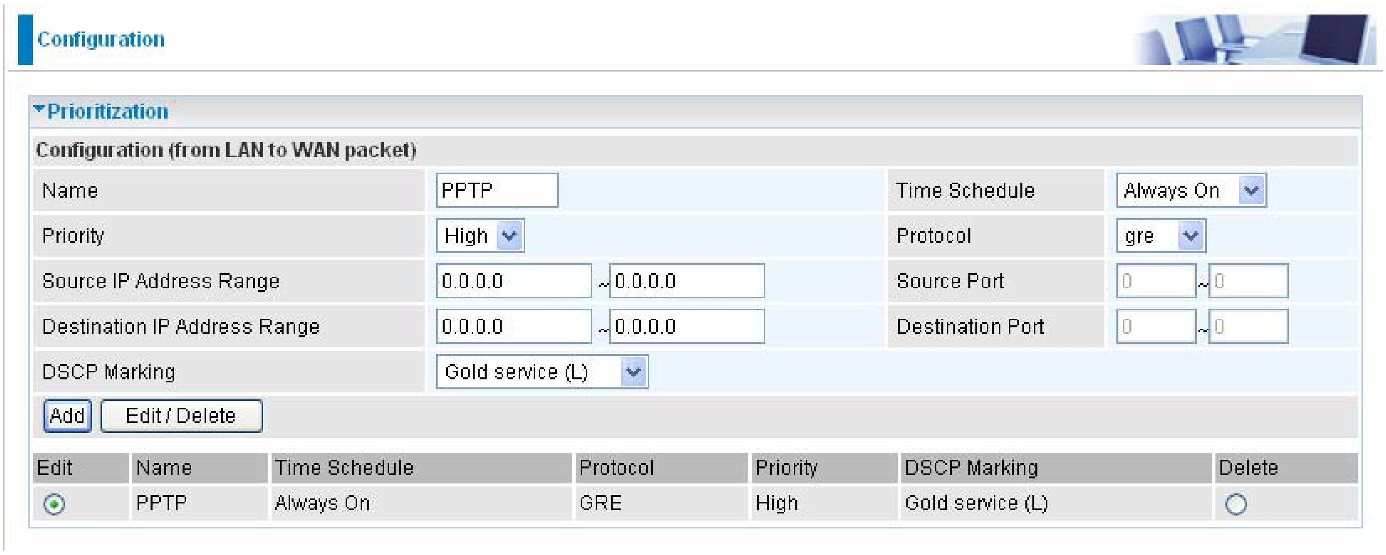
Name		Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled		

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)	○


Throughput
kbps
500
400
300
200
100
0
VoIP/VPN HIGH
Others NORMAL
Restricted LOW
🟥 VoIP/VPN HIGH
🟦 Others NORMAL
🟨 Restricted LOW

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)

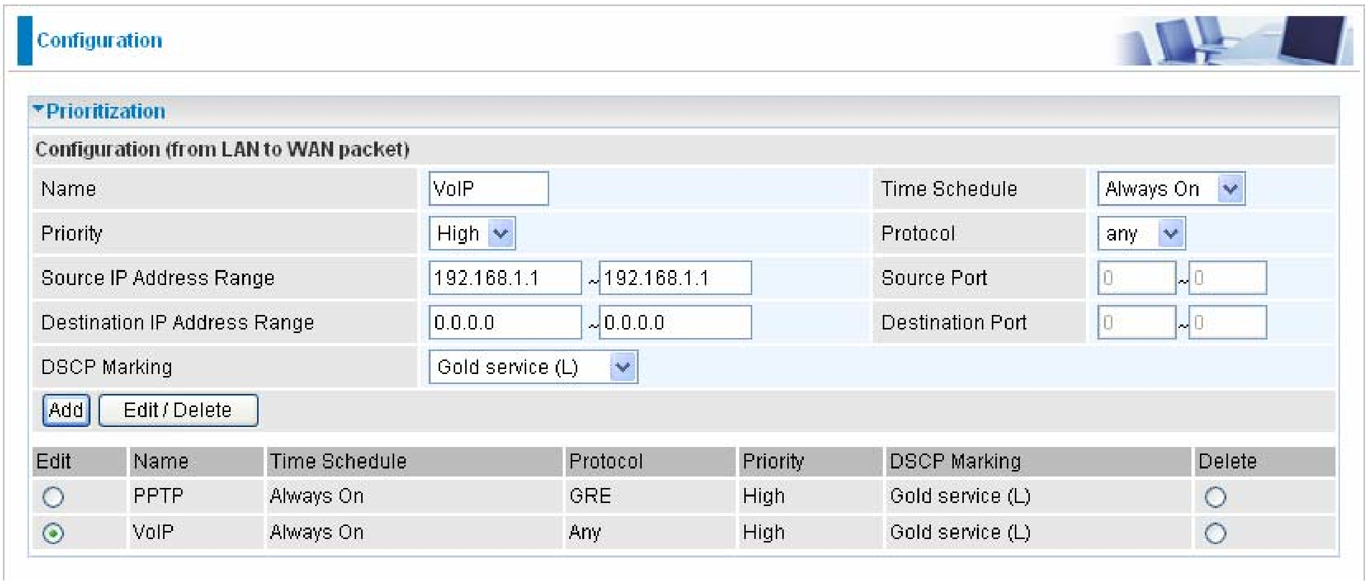
Name	PPTP	Time Schedule	Always On
Priority	High	Protocol	gre
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

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 dropping. Set priority as high level for preventing any other applications to saturate 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)

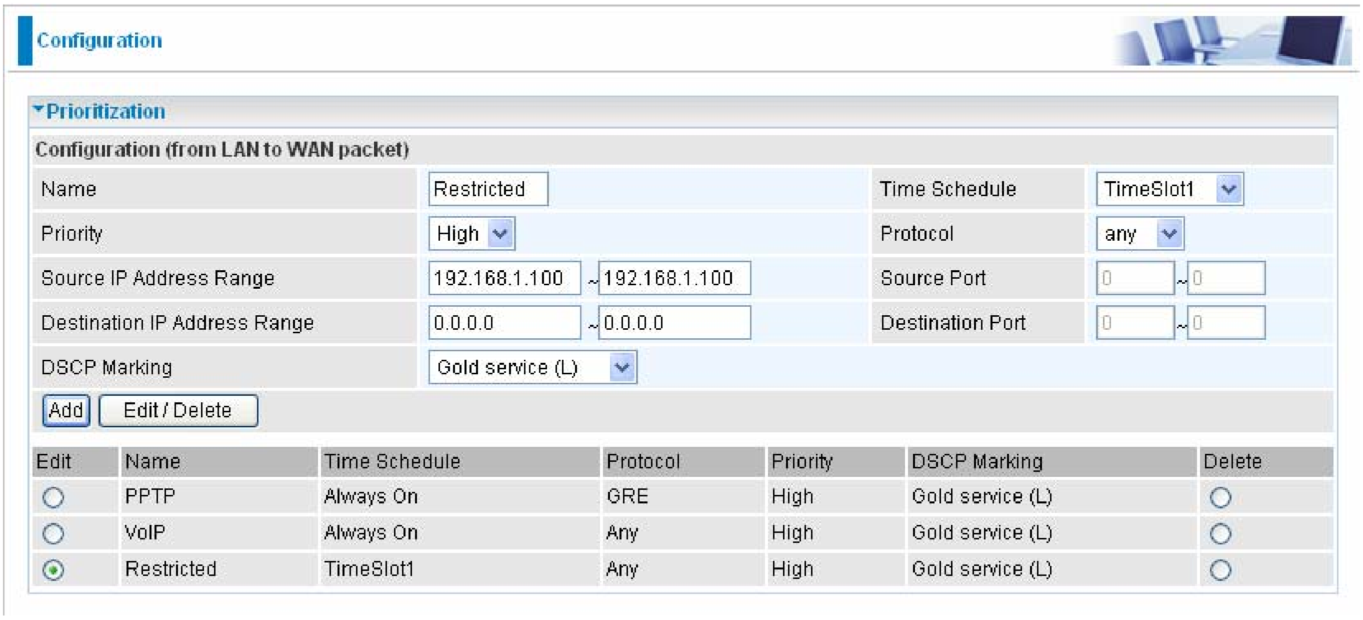
Name	VoIP	Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	192.168.1.1 ~ 192.168.1.1	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

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)	○

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

Restricted Application

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



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)	○

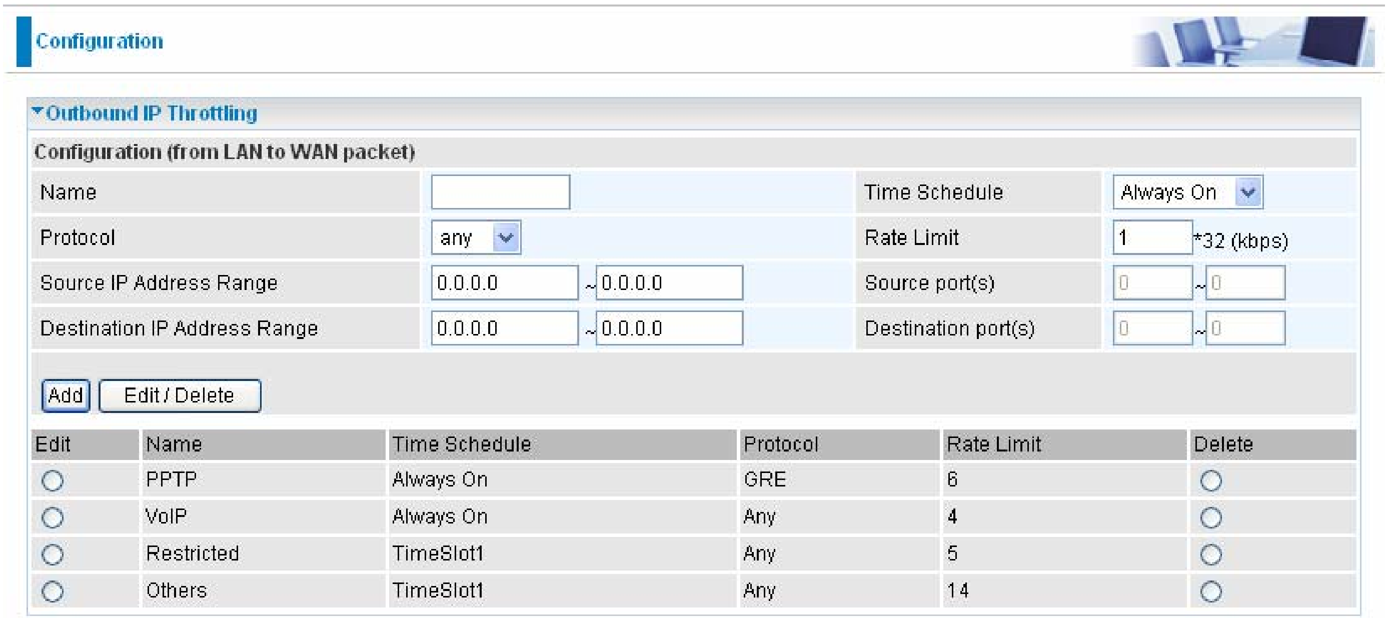
With above settings that help to limit utilization of upstream of FTP. Time schedule also help you to only limit utilization at daytime.

Advanced setting by using IP throttling

With IP throttling you can specify more detail for allocating bandwidth; even the applications are located in 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

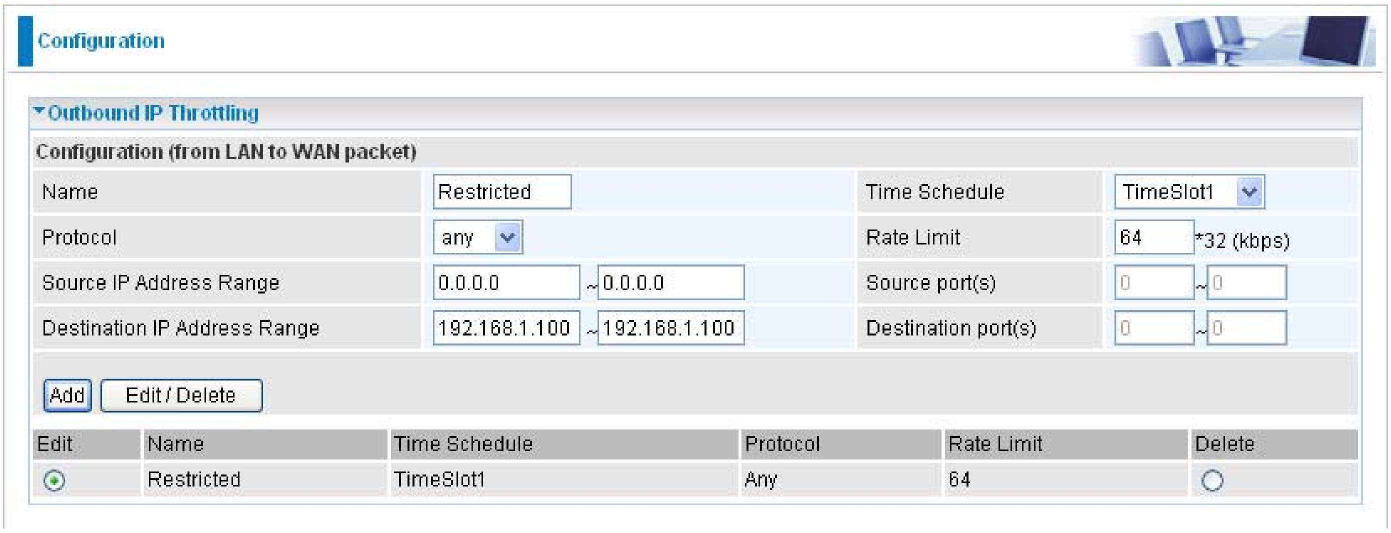
Outbound IP Throttling

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	○
○	VoIP	Always On	Any	4	○
○	Restricted	TimeSlot1	Any	5	○
○	Others	TimeSlot1	Any	14	○

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	TimeSlot1
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	TimeSlot1	Any	64	○

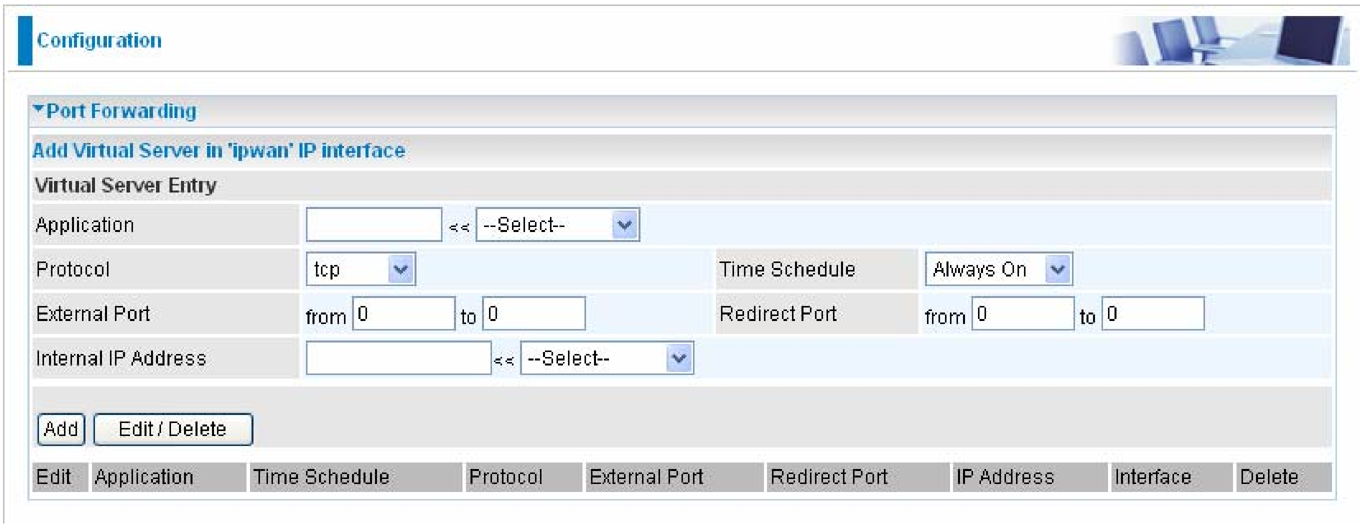
Virtual Server (known as Port Forwarding)

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



Configuration

Port Forwarding

Add Virtual Server in 'ipwan' IP interface

Virtual Server Entry

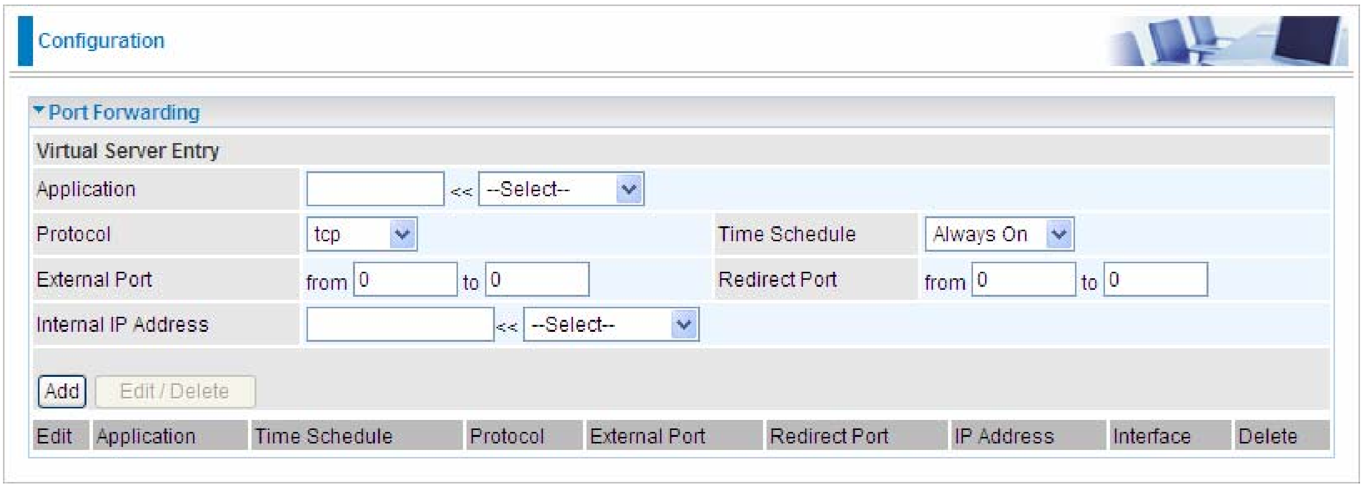
Application	<< --Select--		
Protocol	tcp	Time Schedule	Always On
External Port	from 0 to 0	Redirect Port	from 0 to 0
Internal IP Address	<< --Select--		

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 outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110), When an incoming access request to the router for a specified port is received, it will be forwarded to the corresponding internal server.



Configuration

Port Forwarding

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--		

Add　Edit / Delete

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

Application: Users-define description to identify this entry or click --Select-- drop-down menu to select 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 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 Always on for the usage of 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.

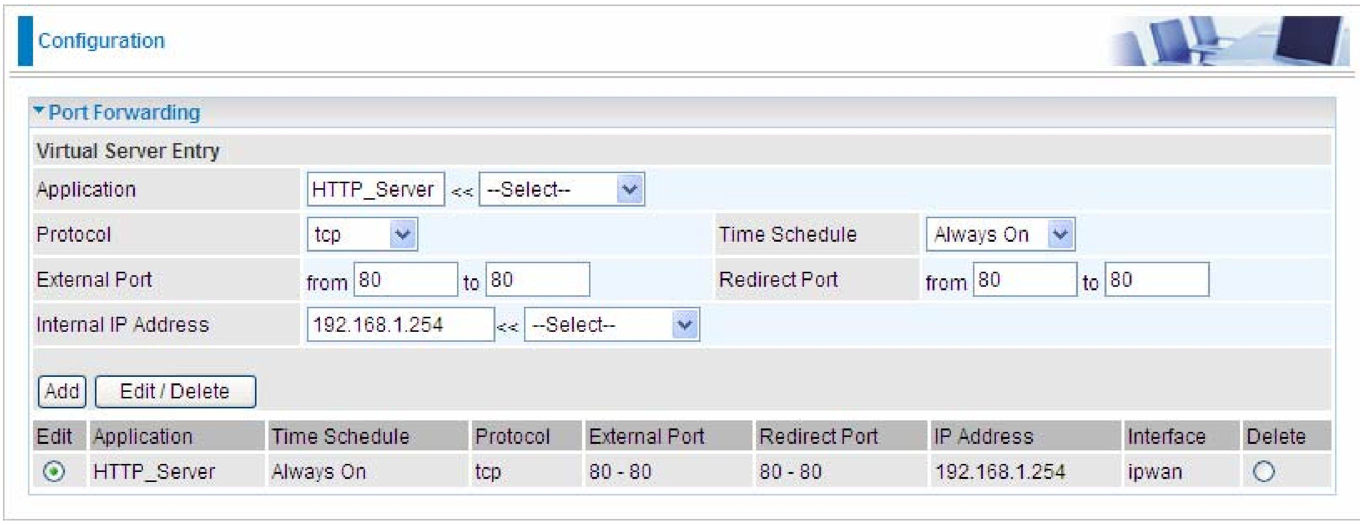
Redirect Port: The Port number used by the Local server in the LAN network.

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 remote accessing your Router through the Web/HTTP at all time, you would need to enable port number 80 (Web/HTTP) and map to Router's IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the **Application** click **Helper.** A list of predefined rules window will pop and 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*



Application	HTTP_Server << --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--		

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
●	HTTP_Server	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 security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

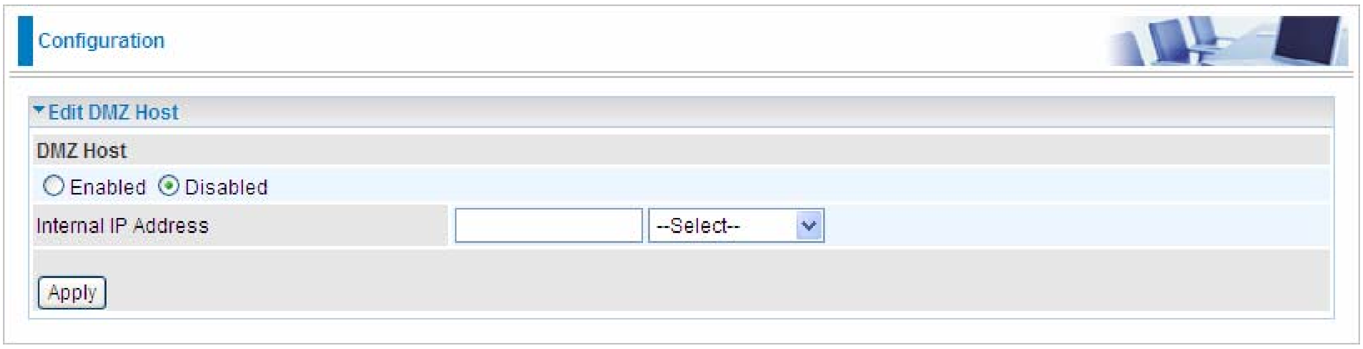
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into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

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

Cautious: This Local computer exposing to the Internet may face varies of security risks.

Go to **Configuration→Virtual Server→Edit DMZ Host**



DMZ Host
○ Enabled ● Disabled
Internal IP Address --Select--

o) **Enabled:** It activates your DMZ function.

p) **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 existing PCs connecting to the network. You may assign a PC with IP address and MAC from this list.

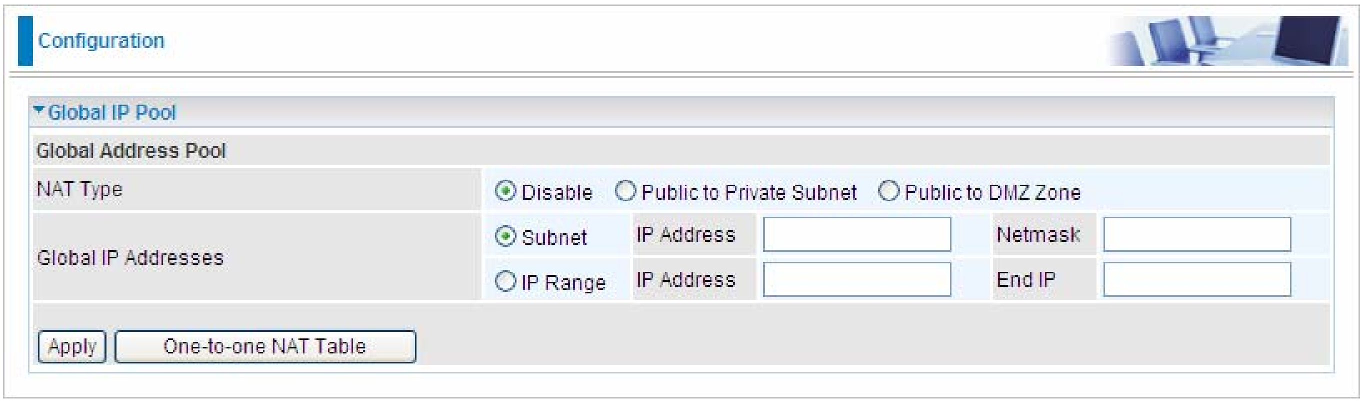
Select the **Apply** button to apply your changes.

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 you ISP, you are eligible for One-to-One NAT to utilize these IP addresses.

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 desired NAT type. As set in default setting, it disables the One-to-One NAT function.

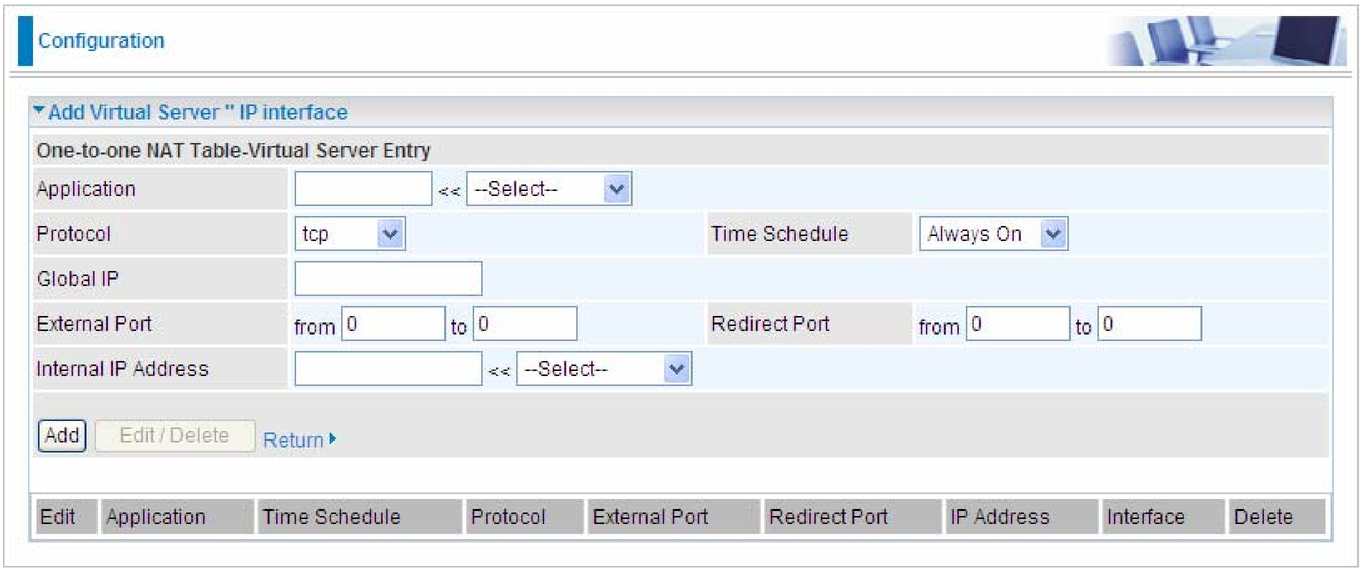
Global IP Address:

⊙ **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: 192.168.1.1, end IP: 192.168.1.10

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: Users-defined description to identify this entry or click --Select-- drop-down menu to select 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 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 Always on for the usage of this Virtual Server Entry. For setup and detail, refer to **Time Schedule** section

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

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.

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

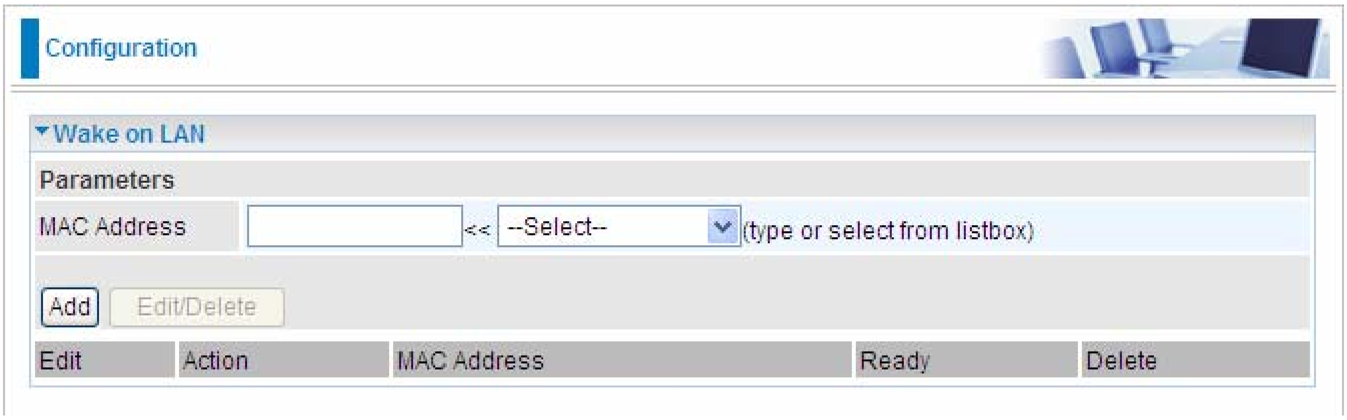
For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at: http://www.billion.com

Table 5: Well-known and registered Ports

Port Number	**Protocol**	**Description**
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / 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

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



Configuration

▾Wake on LAN

Parameters

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

Add | Edit/Delete

Edit	Action	MAC Address	Ready	Delete

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Add: After selecting, click Add then you can perform the Wake-up action.

Edit/Delete: Click to edit or delete the selected MAC address.

Ready: "Yes" indicating the remote computer is ready for your waking up.

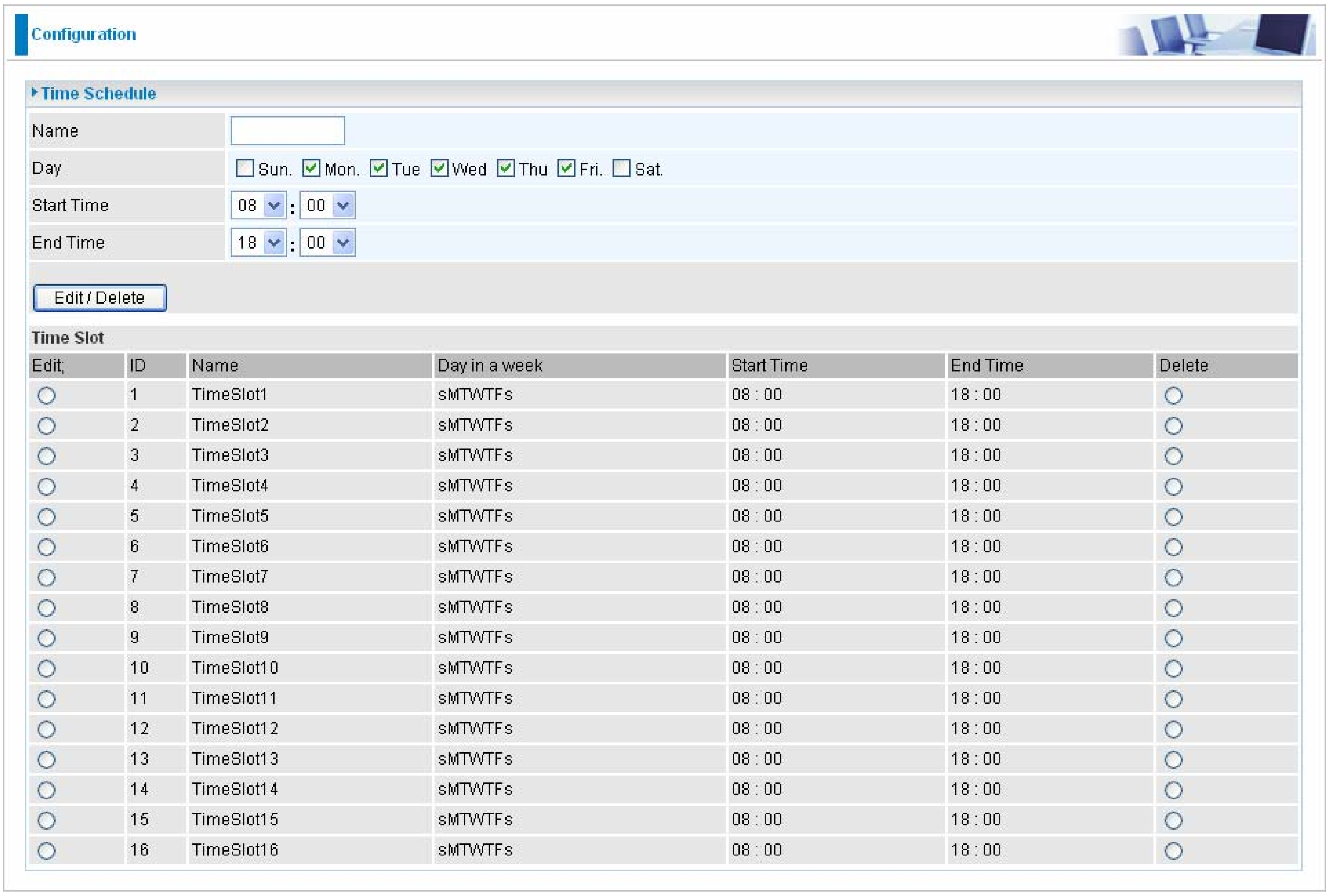
"**No"** indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

Time Schedule

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

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



Time Schedule

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

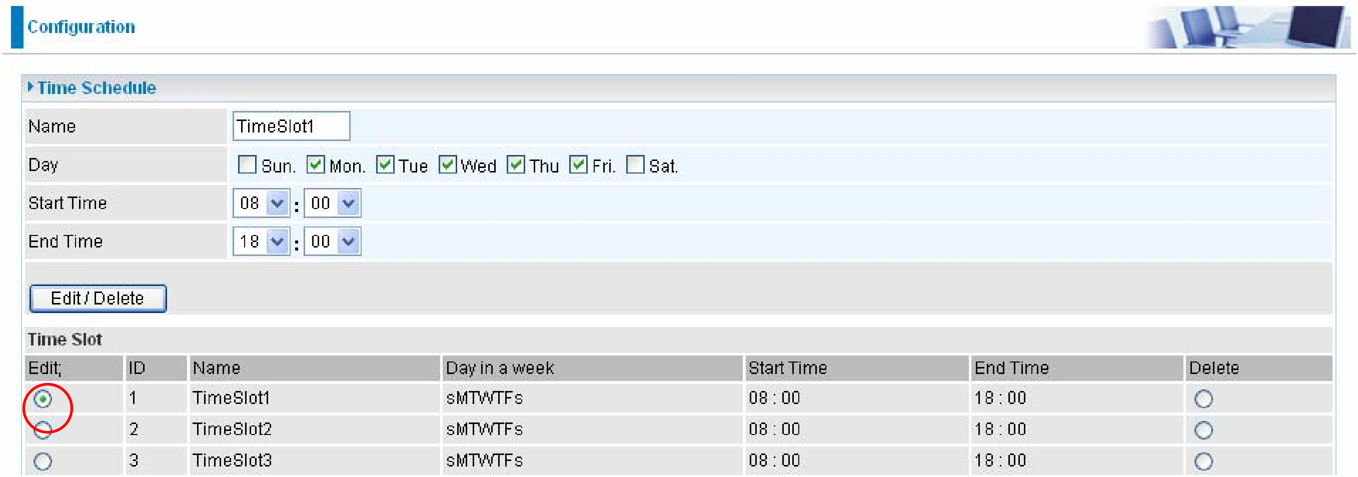
Time Slot

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**.**



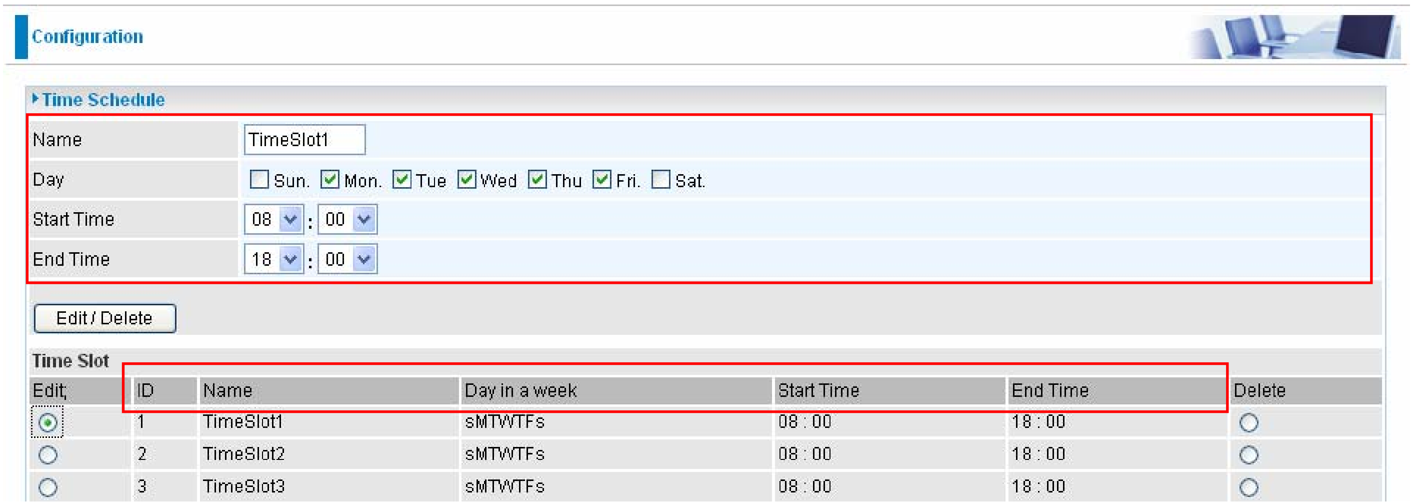
Name	TimeSlot1
Day	□ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. □ Sat.
Start Time	08 : 00
End Time	18 : 00

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.



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	○

ID: This is the index of the time slot.

Name: A user-define description to identify this time portfolio.

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

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

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

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

Delete a Time Slot

Choose Delete radio button, and click **Delete** button to delete the existing Time profile, i.e. erase the Day and back to default setting of Start Time / End Time.

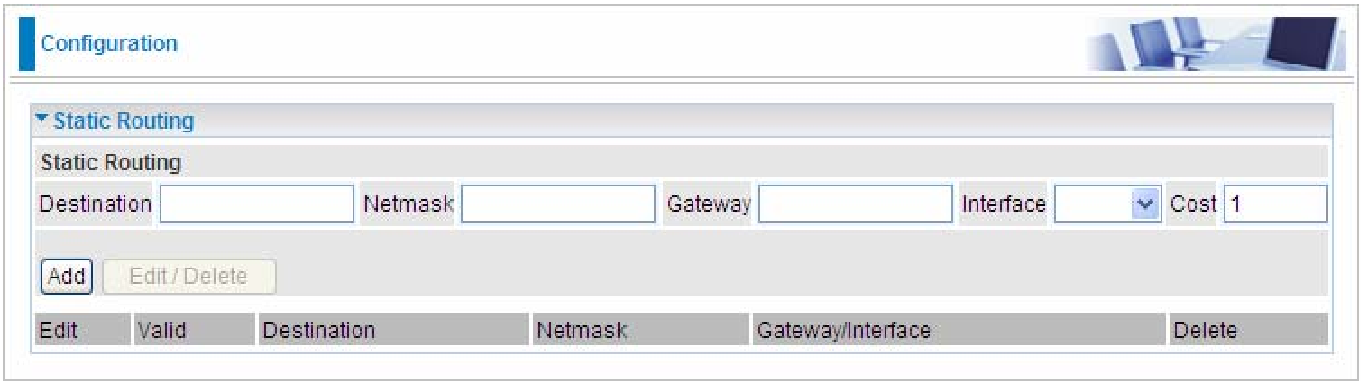
Advanced

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.

Here are the items within the **Advanced** section: **Static Route, Static ARP, Dynamic DNS, Device Management, IGMP** and **VLAN Bridge.**

Static Route

Go to Configuration/Advanced/Static Route.



Configuration

▾ Static Routing

Static Routing

Destination: | Netmask: | Gateway: | Interface: | Cost: 1

Add | Edit / Delete

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 above destination subnet IP.

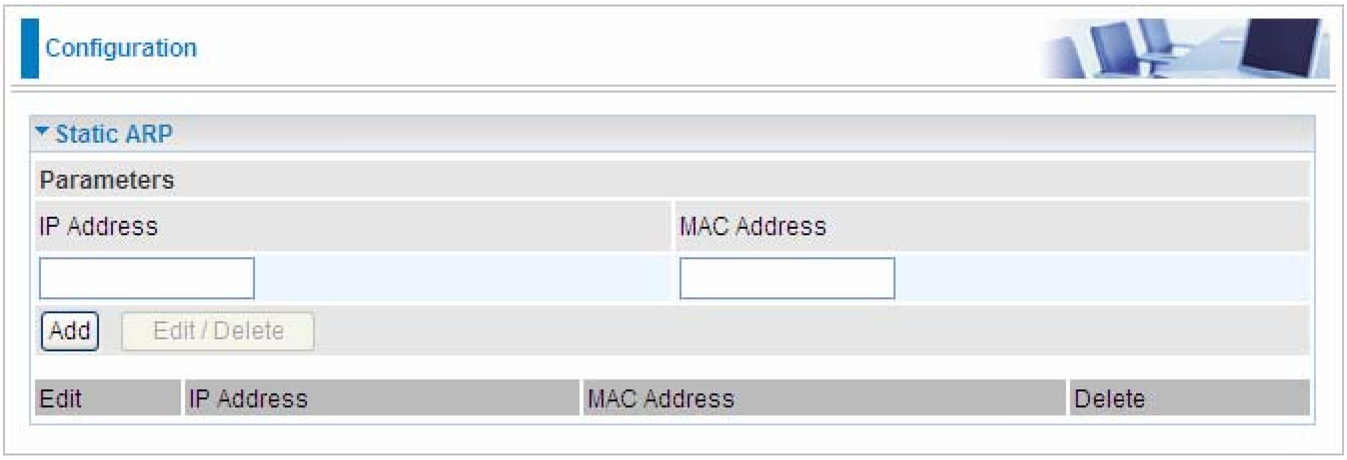
Gateway: This is the gateway IP address to which packets are to be forwarded.

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

Go to Configuration/Advanced/Static Route.



Configuration

▾ Static ARP

Parameters

IP Address: | MAC Address:

Add | Edit / Delete

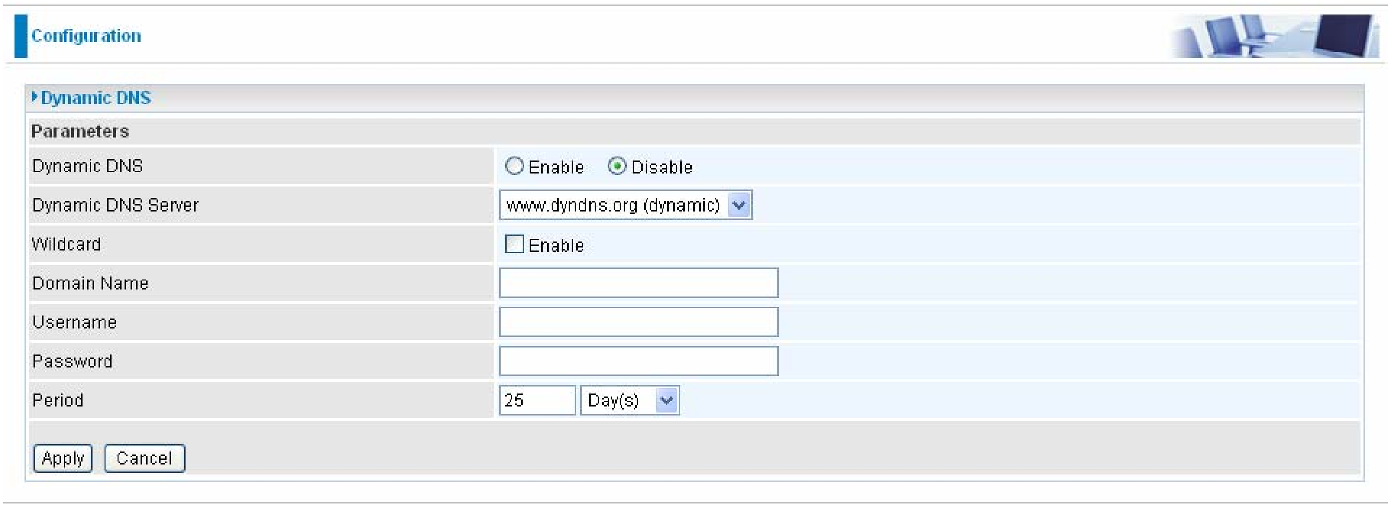
Edit	IP Address	MAC Address	Delete

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 ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



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)

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.

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:

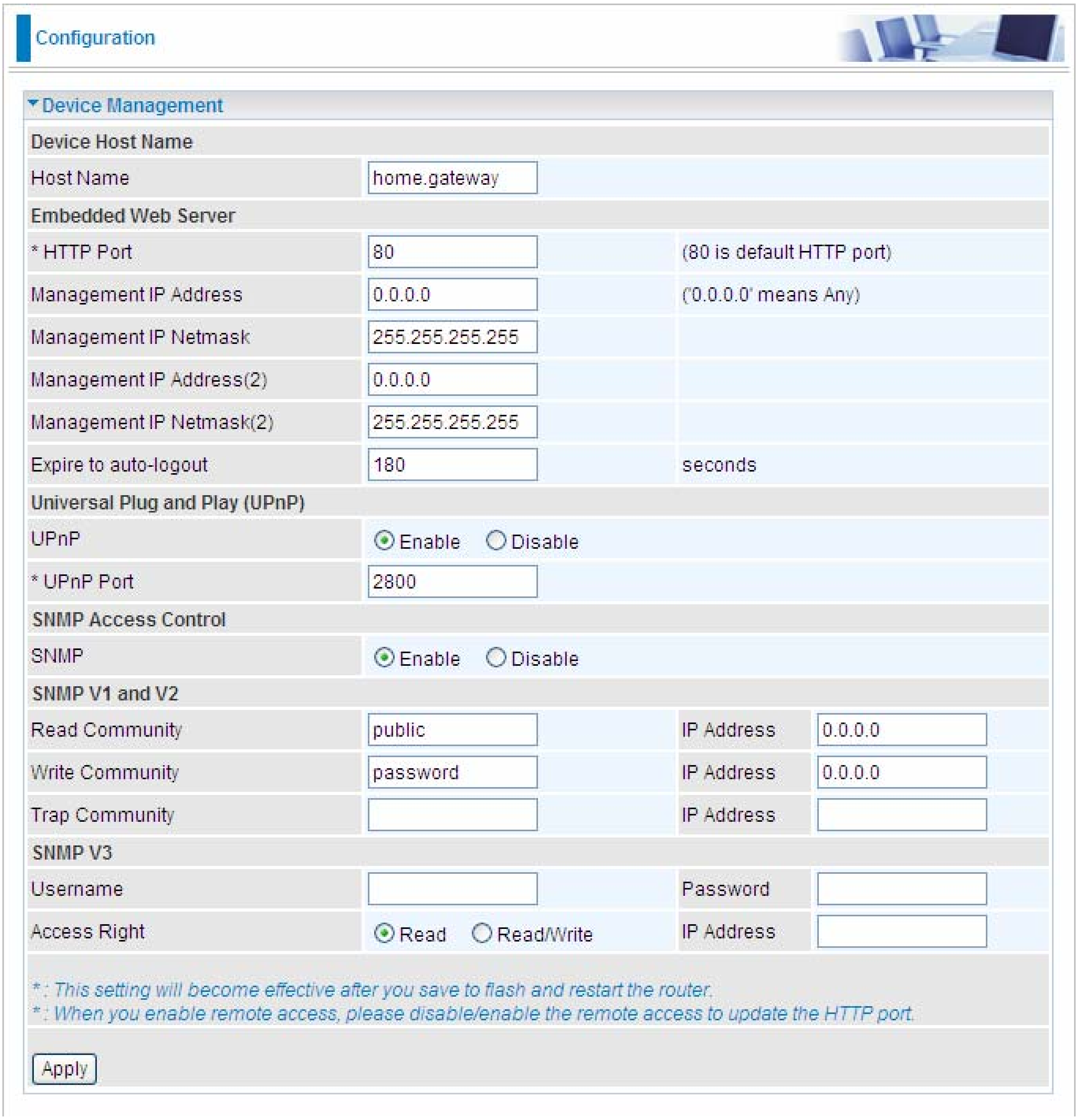
Dynamic DNS Server: Select the DDNS service you have established an account with.

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.

Device Management

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



Configuration

▾Device Management

Device Host Name			
Host Name	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: Give a name for it.

(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.
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 the router's 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 allowed to logon and access the router's 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 time frame for the system to auto-logout the user's configuration session.

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

Universal Plug and Play (UPnP)

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

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

- ⦿ **Disable:** Check to disable the router's UPnP functionality.
- ⦿ **Enable:** Check to enable the router's UPnP functionality.

UPnP Port: 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.

- ⦿ **Disable:** Check to disable the router's SNMP functionality.
- ⦿ **Enable:** Check to enable the router's SNMP functionality.

SNMP V1 and V2:

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

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

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

SNMP V3:

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

SNMP Version: SNMPv2c and SNMPv3

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

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

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

- ☑ System group
- ☑ Interfaces group
- ☑ Address Translation group
- ☑ IP group
- ☑ ICMP group
- ☑ TCP group
- ☑ UDP group
- ☒ EGP (not applicable)
- ☑ Transmission
- ☑ SNMP group

From RFC1650 (EtherLike-MIB):

- ☑ dot3Stats

From RFC 1493 (Bridge MIB):

- ☑ dot1dBase group
- ☑ dot1dTp group
- ☑ dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

- ☑ pppLink group
- ☒ pppLqr group (not applicable)

From RFC 1472 (PPP/Security MIB):

- ☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- ☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- ☑ PPP Bridge Group

From RFC1573 (IfMIB):

☑ ifMIBObjects Group

From RFC1695 (atmMIB):

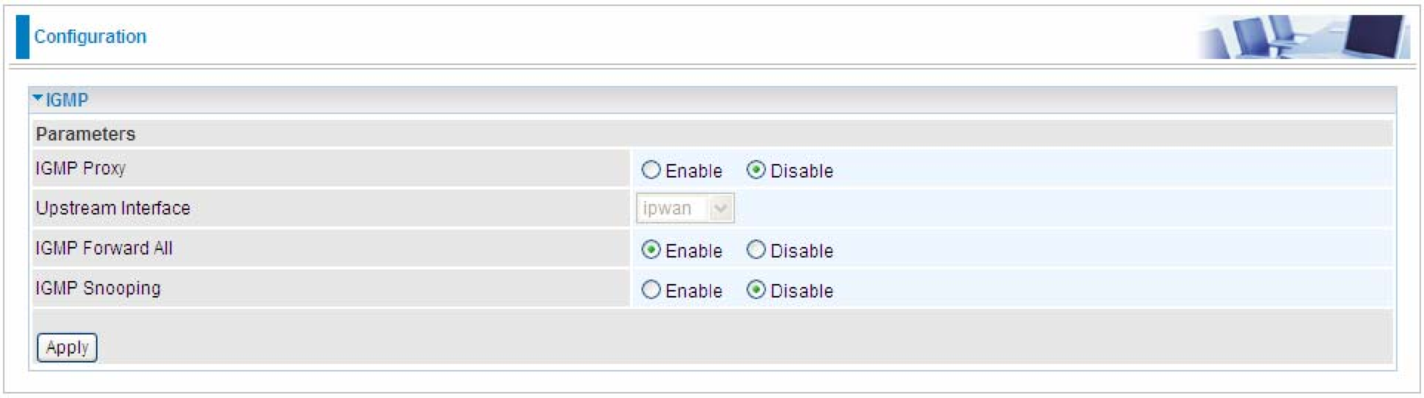
☑ atmMIBObjects

From RFC 1907 (SNMPv2):

☑ only snmpSetSerialNo OID

IGMP

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



Configuration

▾IGMP

Parameters	
IGMP Proxy	○ Enable ● Disable
Upstream Interface	ipwan
IGMP Forward All	● Enable ○ Disable
IGMP Snooping	○ Enable ● Disable

Apply

IGMP Proxy: Enables or disables the router’s IGMP Proxy.

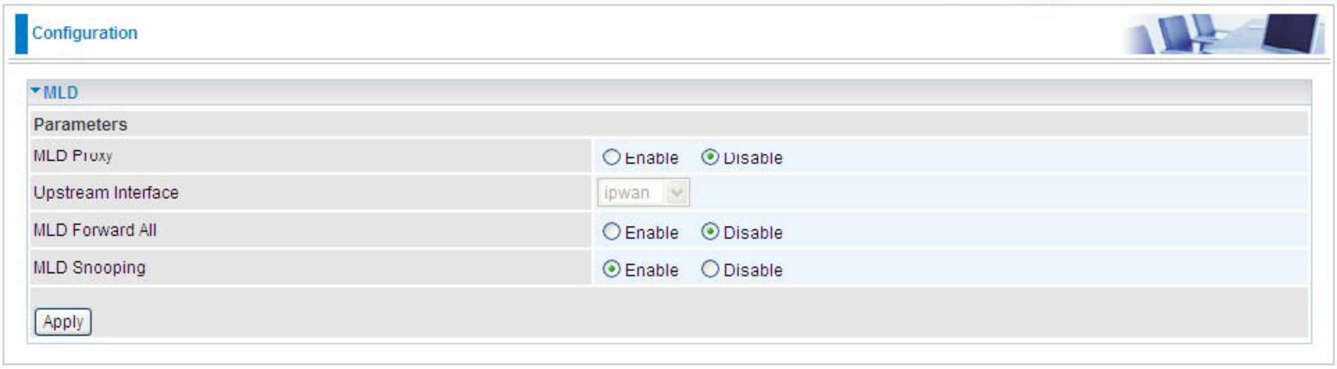
Upstream Interface: When IGMP Proxy enabled, sets one of the router’s existing IP interfaces as the upstream interface; all other router interfaces are designated downstream interfaces.

IGMP Forward All: Enables/Disables your router’s ability to forward multicast traffic to ALL interfaces.

IGMP Snooping: Enables/Disables the IGMP Snoop functionality in the bridge. When the IGMP snoop functionality is enabled, all the attached bridge interfaces are designated as downstream interfaces.

MLD

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.



Configuration

▾MLD

Parameters	
MLD Proxy	○ Enable ● Disable
Upstream Interface	ipwan
MLD Forward All	○ Enable ● Disable
MLD Snooping	● Enable ○ Disable

Apply

MLD Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients and forwards it to the router after some dealings. Support MLDv1 and MLDv2.

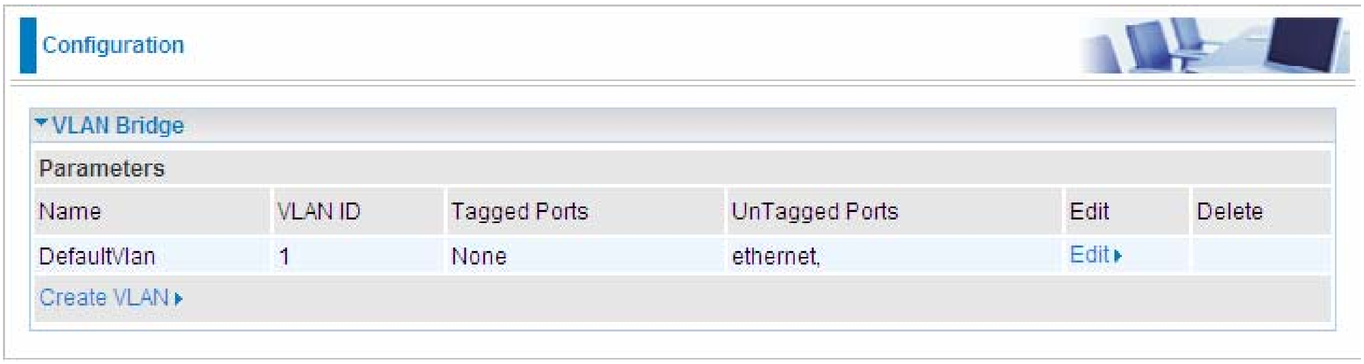
Upstream Interface: When MLD Proxy enabled, sets one of the router’s existing IP interfaces as the upstream interface; all other router interfaces are designated downstream interfaces.

MLD Forward All: select enable to forward the multicast packets to all ports. If select disable, the multicast packets will be forwarded to ports set according to the MLD Snooping below.
MLD Snooping: similar to IGMP snooping, listens in on the MLD conversation between hosts and

routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

VLAN Bridge

This section allows you to create VLAN group and specify the member.



Parameters					
Name	VLAN ID	Tagged Ports	UnTagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,	Edit ▸	
Create VLAN ▸					

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

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

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting your service provider or Billion support.

Problems starting up the router

Problem	*Corrective Action*
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with the WAN Interface

Problem	*Corrective Action*
Initialization of the PVC connection (“linesync”) failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router GE. If you still have problems, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Problems with the LAN Interface

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

APPENDIX A: Product Support and Contact Information

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Billion

WORLDWIDE

http://www.billion.com/