Micronet®
Faster and Easier Networks

User's Manual

ADSL2+ VPN Modem Router

Model No.: SP3366

World Wide Web: www.micronet.com.tw ; www.micronet.info

Table of Contents

Certifications

FCC

This equipment has been tested and found to comply with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference
(2) This device must accept any interference received. Include interference that may cause undesired operation.

CE

This equipment is in compliance with the requirements of the following regulations:
EN 55 022: CLASS B.

RoHS

All contents of this package, including products, packing materials and documentation comply with RoHS.

Chapter 1 Introduction

Micronet SP3366, ADSL2+ VPN Modem Router, delivers highly reliable and scalable network environment. The model has incorporated both modem and router functions into a single unit with VPN support. The modem router allows multiple network devices to share the single Internet connection via ADSL. Sustain network security via router's in-built firewall and DMZ functions. In addition, the scope of the network can be easily expanded by connecting the router to a hub or switch.

1.1 Package Contents

Prior to the installation of the device, please verify the following items are in the package:

- SP3366 ADSL2+ Modem Router
- Quick Installation Guide
- Product CD
- RJ-45/RJ-11 Cables
- RJ-45-RS232 Console Kit
- Power Adapter

Note: *Contact your dealer immediately if any of the above items are missing, damaged, or if the unit does not work.*

1.2 Key Features

- Compliant with ADSL/ADSL2/2+ standards.
- Provide 16 IPSec Virtual Private Network (VPN) connections with powerful 3DES accelerator.
- Quality of Service (QoS) via Traffic Prioritization and Bandwidth Management.
- Support CPE WAN Management Protocol (TR-069) for remote configuration of client side devices.

- Support IGMP Snooping for reducing Multicast traffic to enhance video service.
- In-built Firewall Security with DoS Prevention and SPI for secure networks.
- Support advanced router functions: Static Route, Virtual Sever, DDNS and UPnP.
- Monitoring network traffics through Event, Error and Firewall logs.

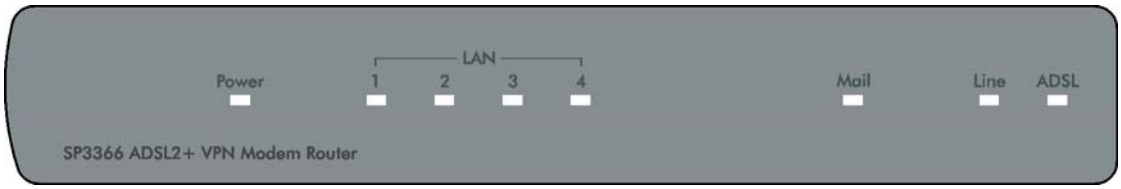
1.3 Specifications

Standards	• ANSI T1.413 ,Issue 2 • G.dmt (ITU G.992.1) • G.lite (ITU G.992.2) • G.hs (ITU G994.1) • G.dmt.bis (ITU G.992.3) • G.dmt.bis.plus (ITU G.992.5)
Interface	• WAN Port: 1 x Port 10/100Mbps RJ-11 • LAN Ports: 4 x Port 10/100Mbps RJ-45
WAN Connection	• PPPoA • PPPoE • IPoA • ATM (Bridge & Routed)
DHCP	DHCP Server & Client
Routing	• NAT/NAPT (Network Address Translation) • Static and RIP1/2 Routing
Advance Features	• Support NAT • DNS Relay • DDNS • QoS • Virtual Server • VLAN Bridge

	• IGMP • UPnP • ALG
Security Features	• Firewall (DoS & SPI) • IP Filtering • Packet Filter • URL Filter • IM/ P2P Blocking
Status Log	• Event Log • Error Log • Packet Filter • Firewall Log
Management	• Web-based Interface • SNMP • Telnet
Power	12V DC, 1A
Humidity	20 ~ 95% (Non-Condensing)
Temperature	• Operating: 0 ~ 40°C • Storage: -20 ~ 70°C
Certification	FCC, CE

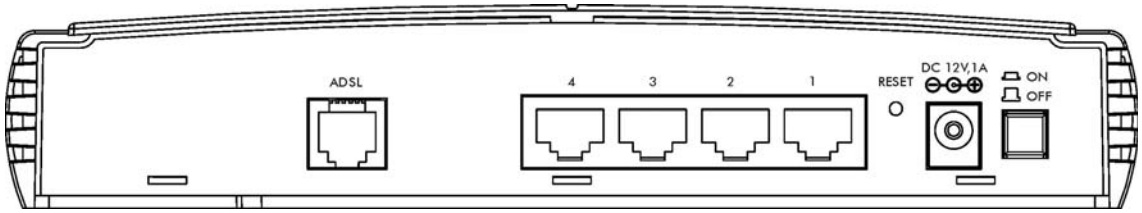
Chapter 2 Tour of Product

2.1 Front Panel



LED	Status	Description
Power	Green	Device is switched on.
	Red	System failure. Restart device.
	Off	No power.
LAN (1-4)	Green	LAN port is connected and operating at 100Mbps.
	Amber	LAN port is connected and operating at 10Mbps.
	Flashing	Data is being sent or received.
Mail	Flashing	Received emails in the inbox.
Line	Green	Device successfully connected to DSLAM (line sync).
ADSL	Green	WAN IP successfully assigned.
	Red	Unable to obtain WAN IP from ISP.

2.2 Back Panel

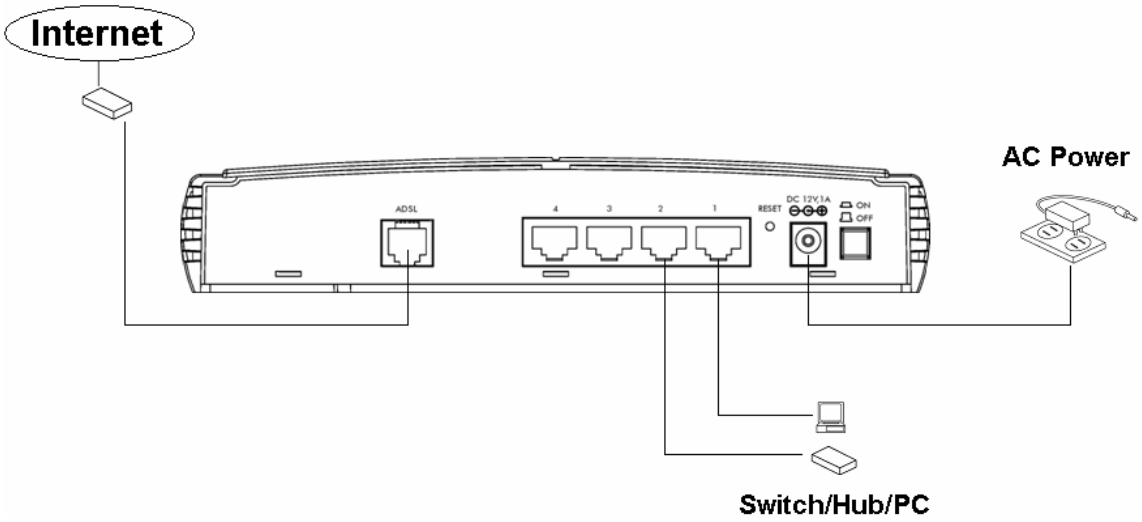


Parameter	Description
Power	Power connector for connecting to power source.
On/Off	For powering device on and off.
Reset	Press and hold this button for more than 6 seconds to reset settings back to factory default.
LAN 1~4	Local Area Network (LAN) ports for 1 to 4.
ADSL	Connection to RJ-11 telephone line for Internet.

Chapter 3 Hardware and Network Setup

3.1 Build Network Connection

To install the SP3366 Modem Router, please perform the following steps:



Step 1. Connect the ADSL port of modem router by telephone cable (RJ-11) to an outlet or splitter.

Step 2. Connect the LAN port to an active PC, switch, or hub using an Ethernet cable (RJ-45).

Step 3. Connect the 12V DC power adapter to a power outlet.

Step 4. Connect the adaptor to the power port on the back of the router. Switch device on using On/Off button.

Step 5. Check the LED indicators to verify that the device is detecting connection on Line and LAN.

Warning: Using an alternate power supply, other than the one supplied, may cause the router to malfunction.

3.2 Connecting to Web-Based Management

After the network connection is established, the next step is to setup the modem router with proper network parameters for the user's network environment.

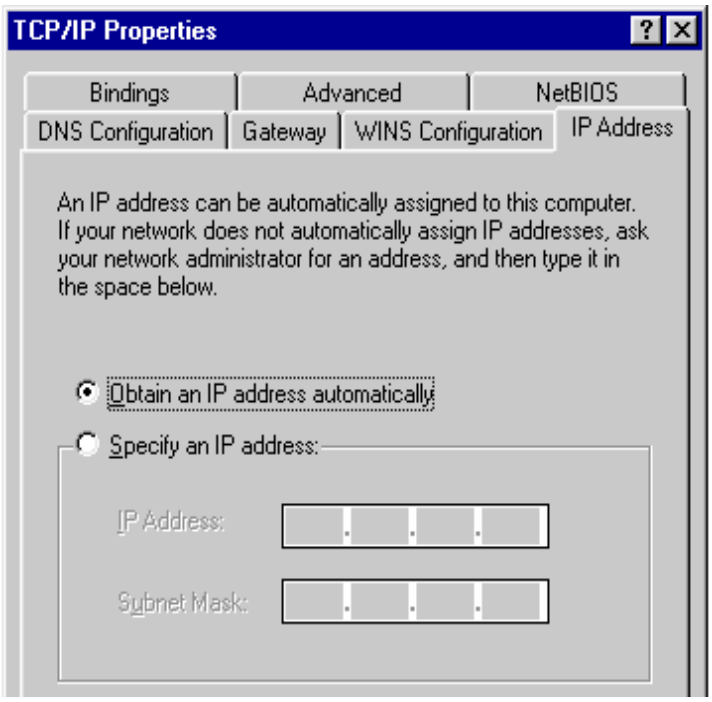
Before connecting to the modem router and start configuration procedures, user's computer must be able to get an IP address automatically (use dynamic IP address). If the PC is set to 'static IP address', then follow instructions below to reconfigure it to 'dynamic IP address'.

3.2.1 IP Address Configuration

a) Windows 95/98/Me

1. Click the Start button and select **<Settings>**, then click **<Control Panel>**. The Control Panel window will appear.
2. Double-click on **<Network>** icon. The Network window will appear.
3. Check the list of Network Components. If TCP/IP is not installed, click the **<Add>** button to install it. If TCP/IP is installed, go to step 6.
4. In the Network Component Type dialog box, select **<Protocol>** and click **<Add>** button.
5. In the Select Network Protocol dialog box, select **<Microsoft>** and **<TCP/IP>** then click the **<OK>** button to start installing the TCP/IP protocol. Windows CD may be needed to complete the installation.
6. After installing TCP/IP, go back to the Network dialog box. Select **<TCP/IP>** from the list of Network Components and then click the <Properties> button.
7. Check each of the tabs and verify the following settings:
   - Bindings: Check Client for Microsoft Networks and File and printer sharing for Microsoft Networks.
   - Gateway: All fields are blank.
   - DNS Configuration: Select Disable DNS.

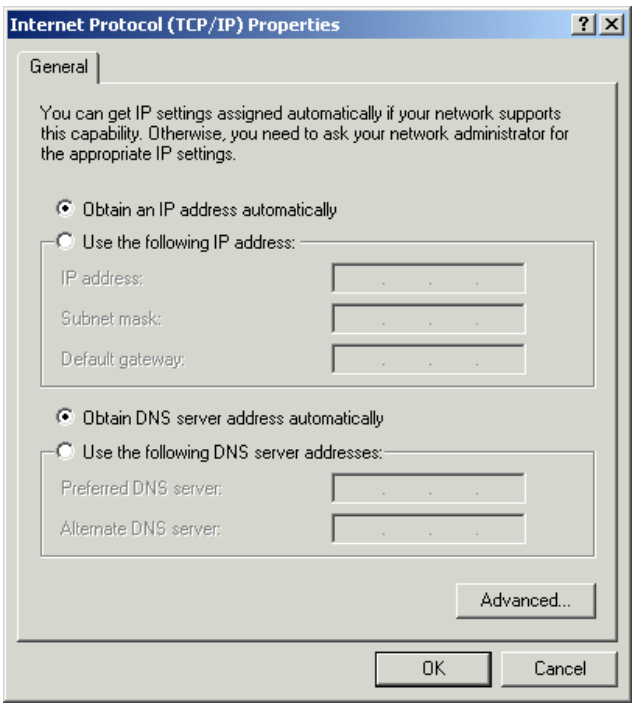
- WINS Configuration: Select Disable WINS Resolution.
- IP Address: Select Obtain IP address automatically.



8. Reboot the PC. PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
9. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.
10. Proceed to Web-based User Interface once IP address is correctly configured.

b) Windows 2000

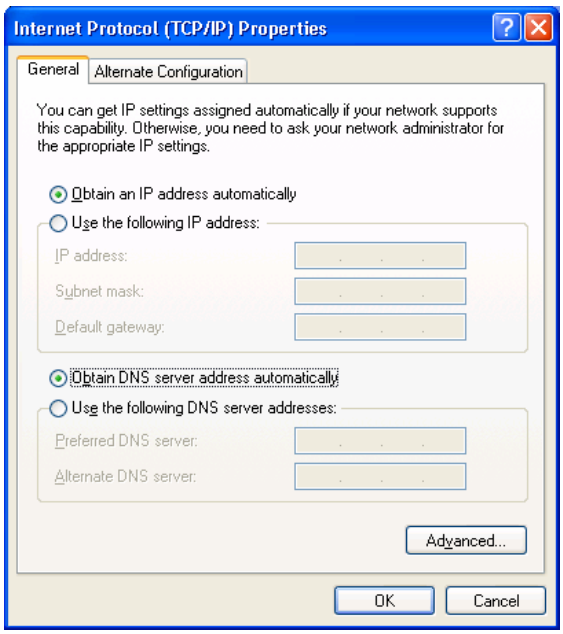
1. Click the **<Start>** button and select **<Settings>**, then click **<Control Panel>**. The Control Panel window will appear.
2. Double-click **<Network and Dial-up Connections>** icon. In the Network and Dial-up Connection window, double-click on <Local Area Connection> icon. The Local Area Connection window will appear.
3. In the Local Area Connection window, click the **<Properties>** button.
4. Check the list of Network Components. Users should see Internet Protocol [TCP/IP] on the list. Select it and click the **<Properties>** button.
5. In the Internet Protocol (TCP/IP) Properties window, select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>** as shown on the following screen.



6. Click **<OK>** to confirm the setting. The PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
7. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.
8. Proceed to Web-based User Interface once IP address is correctly configured.

c) Windows XP

1. Click the **<Start>** button and select **<Settings>**, then click **<Network Connections>**. The Network connections window will appear.
2. Double-click **<Local Area Connection>** icon. The Local Area Connection window will appear.
3. Check the list of Network Components. Users should see Internet Protocol [TCP/IP] on the list. Select it and click the **<Properties>** button.
4. In the Internet Protocol (TCP/IP) Properties window, select **<Obtain an IP address automatically>** and **<Obtain DNS server address automatically>** as shown on the following screen.

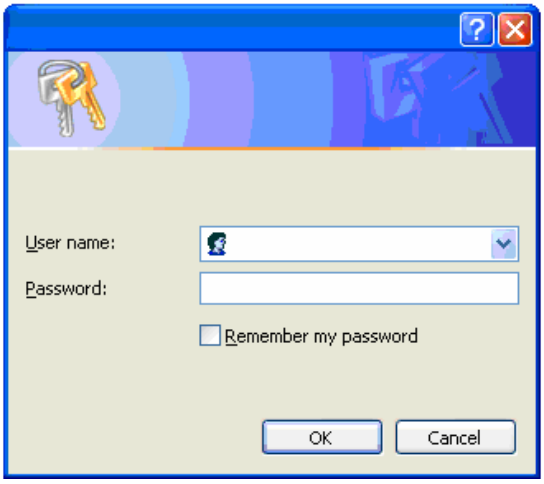


5. Click **<OK>** to confirm the setting. PC will now obtain an IP address automatically from the Broadband Router's DHCP server.
6. Please make sure that the Broadband router's DHCP server is the only DHCP server available on the LAN network.

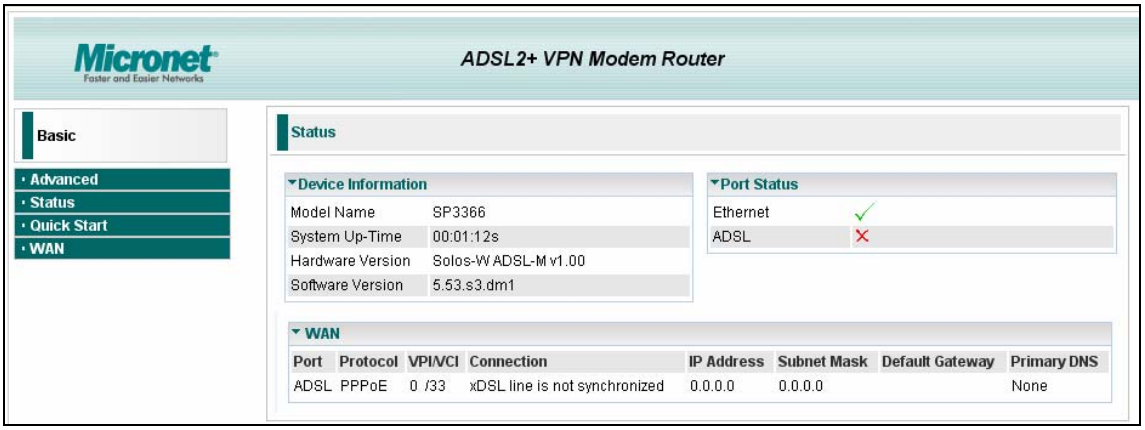
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
Username	'admin'
Password	'admin'

3.2.2 Starting Web-Based Management UI

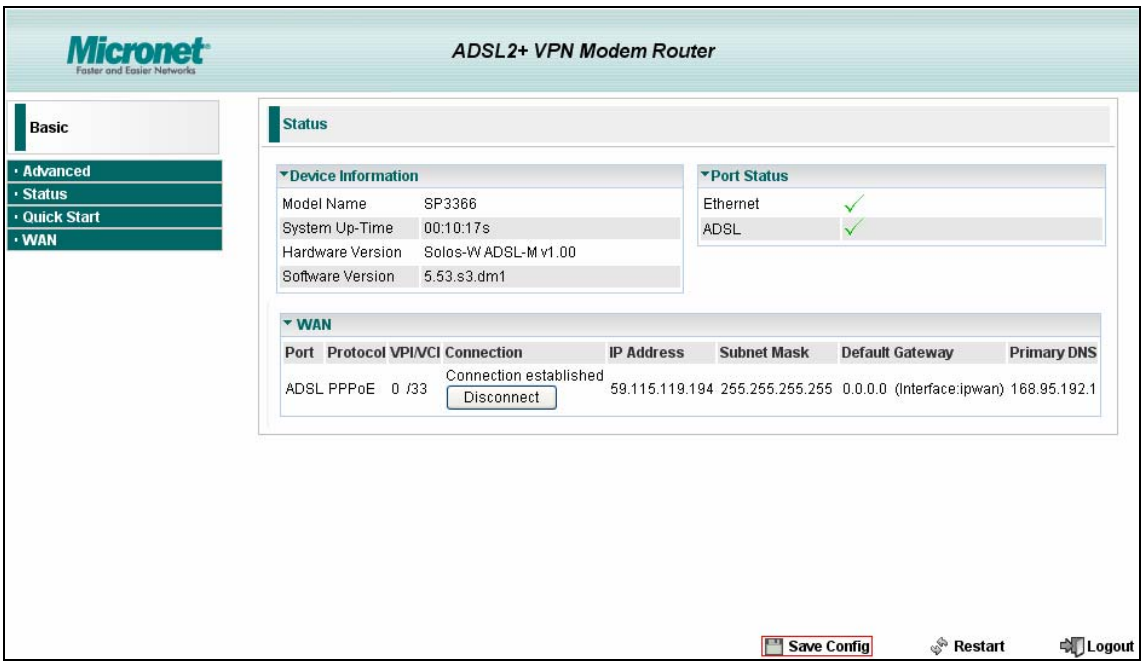
1. After the computer has obtained an IP address from modem router, please start the web browser. Input the IP address of router (Default: 192.168.1.254) in the address bar and the following message should appear:



2. Please input username and password in the field respectively. Default username is ‘admin’ and default password is ‘admin’, then press **<OK>** button. Once the login details are entered correctly, users can see the web management interface of this modem router.



3. For all changes to the setting on the Web UI, please click on ‘Save Config’ to permanetly save configuation to FLASH. Otherwise, rebooting device will cause the current changes to the setting to be ignored.


Micronet
Faster and Easier Networks
ADSL2+ VPN Modem Router
Basic
Advanced
Status
Quick Start
WAN
Status
Device Information
Model Name SP3366
System Up-Time 00:10:17s
Hardware Version Solos-W ADSL-M v1.00
Software Version 5.53.s3.dm1
Port Status
Ethernet
ADSL
WAN
Port Protocol VPI/VCI Connection IP Address Subnet Mask Default Gateway Primary DNS
ADSL PPPoE 0 /33 Connection established Disconnect 59.115.119.194 255.255.255.255 0.0.0.0 (Interface:ipwan) 168.95.192.1
Save Config
Restart
Logout

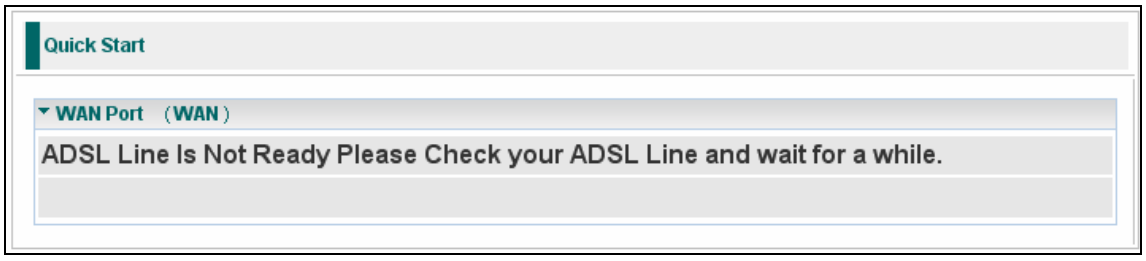
Chapter 4 Web-Based Management UI

4.1 Quick Start

The ‘Quick Start’ section is designed to get the modem router running as quickly as possible. In the ‘Quick Start’, users are required to fill in only the information necessary to access the Internet. Once user clicks on the **<Quick Start>** on the menu to the left, the following screen will appear.

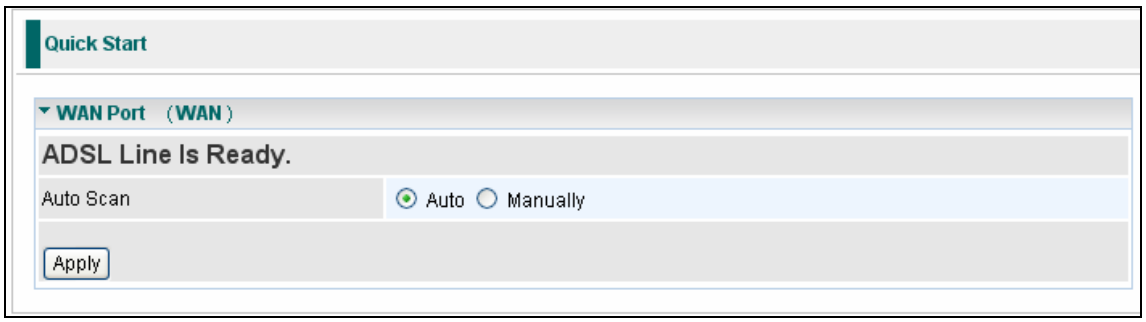
Step 1: ADSL Status

If below message are shown, the ADSL line is not ready. Please wait for few minutes to allow the line to synchronize.



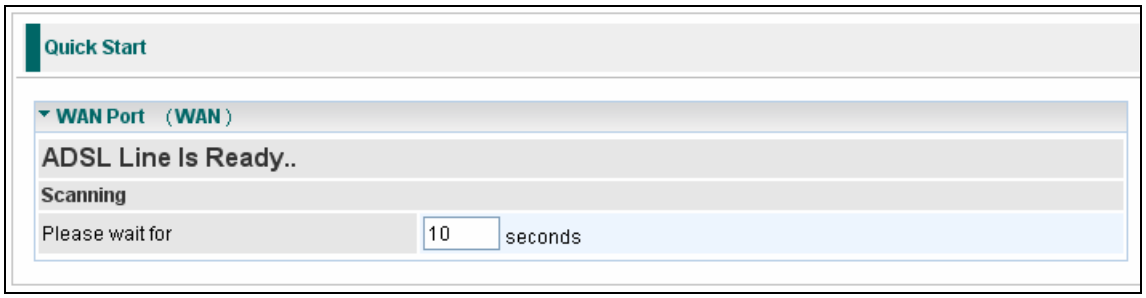
Step 2: ADSL Status

If ADSL line is ready, the screen will appear ‘ADSL Line is Ready’. Choose ‘Auto’ and click **<Apply>**. It will automatically scan the recommended mode for the connection. ‘Manually’ mode requires user to set the ADSL line (Proceed to step 5 if ‘Manually is selected).



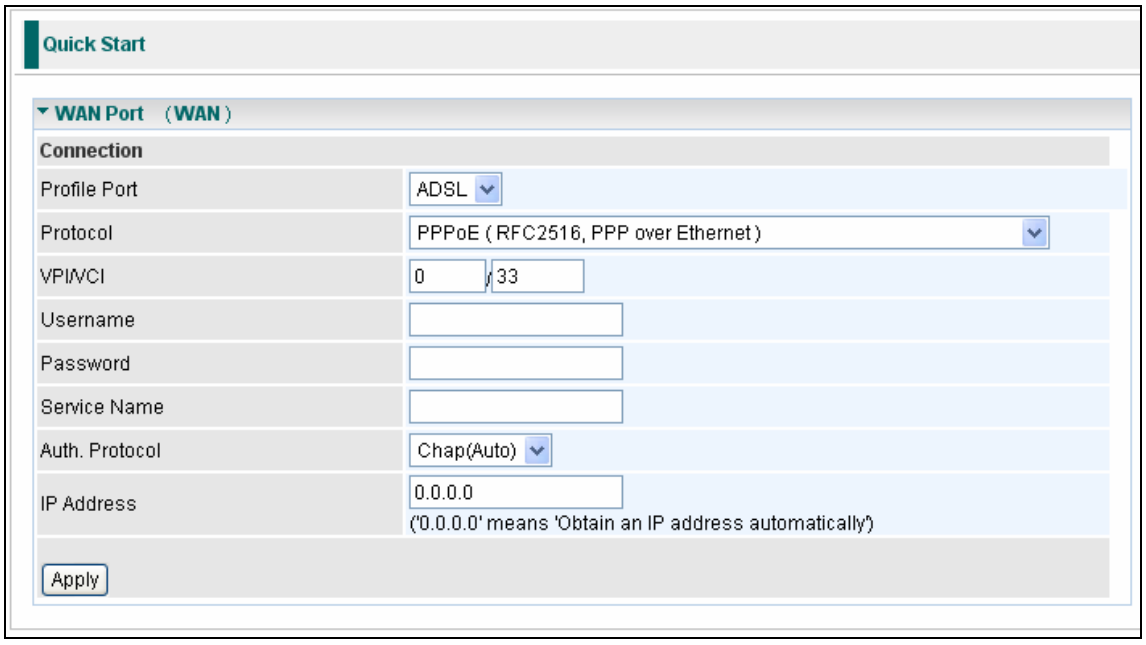
Step 4: Auto Scan

The list below has different mode suitable for the connection.



Step 5: Internet Account

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

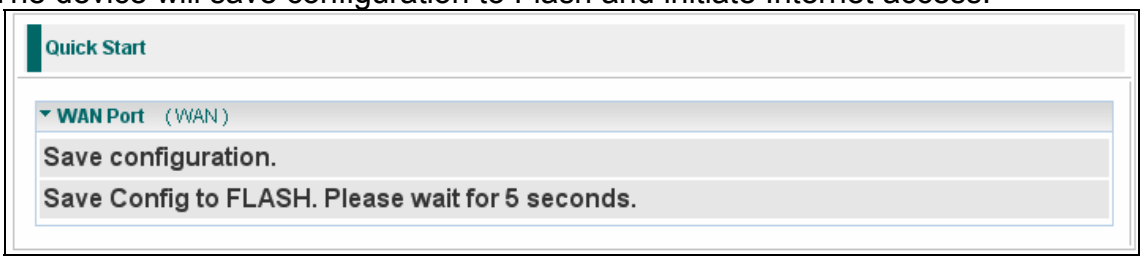


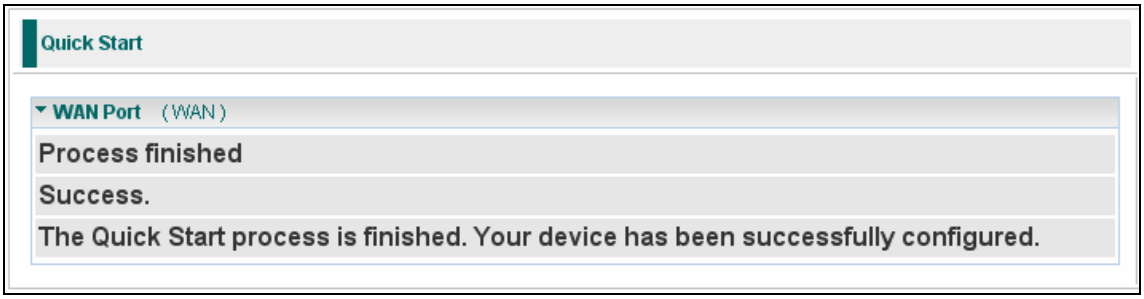
Parameter	Description
Profile Port	Select the connection mode.
Encapsulation	Select the encapsulation mode. Default: ‘PPPoE’.
VPI/VCI	Enter the VPI and VCI information provided by ISP.
Username	Enter the username provided by ISP.
Password	Enter the password provided by ISP.
Service Name	This item is for identification purposes. It is optional depending on ISP.

Authentication Protocol	Chose the protocol used by ISP (CHAP or PAP) Default: 'Auto'.
IP Address	WAN IP address supplied by ISP. Leave this at 0.0.0.0 to automatically obtain an IP address from ISP.

Step 6: Auto Scan

The device will save configuration to Flash and initiate Internet access.

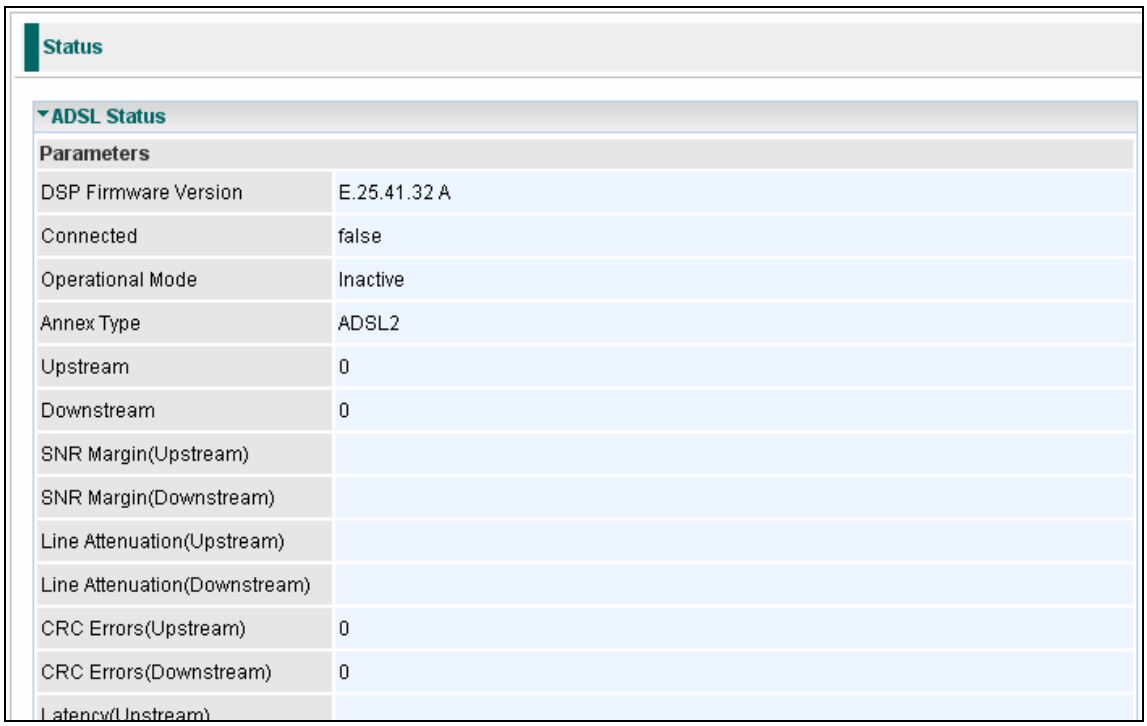




4.2 Status

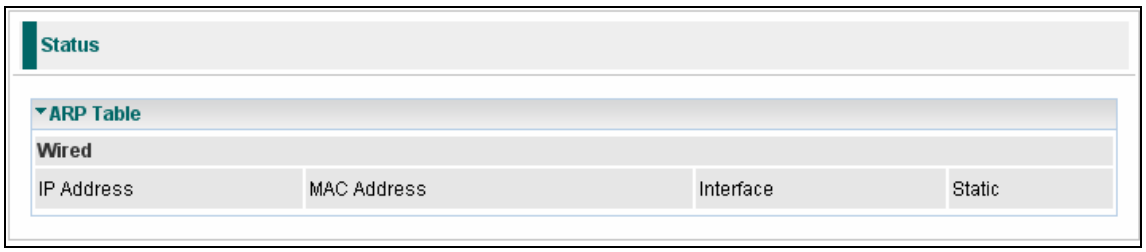
4.2.1 ADSL Status

This section displays the ADSL overall status, which shows a number of helpful information such as DSP firmware version.



4.2.2 ARP Table

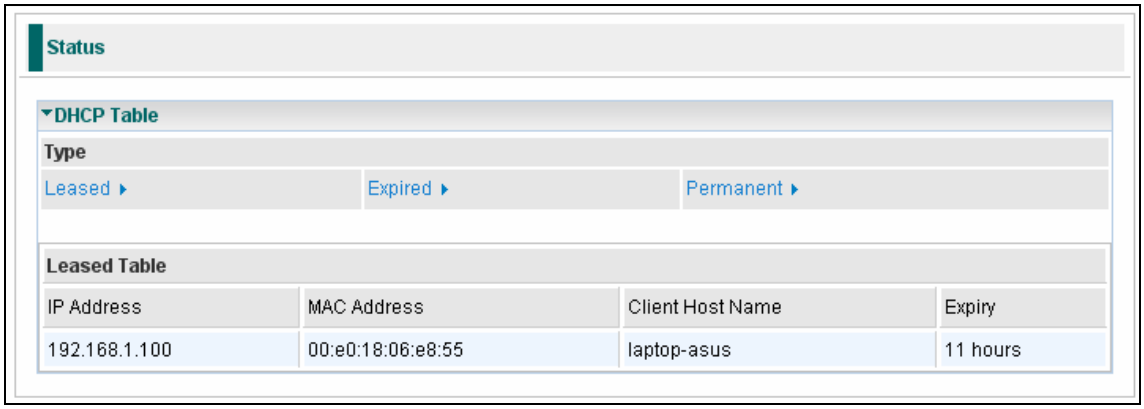
This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of PCs for router's Firewall – MAC Address Filter function.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



Parameter	Description
IP Address	A list of IP addresses of devices on the LAN (Local Area Network).
MAC Address	The MAC (Media Access Control) addresses for each device on the LAN.
Interface	The interface name (on the router) that this IP Address connects to.

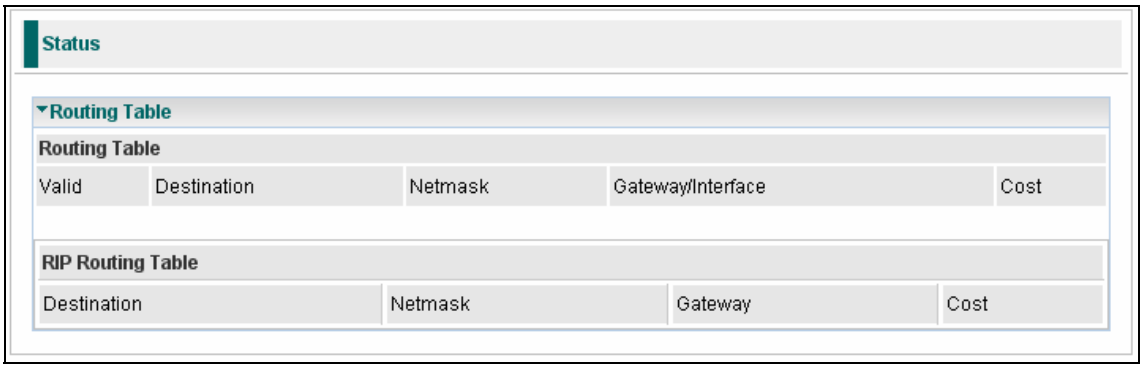
Static	Static status of the ARP table entry. 'No' for dynamically-generated ARP table entries. 'Yes' for static ARP table entries added by the user.

4.2.3 DHCP Table



Parameter	Description
Leased	The DHCP assigned IP addresses information.
Expired	The expired IP addresses information.
Permanent	The fixed host mapping information.

4.2.4 Routing Table

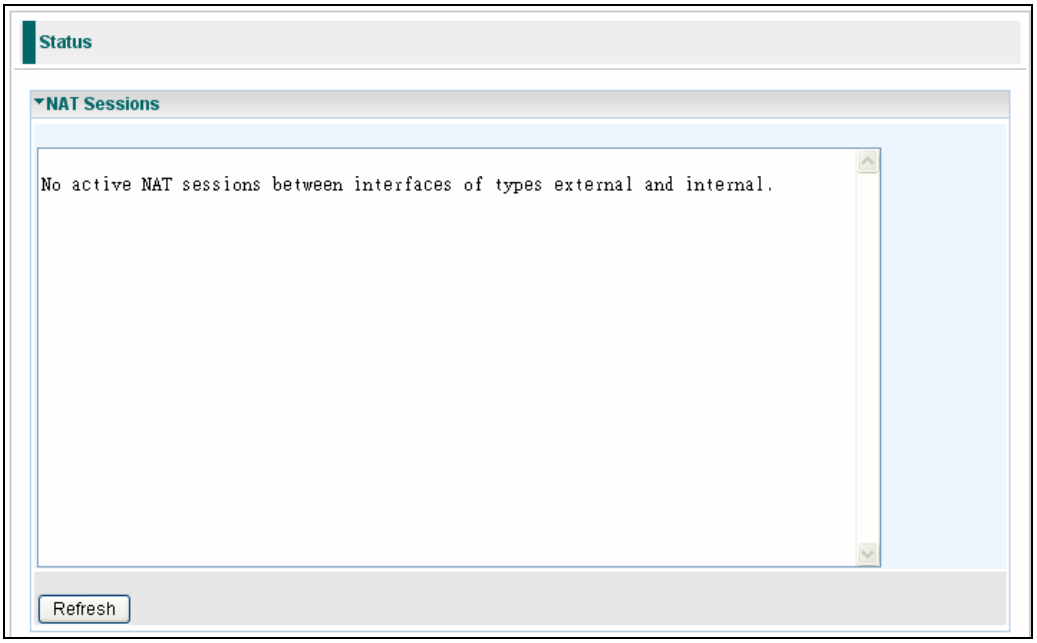


Parameter	Description
Valid	It indicates a successful routing status.
Destination	The IP address of the destination network.
Netmask	The destination Netmask address.
Gateway/Interface	The IP address of the gateway or existing interface that this route will use.

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

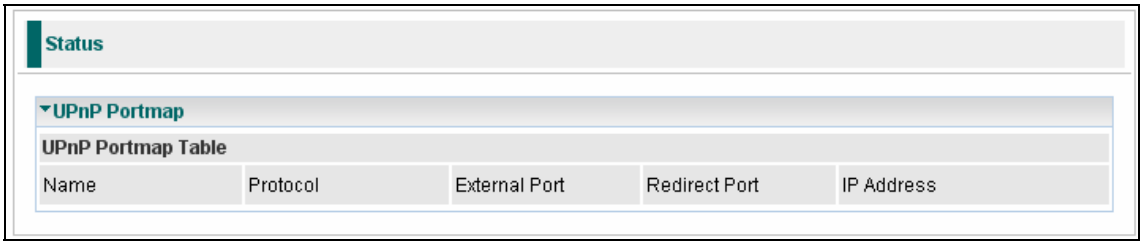
4.2.5 NAT Session

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



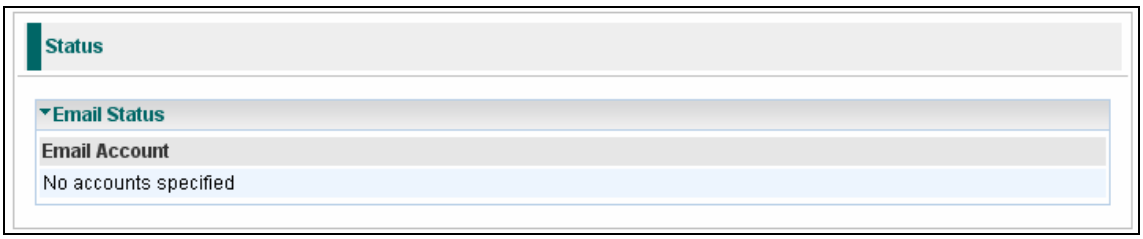
4.2.6 UPnP Portmap

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.



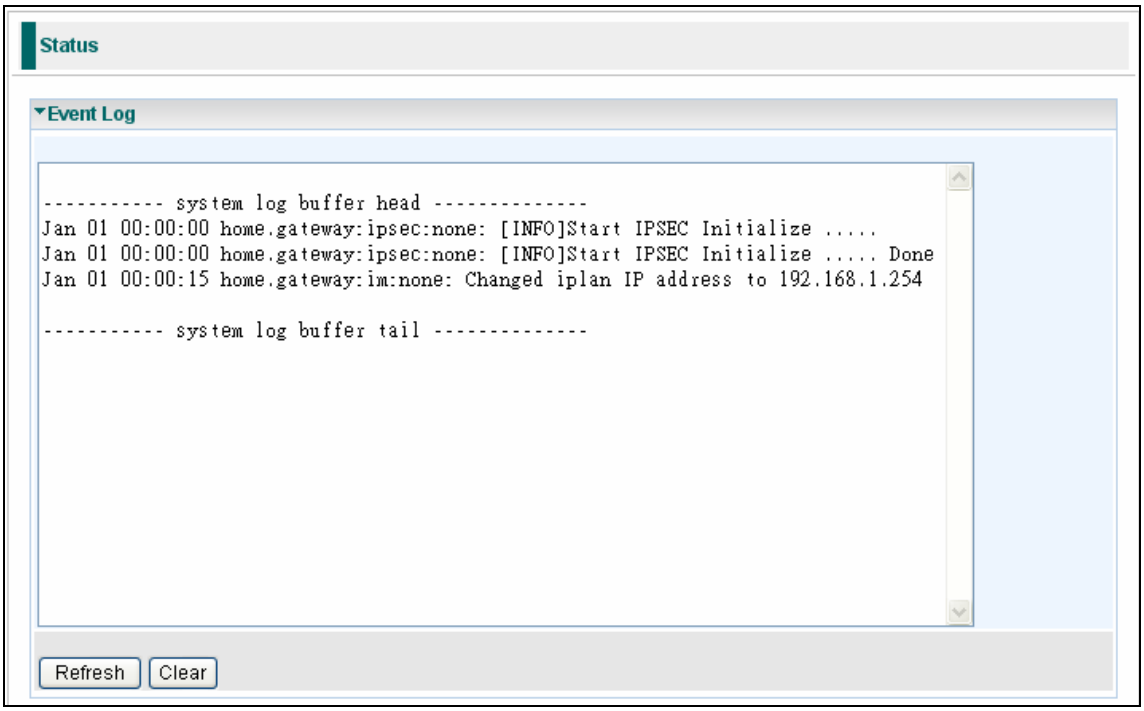
4.2.7 Email Status

Detail status for the Email Account users have configured for the router to check. Please see the 'Advanced' section of this manual for details on this function.



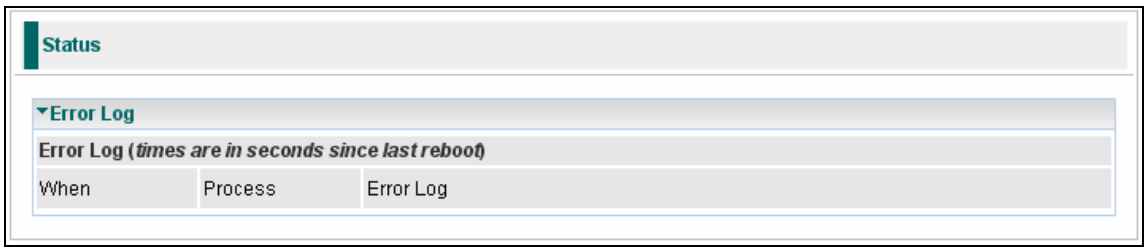
4.2.8 Event Log

This page displays the router's Event Log entries. Major events are logged to this window. For example, when the router's ADSL connection is disconnected or Firewall events when enabled Intrusion or Blocking Logging.



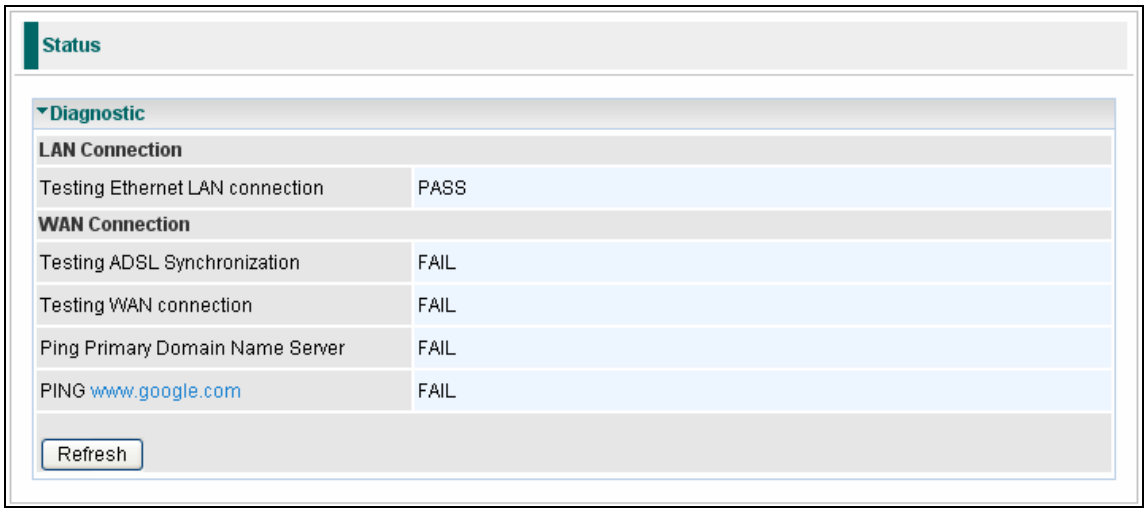
4.2.9 Error Log

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



4.2.10 Diagnostic

The tool is for testing LAN PCs connections to WAN (Internet). If PING ww.google.com is shown as 'FAIL' and the rest of the tests are 'PASS', users ought to check the PC's DNS settings is set correctly.

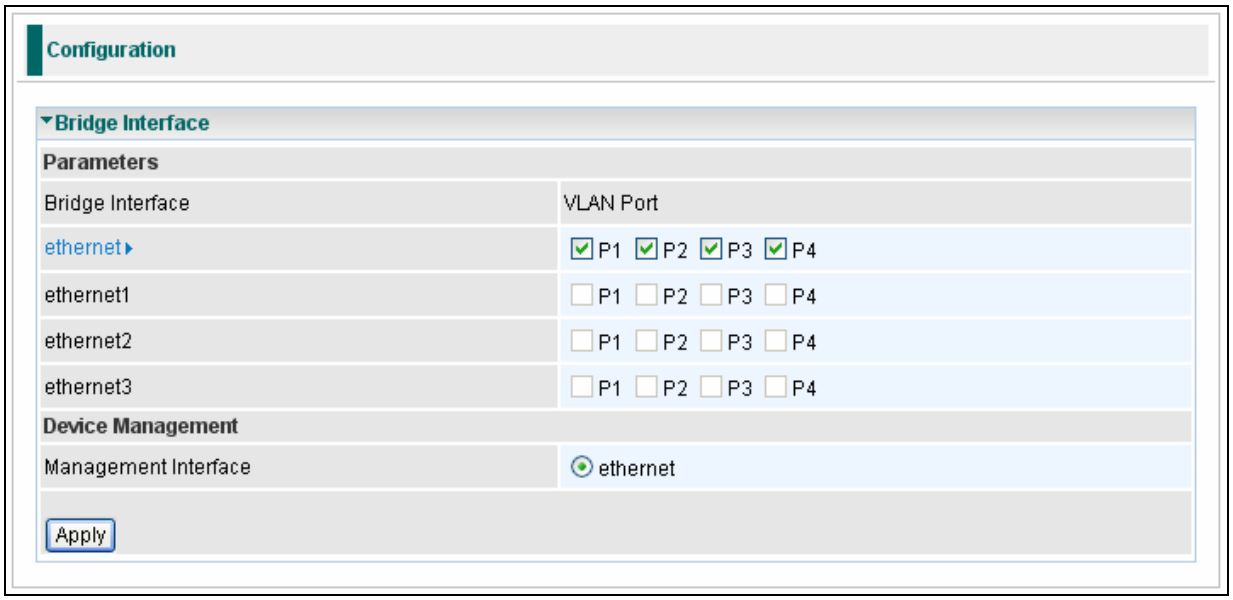


4.3 Configuration

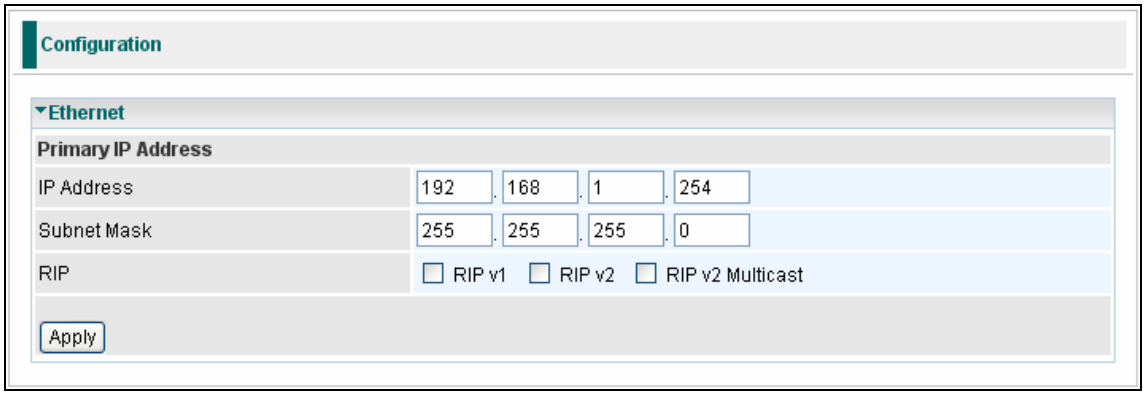
4.3.1 LAN

Bridge Interface

Users can setup member ports for each VLAN group under Bridge Interface section. Management interface is the VLAN that has access right to the Web UI for configuration. NAT/NAPT can only be applied to management interface only.



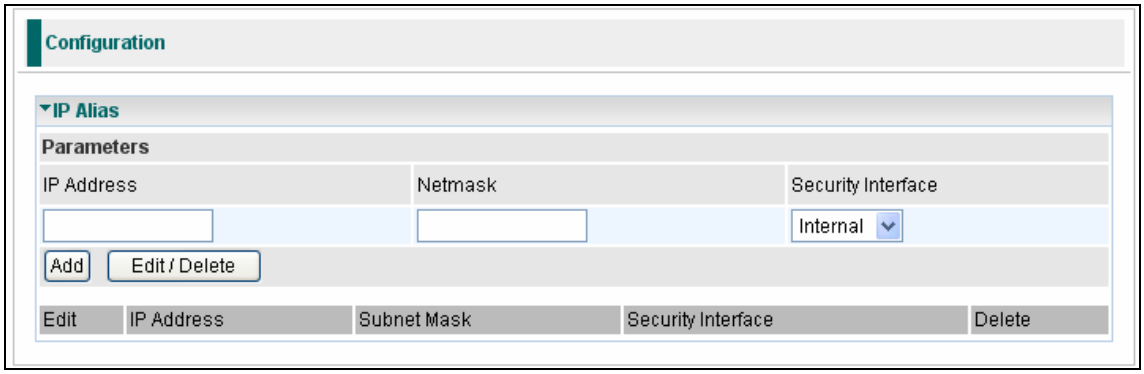
Ethernet



Parameter	Description
IP Address	The default IP on this router.
Subnet Mask:	The default subnet mask on this router.
RIP	Check to enable RIP function.

IP Alias

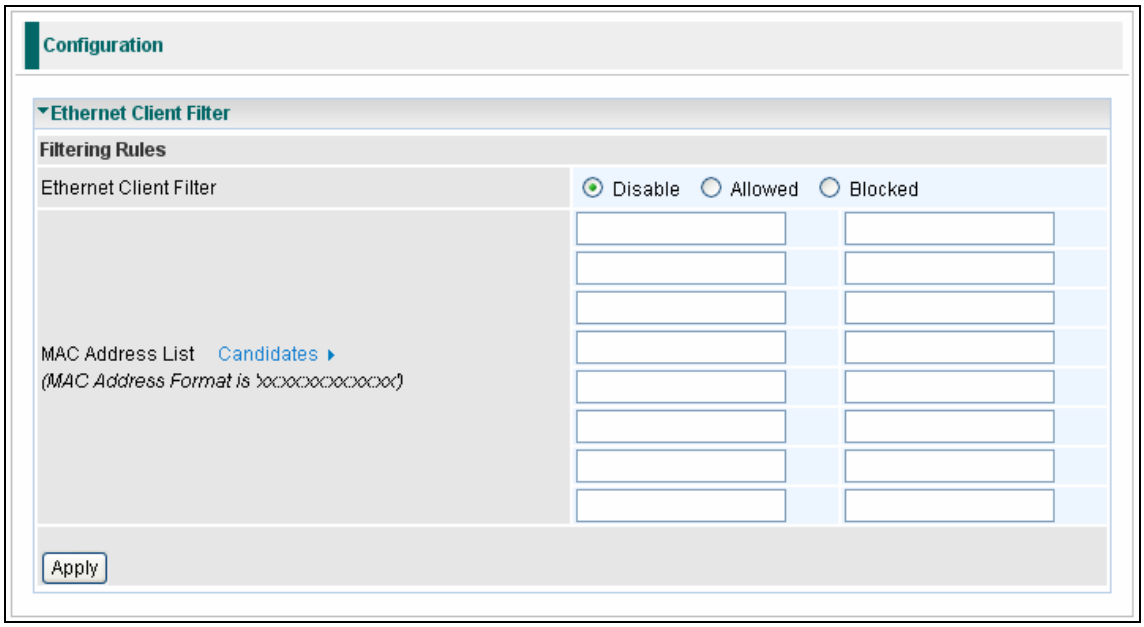
This function creates multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



Parameter	Description
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 conduct 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.
DMZ	Specify this network to DMZ area. There is no NAT on this interface.

Ethernet Client Filter

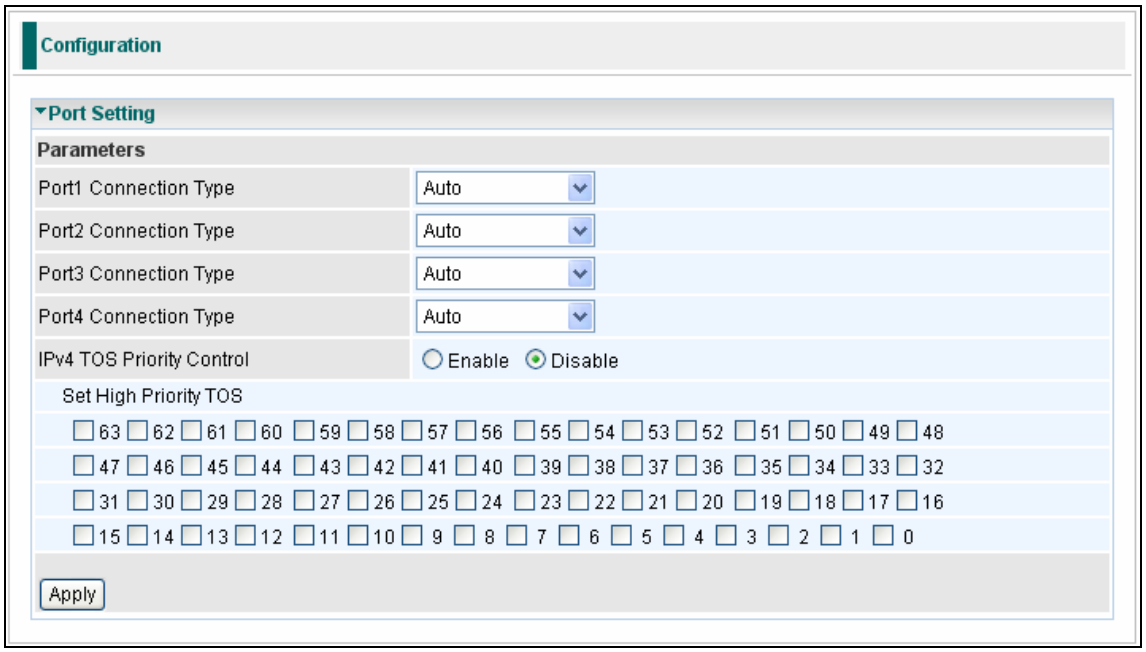
The Ethernet Client Filter supports up to 16 Ethernet network machines that helps users to manage the network control to accept traffic from specific authorized machines or can restrict unwanted machine(s) to access the LAN. There are no pre-defined Ethernet MAC address filter rules. Users can add the filter rules to meet their requirements.



Parameter	Description
Ethernet Client Filter	➢ **Allowed:** check to authorize specific device accessing the LAN. Insert the MAC Address in the space provided or click 'Candidates'. ➢ **Blocked:** check to prevent unwanted device accessing the LAN by insert the MAC Address in the space provided or click 'Candidates'. Max: 16 Clients.
Candidates	Automatically detects devices connected to the router through the Ethernet.

Port Setting

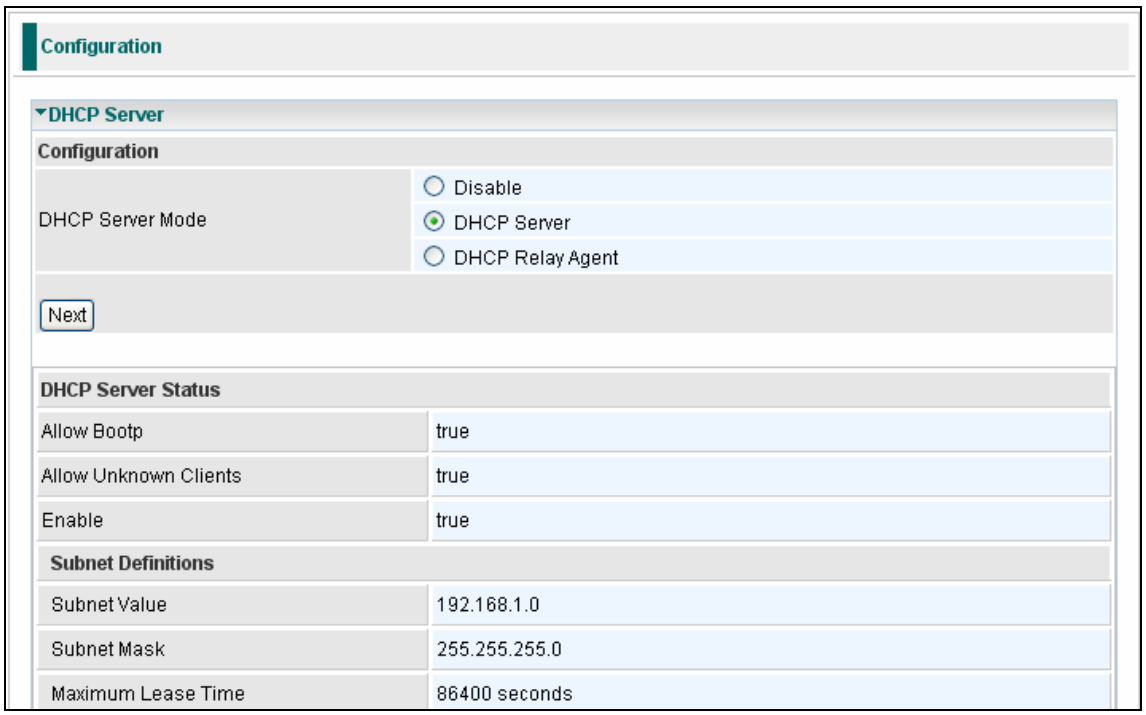
This section allows user to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



Parameter	Description
Port # Connection Type	There are Six options to choose from: Auto, disable, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and users 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 the 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

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



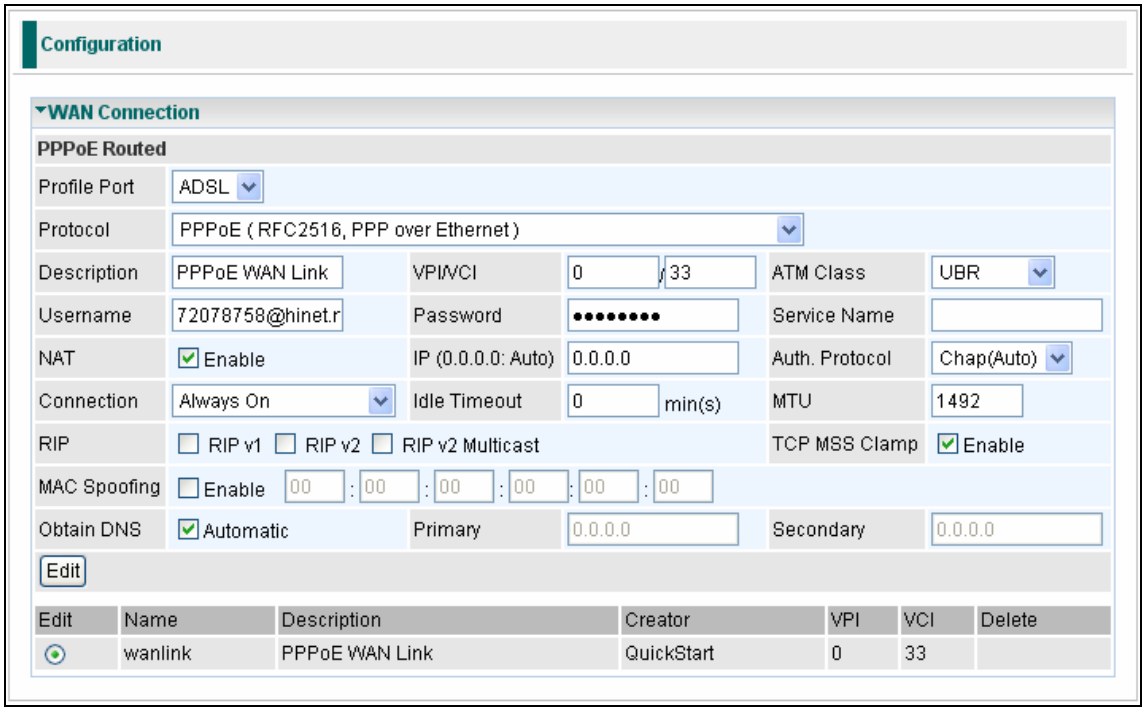
To disable the router's DHCP Server, check 'Disabled' and click **<Next>** and **<Apply>**. When the DHCP Server is disabled users will need to manually assign a fixed IP address to each PCs on the network, and set the default gateway for each PCs to the IP address of the router (default: 192.168.1.254). To configure the router's DHCP Server, check DHCP Server and click **<Next>**. Users 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 users check "Use Router as a DNS Server", the ADSL Router will perform the domain name lookup and find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN. If users check 'DHCP Relay Agent' and click **<Next>**, 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 by network administrator or ISP. Click **<Apply>** to enable this function.

4.3.2 WAN

WAN Profile

PPPoE Connection

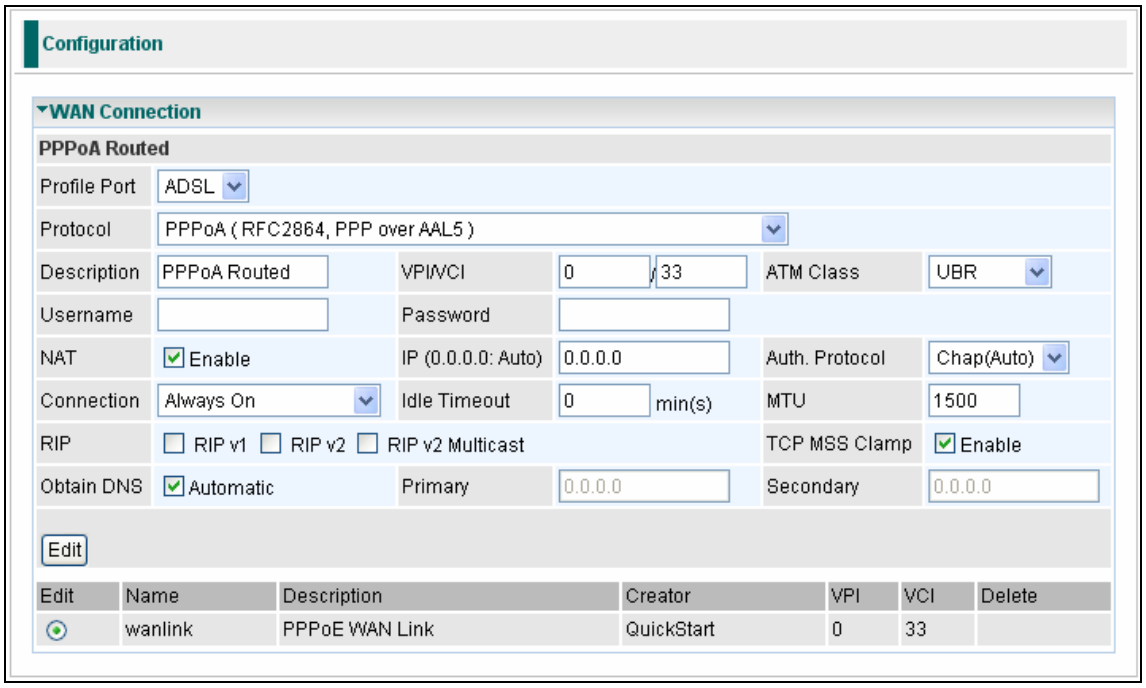
PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.



Parameter	Description
Profile Port	Select the profile port 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 the ISP. Users 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 the ISP. Users can input up to 128 alphanumeric characters (case sensitive).
Service Name	This item is for identification purposes. Optional depending on ISP. Max: 15 alphanumeric characters.

NAT	The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account and address.
IP (0.0.0.0:Auto)	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 on whether to use CHAP or PAP.
Connection	➢ **Always on:** If users 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 users want to establish a PPP session only when there is a packet requesting access to the Internet (i.e. when a program on the 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:** Users can define the destination port and packet type (TCP/UDP) without checking by timer. It allows user 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	Check to enable RIP function.
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default: 'Enabled'.
MAC Spoofing	This option is required by some service providers. Users must fill in the MAC address that specify by service provider when it is required. Default: '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 box to obtain DNS automatically.
Primary DNS	Enter the primary DNS to manually specify server.
Secondary DNS	Enter the secondary DNS to manually specify server.

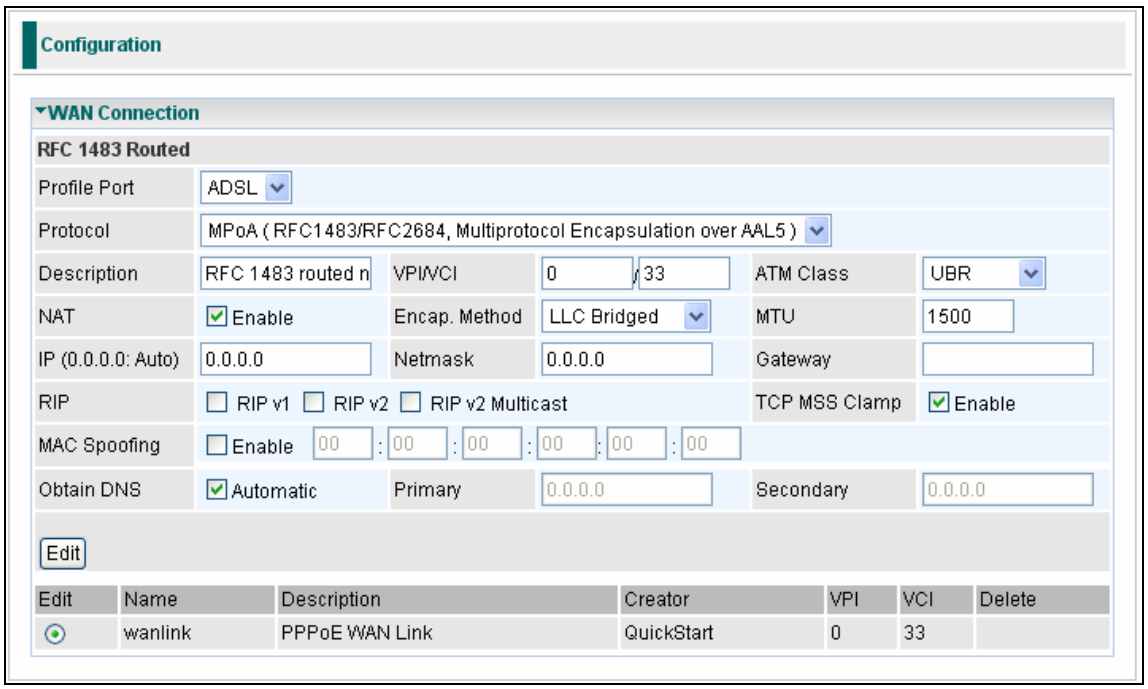
PPoA Connection



Parameter	Description
Profile Port	Select the profile port 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 the ISP. Users 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 the ISP. Users can input up to 128 alphanumeric characters (case sensitive).
Service Name	This item is for identification purposes. Optional depending on ISP. Max: 15 alphanumeric characters.
NAT	The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account and address.
IP (0.0.0.0:Auto)	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 on whether to use CHAP or PAP.

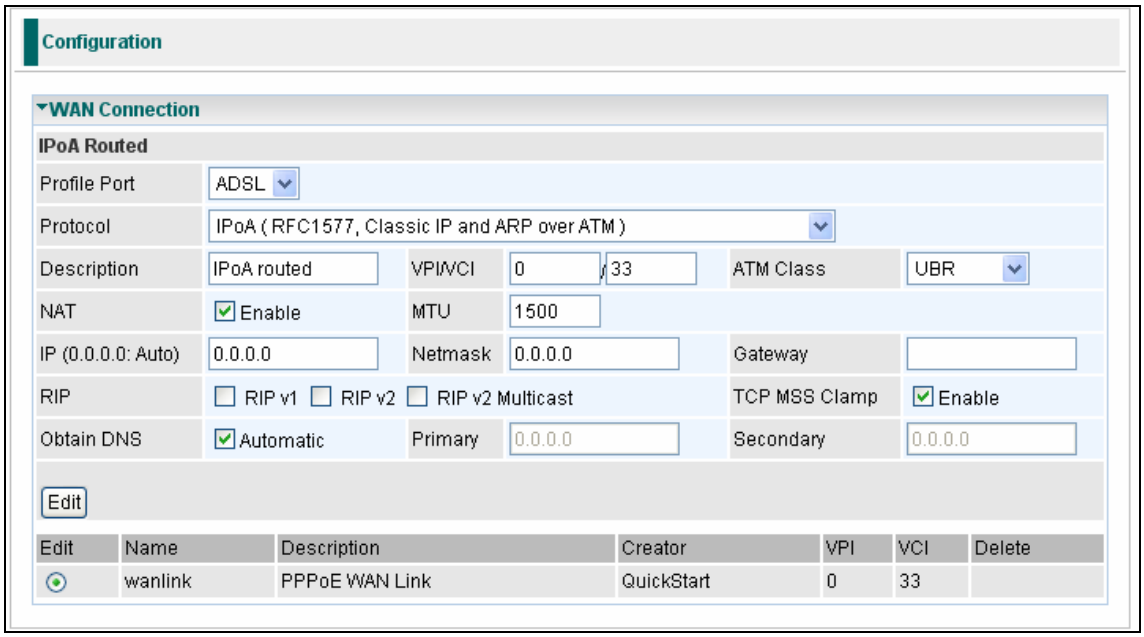
Connection	➢ **Always on:** If users want the router to establish a PPP session when starting up and to automatically re-establish the PPP session when disconnected by the ISP. ➢ **Connect on Demand:** If users want to establish a PPP session only when there is a packet requesting access to the Internet (i.e. when a program on the 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:** Users can define the destination port and packet type (TCP/UDP) without checking by timer. It allows user 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	Check to enable RIP function.
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default: '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 box to obtain DNS automatically.
Primary DNS	Enter the primary DNS to manually specify server.
Secondary DNS	Enter the secondary DNS to manually specify server.

MPoA Connection



Parameter	Description
Profile Port	Select the profile port 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 and address.
Encap. Mode	Choose whether 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)	WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.
Netmask	Type the subnet mask assigned by ISP (if given).
Gateway	Enter the IP address of the default gateway (if given).
RIP	Check to enable RIP function.
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default: 'Enabled'.
MAC Spoofing	This option is required by some service providers. Users must fill in the MAC address that specify by service provider when it is required. Default: '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 box to obtain DNS automatically.
Primary DNS	Enter the primary DNS to manually specify server.
Secondary DNS	Enter the secondary DNS to manually specify server.

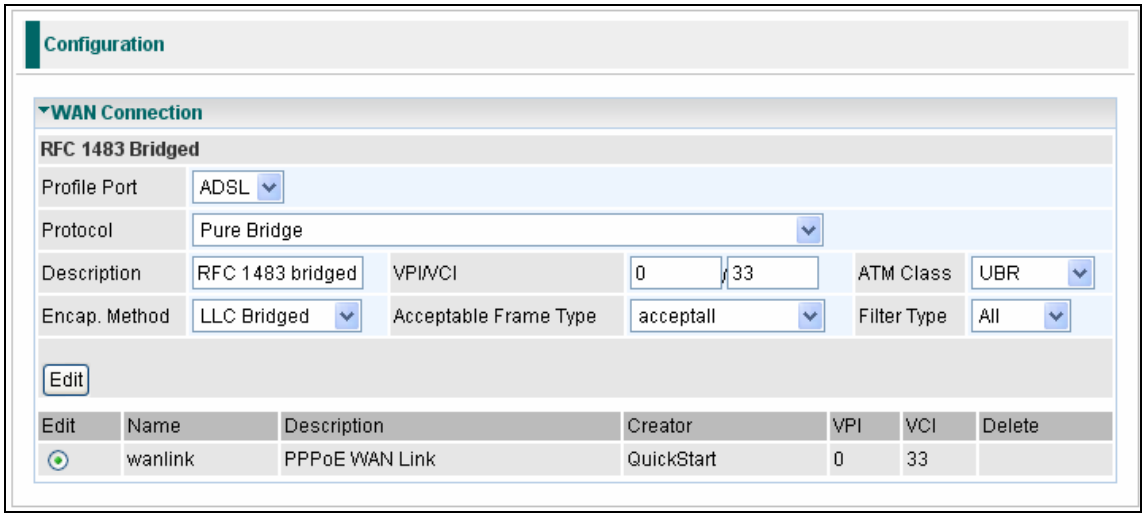
IPoA Routed Connection



Parameter	Description
Profile Port	Select the profile port 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 and address.
Encap. Mode	Choose whether 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)	WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.
Netmask	Type the subnet mask assigned by ISP (if given).
Gateway	Enter the IP address of the default gateway (if given).
RIP	Check to enable RIP function.
TCP MSS Clamp	This option helps to discover the optimal MTU size automatically. Default: '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 box to obtain DNS automatically.
Primary DNS	Enter the primary DNS to manually specify server.

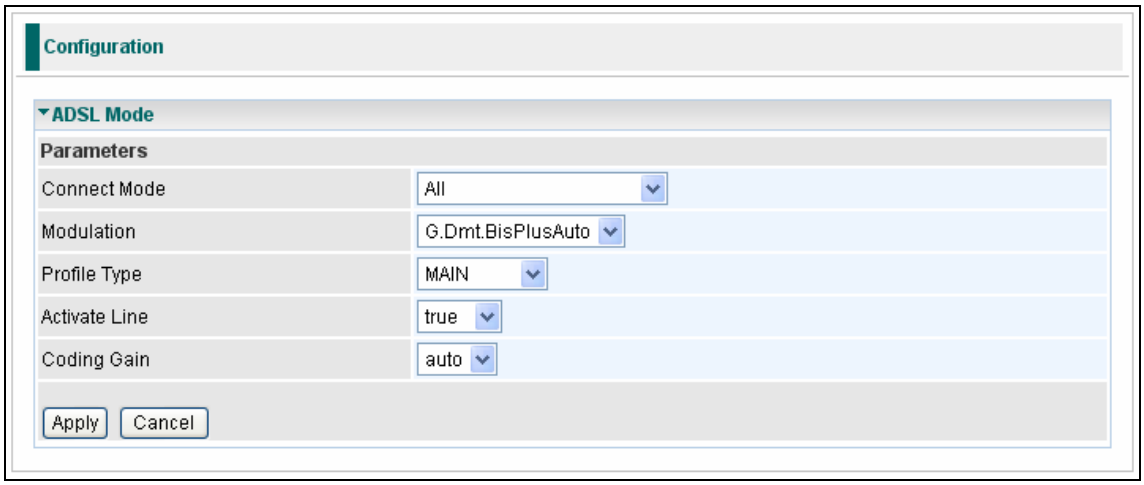
Secondary DNS	Enter the secondary DNS to manually specify server.

Pure Bridge



Parameter	Description
Profile Port	Select the profile port 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.
Encap. Mode	Choose whether the packets in WAN interface as bridged packet or routed packet.
Acceptable Frame Type:	Specify which kind of traffic goes through this connection, all traffic or only VLAN tagged.
Filter Type:	Specify the type of Ethernet filtering performed by the named bridge interface. ➢ **All:** Allows all types of Ethernet packets through the port. ➢ **IP:** Allows only IP/ARP types of Ethernet packets through the port. ➢ **PPPoE:** Allows only PPPoE types of Ethernet packets through the port.
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 box to obtain DNS automatically.
Primary DNS	Enter the primary DNS to manually specify server.
Secondary DNS	Enter the secondary DNS to manually specify server.

ADSL Mode



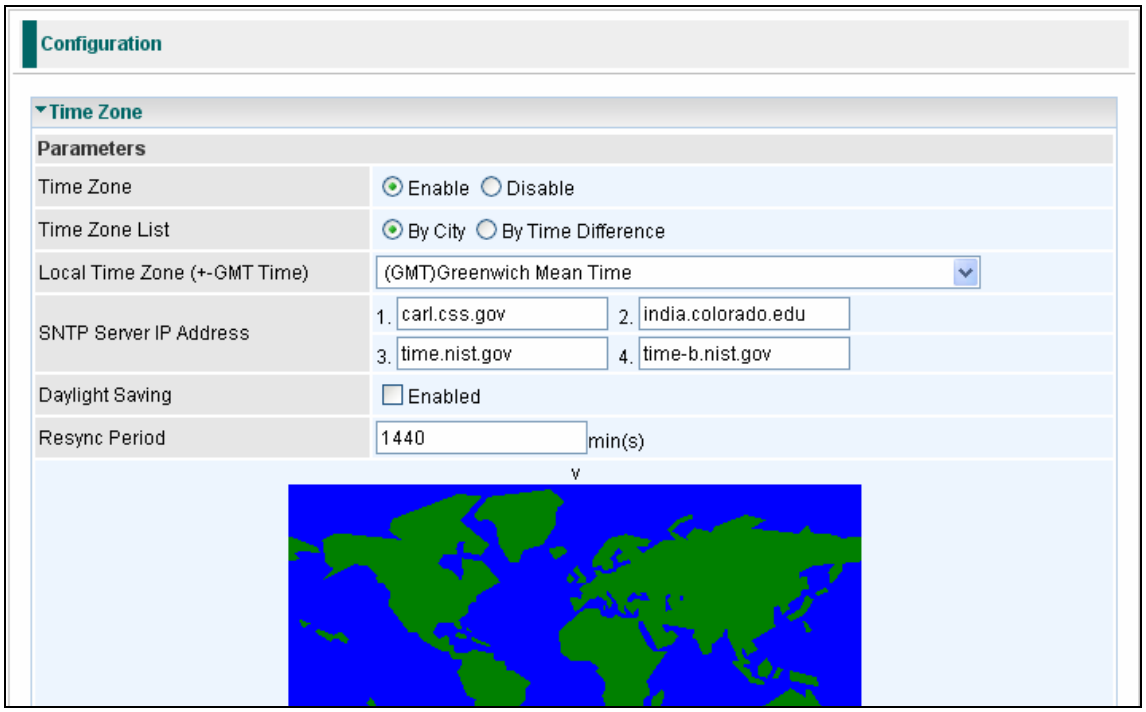
Parameter	Description
Connect Mode	This mode will automatically detect the ADSL line code: ADSL2+, ADSL2, AnnexM2 and AnnexM2+, ADSL. Please keep the factory settings unless ADSL is detected as the symptom of synchronization problem.
Modulation	It will automatically detect capability of the ADSL line mode. Please keep the factory settings 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. Users may need to change the profile setting to reach the best ADSL line rate and depends on the different DSLAM and location.
Activate Line	Aborting (false) the 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.

4.3.3 System

Time Zone

The router does not have a real time clock on board. Instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside the network. Choose user's local time zone and click **<Enable>** then **<Apply>** button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server specified. If user prefer to specify an SNTP server other

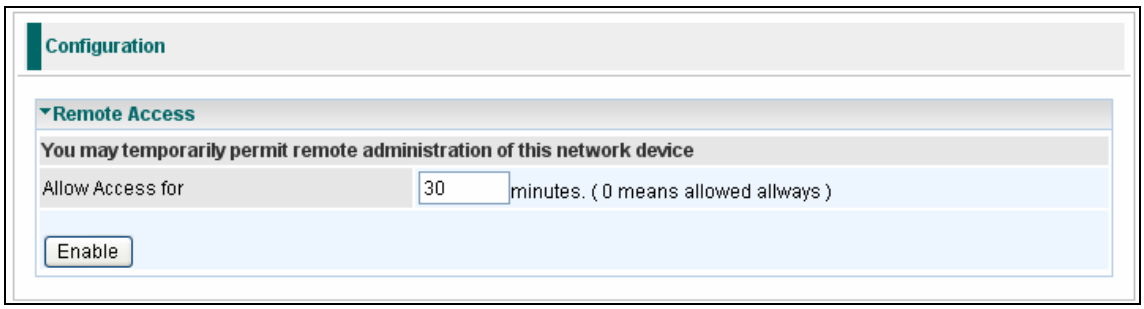
than those in the list, simply enter its IP address in the fields provided. Some ISP may provide an SNTP server for their customers.



Parameter	Description
Daylight Saving	Many places in the world adapt it during summer period to move one hour of daylight from morning to the evening in local standard time. Check 'Automatic' box to auto set the local time.
Resync Period	Periodic interval the router will wait before it re-synchronizes the router's time with SNTP server. In order to avoid unnecessarily increase of the load on SNTP server, users should keep the poll interval as high as possible.

Remote Access

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>**. Users may change other configuration options for the web administration interface using 'Device Management' options in the 'Advanced' section of the GUI. If users wish to permanently enable remote access, choose a time period of 0 minute.

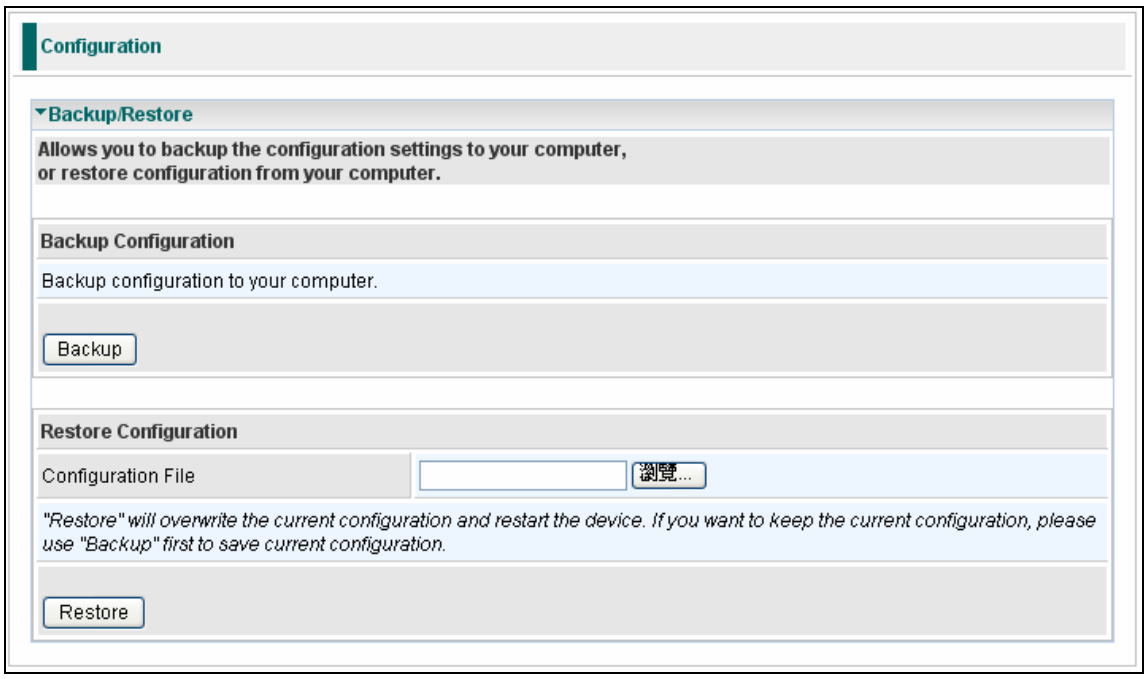


Firmware Upgrade

Router's "firmware" is the software that allows it to operate and provides all its functionality. Over time this software may be improved and revised, and the router allows user to upgrade the software. Click on **<Browse>** will allow users to select the new firmware image file from the PC. Once the correct file is selected, click **<Upgrade>** to update the firmware. Do not power off device with upgrade is in progress.

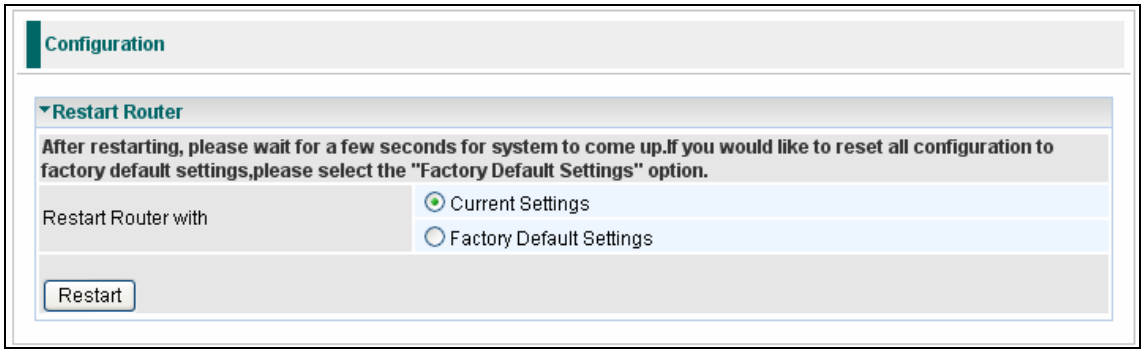
Backup/ Restore

These functions allow user to save and backup the router's current settings to a file on the PC, or to restore a previously saved backup. This is useful if users wish to experiment with different settings, knowing that a backup is handy in the case of any mistakes. It is advisable to backup the router's settings before making any significant changes to the router's configuration. Press **<Backup>** to select where on the local PC to save the settings file. Press **<Browse>** to select a file from the PC to restore router's settings. Users should only restore settings files that have been generated by the Backup function from the current version of the router's firmware. After selecting the settings file, press **<Restore>** will load those settings into the router.



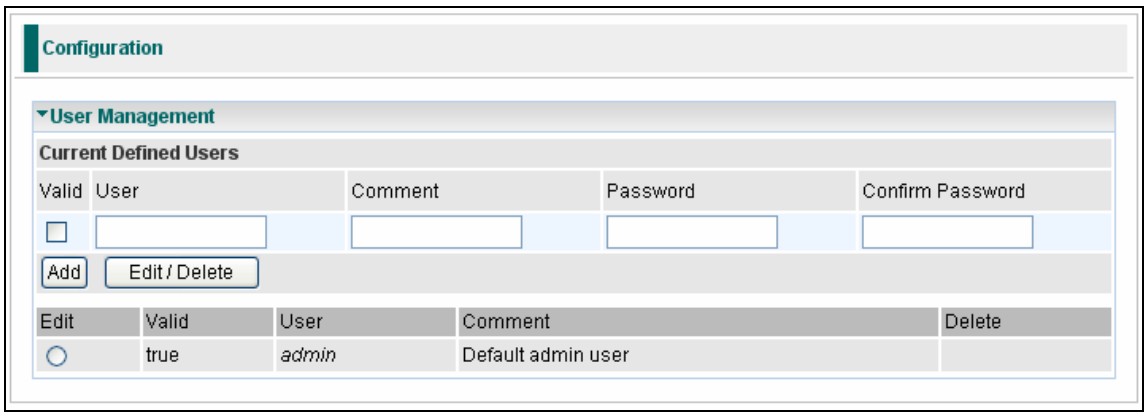
Restart Router

Click **<Restart>** with option 'Current Settings' to reboot your router (and restore your last saved configuration). If users wish to restart the router using the factory default settings, select 'Factory Default Settings' to reset to factory default settings.



User Management

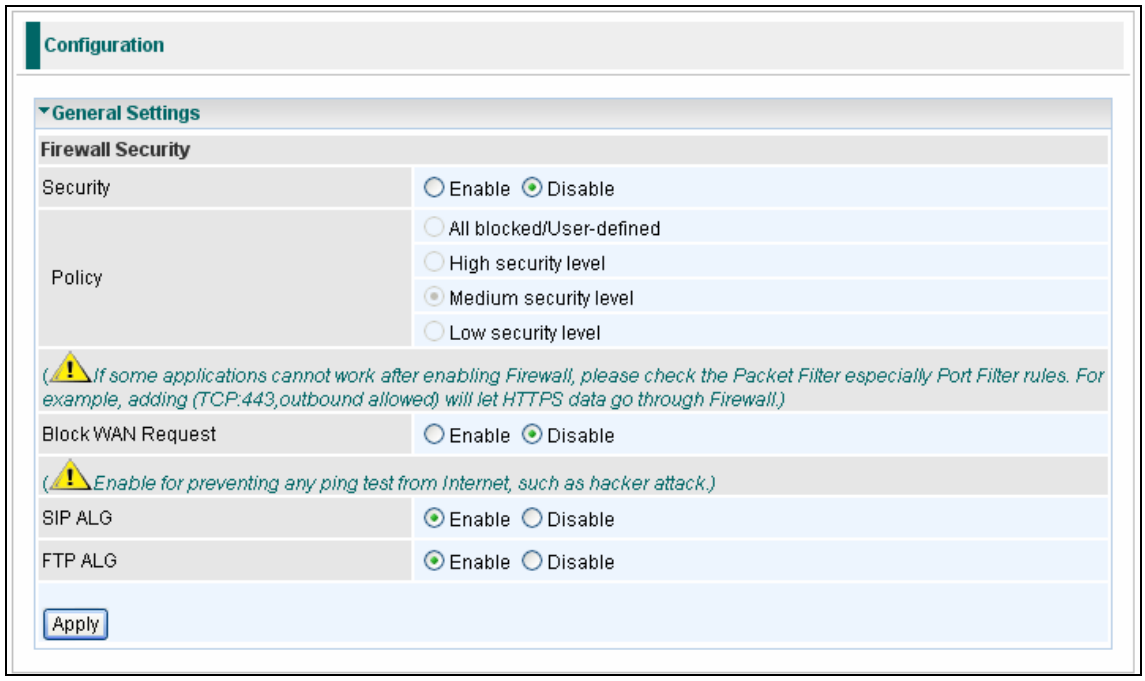
In order to prevent unauthorized access to the router's configuration interface, it requires all users to login with a password. Users can set up multiple user accounts.



4.3.4 Firewall & Access Control

General Settings

Router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from the LAN, as well as helping to prevent attacks from hackers. Besides NAT, the router acts as a “natural” Internet firewall, as all PCs on the LAN will use private IP addresses that cannot be directly accessed from the Internet. 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 in Port Filter section.

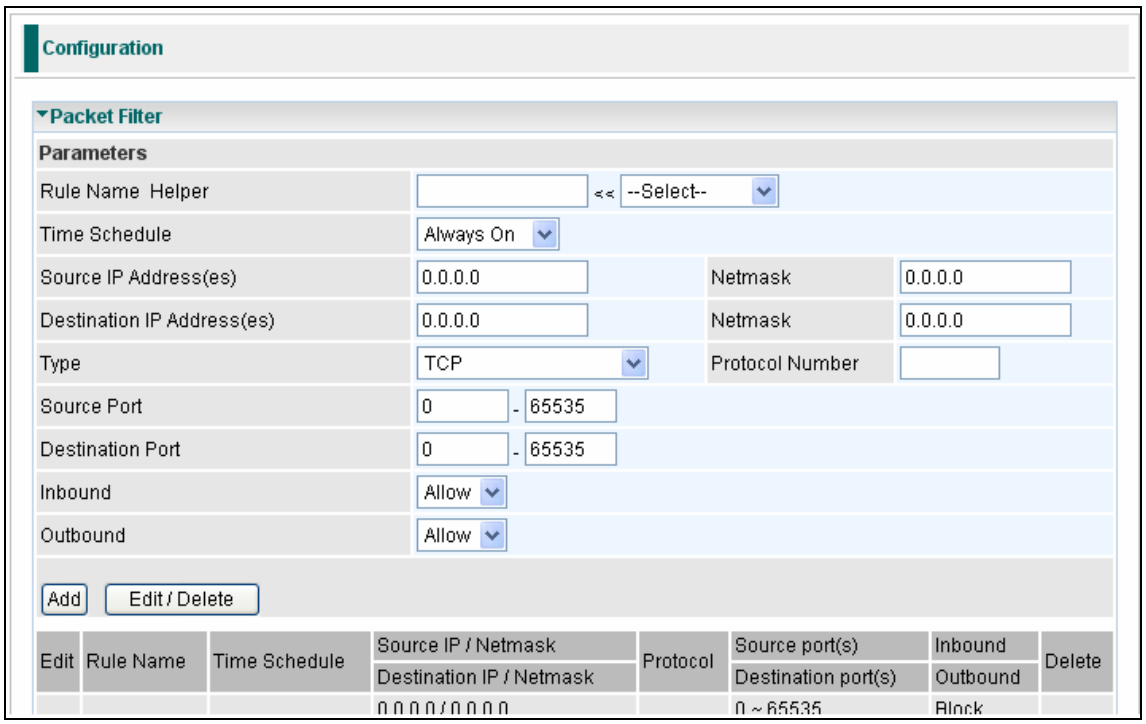


Parameter	Description
Firewall Security and Policy	➢ **All blocked/User-defined:** no pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to 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.
Block WAN Request	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.

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 below table for more detail information.

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

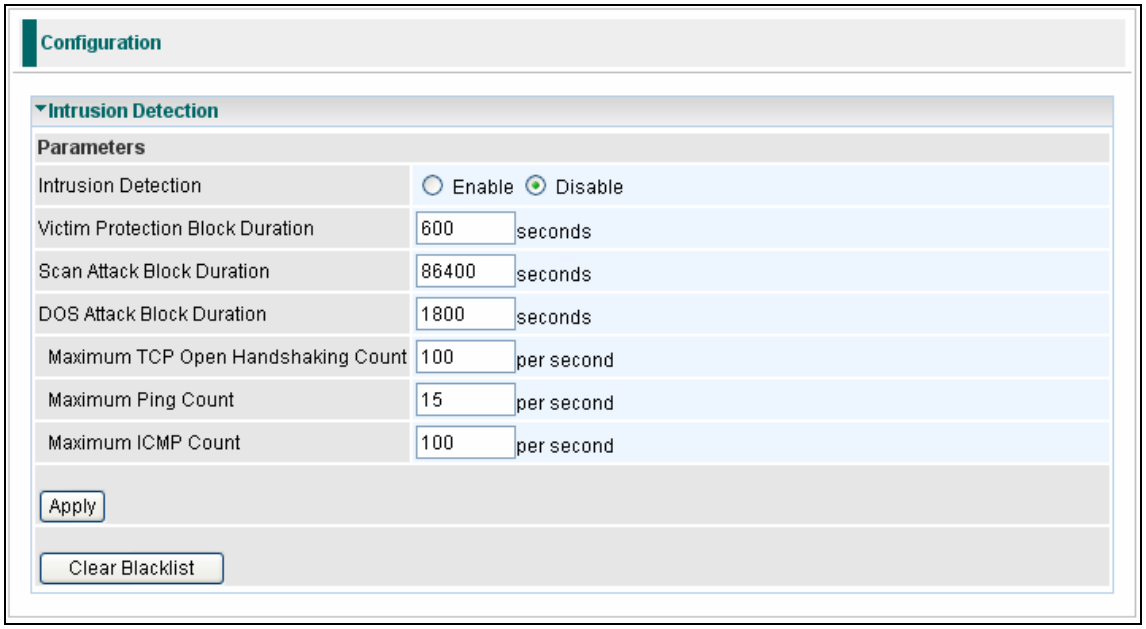


Parameter	Description
Rule Name	Users-define description to identify this entry or click “Select” drop-down menu to select existing predefined rules. The maximum name length is 32 characters.
Time Schedule	It is self-defined time period. Users may specify a time schedule for the prioritization policy. 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. Selecting the Subnet Mask of the IP address range to allow/block the traffic to or form. Set IP address and Subnet Mask to 0.0.0.0 to inactivate the Address-Filter rule.
Source Port	This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. It is recommended that this option be configured by an advanced user. Default: 0 ~ 65535.
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 changes.*

Intrusion Detection

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.



Parameter	Description
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'. Some attack types are denied immediately without using the Blacklist function, such as Land attack and Echo/CharGen scan. Default: False (Disabled).
Block Duration	➢ Victim Protection Block Duration: This is the duration for blocking Smurf attacks. Default: 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: 86400 seconds.
Intrusion Detection	If enabled, IDS will block Smurf attack attempts. Default: False.
Max TCP Open Handshaking Count	This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default: 100 TCP SYN per seconds.

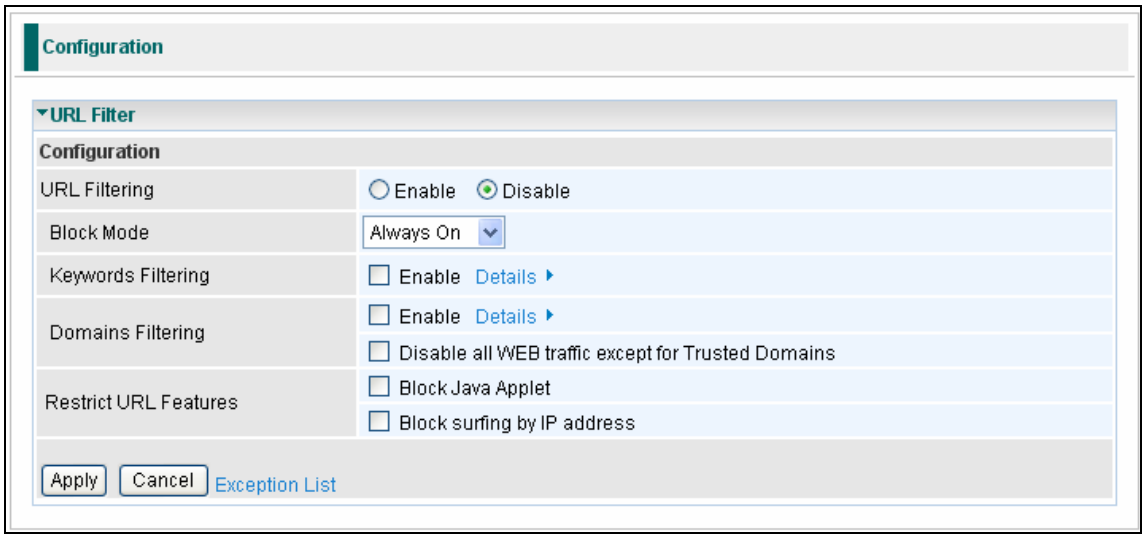
Max PING Count	This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default: 15 ICMP Echo Requests (PING) per second.
Max ICMP Count	This is a threshold to decide whether an ICMP flood is occurring or not. Default: 100 ICMP packets per seconds except ICMP Echo Requests (PING).

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

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

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 users to prevent clients on the network from accessing particular websites by their URL. There are no pre-defined URL filter rules and users can add filter rules to meet their requirements.

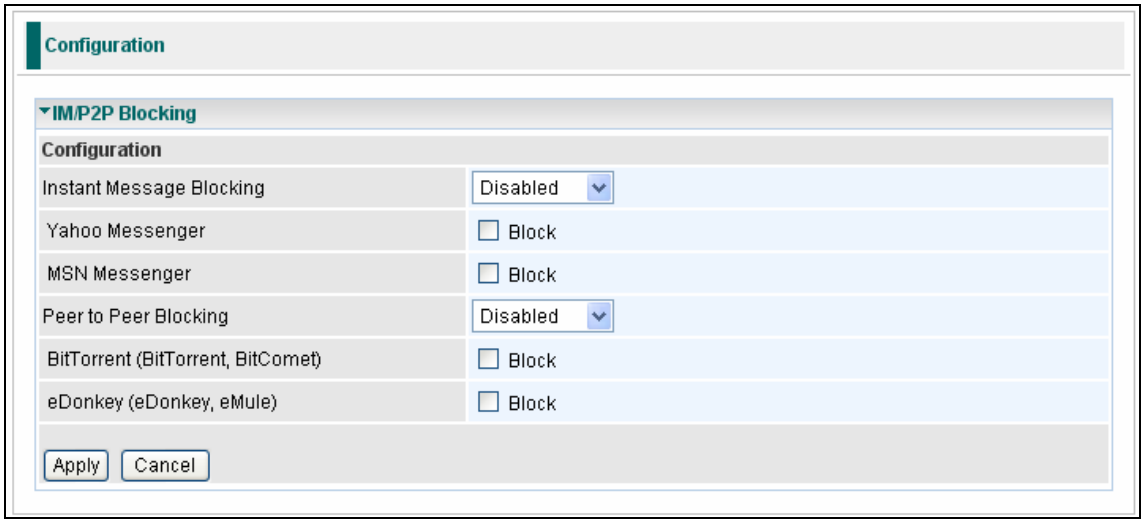


Parameter	Description
Enable/Disable	To enable or disable URL Filter feature.
Block Mode	➢ **Disabled:** No action will be performed by the Block Mode. ➢ **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day. ➢ **TimeSlot1 ~ TimeSlot16:** It is self-defined time period. Users 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, users will specify keyword list for router to check whether the phrase is contained in the URL to determine accessibility. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.
Domains Filtering	This function checks the whole URL and not the IP address to determine whether domains to block or allow. If it matches, the URL request will be sent (Trusted) or otherwise dropped (Forbidden).

Restrict URL Features	➢ **Block Java Applet:** This function can block Web content that includes the Java Applet. It is to prevent someone who wants to damage the 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 the 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 over the Internet.

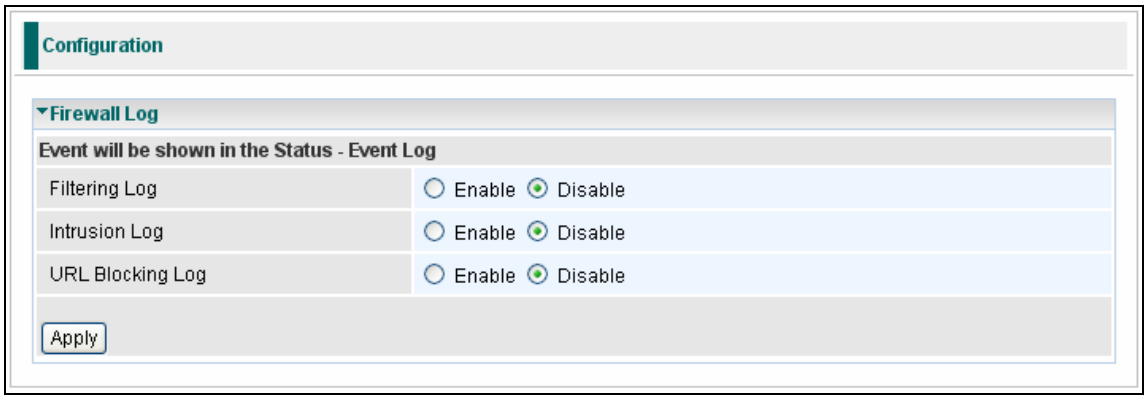


Parameter	Description
Instant Message Blocking	➢ **Disabled:** Instant Message blocking is not triggered. No action will be performed. ➢ **Always On:** Action is enabled. ➢ **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. Users may specify the time period to trigger the blocking, i.e. 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. Make sure users enabled the Instant Message Blocking first.
Peer to Peer Blocking	➢ **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. Users 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 and eDonkey. Make sure users enable the Peer to Peer Blocking first.

Firewall Log

Firewall Log display log information of any unexpected action with the firewall settings. Check the Enable box to activate the logs. Log information can be seen in the Status – Event Log after enabling.

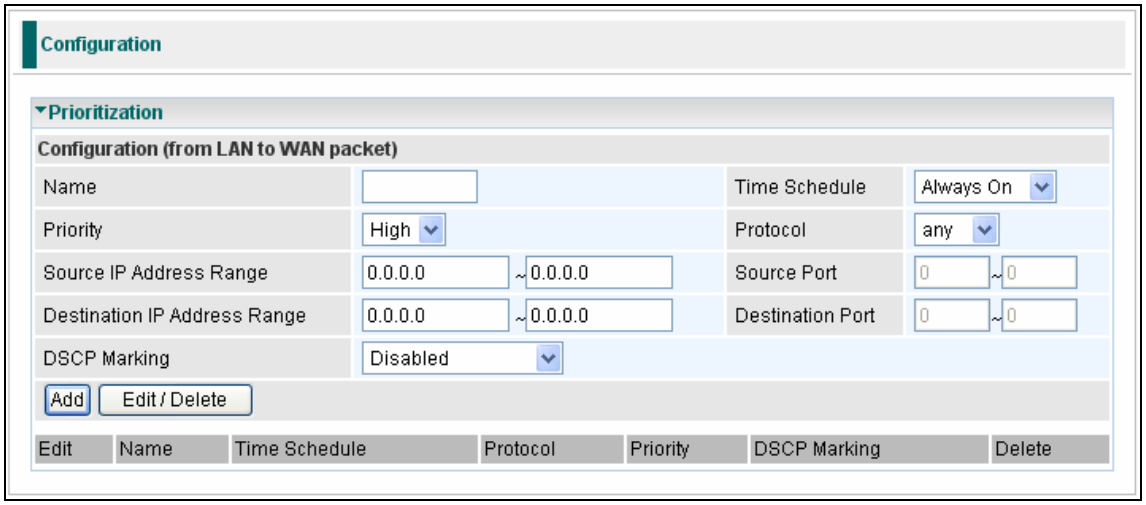


4.3.5 QOS – Quality of Service

QoS function helps user to control the network traffic for each application from LAN (Ethernet and/or Wireless) to WAN (Internet). It facilitates the control to the different quality and throughput for each application when the system is running with full loading.

Prioritization

And the balances of utilization for each priority are High (60%), Normal (30%) and Low (10%). To delete the application, users can chose 'Delete' option and then click **<Edit/Delete>**.

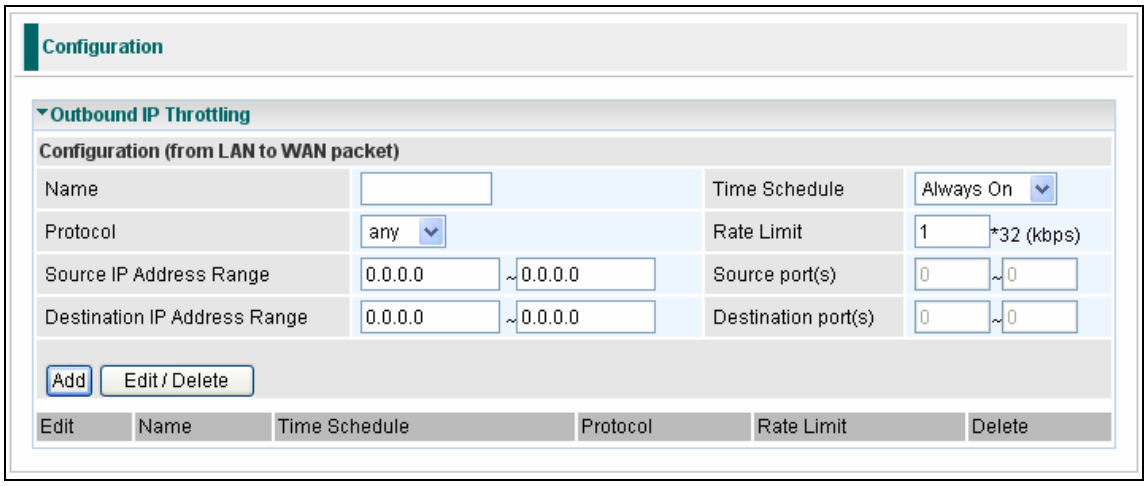


Parameter	Description
Name	User-define description to identify this new policy/application.
Time Schedule	Scheduling the prioritization policy.
Priority	The priority given to each policy/application. Default: High.
Protocol	The name of supported protocol.
Source IP Address Range	The source IP address or range of packets to be monitored.
Destination IP address Range	The destination IP address or range of packets to be monitored.
Source Port	The source port of packets to be monitored.
Destination Port	The destination port of packets to be monitored.
DSCP Marking	Differentiated Services Code Point (DSCP) 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.

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)

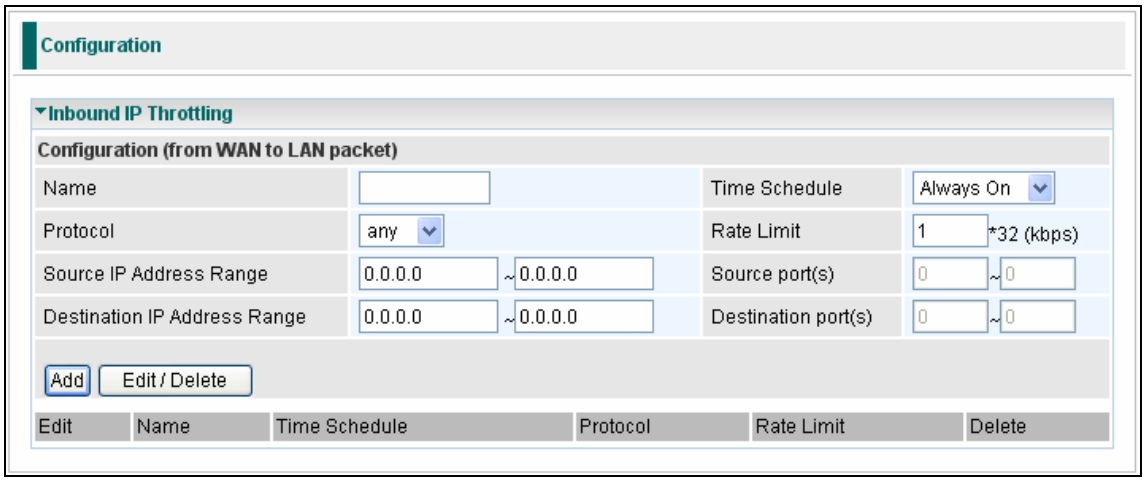
IP Throttling allows user to limit the speed of IP traffic. The value entered will limit the speed of the application that user set to the specified value which is multiple of 32kbps.



Parameter	Description
Name	User-define description to identify this new policy/name.
Time Schedule	Scheduling the 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 user to limit the speed of IP traffic. The value entered will limit the speed of the application that the user has set to the specified value in multiple of 32kbps.



Parameter	Description
Name	User-define description to identify this new policy/application.
Time Schedule	Scheduling the prioritization policy. Refer to Time Schedule for more information.
Protocol	The name of supported protocol.
Rate Limit	To limit the speed of inbound traffic.
Source IP Address Range	The source IP address or range of packets to be monitored.

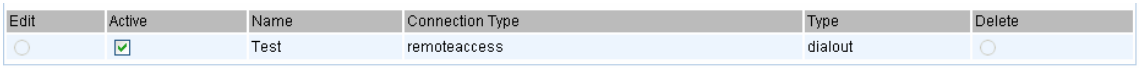
Source Port(s)	The source port of packets to be monitored.
Destination IP Address Range	The destination IP address or range of packets to be monitored.
Destination Port(s)	The destination port of packets to be monitored.

4.3.6 VPN

Virtual Private Network (VPN) is a connection between two end points. It allows private data to be sent securely over a public network, such as Internet. VPN establishes a private network that can send data securely between two networks. We call this is by creating a “tunnel”. A VPN tunnel connects the two PCs or networks. The SP3366 VPN Modem Router uses industry standard VPN protocol. However, due to variations in how manufactures interpret these standards, many VPN products are not interoperable.

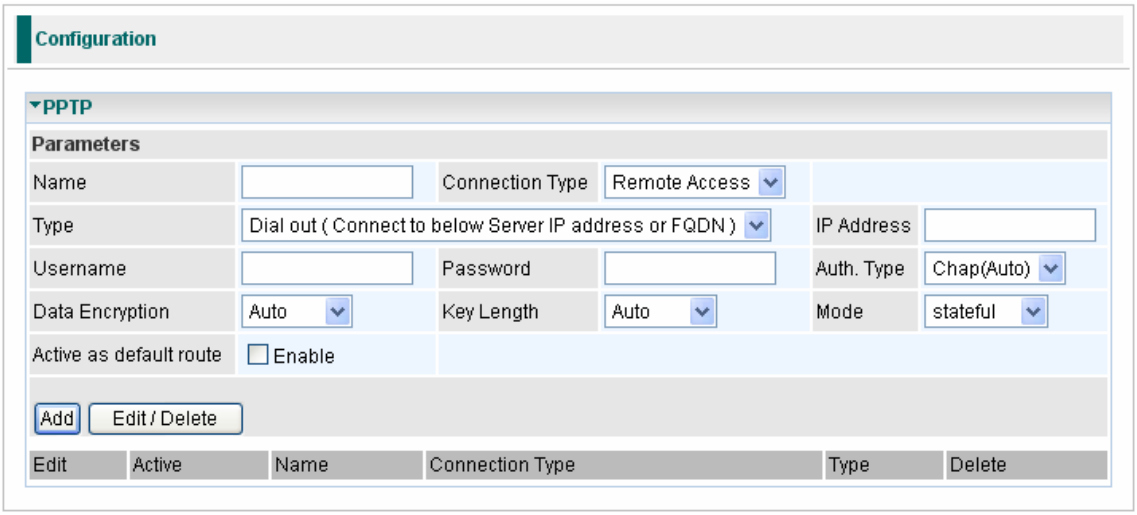
PPTP

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



Parameter	Description
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.
Connection Type	It informs PPTP tunnel connection condition.
Type	This refers to the router to operates as a client or a server, ‘Dialout’ or ‘Dialin’ respectively.

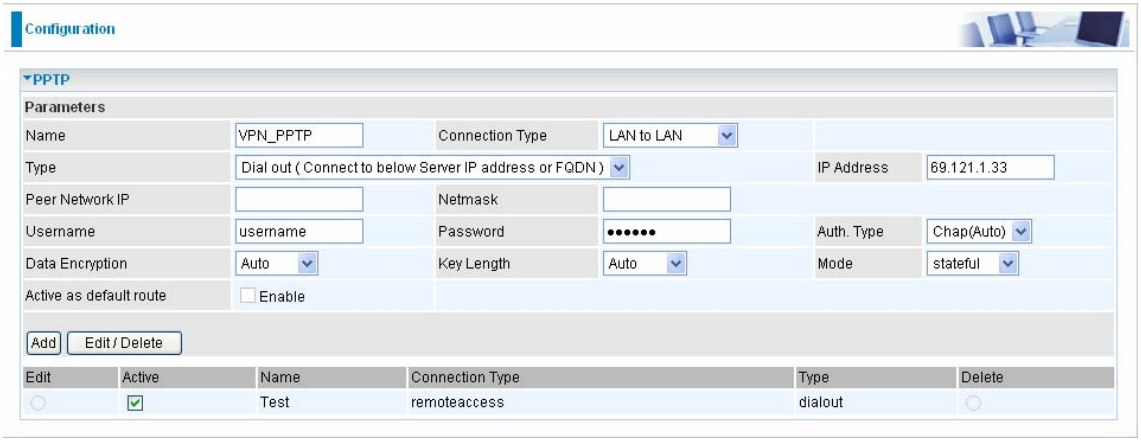
Remote Access



Parameter	Description
Name	A given name for the connection.
Connection Type	Remote Access or LAN to LAN.
Type	Check 'Dial Out' if users want the router to operate as a client (connecting to a remote VPN server, e.g. office server), check 'Dial In' to operates as a VPN server. ➢ When configuring the router as a Client, enter the remote Server IP Address (or Domain Name) users wish to connect to. ➢ When configuring the 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	Users can either allow the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). 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. Default: Auto
Data Encryption	Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default: Auto
Key Length	The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default: Auto

Mode	Users may select ‘Stateful’ or ‘Stateless’ mode. The key will be changed every 256 packets when users select ‘Stateful’ mode. If users 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.
Active	This function activates or deactivates the PPTP connection. Check ‘Active’ checkbox if users want the protocol of tunnel to be activated and vice versa.

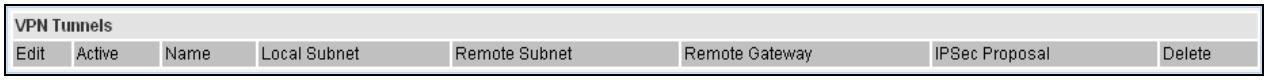
LAN to LAN



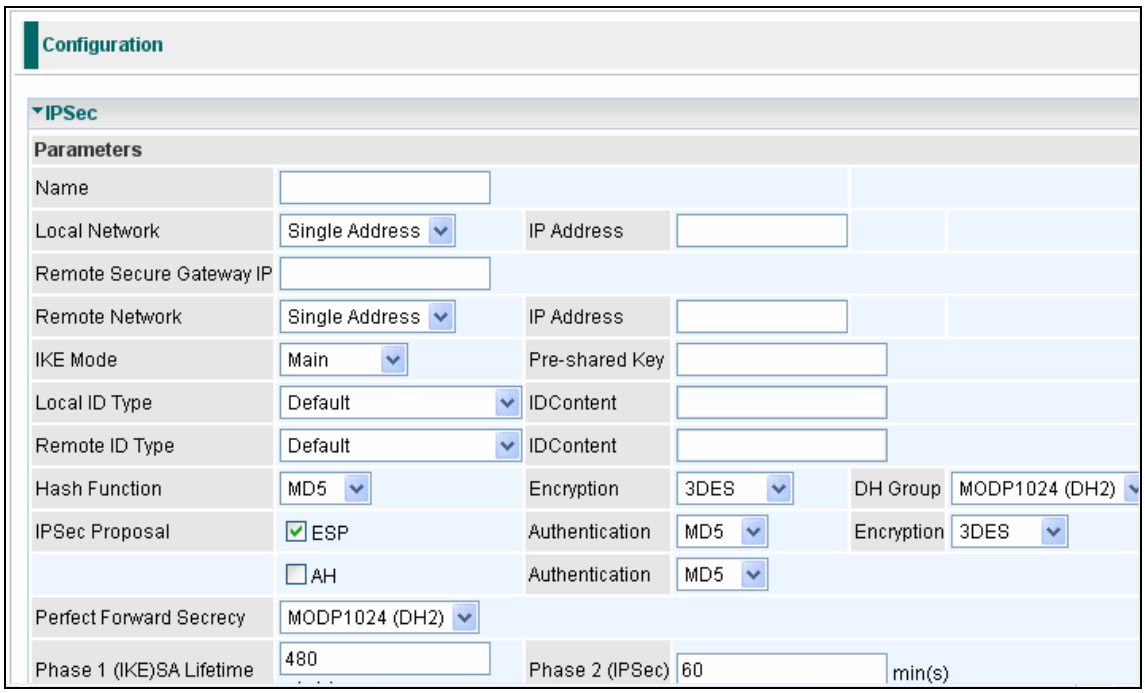
Parameter	Description
Name	A given name for the connection.
Connection Type	Remote Access or LAN to LAN.
Type	Check ‘Dial Out’ if users want the router to operate as a client (connecting to a remote VPN server, e.g. office server), check ‘Dial In’ to operates as a VPN server. ➢ When configuring the router as a Client, enter the remote Server IP Address (or Domain Name) users wish to connect to. ➢ When configuring the 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	Users can either allow the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). 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. Default: Auto
Data Encryption	Data sent over the VPN connection can be encrypted by an MPPE algorithm. Default: Auto
Key Length	The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default: Auto
Mode	Users may select 'Stateful' or 'Stateless' mode. The key will be changed every 256 packets when users select 'Stateful' mode. If users 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.
Active	This function activates or deactivates the PPTP connection. Check 'Active' checkbox if users want the protocol of tunnel to be activated and vice versa.

IPSec



Parameter	Description
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.
Name	A given name for 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.

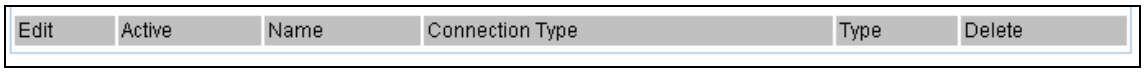


Parameter	Description
Name	A given name for the connection.
Local Network	Set the IP address, subnet or address range of the local network. ➢ Single Address: The IP address of the local host. ➢ Subnet: The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies 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.
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. ➢ 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: Users can use 128, 192 or 256 bits as encryption method.
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. ➢ 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, 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. ➢ 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, user 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).

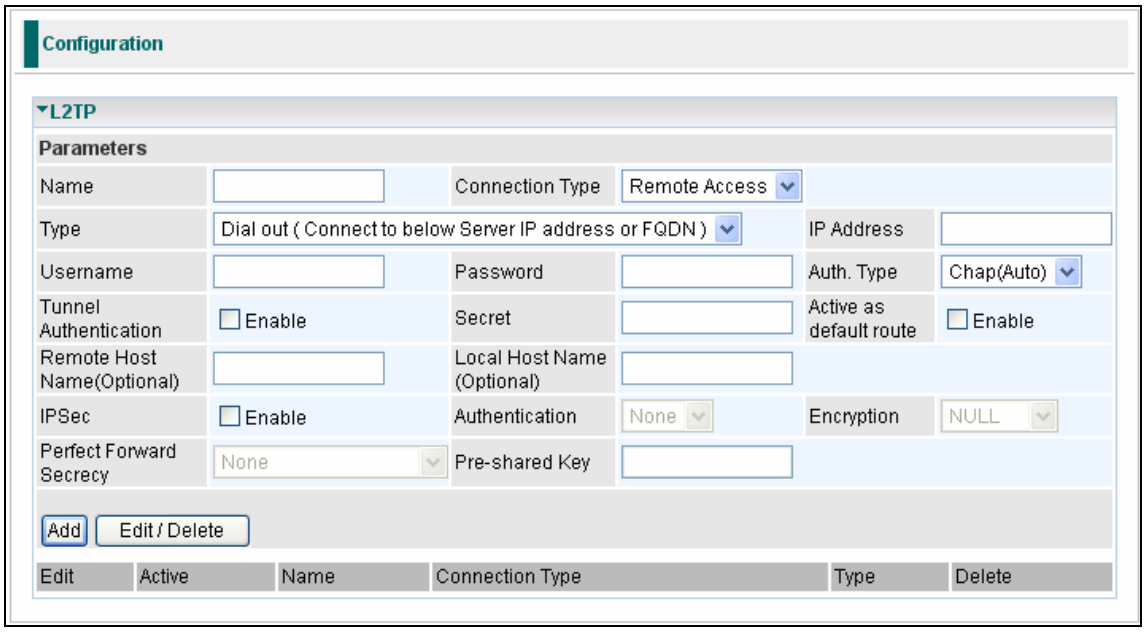
Local ID	Content: Input ID's information, like domain name www.ipsectest.com.
Remote ID	Identifier: Input remote ID's information, like domain name www.ipsectest.com.
SA Lifetime	Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key 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'. 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: 0.0.0.0 (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 and 0 second disables the function.
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.

L2TP



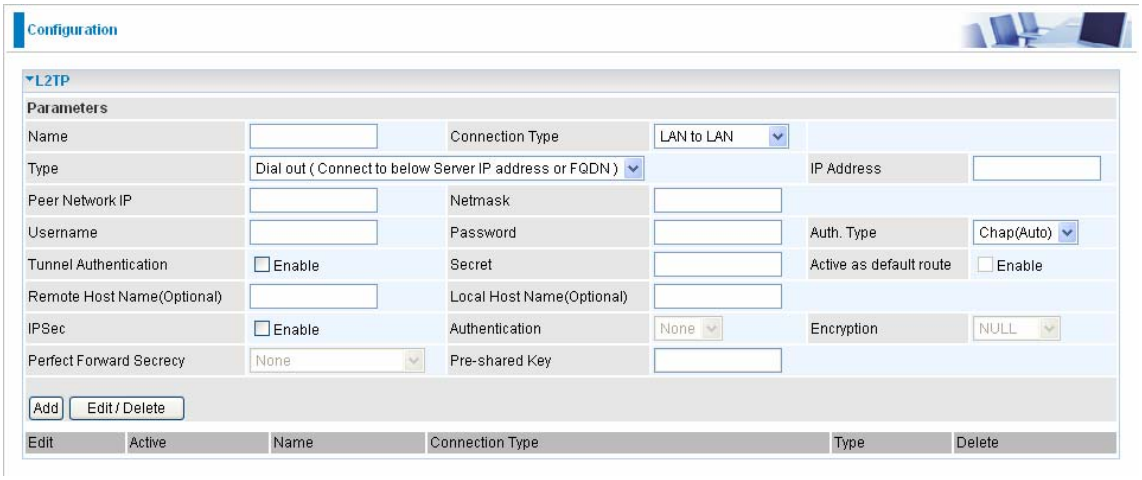
Parameter	Description
Active	This function activates or deactivates the L2TP connection. Check Active checkbox if users want the protocol of tunnel to be activated and vice versa.
Name	This is a given name of the connection.
Connection Type	It informs the user of L2TP tunnel connection condition.
Type	This refers to the router to operate as a client or a server, 'Dialout' or 'Dialin' in respectively.

Remote Access



Parameter	Description
Name	A given name for the connection
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.
Type	Check 'Dial Out' if users want the router to operate as a client (connecting to a remote VPN server, e.g. office server), check 'Dial In' to operates as a VPN server. ➢ When configuring the router as a Client, enter the remote Server IP Address (or Domain Name) users wish to connect to. ➢ When configuring the 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	Users can either allow the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). 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. Default: Auto
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.
Local Host Name (Optional)	Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. Default: home.gateway.
IPSec	Enable to include IPSec security into VPN connection. For detail of the parameters, check IPSec VPN sections.

LAN to LAN

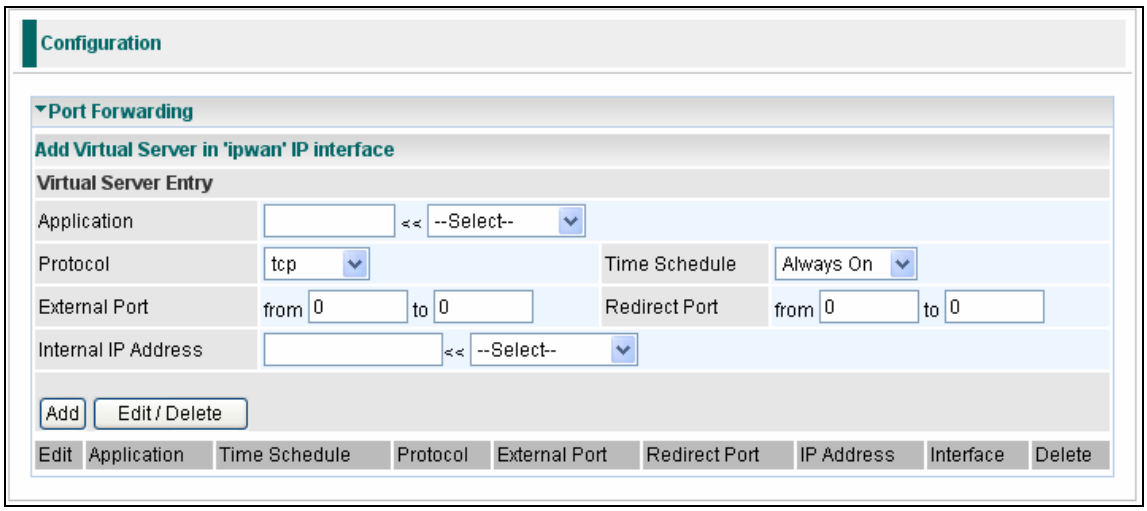

Configuration
L2TP
Parameters
Name
Connection Type
LAN to LAN
Type
Dial out (Connect to below Server IP address or FQDN)
IP Address
Peer Network IP
Netmask
Username
Password
Auth. Type
Chap(Auto)
Tunnel Authentication
Enable
Secret
Active as default route
Enable
Remote Host Name(Optional)
Local Host 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

Parameter	Description
Name	A given name for the connection
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.
Type	Check 'Dial Out' if users want the router to operate as a client (connecting to a remote VPN server, e.g. office server), check 'Dial In' to operates as a VPN server. ➢ When configuring the router as a Client, enter the remote Server IP Address (or Domain Name) users wish to connect to. ➢ When configuring the 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	Users can either allow the router to determine the authentication type to use, or else manually specify CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). 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. Default: Auto
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.
Local Host Name (Optional)	Enter hostname of Local VPN device that is connected / establishes a VPN tunnel. Default: home.gateway.
IPSec	Enable to include IPSec security into VPN connection. For detail of the parameters, check IPSec VPN sections.

4.3.7 Virtual Server/ 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 users wish to run a server on the 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 usually needs to configure the router to forward these incoming connection attempts using specific ports to the PC on the network running the application. User will also need to use port forwarding if you want to host an online game server.

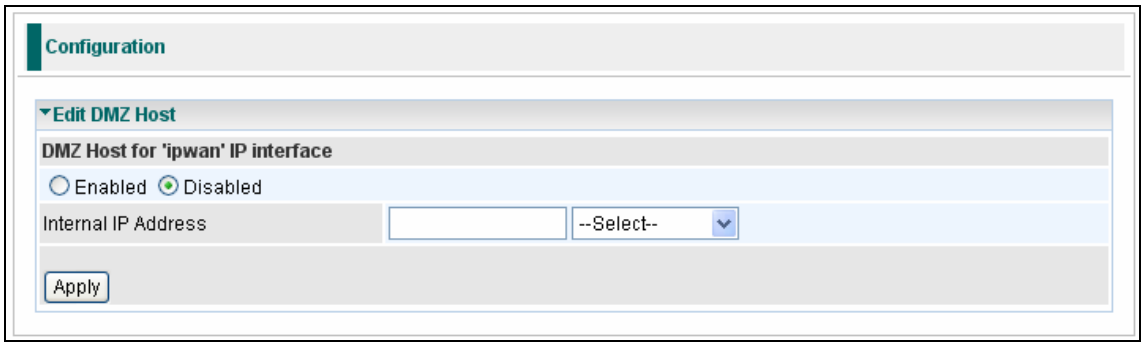
The reason for this is that when using NAT, client’s publicly accessible IP address will be used by and point to the router, which then needs to deliver all traffic to the private IP addresses used by LAN PCs. Please see the WAN configuration section of this manual for more information on NAT. The device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



Parameter	Description
Application	Users-define description to identify this entry or click 'Selection' drop-down menu to select existing predefined rules. 'Selection' dropdown contains 20 predefined rules. Application, Protocol and External/Redirect Ports will be automatically entered after the selection.
Protocol	It is the supported protocol for the virtual server. In addition to specifying the port number to be used, users 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 the virtual server. Users 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. 'Selection' drop-down menu lists all existing PCs connecting to the network. Users may assign a PC with IP address and MAC from this list.

4.3.8 DMZ Host

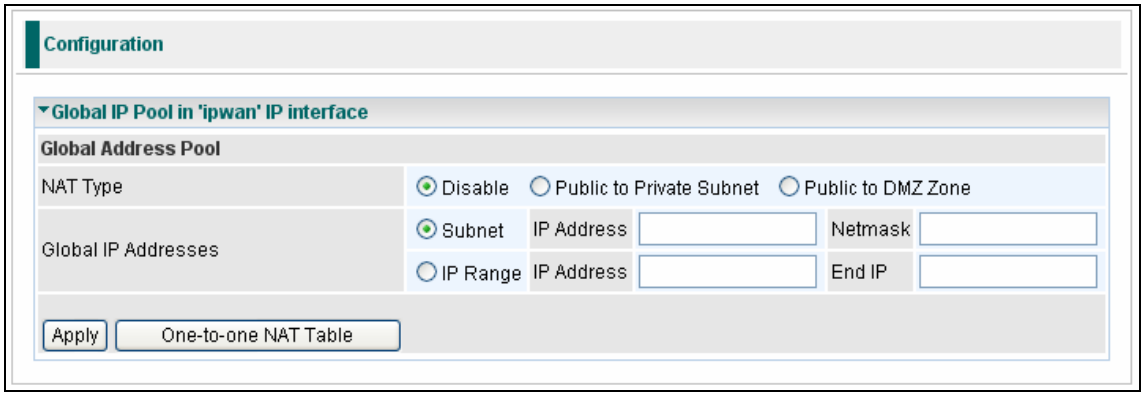
The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host. Make sure when a packet received, it does not use a port number used by any other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



Parameter	Description
Enable/Disable	To activate the function, select ‘Enable’.
Internal IP Address	Give a static IP address to the DMZ Host when ‘Enabled’ is selected. Be aware that this IP will be exposed to the WAN/Internet. ‘Selection’ drop-down menu lists all existing PCs connecting to the network. Users may assign a PC with IP address and MAC from this list.

4.3.9 One-to-One NAT

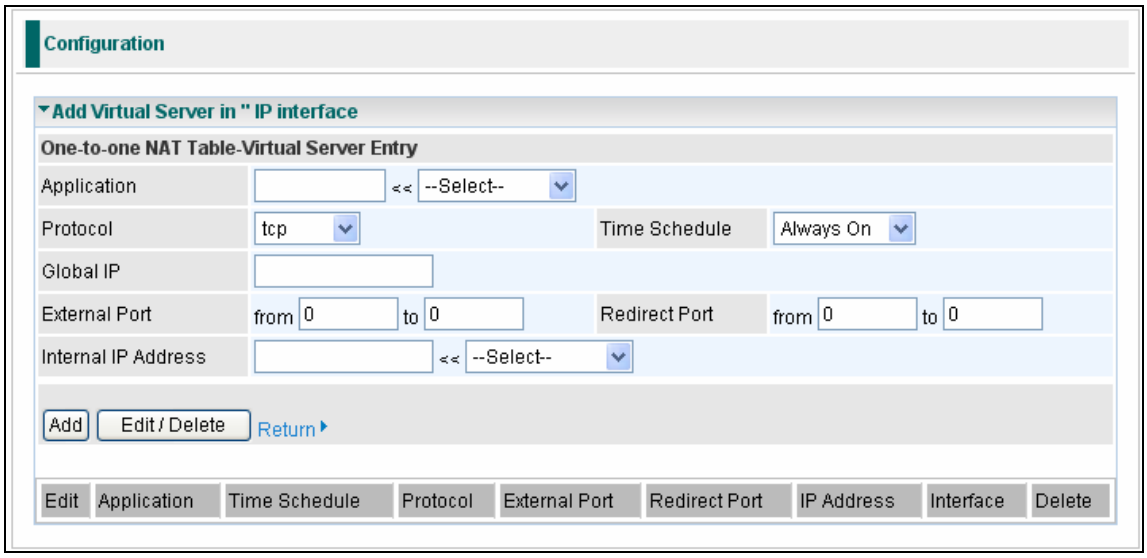
One-to-One NAT maps a specific private/local IP address to a global/public IP address. If users have multiple public/WAN IP addresses from the ISP, they are eligible for One-to-One NAT to utilize these IP addresses. To access the function: Configuration→Virtual Server→Edit One-to-one NAT.



Parameter	Description
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 the ISP. If the ISP has provided this information, users may insert it here. Otherwise, use IP Range method. **IP Range:** The IP address range of the public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10. Press **<Apply>** after entering the information.

Click <**One-to-One NAT Table>** to create a new One-to-One NAT rule.



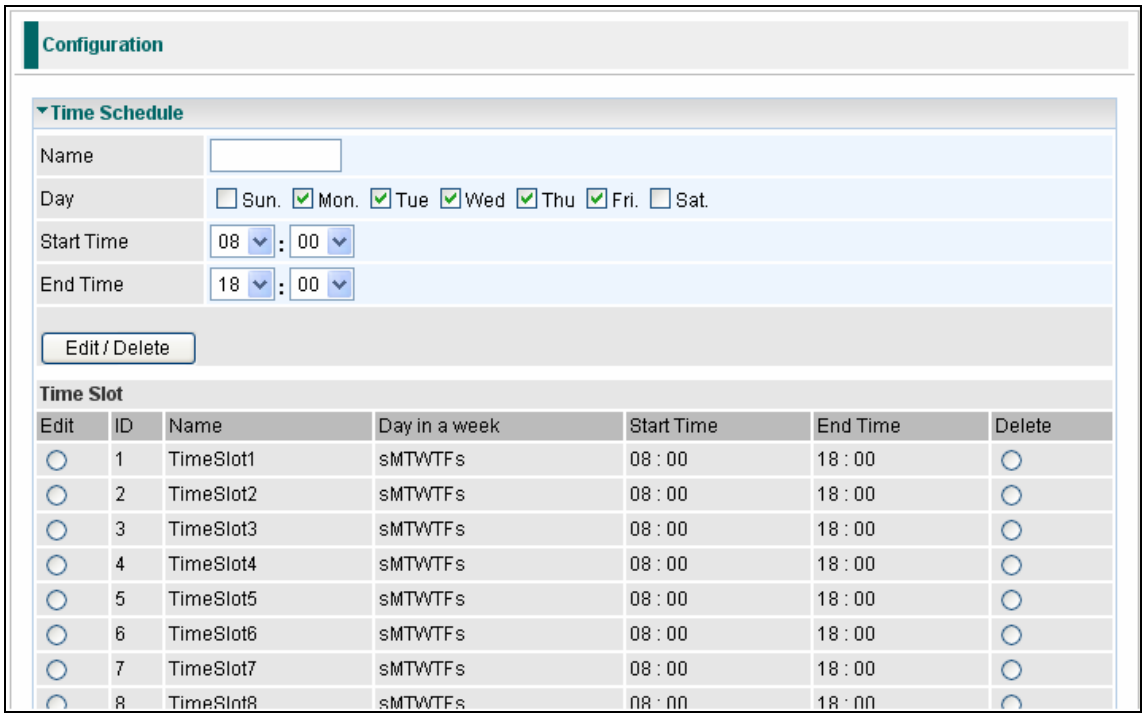
Parameter	Description
Application	Users-defined description to identify this entry or click drop-down menu to select existing predefined rules. 'Selection' dropdown contains 20 predefined rules. Application, Protocol and External/Redirect Ports will be automatically entered after the selection.
Protocol	It is the supported protocol for the virtual server. In addition to specifying the port number to be used, users 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 the virtual server. Users 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. ‘Selection’ drop-down menu lists all existing PCs connecting to the network. Users may assign a PC with IP address and MAC from this list.

Click on **<Add>** button to apply the changes.

4.3.10 Time Schedule

The ‘Time Schedule’ supports up to 16 time slots which helps users to manage the Internet connection. In each time profile, users may schedule specific day(s) i.e. Monday through Sunday to restrict or allow 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. The router time should correspond with the local time. If the time is not set correctly, ‘Time Schedule’ will not function properly.



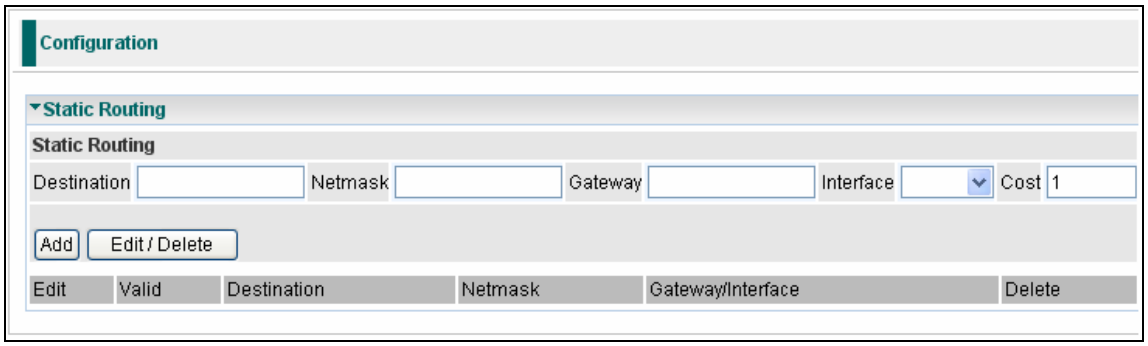
Parameter	Description
ID	This is the index of the time slot.
Name	A user-define description to identify this time portfolio.
Day in a week	The default is set from Monday through Friday. Users may specify the days for the schedule to be applied.

Start Time	The default is set at 8:00 AM. Users may specify the start time of the schedule.
End Time	The default is set at 18:00 (6:00PM). Users may specify the end time of the schedule.

4.3.11 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.

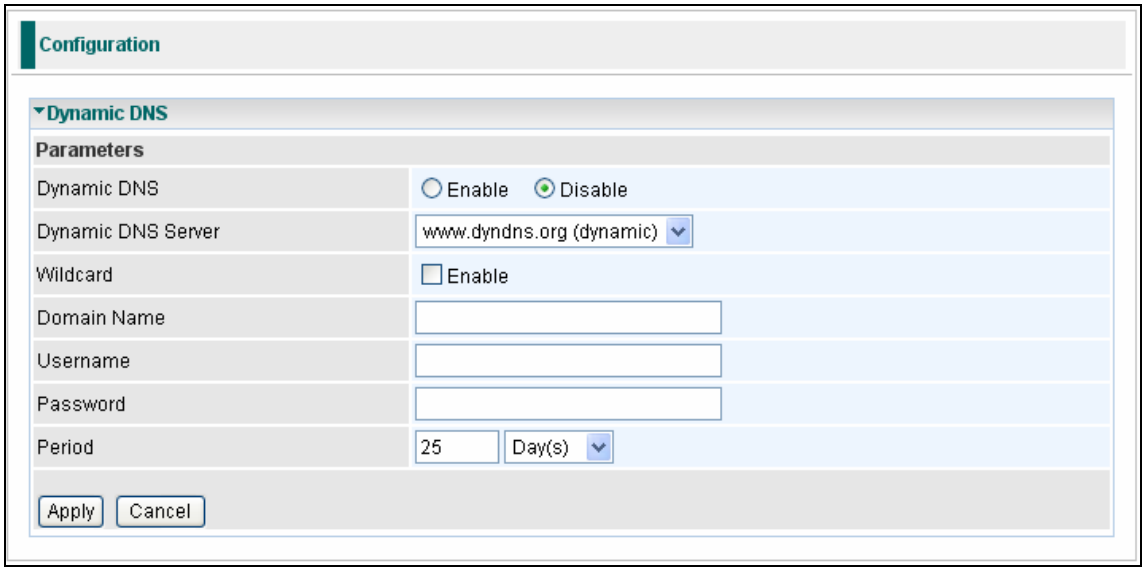
Static Route



Parameter	Description
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.

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 the ADSL connection, so that anyone wishing to connect to the users may use the domain name, rather than having to use the dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned by your ISP. Users will first need to register and establish an account with the Dynamic DNS provider, for example http://www.dyndns.org/

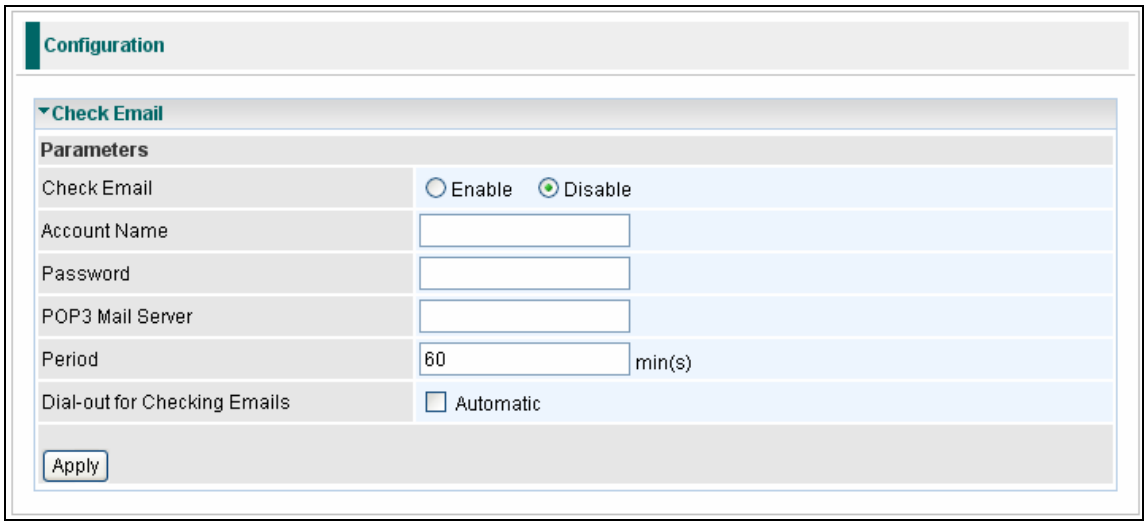


Parameter	Description
Dynamic DNS Server	Select the DDNS service user have established an account with.
Domain Name, Username and Password	Enter the registered domain name, username and password for this service.
Period	Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per settings, the router will perform an update when the dynamic IP address changes.

Check Email

This function allows the router to check the POP3 mailbox for new Email messages. The Mail LED on the router will light when it detects new messages waiting for download. Users may also view the status of this function using the ‘Status’ – ‘Email

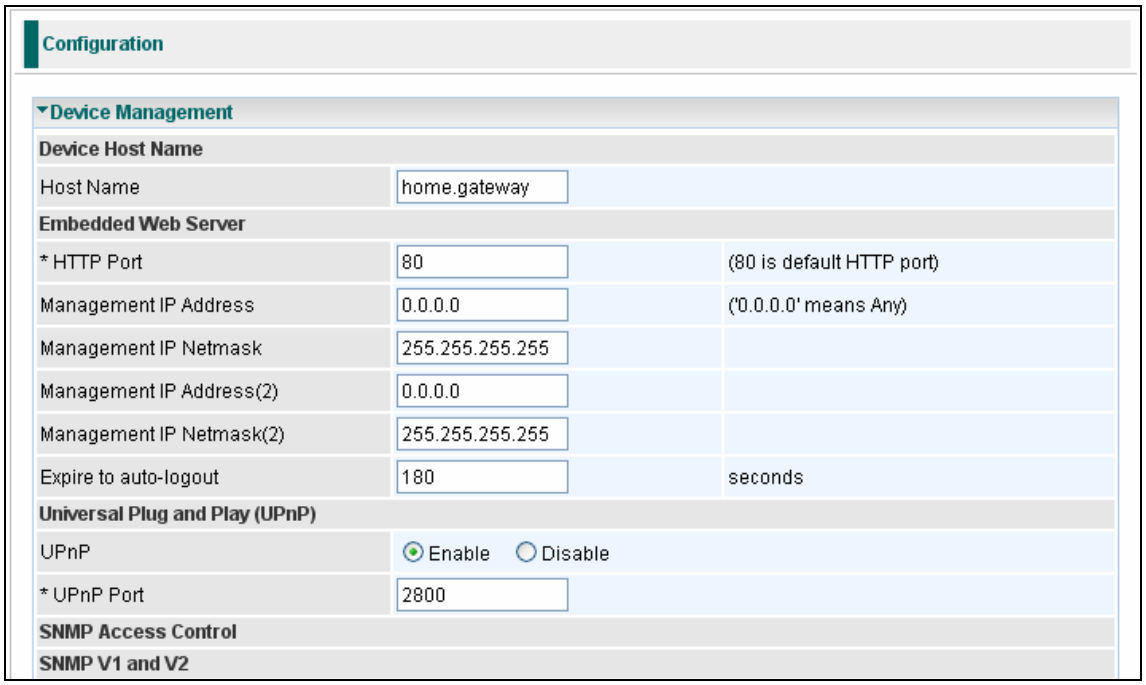
Checking' section of the web interface, which also provides details on the number of new messages waiting. See the 'Status' section of this manual for more information.



Parameter	Description
Account Name	Enter the name (login) of the POP3 account users wish to check. Normally, it is the text in the email address before the "@" symbol. If users have trouble with the detail, please contact the ISP.
Password	Enter the account's password.
POP3 Mail Server	Enter the (POP) mail server name. User's Internet Service Provider (ISP) or network administrator will be able to supply the information.
Period	Enter the value in minutes between periodic mail checks.
Dial-out for checking emails	When the function is enabled, the ADSL router will connect to the ISP automatically to check emails if the Internet connection dropped. Please be careful when using this feature if the ADSL service is charged by online time.

Device Management

The 'Device Management' allows user to control the router's security options and device monitoring features.



Parameter	Description
Host Name	The Host Name cannot only contain one word. There should be two words connected with a full stop (.). Example: Host Name: homegateway ==> Incorrect Host Name: home.gateway or my.home.gateway ==> Correct)
HTTP Port	This is the port number for router's embedded web server (for web-based configuration). The default value is the standard HTTP port, 80.
Management IP Address	Users 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 all 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.

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. It makes tasks such as port forwarding much easier by letting the application control the required settings and removing the need for the user to control advanced configuration. 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.
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 are being used, user may wish to change the port.
Read Community:	Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, user with this IP address will be able to view the data.
Write Community:	Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name matches, 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 matches, users from this IP address will sent SNMP Traps.
SNMP V3	Specify a name and password for authentication. 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.

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.

MIB Support:

- From RFC 1213 (MIB-II):
  - System group
  - Interfaces group

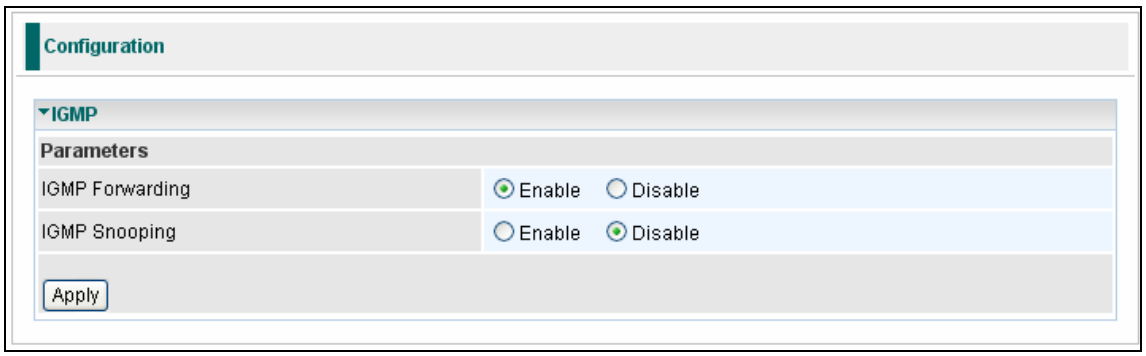
- Address Translation group
- IP group
- ICMP group
- TCP group
- UDP group
- EGP (not applicable)
- Transmission
- SNMP group

- 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

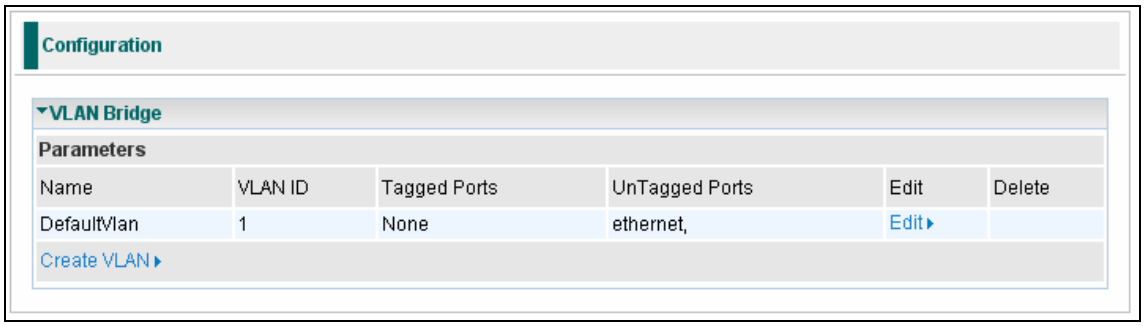
IGMP, known as Internet Group Management Protocol, is used to management hosts from multicast group.



Parameter	Description
IGMP Forwarding	Accepting multicast packet. Default: Enable.
IGMP Snooping	Allowing switched Ethernet to check and make correct forwarding decisions. Default: Disable.

VLAN Bridge

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



Parameter	Description
Edit	Edit the member ports in selected VLAN group.
Create VLAN	To create another VLAN group.

4.4 Logout

To exit the router's web interface, choose 'Logout'. Please ensure that user have saved the configuration settings before 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. Users 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.