810VGTX

ADSL2+ Integrated Access Device with 3G Failover

USER MANUAL

BILLION

www.telkom.co.za

Telkom

Table of Contents

CHAPTER 1: INTRODUCTION

Introduction to your Router

Welcome to the 3G/VoIP/802.11g/ADSL2+/VPN Firewall Router. The router is an “all-in-one” ADSL router, combining an ADSL modem, ADSL router and Ethernet network switch functionalities, providing everything you need to get the machines on your network connected to the Internet over your ADSL broadband connection. With features such as an ADSL Quick-Start wizard and DHCP Server, you can be online in no time at all and with a minimum of fuss and configuration, catering for first-time users to the guru requiring advanced features and control over their Internet connection and network.

Features

Express Internet Access

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

3G

A 3G-based Internet connection (requires an additional 3G USB modem); with automatic fail-over to ensure an always-on Internet connection in the event that one of your Internet services fails. Secure WLAN setup is simplified by the web browser-based configuration for easy access to the Internet wherever a 3G connection is available - whether you're seated at your desk or taking a cross-country train trip.

802.11g Wireless AP with WPA Support

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

Fast Ethernet Switch

A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.

Multi-Protocol to Establish a Connection

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

Quick Installation Wizard

It supports a WEB GUI page to install this device quickly. With this wizard, end users can enter the information easily which they get from their ISP, then surf the Internet immediately.

Universal Plug and Play (UPnP) and UPnP NAT Traversal

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

Network Address Translation (NAT)

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

SOHO Firewall Security with DoS and SPI

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

Domain Name System (DNS) Relay

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo. com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.

Dynamic Domain Name System (DDNS)

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname. This dynamic IP address is the WAN IP address. For example, to use the service, you must first apply for an account from a DDNS service like http://www.dyndns.org/. More than 5 DDNS servers are supported.

Quality of Service (QoS)

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

Virtual Server ("port forwarding")

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

Rich Packet Filtering

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

Dynamic Host Configuration Protocol (DHCP) Client and Server

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

Static and RIP1/2 Routing

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

Simple Network Management Protocol (SNMP)

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

Web based GUI

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

Firmware Upgradeable

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

Rich Management Interfaces

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

Virtual Private Network (VPN)

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

CHAPTER 2: INSTALLING THE ROUTER

Important note for using this router

Warning

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

Attention

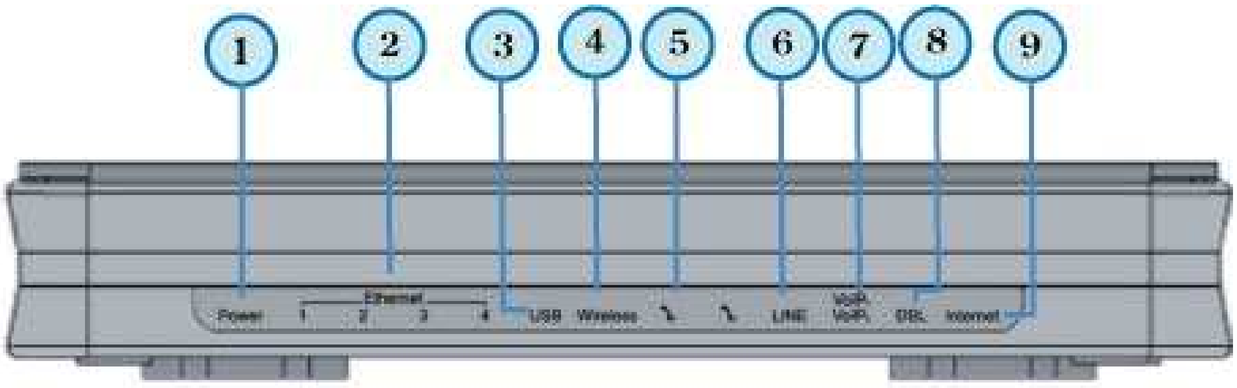
- ✓ **Place the router on a stable surface.**
- ✓ **Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.**

Package Contents

- Billion 810VGTX Router
- CD-ROM containing this online manual
- 3 x RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5) Cable
- Console tool kit
- Integrated surge and AC-DC power adapter (12VDC, 1.2A)
- A detachable antenna
- ADSL Micro Filter
- ADSL Splitter
- Quick Start Guide

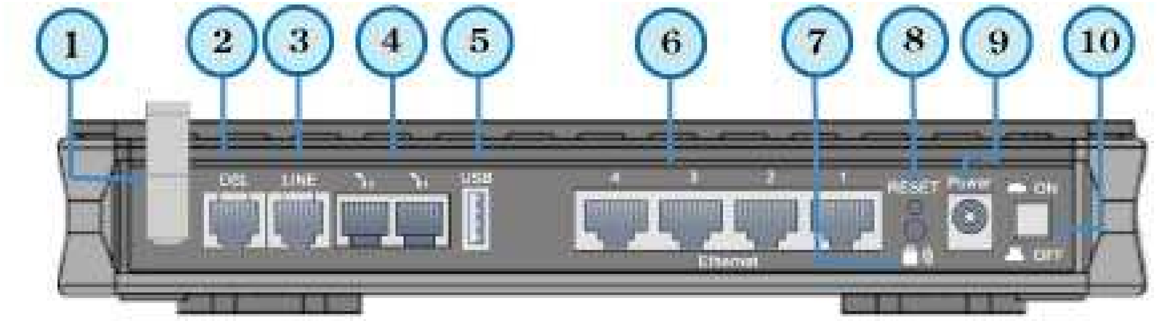
Device Description

The Front LEDs



LED		Meaning
1	**Power**	Both red and green LEDs lit together when power is ON. Lit red means system failure. Restart the device or contact Billion for support. Lit green when the device is ready.
2	**Ethernet Port** **1X — 4X** **(RJ-45 connector)**	Lit when one of LAN ports is connected to an Ethernet device. Lit green when the speed of transmission is 100Mbps; Lit orange when the speed of transmission is 10Mbps. Flashing when data is being Transmitted / Received.
3	**USB**	Lit green when the router is connected to a USB device. Flashing when data is received / transmitted
4	**Wireless**	Lit green when the wireless connection is established. Flashes when sending/receiving data.
5	**Phone 1X – 2X** **(RJ-11 connector)**	Lit green when phone is off hook.
6	**LINE**	Lit green when the inbound and outbound calls are transmitted through PSTN.
7	**VoIP 1x-2x** **(RJ-11 connector)**	After SIP registration is complete, the LED will light up green whenever phone 1 is off hook but will light up orange for phone 2. *Note: Orange light also means that both Phone 1 and 2 have been registered correctly at the same time.*
8	**DSL**	Lit Green when the device is successfully connected to an ADSL DSLAM. (“line sync”).
9	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully.

The Rear Ports



NOTE:

- ✓ **Ethernet port #4 can be used as a console port. You need a special console connector which is included in the package to connect with the LAN.**

LED		Meaning
1	**Antenna**	Connect the detachable antenna to this port.
2	**DSL**	Connect this port to the ADSL/telephone network with the RJ-11 cable (telephone) provided.
3	**Line**	Connect this port to the telephone jack on the wall with RJ-11 cable.
4	**Phone** **1X – 2X** (RJ-11 connector)	Connect this port to an analogue phone set with RJ-11 cable.
5	**USB**	Connect the USB cable to this port.
6	**Ethernet 1X — 4X** **(RJ-45 connector)**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps. *Caution: Port 4 can either be LAN or Console port but not both at the same time.*
7	**WPS**	Push WPS button to trigger Wi-Fi Protected Setup function.
8	**RESET**	After the device is powered on, press it to reset the device or restore to factory default settings. 1-3 seconds: reset the device 6 - 8 seconds: restore to factory default settings (this is useful when you have forgotten the router's administrative password). Note: If the reset button is pressed for more than 10 seconds the device will need to be power cycled before normal operation can be resumed.

Cabling

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

Make sure that all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your router have a line filter connected between them and the wall outlet (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If line filter is not installed and connected properly, it may cause problem to your ADSL connection or may result in frequent disconnections.

CHAPTER 3: BASIC INSTALLATION

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

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

There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router. You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 10.0.0.2 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 10.0.0.100 to 10.0.0199). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as these tend to cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

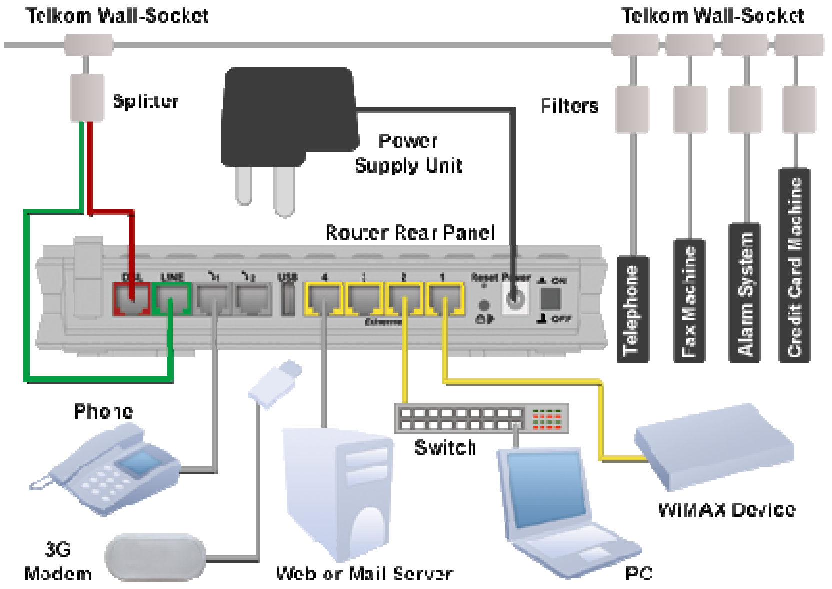
Please follow the following steps to configure your network environment.

NOTE:

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

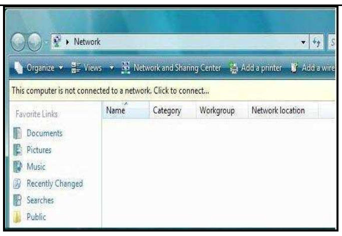
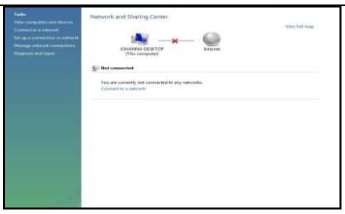
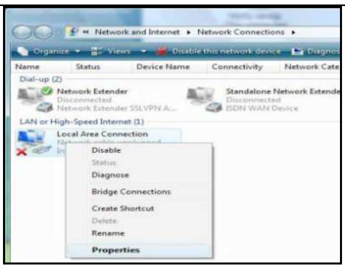
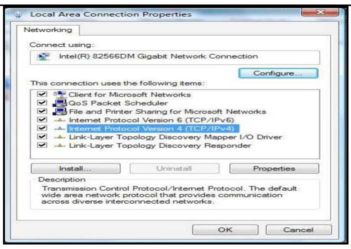
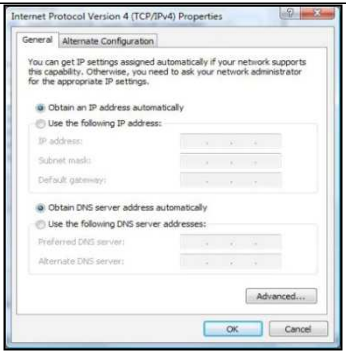
Connecting Your Router

1. Connect the power adapter as illustrated below and power on the device, make sure that the Power LED is lit steadily.
2. Connect your network or computer to the router using the **LAN** (Local Area Network) cable.
3. Connect the ADSL/telephone (**ADSL**) cable to the router's DSL port as illustrated below
4. Connect an RJ11 cable to VoIP port when connecting to an analogue phone set. Refer to figure below.
5. Connect RJ-11 cable to LINE Port when connecting to the telephone wall jack/PSTN network. Refer to figure below.

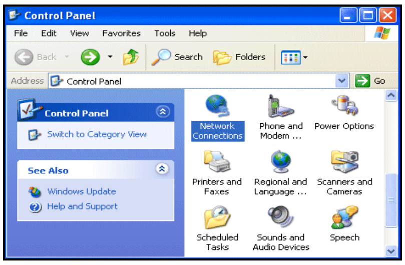
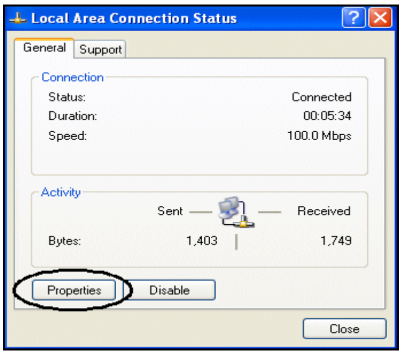
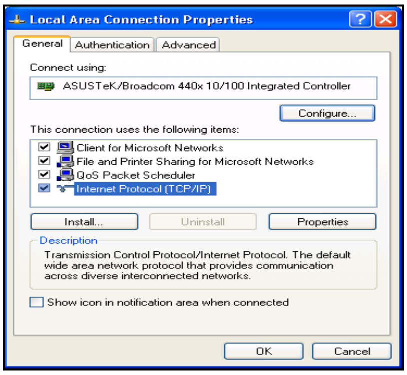
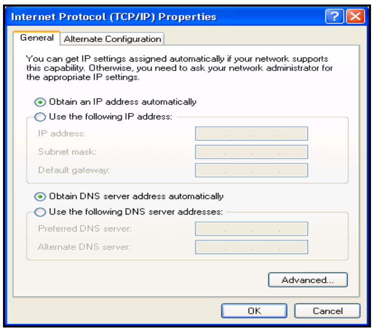


Network Configuration

Configuring PC in Windows Vista

1. Go to **Start**. Click on **Network.**	
2. Then click on **Network and Sharing Center** at the top bar.	 Network Organize Views Network and Sharing Center Add a printer This computer is not connected to a network. Click to connect... Favorite Links Name Category Workgroup Network location Documents Pictures Music Recently Changed Searches Public
3. When the Network and Sharing Center Window pops up, select and click on **Manage Network connections** on the left window column.	
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.	 Network and Internet Network Connections Organize Views Disable this network device Name Status Device Name Connectivity Dial-up (2) Network Extender Disconnected Network Extender SSLVPN A... Standalone Network Extender ISDN WAN Device LAN or High-Speed Internet (1) Local Area Connection Disable Status Diagnose Bridge Connections Create Shortcut Delete Rename Properties
5. Select **Internet Protocol Version 4 (TCP/IP)** then Click **Next.**	 Local Area Connection Properties Networking Connect using: Intel(R) 82566DM Gigabit Network Connection Configure... This connection uses the following items: Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder Install... Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. OK Cancel
6. In the TCP/IPv4 properties window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.	 Internet Protocol Version 4 (TCP/IPv4) Properties General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ● Obtain an IP address automatically ○ Use the following IP address: IP address: Subnet mask: Default gateway: ● Obtain DNS server address automatically ○ Use the following DNS server addresses: Preferred DNS server: Alternate DNS server: Advanced... OK Cancel
7. Click **OK** again in the **Local Area Connection** Properties window to apply the new configuration.	

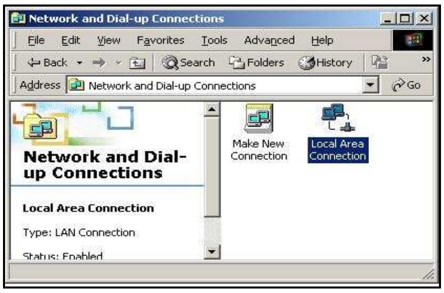
Configuring PC in Windows XP

1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click Network Connections.	
2. Double-click Local Area Connection.	Control Panel File Edit View Favorites Tools Help Back Search Folders Address Control Panel Go Control Panel Switch to Category View See Also Windows Update Help and Support Network Connections Phone and Modem ... Power Options Printers and Faxes Regional and Language ... Scanners and Cameras Scheduled Tasks Sounds and Audio Devices Speech
3. In the LAN Area Connection Status window, click Properties.	Local Area Connection Status General Support Connection Status: Connected Duration: 00:05:34 Speed: 100.0 Mbps Activity Sent — — Received Bytes: 1,403 | 1,749 Properties Disable Close
4. Select Internet Protocol (TCP/IP) and click Properties.	Local Area Connection Properties General Authentication Advanced Connect using: ASUSTeK/Broadcom 440x 10/100 Integrated Controller Configure... This connection uses the following items: ☑ Client for Microsoft Networks ☑ File and Printer Sharing for Microsoft Networks ☑ QoS Packet Scheduler ☑ Internet Protocol (TCP/IP) Install... Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. ☐ Show icon in notification area when connected OK Cancel
5. Select the Obtain an IP address automatically and Obtain DNS server address automatically radio buttons.	Internet Protocol (TCP/IP) Properties General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. ● Obtain an IP address automatically ○ Use the following IP address: IP address: . . . Subnet mask: . . . Default gateway: . . . ● Obtain DNS server address automatically ○ Use the following DNS server addresses: Preferred DNS server: . . . Alternate DNS server: . . . Advanced... OK Cancel
6. Click OK to finish the configuration.	

Configuring PC in Windows 2000

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

2. Double-click Local Area Connection ("LAN")



Network and Dial-up Connections

Address: Network and Dial-up Connections

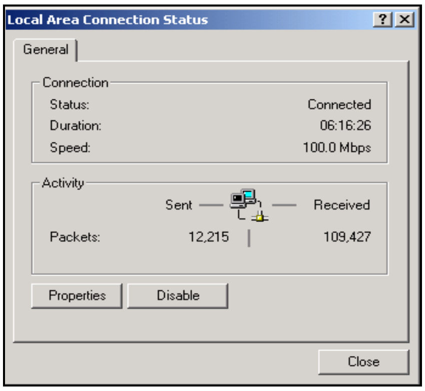
Local Area Connection

Type: LAN Connection

Status: Enabled

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

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



Local Area Connection Status

General

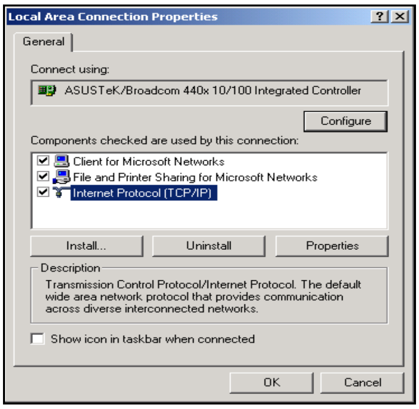
Connection

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

Activity

	Sent	Received
Packets:	12,215	109,427

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



Local Area Connection Properties

General

Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

Components checked are used by this connection:

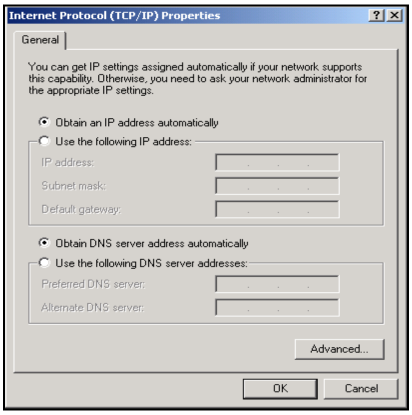
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

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

□ Show icon in taskbar when connected

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



Internet Protocol (TCP/IP) Properties

General

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

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

IP address:

Subnet mask:

Default gateway:

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

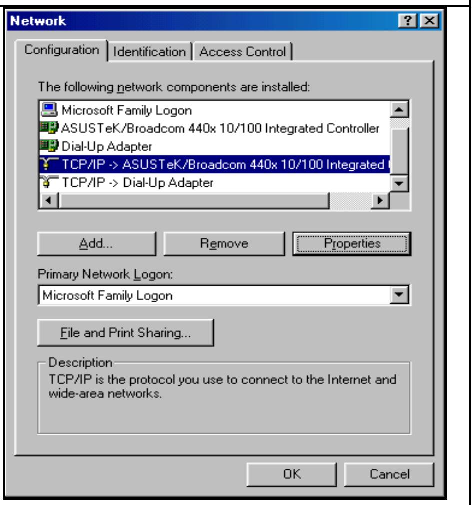
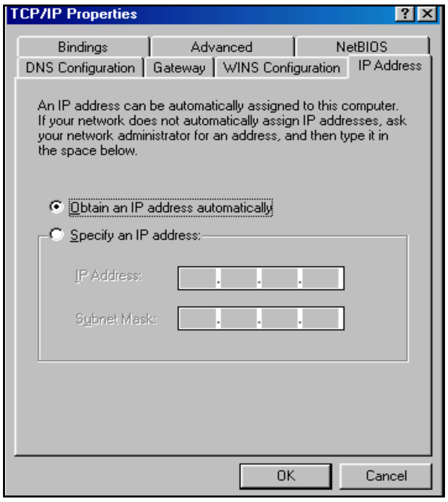
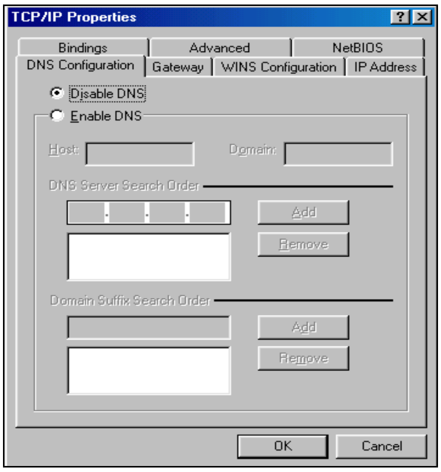
Preferred DNS server:

Alternate DNS server:

6. Click OK to finish the configuration.

.

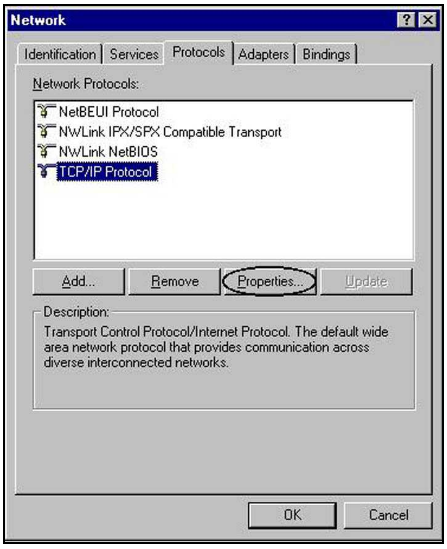
Configuring PC in Windows 95/98/Me

1. Go to Start / Settings / Control Panel. In the Control Panel, double-click Network and choose the Configuration tab.	
2. Select TCP / IP -> NE2000 Compatible, or the name of any Network Interface Card (NIC) in your PC.	 The following network components are installed: Microsoft Family Logon ASUSTeK/Broadcom 440x 10/100 Integrated Controller Dial-Up Adapter TCP/IP -> ASUSTeK/Broadcom 440x 10/100 Integrated TCP/IP -> Dial-Up Adapter Primary Network Logon: Microsoft Family Logon Description TCP/IP is the protocol you use to connect to the Internet and wide-area networks. Network Configuration Identification Access Control Add... Remove Properties File and Print Sharing... OK Cancel
3. Select the IP Address tab. In this page, click the Obtain an IP address automatically radio button.	 An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below. ● Obtain an IP address automatically ○ Specify an IP address: IP Address: . . . Subnet Mask: . . . TCP/IP Properties Bindings Advanced NetBIOS DNS Configuration Gateway WINS Configuration IP Address OK Cancel
4. Then select the DNS Configuration tab.	 ● Disable DNS ○ Enable DNS Host: Domain: DNS Server Search Order Domain Suffix Search Order TCP/IP Properties Bindings Advanced NetBIOS DNS Configuration Gateway WINS Configuration IP Address Add Remove Add Remove OK Cancel
5. Select the Disable DNS radio button and click OK to finish the configuration.	

Configuring PC in Windows NT4.0

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

2. Select TCP/IP Protocol and click Properties.

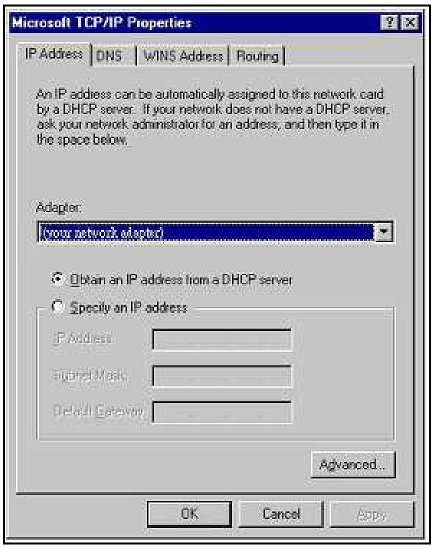


Network Protocols:

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

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

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



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

Adapter: (your network adapter)

● Obtain an IP address from a DHCP server

○ Specify an IP address

Factory Default Settings

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

Web Interface (Username and Password)

- Username: admin
- Password: admin

✓ **If you ever forget the login password, please press and hold the reset button for longer than 6 seconds to restore the factory default settings.**

Attention

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

Device LAN IP settings

- IP Address: 10.0.0.2
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

- DHCP server is enabled.
- Start IP Address: 10.0.0.100
- IP pool counts: 100

LAN and WAN Port Addresses

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

LAN Port		WAN Port
IP address	http://10.0.0.2	The PPPoE function is *enabled* to automatically get the WAN port configuration from the ISP, but you have to set the username and password first.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 10.0.0.100 through 10.0.0.199	

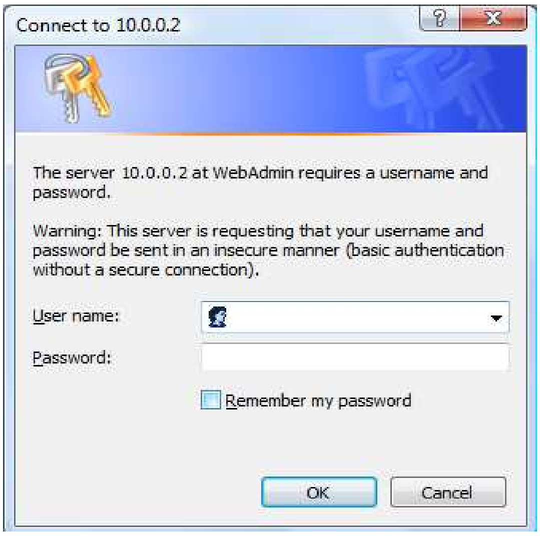
Information from your ISP

Telkom ADSL connections use PPPoE, and automatically assign a WAN IP address to your router. The following information is provided should you wish to connect to an alternative ISP.
Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (this is automatically set by the Telkom network but be set manually should this be required).
PPPoE (Multisession)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, Domain Name System (DNS) IP address and multiple-sessions on the same PVC.
PPPoE / PPPoE with Pass-through	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (this is automatically set by the Telkom network but be set manually should this be required). In addition, additional WAN address can be assigned using PPPoE dialler.
PPPoA	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC 1483 Bridged	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.
RFC 1483 Routed	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA Routed	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is 10.0.0.2, and click “Go”, a user name and password window prompt will appear. The default username and password are “admin” and “admin” respectively. (See Figure below)



Connect to 10.0.0.2

The server 10.0.0.2 at WebAdmin requires a username and password.

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

User name:

Password:

□ Remember my password

Figure: User name & Password Prompt Window

Congratulations! You are now successfully logged onto your Router!

CHAPTER4: CONFIGURATION

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

Status

ADSL Table

3G Status

ARP Table

DHCP Table

Routing Table

NAT Sessions

UpnP Portmap

PPTP Status

IPSec Status

L2TP Status

Email Status

VoIP Status

VoIP Call Log

Event Log

Error Log

Diagnostic

Quick Start

Configuration

LAN

WAN

System

Firewall

VPN

VoIP

QoS

Virtual Server

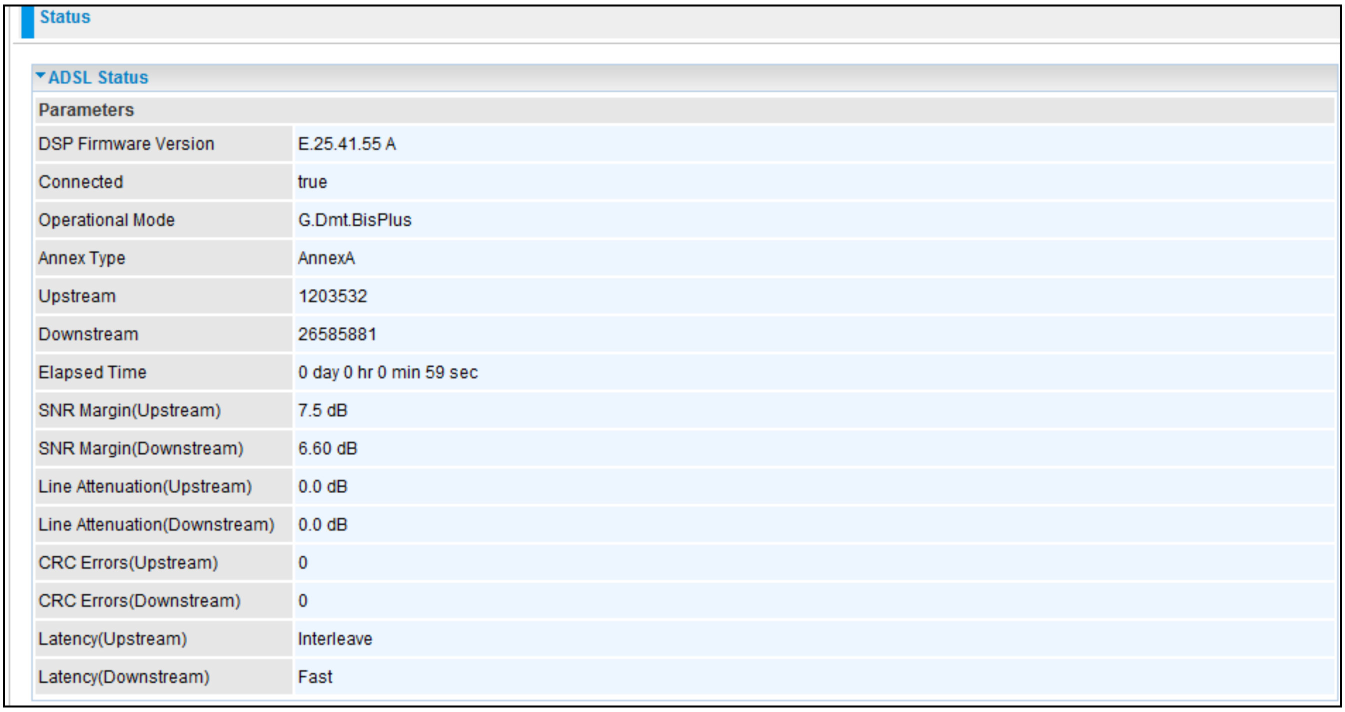
Time Schedule

Advanced

Status

ADSL Status

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



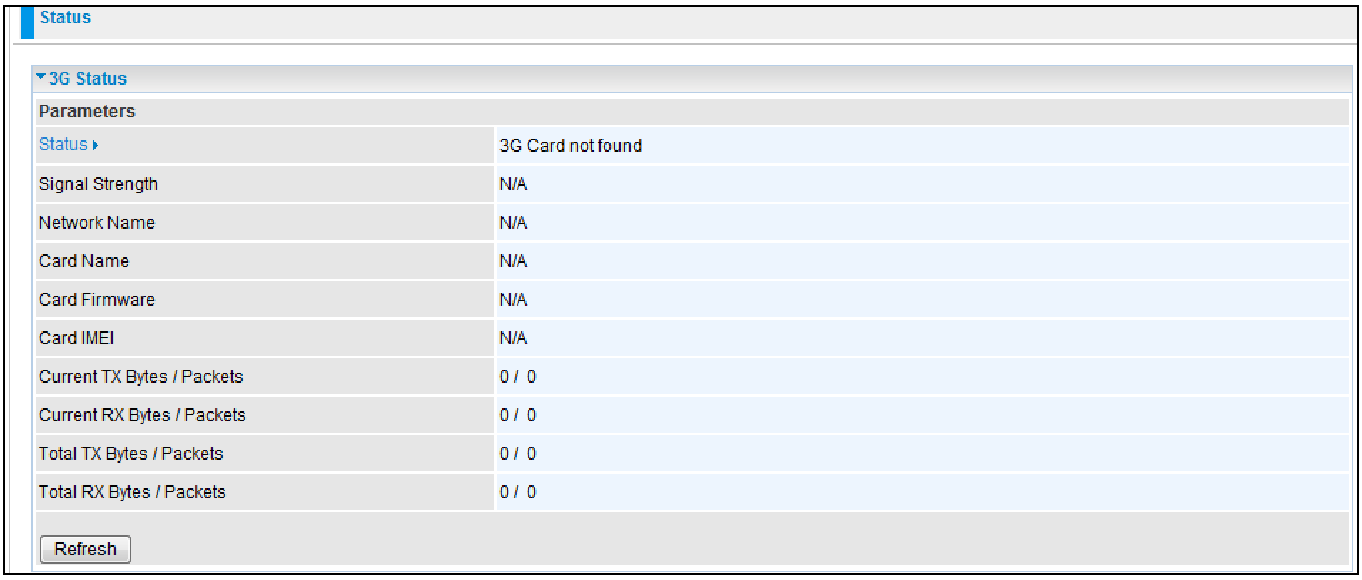
Status

ADSL Status

Parameters	
DSP Firmware Version	E.25.41.55 A
Connected	true
Operational Mode	G.Dmt.BisPlus
Annex Type	AnnexA
Upstream	1203532
Downstream	26585881
Elapsed Time	0 day 0 hr 0 min 59 sec
SNR Margin(Upstream)	7.5 dB
SNR Margin(Downstream)	6.60 dB
Line Attenuation(Upstream)	0.0 dB
Line Attenuation(Downstream)	0.0 dB
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	Interleave
Latency(Downstream)	Fast

3G Status

This section displays the 3G Card overall status with information such as the current signal strength, statistics of current data transmission and total data transmission.



Status

3G Status

Parameters	
Status ▸	3G Card not found
Signal Strength	N/A
Network Name	N/A
Card Name	N/A
Card Firmware	N/A
Card IMEI	N/A
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0

Status: The current status of the 3G card.

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

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

Card Name: The name of the 3G card.

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

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

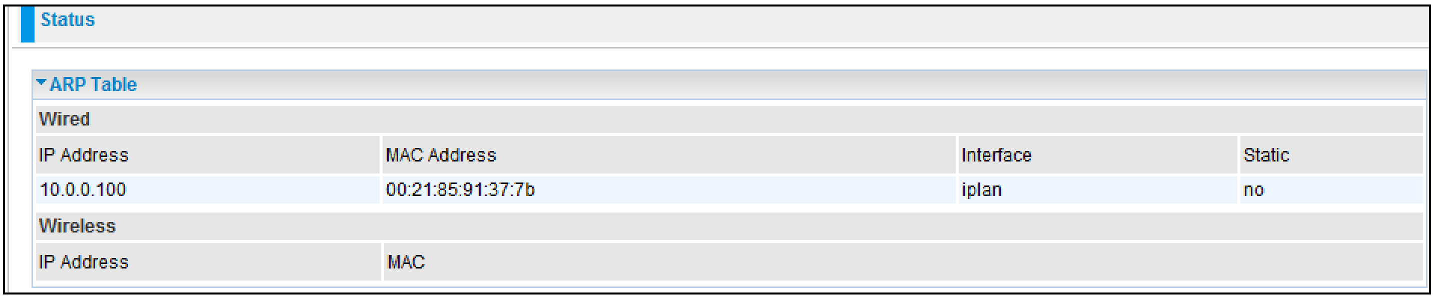
Current RX Bytes / Packets: The statistics of data received in bytes / packets during a call.

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

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

ARP Table

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



Wired			
IP Address	MAC Address	Interface	Static
10.0.0.100	00:21:85:91:37:7b	iplan	no
Wireless			
IP Address	MAC		

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

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

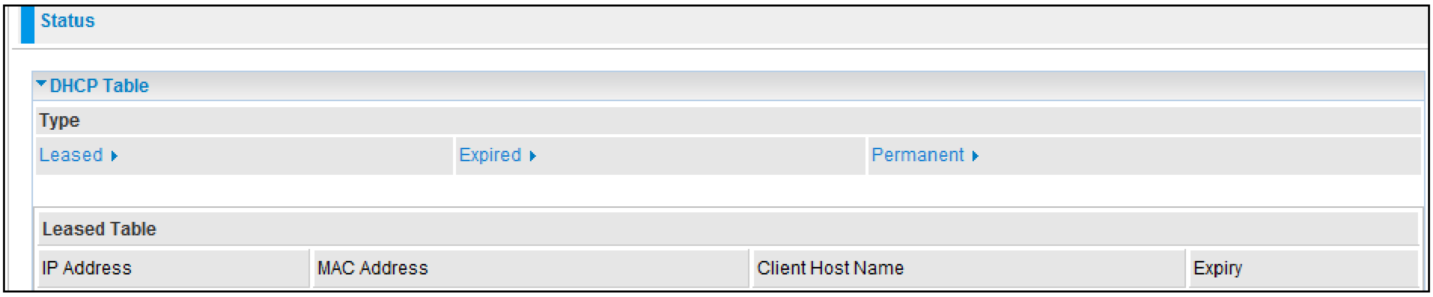
Interface: Shows the interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

“**no**” for dynamically-generated ARP table entries.

“**yes**” for static ARP table entries added by the user.

DHCP Table



Status

▾DHCP Table

Type		
Leased ▸	Expired ▸	Permanent ▸

Leased Table

IP Address	MAC Address	Client Host Name	Expiry

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

Expired: Shows the information of all expired IP addresses.

Permanent: Shows the fixed host mapping information.

<u>Leased Table</u>

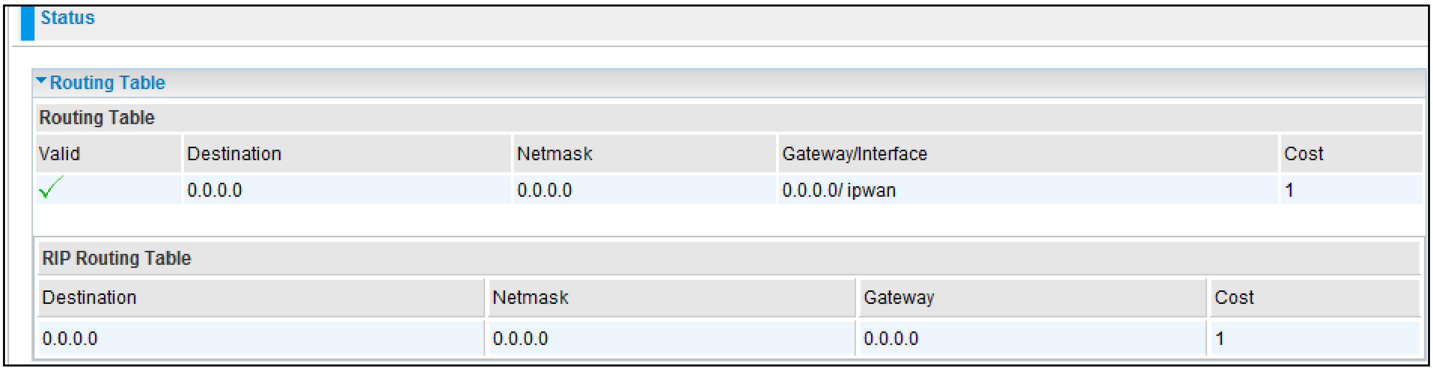
IP Address: Shows the IP address that is assigned to each client.

MAC Address: Shows the MAC address of each client.

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

Expiry: Shows the current lease time of each client.

Routing Table



Status

▾Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost
✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	1

RIP Routing Table

Destination	Netmask	Gateway	Cost
0.0.0.0	0.0.0.0	0.0.0.0	1

<u>Routing Table</u>

Valid: A check mark indicates a successful routing status.

Destination: Shows the IP address of the destination network.

Netmask: Shows the destination Netmask address.

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

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

RIP Routing Table

Destination: Shows the IP address of the destination network.

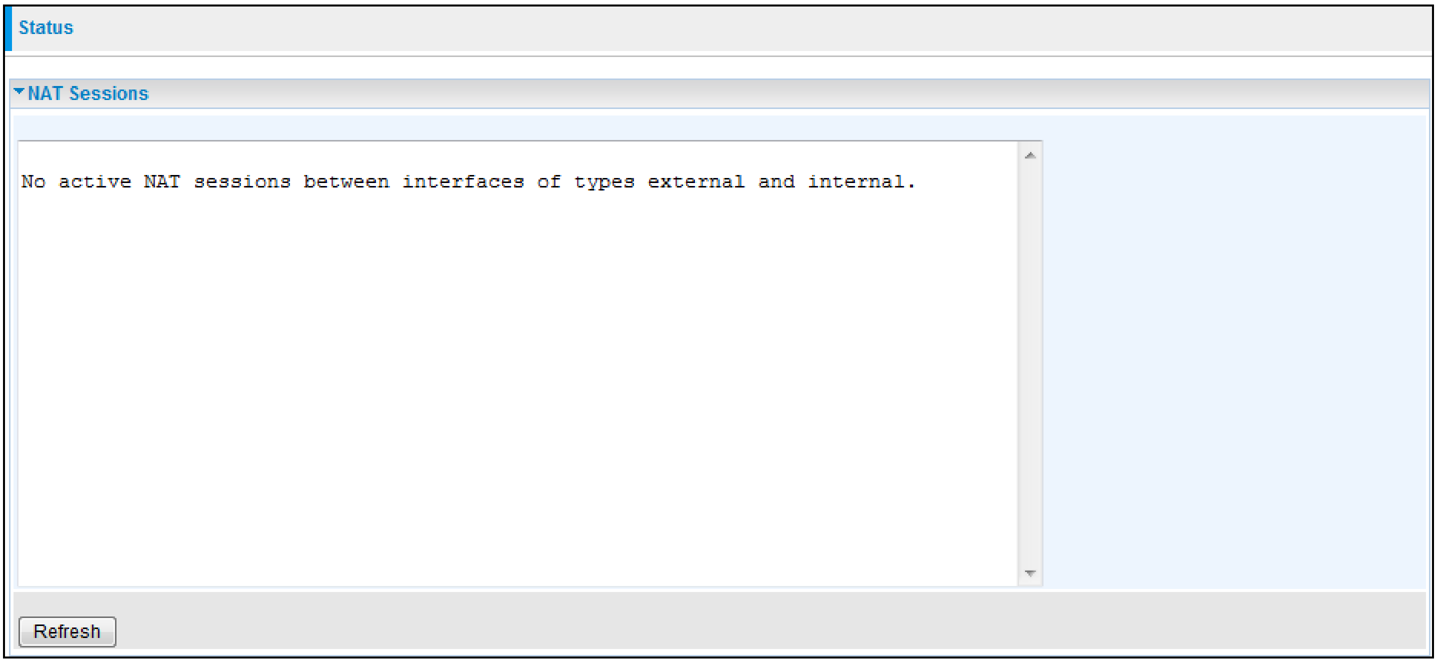
Netmask: Shows the destination Netmask address.

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

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

NAT Sessions

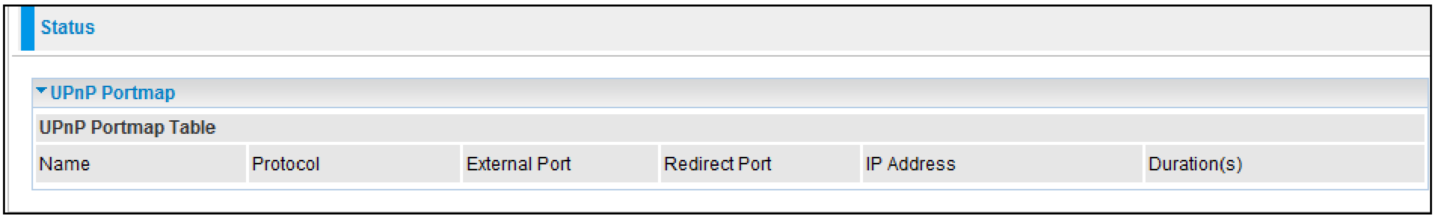
This section lists all the current NAT sessions between external (WAN) and internal (LAN) interface.



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

UPnP Portmap

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

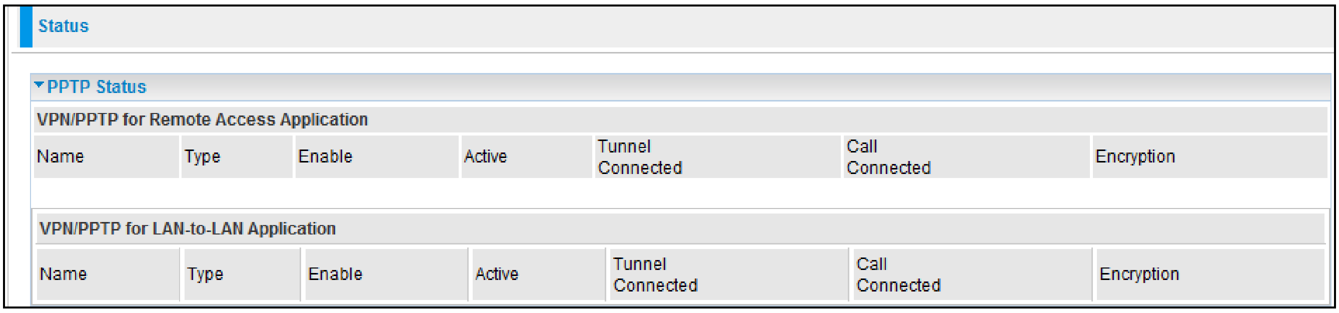


UPnP Portmap Table

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

PPTP Status

This shows details of your configured PPTP VPN Connections.



Status

PPTP Status

VPN/PPTP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/PPTP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: Shows the name you assign to a particular PPTP connection in your VPN configuration.

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

Enable: Shows whether the connection is currently enabled.

Active: Shows whether the connection is currently active.

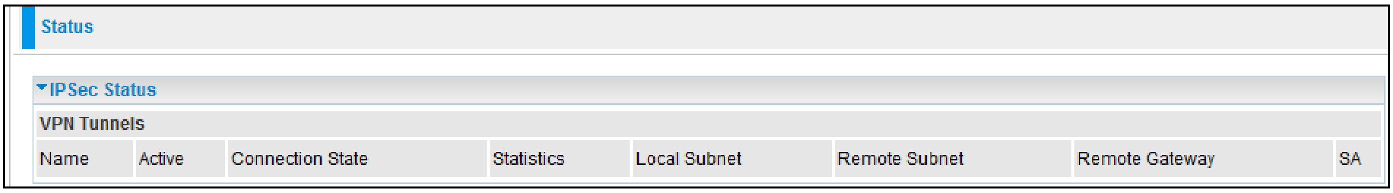
Tunnel Connected: Shows whether the VPN Tunnel is currently connected.

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

Encryption: Shows the encryption type used for this VPN connection.

IPSec Status

This shows the details of your configured IPSec VPN Connections.



Status

IPSec Status

VPN Tunnels

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

Name: Shows the name you assign to a particular VPN entry.

Active: Shows whether the VPN Connection is currently Active.

Connection State: Shows the connection status of VPN.

Statistics: Shows the statistics of your VPN Connection.

Local Subnet: Shows the local IP Address or Subnet that is being used.

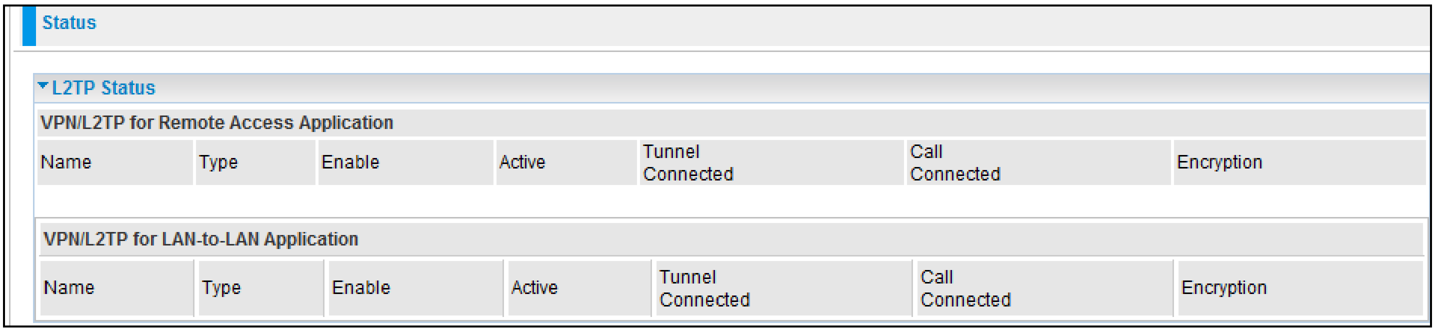
Remote Subnet: Shows the Subnet of the remote site.

Remote Gateway: Shows the Remote Gateway IP address.

SA: Shows the Security Association of this VPN entry.

L2TP Status

This shows the details of your configured L2TP VPN Connections.



VPN/L2TP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/L2TP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

Name: Shows the name you assign to a particular L2TP connection in your VPN configuration.

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

Enable: Shows whether the connection is currently enabled.

Active: Shows whether the connection is currently active.

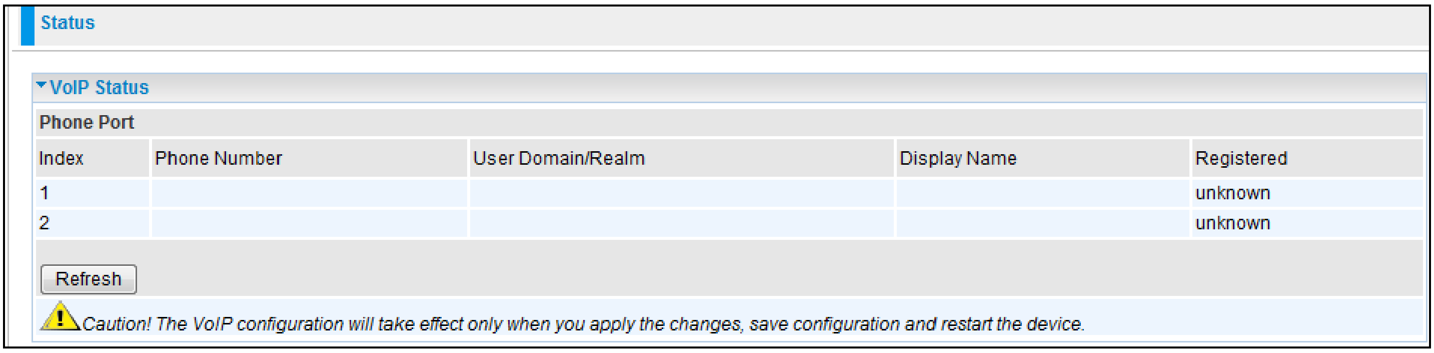
Tunnel Connected: Shows the current connection status of the VPN Tunnel.

Call Connected: Shows the current connection status of a particular VPN entry call.

Encryption: Shows the encryption type used for this VPN connection.

VoIP Status

This table shows the status of the phone ports when VoIP feature has been activated. It displays information such as domain name, display name & phone number of the VoIP device.



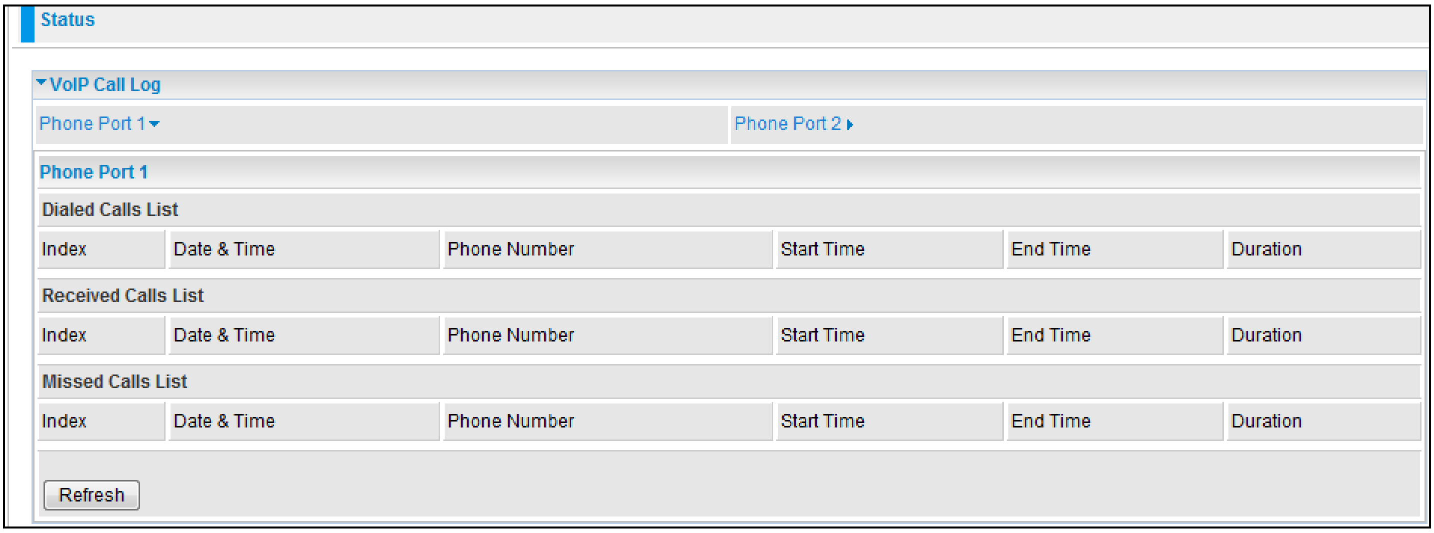
Phone Port

Index	Phone Number	User Domain/Realm	Display Name	Registered
1				unknown
2				unknown

⚠*Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.*

VoIP Call Log

The call log records the data from your VoIP devices such as the date / time of dial out calls, the duration of the calls, information about the missed calls and also incoming calls.



Phone Port 1

Dialed Calls List

Index	Date & Time	Phone Number	Start Time	End Time	Duration

Received Calls List

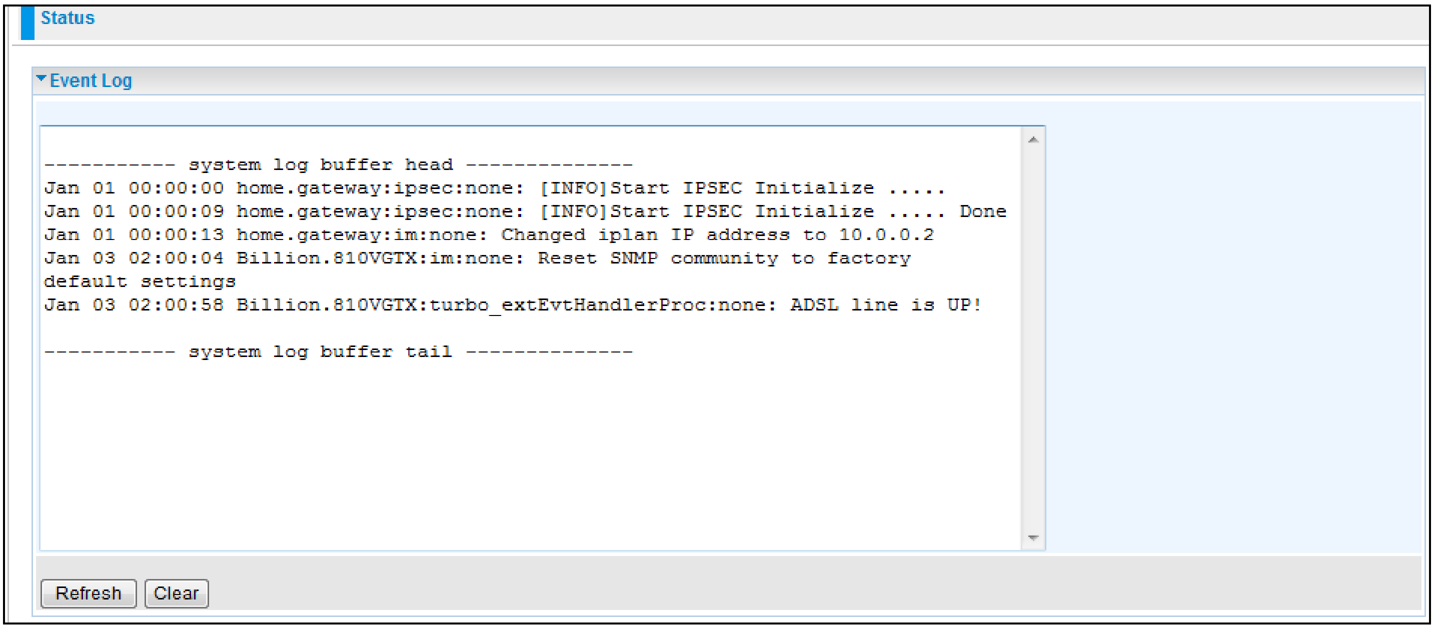
Index	Date & Time	Phone Number	Start Time	End Time	Duration

Missed Calls List

Index	Date & Time	Phone Number	Start Time	End Time	Duration

Event Log

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

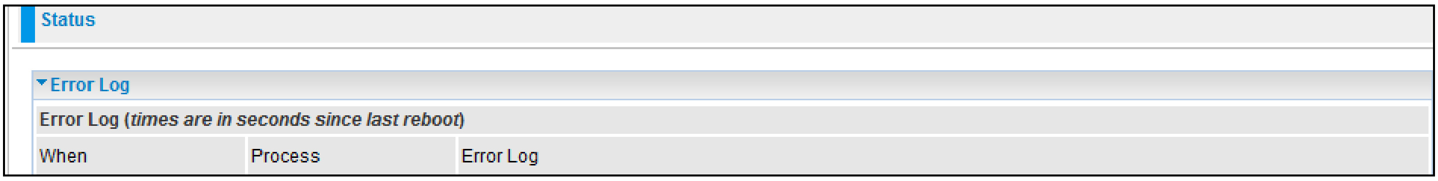


```
----------- system log buffer head --------------
Jan 01 00:00:00 home.gateway:ipsec:none: [INFO]Start IPSEC Initialize .....
Jan 01 00:00:09 home.gateway:ipsec:none: [INFO]Start IPSEC Initialize ..... Done
Jan 01 00:00:13 home.gateway:im:none: Changed iplan IP address to 10.0.0.2
Jan 03 02:00:04 Billion.810VGTX:im:none: Reset SNMP community to factory
default settings
Jan 03 02:00:58 Billion.810VGTX:turbo_extEvtHandlerProc:none: ADSL line is UP!

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

Error Log

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



Status

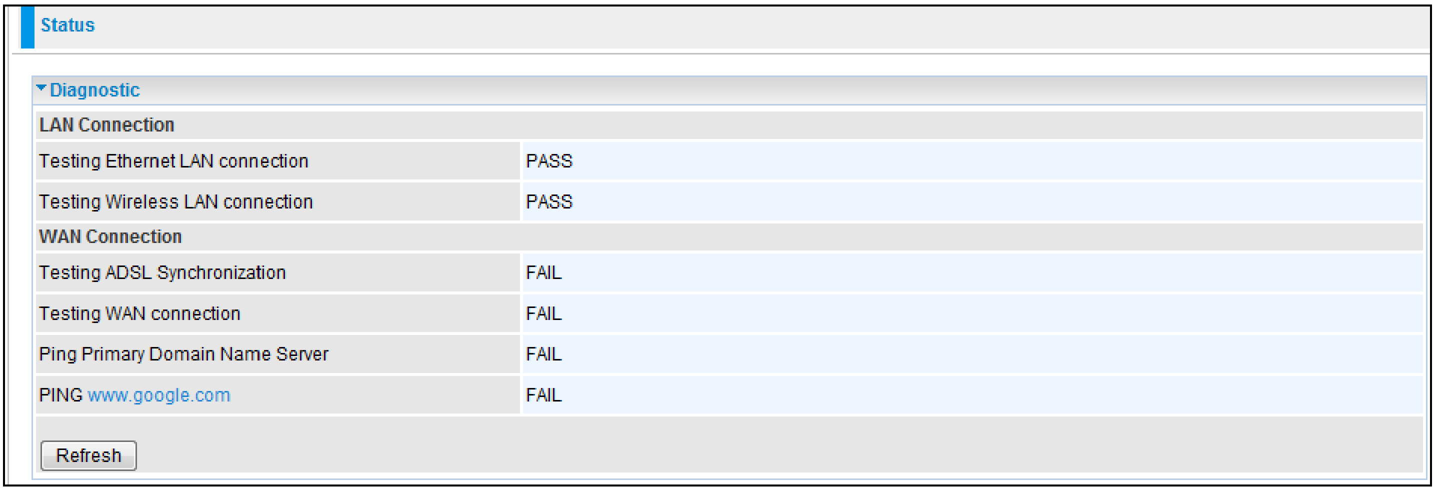
▾Error Log

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

When	Process	Error Log

Diagnostic

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



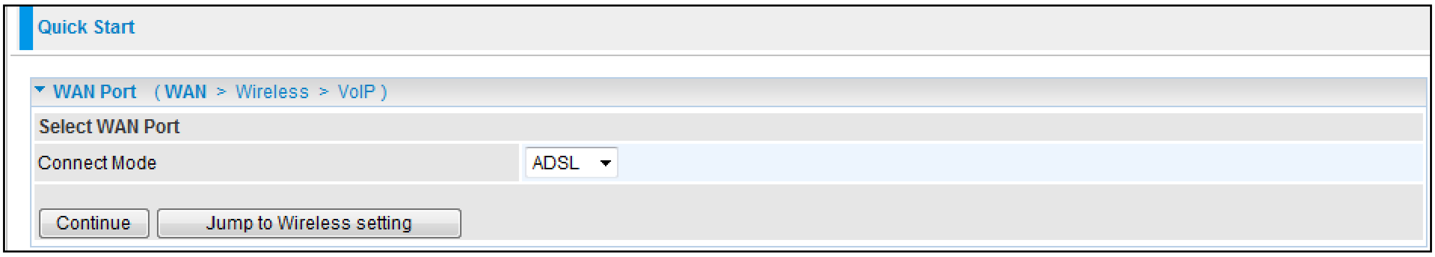
Status

▾Diagnostic

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

Quick Start

1. Click Quick Start. Select the connect mode you want. There are 3 options to choose from: ADSL, EWAN or 3G. Select ADSL mode from the drop down menu and click Continue.



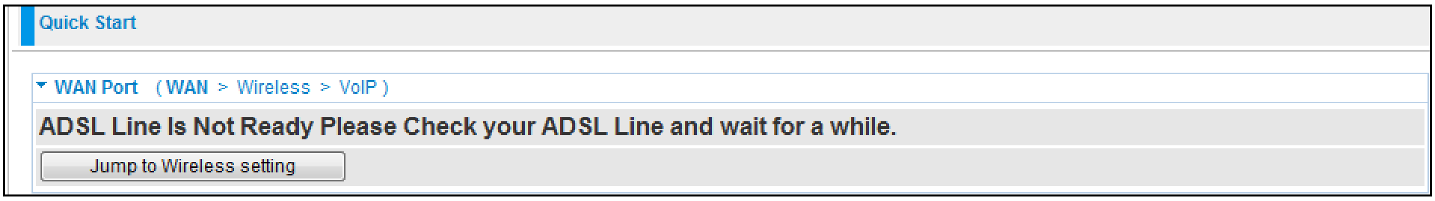
Quick Start

WAN Port (WAN > Wireless > VoIP)

Select WAN Port

Connect Mode: ADSL

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

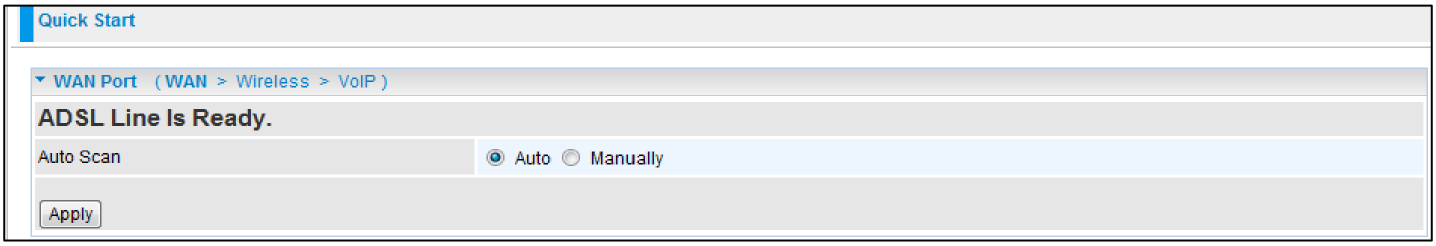


Quick Start

WAN Port (WAN > Wireless > VoIP)

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

3. If your ADSL line is ready, the ADSL Line is Ready screen will appear. Choose the Auto radio button and click Apply. It will automatically scan the recommended mode for you. If you choose to configure it manually then you must up the ADSL line settings manually.

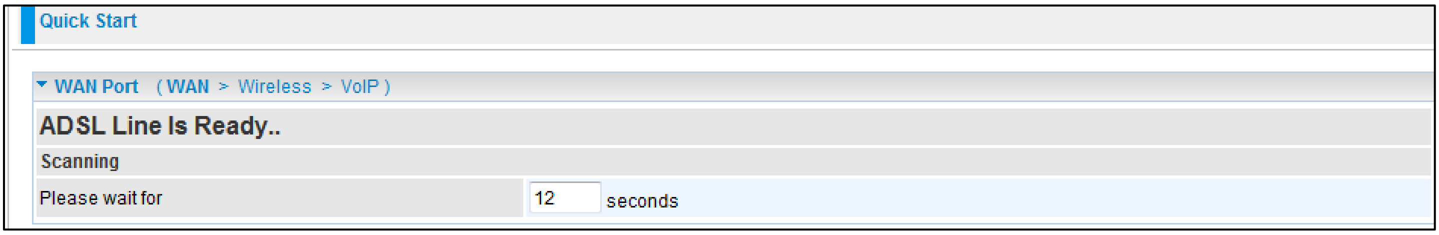


Quick Start

WAN Port (WAN > Wireless > VoIP)

ADSL Line Is Ready.

Auto Scan: ● Auto ○ Manually



Quick Start

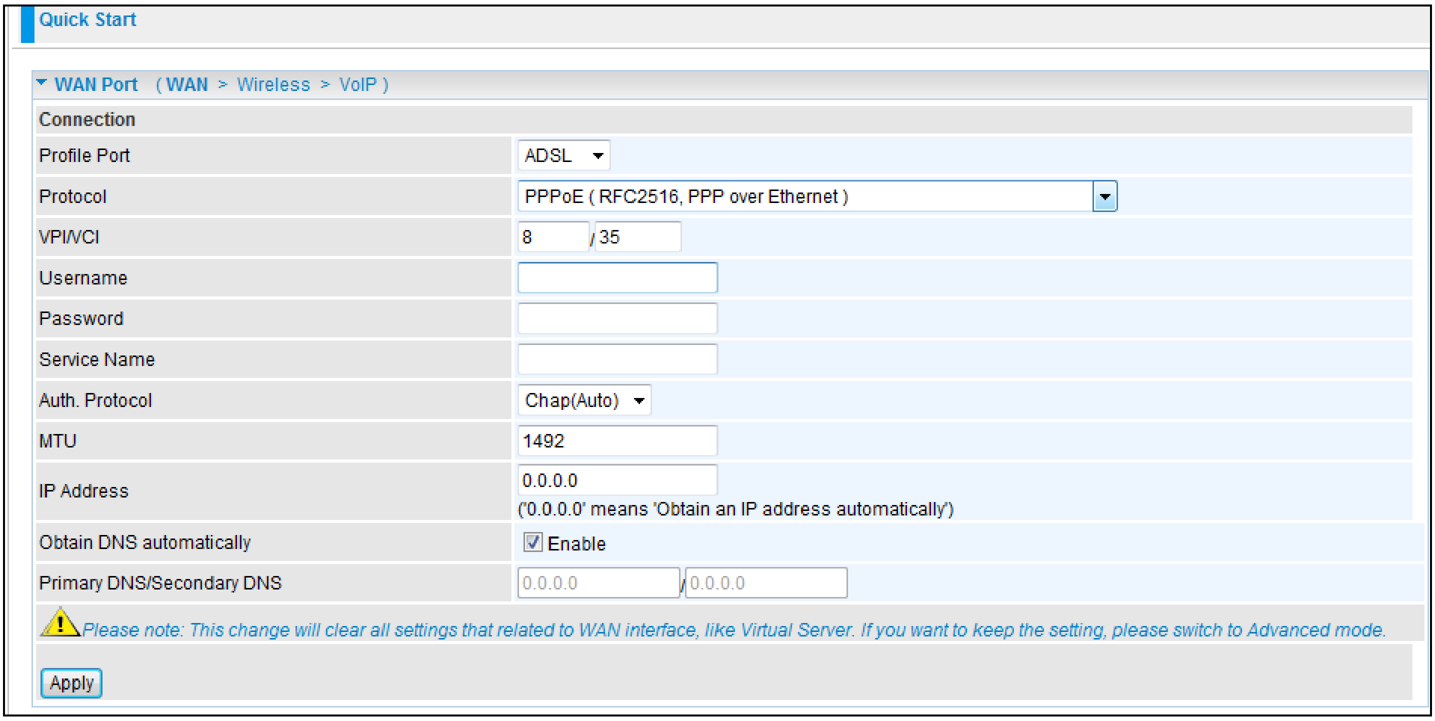
WAN Port (WAN > Wireless > VoIP)

ADSL Line Is Ready..

Scanning

Please wait for 12 seconds

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



Quick Start

▾ WAN Port (WAN > Wireless > VoIP)

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

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

Profile Port: Select the connection mode.

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

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

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

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

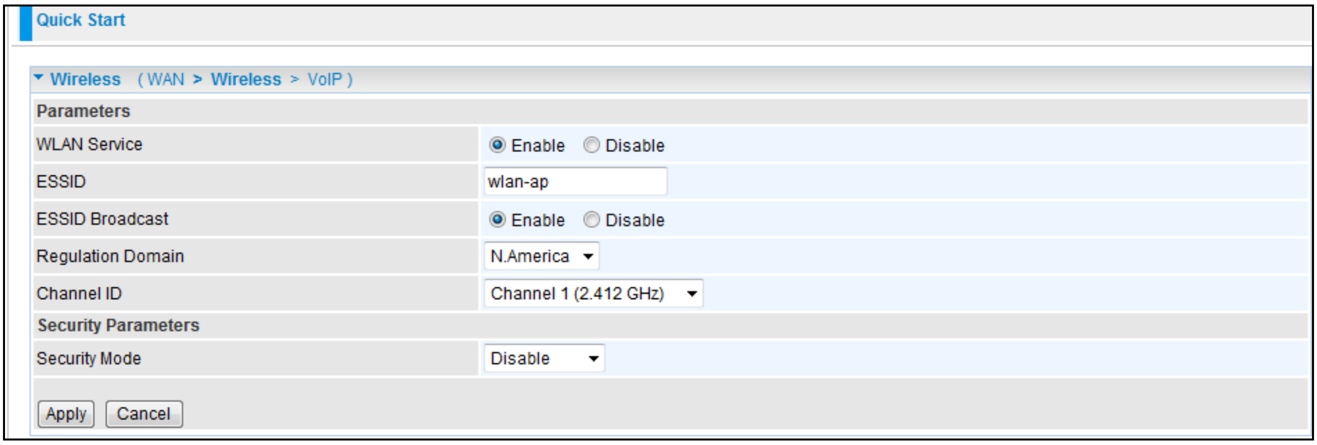
Authentication Protocol: Default is **Auto.** Your ISP advises on using **Chap** or **Pap.**

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

Obtain DNS automatically: Click to activate DNS and to enable the system to automatically detect DNS.

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

5. Configure the Wireless LAN setting.



Quick Start

Wireless (WAN > Wireless > VoIP)

Parameters	
WLAN Service	● Enable ○ Disable
ESSID	wlan-ap
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Security Parameters	
Security Mode	Disable

WLAN Service: Default setting is set to Enable. If you want to use wireless, both 802.11g and

802.11b, you can select Enable.

ESSID: The ESSID is the unique name of a wireless access point (AP). For security proposes, change the SSID to an ID other than the default ID set on the Access Point (AP). It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have the correct ESSID, in order to connect to your network.

ESSID Broadcast: It is function in which the ESSID will not be broadcast. A wireless client will not be able to view your wireless network unless they enter your ESSID manually. Default setting is **Enable.**

Enable: When **Enable** is selected, anybody with a wireless network adapter will be able to view your wireless network.

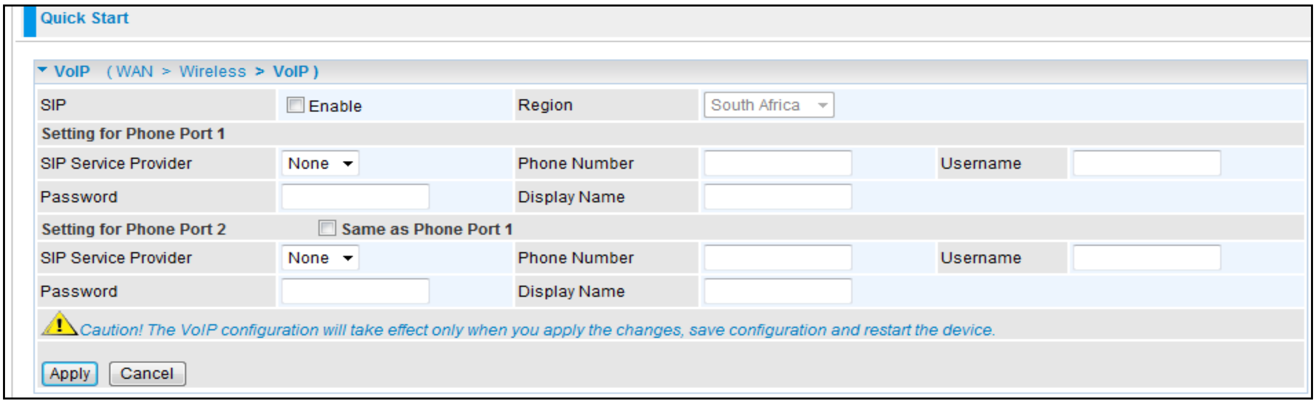
Disable: Select **Disable** if you do not want to broadcast your ESSID. When **Disable** is selected, no one will be able to view your wireless network.

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

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

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

6. Set up VoIP.



Quick Start

▾ VoIP (WAN > Wireless > VoIP)

SIP	□ Enable	Region	South Africa ▾		
Setting for Phone Port 1					
SIP Service Provider	None ▾	Phone Number		Username	
Password		Display Name			
Setting for Phone Port 2	□ Same as Phone Port 1				
SIP Service Provider	None ▾	Phone Number		Username	
Password		Display Name			

⚠ Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.

SIP: To use VoIP SIP as VoIP call signaling protocol. Default is set to ***Disable.***

Region: This selection is a drop-down box, which allows user to select the country for which the VoIP device must work. When a country is selected, the country parameters are automatically loaded.

SIP Service Provider: This section allows you to select the service provider. When the selection is done, respective parameters below are automatically displayed.

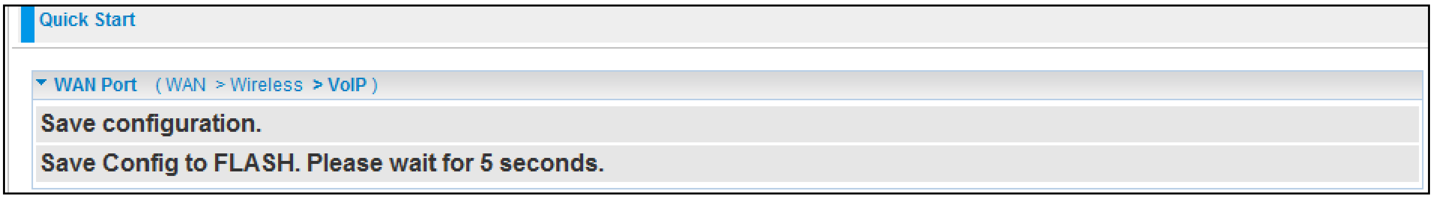
Phone Number: This parameter holds the registration ID of the user within the VoIP SIP registrar.

Username: If the username is the same as the Phone Number, leave it blank. Otherwise, fill in the space with your username given by your VoIP provider.

Password: This parameter holds the password used for authentication within VoIP SIP registrar.

Display Name: This parameter will be displayed on Caller ID.

7. Wait for the configuration to save.

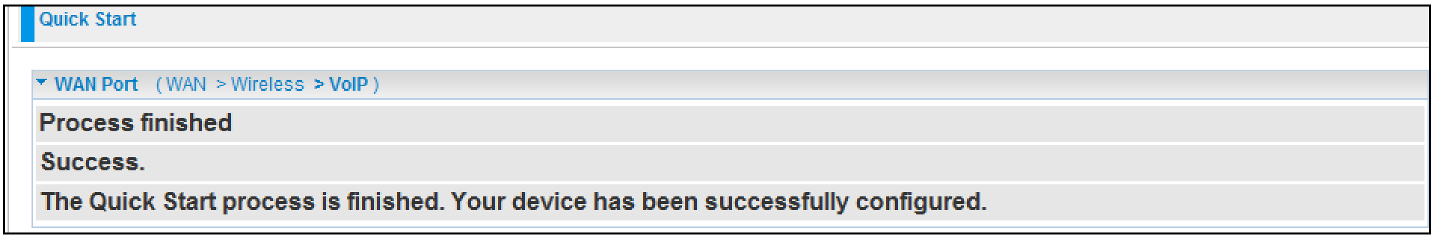


Quick Start

▾ WAN Port (WAN > Wireless > VoIP)

Save configuration.

Save Config to FLASH. Please wait for 5 seconds.



Quick Start

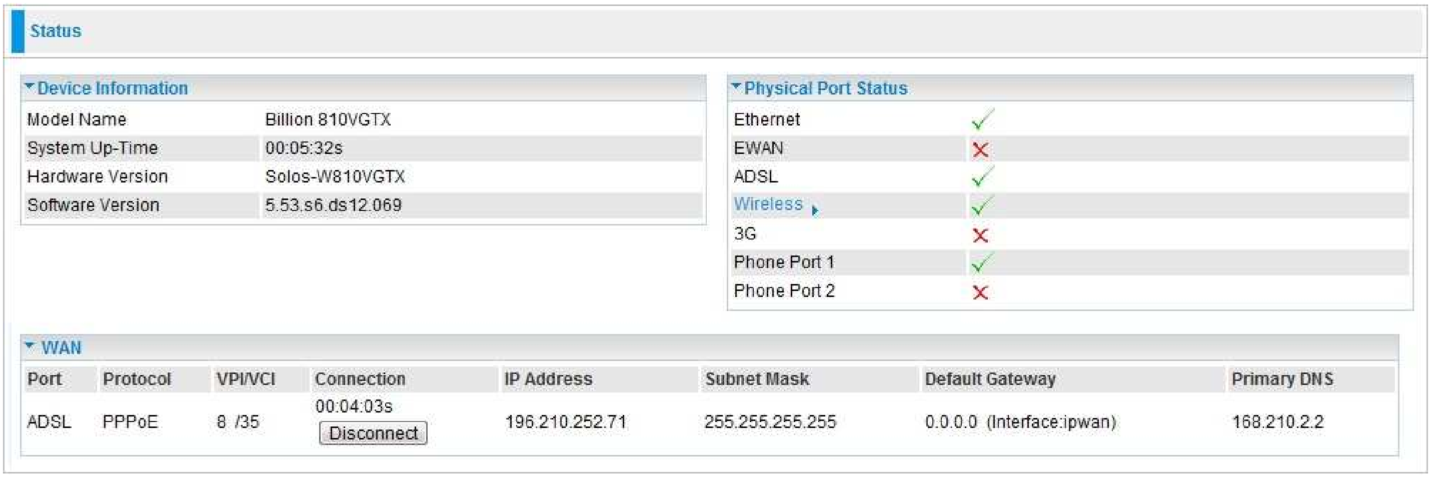
▾ WAN Port (WAN > Wireless > VoIP)

Process finished

Success.

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

8. When the ADSL line has synchronized, a “check” mark will appear next to the ADSL Port.



Status

Device Information

Model Name	Billion 810VGTX
System Up-Time	00:05:32s
Hardware Version	Solos-W810VGTX
Software Version	5.53.s6.ds12.069

Physical Port Status

Ethernet	✓
EWAN	✗
ADSL	✓
Wireless	✓
3G	✗
Phone Port 1	✓
Phone Port 2	✗

WAN

Port	Protocol	VPI/VCI	Connection	IP Address	Subnet Mask	Default Gateway	Primary DNS
ADSL	PPPoE	8 /35	00:04:03s Disconnect	196.210.252.71	255.255.255.255	0.0.0.0 (Interface:ipwan)	168.210.2.2

Configuration

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

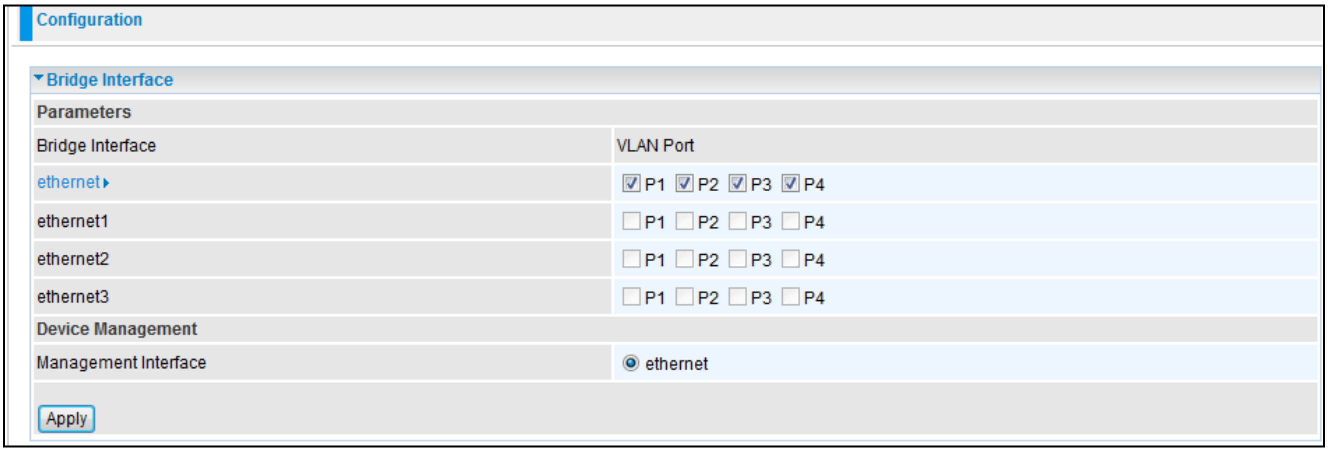
LAN, WAN, System, Firewall, VoIP, QoS, Virtual Server, Time Schedule and Advanced

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

LAN - Local Area Network

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

Bridge Interface



Configuration

▾Bridge Interface

Parameters	
Bridge Interface	VLAN Port
ethernet▸	☑P1 ☑P2 ☑P3 ☑P4
ethernet1	□P1 □P2 □P3 □P4
ethernet2	□P1 □P2 □P3 □P4
ethernet3	□P1 □P2 □P3 □P4
Device Management	
Management Interface	● ethernet

You can setup member ports for each VLAN group under Bridge Interface section.

Ethernet: P1 & P2 (Port 1, 2)

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

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

Bridge Interface	**VLAN Port (Always starts with)**
Ethernet	P1 / P2 / P3 / P4
Ethernet1	P2 / P3 / P4
Ethernet2	P3 / P4
Ethernet3	P4

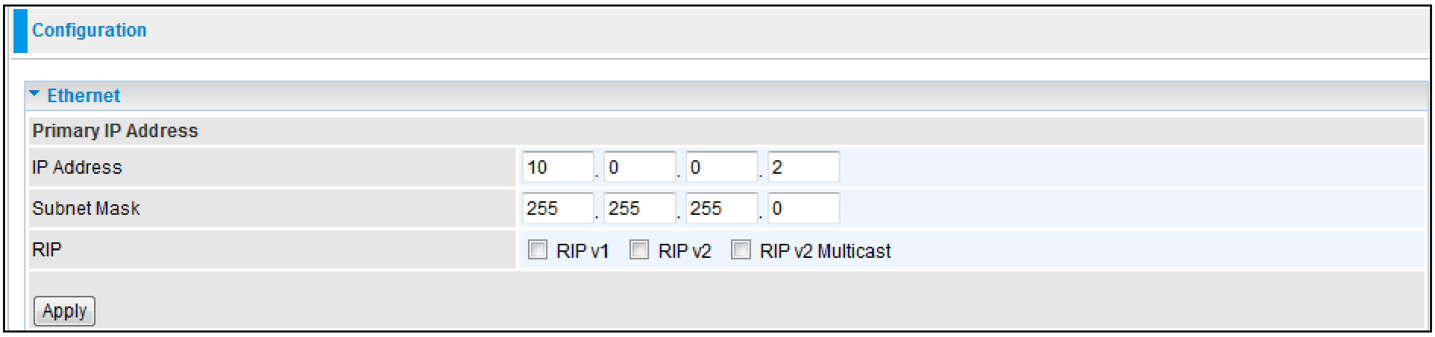
Management Interface: To specify which VLAN group is able to perform device management, for e.g.: web management.

NOTE:

- ✓ **NAT/NAPT can be applied to management interfaces only**

Ethernet

The router supports more than one Ethernet IP address. The LAN allows multiple PC's to access the internet at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 10.0.0.2.



Configuration

Ethernet

Primary IP Address	
IP Address	10 . 0 . 0 . 2
Subnet Mask	255 . 255 . 255 . 0
RIP	□ RIP v1 □ RIP v2 □ RIP v2 Multicast

Primary IP Address:

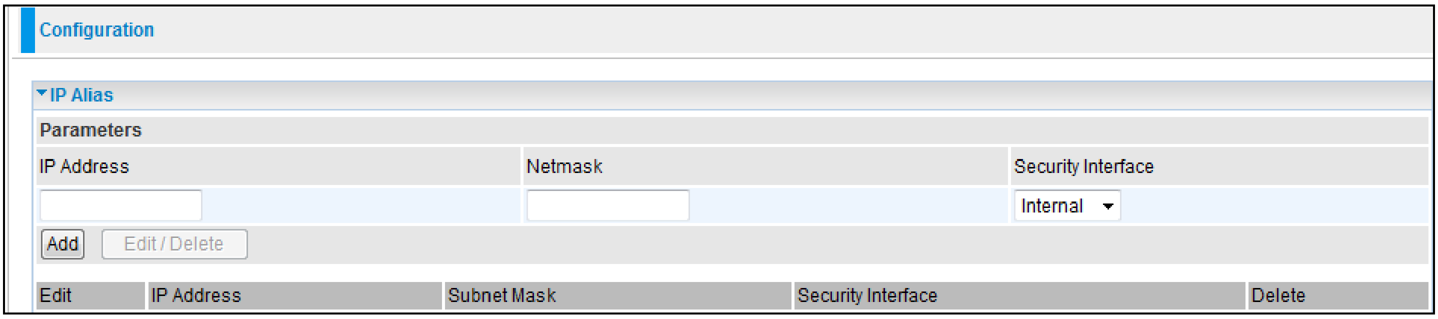
IP Address: The default IP on this router.

Subnet Mask: The default subnet mask on this router.

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

IP Alias

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



Configuration

IP Alias

Parameters

IP Address	Netmask	Security Interface
		Internal

Edit	IP Address	Subnet Mask	Security Interface	Delete

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

Netmask: Specify a subnet mask for this virtual interface.

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

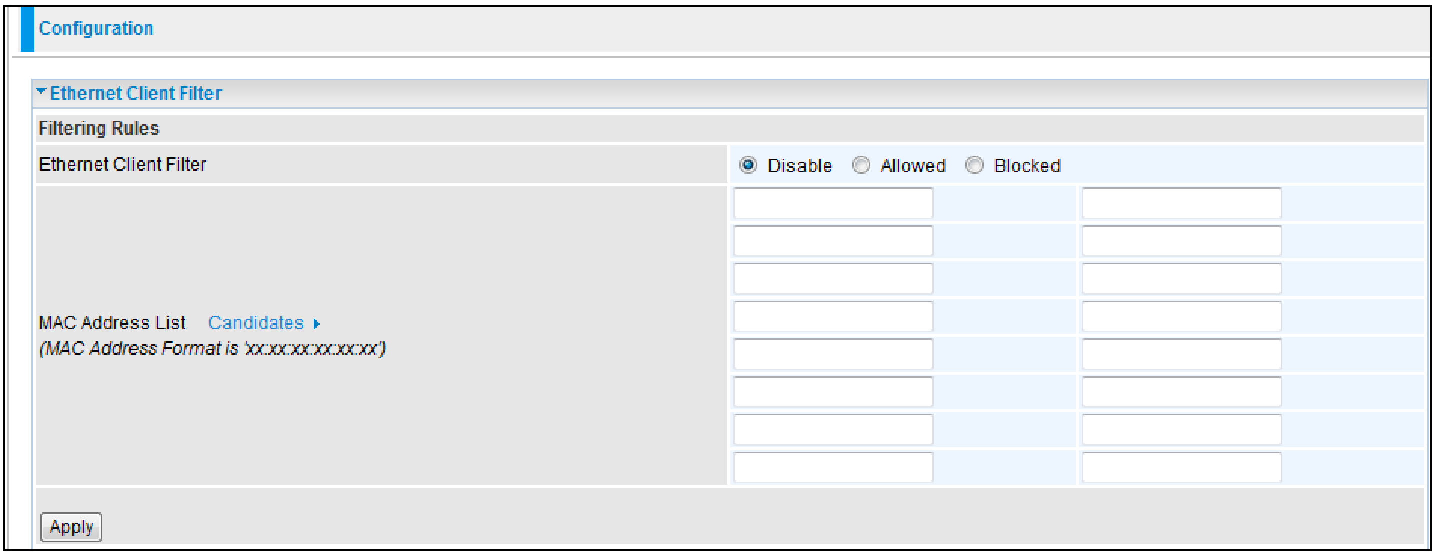
> **Internal**: This means the network is behind NAT. All traffic will do network address translation when sending out data to the Internet if NAT is enabled.
>
> **External:** This means there is no NAT on this IP interface and it is connected directly to the Internet. This function is mostly used when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

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

Ethernet Client Filter

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

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



Configuration

Ethernet Client Filter

Filtering Rules

Ethernet Client Filter: ● Disable ○ Allowed ○ Blocked

MAC Address List Candidates
(MAC Address Format is 'xx:xx:xx:xx:xx:xx')

Ethernet Client Filter: Default setting is set to 'Disable'.

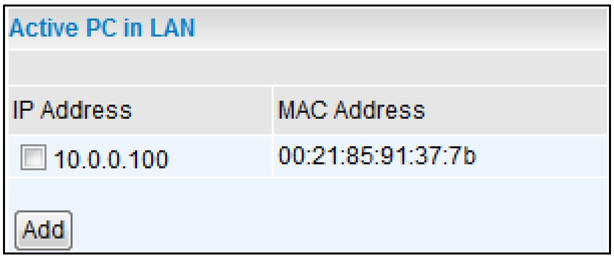
> **Allowed**: Check to enable a specific PC to access your LAN by inserting the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.
>
> **Blocked**: Check to prevent an unwanted PC from accessing your LAN by inserting the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is not listed.

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

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

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

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



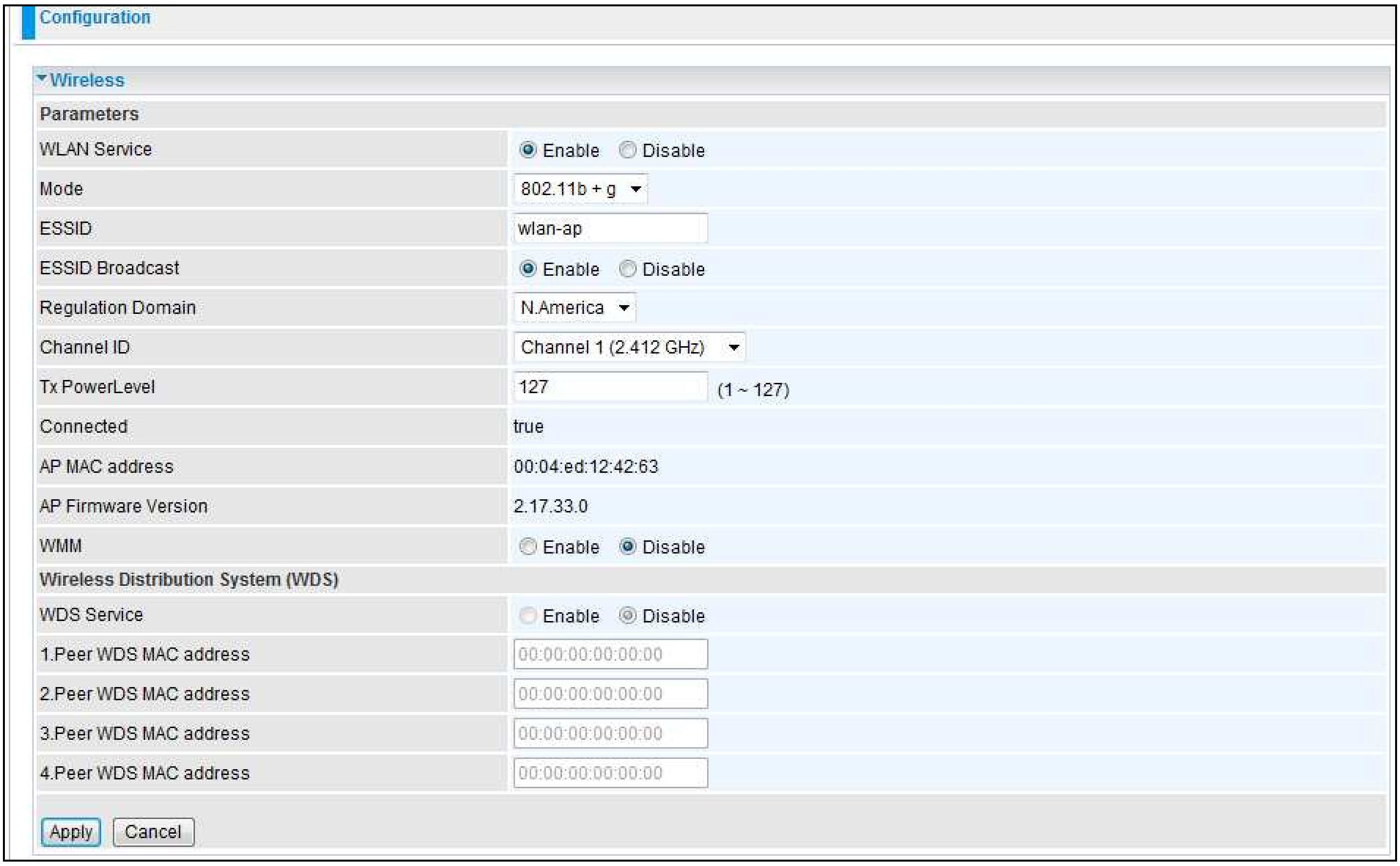
Active PC in LAN

IP Address	MAC Address
□ 10.0.0.100	00:21:85:91:37:7b

Active PC in LAN: Active PC in LAN window displays a list of IP Address & MAC Addresses of Ethernet devices which are currently connected to the router.

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

Wireless



Configuration

Wireless

Parameters	
WLAN Service	● Enable ○ Disable
Mode	802.11b + g
ESSID	wlan-ap
ESSID Broadcast	● Enable ○ Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Tx PowerLevel	127 (1 ~ 127)
Connected	true
AP MAC address	00:04:ed:12:42:63
AP Firmware Version	2.17.33.0
WMM	○ Enable ● Disable
Wireless Distribution System (WDS)	
WDS Service	○ Enable ● Disable
1.Peer WDS MAC address	00:00:00:00:00:00
2.Peer WDS MAC address	00:00:00:00:00:00
3.Peer WDS MAC address	00:00:00:00:00:00
4.Peer WDS MAC address	00:00:00:00:00:00

Parameters

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

Mode: The default setting is 802.11b+g+n (Mixed mode). If you do not know or you have both 11g and 11b devices on your network, then keep the setting in mixed mode. From the drop-down menu, you can select 802.11g if you know that there are only 802.11g cards. You may do the same for 802.11b as well as 802.11n.

ESSID: The ESSID is the unique name given to a wireless access point (AP) used to distinguish one access point from another. For security purposes, please change the default wlan-ap to a unique ID. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have the same ESSID as the device in order to connect to your network.

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

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

Enable: When enabled, you allow anybody with a wireless client to locate the Access Point (AP) of your router.

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

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

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

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

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

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

Connected: Displayed either as true or false. This is the connection status between the system and the built-in wireless card.

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

AP Firmware Version: The Access Point firmware version.

Wireless Distribution System (WDS)

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

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

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

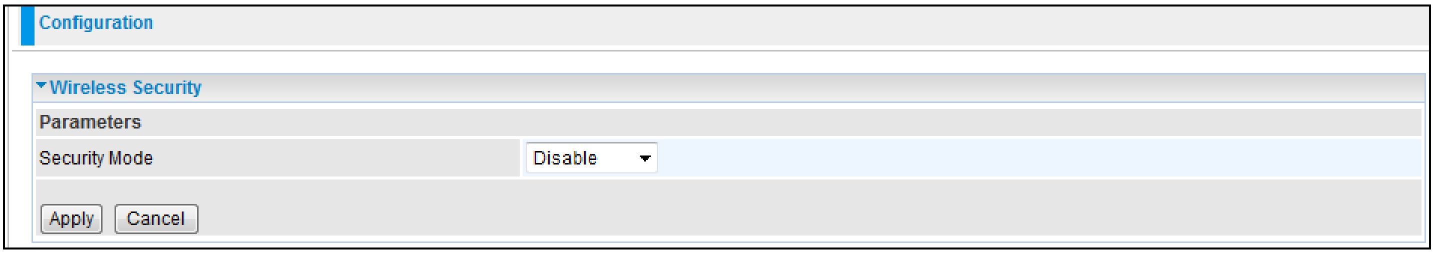
1. Peer WDS MAC Address: It is the associated AP MAC Address. It is important that your peer's AP include your MAC address in order to acknowledge and communicate with each other.
2. Peer WDS MAC Address: It is the second associated AP MAC Address.
3. Peer WDS MAC Address: It is the third associated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

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

Wireless Security

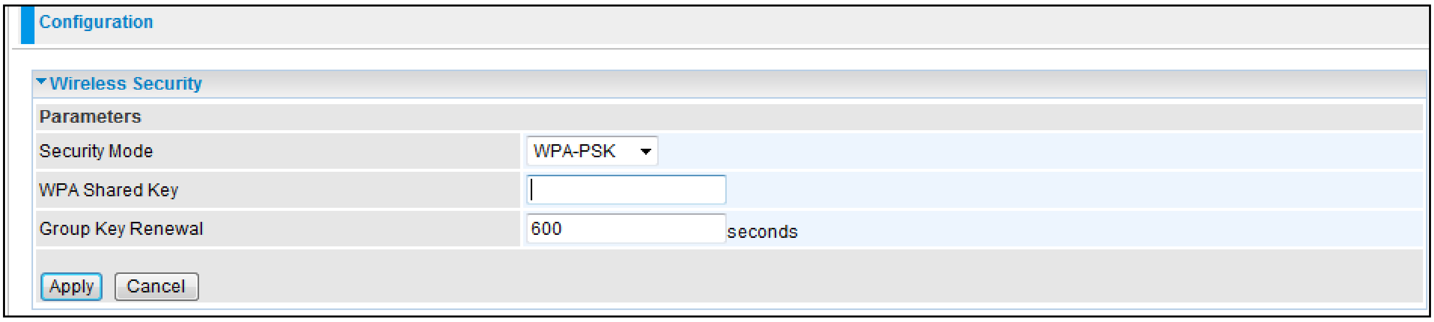
You can disable or enable the wireless security function using WPA or WEP for wireless network protection.

The default mode of wireless security is set to 'Disabled'.



Security Mode: Disable

WPA-PSK / WPA2-PSK



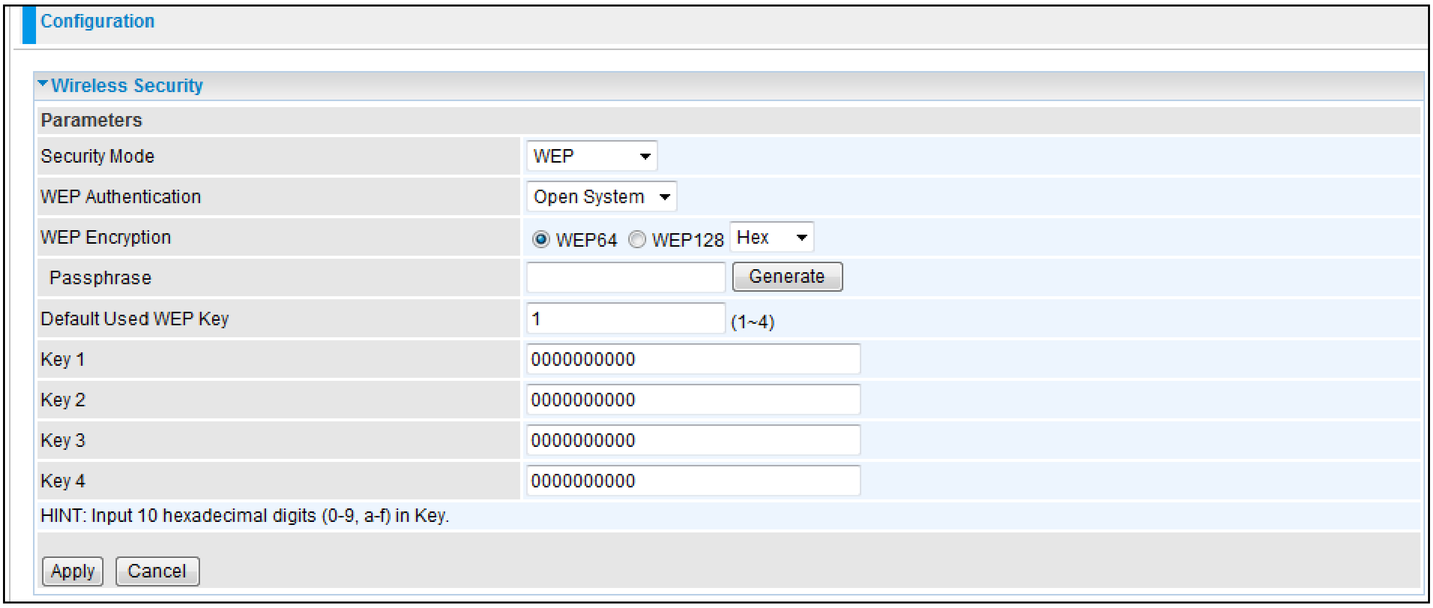
Parameters	
Security Mode	WPA-PSK
WPA Shared Key	
Group Key Renewal	600 seconds

Security Mode: You can disable or enable security mode with WPA or WEP for protecting your wireless network. The default mode of wireless security is set to ‘Disable’.

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

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

WEP



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

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

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

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

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

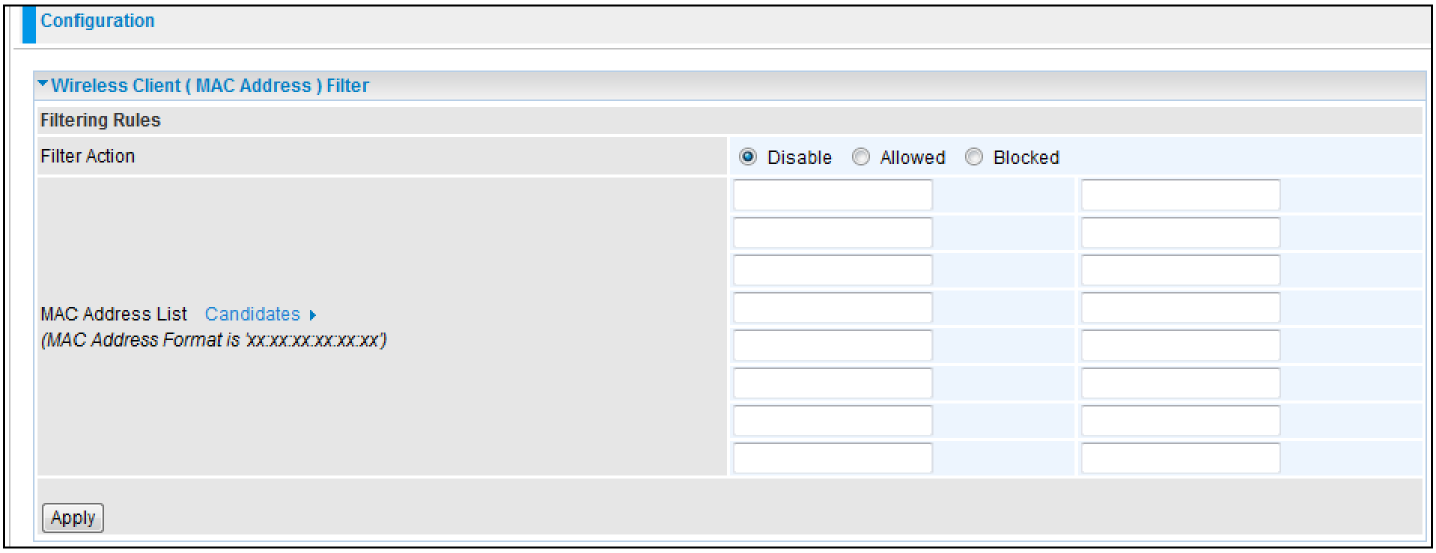
Default Used WEP Key: Select the encryption key ID; please refer to Key (1~4) below.

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

Wireless Client / MAC Address Filter

The MAC Address filter supports up to 16 wireless network clients. It allows you to manage your network to allow traffic from authorized clients or to restrict unwanted clients from accessing your Wireless network.

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



Configuration

Wireless Client (MAC Address) Filter

Filtering Rules

Filter Action ● Disable ○ Allowed ○ Blocked

MAC Address List Candidates ▸
(MAC Address Format is 'xx:xx:xx:xx:xx:xx')

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

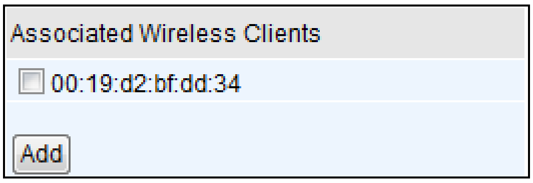
Allowed: To authorize devices to access your network by inserting the MAC Address in the space provided or by clicking on the Candidate button. Make sure your PC's MAC is listed.

Blocked: To prevent unwanted devices from accessing network by inserting the MAC Address in the space provided or by clicking on the Candidate button. Make sure your PC's MAC is not listed.

The maximum number of clients is 16. The MAC addresses are 6 bytes long; they are represented only in hexadecimal characters. The numbers 0 - 9 and letters a - f are acceptable.

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

Candidates: It automatically detects devices that are connected to the router through the Wireless access point (AP).Click the Candidate button to access the **Associated Wireless Clients** window.



Associated Wireless Clients

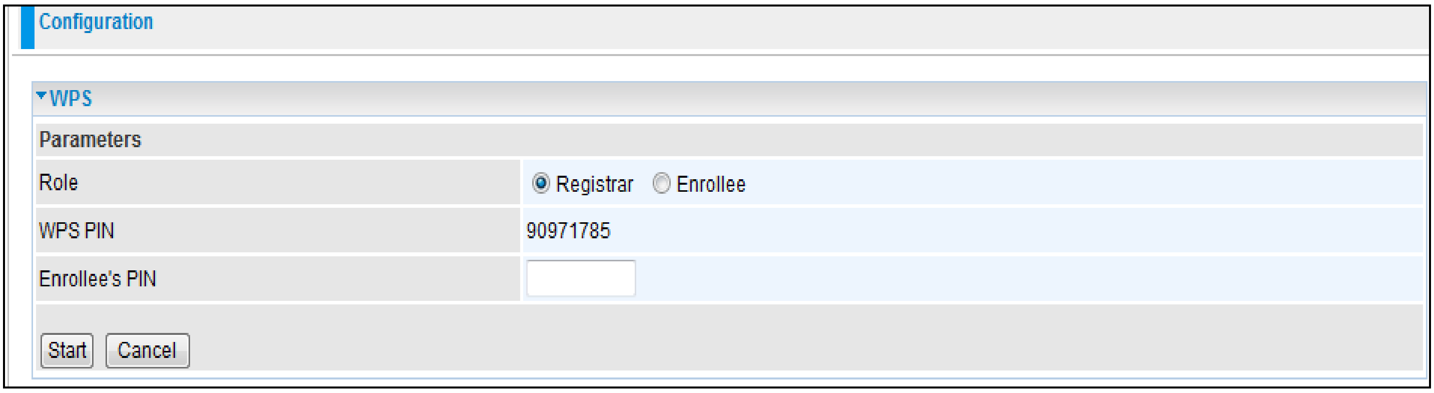
□ 00:19:d2:bf:dd:34

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

You can check the checkbox next to the MAC address to block or allow the wireless client to access the network. Then click Add to insert the Wireless Clients MAC Address into the Filter table. The maximum number of Wireless clients is 16.

WPS

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



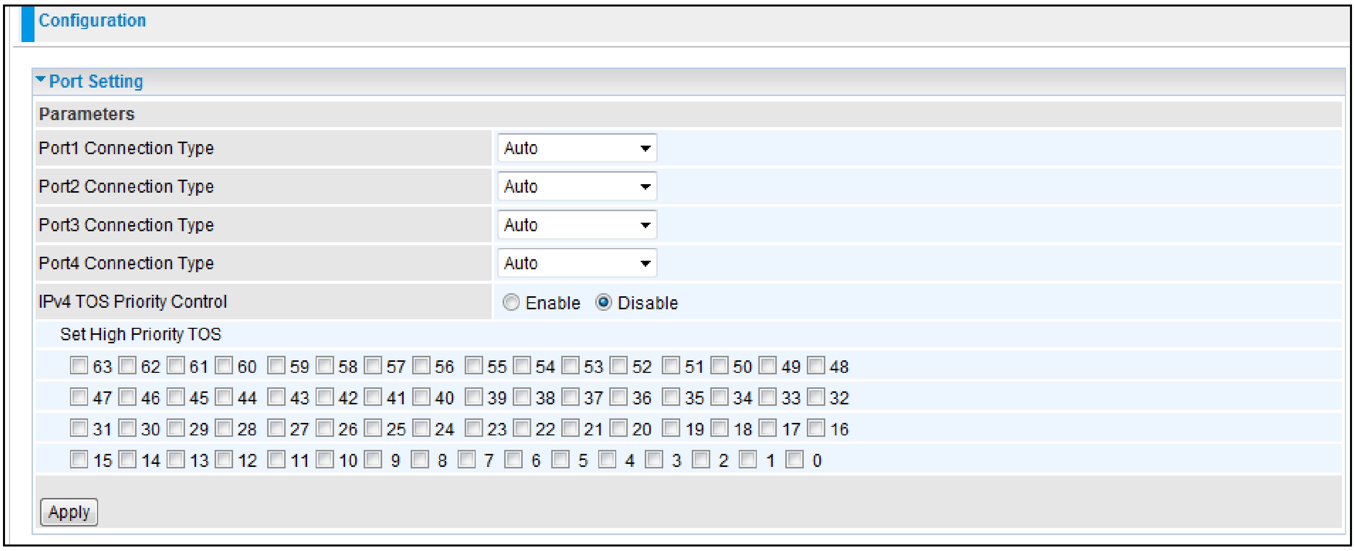
Configuration

▾WPS

Parameters	
Role	● Registrar ○ Enrollee
WPS PIN	90971785
Enrollee's PIN	

Port Setting

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



Configuration

▾Port Setting

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

Set High Priority TOS

□ 63 □ 62 □ 61 □ 60 □ 59 □ 58 □ 57 □ 56 □ 55 □ 54 □ 53 □ 52 □ 51 □ 50 □ 49 □ 48
□ 47 □ 46 □ 45 □ 44 □ 43 □ 42 □ 41 □ 40 □ 39 □ 38 □ 37 □ 36 □ 35 □ 34 □ 33 □ 32
□ 31 □ 30 □ 29 □ 28 □ 27 □ 26 □ 25 □ 24 □ 23 □ 22 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 □ 14 □ 13 □ 12 □ 11 □ 10 □ 9 □ 8 □ 7 □ 6 □ 5 □ 4 □ 3 □ 2 □ 1 □ 0

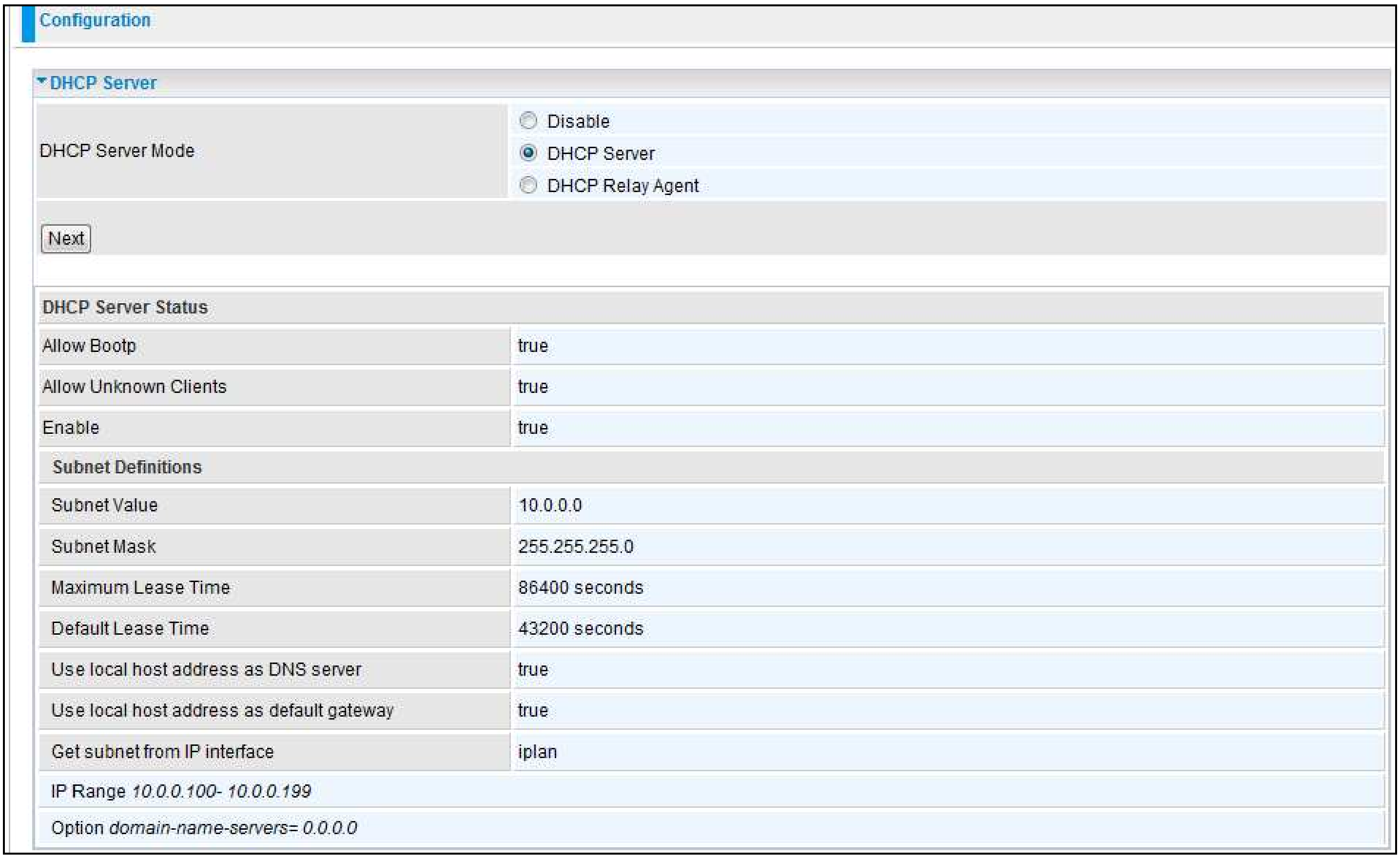
Port # Connection Type: There are six options to choose from: Auto, disable, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure different types to solve compatibility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

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

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

DHCP Server

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



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

DHCP Server Status	
Allow Bootp	true
Allow Unknown Clients	true
Enable	true
Subnet Definitions	
Subnet Value	10.0.0.0
Subnet Mask	255.255.255.0
Maximum Lease Time	86400 seconds
Default Lease Time	43200 seconds
Use local host address as DNS server	true
Use local host address as default gateway	true
Get subnet from IP interface	iplan
IP Range *10.0.0.100- 10.0.0.199*	
Option *domain-name-servers= 0.0.0.0*	

To disable the router DHCP Server, check Disabled and click Next, then click Apply. When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (by default this is 10.0.0.2).

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

If you check DHCP Relay Agent and click Next, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

Click Apply to enable this function.

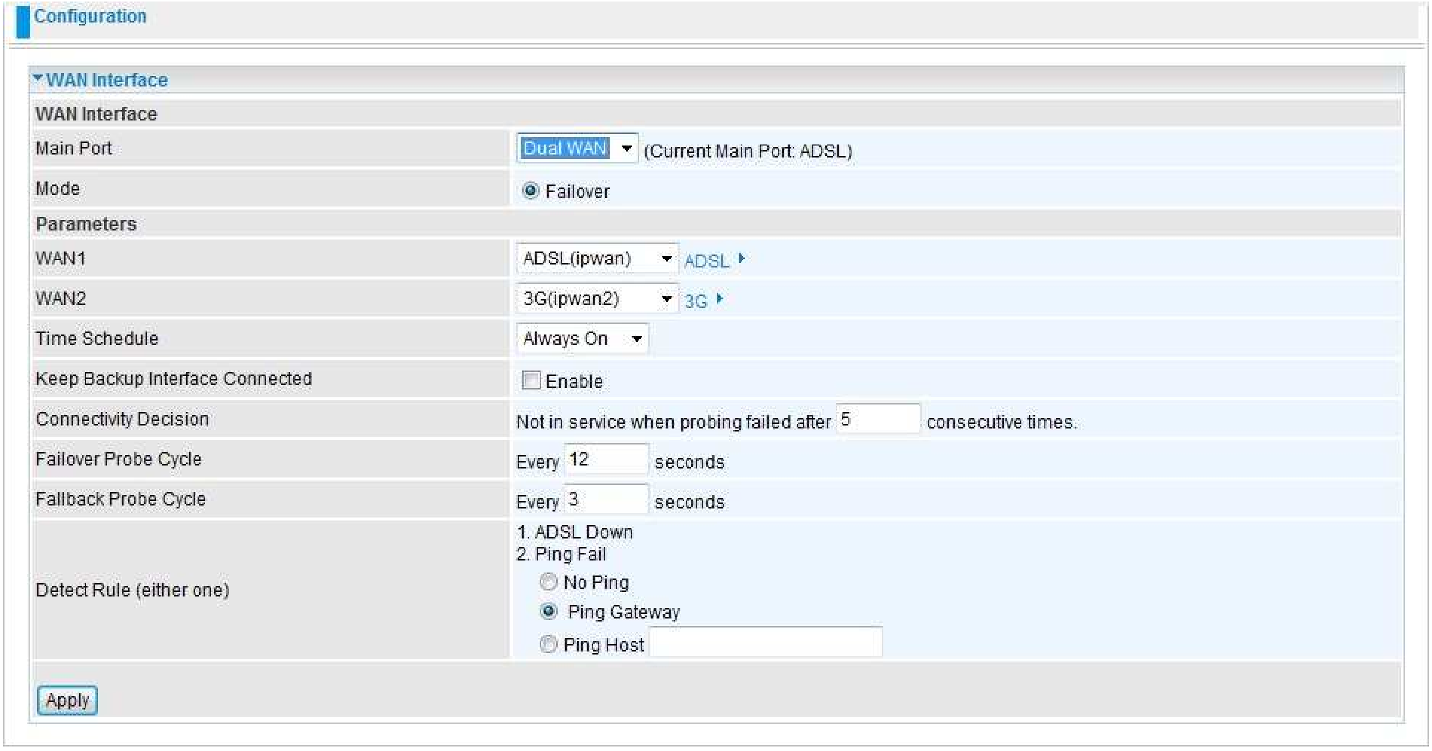
WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and the Internet. Here are the items within the WAN section: **WAN Interface, WAN Profile** and **ADSL Mode.**

WAN Interface

WAN Connection-ADSL Mode

The default setting for Connection Mode is ADSL and the default Protocol is PPPoE.



Configuration

▾WAN Interface

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

Main Port: User can select either ADSL, 3G mode or Dual WAN.

Mode: Select the radio button if you want to enable the ADLS / 3G failover / failback function.

WAN1: Select the primary WAN Interface it should use. You may select ADSL or 3G.

WAN2: Select the secondary or failover WAN interface. i.e. If your primary connection fails, the secondary connection will start up and connect to the internet automatically.

Time Schedule: Select the time schedule when failover should be active. Always on is the default value.

Keep Backup Interface Connected: Keeps the backup interface connected to allow seamless changeover when your primary interface fails.

Connectivity Decision: Set how many times probing must fail in order to switch to the backup port.

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

Note: The time set is for each probe cycle, but the decision to change to backup port is determined by the Probe Cycle duration multiplied by the connection Decision amount (e.g. From the image above it will be 12 seconds multiplied by 5 consecutive fails).

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

Note: The time set is for each probe cycle, but the decision to change to the backup port is determined by the Probe Cycle duration multiplied by the Connection Decision amount (e.g. From the image above it will be 3 seconds multiplied by 5 consecutive fails).

Detect Rule:

Rule 1. ADSL Down

Rule 2. Ping Fail

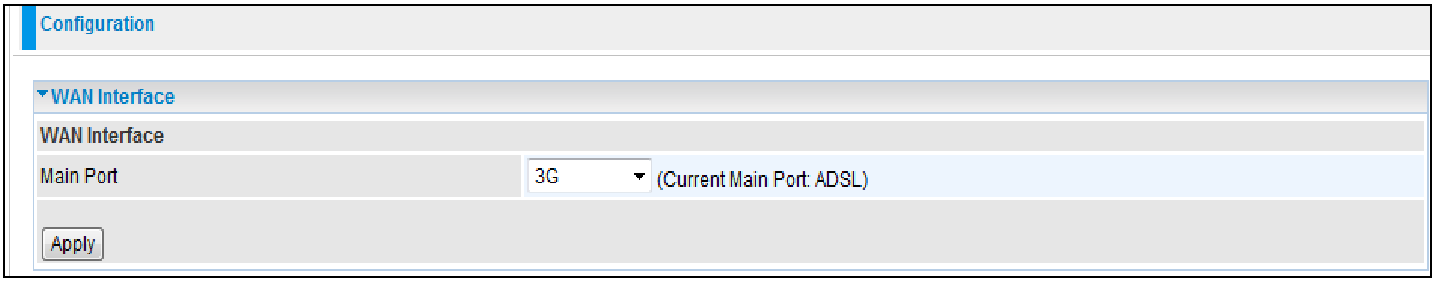
No Ping: It will not send any ping packets to determine if the connection is active. It disables ping detection.

Ping Gateway: It will send ping packets to the gateway and wait for a response from the gateway in every "Probe Cycle".

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

WAN Connection-3G Mode

In ADSL mode, as the ADSL is not available (failover/failback), it will switch to 3G mode for WAN Connection support. However, in 3G Mode ADSL cannot support WAN Connection when 3G Mode is unavailable.



Configuration

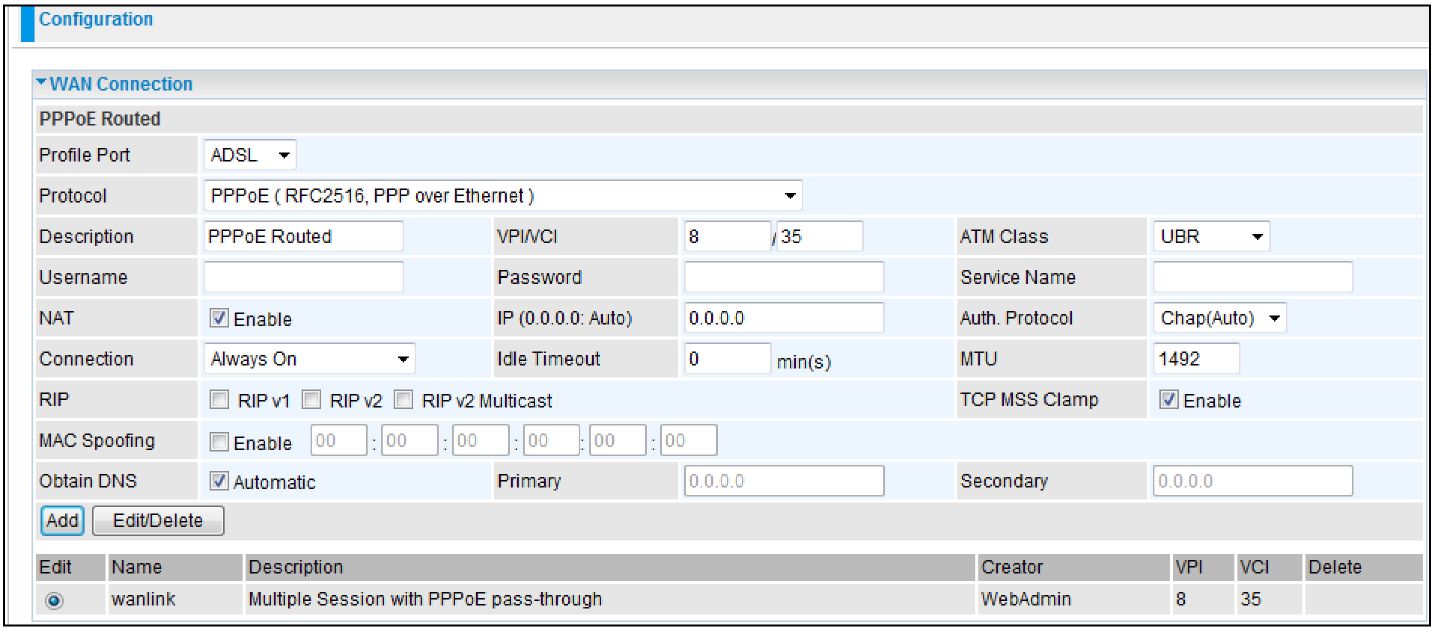
▾WAN Interface

WAN Interface	
Main Port	3G (Current Main Port: ADSL)

WAN Profile

PPPoE Connection

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



Configuration

WAN Connection

PPPoE Routed

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

Add | Edit/Delete

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	Multiple Session with PPPoE pass-through	WebAdmin	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The PPPoE protocol will be used.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

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

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

Connection:

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

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

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

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

TCP MSS Clamp: This option enables discovery of the optimal MTU size automatically. Default is enabled.

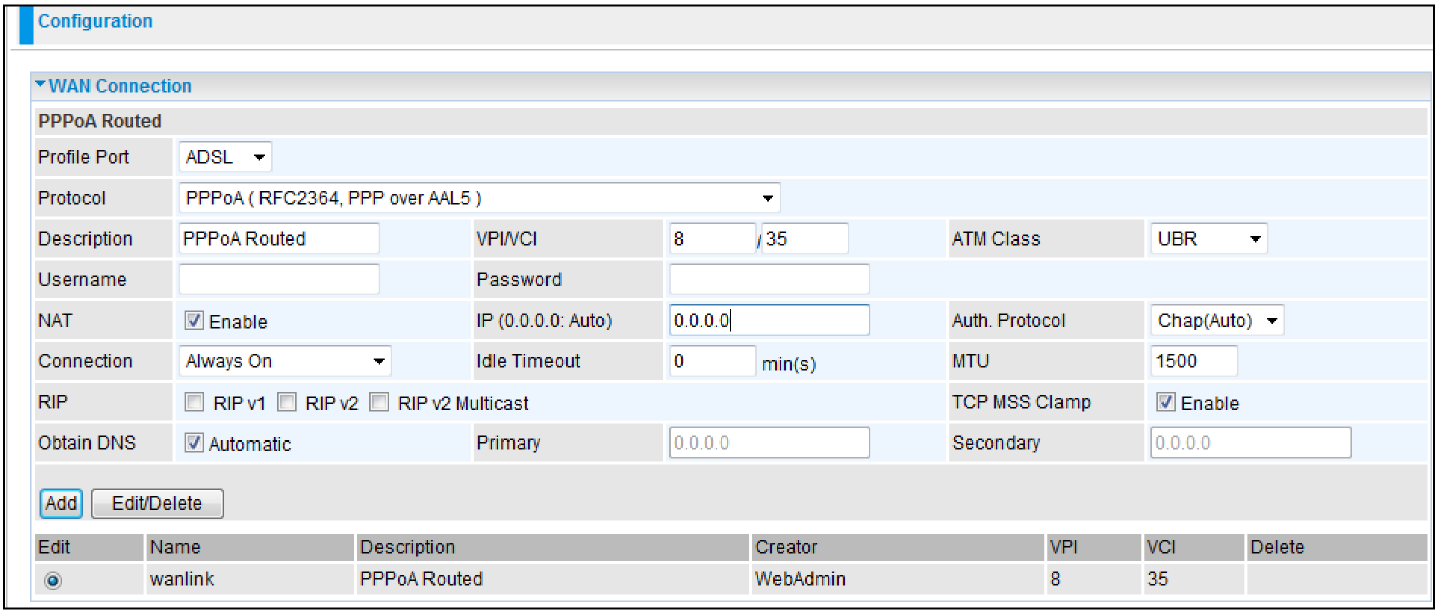
MAC Spoofing: Some service providers require the configuration of this option. You must fill in the MAC address that is specified by the service provider when it is required. Default is disabled.

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

PPPoA Connection



Configuration

WAN Connection

PPPoA Routed

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

Add Edit/Delete

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	PPPoA Routed	WebAdmin	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The PPPoA protocol will be used.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

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

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

Connection:

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

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

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

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

TCP MSS Clamp: This option enables discovery of the optimal MTU size automatically. Default is enabled.

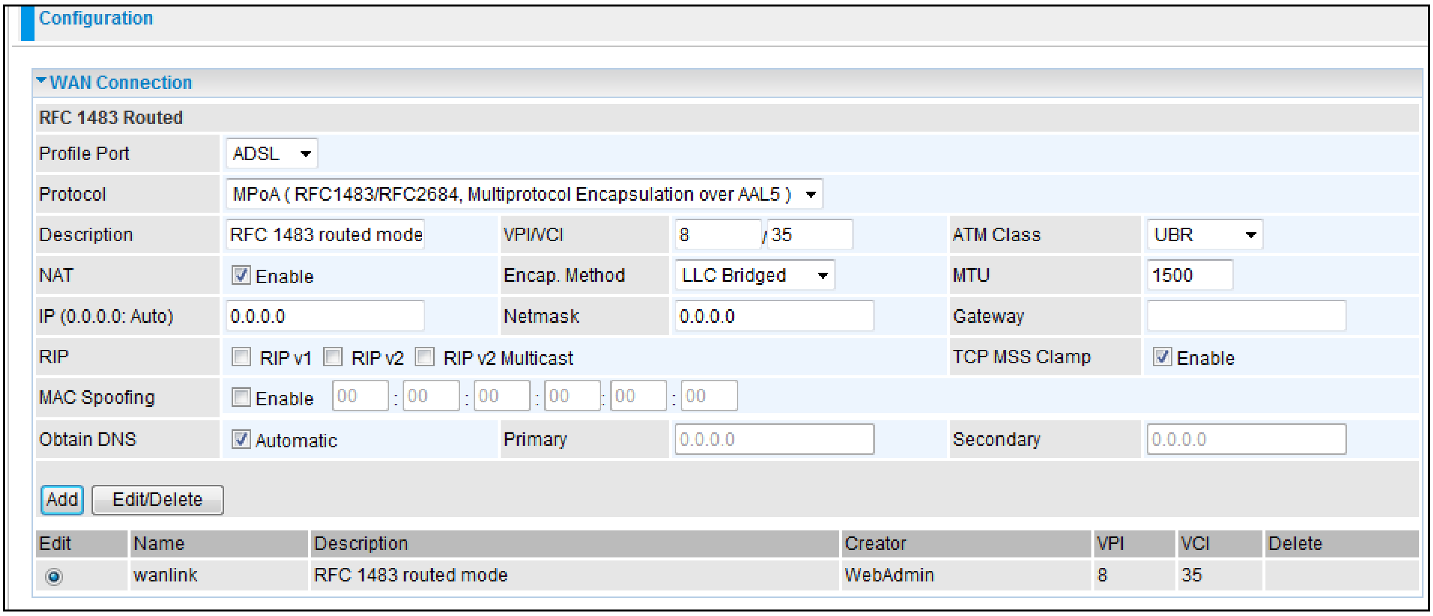
MAC Spoofing: Some service providers require the configuration of this option. You must fill in the MAC address that is specified by the service provider when it is required. Default is disabled.

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

MPoA Connection



Configuration

WAN Connection

RFC 1483 Routed

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

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	RFC 1483 routed mode	WebAdmin	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The MPoA protocol will be used.

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

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

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

Connection:

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

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

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

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

TCP MSS Clamp: This option enables discovery of the optimal MTU size automatically. Default is enabled.

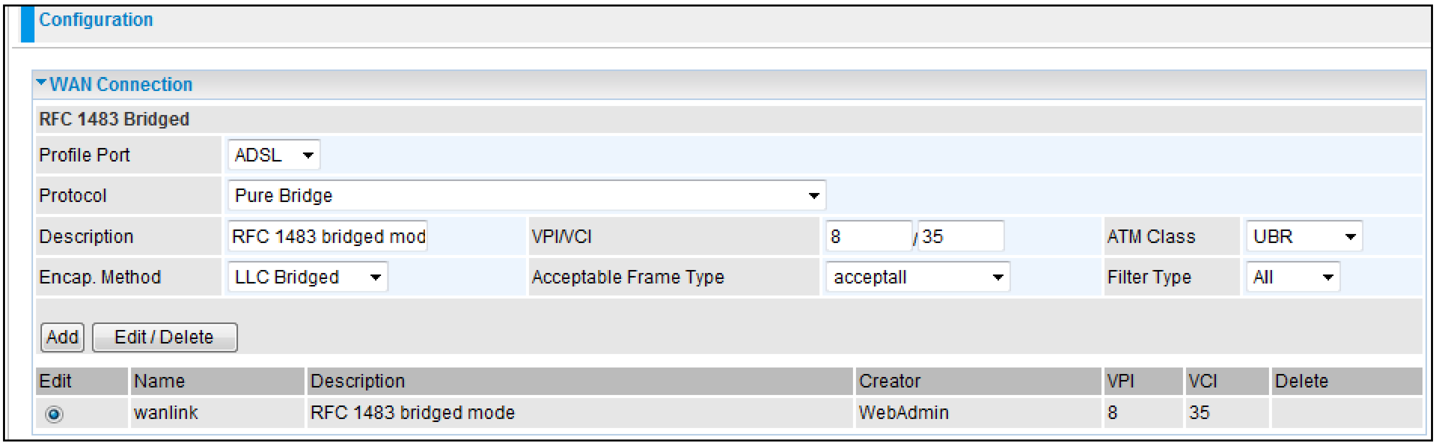
MAC Spoofing: Some service providers require the configuration of this option. You must fill in the MAC address that is specified by the service provider when it is required. Default is disabled.

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Pure Bridge



Configuration

WAN Connection

RFC 1483 Bridged

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

Edit	Name	Description	Creator	VPI	VCI	Delete
●	wanlink	RFC 1483 bridged mode	WebAdmin	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The Pure Bridge protocol will be used.

Description: A given name for this connection.

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

ATM Class: The Quality of Service for ATM layer.

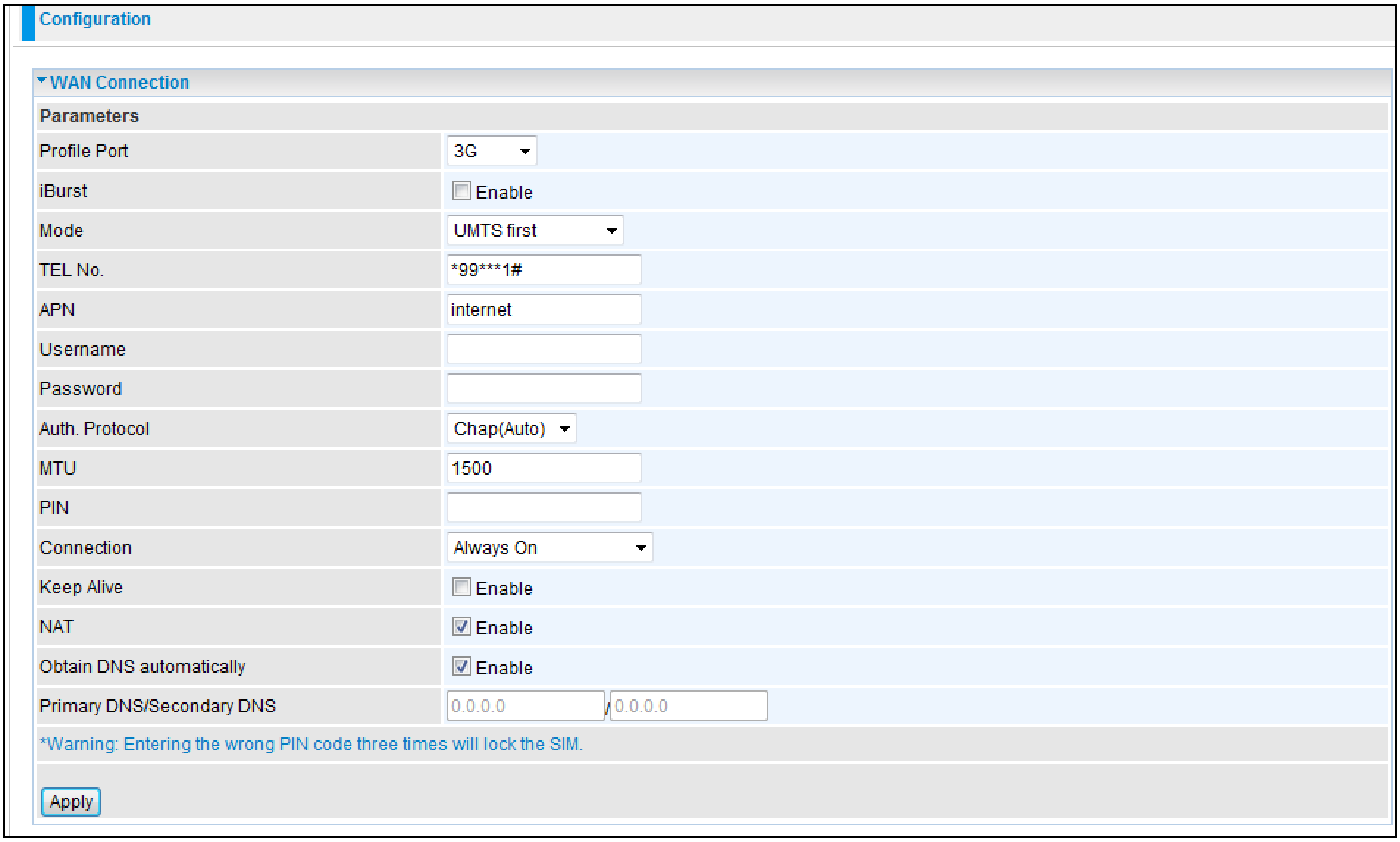
Encap. method: Choose whether you want the packets in the WAN interface to be bridged packets or routed packets.

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

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

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

3G



Configuration

▾WAN Connection

Parameters	
Profile Port	3G ▾
iBurst	□ Enable
Mode	UMTS first ▾
TEL No.	*99***1#
APN	internet
Username	
Password	
Auth. Protocol	Chap(Auto) ▾
MTU	1500
PIN	
Connection	Always On ▾
Keep Alive	□ Enable
NAT	☑ Enable
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

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

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

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

Username: Enter the username provided by your service provider.

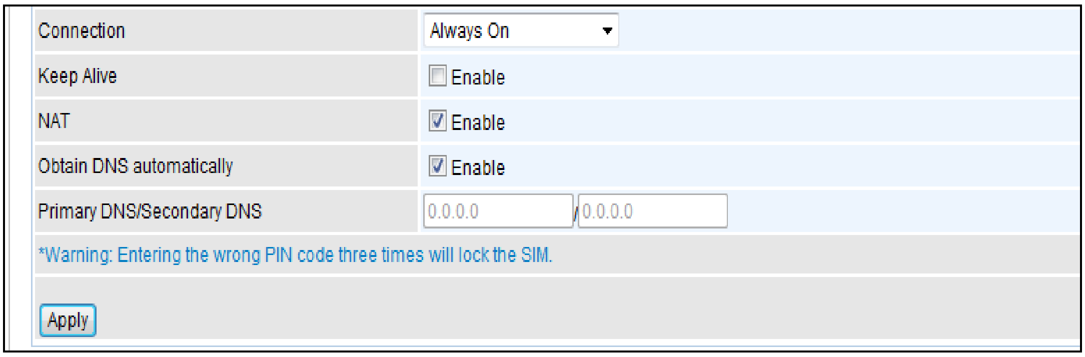
Password: Enter the password provided by your service provider.

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

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

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

Connection:

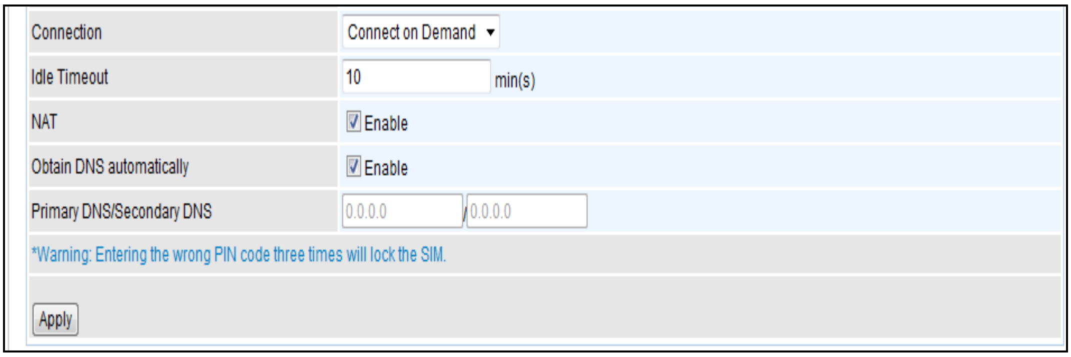


Connection	Always On
Keep Alive	□ Enable
NAT	☑ Enable
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

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

Always On: A UMTS/GPRS call will be made when the router starts up. Enabling Always On will give you the option of Keep Alive.

Keep Alive: Set Enable to allow the router to automatically reconnect the connection when the ISP disconnects it.



Connection	Connect on Demand
Idle Timeout	10 min(s)
NAT	☑ Enable
Obtain DNS automatically	☑ Enable
Primary DNS/Secondary DNS	0.0.0.0 / 0.0.0.0

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

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

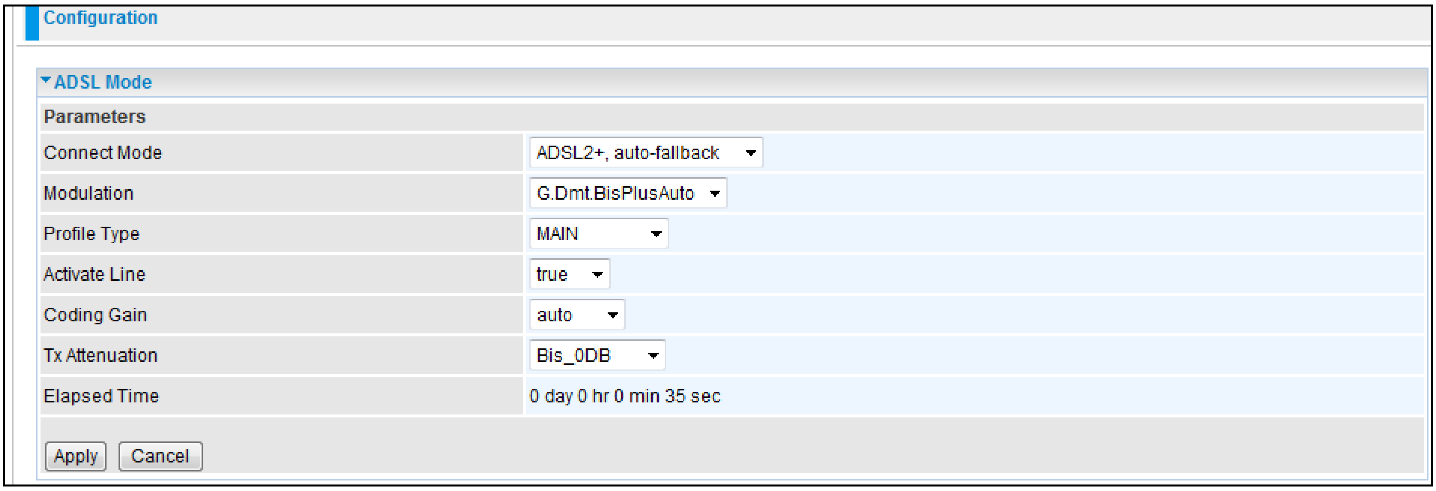
Idle Timeout: Auto-disconnect the connection when there is no activity on this call for a pre- determined period of time. The default value is 10 seconds.

Obtain DNS Automatically: Select this check box to use DNS.

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

Note: If you don't know how to set these values then please leave them unchanged.

ADSL Mode



Parameters	
Connect Mode	ADSL2+, auto-fallback
Modulation	G.Dmt.BisPlusAuto
Profile Type	MAIN
Activate Line	true
Coding Gain	auto
Tx Attenuation	Bis_0DB
Elapsed Time	0 day 0 hr 0 min 35 sec

Connect Mode: This mode will automatically detect your ADSL line code, ADSL2+, ADSL2, AnnexM2 and AnnexM2+, ADSL, All. Please keep the factory settings unless ADSL is the reason for a synchronization problem.

Modulation: It will automatically detect capability of your ADSL line mode. Please keep the factory settings unless ADSL is reason for a synchronization problem.

Profile Type: Please keep the default factory settings. If ADSL is the reason for low link rates, or making your connection unstable then consider changing the value. You may need to change the profile setting to reach the best ADSL line rate; it depends on the DSLAM and location.

Activate Line: Aborting (false) your ADSL line and making it active (true) again will take effect when setting the Connect Mode.

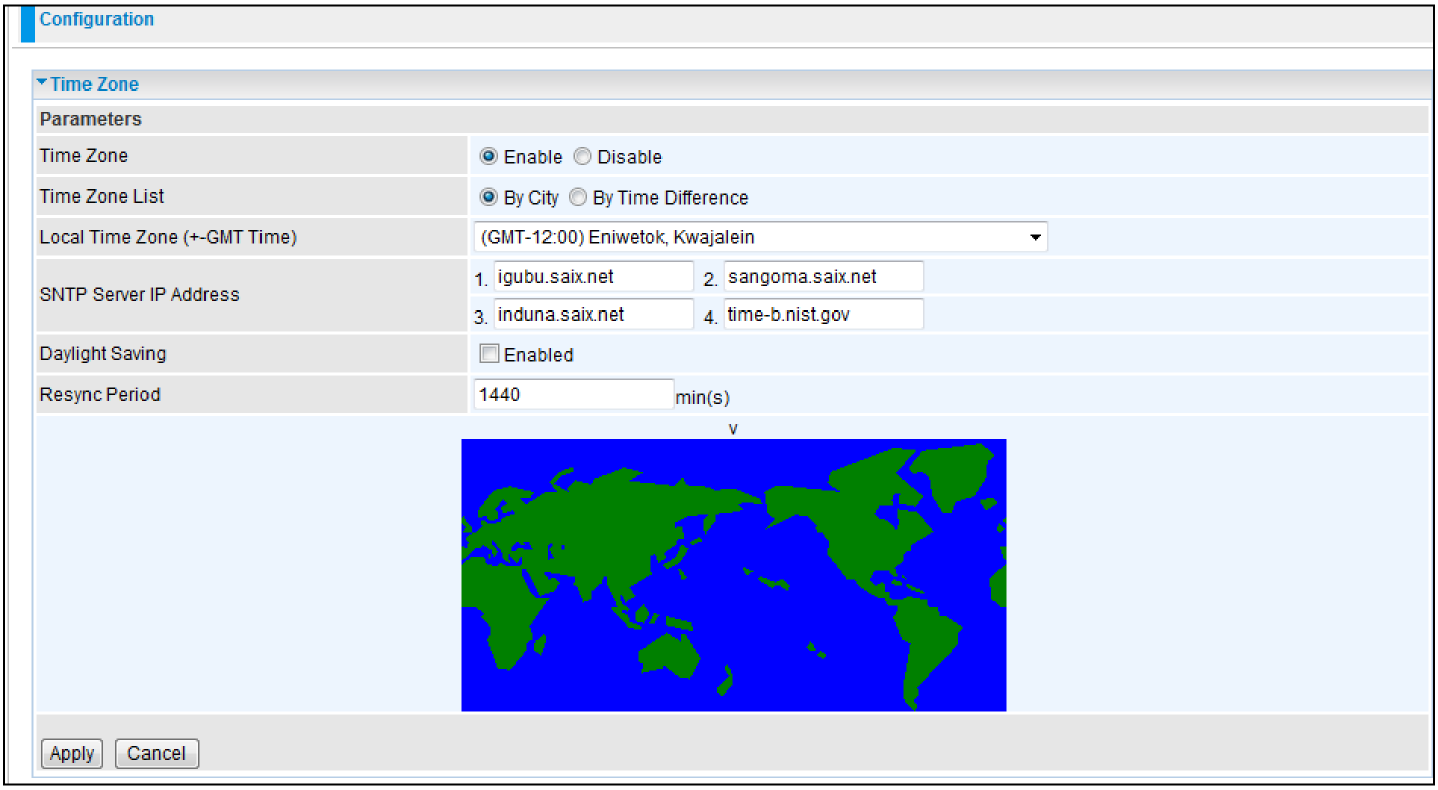
Coding Gain: It reduces the router’s transmit power which will affect the router’s downstream performance. Making the gain Higher will increase the downstream rate but might cause your ADSL line to be unstable. The configurable ADSL coding gain is from 0 dB to 7dB, or automatic.

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

System

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

Time Zone



Configuration

▾ Time Zone

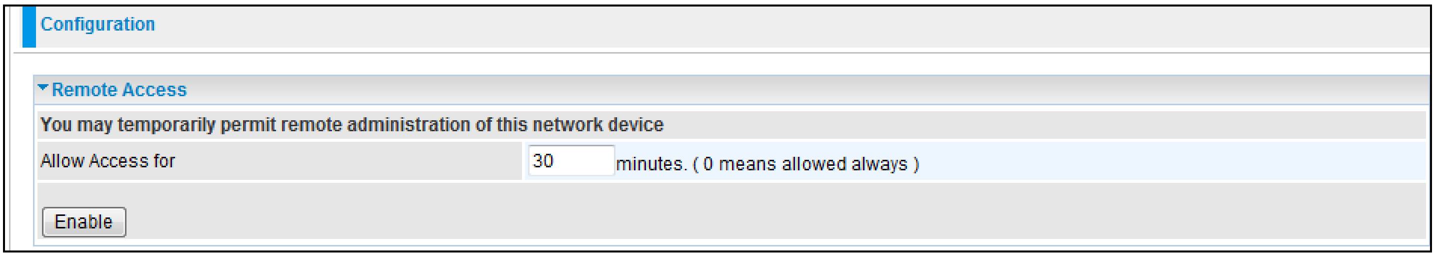
Parameters	
Time Zone	● Enable ○ Disable
Time Zone List	● By City ○ By Time Difference
Local Time Zone (+-GMT Time)	(GMT-12:00) Eniwetok, Kwajalein
SNTP Server IP Address	1. igubu.saix.net 2. sangoma.saix.net 3. induna.saix.net 4. time-b.nist.gov
Daylight Saving	□ Enabled
Resync Period	1440 min(s)

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

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

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

Remote Access



Configuration

Remote Access

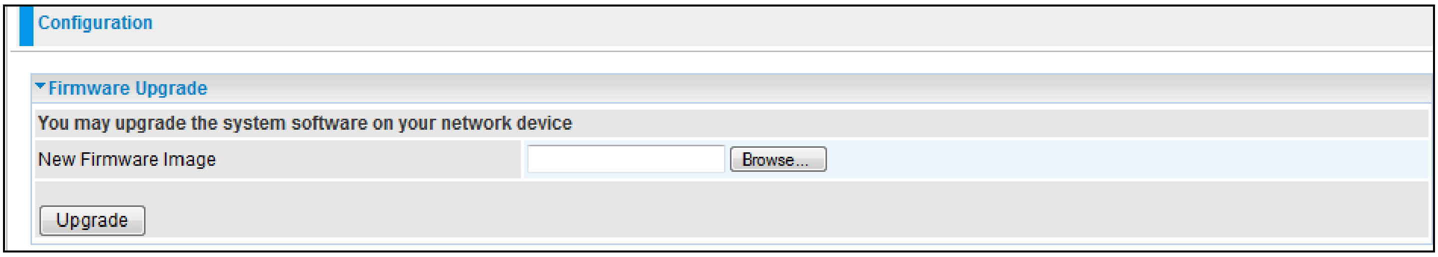
You may temporarily permit remote administration of this network device

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

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

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

Firmware Upgrade



Configuration

Firmware Upgrade

You may upgrade the system software on your network device

New Firmware Image	Browse...

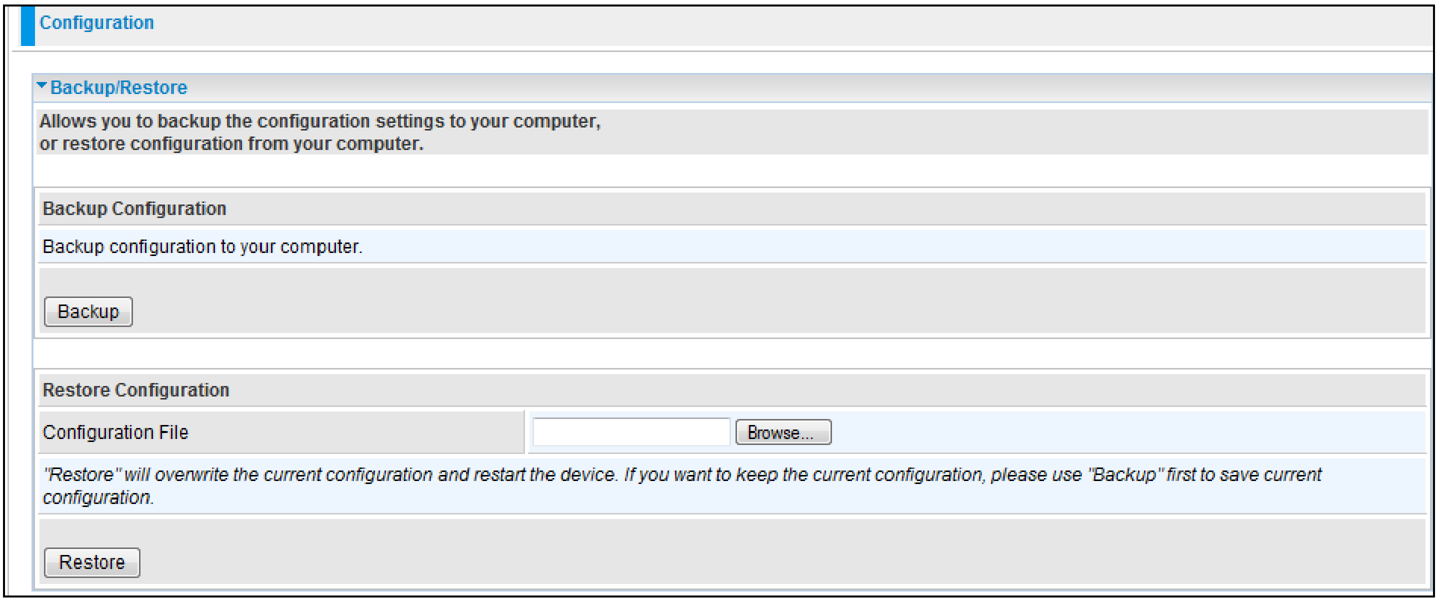
Your router firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to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

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

Warning

✓ **DO NOT turn off or interrupt the router during a firmware upgrade. This could seriously damage the router.**

Backup / Restore



Configuration

▾Backup/Restore

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

Backup Configuration

Backup configuration to your computer.

Restore Configuration

Configuration File

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

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

Create a Router Configuration Backup:

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

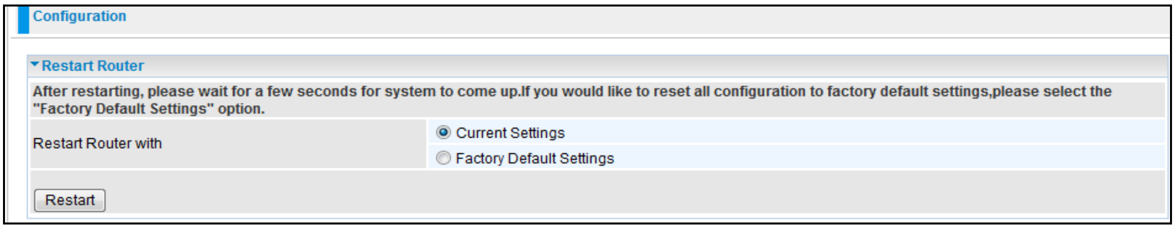
Restoring the Router Configuration

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

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

Restart Router

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



Configuration

▾Restart Router

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

Restart Router with ● Current Settings ○ Factory Default Settings

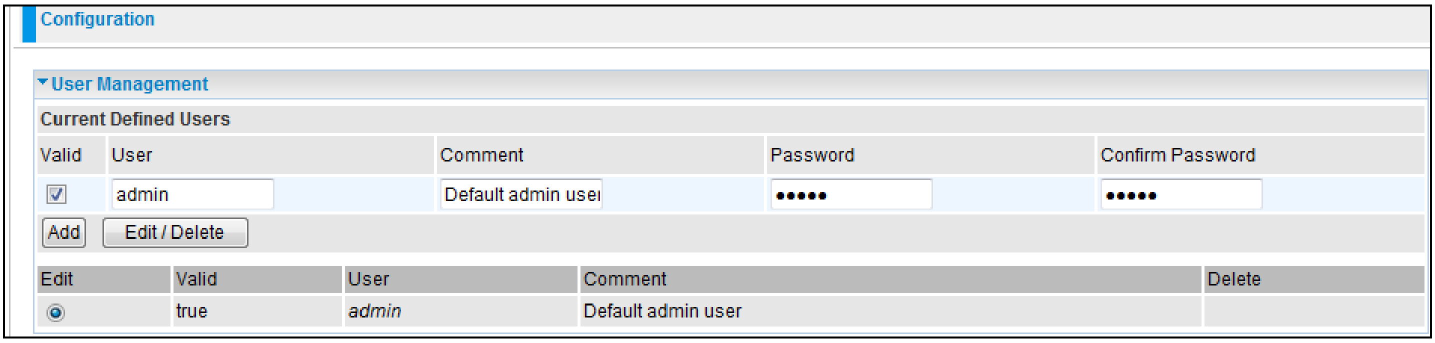
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

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

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

User Management

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



Configuration

User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
☑	admin	Default admin usei	•••••	•••••

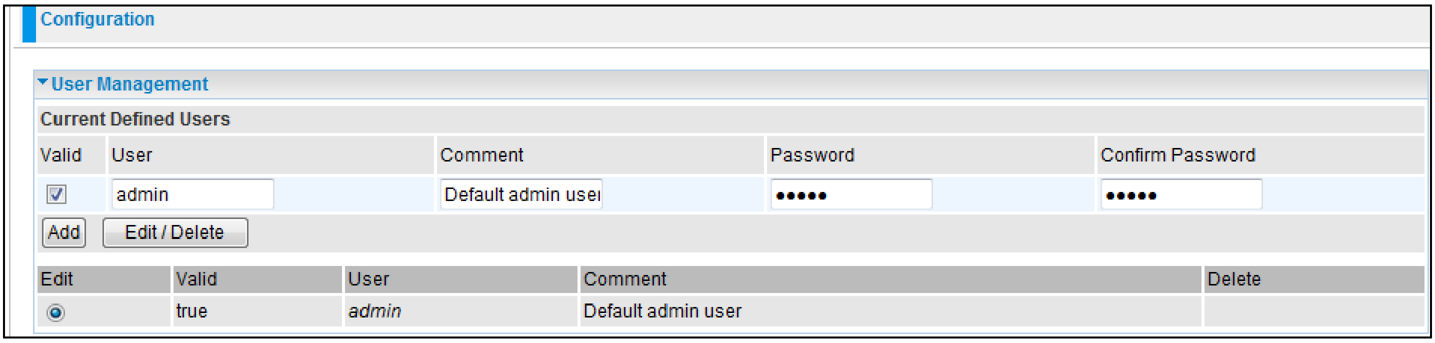
Edit	Valid	User	Comment	Delete
●	true	*admin*	Default admin user	

Edit Account Information

You can change the information of any account whether the account is active or not.

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

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



Configuration

User Management

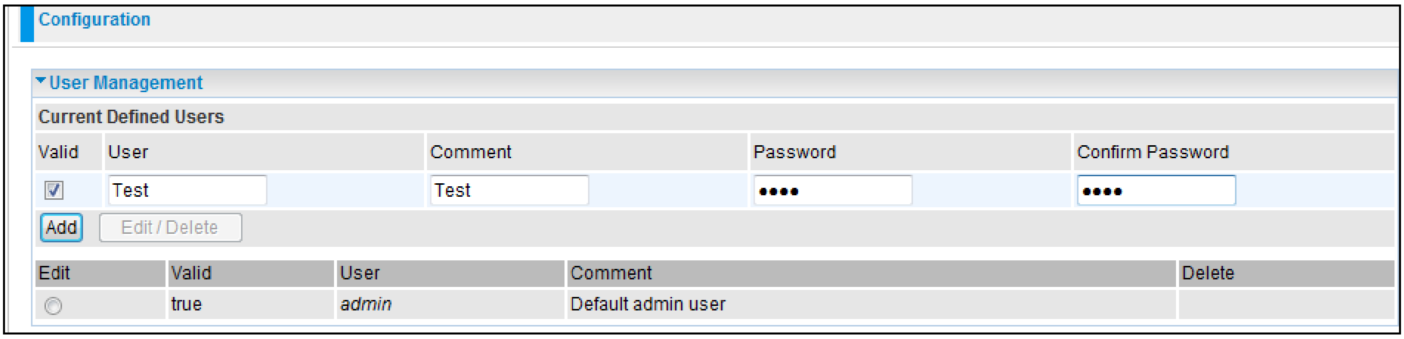
Current Defined Users

Valid	User	Comment	Password	Confirm Password
☑	admin	Default admin usei	•••••	•••••

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

To Add an Account

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



Current Defined Users

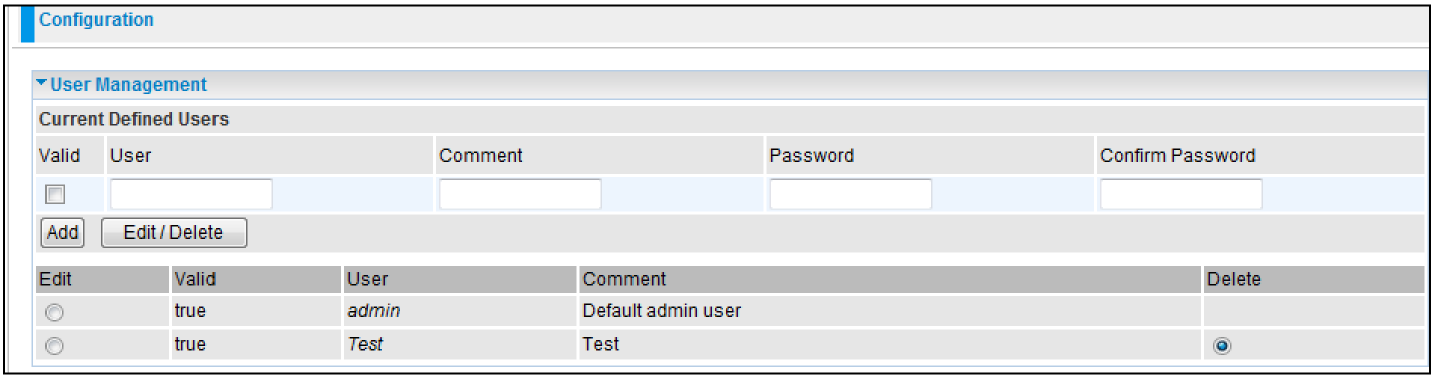
Valid	User	Comment	Password	Confirm Password
☑	Test	Test	••••	••••

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

To delete a user Account:

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

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



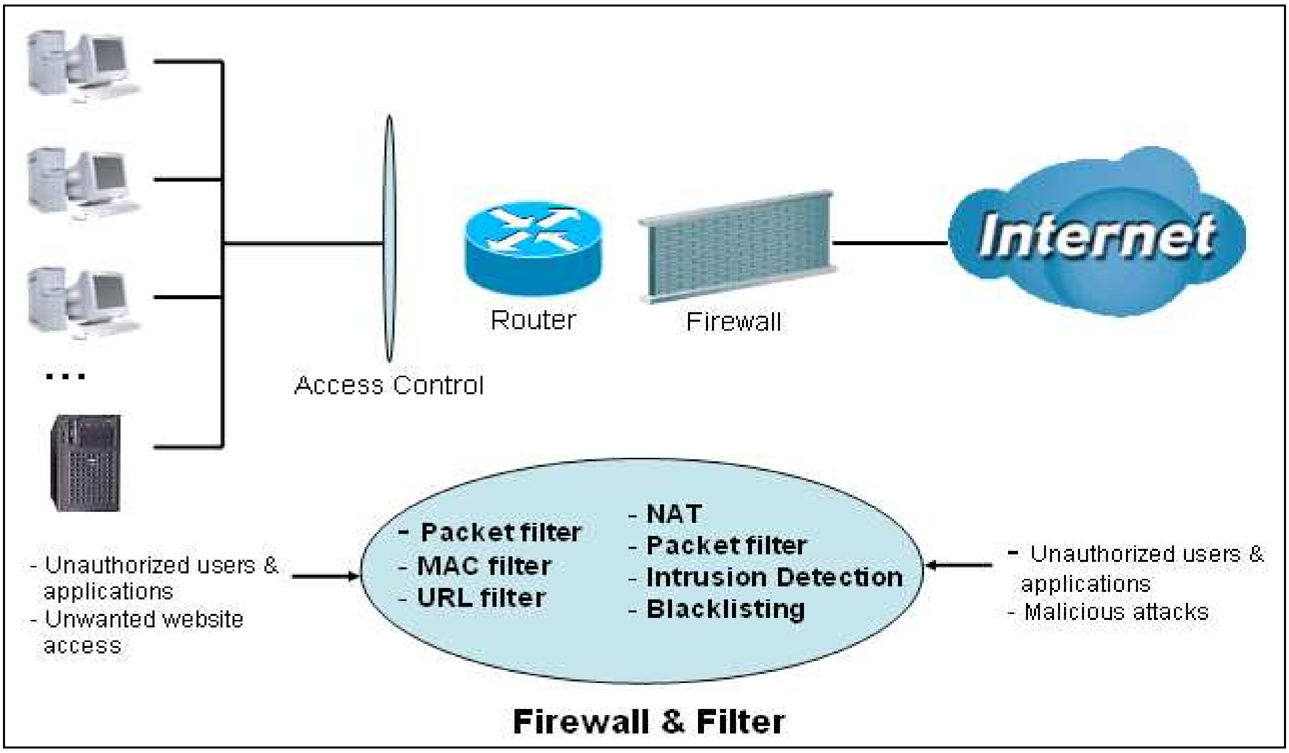
Current Defined Users

Valid	User	Comment	Password	Confirm Password
☐				

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

Firewall and Access Control

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



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

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

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

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

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

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

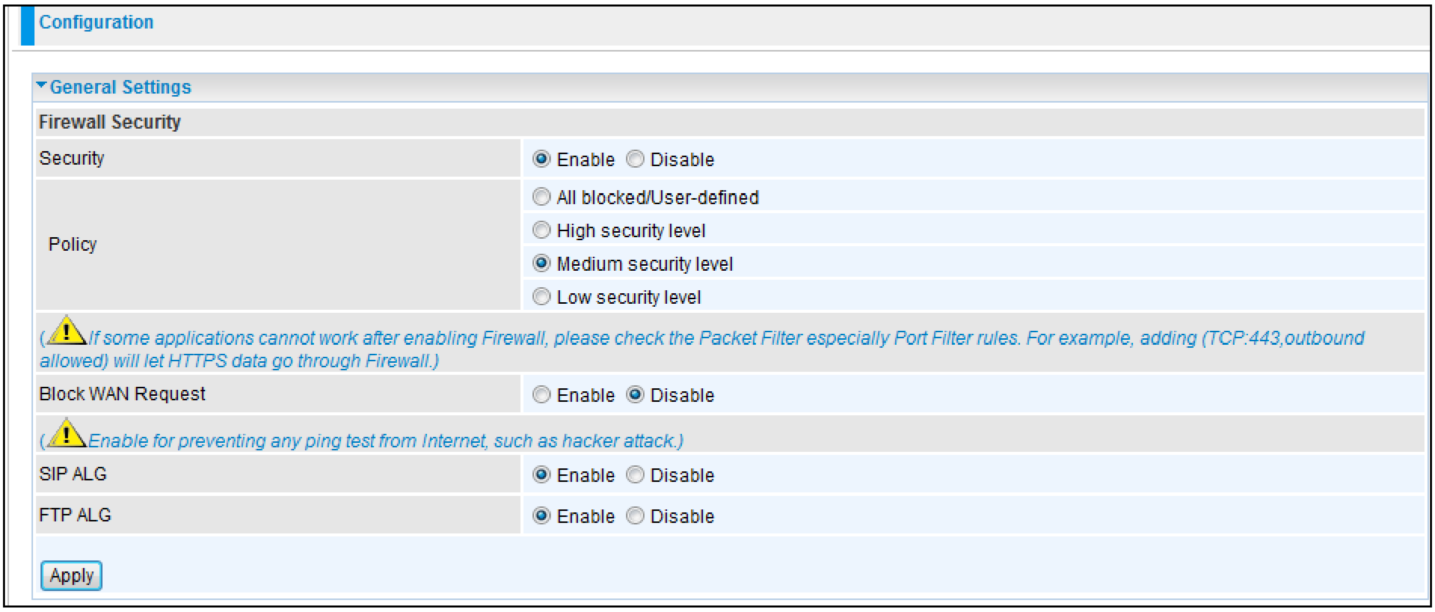
NOTE:

- ✓ **When using Virtual Server, your PC will become exposed to a certain degree to unknown users if specific ports are opened in the firewall packet filter setting. The degree of exposure depends on the parameter set in the Virtual Server setting.**

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

General Settings

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



Configuration

▾General Settings

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

There are four policy options to choose from:

All blocked/User-defined: no predefined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules to access the Internet.

High/Medium/Low security level: the predefined port filter rules for High, Medium and Low security are displayed in the Port Filters of the Packet Filter.

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

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

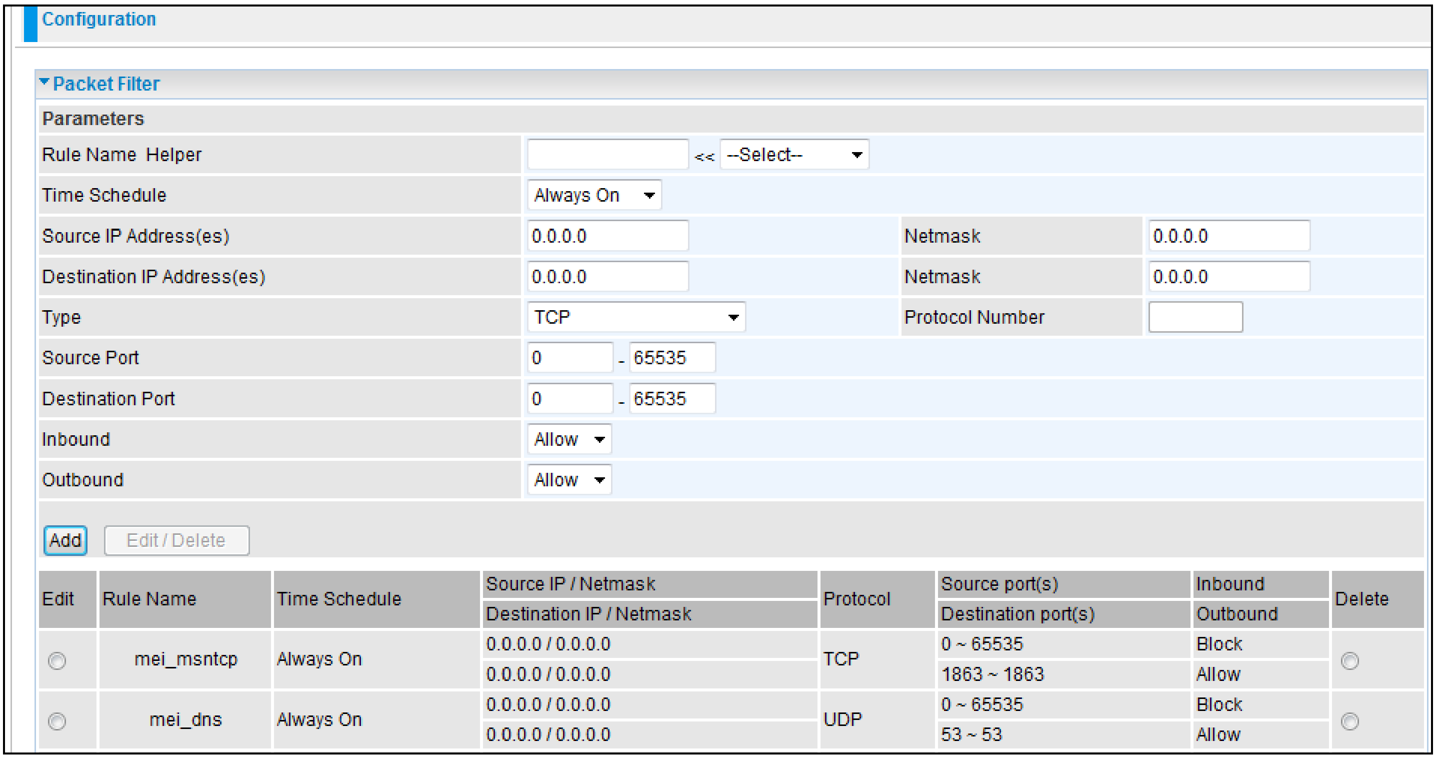
The “Block WAN Request” is a standalone function that is not affected by whether the security is enabled or disabled. This is used to prevent any scan tools that might come from hackers.

NOTE:

✓ **Any remote user attempting to perform this action may cause all access to the router to be blocked, which will result in no configuration or managing of the device from the internet.**

Packet Filter

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



Configuration

Packet Filter

Parameters

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

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

Table 1: Predefined Port Filters Rules

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

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)	443	443	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN

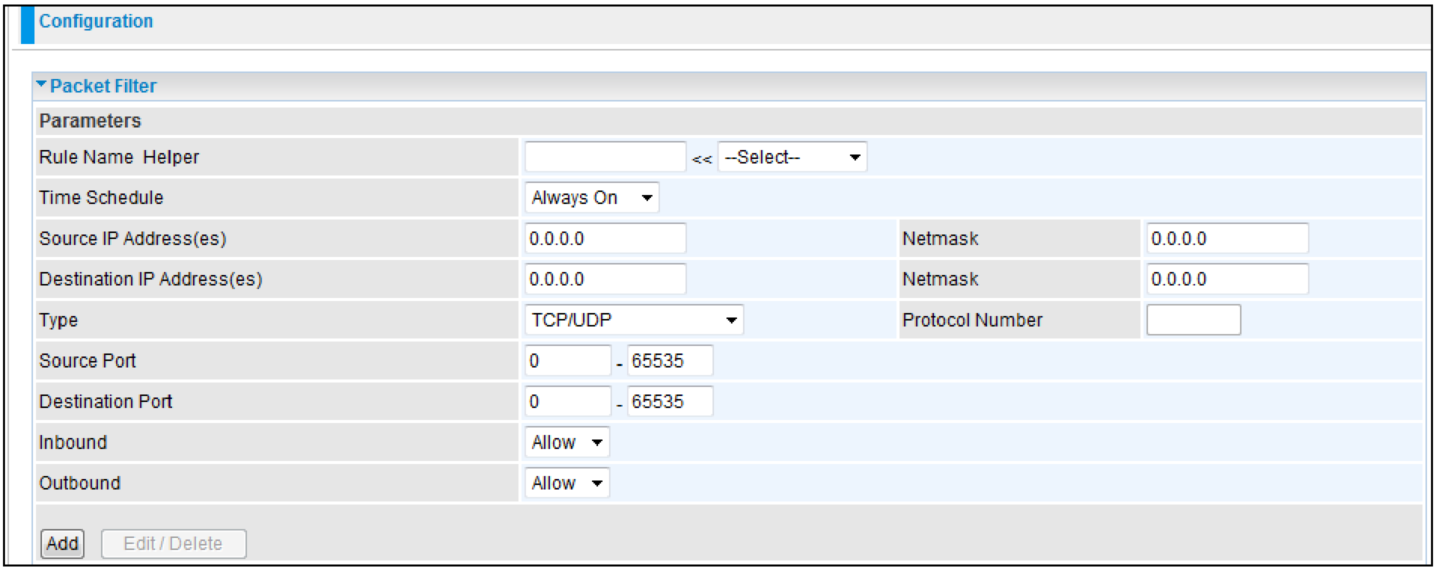
Outbound: LAN to Internet

YES: Allowed

NO: Blocked

N/A: Not Applicable

Packet Filter – Add TCP/UDP Filter



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

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

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

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

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

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

Protocol Number: Insert the port number.

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

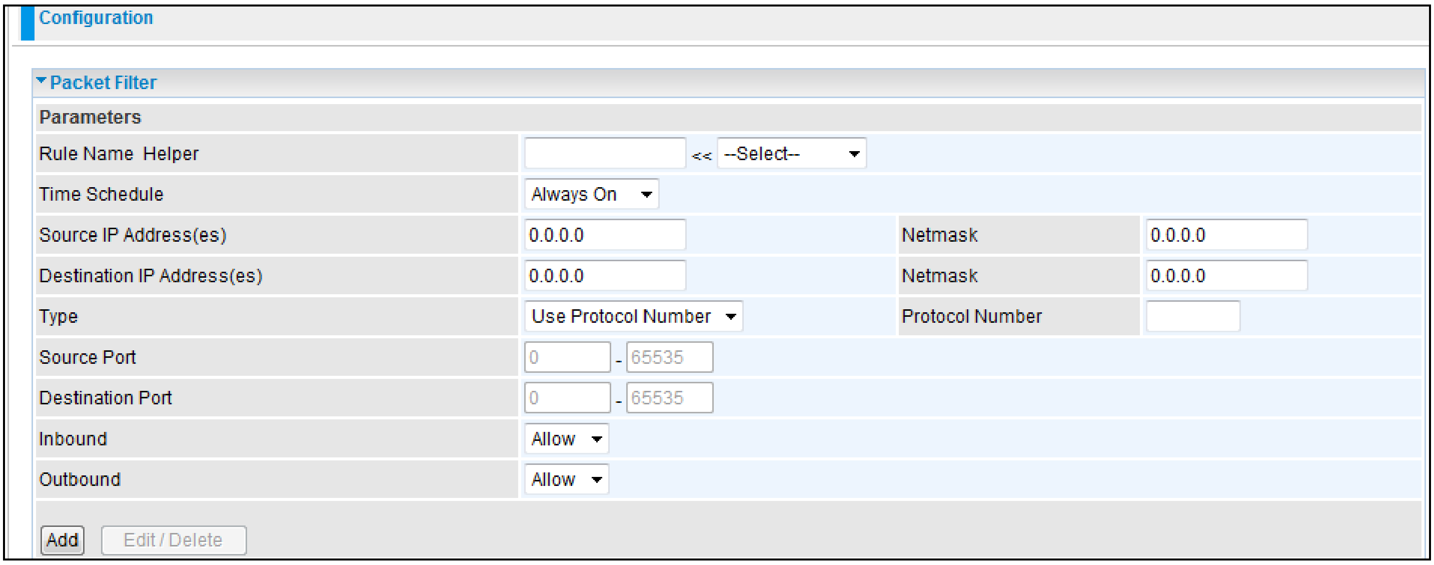
Destination Port: This is the Port or Port Ranges that defines the application.

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

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

Packet Filter – Add Raw IP Filter

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



Configuration

Packet Filter

Parameters

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

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

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

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

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

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

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

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

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

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

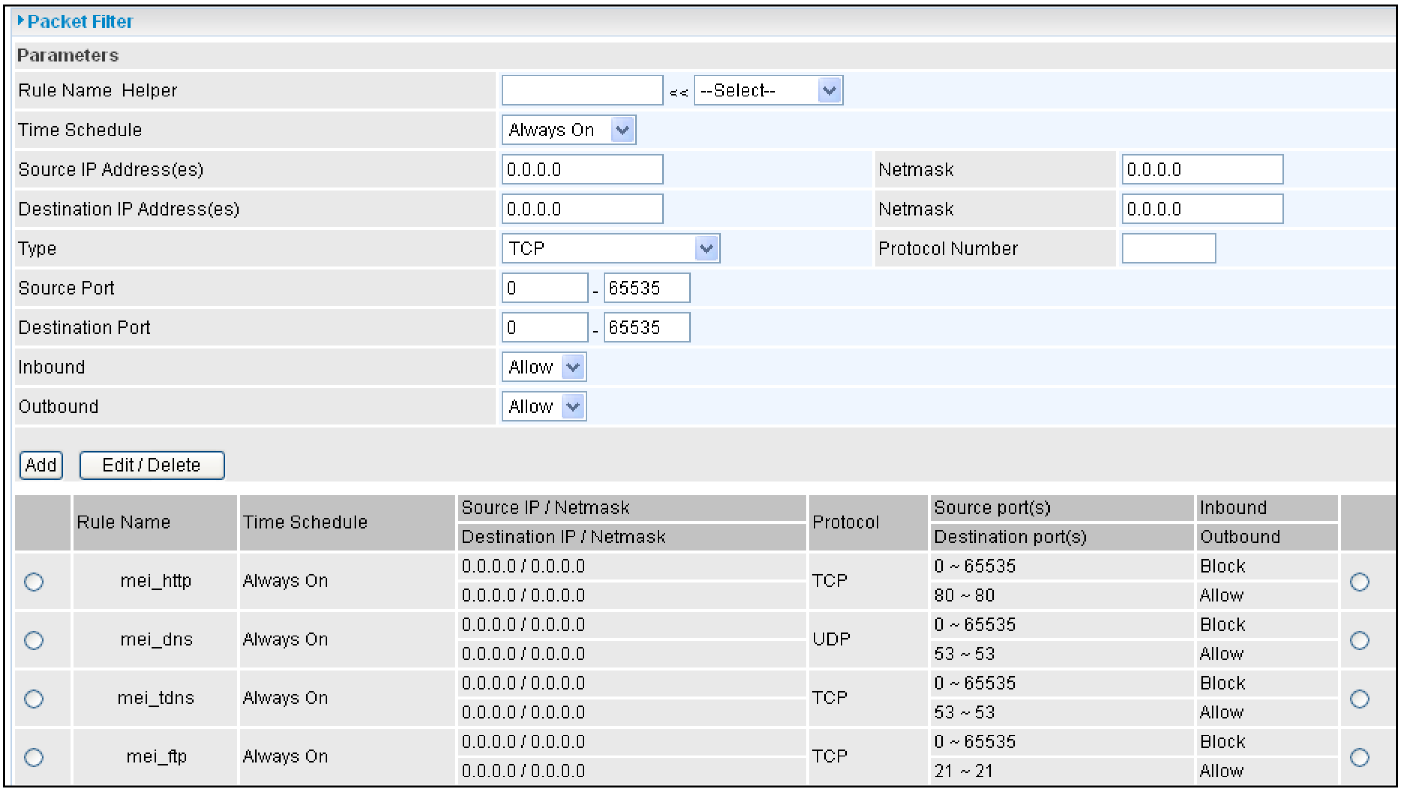
When all changes are made, click the Add button to apply your changes.

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

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

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

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



▸ Packet Filter

Parameters

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

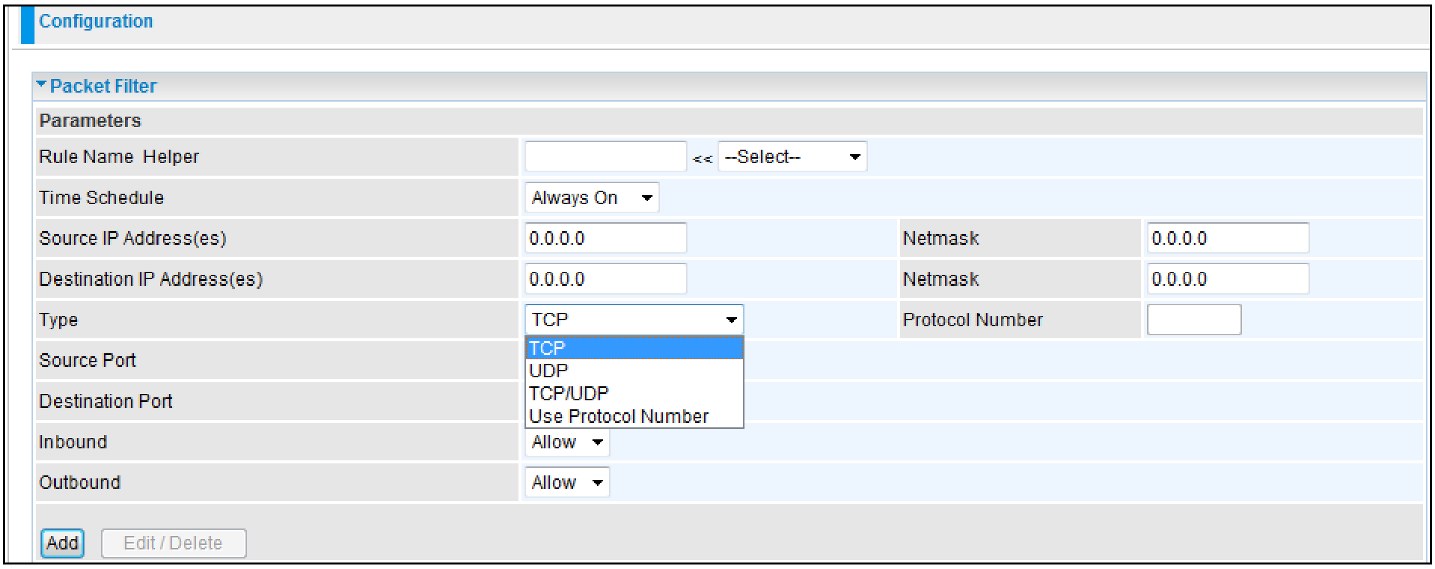
Add | Edit / Delete

	Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound	
○	mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	○
○	mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	○
○	mei_tdns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 53 ~ 53	Block Allow	○
○	mei_ftp	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 21 ~ 21	Block Allow	○

Configuring Packet Filter:

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

Note: You may choose to Edit the predefined rule instead of Deleting0 it. This is an example to show you how to add a filter on your own.



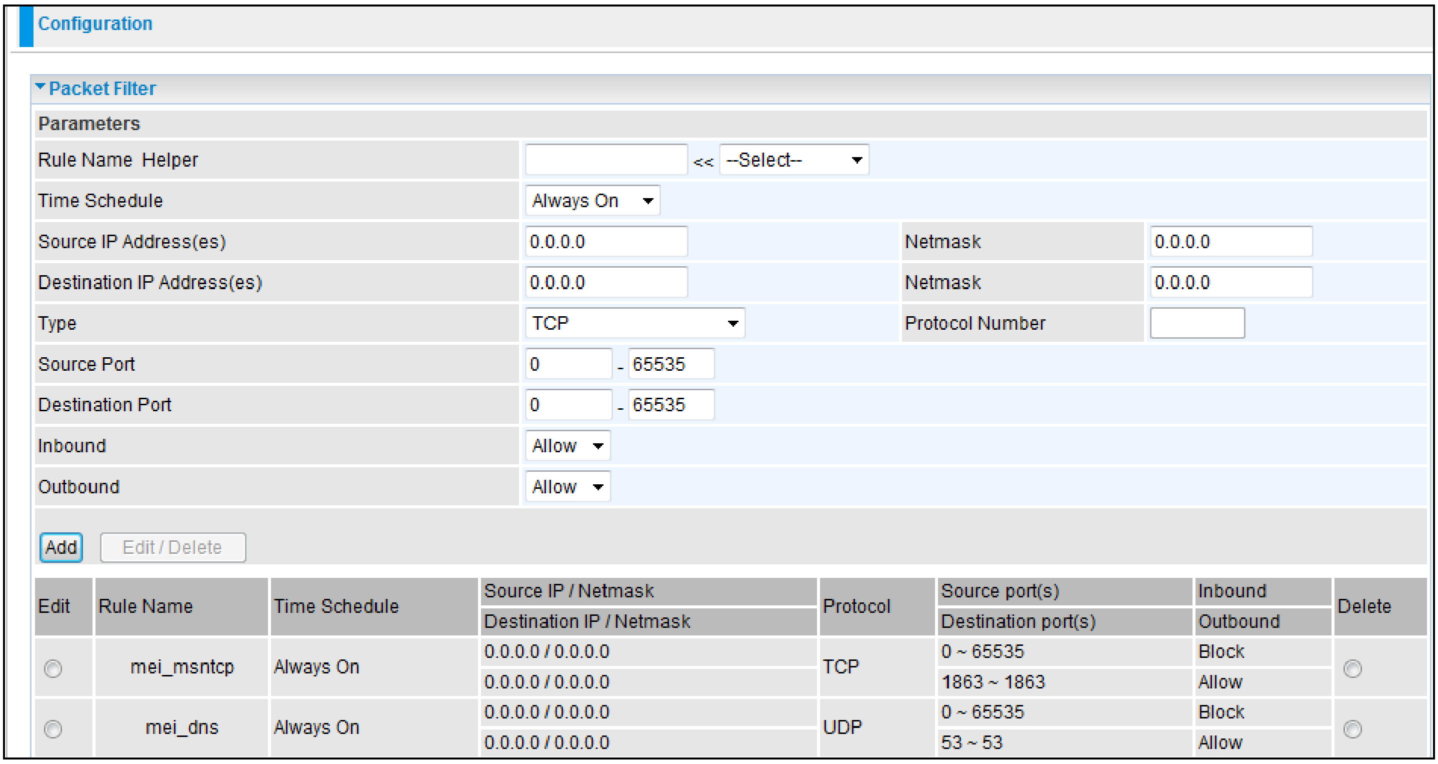
Configuration

▾ Packet Filter

Parameters

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

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



Configuration

Packet Filter

Parameters

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

Add   Edit / Delete

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

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

Example:

Application: Cindy_HTTP

Time Schedule: Always On

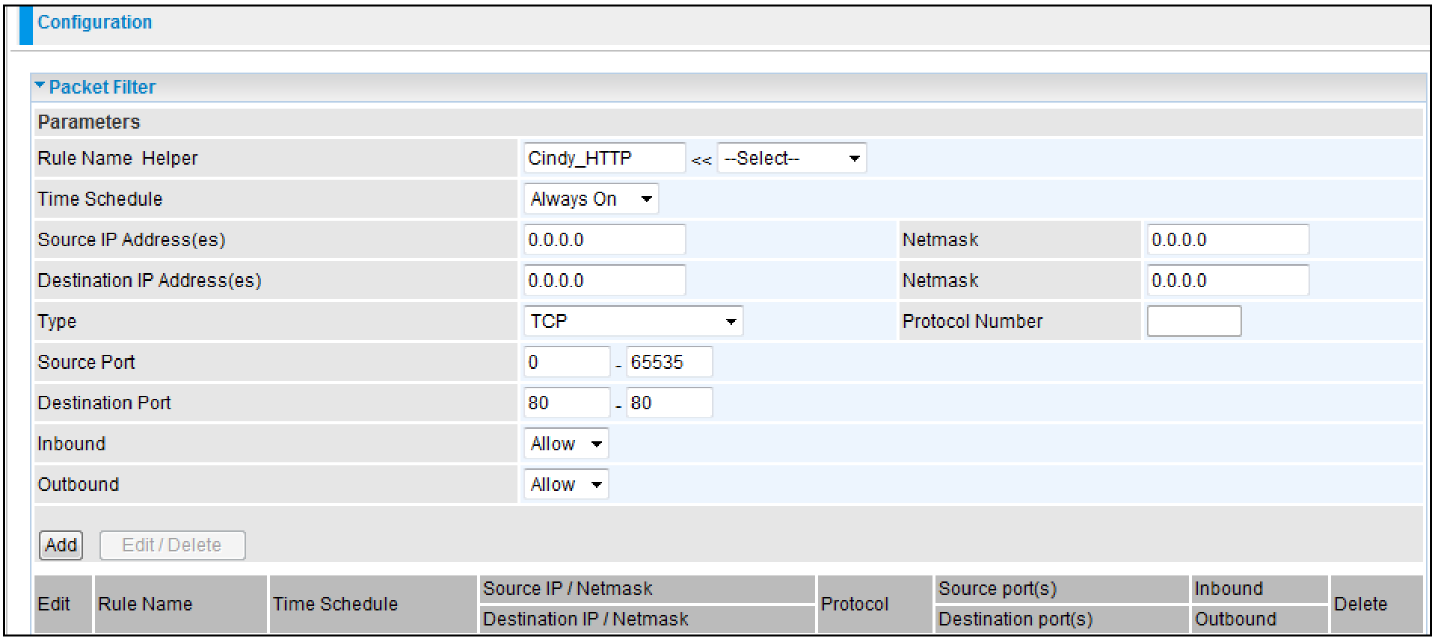
Source / Destination IP Address (es): 0.0.0.0 (I do not wish to activate the address-filter, using the port-filter instead)

Type: TCP (Please refer to Table1: Predefined Port Filter)

Source Port: 0-65535 (I am allowing all ports to connect to the application)

Redirect Port: 80-80 (This is the Port defined for HTTP)

Inbound / Outbound: Allow



Configuration

Packet Filter

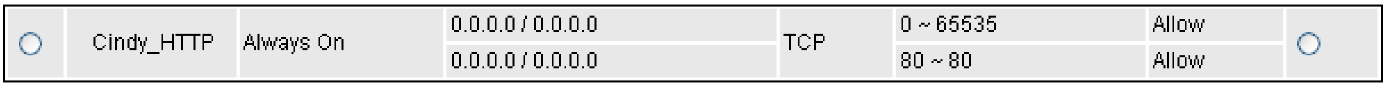
Parameters

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

Add | Edit / Delete

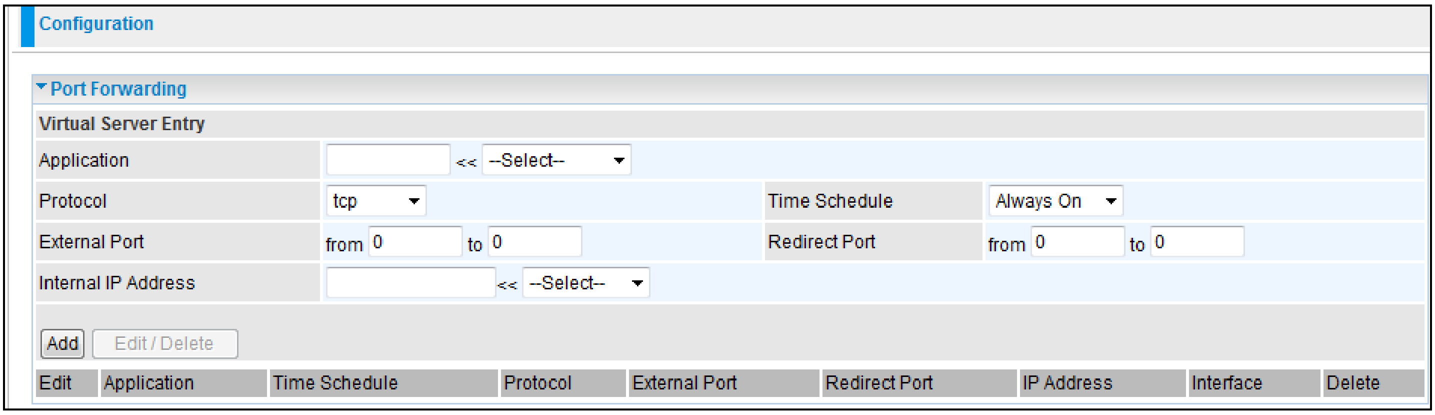
Edit	Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound	Delete

The new port filter rule for HTTP is shown below:



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

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



Configuration

Port Forwarding

Virtual Server Entry

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

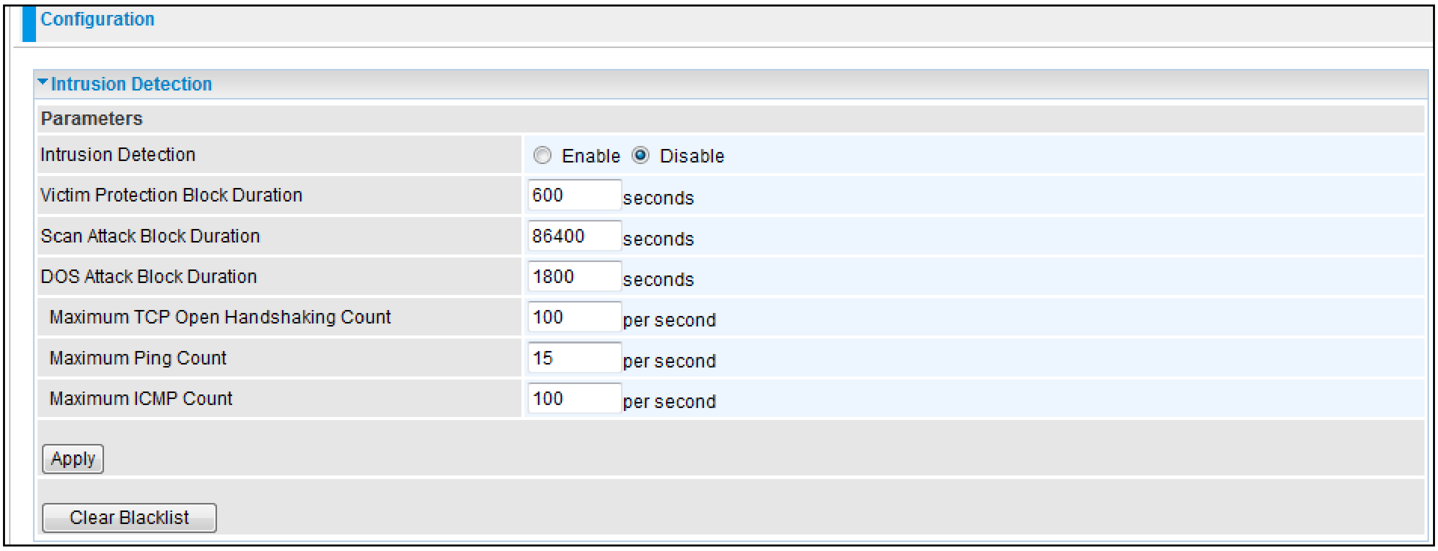
Add | Edit / Delete

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

NOTE:

✓ **For instructions on how to configure the HTTP in Virtual Server, please refer to the Add Virtual Server sub-section under the Virtual Server section.**

Intrusion Detection



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

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

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

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

Block Duration:

> **Victim Protection Block Duration**: This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.
>
> **Scan Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan, IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.
>
> **DoS Attack Block Duration**: This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks that are blocked include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

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

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

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

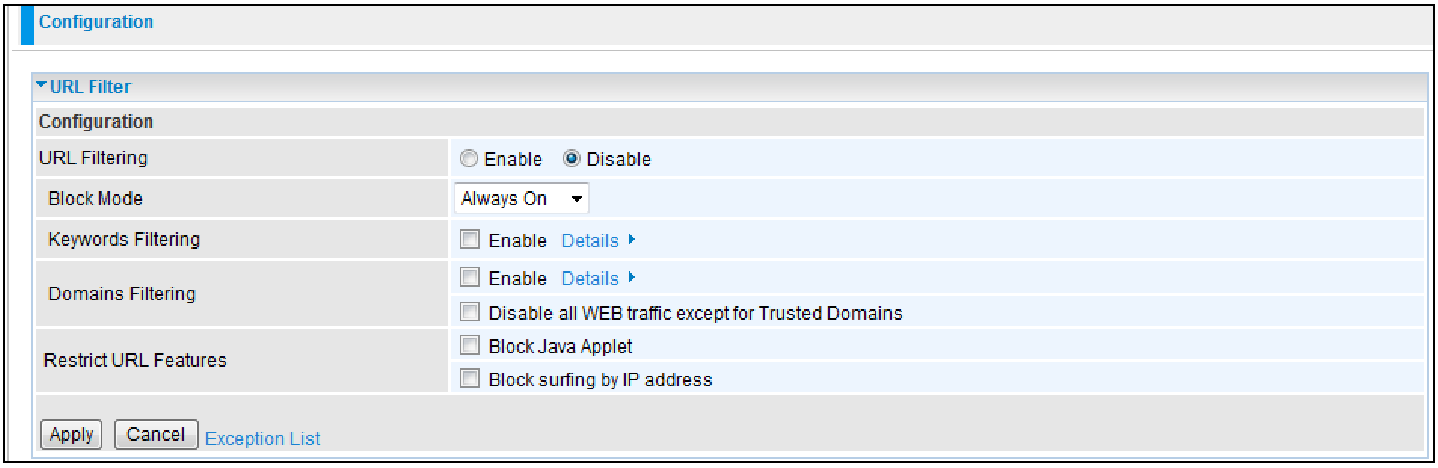
For SYN Flood, ICMP Echo Storm and ICMP flood, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

Table 2: Hacker attack types recognized by the IDS

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

URL Filter

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



Configuration

URL Filter

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

Apply Cancel Exception List

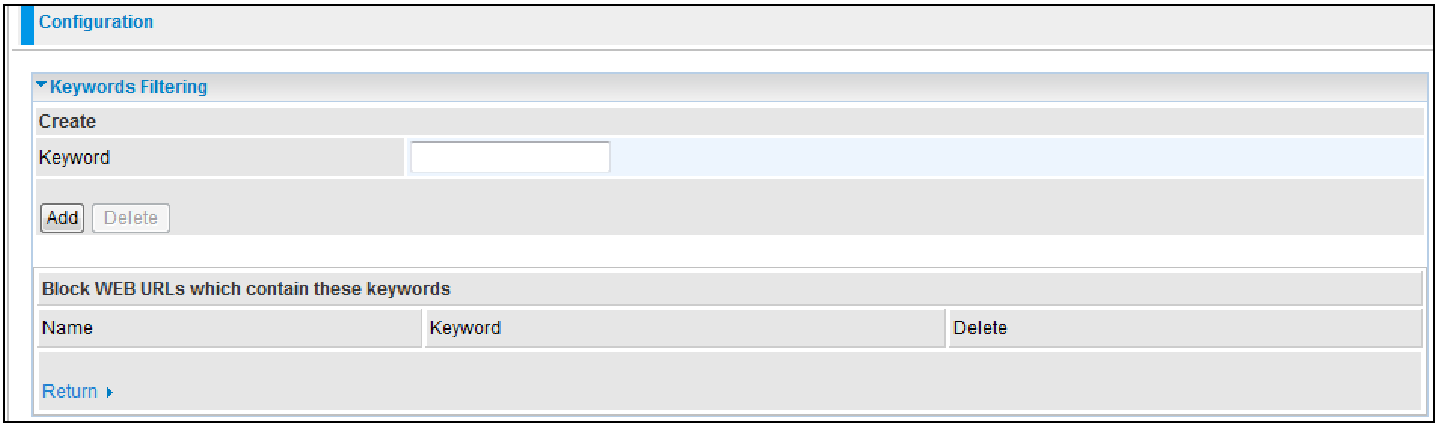
Enable/Disable: Select to enable or disable URL Filter feature.

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

> **Disabled:** No action will be performed by the Block Mode.
>
> **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.
>
> **TimeSlot1 ~ TimeSlot16:** It is a self defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

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

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



Configuration

Keywords Filtering

Create	
Keyword	

Add Delete

Block WEB URLs which contain these keywords

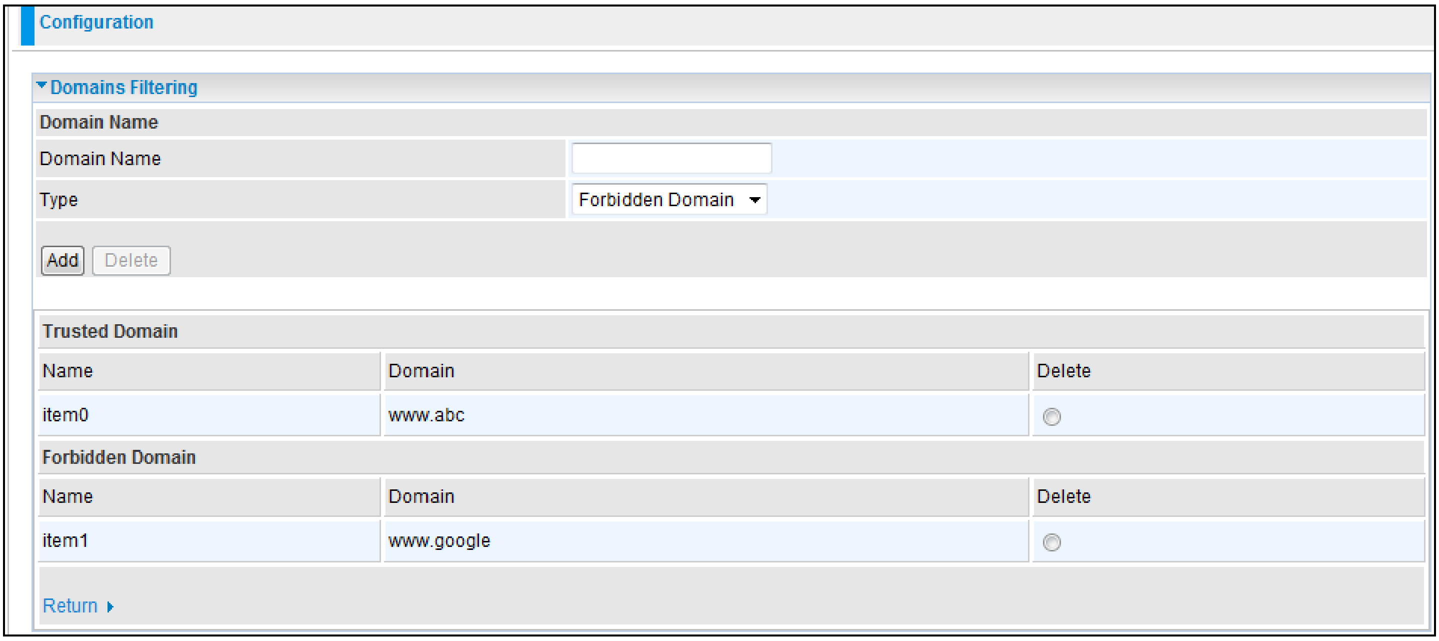
Name	Keyword	Delete

Return

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

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

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



Domain Name

Domain Name:

Type: Forbidden Domain

Trusted Domain

Name	Domain	Delete
item0	www.abc	○

Forbidden Domain

Name	Domain	Delete
item1	www.google	○

Example:

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

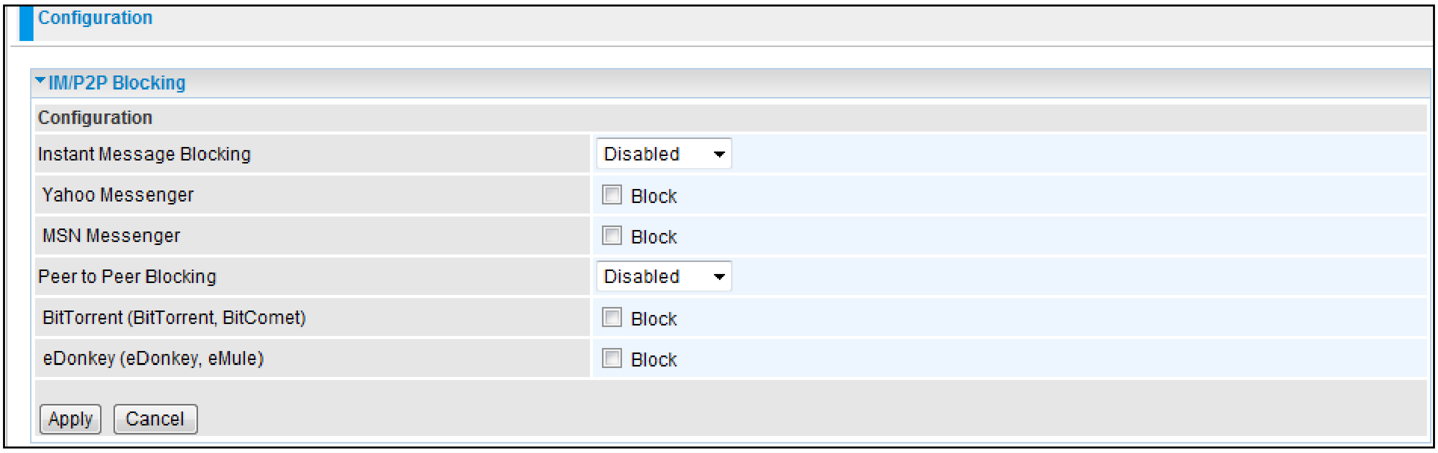
Restrict URL Features: This function enhances the restrictions to your URL rules.

Block Java Applet: This function can block Web content that includes Java Applets. It prevents someone from damaging your system via standard HTTP protocol.

Block surfing by IP address: A further restriction against someone who uses IP addresses as a URL to cheat the Domains Filtering rule. Only activates if Domain Filtering is enabled.

IM / P2P Blocking

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



Configuration

IM/P2P Blocking

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

Instant Message Blocking: The default is set to Disabled.

Disabled: Instant Message blocking is not enabled. No action will be taken.

Always On: Instant Message blocking is enabled. IM messages will be blocked.

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

Yahoo/MSN Messenger: Check the checkbox to block either Yahoo or/and MSN Messenger or both.
Be sure to enable the *Instant Message Blocking* first.

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

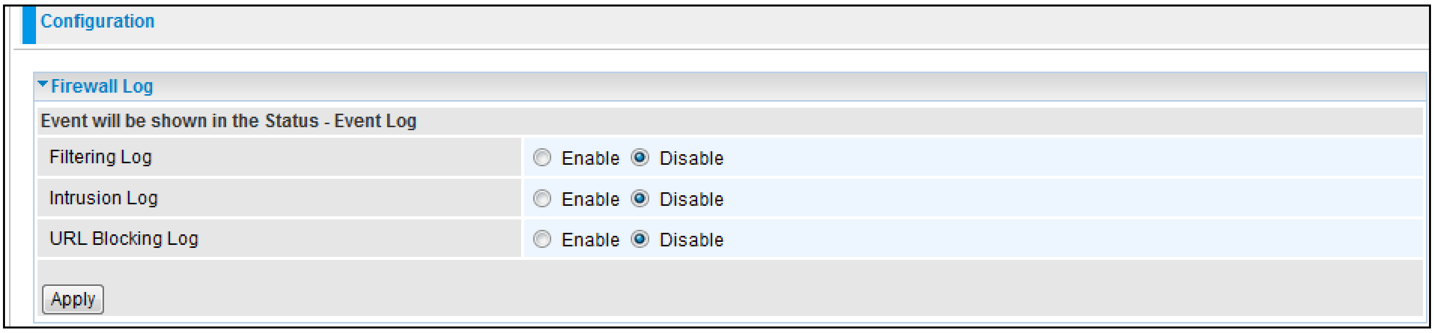
Disabled: Peer to Peer blocking is not enabled. No action will be taken.

Always On: Peer to Peer blocking is enabled. P2P will be blocked.

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

BitTorrent / eDonkey: Check the checkbox to block either Bit Torrent or eDonkey or both. Be sure to enable the *Peer to Peer Blocking* first.

Firewall Log



Configuration

▾Firewall Log

Event will be shown in the Status - Event Log

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

The Firewall Log contains information of any unexpected actions that occur to your firewall.

Check the Enable checkbox to activate event logging.

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

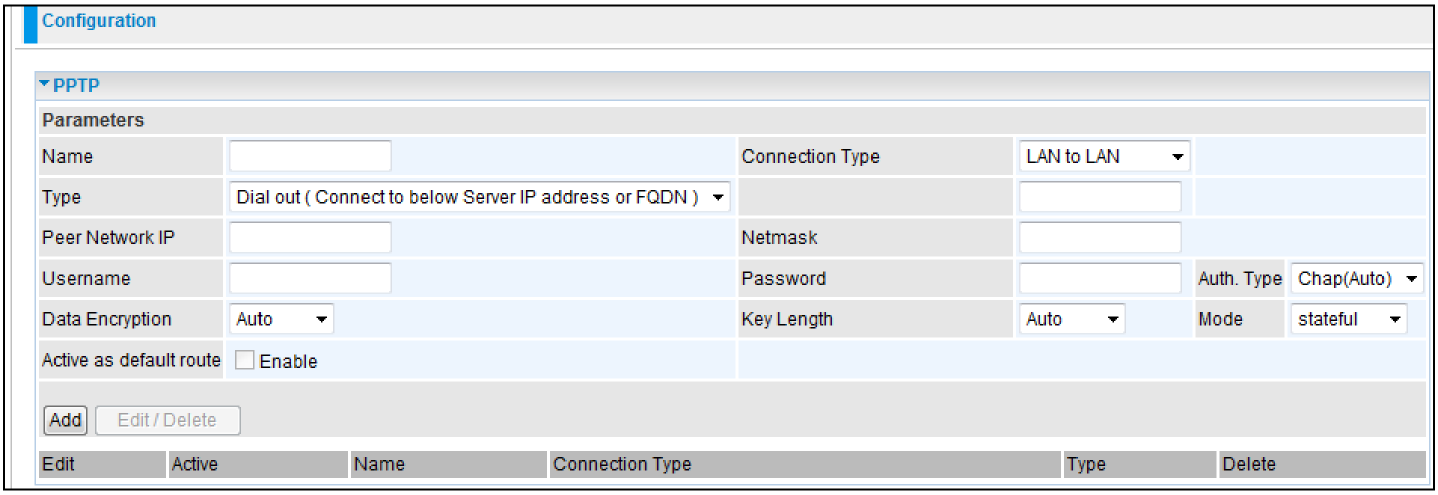
VPN - Virtual Private Networks

Virtual Private Networks is a way to establish a secured communication tunnel with an organization network via the Internet. Your router supports three main types of VPN (Virtual Private Network): **PPTP, IPSec and L2TP**.

PPTP (Point-to-Point Tunneling Protocol)

<u>PPTP Connection - LAN to LAN</u>

There are two types of PPTP VPN: Remote Access and LAN-to-LAN (please refer below for more information). Click Configuration > VPN > PPTP. Choose LAN to LAN from Connection Type drop down menu.



Configuration

▾PPTP

Parameters

Name		Connection Type	LAN to LAN		
Type	Dial out (Connect to below Server IP address or FQDN)				
Peer Network IP		Netmask			
Username		Password		Auth. Type	Chap(Auto)
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Active as default route	□ Enable				

Edit	Active	Name	Connection Type	Type	Delete

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

Connection Type: Remote Access or LAN to LAN.

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

> When configuring your router as a Client, enter the remote Server IP Address (or Domain Name) you wish to connect to.
>
> When configuring your router as a server, enter the Private IP Address assigned to the Dial in User.

IP Address: Enter the IP address.

Peer Network IP: Enter your peer’s network IP address.

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

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

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

Authentication Type: Default is Auto if you want the router to automatically determine the authentication type to use. If you know which authentication type the server is using (when acting as a client), you may manually specify the Authentication type whether CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). When acting as a server, you can set the authentication type you want the clients connecting to you to use. When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending it.

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

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

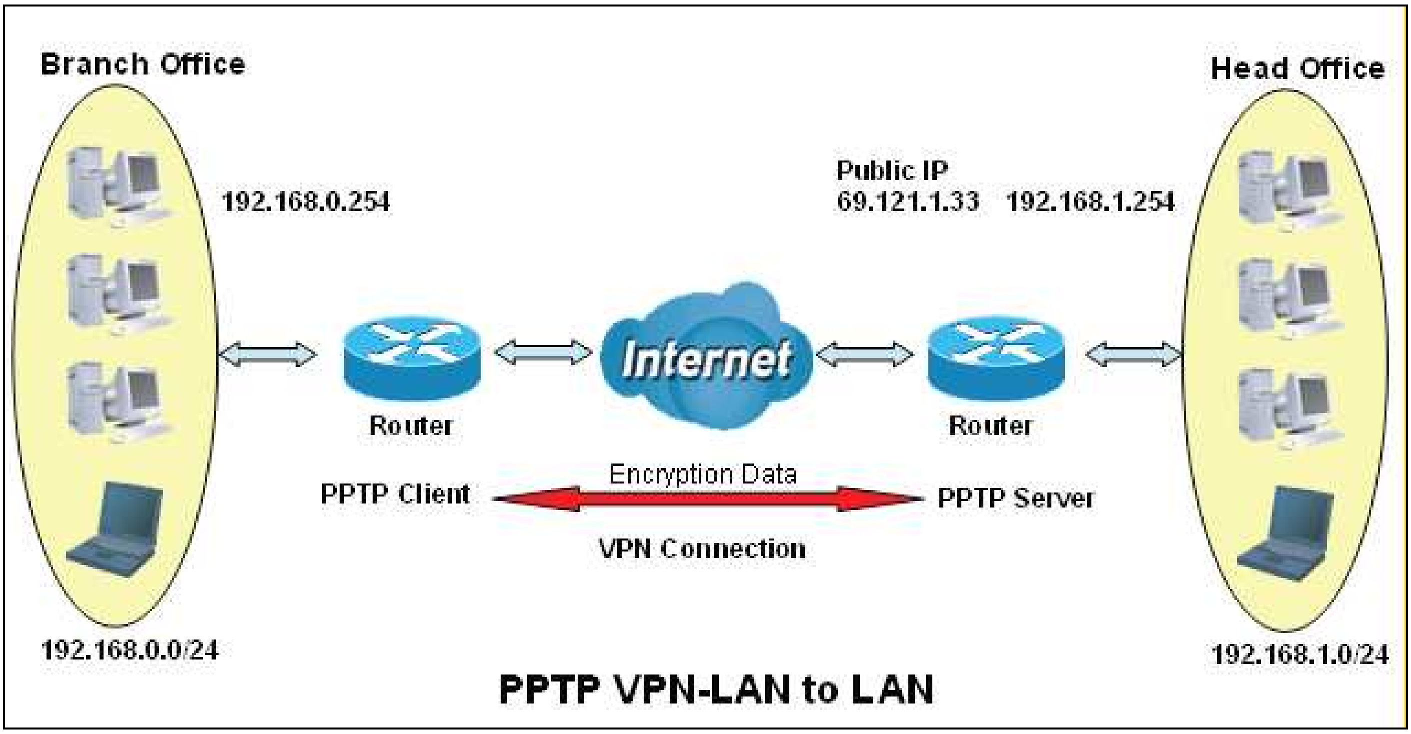
Mode: You may select Stateful or Stateless mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Active as default route: Commonly used by the Dial-out connection where all packets will route through the VPN tunnel to the Internet. Therefore activating this function may degrade the Internet performance.

Click Edit/Delete button to save your changes.

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

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

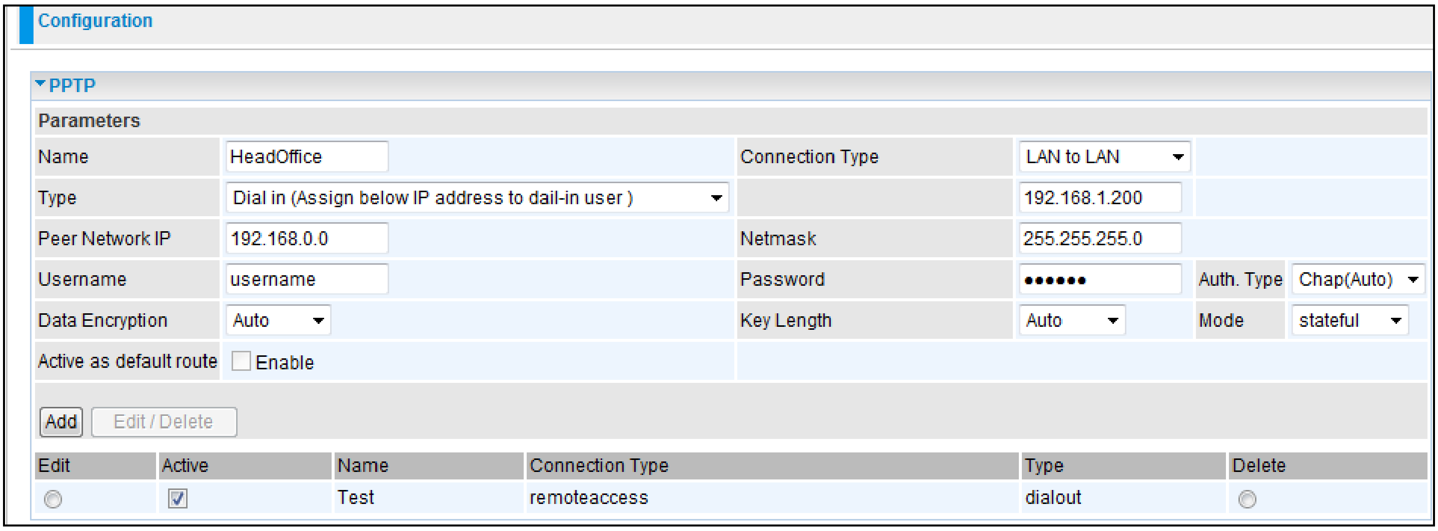


Attention

✓ **Both office LAN networks must be in different subnets with LAN-LAN application**

Configuring the PPTP VPN in the Head Office

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



Configuration

PPTP

Parameters

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

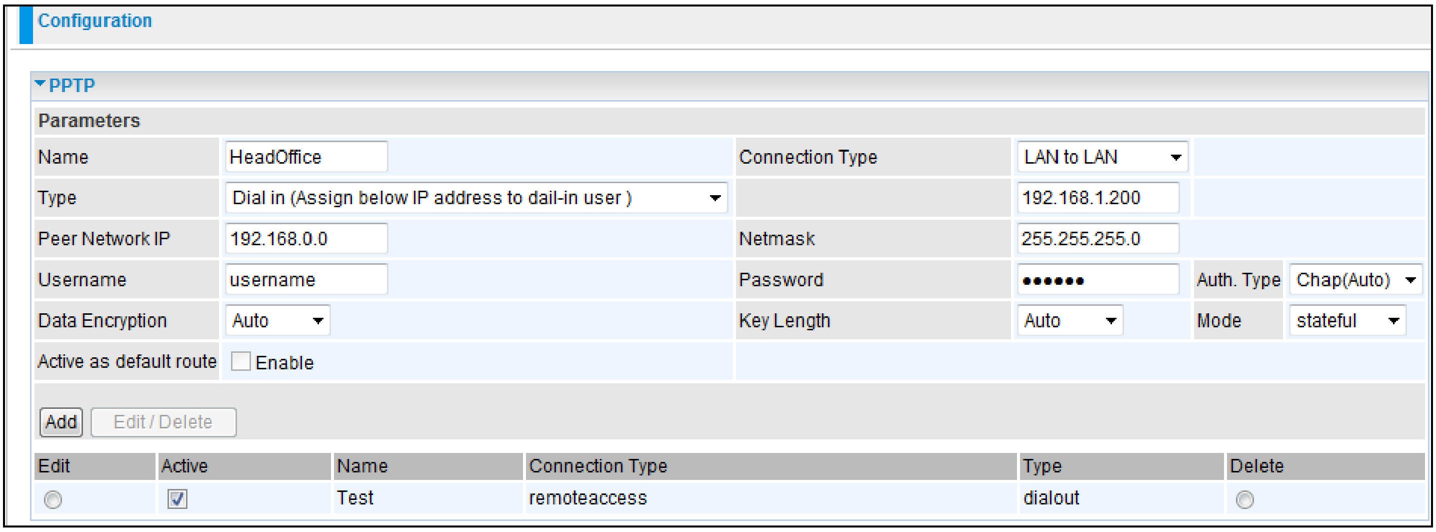
Add | Edit / Delete

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

Function		**Description**
Name	**Head Office**	Given name of PPTP connection
Connection type	**LAN to LAN**	Select LAN to LAN from the Connection Type drop-down menu
Type	**Dial in**	Select Dial in from the Type drop-down menu
IP Address	**192.168.1.200**	IP address assigned to branch office network
Peer Network IP	**192.168.0.0**	Branch office network
Netmask	**255.255.255.0**	
Username	**Username**	A given username & password to authenticate the branch office network.
Password	**123456**	
Auth. Type	**Chap(Auto)**	Keep as the default value in most cases, PPTP server & client will determine the value automatically. Refer to the manual for details if you want to change the settings.
Data Encryption	**Auto**	
Key Length	**Auto**	
Mode	**Stateful**	

Configuring the PPTP VPN in the Head Office

The IP address 69.1.121.30 is the Public IP address of the router located in head office. If you registered the DDNS (please refer to the DDNS section of this manual), you can also use the domain name instead of the IP address to reach the router.



Configuration

PPTP

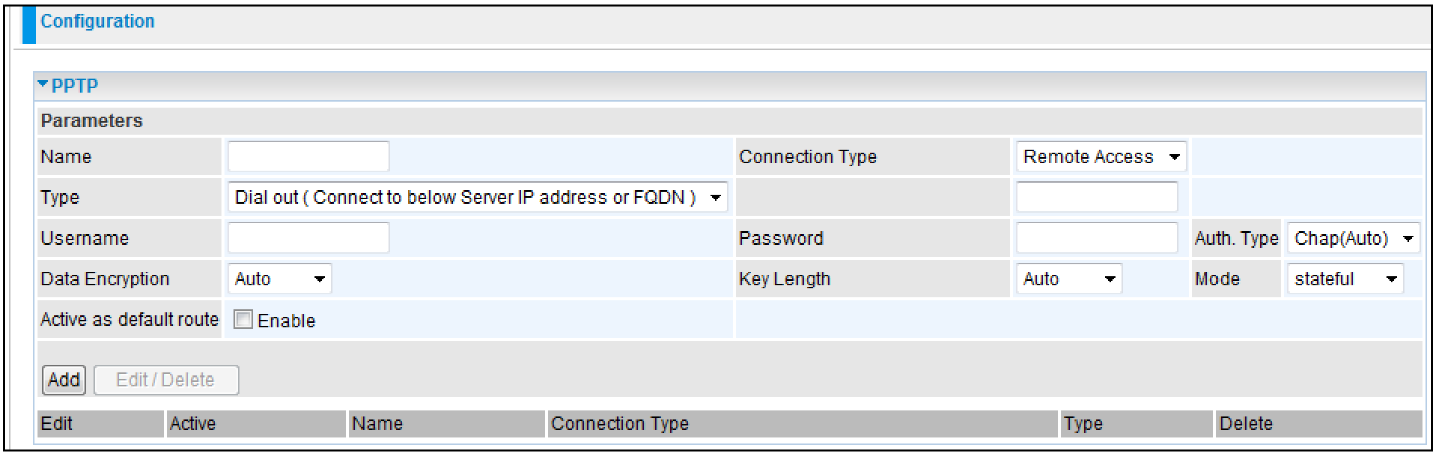
Parameters

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

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

Function		Description
Name	**Head Office**	Given name of PPTP connection
Connection type	**LAN to LAN**	Select LAN to LAN from the Connection Type drop-down menu
Type	**Dial in**	Select Dial in from the Type drop-down menu
IP Address	**69.121.1.33**	IP address assigned to branch office network
Peer Network IP	**192.168.1.0**	Head office network
Netmask	**255.255.255.0**	
Username	**Username**	A given username & password to authenticate branch office network.
Password	**123456**	
Auth. Type	**Chap(Auto)**	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
Data Encryption	**Auto**	
Key Length	**Auto**	
Mode	**Stateful**	

PPTP Connection - Remote Access



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

Edit	Active	Name	Connection Type	Type	Delete

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

Connection Type: Remote Access or LAN to LAN.

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

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

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

IP Address: Enter the IP address.

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

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

Authentication Type: Default is Auto if you want the router to automatically determine the authentication type to use. If you know which authentication type the server is using (when acting as a client), you may manually specify the Authentication type whether CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). When acting as a server, you can set the authentication type you want the clients connecting to you to use. When using PAP, the password is sent unencrypted, while CHAP encrypts the password before sending it.

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

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

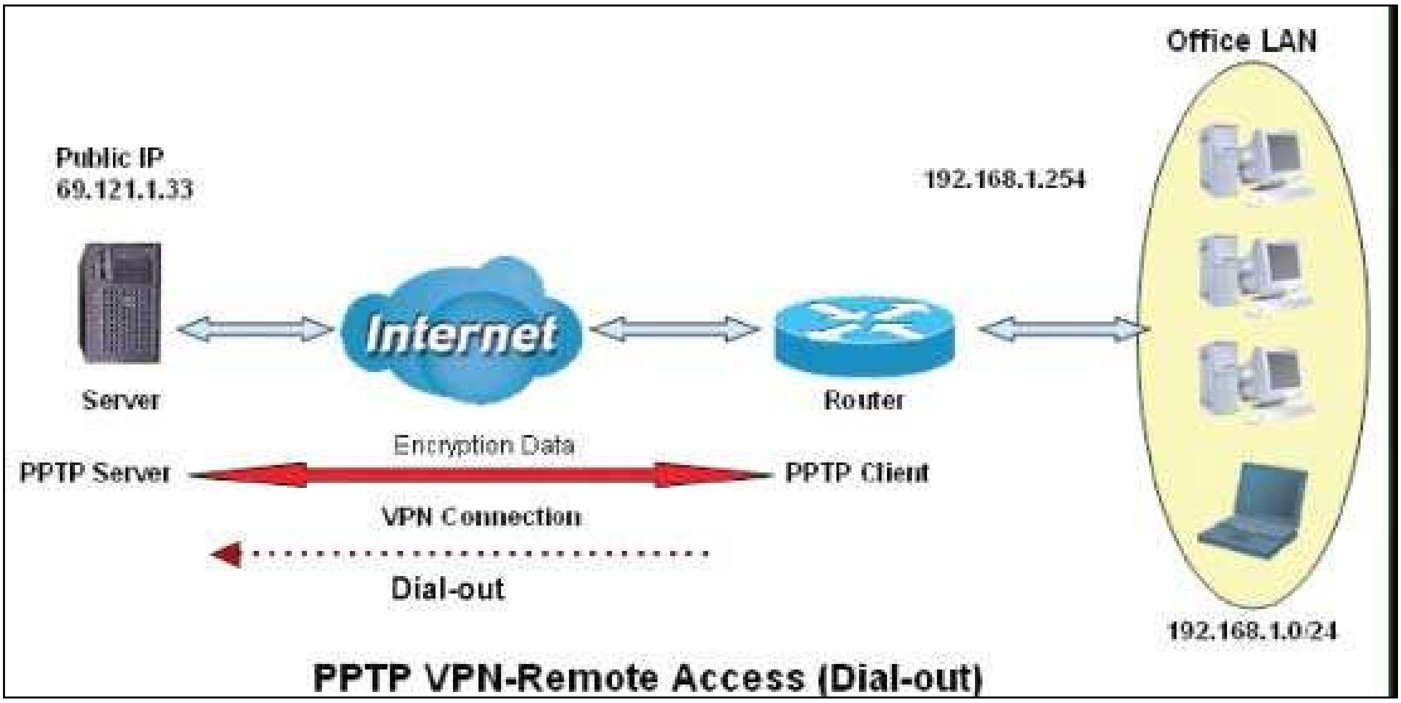
Mode: You may select Stateful or Stateless mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Active as default route: Commonly used by the Dial-out connection where all packets will route through the VPN tunnel to the Internet. Therefore activating this function may degrade the Internet performance.

Click Edit/Delete button to save your changes.

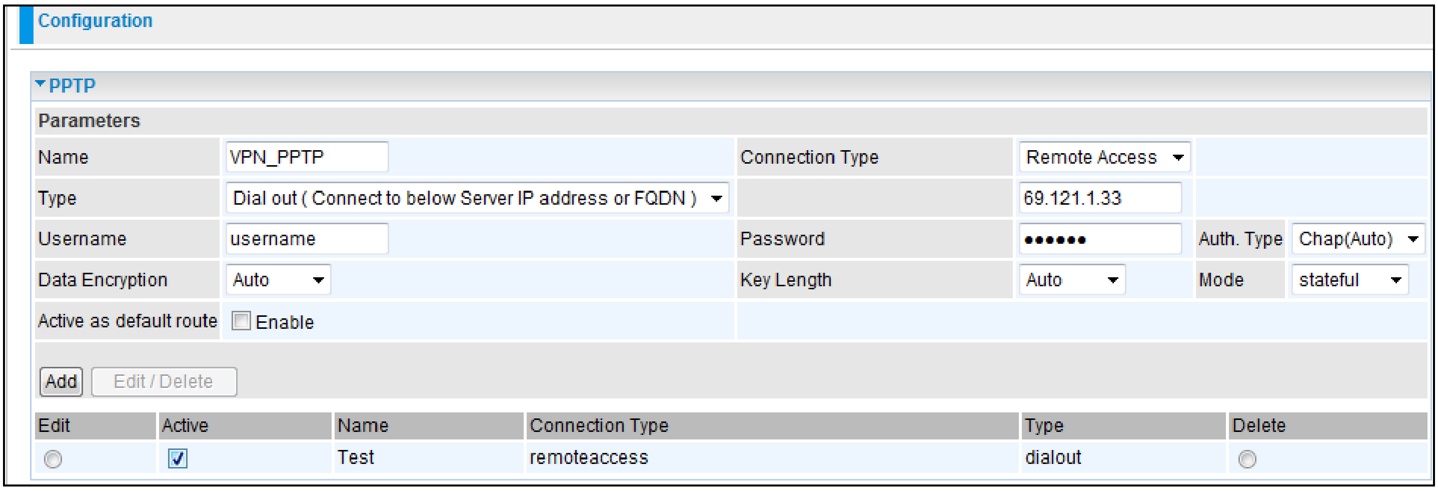
Example: Configuring a Remote Access PPTP VPN Dial-out Connection

An office establishes a PPTP VPN connection with a file server located at a different location. The router is installed in the office, connected to a couple of PCs and Servers.



Configuring the PPTP VPN in the Office

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



Configuration

▾ PPTP

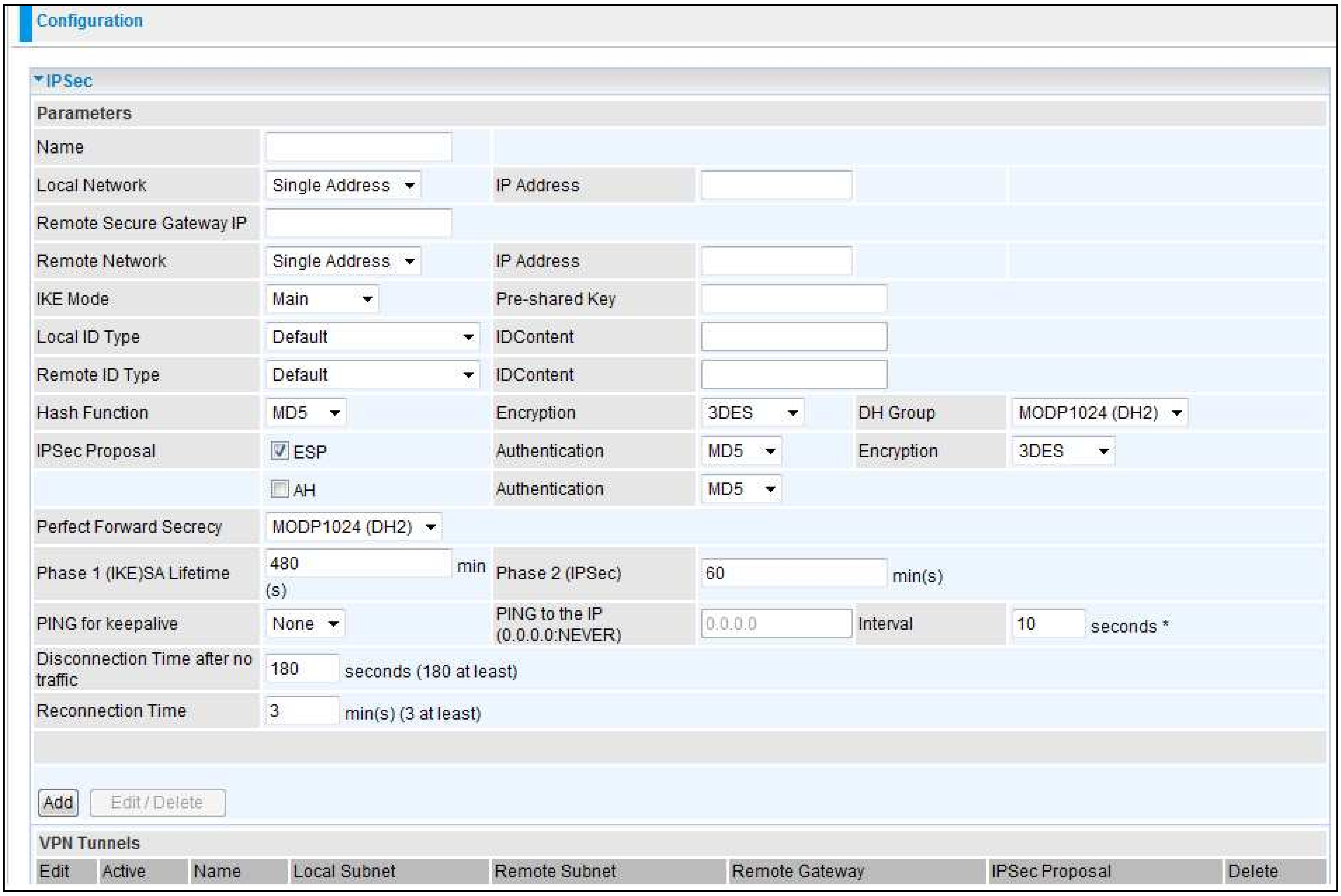
Parameters

Name	VPN_PPTP	Connection Type	Remote Access ▾		
Type	Dial out (Connect to below Server IP address or FQDN) ▾		69.121.1.33		
Username	username	Password	••••••	Auth. Type	Chap(Auto) ▾
Data Encryption	Auto ▾	Key Length	Auto ▾	Mode	stateful ▾
Active as default route	□ Enable				

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

Function		Description
Name	**VPN PPTP**	Given name of PPTP connection
Connection type	**Remote Access**	Select Remote Access from the Connection Type drop-down menu
Type	**Dial out**	Select Dial out from the Type drop-down menu
IP Address (or Domain name)	**69.121.1.33**	A Dialed server IP
Username	**Username**	A given username & password to authenticate branch office network.
Password	**123456**	
Auth. Type	**Chap(Auto)**	Keep as default value in most cases, PPTP server & client will determine the value automatically. Refer to the manual for details if you want to change the settings.
Data Encryption	**Auto**	
Key Length	**Auto**	
Mode	**Stateful**	

IPSec (IP Security Protocol)



Configuration

▾IPSec

Parameters

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

Add | Edit / Delete

VPN Tunnels

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

IPSec VPN Connection

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

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

Single Address: The IP address of the local host.

Subnet: The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 10.0.0.2).

IP Range: The IP address range of the local network. For Example, IP: 192.168.1.1, end IP: 192.168.1.10.

IP Address: Enter the IP address.

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.

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 ww.ipsectest.com

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

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

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

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

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, you can use 128, 192 or 256 bits as an 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 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, you can use 128, 192 or 256 bits as encryption method.

Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function of a cryptography protocol is to allow 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.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication keys 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'. In this mode, it will not detect if the remote IPSec peer has been lost or not. It 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 if the remote IPSec peer has been lost or not by pinging the specified IP address.

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

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

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

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

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

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

Click Edit/Delete to save your changes.

Example: Configuring an IPSec LAN to LAN VPN Connection

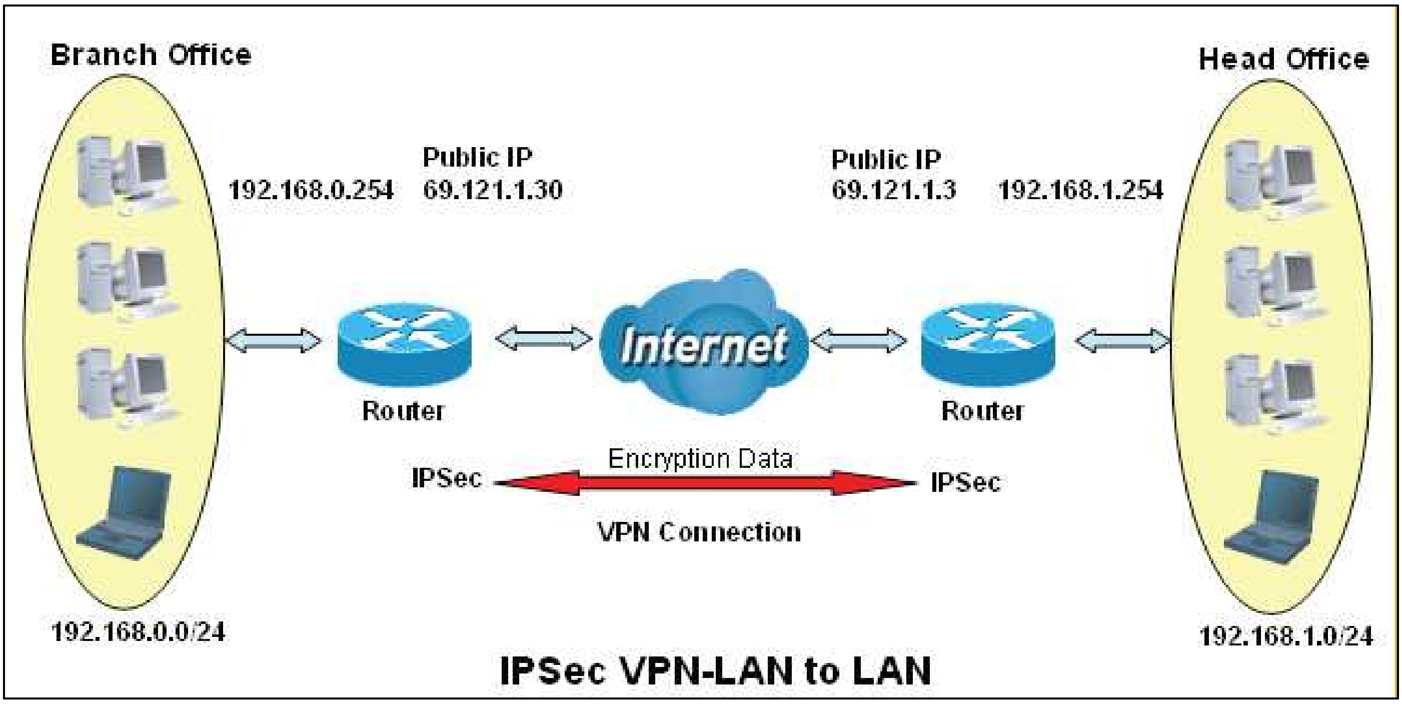


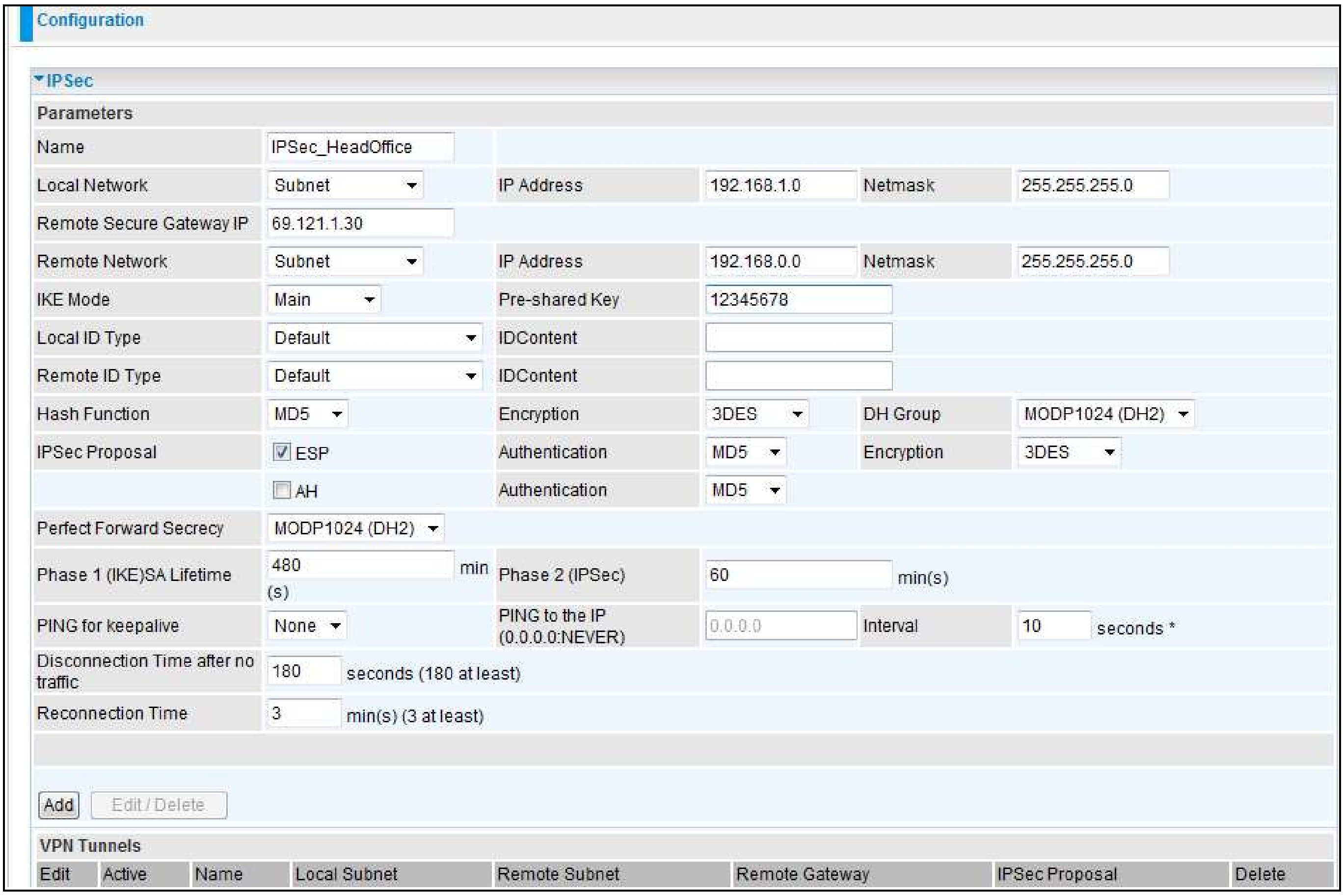
Table 3: Network Configuration and Security Plan

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

Attention

- ✓**Both office Networks MUST be in different subnets with the LAN-LAN application.**
- ✓**Functions of Pre –shared keys, VPN Connection Type and Security Algorithms must be identical on both sides.**

Configuring IPSec VPN in the Head Office



Configuration

IPSec

Parameters

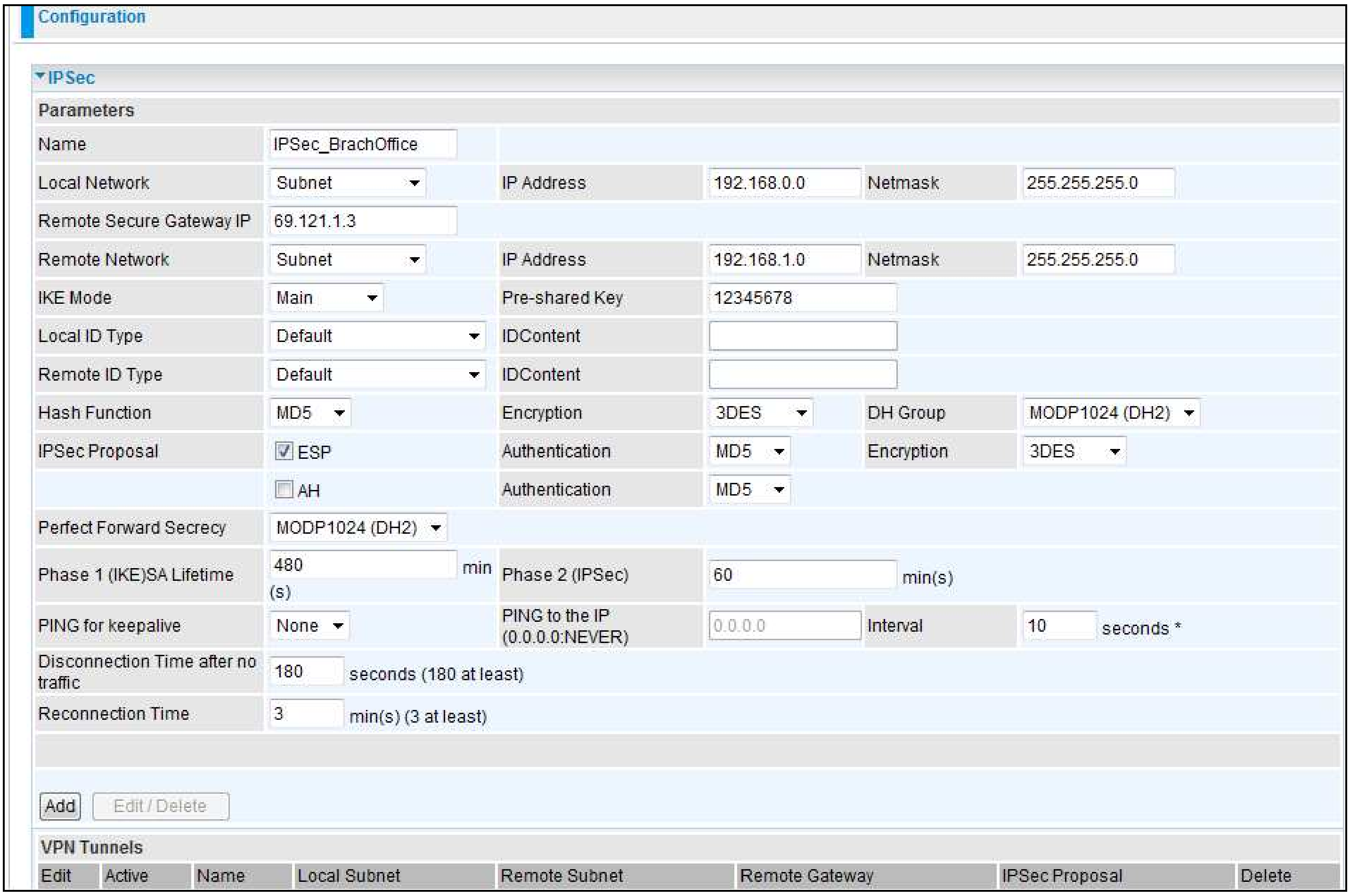
Name	IPSec_HeadOffice				
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Secure Gateway IP	69.121.1.30				
Remote Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
IKE Mode	Main	Pre-shared Key	12345678		
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	☐ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min (s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

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

Function		**Description**
Name	**IPSec_HeadOffice**	A given name for the IPSec Connection.
Local Area	**Subnet**	Select Subnet from the Local Network drop-down menu.
IP Address	**192.168.1.0**	Head office network.
Netmask	**255.255.255.0**	
Remote Secure Gateway IP (or Hostname)	**69.121.1.30**	A given username & password to authenticate branch office network.
Remote Network	**Subnet**	Select Subnet from the Remote Network drop- down menu.
IP Address	**192.168.1.0**	Branch office network.
Netmask	**255.255.255.0**	
Pre-shared Key	**12345678**	Security plan
Authentication	**MD5**	
Encryption	**3DES**	
Prefer Forward Security	**None**	

Configuring IPSec VPN in the Branch Office



Configuration

IPSec

Parameters

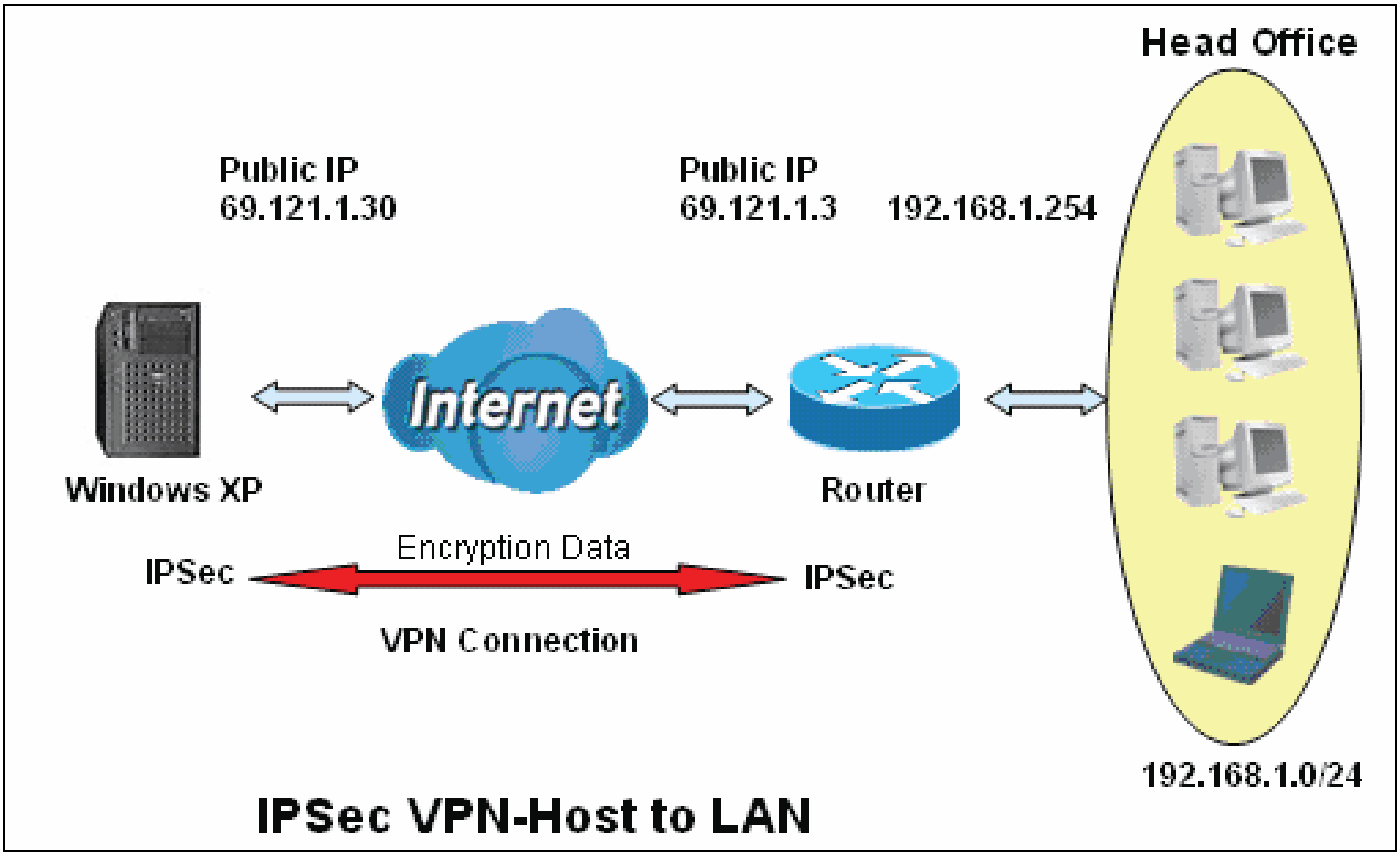
Name	IPSec_BrachOffice				
Local Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Remote Secure Gateway IP	69.121.1.3				
Remote Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
IKE Mode	Main	Pre-shared Key	12345678		
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	□ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min (s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

VPN Tunnels

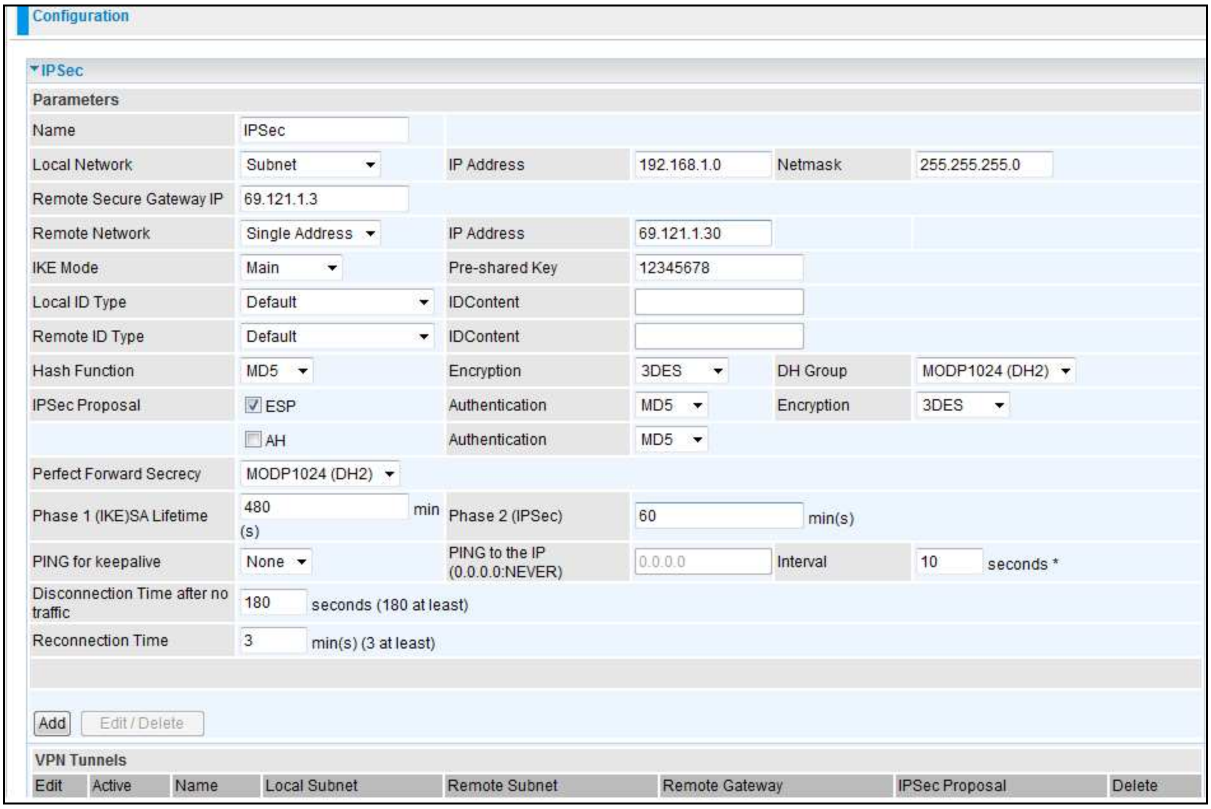
Edit	Active	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal	Delete

Function		Description
Name	**IPSec_HeadOffice**	A given name for the IPSec Connection.
Local Area	**Subnet**	Select Subnet from the Local Network drop-down menu.
IP Address	**192.168.0.0**	Branch office network.
Netmask	**255.255.255.0**	
Remote Secure Gateway IP (or Hostname)	**69.121.1.3**	IP address of the head office router (in WAN side
Remote Network	**Subnet**	Select Subnet from the Remote Network drop- down menu.
IP Address	**192.168.1.0**	Head office network.
Netmask	**255.255.255.0**	
Pre-shared Key	**12345678**	Security plan
Authentication	**MD5**	
Encryption	**3DES**	
Prefer Forward Security	**None**	

Example: Configuring an IPSec Host to LAN VPN Connection



Configuring IPSec VPN in the Office



Parameters

Name	IPSec				
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Secure Gateway IP	69.121.1.3				
Remote Network	Single Address	IP Address	69.121.1.30		
IKE Mode	Main	Pre-shared Key	12345678		
Local ID Type	Default	IDContent			
Remote ID Type	Default	IDContent			
Hash Function	MD5	Encryption	3DES	DH Group	MODP1024 (DH2)
IPSec Proposal	☑ ESP	Authentication	MD5	Encryption	3DES
	☐ AH	Authentication	MD5		
Perfect Forward Secrecy	MODP1024 (DH2)				
Phase 1 (IKE)SA Lifetime	480 min (s)	Phase 2 (IPSec)	60 min(s)		
PING for keepalive	None	PING to the IP (0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds *
Disconnection Time after no traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

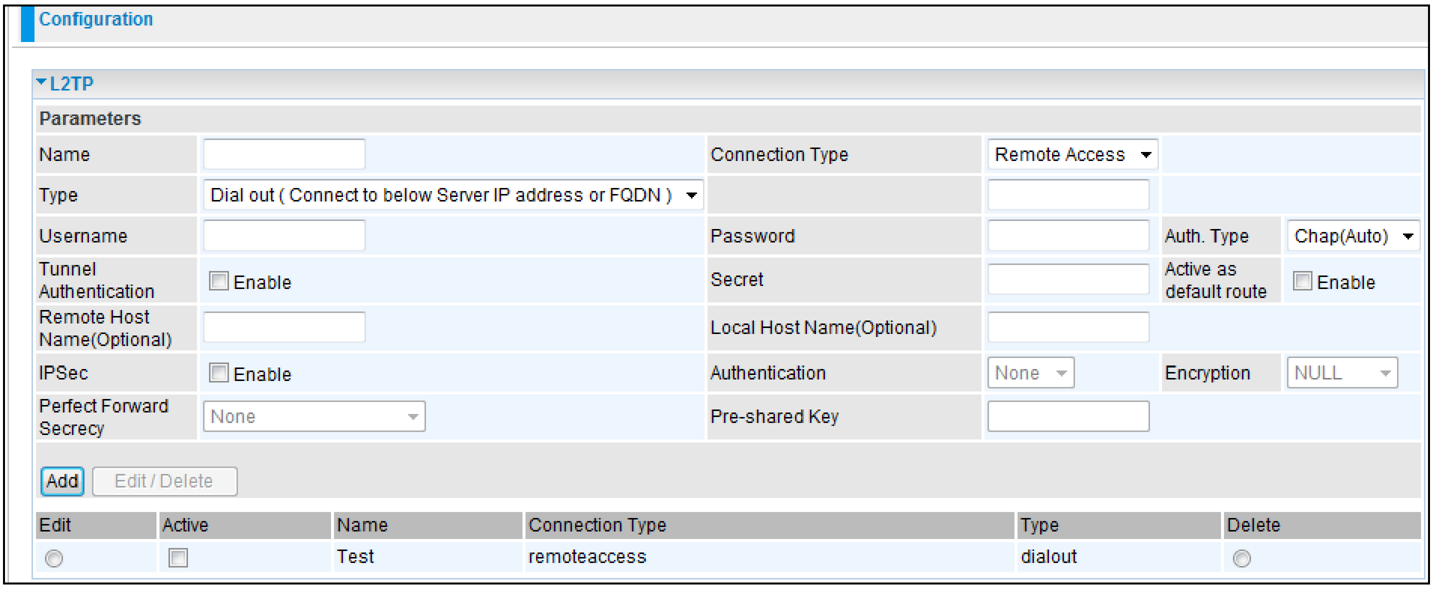
VPN Tunnels

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

Function		Description
Name	**IPSec**	A given name for the IPSec Connection.
Local Area	**Subnet**	Select Subnet from the Local Network drop-down menu.
IP Address	**192.168.1.0**	Branch office network.
Netmask	**255.255.255.0**	
Remote Secure Gateway IP (or Hostname)	**69.121.1.30**	IP address of the head office router (in WAN side
Remote Network	**Subnet**	Select Subnet from the Remote Network drop- down menu.
IP Address	**69.121.1.30**	Head office network.
Pre-shared Key	**12345678**	Security plan
Authentication	**MD5**	
Encryption	**3DES**	
Prefer Forward Security	**None**	

L2TP (Layer Two Tunneling Protocol)

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



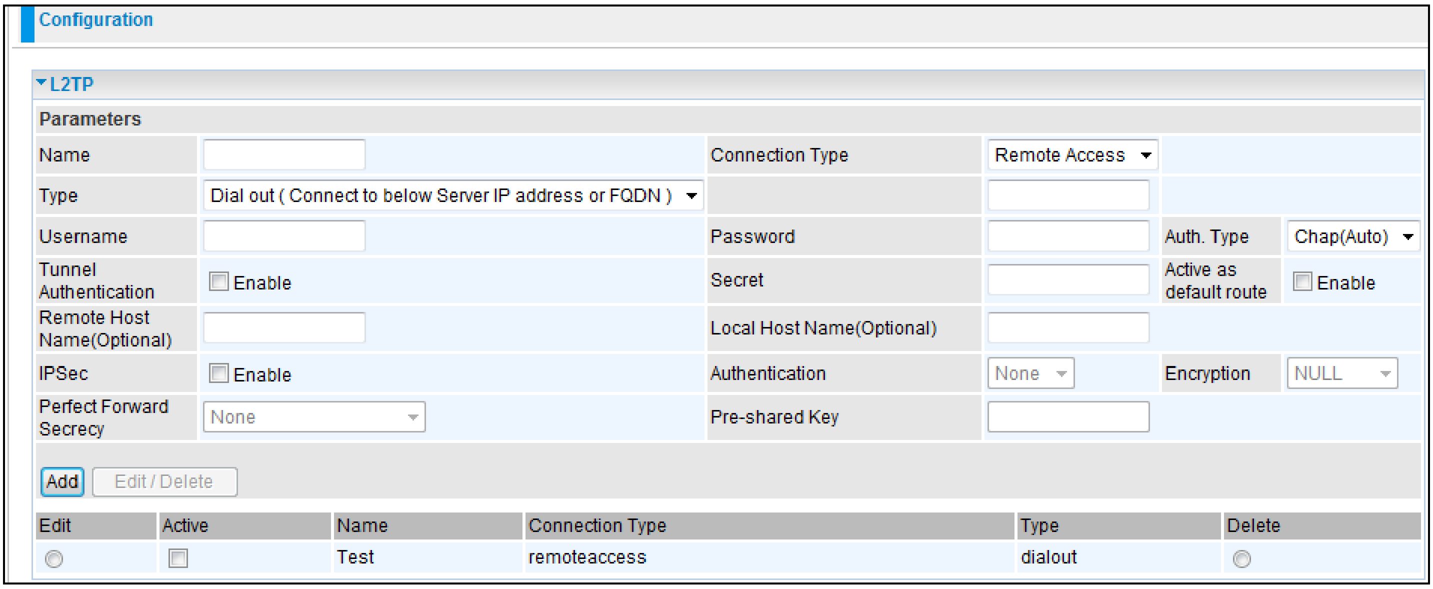
Parameters

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

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

L2TP Connection-Remote Access

Connection Type: Remote Access or LAN to LAN


Configuration
L2TP

Parameters

Name		Connection Type	Remote Access ▾		
Type	Dial out (Connect to below Server IP address or FQDN) ▾				
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
○	□	Test	remoteaccess	dialout	○

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

Connection Type: Remote Access or LAN to LAN.

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

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

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

IP Address: Enter the IP address.

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

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

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

Tunnel Authentication: This enables the 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, all packets will route through the VPN tunnel to the Internet; therefore, activating the function may degrade Internet performance.

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

Caution: This only applies when the router is acting as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter the hostname of a Local VPN device that is connected / established a VPN tunnel. By default, the router's default Hostname is **home.gateway**.

IPSec: Enable to enhance your L2TP VPN security.

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

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

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

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

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

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

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

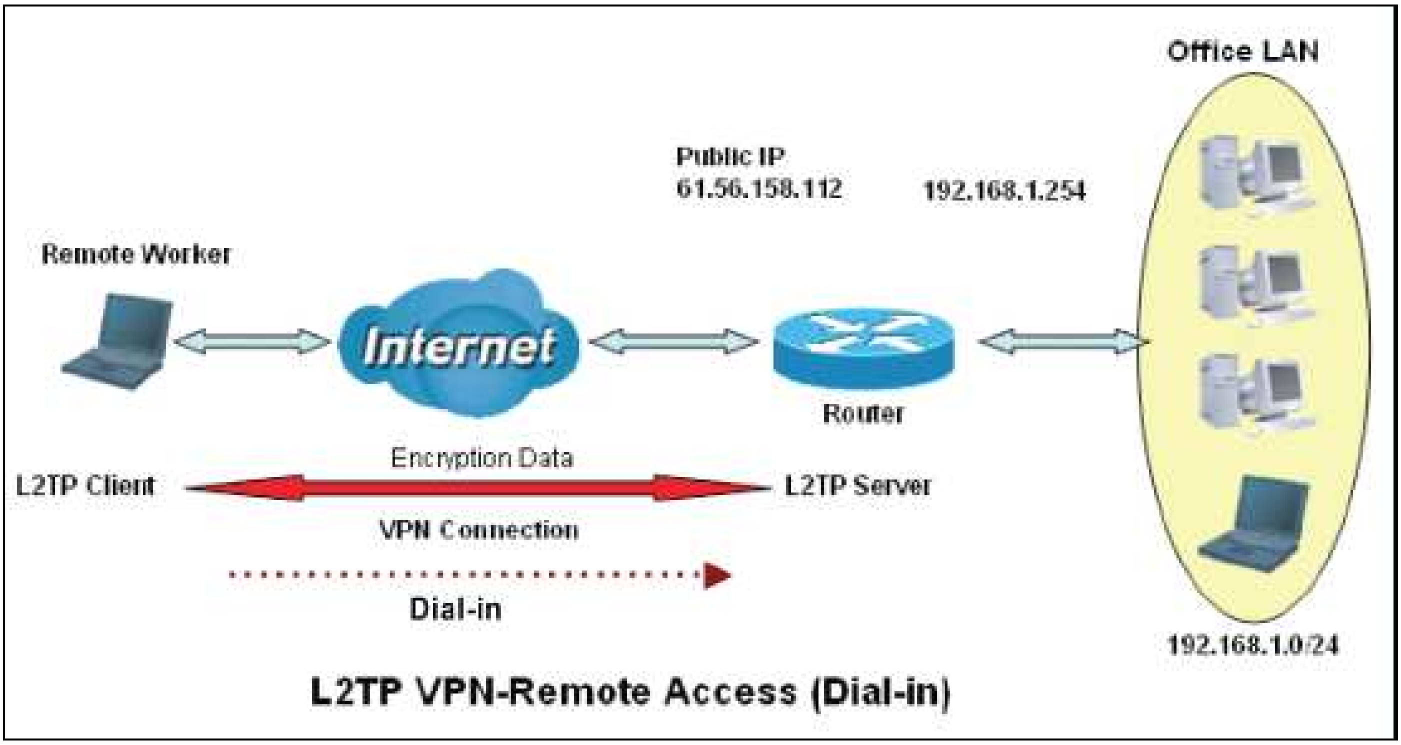
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol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

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

Click Edit/Delete to save your changes.

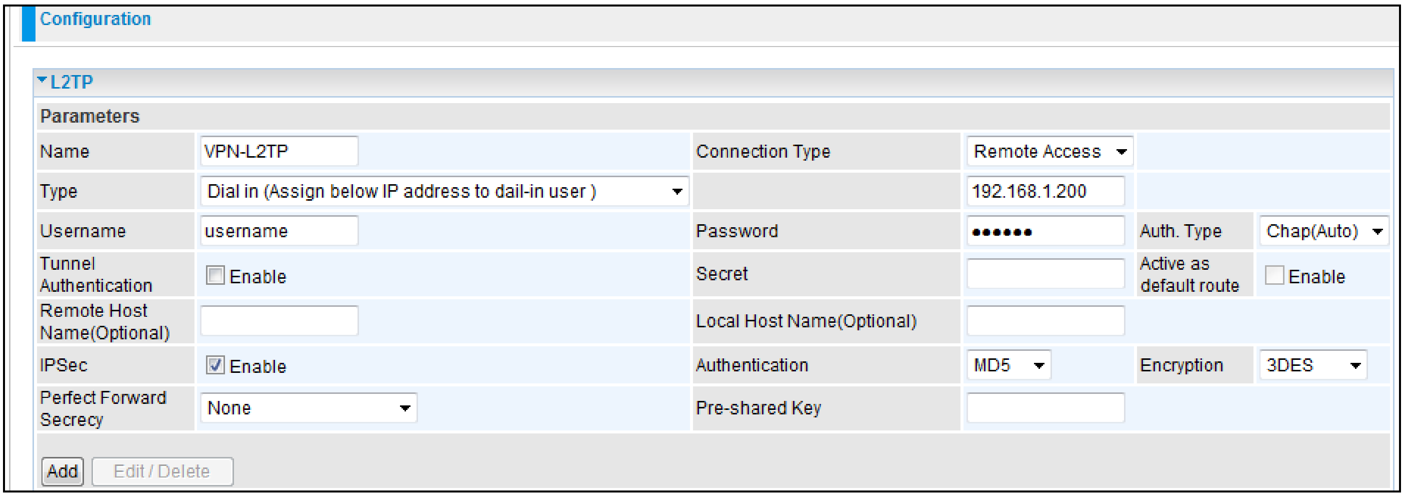
Example: Configuring a L2TP VPN - Remote Access Dial-in Connection

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



Configuring L2TP VPN in the Office

The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN. Pre-Shared Key 12345678



Configuration

L2TP

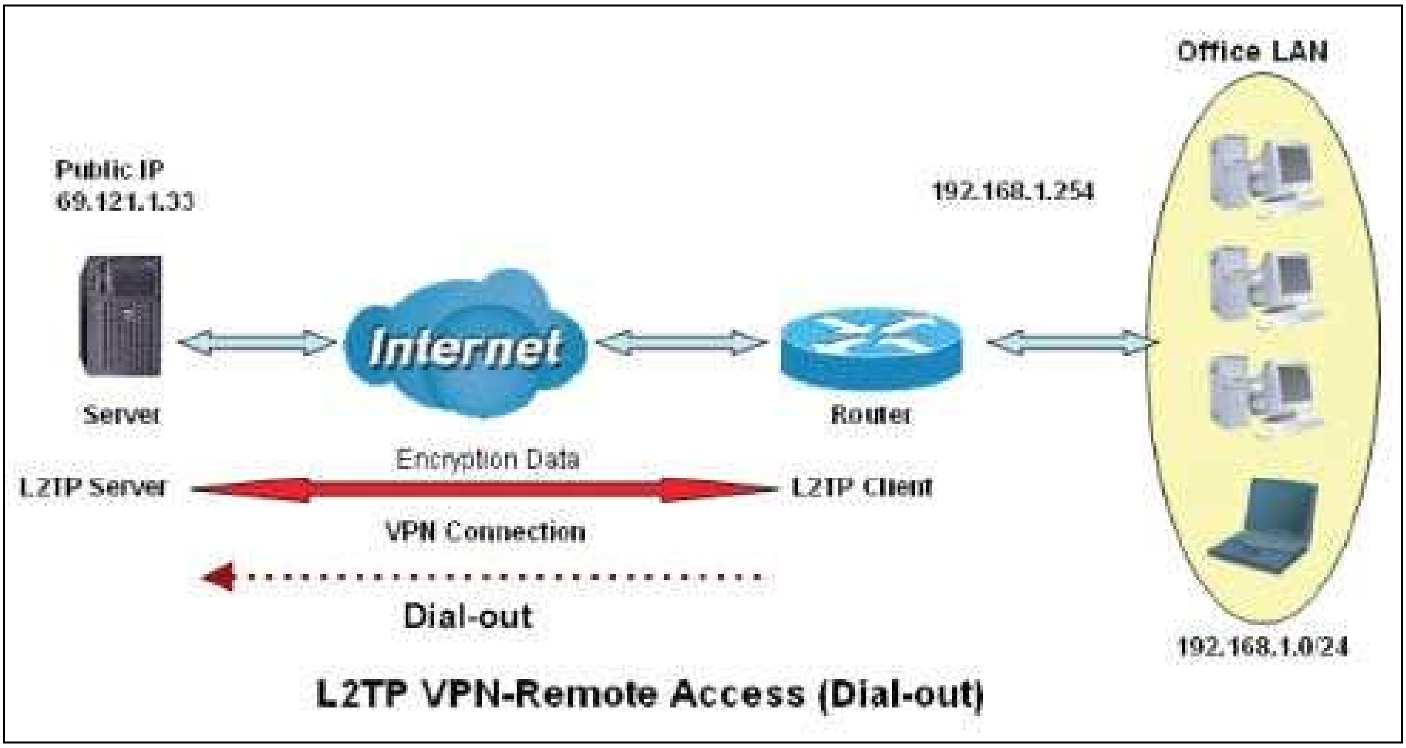
Parameters

Name	VPN-L2TP	Connection Type	Remote Access		
Type	Dial in (Assign below IP address to dail-in user)		192.168.1.200		
Username	username	Password	••••••	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name(Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key			

Function		Description
Name	VPN_L2TP	Give a name to the L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	An IP assigned to the remote client
Username	username	Enter the username and password to authenticate a remote client
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value in most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides should use the same value
Encryption	3DES	
Prefer Forward Security	None	
Pre-Shared Key	12345678	

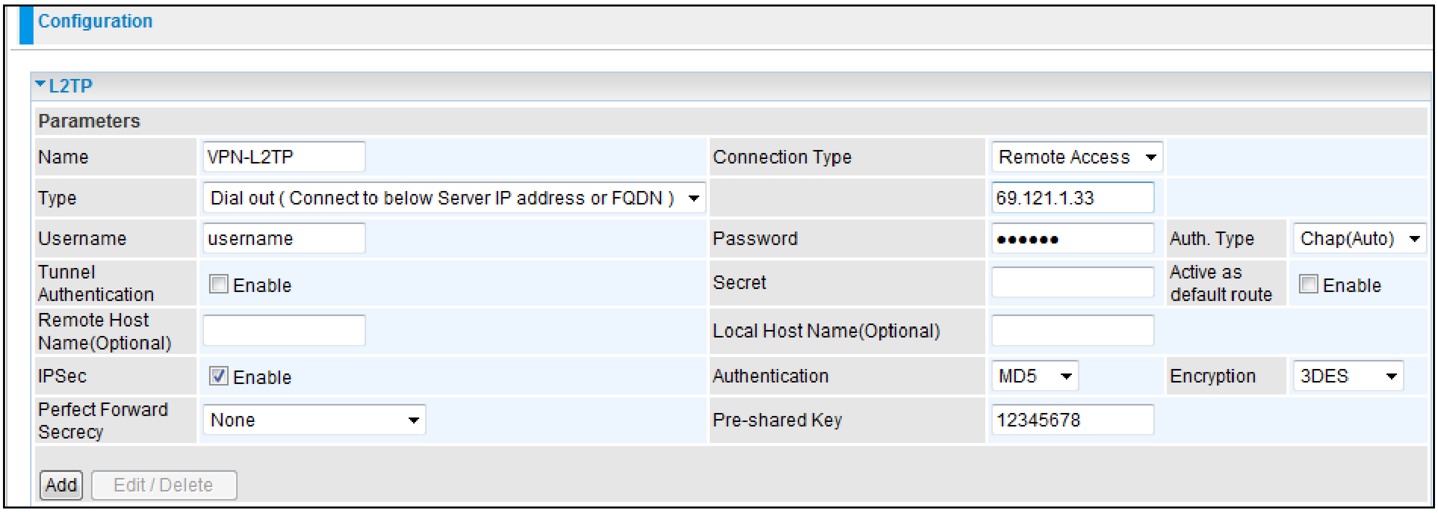
Example: Configuring a Remote Access L2TP VPN Dial-out Connection

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



Configuring L2TP VPN in the Office

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


Configuration

▾L2TP

Parameters

Name	VPN-L2TP	Connection Type	Remote Access		
Type	Dial out (Connect to below Server IP address or FQDN)		69.121.1.33		
Username	username	Password	••••••	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name(Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

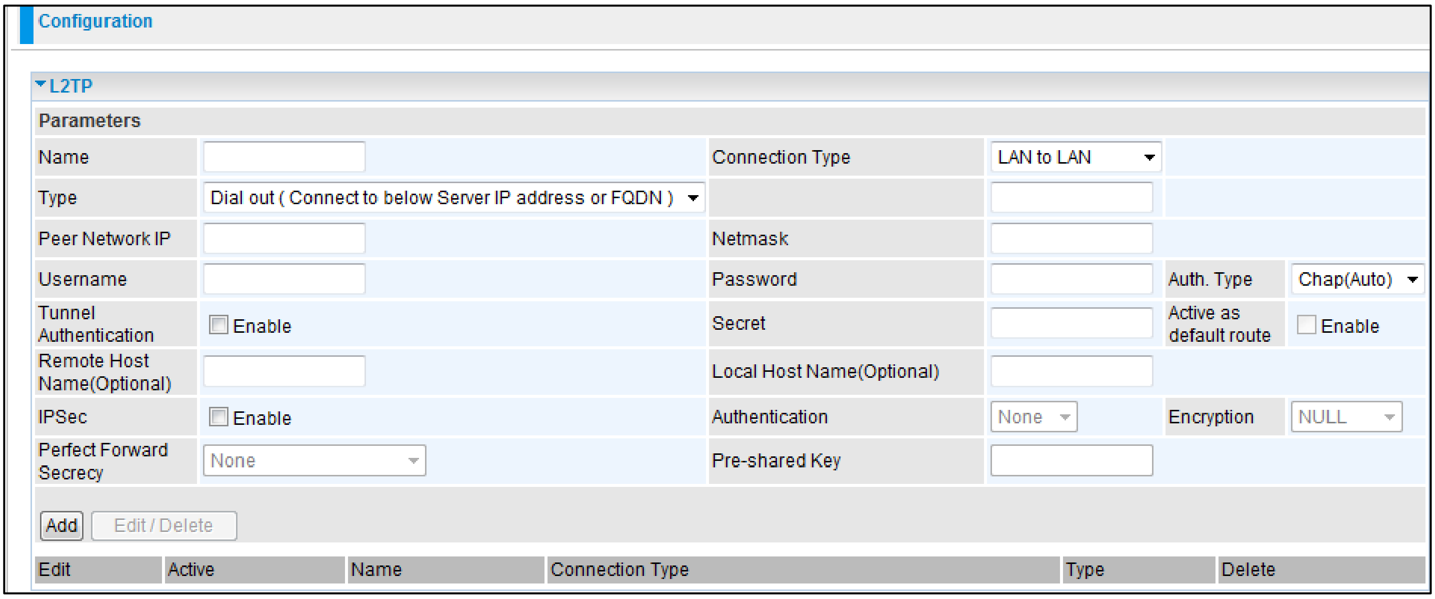
Function		Description
Name	**VPN_L2TP**	Give a name of L2TP Connection
Connection Type	**Remote Access**	Select Remote Access from the Connection Type drop-down menu
Type	**Dial Out**	Select Dial out from the Type drop down menu
IP Address (or Hostname)	**69.121.1.33**	A Dialed Server IP
Username	**username**	An assigned username and password
Password	**123456**	
Auth. Type	**Chap (Auto)**	Keep this as the default value for most cases
IPSec	**Enable**	Enable this to enhance your L2TP VPN security
Authentication	**MD5**	Both sides should use the same value
Encryption	**3DES**	
Prefer Forward Security	**None**	
Pre-Shared Key	**12345678**	

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

Currently, Microsoft Windows operating systems do not support L2TP incoming services. Additional software may be required to set up your L2TP incoming service.

L2TP Connection - LAN to LAN

L2TP VPN Connection



Configuration

L2TP

Parameters

Name		Connection Type	LAN to LAN		
Type	Dial out (Connect to below Server IP address or FQDN)				
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

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 to you 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 to you by your Host. If you are a Dial-In user (server), enter your own password.

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

Tunnel Authentication: This enables the router to authenticate both the L2TP remote and L2TP host systems. This is only valid when L2TP the remote system 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. All packets will route through the VPN tunnel to the Internet; therefore, activating the function may degrade Internet performance.

Remote Host Name (Optional Enter the hostname of the remote VPN device. It is a tunnel identifier to check if the Remote VPN device matches with the Remote hostname provided. If the remote hostnames match, the tunnel will be connected; otherwise, it will be dropped.

Caution: This only applies when the router is acting as a VPN server. This option should be used by advanced users only.

Local Host Name (Optional): Enter hostname of Local VPN device that is connected / established a VPN tunnel. By default, the router's default hostname is **home.gateway**.

IPSec: Enable to enhance your L2TP VPN security.

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

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

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

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

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

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

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

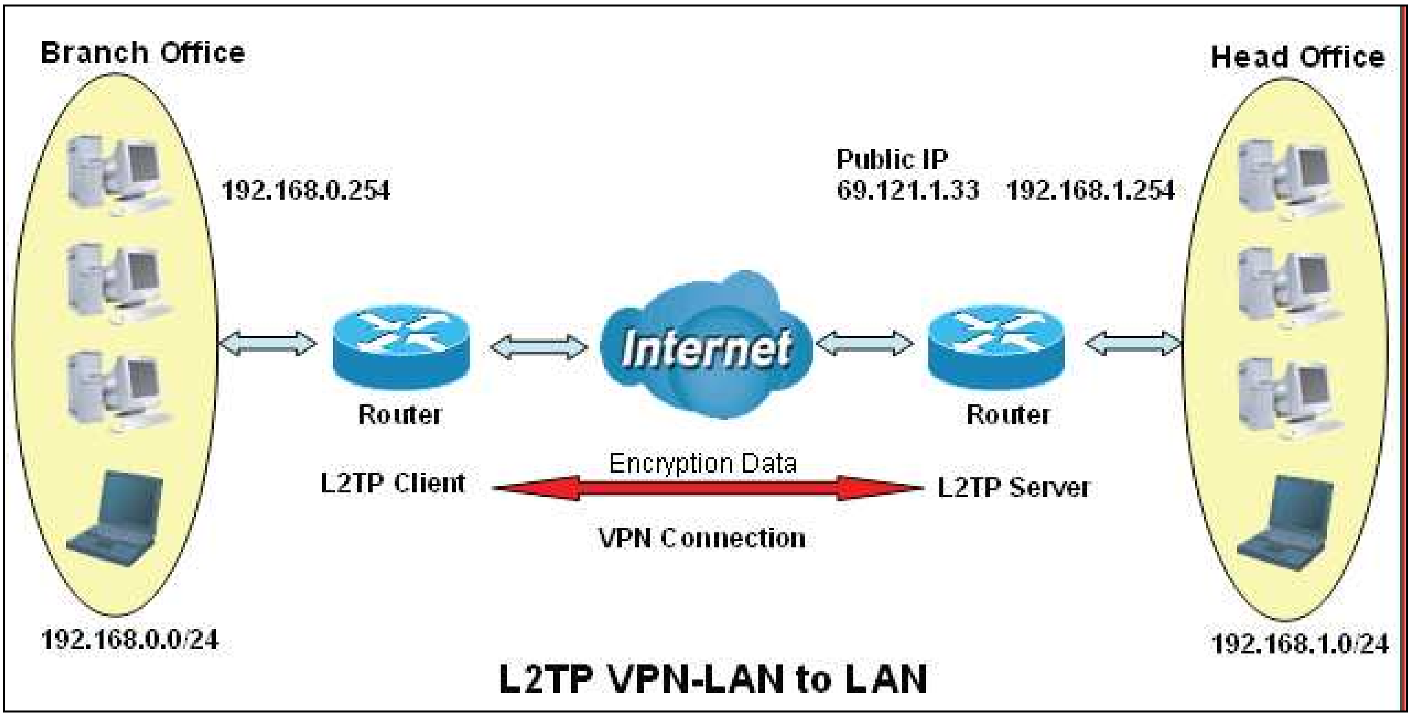
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol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

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

Click Edit/Delete to save your changes.

Example: Configuring L2TP LAN-to-LAN VPN Connection

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

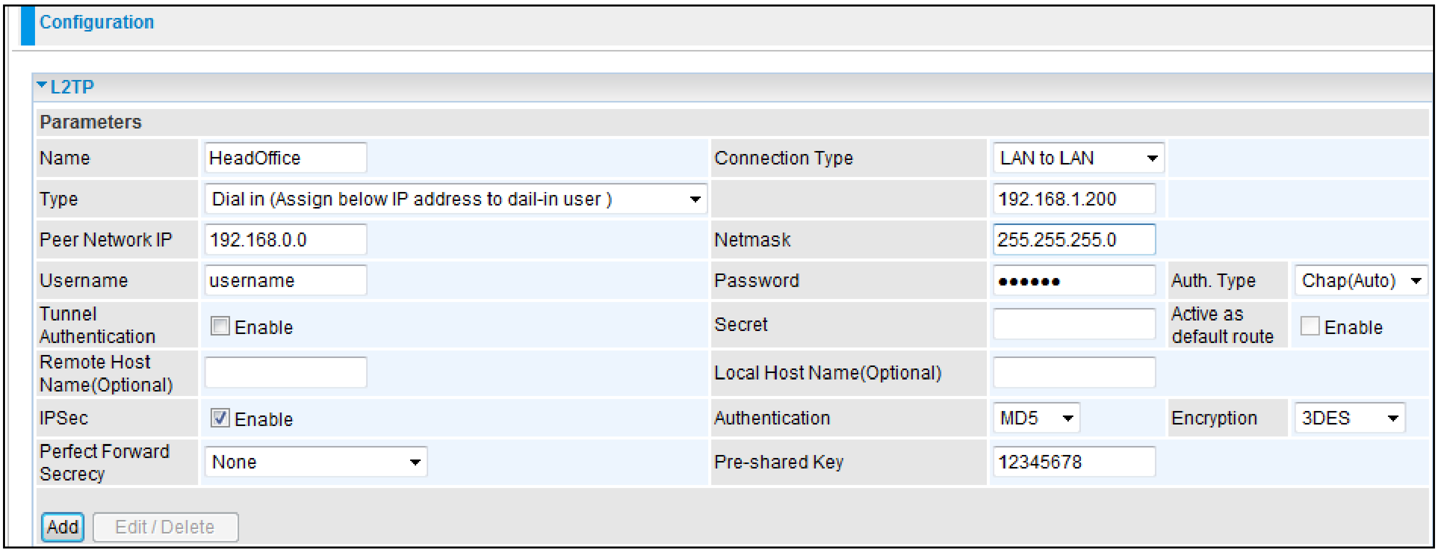


- ✓Both office Networks MUST be in different subnets with the LAN-LAN application.
- ✓Functions of Pre –shared keys, VPN Connection Type and Security Algorithms must be identical on both sides.

Attention

Configuring L2TP VPN in the Head Office

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



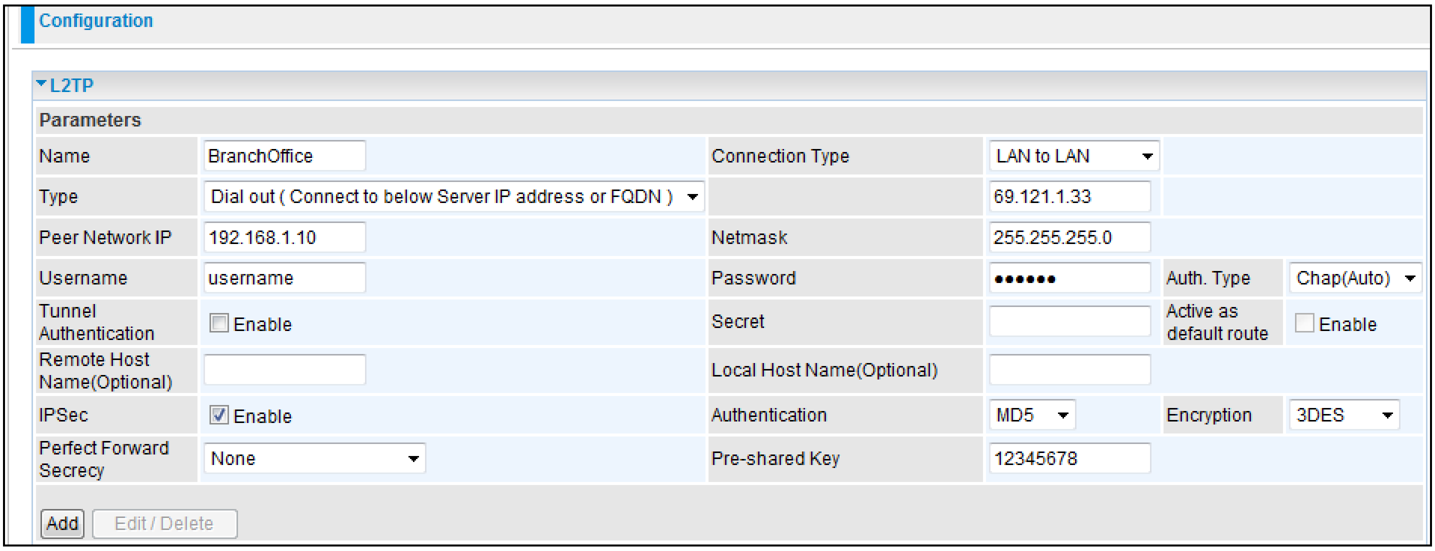
Parameters

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

Function		Description
Name	Head Office	Give a name to the L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	IP address assigned to the branch office network
Peer Network IP	192.168.0.0	Branch office network
Username	username	A username and password assigned to authenticate the branch office network
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value in most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides should use the same value
Encryption	3DES	
Prefer Forward Security	None	
Pre-Shared Key	12345678	

Configuring L2TP VPN in the Branch Office

The IP address 69.1.121.30 is the Public IP address of the router located in head office. If you registered the DDNS (please refer to the DDNS section of this manual), you can also use the domain name instead of the IP address to reach the router.


Configuration

L2TP

Parameters

Name	BranchOffice	Connection Type	LAN to LAN		
Type	Dial out (Connect to below Server IP address or FQDN)		69.121.1.33		
Peer Network IP	192.168.1.10	Netmask	255.255.255.0		
Username	username	Password	●●●●●●	Auth. Type	Chap(Auto)
Tunnel Authentication	□ Enable	Secret		Active as default route	□ Enable
Remote Host Name(Optional)		Local Host Name(Optional)			
IPSec	☑ Enable	Authentication	MD5	Encryption	3DES
Perfect Forward Secrecy	None	Pre-shared Key	12345678		

Function		Description
Name	Head Office	Give a name to the L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	69.121.1.33	IP address assigned to the branch office network
Peer Network IP	192.168.1.0	Head office network
Netmask	255.255.255.0	
Username	username	A username and password assigned to authenticate the branch office network
Password	123456	
Auth. Type	Chap (Auto)	Keep this as the default value in most cases
IPSec	Enable	Enable this to enhance your L2TP VPN security
Authentication	MD5	Both sides should use the same value
Encryption	3DES	
Prefer Forward Security	None	
Pre-Shared Key	12345678	

VoIP - Voice over Internet Protocol

VoIP enables telephone calls through existing Internet connection instead of going through the PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long distance telephone charges, but also toll-quality voice calls over the Internet.

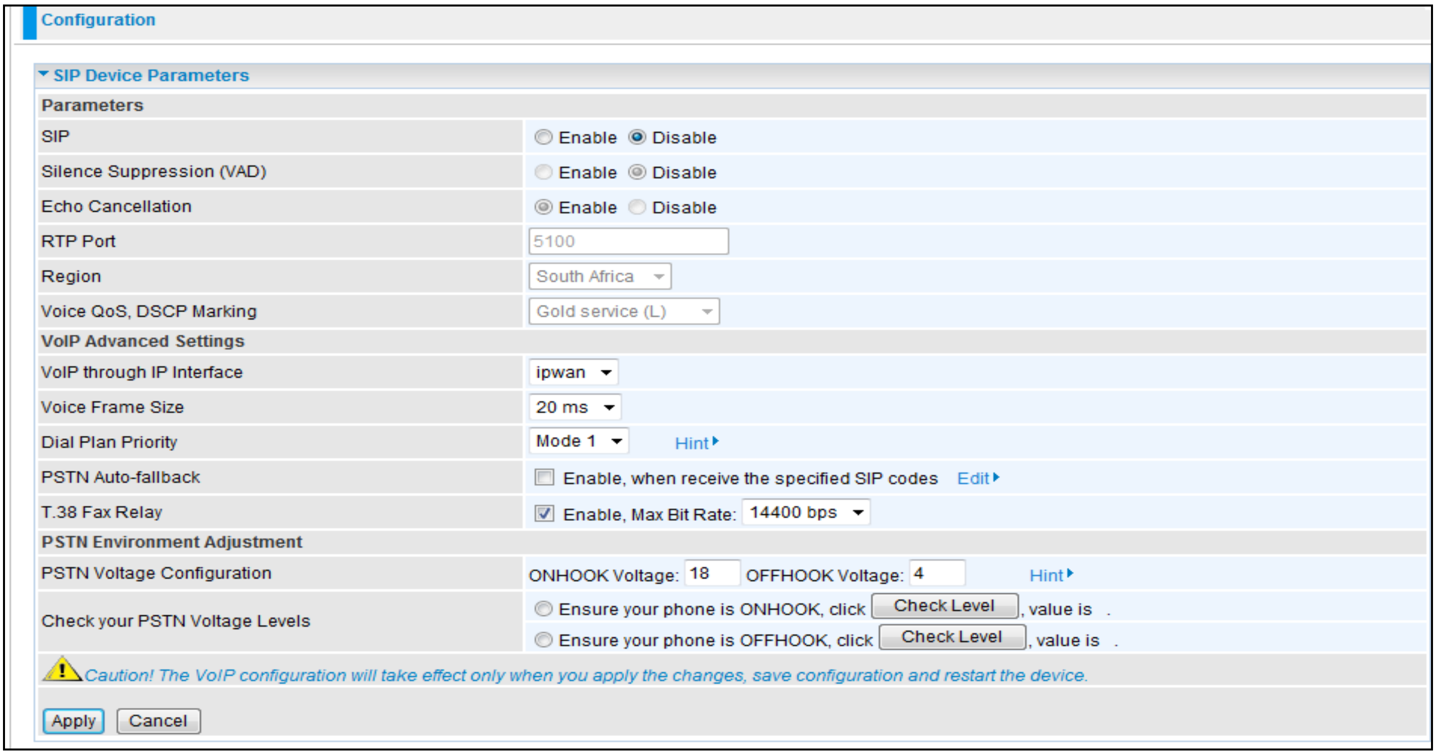
Attention

✓ **Remember to apply changes, SAVE CONFIG and restart the router after completing your VoIP configuration. This is to ensure that your VoIP is activated.**

Here are the items within the VoIP section: **SIP Device Parameters, SIP Accounts, Phone Port, PSTN Dial Plan, VoIP Dial Plan, Call Features, Speed Dial** and **Ring &Tone.**

SIP Device Parameters

This section provides easy setup for your VoIP service. Phone port 1 and 2 can be registered to different SIP Service Providers.



Configuration

▾ SIP Device Parameters

Parameters	
SIP	○ Enable ● Disable
Silence Suppression (VAD)	○ Enable ● Disable
Echo Cancellation	● Enable ○ Disable
RTP Port	5100
Region	South Africa
Voice QoS, DSCP Marking	Gold service (L)
VoIP Advanced Settings	
VoIP through IP Interface	ipwan
Voice Frame Size	20 ms
Dial Plan Priority	Mode 1 Hint
PSTN Auto-fallback	□ Enable, when receive the specified SIP codes Edit
T.38 Fax Relay	☑ Enable, Max Bit Rate: 14400 bps
PSTN Environment Adjustment	
PSTN Voltage Configuration	ONHOOK Voltage: 18 OFFHOOK Voltage: 4 Hint
Check your PSTN Voltage Levels	○ Ensure your phone is ONHOOK, click Check Level , value is . ○ Ensure your phone is OFFHOOK, click Check Level , value is .

Caution! The VoIP configuration will take effect only when you apply the changes, save configuration and restart the device.

SIP Device Parameters

SIP: To use VoIP SIP as VoIP call signaling protocol. Default is set to ‘Disable’.

Silence Suppression (VAD): Voice Activation Detection (VAD) prevents transmitting the nature silence to consume the bandwidth. It is also known as Silence Suppression which is a software application that ensures the bandwidth is reserved only when voice activity is activated. Default is set to ‘Enable’.

Echo Cancellation: G.168 echo canceller is an ITU-T standard. It is used to isolate the echo while you are on the phone. This helps you not hear your own voice on the phone while you talk. Default is set to ‘Enable’.

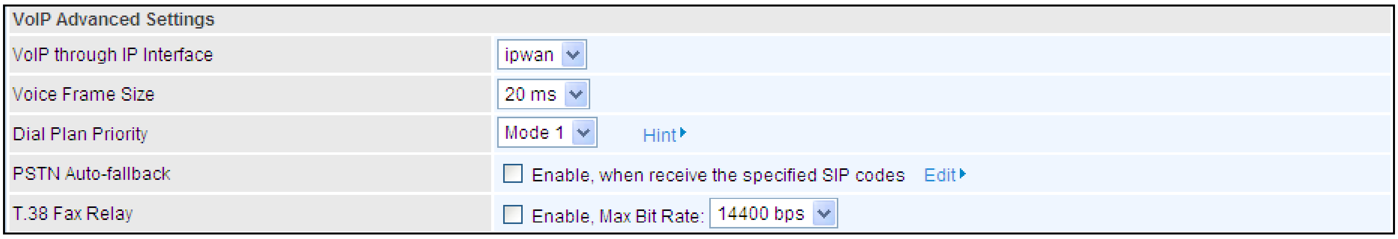
RTP Port: Provides the base value from the media (RTP) ports that are assigned for various endpoints and the different call sessions that may exist within an end-point. (Range from 5100 to 65535, default value is 5100)

Region: This selection is a drop-down box, which allows a user to select the country in which the VoIP device is active. When a country is selected, the country parameters are automatically loaded.

Voice QoS, DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the next Router based on the DSCP value. See Table 4. The DSCP Mapping Table:

Note: Be sure that the router(s) in the backbone network have the ability to execute and check the DSCP* markings *through-out the QoS network.

Advanced – Parameters



VoIP Advanced Settings	
VoIP through IP Interface	ipwan
Voice Frame Size	20 ms
Dial Plan Priority	Mode 1 Hint
PSTN Auto-fallback	□ Enable, when receive the specified SIP codes Edit
T.38 Fax Relay	□ Enable, Max Bit Rate: 14400 bps

VoIP through IP Interface: IP Interface decides where to send/receive the VoIP traffic; it includes: ipwan and iplan. Easy way to select the interface is to check the location of the SIP server. If it is located somewhere on the Internet then select **ipwan.** If the VoIP SIP server is on the local Network then select **iplan.**

Voice Frame Size: Frame size is available from 10ms to 60ms. Frame size meaning how many milliseconds the Voice packets will be queued and sent out. It is ideal to have the same frame size on both Caller and Receiver.

Dial Plan Priority: Define the priority between VoIP and PSTN dial plan.

PSTN Auto-fallback: Whenever VoIP SIP responds with an error or an error code matching the codes in the **Edit** section, the VoIP calls will automatically fallback to PSTN. In other words, the call will be made via the PSTN when VoIP SIP returns an error code.

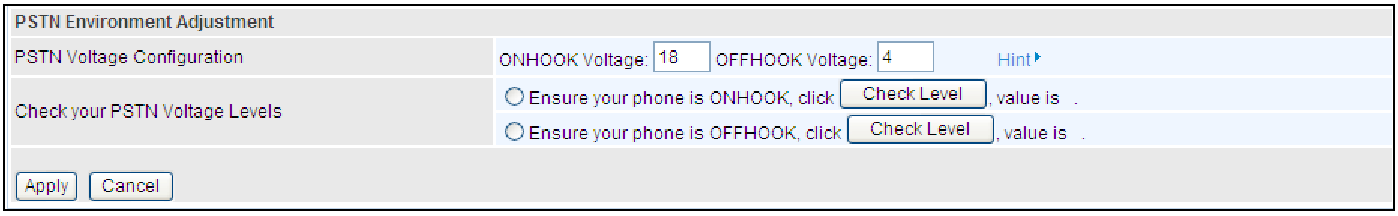
Click ‘Edit’ to add or remove response codes. Be sure that the codes are separated by a comma (,).

For more information about SIP response codes, please go to this link **http://voip-info.org/wiki/view/sip+response+codes**. You will get the meaning of all the SIP responses here.

T.38 Fax Relay: It allows the transfer of facsimile documents in real-time between two standard Group 3 facsimile terminals over the Internet or other networks using IP protocols. It will only function when both sites support this feature and have it enabled.

Advanced – PSTN Environment Adjustment

PSTN Environment Adjustment options will help you to adjust the onhook and offhook voltage detection values for your environment. You should use these if the default values are incorrect and result in PSTN calls not being detected properly, e.g. calls being terminated within 5 seconds of being answered. The actual levels are determined by your environment including the number and type of telephones used.



PSTN Environment Adjustment

PSTN Voltage Configuration	ONHOOK Voltage: 18 OFFHOOK Voltage: 4 Hint
Check your PSTN Voltage Levels	○ Ensure your phone is ONHOOK, click Check Level, value is . ○ Ensure your phone is OFFHOOK, click Check Level, value is .

Note: ONHOOK means hung up.

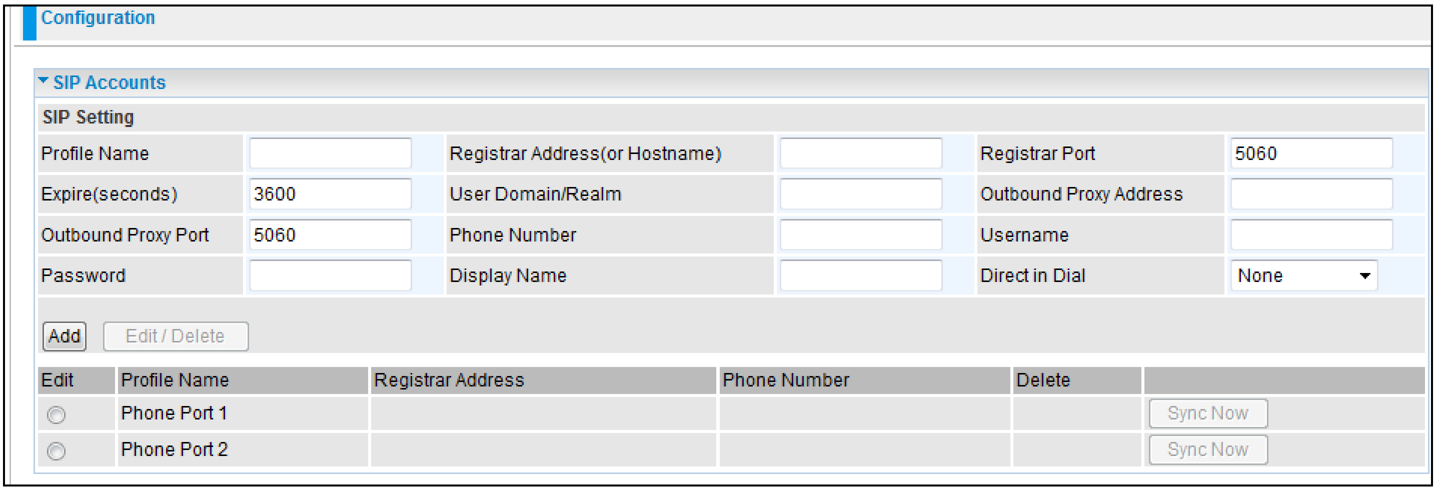
To take your phone OFFHOOK, lift the receiver then press Hook/Flash until you hear your normal PSTN dial tone, and not your VoIP dial tone. Wait several seconds and then press Check Level.

You should check the OFFHOOK value for each telephone you have connected to this device. Set the OFFHOOK voltage to the lowest setting registered for all your telephones, e.g. if your telephones return values of 4, 5 and 7 then you should set your OFFHOOK voltage to 4.

Note: The detected values will not automatically be set by the Check Level function; you must enter the lowest level detected after testing all your telephones.

SIP Accounts

This section contains the basic settings of the VoIP module from the selected provider in the Wizard section. Providing the incorrect information will cause it to stop making calls through the Internet.



Configuration

SIP Accounts

SIP Setting

Profile Name		Registrar Address(or Hostname)		Registrar Port	5060
Expire(seconds)	3600	User Domain/Realm		Outbound Proxy Address	
Outbound Proxy Port	5060	Phone Number		Username	
Password		Display Name		Direct in Dial	None

Edit	Profile Name	Registrar Address	Phone Number	Delete	
○	Phone Port 1				Sync Now
○	Phone Port 2				Sync Now

Profile Name: Assign a name for profile identification.

Registrar Address (or Hostname): Indicate the VoIP SIP registrar IP address.

Registrar Port: Specify the port of the VoIP SIP registrar on which it will listen for register requests from VoIP devices.

Expire: This is the duration for the registration message being sent.

User Domain/Realm: Set a different domain name for the VoIP SIP proxy server.

Outbound Proxy Address: Indicate the VoIP SIP outbound proxy server IP address. This parameter is very useful when VoIP devices are behind a NAT.

Outbound Proxy Port: Specify the port of the VoIP SIP outbound proxy on which it will listen for messages.

Phone Number: This parameter holds the registration ID of the user within the VoIP SIP registrar.

Username: Same as Phone Number.

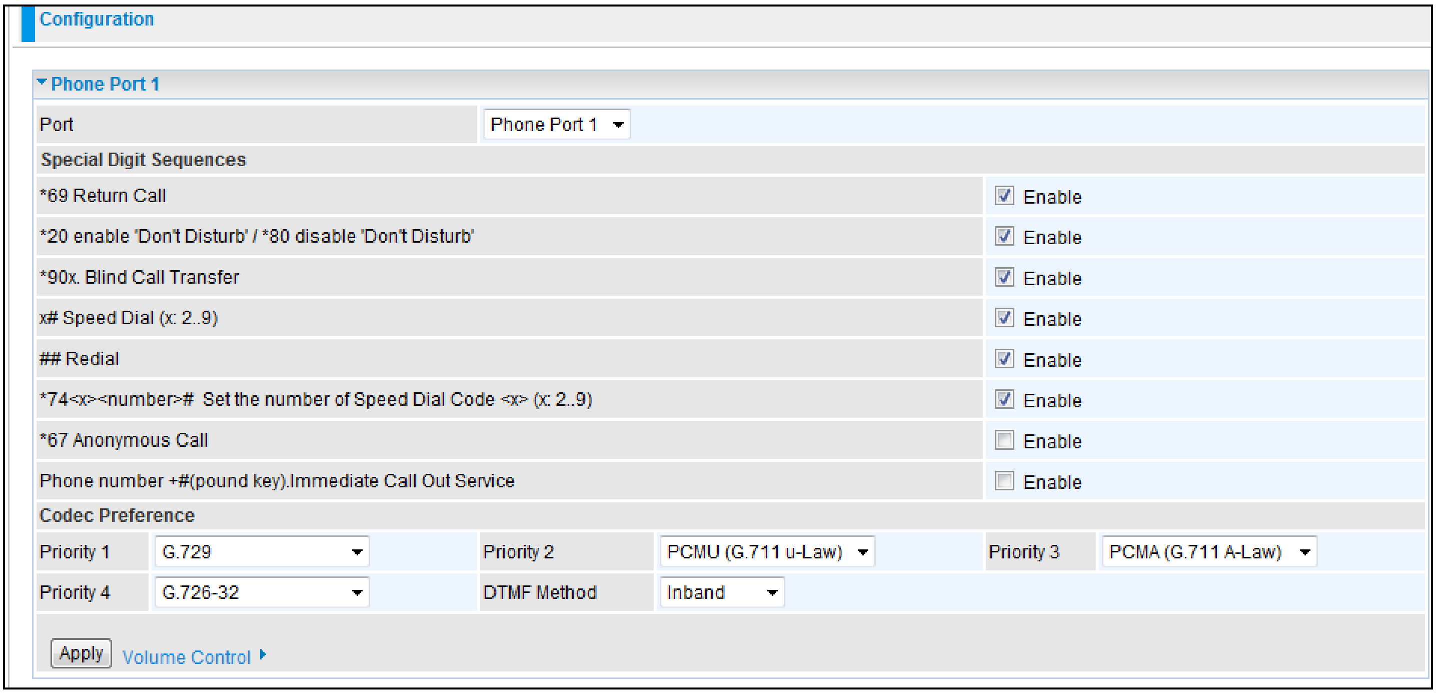
Password: This parameter holds the password used for authentication within the VoIP SIP registrar.

Display Name: This parameter will appear on the Caller ID.

Direct in Dial: Select the ringing port when getting an incoming VoIP call.

Phone Port

This section displays the status and allows for further editing of the account information of the Phones. Click Edit to update your phone information.



Configuration

▾ Phone Port 1

Port	Phone Port 1 ▾
Special Digit Sequences	
*69 Return Call	☑ Enable
*20 enable 'Don't Disturb' / *80 disable 'Don't Disturb'	☑ Enable
*90x. Blind Call Transfer	☑ Enable
x# Speed Dial (x: 2..9)	☑ Enable
## Redial	☑ Enable
*74<x><number># Set the number of Speed Dial Code <x> (x: 2..9)	☑ Enable
*67 Anonymous Call	☐ Enable
Phone number +#(pound key).Immediate Call Out Service	☐ Enable

Codec Preference

Priority 1	G.729 ▾	Priority 2	PCMU (G.711 u-Law) ▾	Priority 3	PCMA (G.711 A-Law) ▾
Priority 4	G.726-32 ▾	DTMF Method	Inband ▾		

Port: It allows you to change the phone port setting for a specific FXS port.

***69 (Return Call):** Dial *69 to return the last missed call. It is only available for VoIP call(s).

***20 (Do not Disturb ON):** Dial *20 to enable the No Disturb feature. Your phone will not ring if someone calls.

***90x (Blind Call Transfer):** Dial *90 + phone-number to transfer a call to a third party. This feature is enabled by default.

x# Speed Dial (x:2..9): Refer to the Phone Port section in the Web GUI. Set up your Speed Dial phone book first before accessing the Speed Dial feature. This feature is enabled by default.

## Redial: Press ## to redial the last phone number. This feature is enabled by default.

***74<x><number>#:** Use your phone key pad to insert a phone number to the Speed Dial phone book. Or you can update your Speed Dial phone number manually. Refer to the Phone Port section in the Web GUI for details.

***67 Anonymous Call:** Hide your phone number from being displayed at the remote terminal. It is only applied to the next call when you enter this control character. The detailed operation procedure is “Off Hook -> *67 -> On Hook -> Off Hook -> Dial”. This feature is disabled by default.

Phone Number + #: This is the fast dial which you can dial out a phone number immediately without waiting.

Note: Refer to the Special Dial Code section in this Manual for more details.

Codec Preference

Codec is known as Coder-Decoder, it is used for data signal conversion. Setting the priority of voice compression with Priority 1 represents the top priority.

G.729: It is used to encode and decode voice information into a single packet to reduce bandwidth consumption.

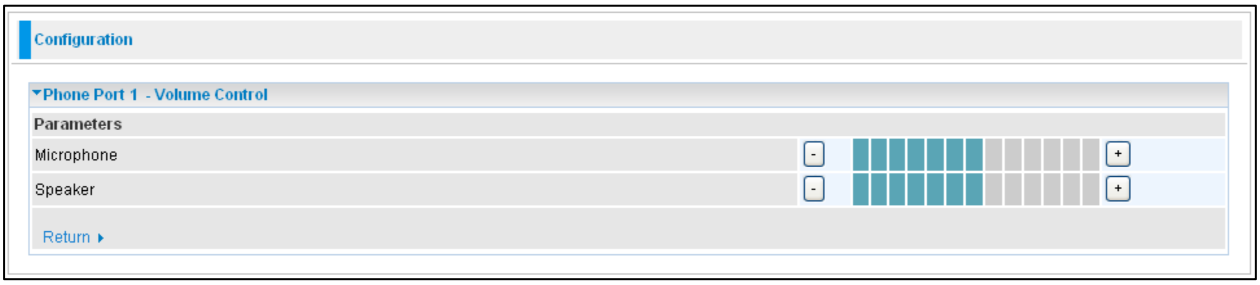
G.711μ-LAW: It is a basic non-compressed encoder and decoder technique. μ-LAW uses pulse code modulation (PCM) encoder and decoder to convert a 14-bit linear sample.

G.711A-LAW: It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert a 13-bit linear sample.

G.726-32: It is used to encode and decode voice information into a single packet to reduce bandwidth consumption. Currently only supports bit rates of 32Kbps.

DTMF Method: The Inband, RFC 2833 and SIP INFO (RFC 2976) are supported.

Volume Control



Configuration

▾Phone Port 1 - Volume Control

Parameters	
Microphone	- 🟦🟦🟦🟦🟦🟦⬜⬜⬜⬜⬜⬜ +
Speaker	- 🟦🟦🟦🟦🟦🟦⬜⬜⬜⬜⬜⬜ +

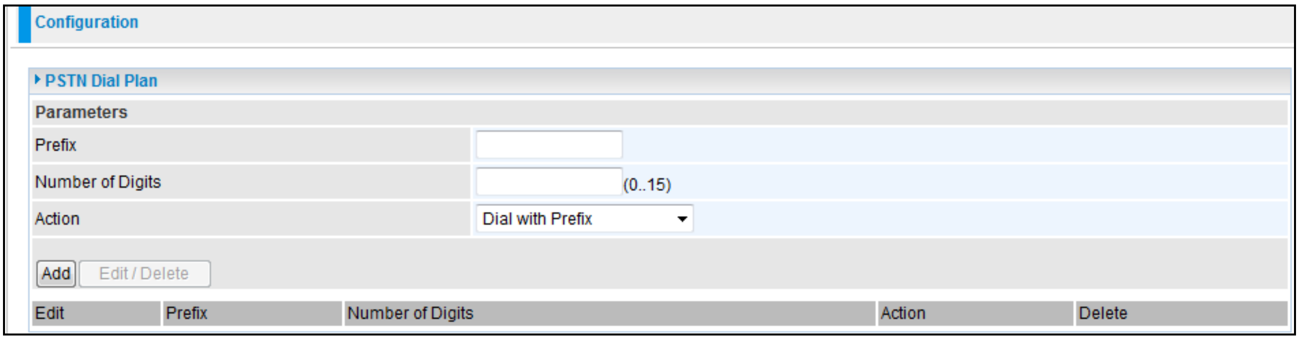
Return ▸

Volume control enables you to adjust the voice quality of the telephones to a comfortable level. Press the “-” minus sign to reduce either the microphone or speaker level of your telephone. Press the “+”, plus sign to increase either the microphone or speaker level of your telephone.

PSTN Dial Plan (Router with LINE port only)

This section enables you to configure the “VoIP with PSTN switching” on your system. You can define a range of dial plans that will make regular call switch from VoIP to the PSTN line. Prefix numbers are an essential key to make a difference between VoIP and Regular phone calls. If the actual numbers dialed match with the prefix number defined in this dial plan, the dialed number will be rerouted to the PSTN to make a regular call. Otherwise, the number will be rerouted to the VoIP networks.

Note: In order to utilize this feature, you must have registered and connected to your SIP Server first.



Configuration

PSTN Dial Plan

Parameters	
Prefix	
Number of Digits	(0..15)
Action	Dial with Prefix

Add | Edit / Delete

Edit	Prefix	Number of Digits	Action	Delete

Prefix: Specify the number(s) that will be used to switch from VoIP to PSTN when making a call.

Number of Digits: Specify the total number of digits you wish to dial out. The maximum number of digits is 15.

Action: Specify a dialing method that you wish to use when making PSTN call(s).

Dial with Prefix: With this selected, the prefix which is dialed together with the phone number will be dialed out via FXO when making a regular call.

Note: The prefix number dialed has to match the number of digits specified.

Dial without Prefix: With this selected, the prefix which is dialed together with the phone number will not be dialed out with the phone number via the FXO when making a regular call.

Note: The length of the number of digits dialed should match the number of digits specified.

Dial at Timeout: The number & the prefix entered will be dialed out via the FXO port after a defined timeout interval even though the number of digits in the phone number entered does not match the number of digits specified.

Note: The total number of digits dialed must not exceed the number of digits defined otherwise dialing will be invalid.

Dial at Timeout no Prefix: The phone number will be dialed out via the FXO port excluding the prefix after a defined timeout interval even though the number of digits in the phone number entered does not match the number of digits specified.

Note: The total number of digits dialed must not exceed the number of digits defined otherwise dialing will be invalid.

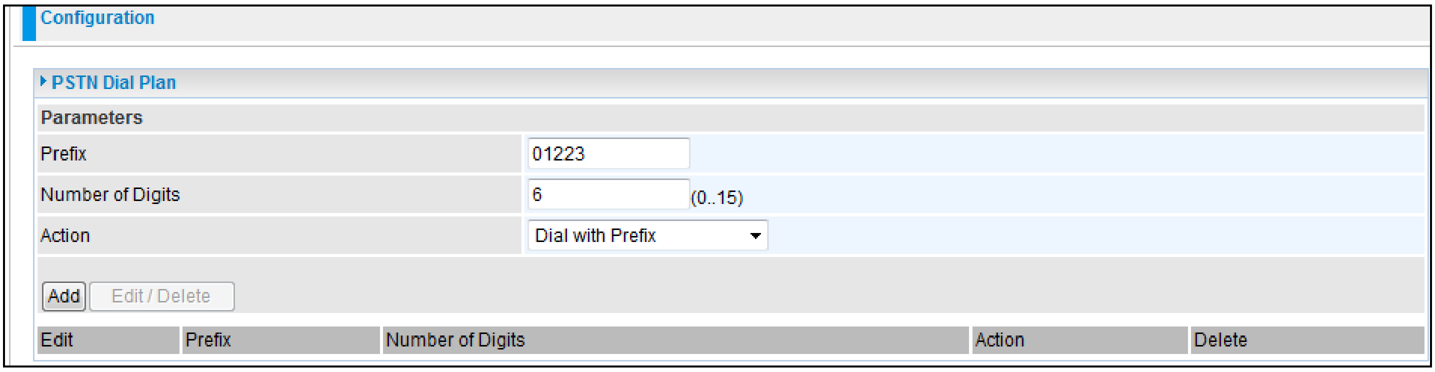
Attention

Phone port 1 & 2 will automatically revert to a PSTN line when:

- ✓ **Power is down**
- ✓ **Internet service fails (e.g. loss of WAN IP Address)**
- ✓ **SIP option has been disabled (refer to VoIP General Setting Section)**
- ✓ **Calls that match the rules defined in the PSTN dial plan**
- ✓ **SIP service is inaccessible when:**
  - o **User manually disables the registration**
  - o **Invalid username & password has been entered**
  - o **An invalid SIP number is dialed**
  - o **PSTN auto-failback function is disabled**

PSTN Dial Plan Examples:

1. Dial with Prefix



Configuration

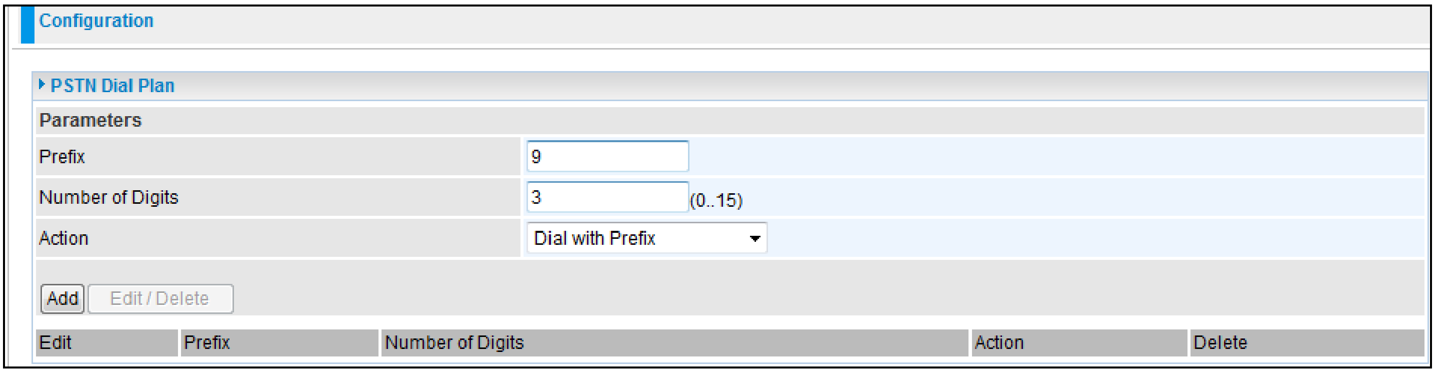
PSTN Dial Plan

Parameters	
Prefix	01223
Number of Digits	6 (0..15)
Action	Dial with Prefix

Edit	Prefix	Number of Digits	Action	Delete

If you dial 01223 707070, the number 01223707070 will be dialed out via FXO for making a regular phone call.

2. Dial without Prefix



Configuration

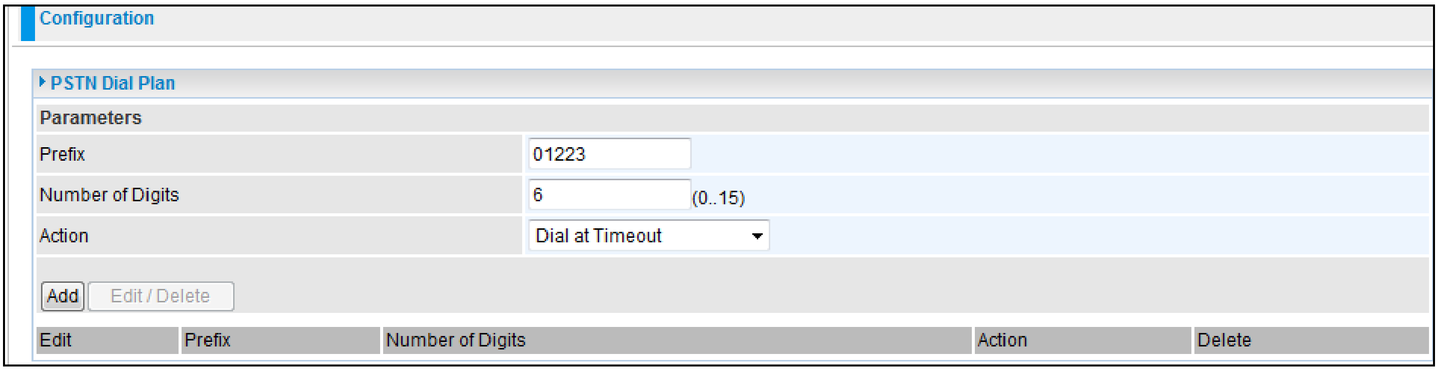
PSTN Dial Plan

Parameters	
Prefix	9
Number of Digits	3 (0..15)
Action	Dial with Prefix

Edit	Prefix	Number of Digits	Action	Delete

If you dial 9102, only 102 will be dialed out via FXO port for making a regular phone call.

3. Dial at Timeout



Configuration

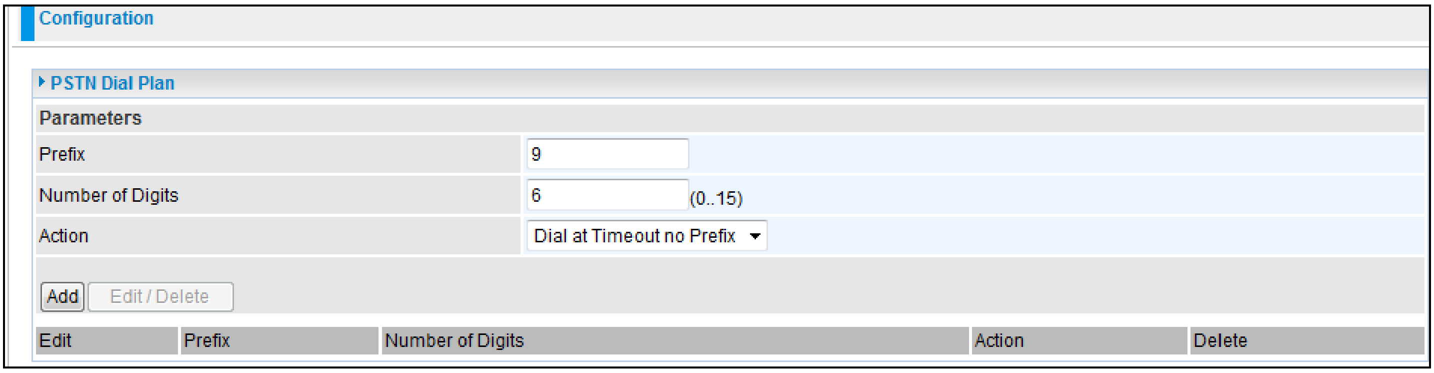
PSTN Dial Plan

Parameters	
Prefix	01223
Number of Digits	6 (0..15)
Action	Dial at Timeout

Edit	Prefix	Number of Digits	Action	Delete

If you dial 01223 7070, the number 012237070 will be dialed to make a regular call via FXO port after a defined timeout interval even though the number of digits entered does not match the number of digits defined. Number 7070 will still be a valid number for the device to complete the dialing because it does not exceed the number of digits defined.

4. Dial at Timeout no Prefix



Configuration

▸ PSTN Dial Plan

Parameters	
Prefix	9
Number of Digits	6 (0..15)
Action	Dial at Timeout no Prefix ▾

Add | Edit / Delete

Edit	Prefix	Number of Digits	Action	Delete

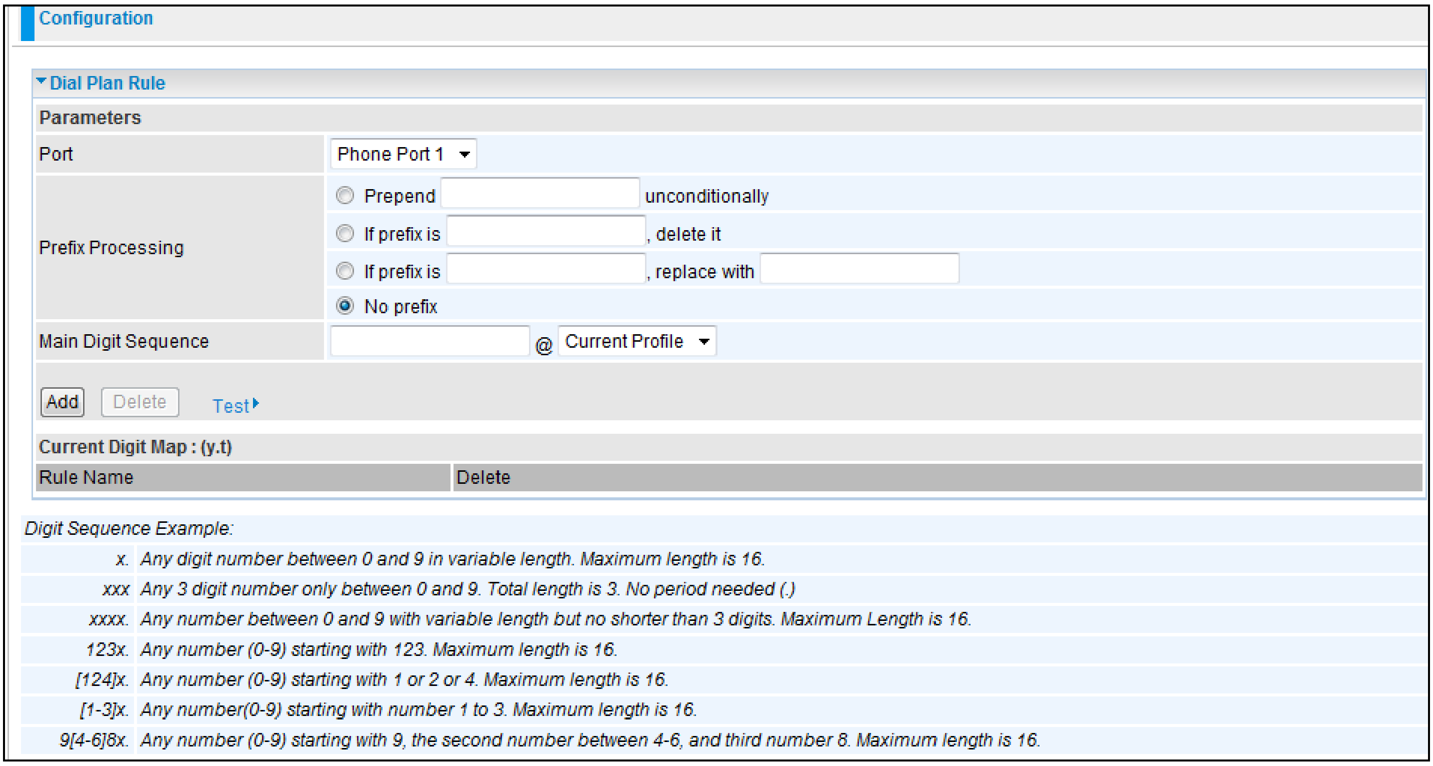
If you dial 97070, the number that is dialed out via the FXO port will not have a prefix. Even though 7070 (only 4 digits) does not match the number of digits defined in the field, 7070 is still a valid phone number since it has not exceeded the number of digits defined.

VoIP Dial Plan

This feature makes dialing a phone number more convenient and easy. Instead of having to memorize the phone number of every contact, VoIP Dial Plan gives you the option of create a dial plan that will enable you to make your phone calls without the need to memorize the phone number. To access this feature, go to Configuration > VoIP > VoIP Dial Plan.

Dial Plan Rules

Click the Add button to create and define a VoIP dial plan rule.



Configuration

▾ Dial Plan Rule

Parameters	
Port	Phone Port 1 ▾
Prefix Processing	○ Prepend [ ] unconditionally ○ If prefix is [ ] , delete it ○ If prefix is [ ] , replace with [ ] ● No prefix
Main Digit Sequence	[ ] @ Current Profile ▾

Add | Delete | Test▸

Current Digit Map : (y.t)

Rule Name	Delete

Digit Sequence Example:

x.	*Any digit number between 0 and 9 in variable length. Maximum length is 16.*
xxx	*Any 3 digit number only between 0 and 9. Total length is 3. No period needed (.)*
xxxx.	*Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum Length is 16.*
123x.	*Any number (0-9) starting with 123. Maximum length is 16.*
[124]x.	*Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.*
[1-3]x.	*Any number(0-9) starting with number 1 to 3. Maximum length is 16.*
9[4-6]8x.	*Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16.*

Prefix Processing:

Prepend xxx unconditionally: xxx number is added unconditionally to the front of the number dialed when making a call. Prefix can also be included with any number and/or character such as +, *, #.

*Note: For special service with +, *, #, you may need to check with your VoIP or Local Telephone Service Provider for information.*

If Prefix is xxx, delete it: Prefix xxx is removed from the dialed numbers before making a call.

If Prefix is xxx, replace with: Prefix xxx is added to the front of the dialed numbers when making a call.

No prefix: No prefix is added to the front of the numbers dialed. This is the default setting for the Prefix Processing section.

Main Digit Sequence: The call(s) can be made via SIP, PSTN or ENUM.

x: Any numeric number between 0 and 9.

. (period): Repeat numeric number(s) between 0 and 9.

*** (asterisk sign):** It is a normal character '*' on the phone key pad. Please check if any special service is provided by your VoIP Service Provider or your Local Telephone Service Provider.

# (pound sign): It is a normal character '#' on the phone key pad. Please check if any special service is provided by your VoIP Service Provider or the Local Telephone Service Provider.

<@ Current Profile>: Refer to the VoIP account registered on the *VoIP Wizard* for Port 1 or 2.

<@ PSTN>: Making a telephone call via the PSTN line.

<@ENUM>: Making a VoIP SIP direct call via an Electronic number (ENUM) 164 to an ENUM caller.

Electronic Number (ENUM) uses DNS (Domain Network System) based technology to map between a traditional phone number (PSTN) to an Internet addresses/ SIP URL. The ENUM number must be registered via a public ENUM site or your VoIP Service Provider.

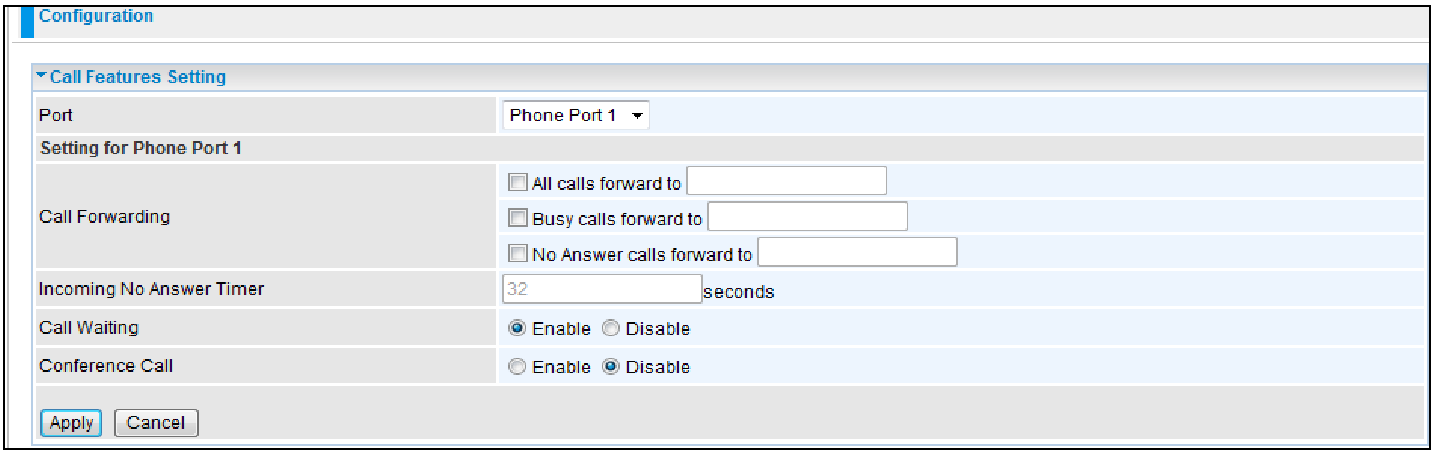
<@ SIPgateway>: It is used for the Intelligent Call Routing feature where you need to set up your SIP account on the VoIP User defined Profiles link on the VoIP Wizard page. Go to the VoIP Wizard in this manual for more information.

Dial-Plan Examples:	**Description**
X	Any digit number between 0 and 9 in variable length. Maximum length is 16.
Xxx	Any 3 digit number only between 0 and 9. Total length is 3. *Note: No period is needed (.)*
xxxx	Any number between 0 and 9 with variable length but no shorter than 3 digits. Maximum length is 16.
123x	Any number (0-9) starting with 123. Maximum length is 16.
[x…x]x. **For example: [124]x**	Any number (0-9) starting with 1 or 2 or 4. Maximum length is 16.
[x-x]x. For example: [1-3]x	Any number (0-9) starting with number 1 to 3. Maximum length is 16.
x[x-x]x. For example: 9[4-6]8x.	Any number (0-9) starting with 9, the second number between 4-6, and third number 8. Maximum length is 16

Special Dial Plan Examples	Description
*xx*x	Starting with '* sign' + any two digit numbers + any number (0-9) in variable length. Maximum length is 16.
*xx	Starting with '* sign' + any 2 digit numbers between 0 and 9. Total length including the * is 3. *Note: No period is needed (.)*
**xx*x.	Starting with '** sign' + any two digit numbers between 0 + any number (0-9) in variable length. Maximum length is 16
#xx	Starting with '# sign' + any digit number (0-9) in variable length but no shorter than 1 digits. Maximum length is 16
##xx*x	Starting with '## sign' + any two digit numbers + '* sign' + any number (0-9) in variable length. Maximum length is 16

Call Feature

VoIP has all the basic features of a traditional phone. Besides the provided basic features, VoIP also comes with several enhanced features that allow you to further customize the settings to suit your personal needs, such as call forwarding, call waiting time length, conference call feature, anonymous call feature and incoming no answer timer.



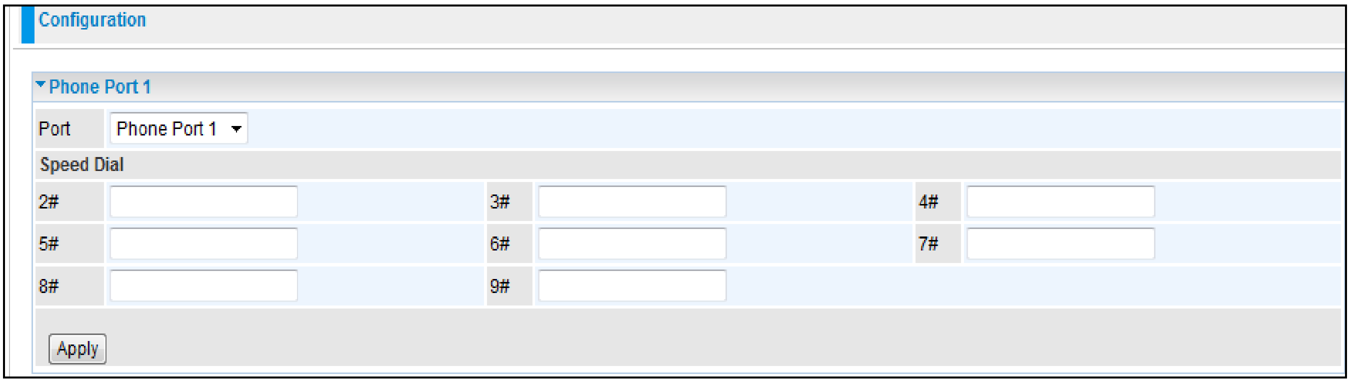
Configuration

Call Features Setting

Port	Phone Port 1
Setting for Phone Port 1	
Call Forwarding	□ All calls forward to □ Busy calls forward to □ No Answer calls forward to
Incoming No Answer Timer	32 seconds
Call Waiting	● Enable ○ Disable
Conference Call	○ Enable ● Disable

Speed Dial

Speed Dial comes in handy to store frequently used telephone numbers which you can press a number from 0 to 9 and the pound sign (#) on the phone keypad to activate the function. For example, to speed dial to the phone number listed on 9, just press keypad 9 then #. Your router will automatically call the number listed on entry 9.



Configuration

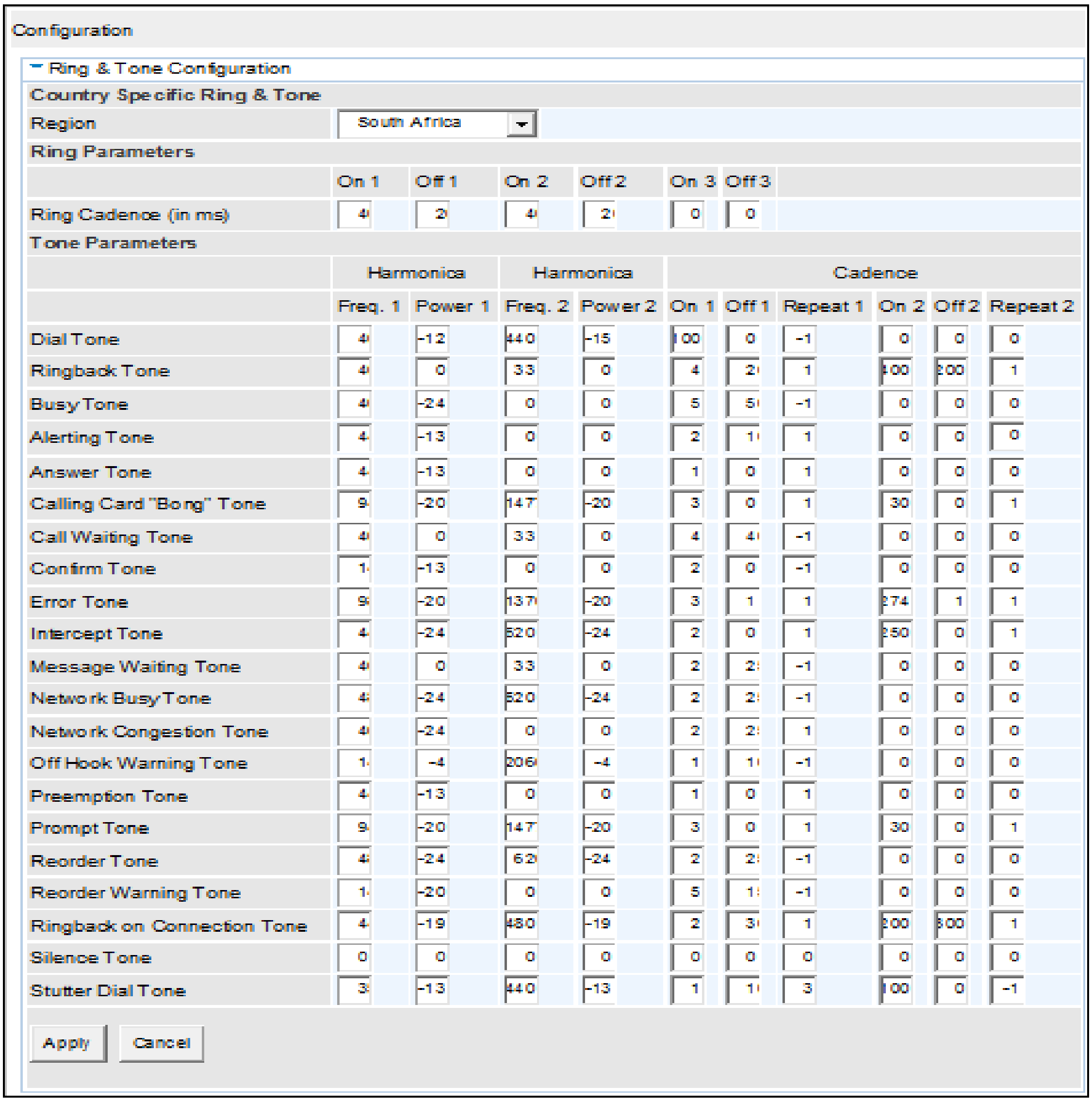
▾ Phone Port 1

Port	Phone Port 1 ▾				
Speed Dial					
2#		3#		4#	
5#		6#		7#	
8#		9#			

Apply

Ring & Tone

This section allows advanced users to change the existing or newly defined parameters for various ring tones (dial tone, busy tone, answer tone etc.)



Configuration

▾ Ring & Tone Configuration

Country Specific Ring & Tone

Region: South Africa ▾

Ring Parameters

	On 1	Off 1	On 2	Off 2	On 3	Off 3
Ring Cadence (in ms)	4	2	4	2	0	0

Tone Parameters

	Harmonica		Harmonica		Cadence					
	Freq. 1	Power 1	Freq. 2	Power 2	On 1	Off 1	Repeat 1	On 2	Off 2	Repeat 2
Dial Tone	4	-12	440	-15	100	0	-1	0	0	0
Ringback Tone	4	0	33	0	4	2	1	400	200	1
Busy Tone	4	-24	0	0	5	5	-1	0	0	0
Alerting Tone	4	-13	0	0	2	1	1	0	0	0
Answer Tone	4	-13	0	0	1	0	1	0	0	0
Calling Card "Bong" Tone	9	-20	147	-20	3	0	1	30	0	1
Call Waiting Tone	4	0	33	0	4	4	-1	0	0	0
Confirm Tone	1	-13	0	0	2	0	-1	0	0	0
Error Tone	9	-20	137	-20	3	1	1	274	1	1
Intercept Tone	4	-24	520	-24	2	0	1	250	0	1
Message Waiting Tone	4	0	33	0	2	2	-1	0	0	0
Network Busy Tone	4	-24	520	-24	2	2	-1	0	0	0
Network Congestion Tone	4	-24	0	0	2	2	1	0	0	0
Off Hook Warning Tone	1	-4	206	-4	1	1	-1	0	0	0
Preemption Tone	4	-13	0	0	1	0	1	0	0	0
Prompt Tone	9	-20	147	-20	3	0	1	30	0	1
Reorder Tone	4	-24	62	-24	2	2	-1	0	0	0
Reorder Warning Tone	1	-20	0	0	5	1	-1	0	0	0
Ringback on Connection Tone	4	-19	480	-19	2	3	1	200	300	1
Silence Tone	0	0	0	0	0	0	0	0	0	0
Stutter Dial Tone	3	-13	440	-13	1	1	3	100	0	-1

Apply Cancel

Country Specific Ring & Tone

Region: Select a country ring tone from the drop-down list that pertains to your country of residence. This VoIP router will display the default parameters of each ring tone according to the country selected. If your country is not found in the list, you may manually enter the parameters of the ring tone that pertains to your country.

Ring Parameters

Ring Cadence (in ms): Ring cadence is defined by three fields, Frequency: On Time1, Off Time1, On Time2, Off Time2 and On Time3, Off Time3. Frequency is specified in Hertz. Time is given in milliseconds.

Tone Parameters

You may need to check with your local telephone service provider for such information. Also, it is recommended that this option be configured by an advanced user unless you are instructed to do so.

Click Apply to apply the settings.

QoS - Quality of Service

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

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

Prioritization

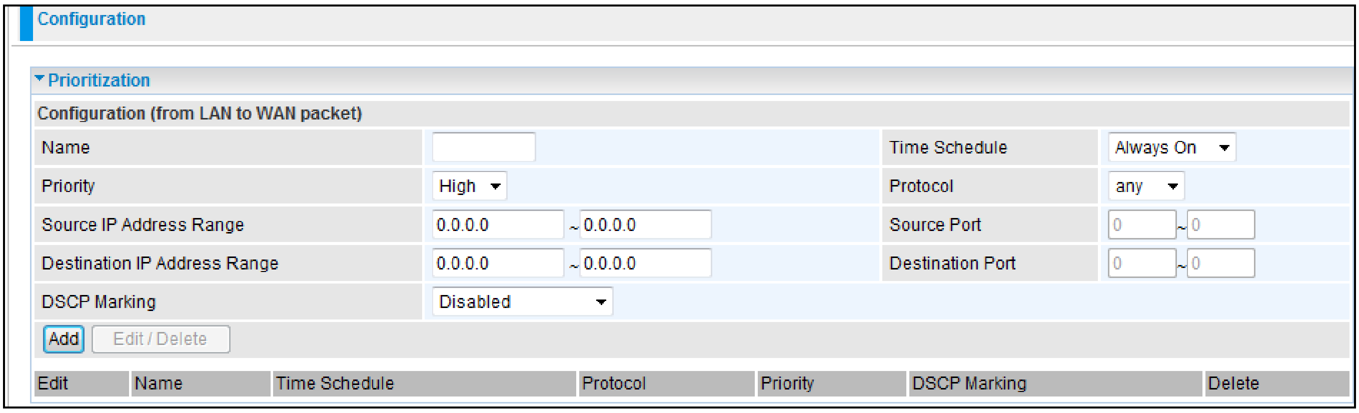
There are three priority settings provided:

High

Normal (The default setting is 'Normal' for all traffic that has not been set)

Low

The utilization percentage of each priority setting is High (60%), Normal (30%) and Low (10%). To delete an application, you can click on the Delete radio button of the application and then click the Edit/Delete button.



Configuration

▾ Prioritization

Configuration (from LAN to WAN packet)

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

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete

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

Time Schedule: Schedule your prioritization policy.

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

Protocol: The name of the supported protocol.

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

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

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

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

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

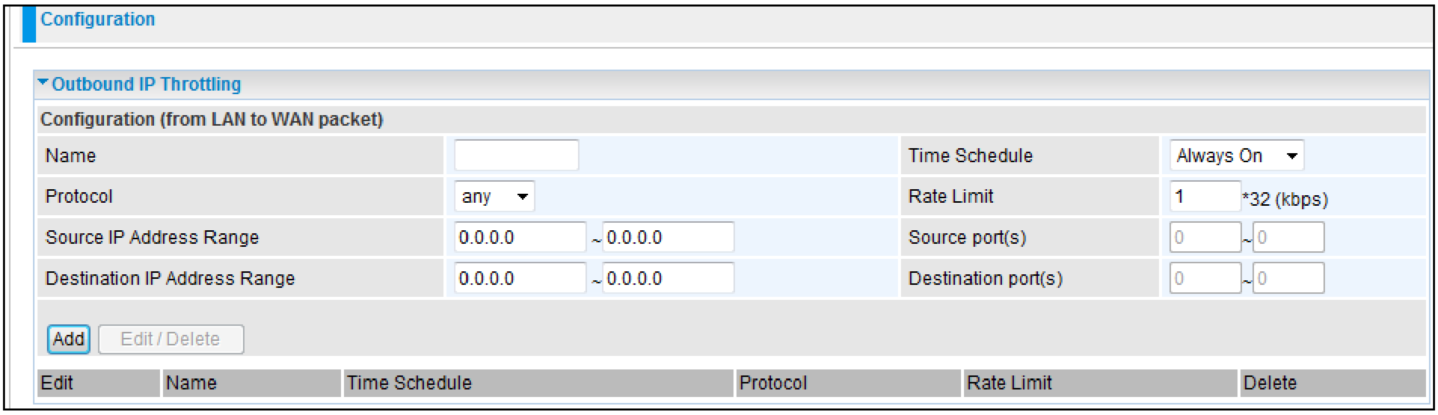
Note: Make sure that the router(s) in the network backbone are capable of executing and checking the DSCP throughout the QoS network.

Table 4: DSCP Mapping Table

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

Outbound IP Throttling (LAN to WAN)

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



Configuration

Outbound IP Throttling

Configuration (from LAN to WAN packet)

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

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete

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

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

Protocol: The name of the supported protocol.

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

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

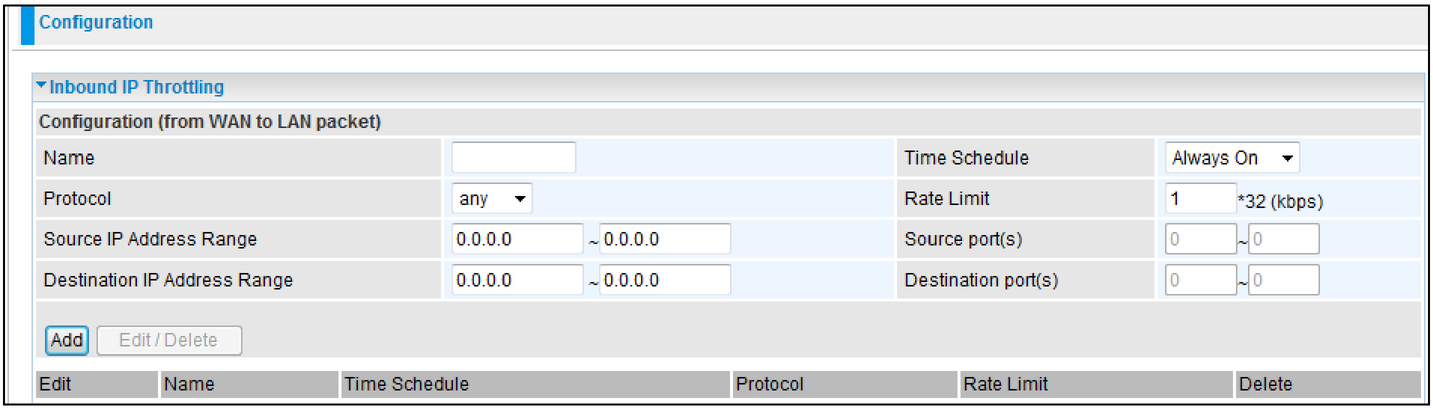
Source Port(s): The source port of the packets to be monitored.

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

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

Inbound IP Throttling (WAN to LAN)

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



Configuration

Inbound IP Throttling

Configuration (from WAN to LAN packet)

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

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete

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

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

Protocol: The name of the supported protocol.

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

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

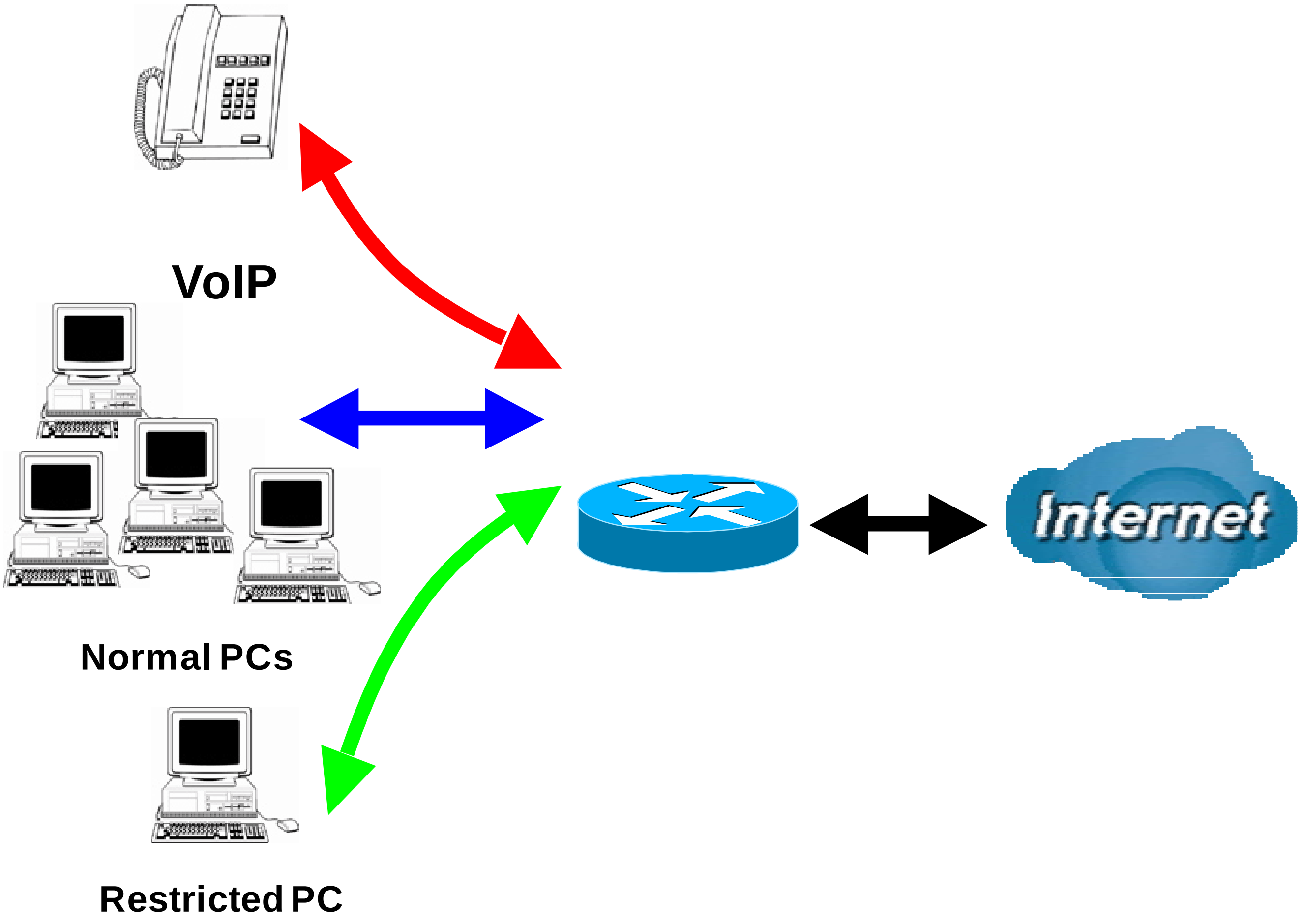
Source Port(s): The source port of the packets to be monitored.

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

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

Example: QoS for your Network

Connection Diagram



Information and Settings

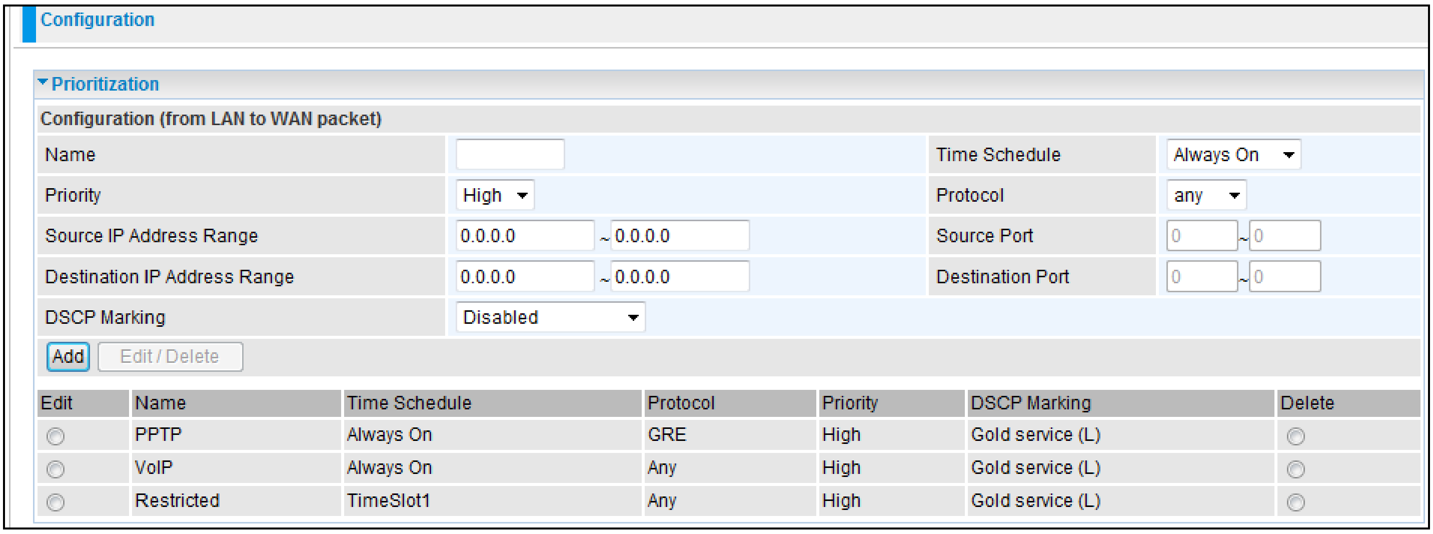
Upstream: 928 kbps

Downstream: 8 Mbps

VoIP User : 192.168.1.1

Normal Users : 192.168.1.2~192.168.1.5

Restricted User: 192.168.1.100



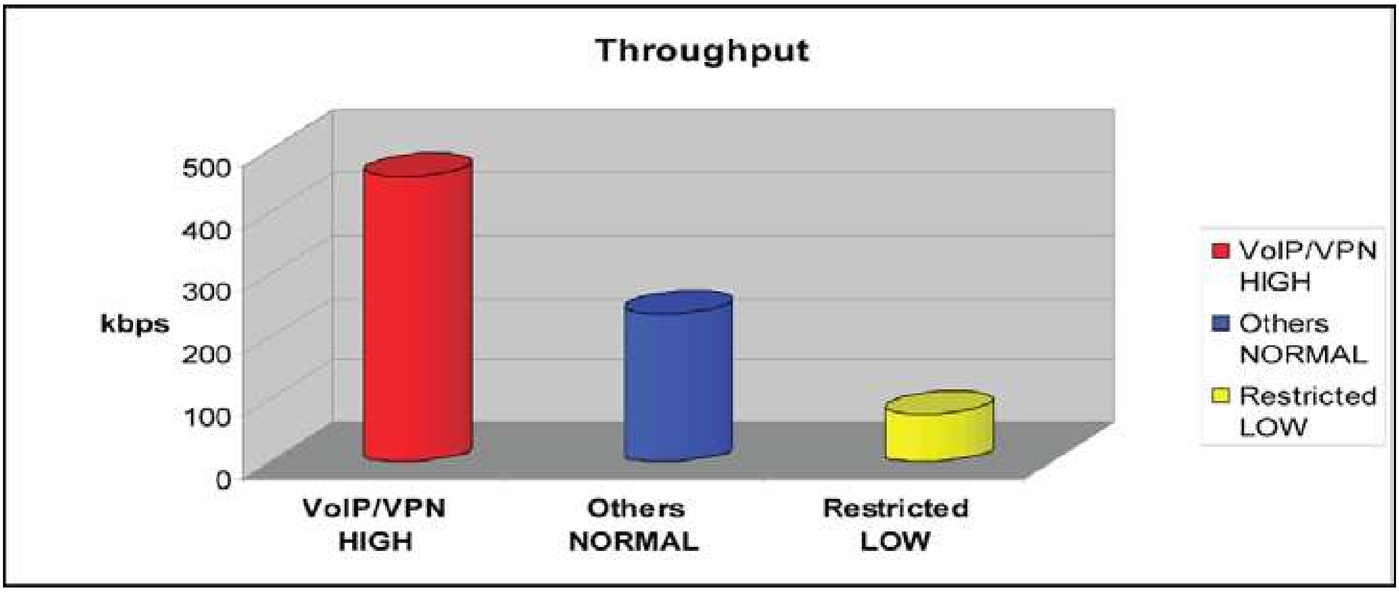
Configuration

▾ Prioritization

Configuration (from LAN to WAN packet)

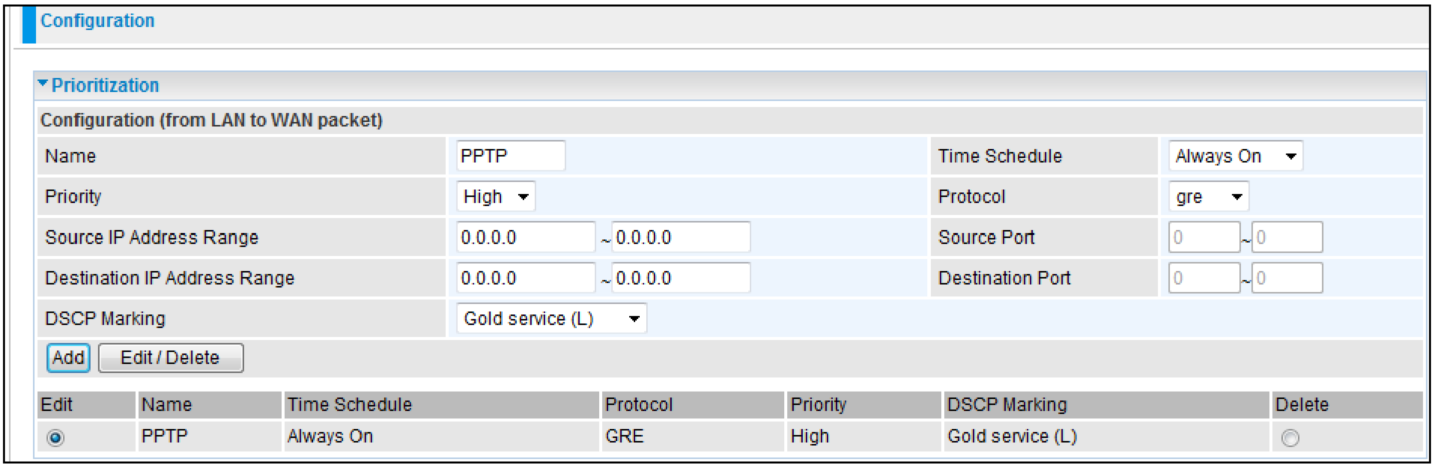
Name		Time Schedule	Always On ▾
Priority	High ▾	Protocol	any ▾
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled ▾		

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



Mission-critical application

A VPN connection is normally a mission-critical application for doing data exchange between a head office and a branch office.



Configuration (from LAN to WAN packet)

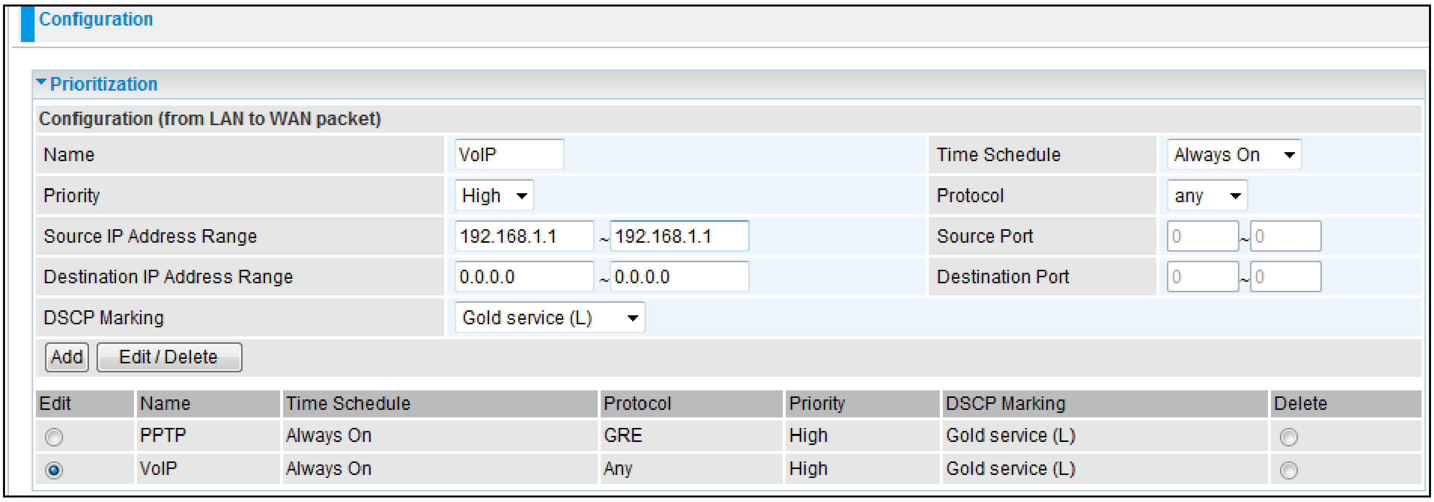
Name	PPTP	Time Schedule	Always On
Priority	High	Protocol	gre
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

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

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

Voice application

Voice is a latency-sensitive application. Most VoIP devices use SIP protocol and the port number will be assigned by SIP modules automatically. It is better to use fixed IP addresses to catch VoIP packets as high priority.



Configuration (from LAN to WAN packet)

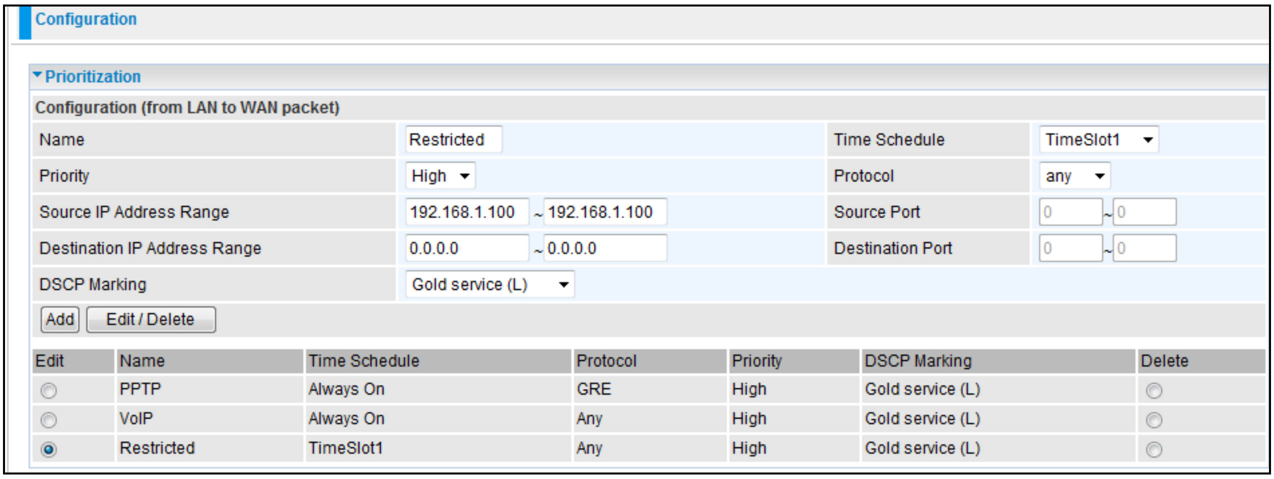
Name	VoIP	Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	192.168.1.1 ~ 192.168.1.1	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

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

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

Restricted Application

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



Configuration

Prioritization

Configuration (from LAN to WAN packet)

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

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

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

Advanced settings by using IP throttling

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

Upstream: 928kbps (29*32kbps)

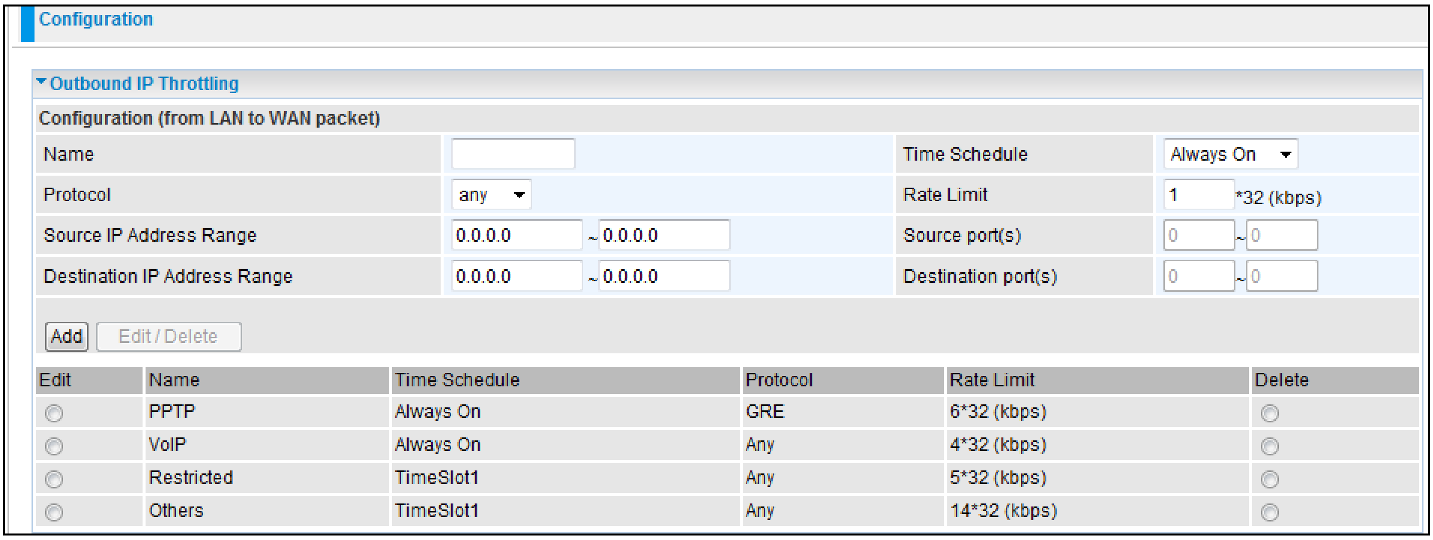
Mission-critical Application: 192kbps (6*32kbps)

Voice Application: 128kbps (4*32kbps)

Restricted Application: 160kbps (5*32kbps)

Other Applications: 448kbps (14*32kbps)

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



Configuration

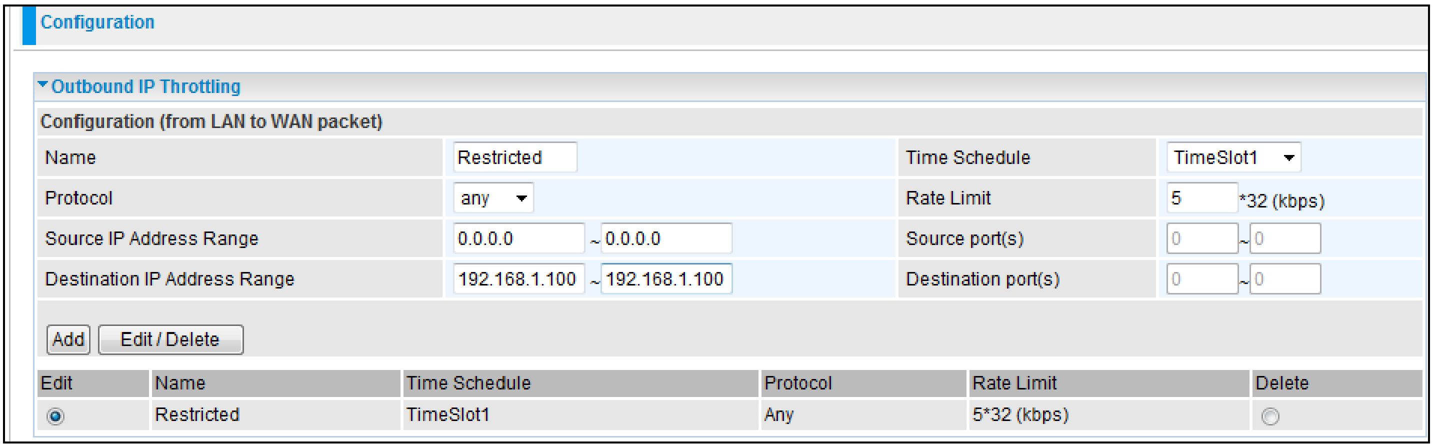
Outbound IP Throttling

Configuration (from LAN to WAN packet)

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

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
○	PPTP	Always On	GRE	6*32 (kbps)	○
○	VoIP	Always On	Any	4*32 (kbps)	○
○	Restricted	TimeSlot1	Any	5*32 (kbps)	○
○	Others	TimeSlot1	Any	14*32 (kbps)	○

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



Configuration

▾ Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name	Restricted	Time Schedule	TimeSlot1 ▾
Protocol	any ▾	Rate Limit	5 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	192.168.1.100 ~ 192.168.1.100	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
●	Restricted	TimeSlot1	Any	5*32 (kbps)	○

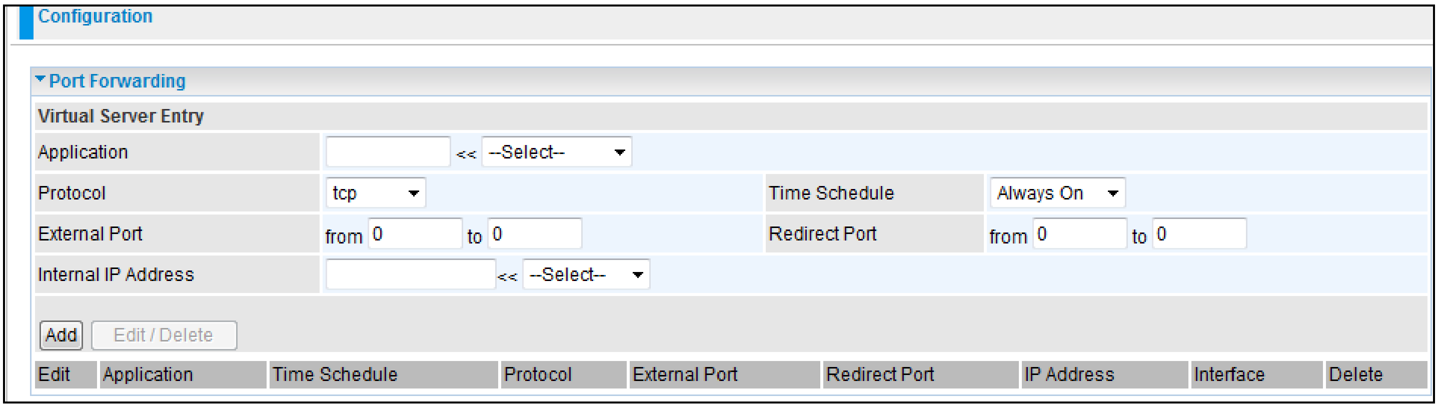
Virtual Server (known as Port Forwarding)

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

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

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

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



Configuration

▾ Port Forwarding

Virtual Server Entry

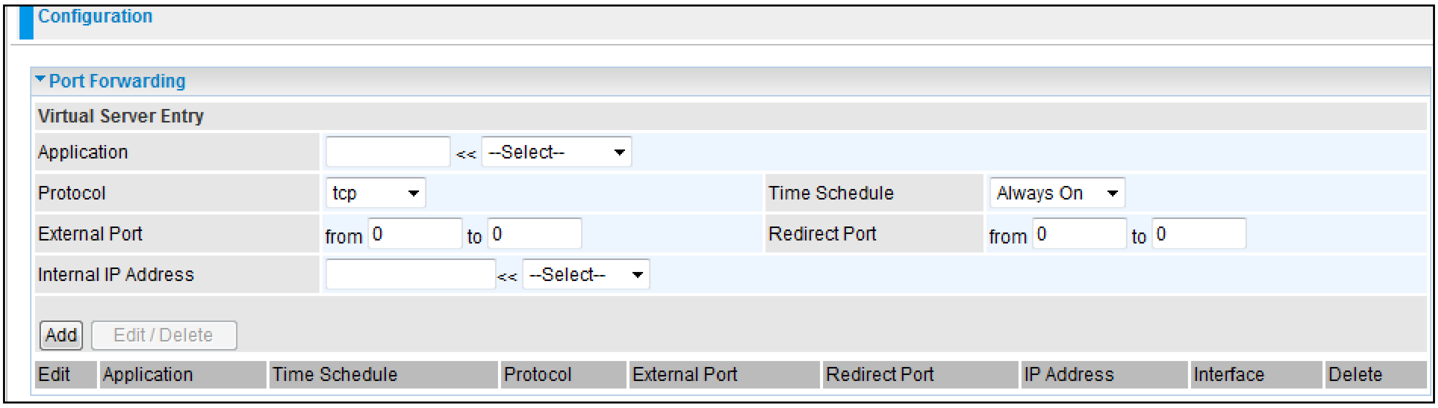
Application	<< --Select-- ▾		
Protocol	tcp ▾	Time Schedule	Always On ▾
External Port	from 0 to 0	Redirect Port	from 0 to 0
Internal IP Address	<< --Select-- ▾		

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

Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when using NAT, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

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



Configuration

Port Forwarding

Virtual Server Entry

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

Add | Edit / Delete

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

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

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

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

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

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

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

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application.
--Select-- Lists all PC’s currently connected to the network. You may assign a PC with IP address and MAC from this list.

Example:

If you would like to remotely access your Router through the Web/HTTP all the time, you will need to enable port number 80 (Web/HTTP) and map to the Router’s IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with an IP address of

10.0.0.2. Since port number 80 has already been predefined, next to the Application click on the drop down box. A window with a list of predefined rules will pop up, you can then select HTTP_Sever.

Application: *HTTP_Sever*

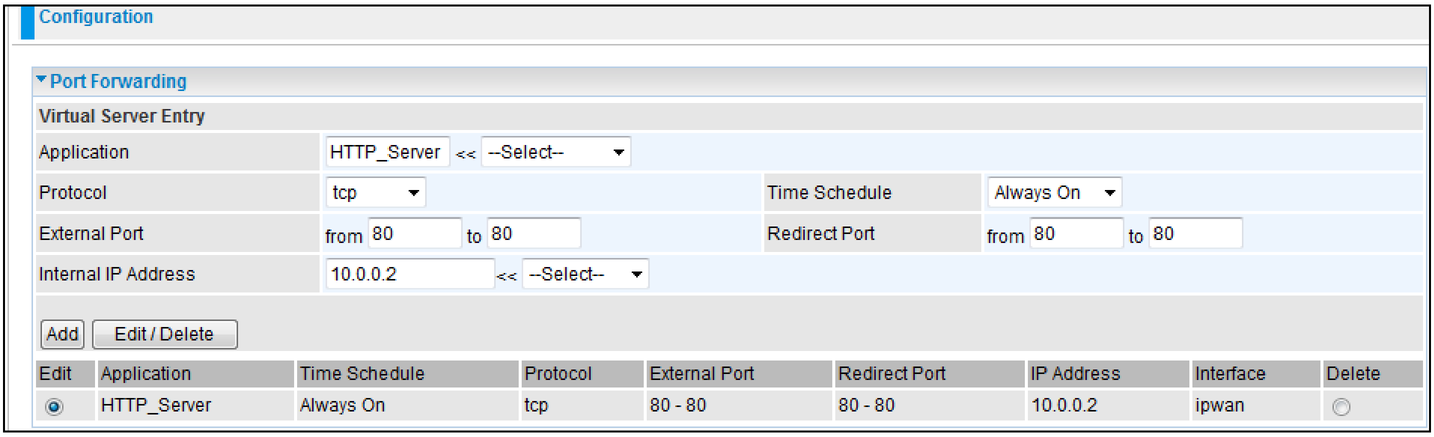
Time Schedule: *Always On*

Protocol: *tcp*

External Port: *80-80*

Redirect Port: *80-80*

IP Address: *10.0.0.2*



Configuration

▾ Port Forwarding

Virtual Server Entry

Application	HTTP_Server << --Select--		
Protocol	tcp	Time Schedule	Always On
External Port	from 80 to 80	Redirect Port	from 80 to 80
Internal IP Address	10.0.0.2 << --Select--		

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
●	HTTP_Server	Always On	tcp	80 - 80	80 - 80	10.0.0.2	ipwan	○

Add: Click it to apply your settings.

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

NOTE:

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

Attention

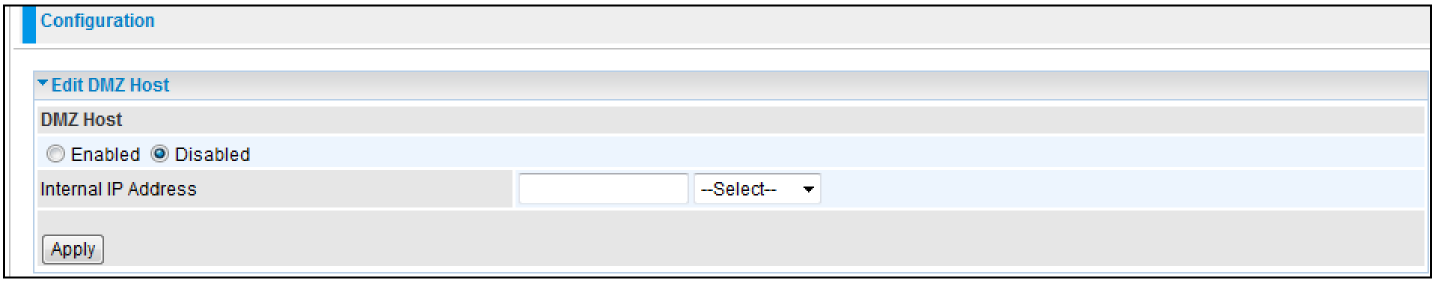
✓If you have disabled NAT in the WAN-ISP section, the Virtual Server will not function. If the DHCP option is enabled, you must be careful while assigning IP addresses to Virtual Servers in order to avoid IP conflicts. The easiest way of configuring a Virtual Server is to assign static IP addresses to each Virtual Server PC, with addresses that do not fall into the range of IP addresses reserved for DHCP. If you configure the IP address manually, be sure that it is in the same subnet.

Edit DMZ Host

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

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

Go to Configuration > Virtual Server > Edit DMZ Host



Configuration

Edit DMZ Host

DMZ Host

○ Enabled ● Disabled

Internal IP Address		--Select--

Enabled: It activates your DMZ function.

Disabled: This is the default setting, it disables the DMZ function.

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

--Select-- Lists all PC's connected to the network. You may assign a PC with an IP address from this list

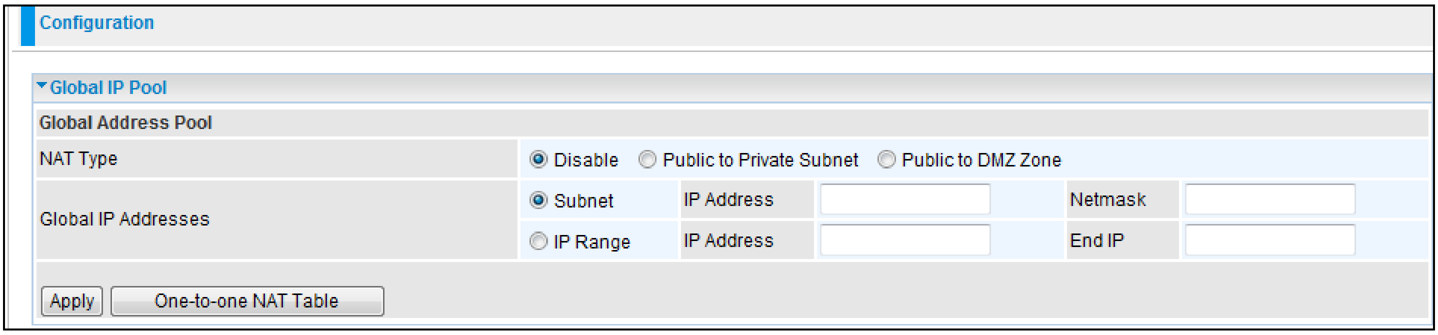
Select the Apply button to apply your changes.

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

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

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

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



Configuration

Global IP Pool

Global Address Pool

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

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

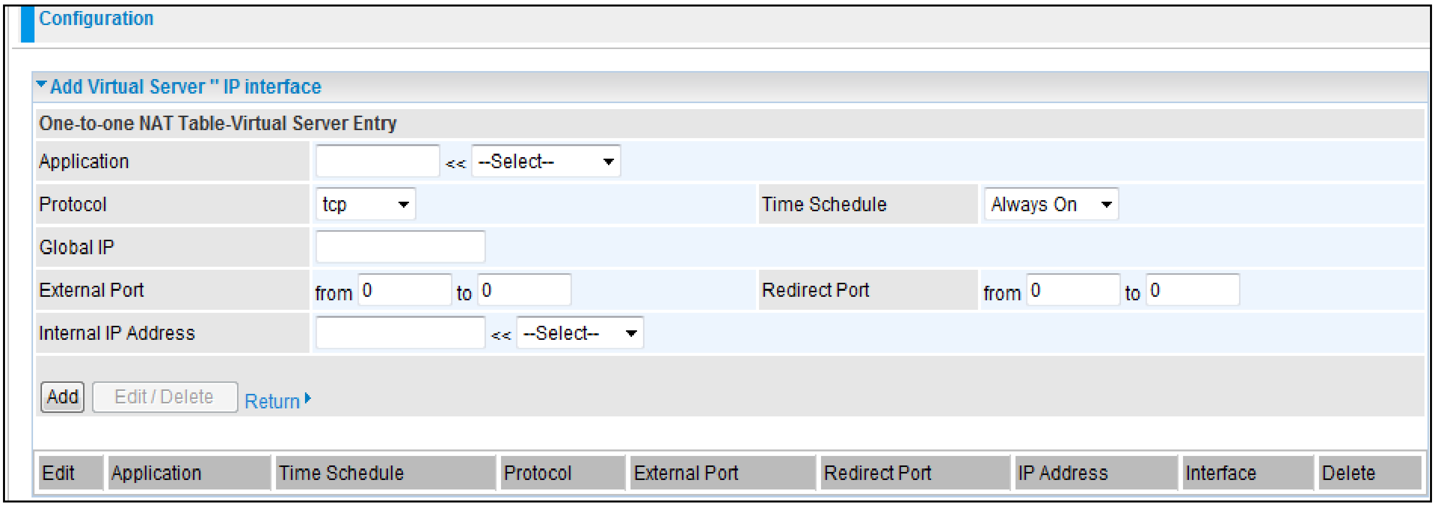
Global IP Address:

Subnet: The subnet of the public/WAN IP address given to you by your ISP. If your ISP has provided this information, you may type it in here. Otherwise, use IP Range method.

IP Range: The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP:192.168.1.10

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

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



Configuration

▾ Add Virtual Server " IP interface

One-to-one NAT Table-Virtual Server Entry

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

Add | Edit / Delete | Return ▸

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

Application: User defined description to identify this entry, or click the --Select-- drop-down menu to select a predefined rule.

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

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

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

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

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

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

Internal IP Address: The private IP in the LAN network which provides the virtual server application. --Select-- Lists all the PC’s currently connected to the network. You may assign a PC with an IP address from this list.

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

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

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

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

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

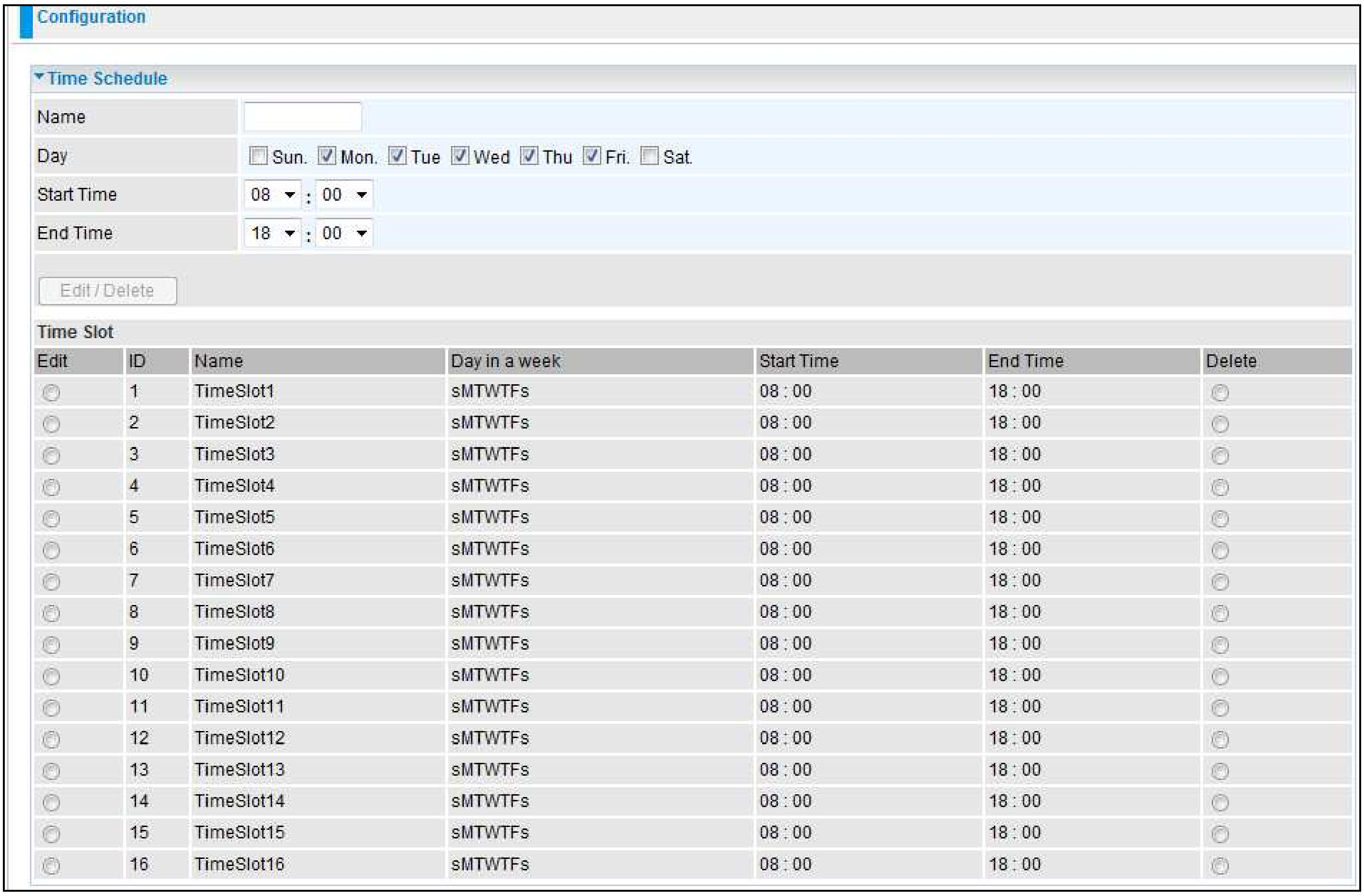
Table 5: Well-known and registered Ports

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

Time Schedule

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

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



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

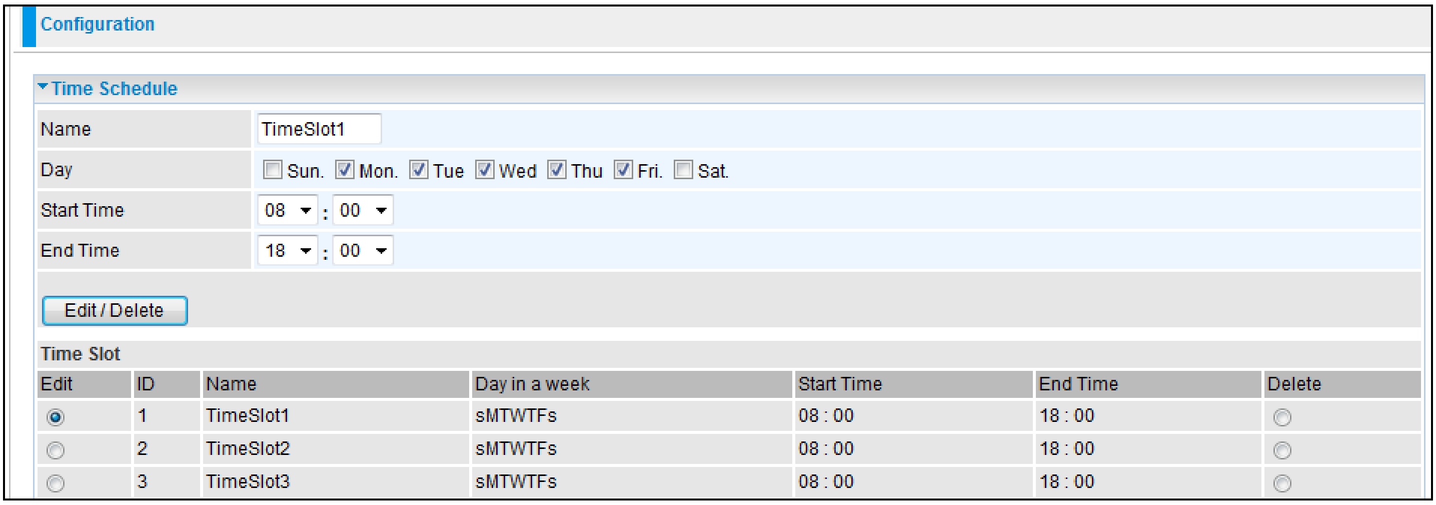
Time Slot

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

Configuration of Time Schedule

Edit a Time Slot

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



Configuration

Time Schedule

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

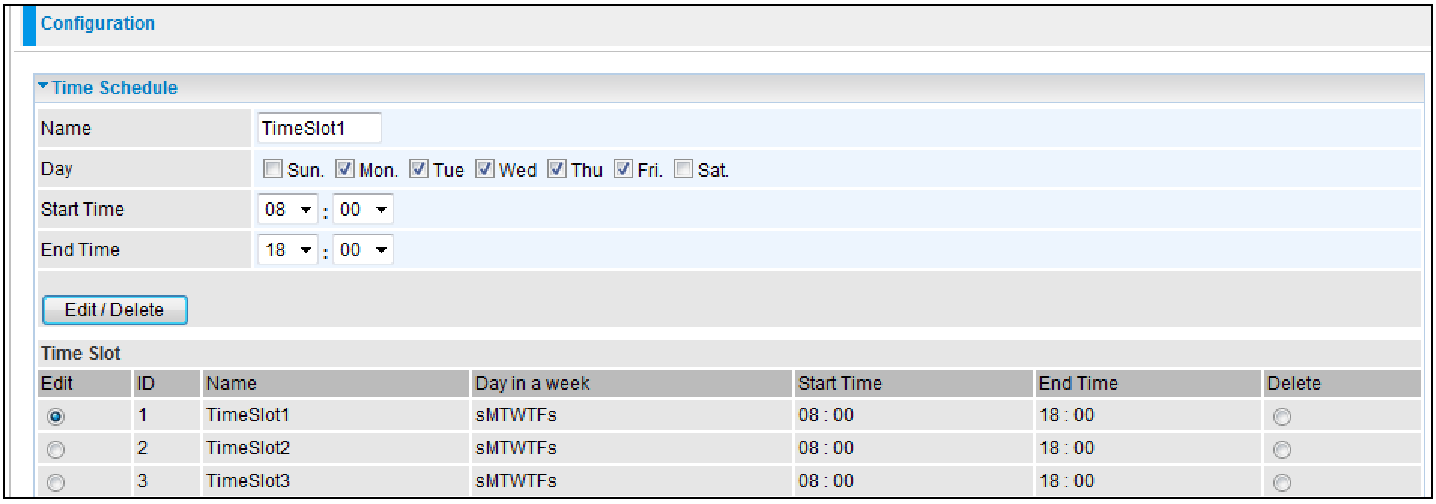
Edit / Delete

Time Slot

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

Note: Watch it carefully, the days you have selected will present in capital letter. Lower case letter shows the days that are not selected, and no rule will apply on these days.

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



Configuration

Time Schedule

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

Edit / Delete

Time Slot

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

ID: This is the index of the time slot.

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

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

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

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

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

Delete a Time Slot

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

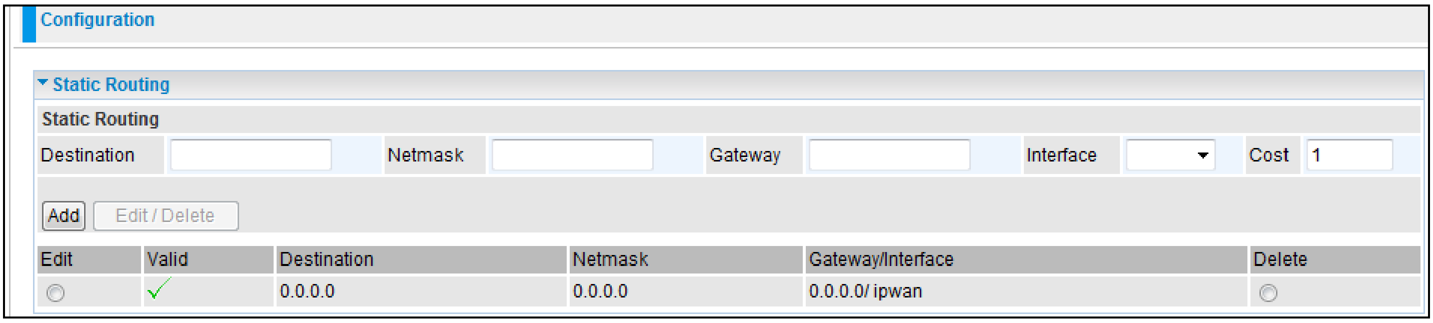
Advanced

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

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

Static Route

Go to Configuration > Advanced > Static Route.



Static Routing

Destination		Netmask		Gateway		Interface	▾	Cost	1

Edit	Valid	Destination	Netmask	Gateway/Interface	Delete
○	✓	0.0.0.0	0.0.0.0	0.0.0.0/ ipwan	○

Destination: This is the destination subnet IP address.

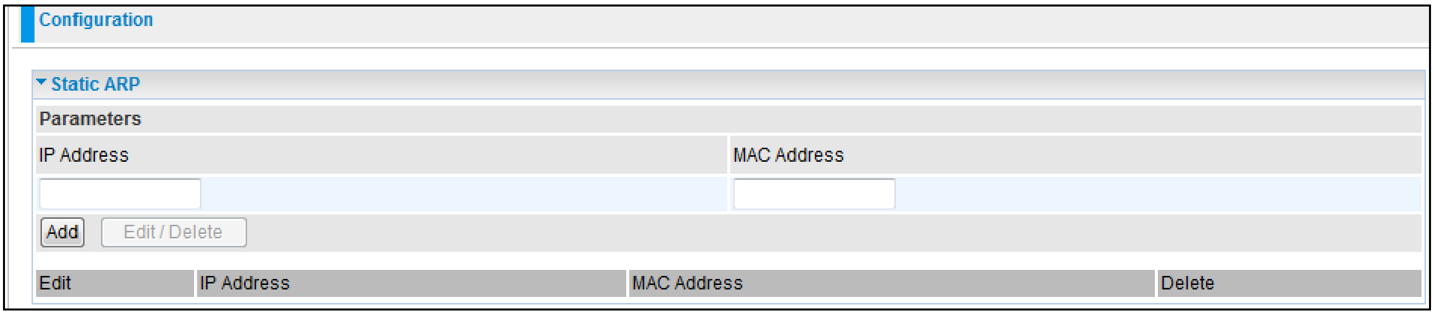
Netmask: Subnet mask of the destination IP addresses based on the above destination subnet IP.

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

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

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

Static ARP



Parameters

IP Address	MAC Address

Edit	IP Address	MAC Address	Delete

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

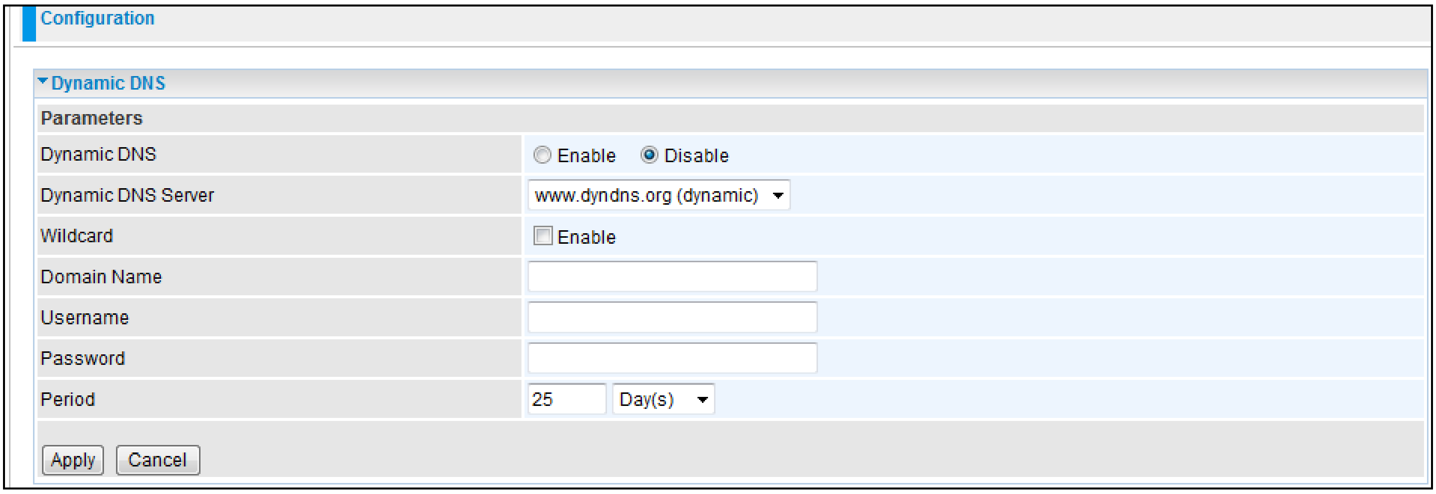
MAC Address: Fill in the MAC address of the computer that the incoming data packets should be forwarded to.

Dynamic DNS

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

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

There are more than 5 DDNS services supported.



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

Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

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

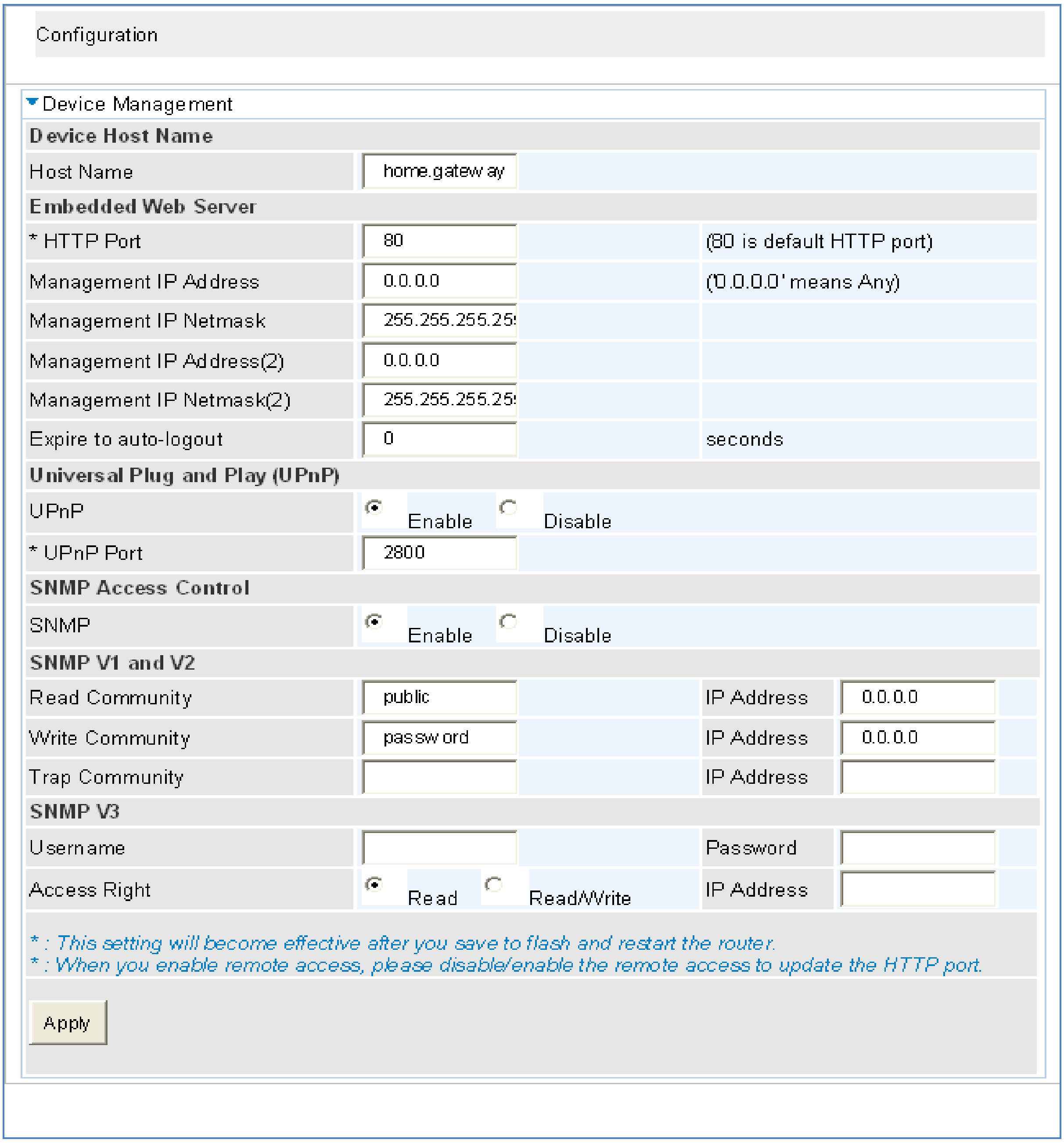
Dynamic DNS Server: Select the DDNS service you have established an account with.

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

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

Device Management

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



Configuration

▾ Device Management

Device Host Name			
Host Name	home.gateway		
Embedded Web Server			
* HTTP Port	80	(80 is default HTTP port)	
Management IP Address	0.0.0.0	('0.0.0.0' means Any)	
Management IP Netmask	255.255.255.25		
Management IP Address(2)	0.0.0.0		
Management IP Netmask(2)	255.255.255.25		
Expire to auto-logout	0	seconds	
Universal Plug and Play (UPnP)			
UPnP	● Enable ○ Disable		
* UPnP Port	2800		
SNMP Access Control			
SNMP	● Enable ○ Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	● Read ○ Read/Write	IP Address	

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

Device Host Name

Host Name: Assign it a name.

Note: The Host Name must have more than one word. These two words should be separated bya '.' period in between.

Example:

Host Name: homegateway ==> Incorrect

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

Embedded Web Server (2 Management IP Accounts)

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

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

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

For Example:

User A changes the HTTP port number to 100, specifies their own IP address as 192.168.1.55 and sets the logout time as 100 seconds. The router will only allow User A to access the Web GUI from the IP address 192.168.1.55 by typing http://10.0.0.2:100 in their web browser. Nevertheless, after 100 seconds the device will automatically log User A out of the system.

Universal Plug and Play (UPnP)

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

Both operating system and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed) while Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to gain support for UPnP. Nevertheless Windows 2000 does not support UPnP.

Disable: Check to disable the router's UPnP functionality.

Enable: Check to enable the router's UPnP functionality.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value is conflicting with other ports, you may change the port.

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

SNMP V1 and V2:

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

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

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

SNMP V3: Specify a name and password for authentication and define the access rights from an identified IP address. Once the authentication has succeeded, users with this IP address will be able to view and modify the data.

<u>SNMP Version: SNMPv2c and SNMPv3</u>

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

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

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II)

System group

System group

Interface group

Address Translation group

IP group

ICMP Group

TCP group

UDP group

EGP (not applicable) Transmission

SNMP group

From RFC 1650 (EtherLike-MIB)

dot3stats

From RFC 1493 (Bridge MIB)

dot1 dBase group

dot1 dTp group

dot1 dStp group (if configured as span- ning tree)

From RFC 1472 (PPP/Security MIB)

PPP security group

From RFC 1473 (PPP/IP MIB)

PPP IP group

From RFC 1474 (PPP/Bridge MIB)

PPP Bridge group

From RFC 1573 (IfMIB)

ifMIBObjects group

From RFC 1695 (atmMIB)

atmMIBObjects

From RFC 1907 (SNMPv2)

only snmpSetSerialNo OID

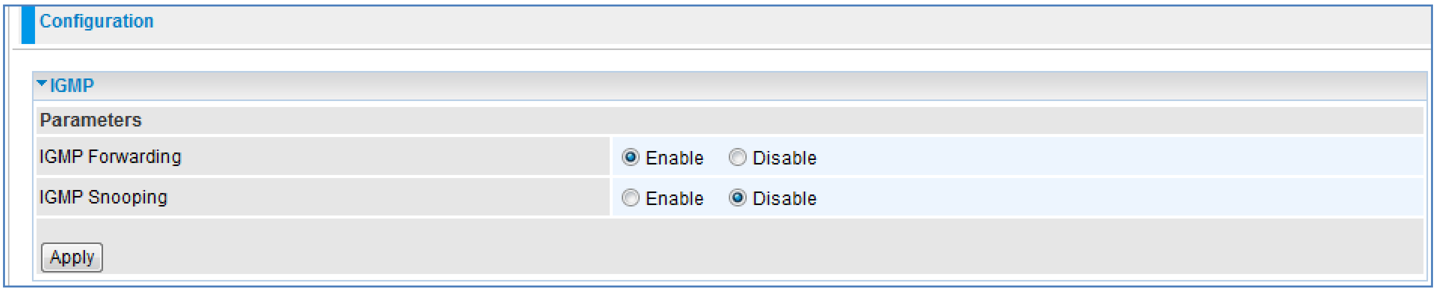
From RFC 1471 (PPP/LCP MIB)

pppLink group

pppLgr group (not applicable)

IGMP

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



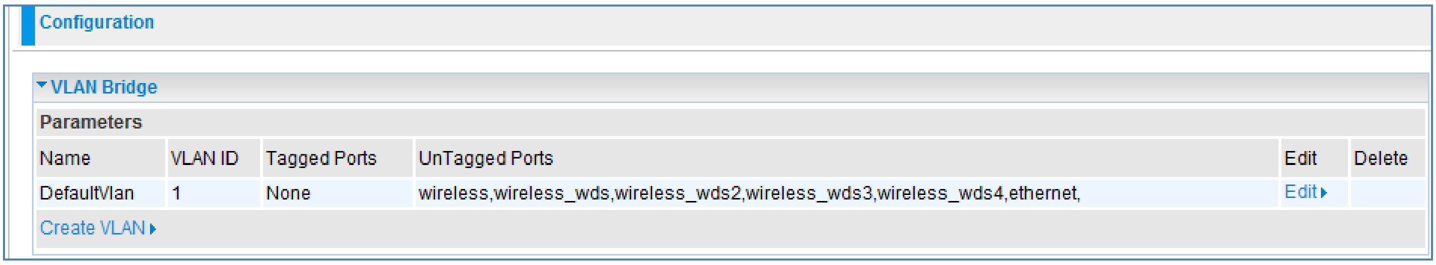
Parameters	
IGMP Forwarding	● Enable ○ Disable
IGMP Snooping	○ Enable ● Disable

IGMP Forwarding: Accepting multicast packets. Default is set to ‘Enable’.

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

VLAN Bridge

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



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

Edit: Edit your member ports in the selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

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

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

Chapter 5: Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting the Help desk .

Problems with the router

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

Problems with WAN interface

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

Problem with LAN interface

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

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

Contact Telkom ADSL Support

Telephone:	**0800 375 375**
Operating Hours:	**24hrs – 7 days a week**

Contact Modem Support

Telephone:	**0860 110 041**
Website:	**www.sizwebroadband.co.za**
Operating Hours:	**8:00am to 17:00pm (Mon – Fri only)**