



BiPAC 7404V(G)PX

**3G/VoIP/(802.11g)
ADSL2+ (VPN) Firewall Router**

User Manual

Version release:1.09(5.53.s6.b1.dg8)

Last Revised Date: 03-02-2010

Table of Contents

Chapter 1: Introduction	1
Chapter 2: Installing the Router	5
Package Contents	5
The Front LEDs	6
The Rear Ports	7
Cabling	8
Chapter 3: Basic Installation	9
Connecting Your Router	10
Network Configuration	11
Configuring PC in windows 7	11
Configuring PC in Windows Vista	13
Configuring PC in Windows XP	15
Configuring PC in Windows 2000	16
Configuring PC in Windows 95/98/Me	17
Configuring PC in Windows NT4.0	18
Factory Default Settings	19
Information from your ISP	20
Configuring with your Web Browser	21
Chapter 4: Configuration	22
Status	23
ADSL Status	23
3G Status	23
EWAN Status	24
iBurst Status	25
ARP Table	25
DHCP Table	26
Routing Table	28
NAT Sessions	29
UPnP Portmap	29
PPTP Status	30
IPSec Status	31
L2TP Status	31
VoIP Status	32
VoIP Call Log	32
Event Log	33
Error Log	34
Diagnostic	34
Quick Start	35
Configuration	40
LAN - Local Area Network	41
Bridge Interface	41
Ethernet	42
IP Alias	42
Ethernet Client Filter	43

Wireless	45
Wireless Security	47
Wireless Client / MAC Address Filter	50
WPS	51
Port Setting	60
DHCP Server	61
WAN - Wide Area Network	62
WAN Interface	62
WAN Profile	65
ADSL Mode	81
System	82
Time Zone	82
Remote Access	83
Firmware Upgrade	83
Backup / Restore	84
Restart Router	85
User Management	86
Mail Alert	88
Firewall and Access Control	90
General Settings	91
Packet Filter	92
Intrusion Detection	100
URL Filter	103
IM / P2P Blocking	106
Firewall Log	107
VPN - Virtual Private Networks	108
PPTP (Point-to-Point Tunneling Protocol)	108
IPSec (IP Security Protocol)	117
L2TP (Layer Two Tunneling Protocol)	127
VoIP - Voice over Internet Protocol	139
SIP Device Parameters	140
SIP Accounts	143
Phone Port	144
PSTN Dial Plan (Router with LINE port only)	146
VoIP Dial Plan	150
Call Feature	153
Speed Dial	153
Ring & Tone	154
QoS - Quality of Service	156
Prioritization	156
Outbound IP Throttling (LAN to WAN)	157
Inbound IP Throttling (WAN to LAN)	159
Virtual Server (known as Port Forwarding)	165
Porting Forwarding	166
Edit DMZ Host	168
Edit One-to-One NAT (Network Address Translation)	169
Wake on LAN	172

Time Schedule	173
Advanced	176
Static Route	176
Static ARP	177
Dynamic DNS	178
Device Management.....	179
IGMP	183
VLAN Bridge	183
Logout	184
Chapter 5: Troubleshooting.....	185
Appendix: Product Support & Contact	187

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

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.

EWAN

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

Dual WAN

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

802.11g Wireless AP with WPA Support (Wireless Router only)

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 Wi-Fi Protected Access

(WPA-PSK and WPA2-PSK) and Wired Equivalent Privacy (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 over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA (RFC1577) to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing.

Quick Installation Wizard

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

Universal Plug and Play (UPnP) and UPnP NAT Traversal

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

Network Address Translation (NAT)

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

SOHO Firewall Security with DoS and SPI

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

Domain Name System (DNS) Relay

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

Dynamic Domain Name System (DDNS)

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

Quality of Service (QoS)

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router 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) (BiPAC 7404V(G)OX only)

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

Chapter 2: Installing the Router

Important note for using this router



Warning

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



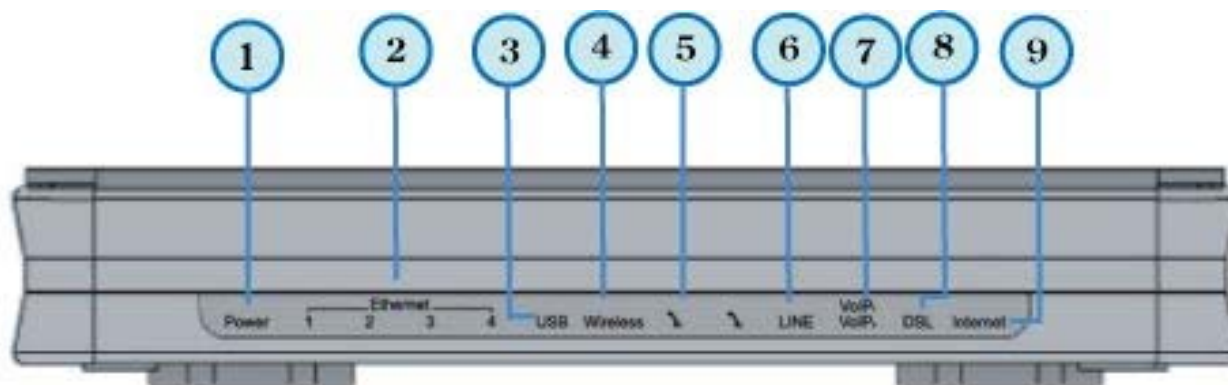
Attention

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

Package Contents

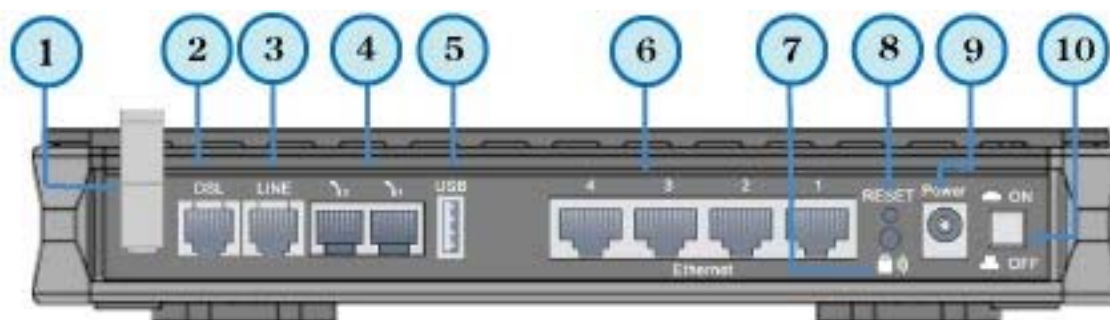
- 3G/VoIP/(802.11g) ADSL2+ (VPN) Firewall Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5) Cable
- Console kit
- Power adapter
- A detachable antenna
- Quick Start Guide

The Front LEDs.



LED		Meaning
1	Power	Lit when power is ON. Lit red means system failure. Restart the device or contact Billion for support.
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 hits 100Mbps; Lit orange when the speed of transmission hits 10Mbps. Blink when data is being Transmitted / Received.
3	USB	Lit when the router is connected to a USB device. Flash when data is received / transmitted.
4	Wireless	Lit green when a wireless connection is established. Flash when the device is sending/receiving data. Flash once per second while Wi-Fi protected setup is in progress.
5	Phone 1x-2x (RJ-11 connector)	Lit green when phone is off hook.
6	Line (Router with LINE port only)	Lit when the inbound and outbound calls are transmitted through PSTN.
7	VoIP 1x-2x (RJ-11 connector)	After SIP registration is OK, the LED will lit green whenever phone 1 is off hook but will lit orange for phone 2. Note: Orange light also means when both Phone 1 and 2 are registered OK 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



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

Port		Meaning
1	Antenna (Wireless Router only)	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 (Router with LINE port only)	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 analog 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 be either a LAN or Console port at a time but not both.
7	WPS	Push WPS button to trigger Wi-Fi Protected Setup function.
8	RESET	To be sure the device is being turned on press RESET button for: 1-3 seconds: quick reset the device. 6 seconds and above, power off, power on the device: restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.
9	Power	Connect it with the supplied power adapter.
10	Power Switch	Power ON/OFF switch

Cabling

One of the most common causes of problem 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.

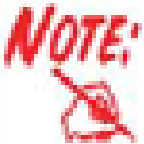
Chapter 3: Basic Installation

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 ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.1.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

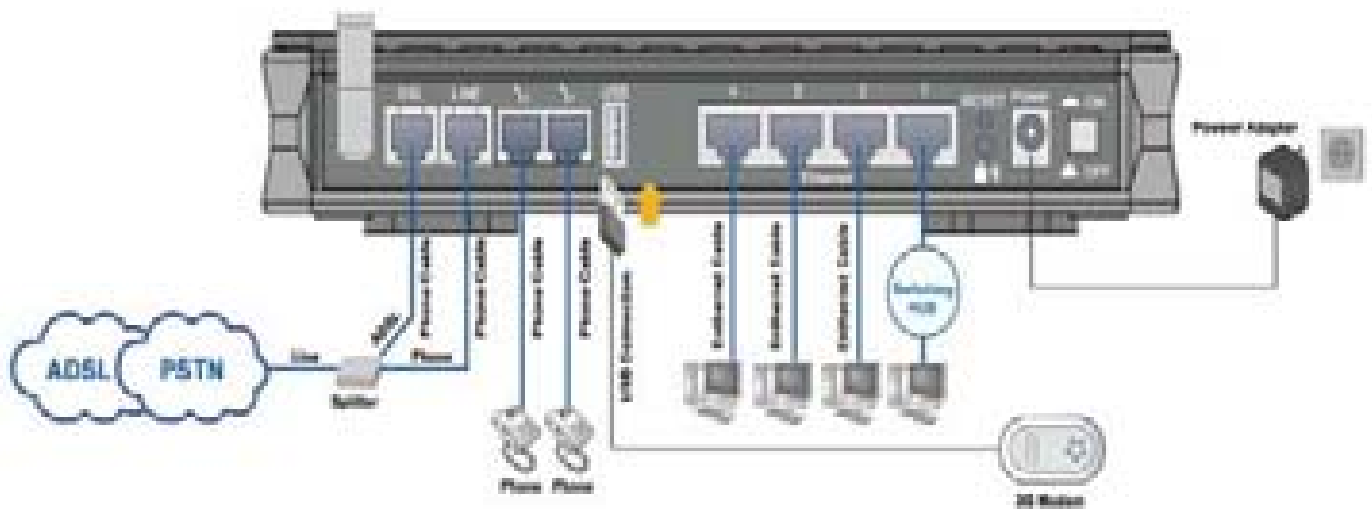
Please follow the following steps to configure your PC network environment.



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

Connecting Your Router

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

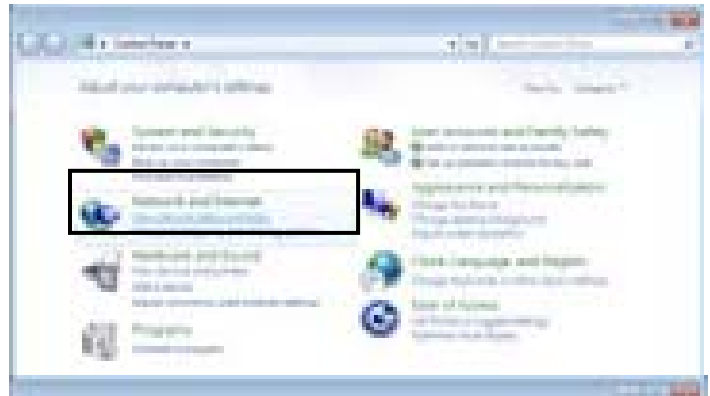


Network Configuration

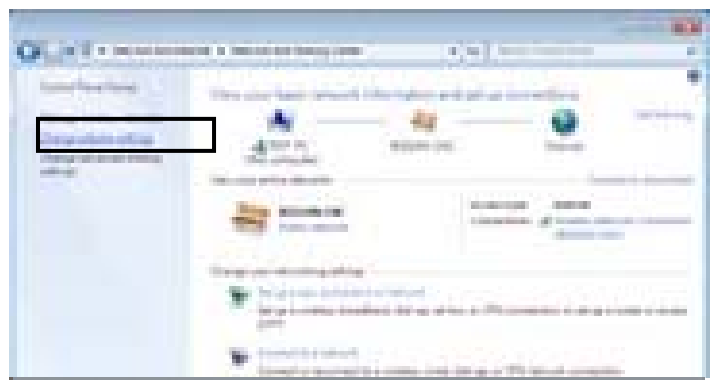
Configuring PC in windows 7

1. Go to Start. Click on Control Panel.

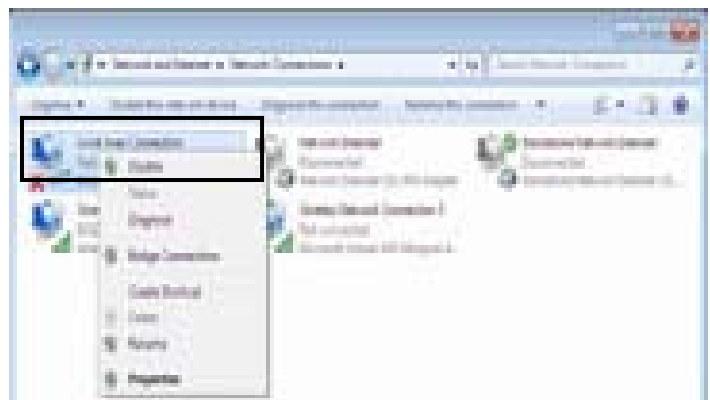
Then click on Network and Internet.



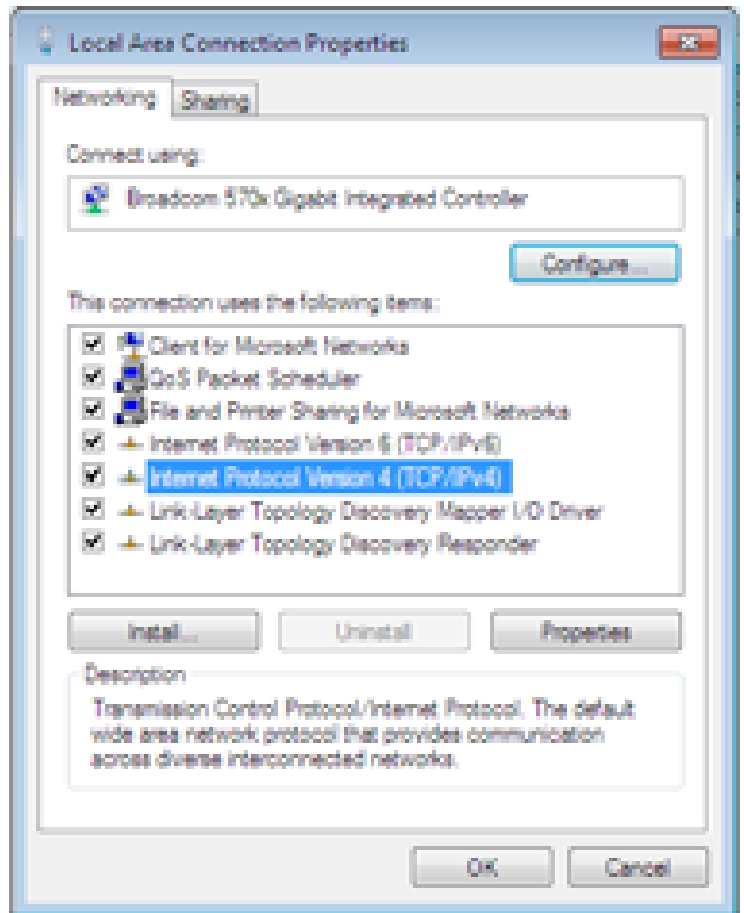
2. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.



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



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



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

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

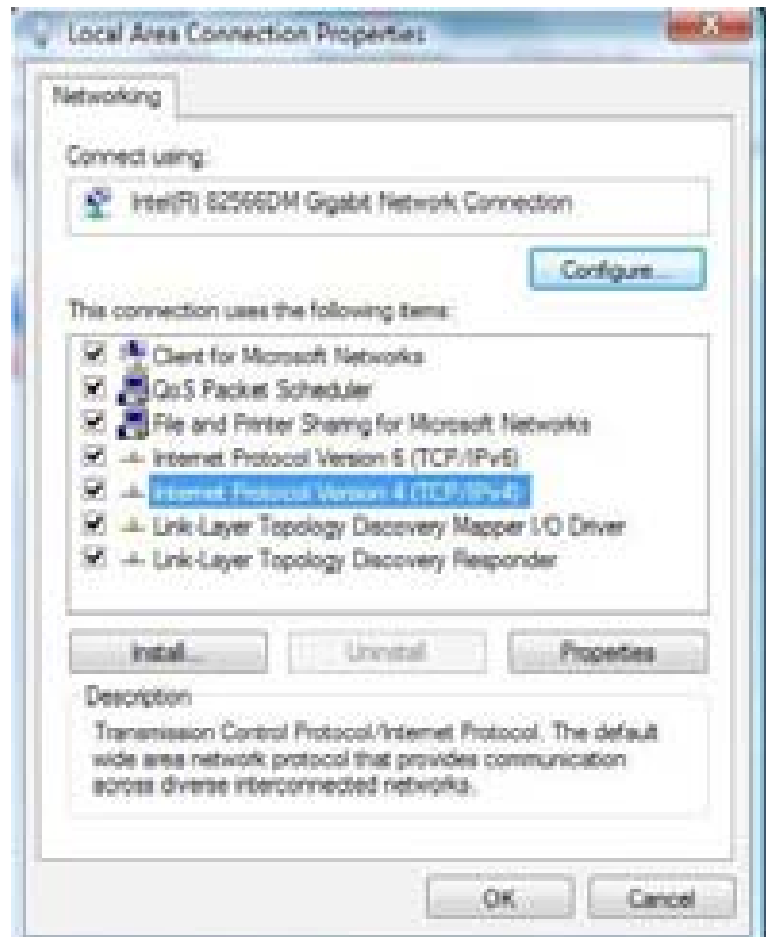


Configuring PC in Windows Vista

1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.
4. Select the Local Area Connection, and right click the icon to select Properties.



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

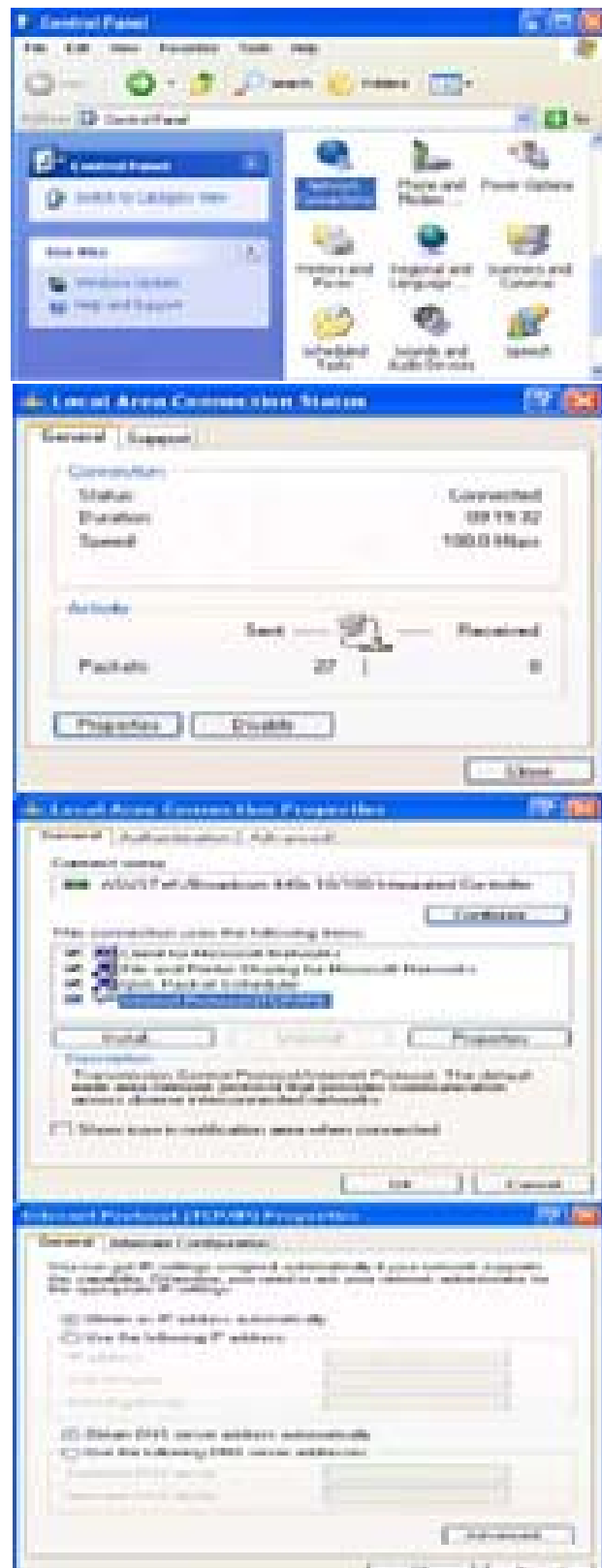


6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.
7. Click OK again in the Local Area Connection Properties window to apply the new configuration.



Configuring PC in Windows XP

1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.
3. In the Local Area Connection Status window, click Properties.
4. Select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.



Configuring PC in Windows 2000

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

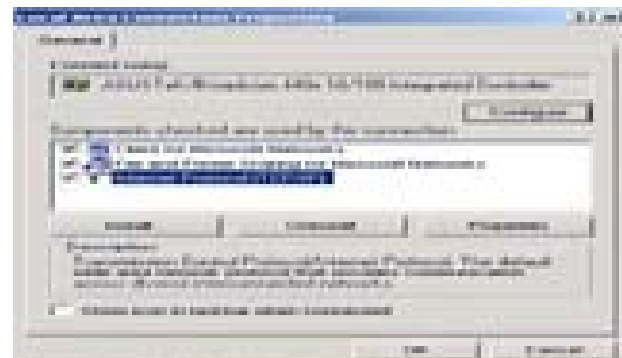
2. Double-click Local Area Connection.



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

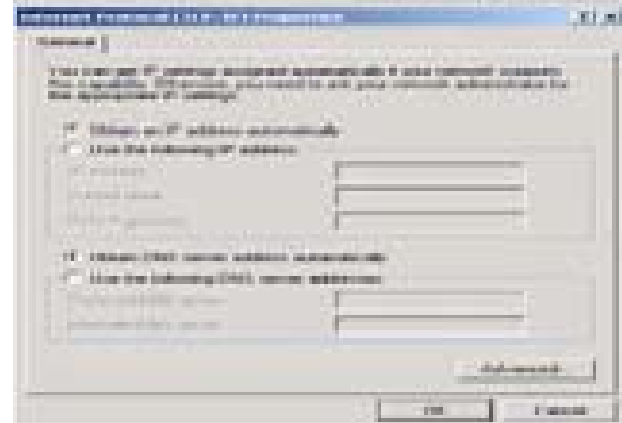


4. Select Internet Protocol (TCP/IP) and click Properties.



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

6. Click OK to finish the configuration.



Configuring PC in Windows 95/98/Me

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.
3. Select the Obtain an IP address automatically radio button.
4. Then select the DNS Configuration tab.
5. Select the Disable DNS radio button and click OK to finish the configuration.



Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.
3. Select the Obtain an IP address from a DHCP server radio button and click OK.



Factory Default Settings

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

Web Interface (Username and Password)

- ▶ Username: admin
- ▶ Password: admin



Attention

If you ever forget the login password, please press the reset button for more than 5 seconds to restore the factory default setting.

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

Device LAN IP settings

- ▶ IP Address: 192.168.1.254
- ▶ Subnet Mask: 255.255.255.0

ISP setting in WAN site

- ▶ PPPoE

DHCP server

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

LAN and WAN Port Addresses

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

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

Information from your ISP

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

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

PPPoE(RFC2516)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoA(RFC2364)	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
MPoA(RFC1483/ RFC2684)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA(RFC1577)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
Pure Bridge	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a user name and password window prompt will appear. The default username and password are “admin” and “admin” respectively. (See Figure 3.14)

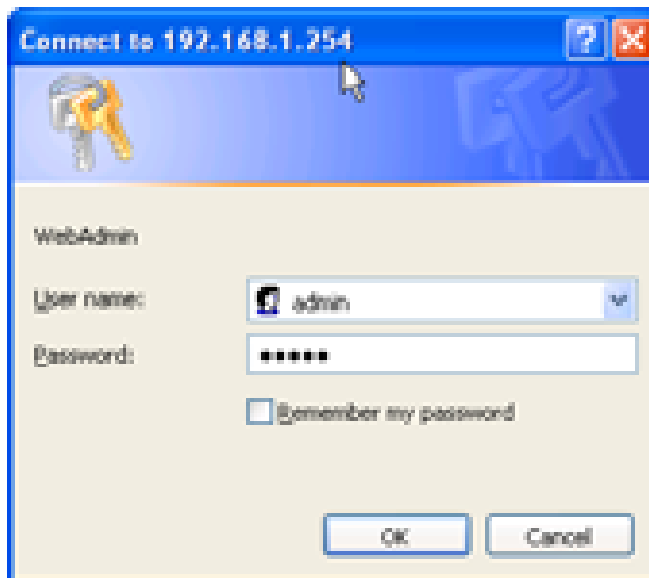


Figure 3.14: User name & Password Prompt Window

Congratulations! You are now successfully logon to the 3G/VoIP/(802.11g) ADSL2+ (VPN) Firewall Router!

Chapter 4: Configuration

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

Status

- ADSL Table
- 3G Status
- EWAN Status
- iBurst Status
- ARP Table
- DHCP Table
- Routing Table
- NAT Sessions
- UPnP Pormap
- PPTP Status
- IPSec Status
- L2TP Status
- VoIP Status
- VoIP Call Log
- Event Log
- Error Log
- Diagnostic

Quick Start

Configuration

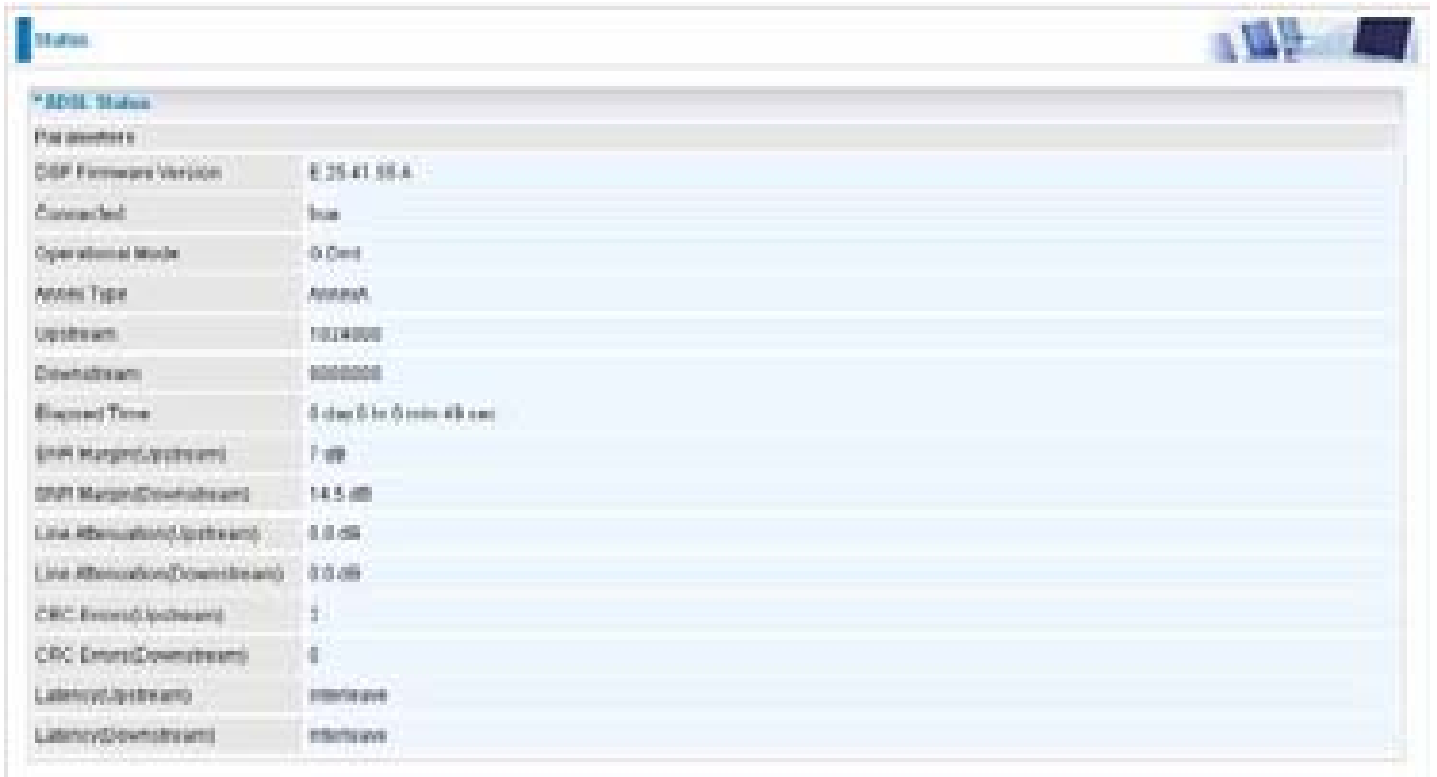
- LAN
- WAN
- System
- Firewall
- VPN
- VoIP
- QoS
- Virtual Server
- Wake on LAN
- Time Schedule
- Advanced

Language (provides user interface in English and French languages)

Status

ADSL Status

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

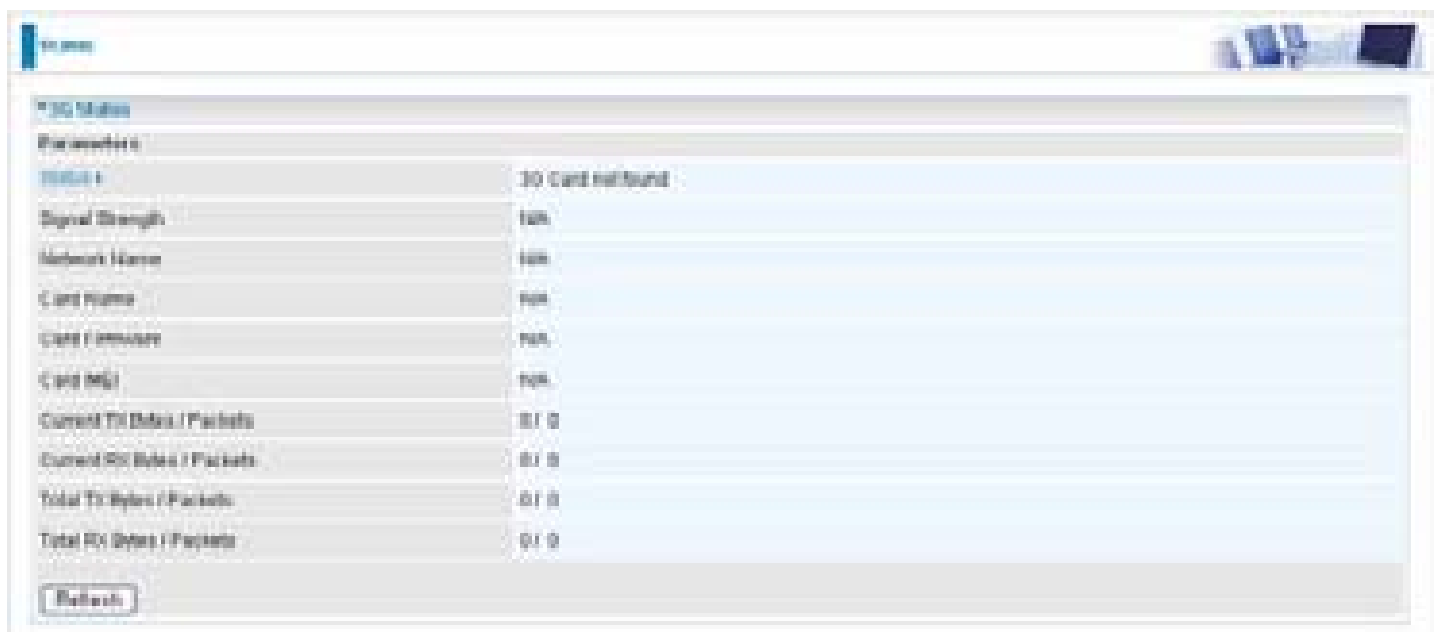


The screenshot shows the ADSL Status page with a table of parameters. The table has two columns: Parameter and Value. The parameters include DSP Firmware Version, Connected status, Operational Mode, Access Type, Upstream and Downstream rates, Elapsed Time, and various error and latency metrics.

Parameter	Value
DSP Firmware Version	E 25.41 98.4
Connected	Yes
Operational Mode	0 Cont
Access Type	Asynchronous
Upstream	1024000
Downstream	8000000
Elapsed Time	0 day 0 hr 0 min 00 sec
SNR Margin(Upstream)	7.0dB
SNR Margin(Downstream)	14.5 dB
Line Attenuation(Upstream)	0.0 dB
Line Attenuation(Downstream)	0.0 dB
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	Milliseconds
Latency(Downstream)	Milliseconds

3G Status

This section displays the 3G Card's overall status, which shows you a number of helpful information such as the current signal strength and statistics on current and total bytes transferred and received.



The screenshot shows the 3G Status page with a table of parameters. The table has two columns: Parameter and Value. The parameters include Signal Strength, Network Name, Card Name, Card Firmware, Card IMEI, and statistics for current and total TX and RX bytes and packets. A Refresh button is located at the bottom left.

Parameter	Value
Signal Strength	100%
Network Name	3G
Card Name	3G
Card Firmware	3G
Card IMEI	3G
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 current 3G signal strength.

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

Card Name: The name of the 3G card.

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

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

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

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

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

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

EWAN Status

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



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

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

iBurst Status

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



iBurst Status	
Parameters	
Version	1.00
Port Class (Ethernet)	true
Modem Attached	false
Connecting	none
Card Name	FGA
Signal Strength	100
Status	iBurst Card not found
MAC	00:0E:0C:00:04:50
To Error Packets	0
Rx Error Packets	0
Current Tx Bytes / Packets	0 / 0
Current Rx Bytes / Packets	0 / 0
Total Tx Bytes / Packets	0 / 0
Total Rx Bytes / Packets	0 / 0

Refresh

ARP Table

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



ARP Table			
Wireless			
IP Address	MAC Address	Interface	Status
192.168.1.110	18:00:00:00:04:50	igmp	no
Wired			
IP Address	MAC		

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

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

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

Static: Static status of the ARP table entry:

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

DHCP Table



DHCP Table		
Type		
Leased	Expired	Permanent

Leased: The DHCP assigned IP addresses information.

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information.

Leased Table

Leased Table			
IP ADDRESS	MAC ADDRESS	CLIENT HOST NAME	Expiry
192.168.1.100	00:0C:29:11:00:00	lanwin100	11 Hours

IP Address: The IP address that assigned to client.

MAC Address: The MAC address of client.

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

Expiry: The current lease time of client.

Routing Table



The screenshot shows a network configuration interface with two routing tables. The first table is titled 'Routing Table' and has columns for 'Valid', 'Destination', 'Netmask', 'Gateway/Interface', and 'Cost'. It contains one entry with a checkmark in the 'Valid' column, '0.0.0.0' in 'Destination', '0.0.0.0' in 'Netmask', '0.0.0.0/0.0.0.0' in 'Gateway/Interface', and '1' in 'Cost'. The second table is titled 'RIP Routing Table' and has columns for 'Destination', 'Netmask', 'Gateway', and 'Cost'. It contains one entry with '0.0.0.0' in 'Destination', '0.0.0.0' in 'Netmask', '0.0.0.0' in 'Gateway', and '1' in 'Cost'.

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

Destination	Netmask	Gateway	Cost
0.0.0.0	0.0.0.0	0.0.0.0	1

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination Netmask address.

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

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

RIP Routing Table

Destination: The IP address of the destination network.

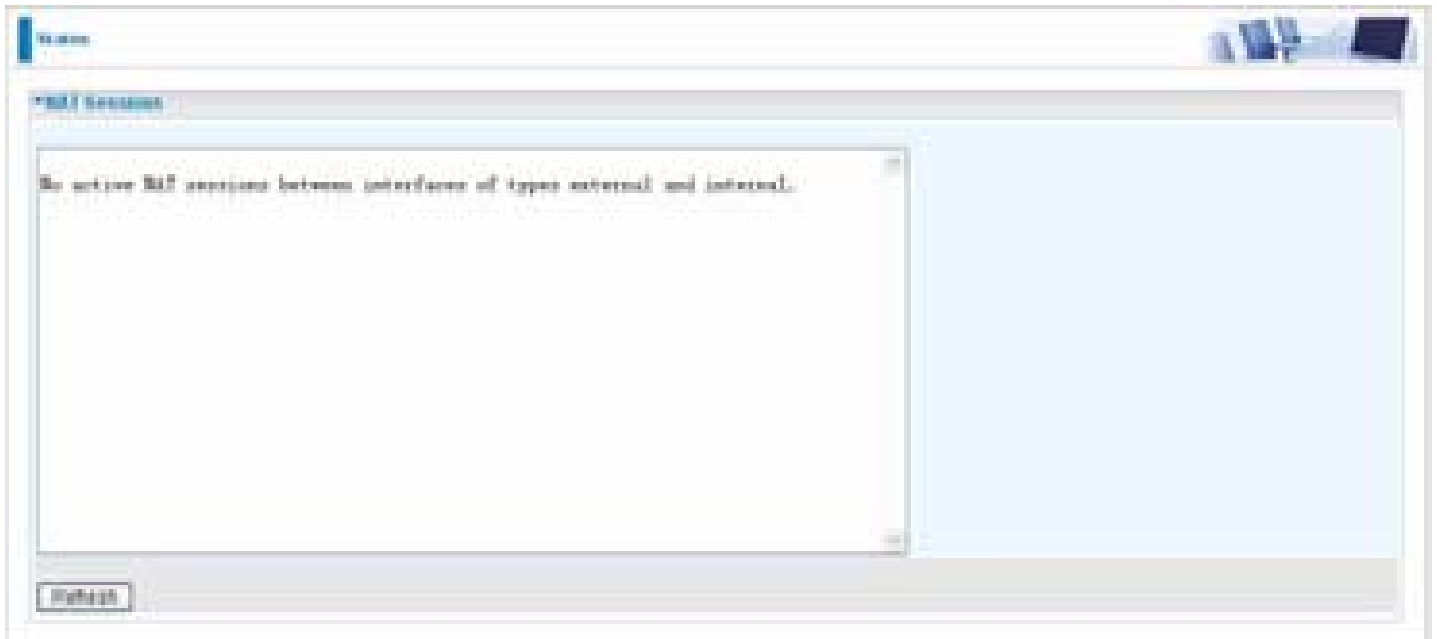
Netmask: The destination Netmask address.

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

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

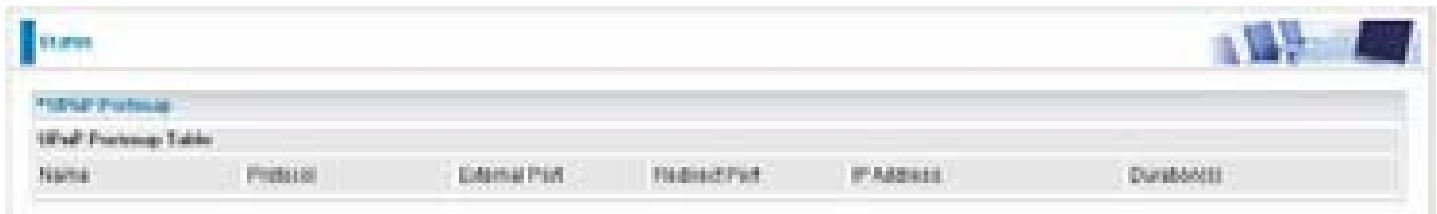
NAT Sessions

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



UPnP Portmap

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



PPTP Status

This shows details of your configured PPTP VPN Connections.



The screenshot shows a web-based interface with a header bar containing a logo and navigation icons. Below the header, there are two sections, each containing a table of PPTP connections. The first section is titled "PPTP Status" and "PPTP for Remote Access Application". The second section is titled "PPTP for L2M to L2M Application". Both tables have the same columns: Name, Type, Enable, Active, Tunnel Connected, Call Connected, and Encryption. The tables are currently empty.

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

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

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

Tunnel Connected: Whether the VPN Tunnel is currently connected.

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

Encryption: The encryption type used for this VPN connection.

IPSec Status

This shows details of your configured IPSec VPN Connections.



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

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

Active: Whether the VPN Connection is currently Active.

Connection State: Whether the VPN is Connected or Disconnected.

Statistics: Statistics for this VPN Connection.

Local Subnet: The local IP Address or Subnet used.

Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

L2TP Status

This shows details of your configured L2TP VPN Connections.



Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption
------	------	--------	--------	------------------	----------------	------------

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption
------	------	--------	--------	------------------	----------------	------------

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

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

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

Tunnel Connected: Whether the VPN Tunnel is currently connected.

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

Encryption: The encryption type used for this VPN connection.

VoIP Status

This table shows the status of the phone ports after they are being used for the VoIP feature. It will display some information such as domain name, display name & phone number of the VoIP device.

Index	Phone Number	User Domain/Realm	Display Name	Registered
1		voip.infomode.com.nat		unknown
2		voip.infomode.com.nat		unknown

VoIP Call Log

Index	Date & Time	Phone Number	Start Time	End Time	Duration
[Empty Row]					

Index	Date & Time	Phone Number	Start Time	End Time	Duration
[Empty Row]					

Index	Date & Time	Phone Number	Start Time	End Time	Duration
[Empty Row]					

Event Log

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



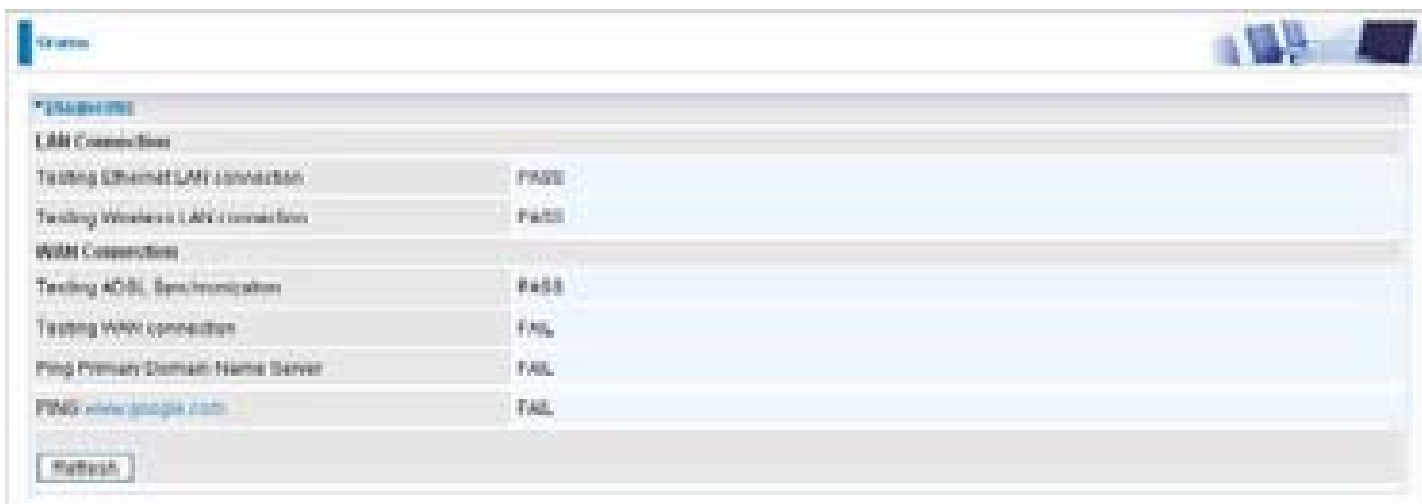
Error Log

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



Diagnostic

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



Quick Start

1. Click Quick Start. Select the connect mode you want. There are 2 options to choose from: ADSL or 3G. Select ADSL mode from the drop down menu and click Continue.



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



3. If your ADSL line is ready, the screen appears ADSL Line is Ready. Choose Auto radio button and click Apply. It will automatically scan the recommended mode for you. Manually mode makes you to set the ADSL line by manual. (If you choose Manually, you will directly go to step 5.)



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



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

The screenshot shows a network configuration window titled "WAN Port 1". The settings are as follows:

- Profile Port: ADSL
- Protocol: PPPoE (RFC2516, PPP over Ethernet)
- VPI/VCI: 8 / 35
- Username: [Empty field]
- Password: [Empty field]
- Service Name: [Empty field]
- Auth. Protocol: Chap/Auto
- MTU: 1460
- IP Address: 0.0.0.0 (Note: 0.0.0.0 means Obtain an IP address automatically)
- Obtain DNS automatically: Enable
- Primary DNS / Secondary DNS: [Empty fields]

A warning icon and message are visible at the bottom: "Warning: This change will reset all settings that relate to WAN settings. Are you sure you want to save the settings please switch to Advanced mode." An "Apply" button is located at the bottom left.

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

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**.

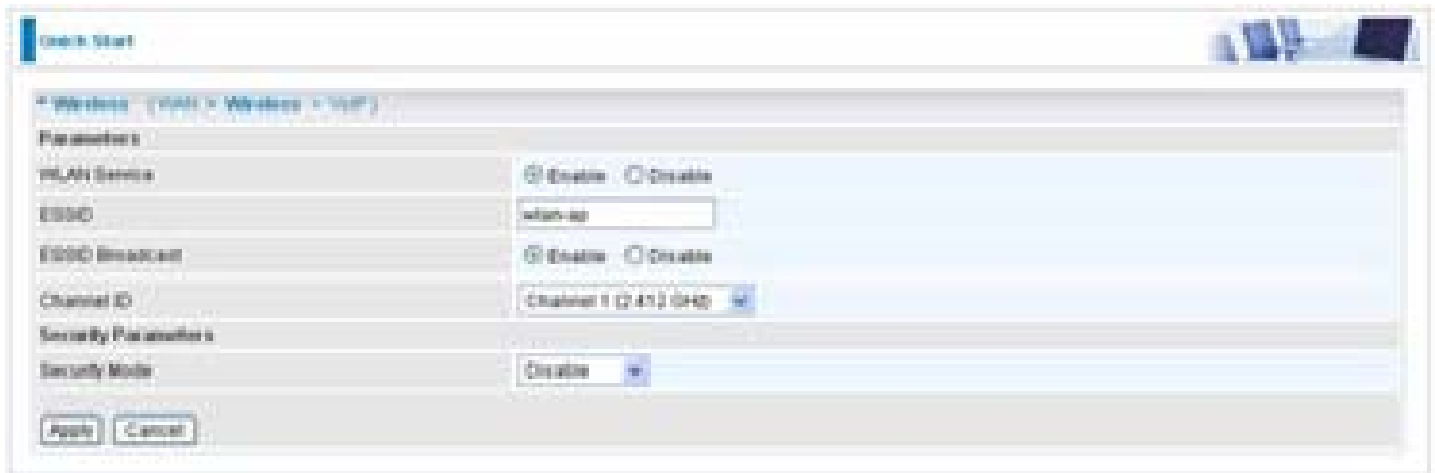
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

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

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.



6. Configure the Wireless LAN setting.



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

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

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

-  **Enable:** When Enable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.
-  **Disable:** Select Disable if you do not want broadcast your ESSID. When select Disable, no one will be able to locate the Access Point (AP) of your router.

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

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

7. Set up VoIP.

Quick Start

SIP Enable Region Australia

Setting for Phone Part 1

SIP Service Provider: NodePhone Phone Number: Username: Password: Display Name:

Setting for Phone Part 2 Same as Phone Part 1

SIP Service Provider: NodePhone Phone Number: Username: Password: Display Name:

Caution: The configuration will take effect only when you apply the changes, save configuration and reboot the device.

Apply Cancel

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 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 appeared on the Caller ID.

8. Wait for the configuration.

Quick Start

Save configuration.
Save Config to FLASH. Please wait for 2 seconds.

Quick Start

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

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

The screenshot displays a network configuration interface with the following sections:

- Device Information:**
 - Model Name: BPAC 7484V001
 - System Up Time: 00:20:54s
 - Hardware Version: 3000-00-00000000-00000000-01-00
 - Software Version: 3.2.1.01.000
- Physical Port Status:**
 - Ethernet: ✓
 - DMZ: ✗
 - ADSL: ✓
 - Phone: ✓
 - SD: ✗
 - Phone Port 1: ✗
 - Phone Port 2: ✗
- Table:**

Port	Protocol	VLAN ID	Connection	IP Address	Subnet Mask	Default Gateway	Primary DNS
ADSL	PPPoE	0.114	Attempting to Connect Disconnect	0.0.0	0.0.0		0.0.0

Configuration

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

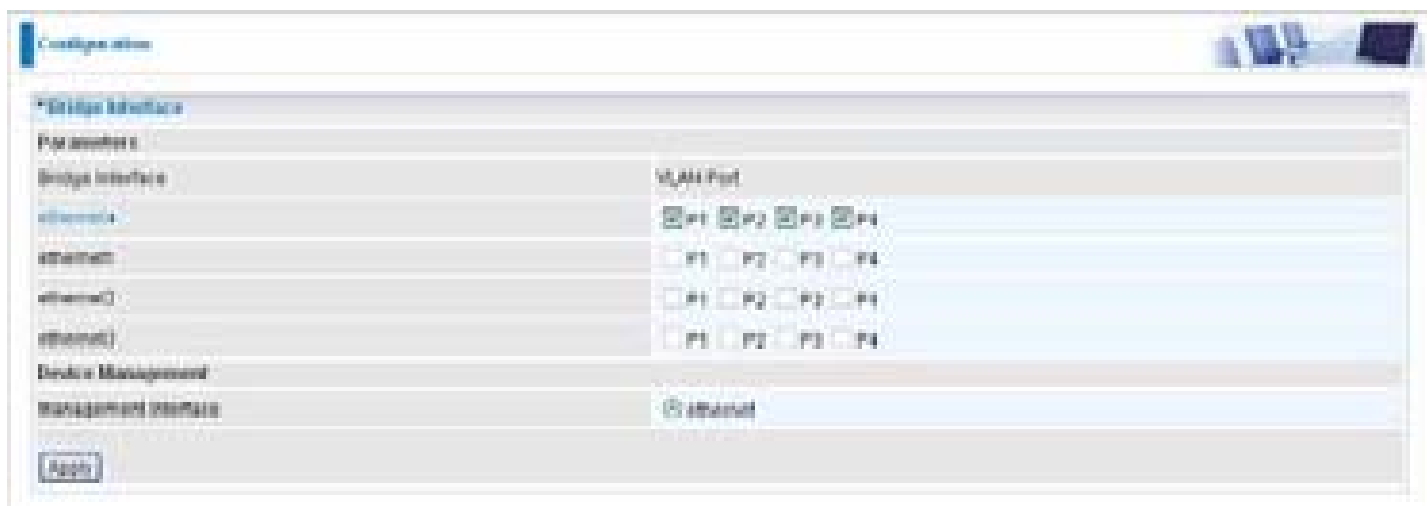
LAN, WAN, System, Firewall, VPN, VoIP, QoS, Virtual Server, Wake on LAN, Time Schedule and Advanced

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

LAN - Local Area Network

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

Bridge Interface



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

Ethernet: P1 (Port 1)

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

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

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

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

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

Ethernet



Primary IP Address

IP Address: The default IP on this router.

Subnet Mask: The default subnet mask on this router.

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

IP Alias


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





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

SubNetmask: Specify a subnet mask on this virtual interface.

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

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

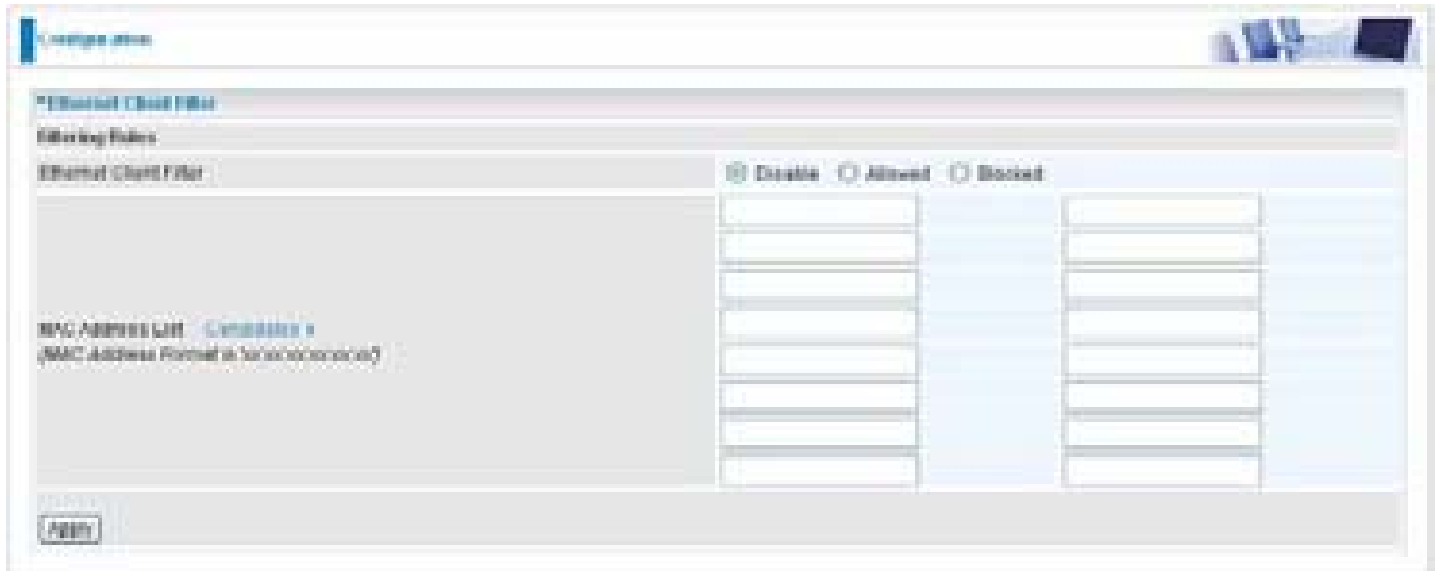
 **External:** There is no NAT on this IP interface and connected to the Internet directly. Mostly it will be used when providing multiple public IP addresses by ISP. In this case, you can use public IP address in local network which gateway IP address point to the IP address on this interface.

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

Ethernet Client Filter

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

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



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

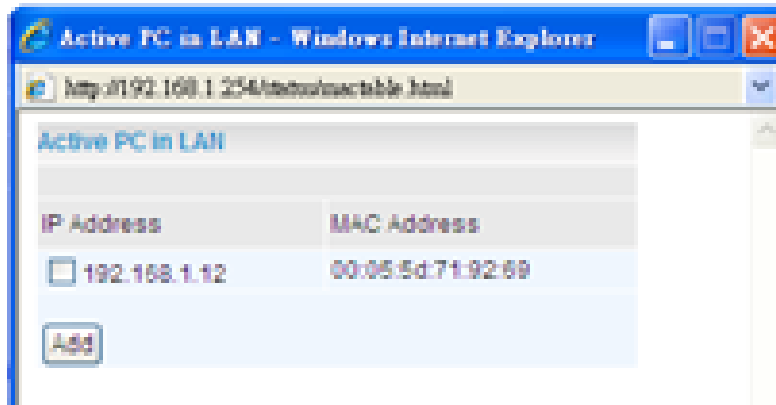
- Allowed:** check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.
- Blocked:** check to prevent unwanted device accessing your LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is not listed.

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

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

Candidates: automatically detects devices connected to the router through the

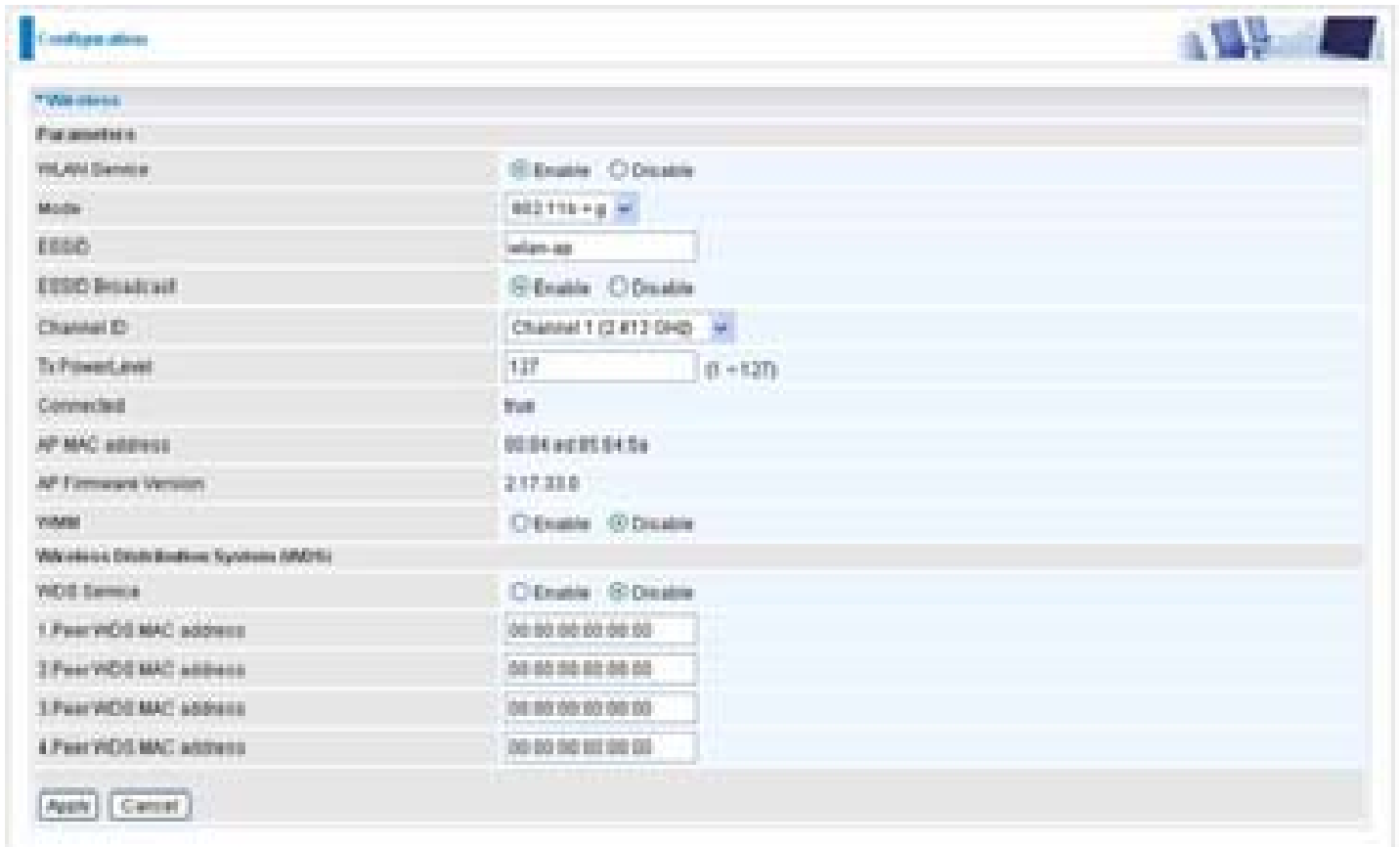
Ethernet. . Click the Candidate button to access the **Active PC in LAN** window.



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

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

Wireless



Parameters



WLAN Service: Default setting is set to Enable. If you do not have any wireless, both 802.11g and 802.11b, device in your network, select Disable.

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

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

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

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

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

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

Note: Wireless performance may degrade if select ID channel is already being occupied by

other AP(s).

TX PowerLevel: It is a function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 1 up to maximum 127.

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

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

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

AP Firmware Version: The Access Point firmware version.

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

 **Enable:** Click to activate WMM feature.

 **Disable:** Click to deactivate WMM feature

Wireless Distribution System (WDS)

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

In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

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

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

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

Wireless Security

You can disable or enable with WPA or WEP for protecting wireless network.

The default mode of wireless security is disabled.



WPA-PSK / WPA2-PSK



The screenshot shows the 'Wireless Security' configuration page. Under the 'Parameters' section, the 'Security Mode' is set to 'WPA-PSK'. The 'WPA Shared Key' field is empty. The 'Group Key Renewal' is set to '600' seconds. There are 'Apply' and 'Cancel' buttons at the bottom left.

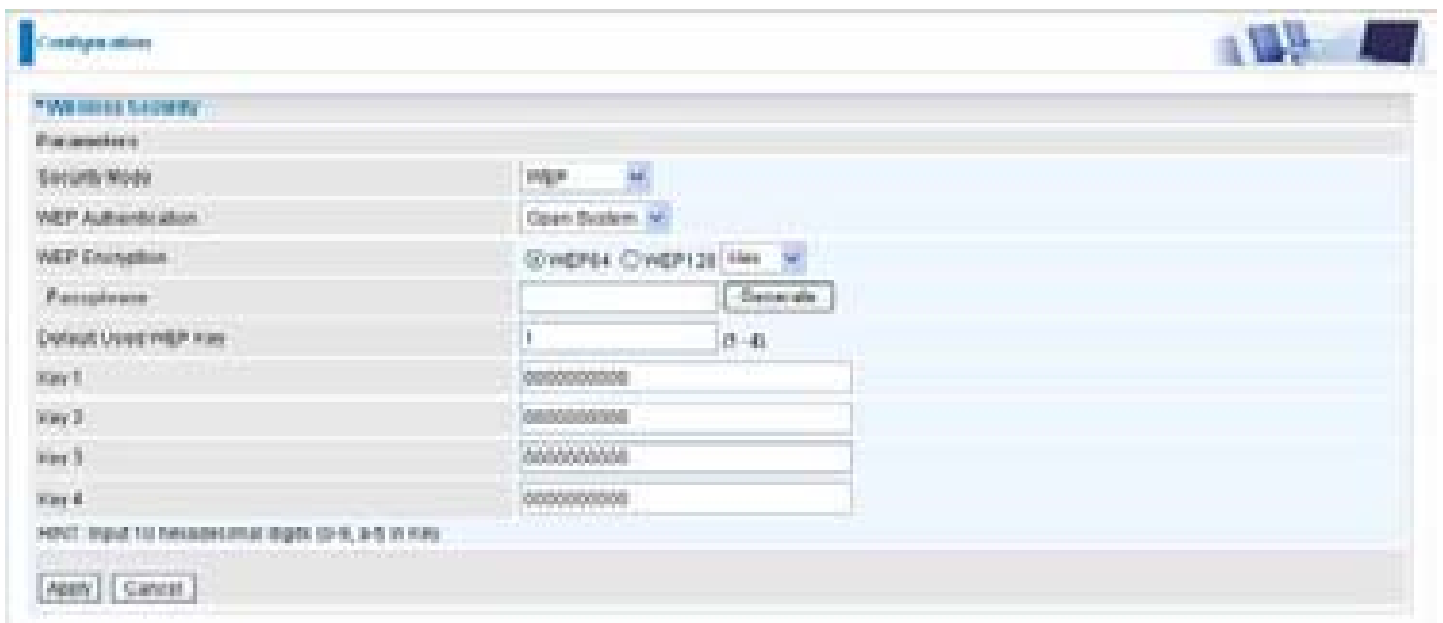
Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

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

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

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

WEP



The screenshot shows the 'Wireless Security' configuration page for WEP. Under the 'Parameters' section, the 'Security Mode' is set to 'WEP'. The 'WEP Authentication' is set to 'Open System'. The 'WEP Encryption' is set to 'WEP64'. The 'Pre-shared key' field is empty with a 'Generate' button next to it. The 'Default Used WEP key' is set to '1'. There are four 'Key' fields (Key 1 to Key 4) with empty text boxes. A 'Hint' at the bottom says 'Input 10 hexadecimal digits (0-9, a-f) in key'. There are 'Apply' and 'Cancel' buttons at the bottom left.

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

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

128 will offer increased security over WEP 64.

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

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

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

Wireless Client / MAC Address Filter

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

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

The screenshot shows a web-based configuration interface for a wireless client filter. At the top, there's a 'Configuration' tab. Below it, the title is 'Wireless Client / MAC Address / Filter'. Under 'Filtering Rules', there are three radio buttons: 'Disable' (selected), 'Allowed', and 'Blocked'. Below these are three columns of input fields for MAC addresses. The 'MAC Address List' section includes a 'Candidates' button and a note: '(MAC Address Format is xx:xx:xx:xx:xx:xx)'. An 'Apply' button is located at the bottom left of the configuration area.

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

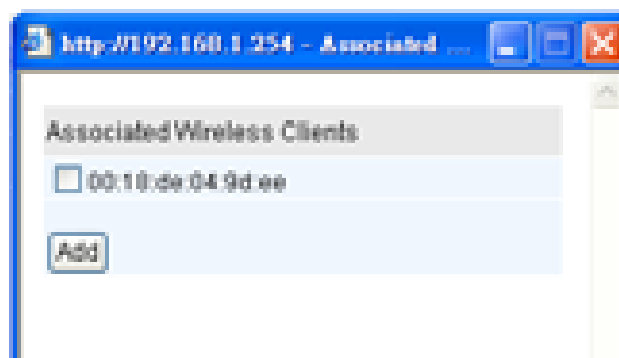
- **Allowed:** To authorize specific device accessing your LAN by insert the MAC Address in the space provided or click the Candidate button. Make sure your PC's MAC is listed.
- **Blocked:** To prevent unwanted device accessing the LAN by insert the MAC Address in the space provided or click the Candidate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

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

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

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

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

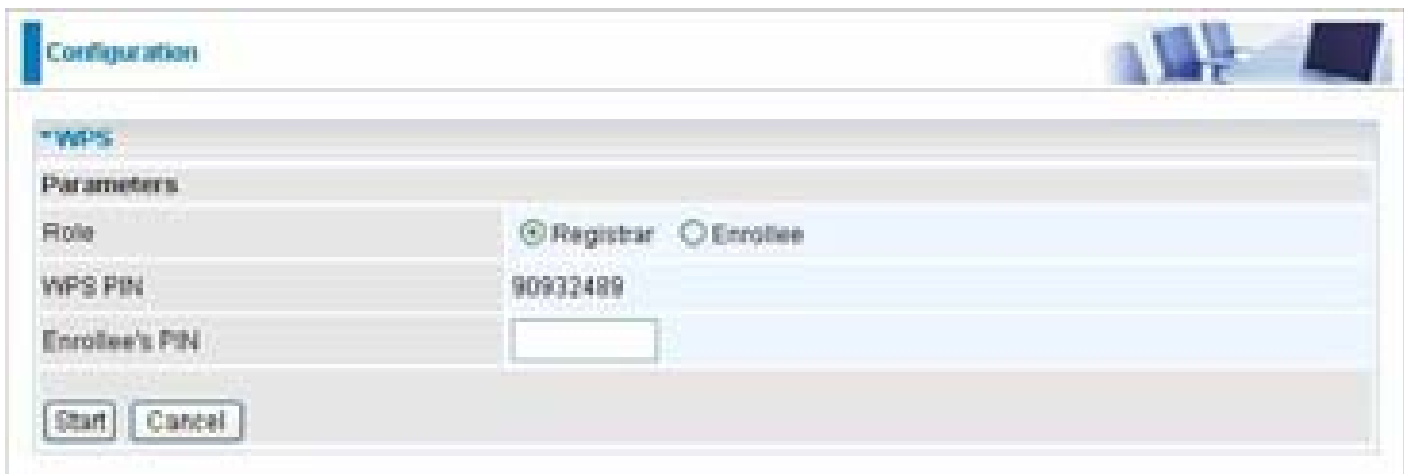


Associate Wireless Client: Displays a list of individual wireless device's MAC Address that currently connects to the router.

You can easily by checking the box next to the MAC address to be blocked or allowed. Then, Add to insert to the Wireless Client (MAC Address) Filter table. The maximum Wireless client is 16.

WPS

WPS feature is follow Wi-Fi Alliance WPS standard and it easily set up security-enabled Wi- Fi networks in the home and small office environment. It is reduced by half the user steps to configure a network and supports two methods that are familiar to most consumers to configure a network and enable security.



Set up of security-enabled Wi-Fi network

Step 1: Note down the AP's PIN from Web (Ex: 90932489).

Step 2: Open wireless client's WPS utility (Ex: Atheros Jumpstart WPS utility), select "Configure a wireless network" and apply "next" button.



Step 3: Enter AP's PIN into the utility and click on the "next" button.

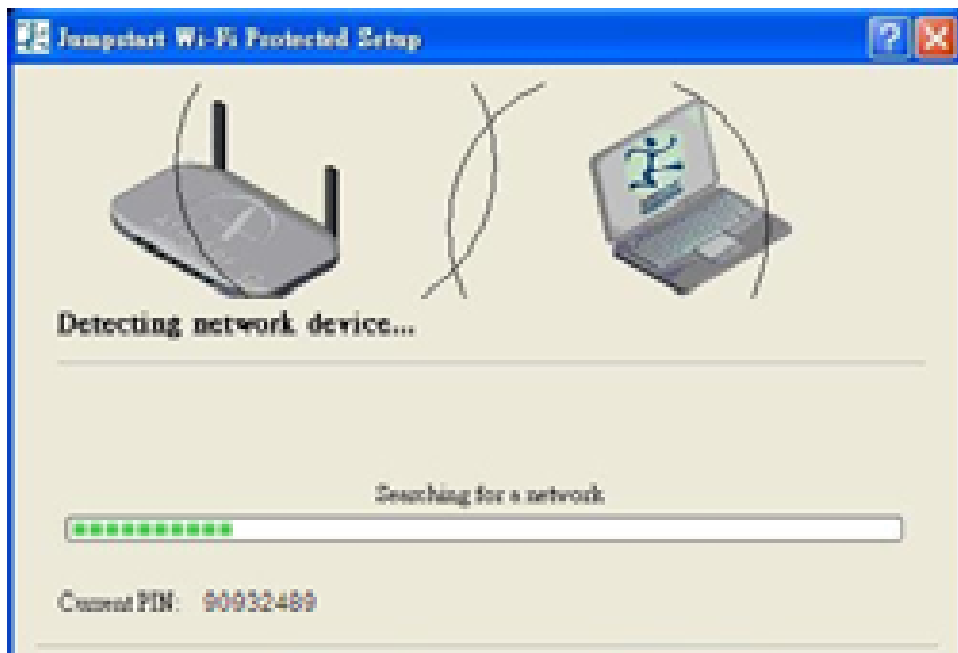


Step 4: These are two ways to trigger AP as Enrollee role, you can choose one to do it.

- ➊ Push AP's WPS button 1 second and release it. Or
- ➋ In the AP's WPS configuration page, change Role to "Enrollee" and apply "Start" button.



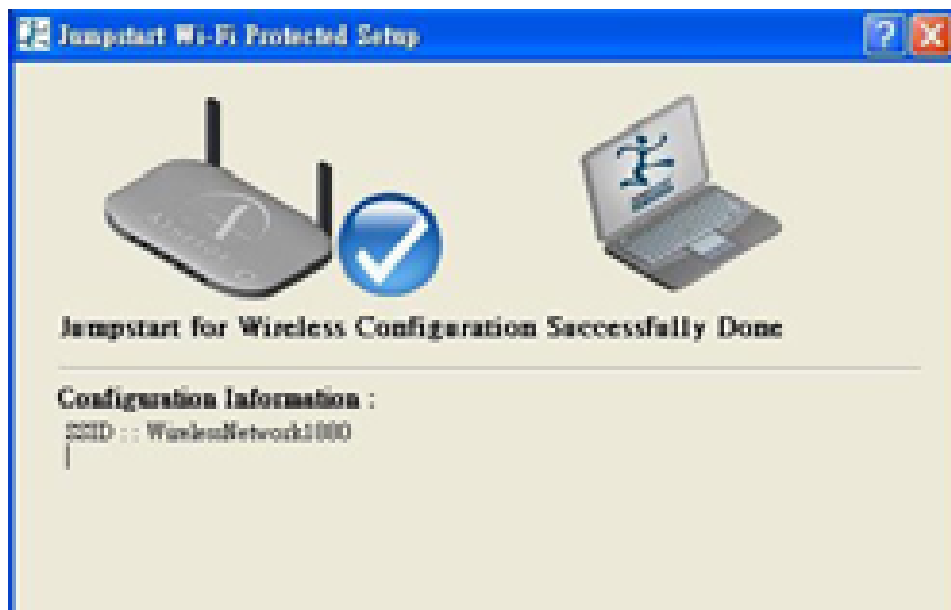
Step 5: Jump start WPS utility search WPS AP.



Step 6: SSID and security will be generated automatically (You can change it) and apply "next" button.



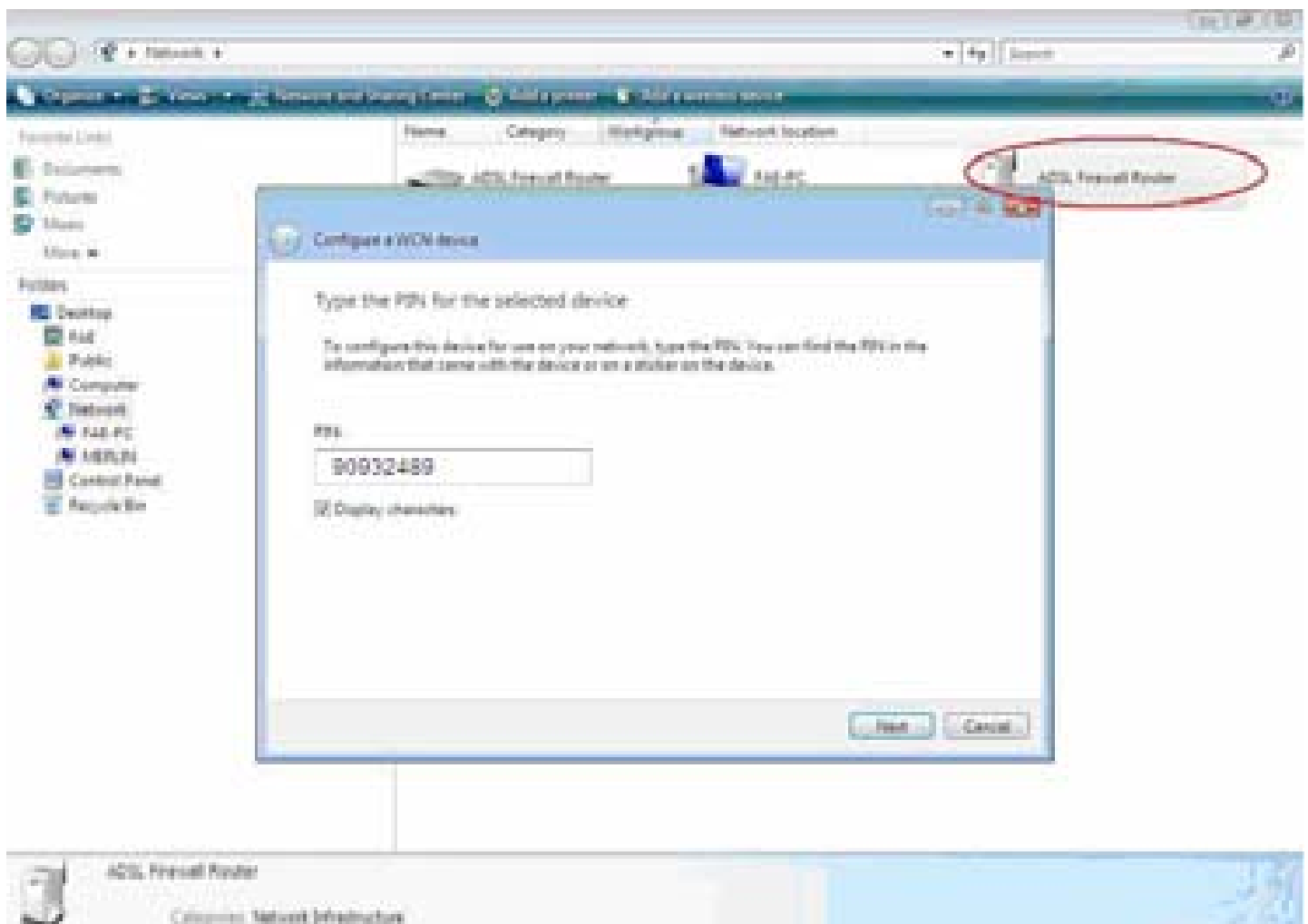
Step 7: WPS set up complete. And you have set up security-enabled Wi-Fi networks.



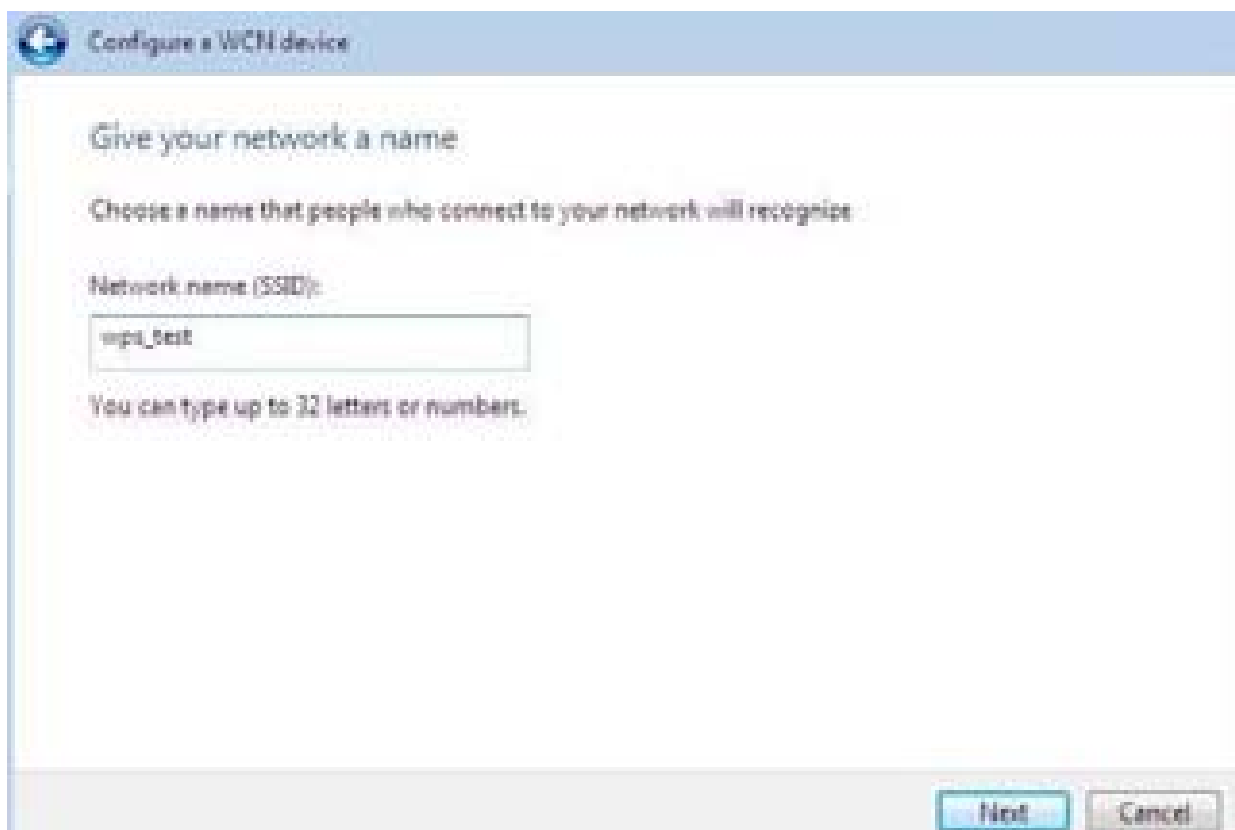
Set up of security-enabled Wi-Fi network using WCN in Vista

Step 1: Note down the AP's PIN from Web (Ex: 90932489).

Step 2: In Vista's Control Panel, select **Network and Internet** and choose **View network computers and devices**. Double click the "ADSL Firewall Router" icon and enter the AP's PIN code then click "Next".



Step 3: Enter the AP SSID and apply “Next” button.



Configure a WCN device

Give your network a name

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

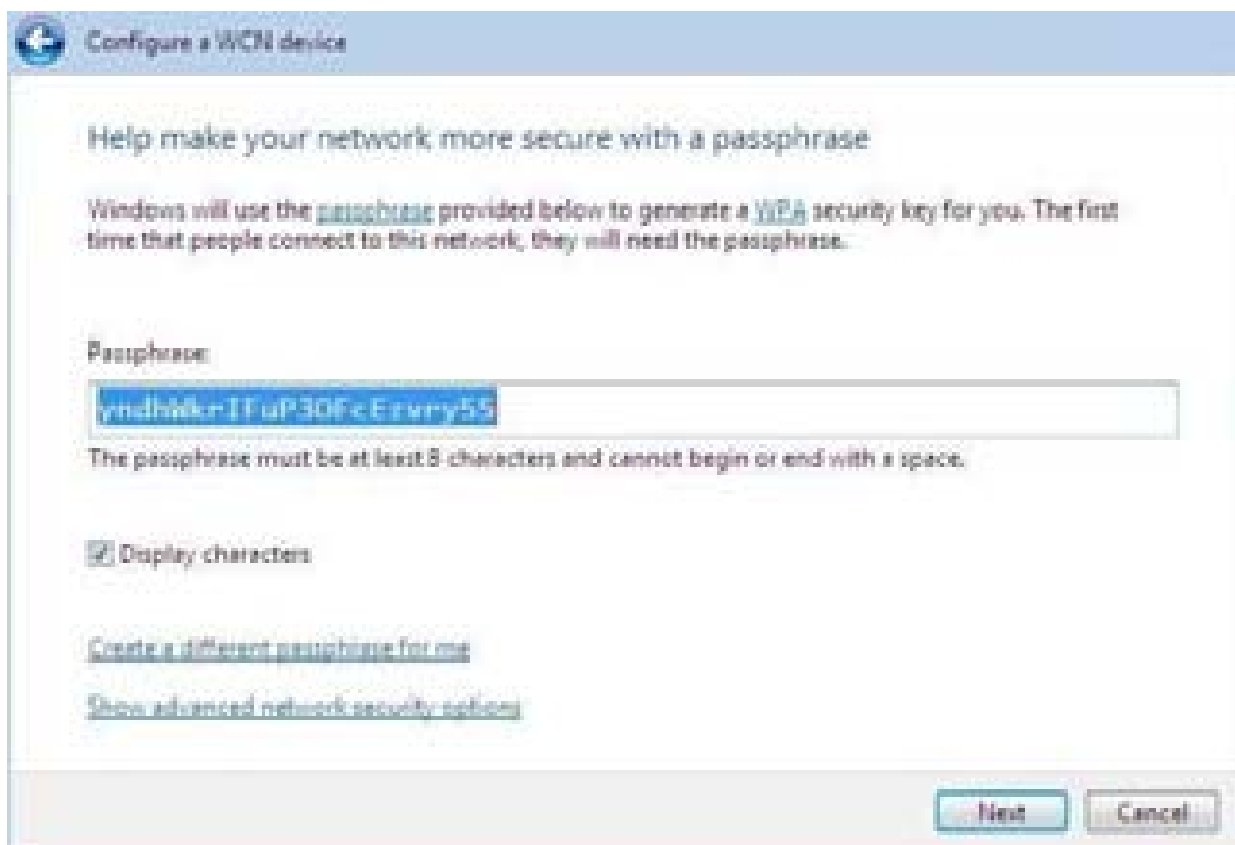
Network name (SSID):

wpa_test

You can type up to 32 letters or numbers.

Next Cancel

Step 4: Enter the Passphrase and apply “Next” button.



Configure a WCN device

Help make your network more secure with a passphrase

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

Passphrase:

yndhWk-1FuP30FcErwry55

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

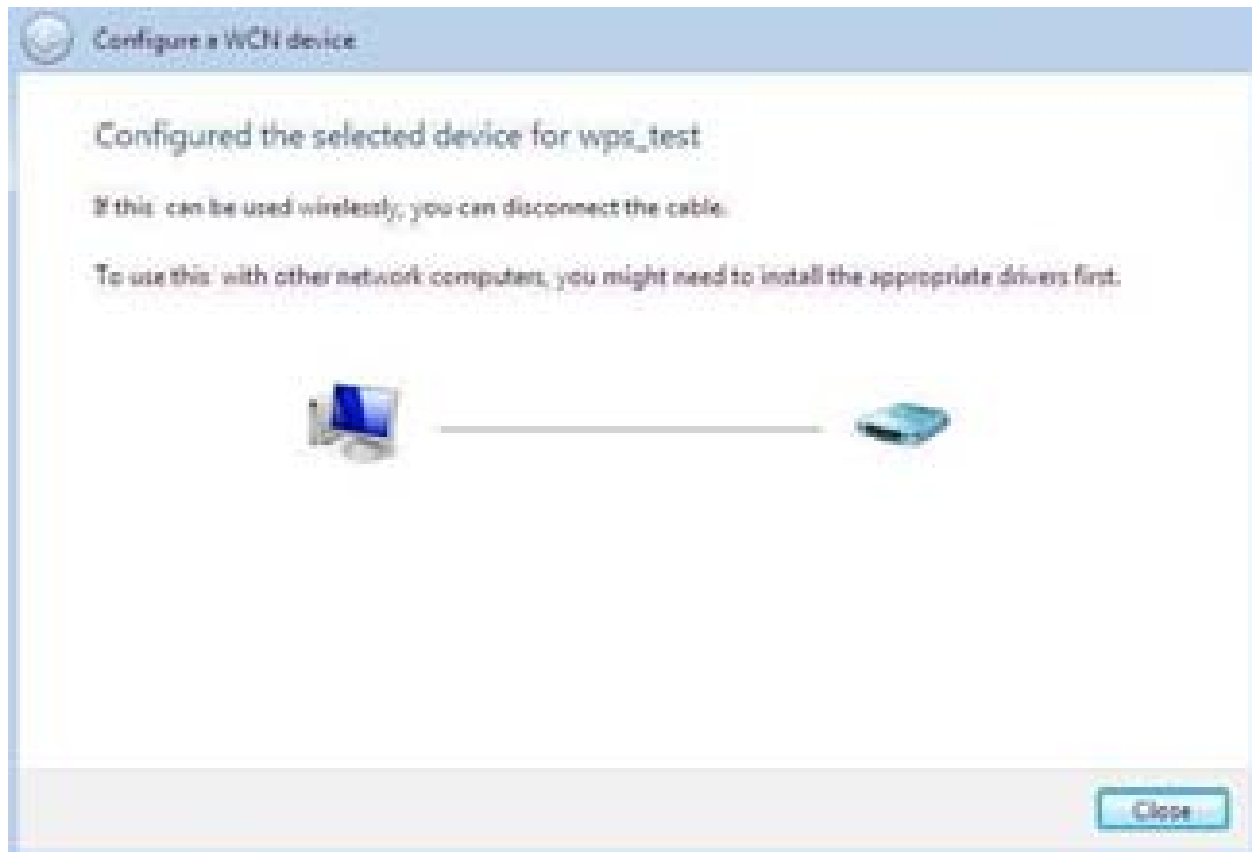
Display characters

[Create a different passphrase for me](#)

[Show advanced network security options](#)

Next Cancel

Step 5: WCN set up complete. And you have set up security-enabled Wi-Fi networks.



Adding a new WPS device (wireless client) to a network - Use PBC Method

Step 1: Push AP's WPS button more than one second and you will see AP's WLAN led will flashing per second.

Step 2: Open wireless client's WPS utility, select "Join a wireless network" and apply "next" button.
Note: After you push AP's WPS button, below steps should be completed between 2 minutes.



Step 3: Select “Push the button on my access point” and apply “next” button.



Step 4: New WPS device have join into the wireless network.

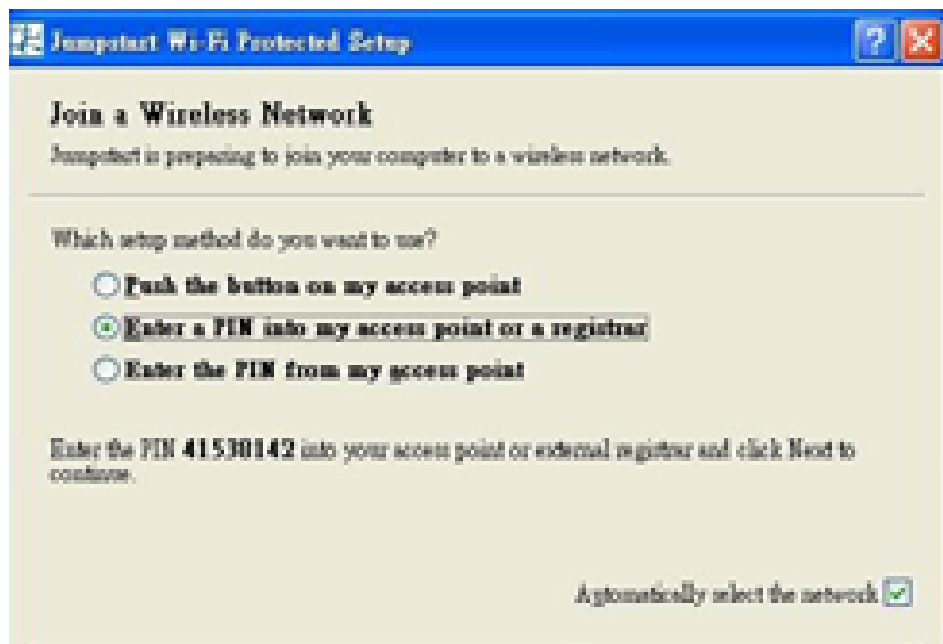


Adding a new WPS device (wireless client) to a network - Use PIN Method

Step 1: Open wireless client's WPS utility, select "Join a wireless network" and apply "next" button



Step 2: Note down the wireless client's PIN (Ex: 41538142) and apply "Start" button for active wireless client WPS PIN method.



Step 3: Enter wireless client's PIN into "Enrollee's PIN" of Web and apply "Start" button.

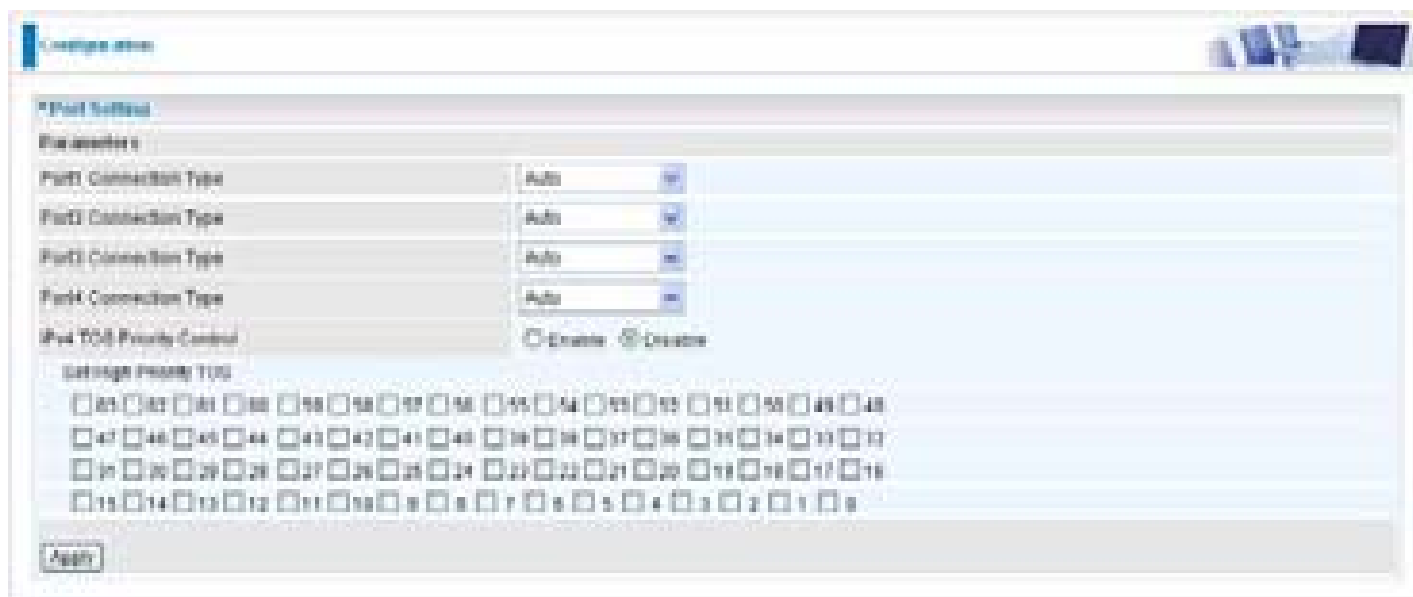


Step 4: New WPS device have join into the wireless network.



Port Setting

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



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

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

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

DHCP Server

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

The screenshot shows the DHCP Server configuration page. At the top, there are three radio buttons for 'DHCP Server Mode': 'Disable', 'DHCP Server' (which is selected), and 'DHCP Relay Agent'. Below this is a 'Next' button. The 'DHCP Server Status' section contains three rows: 'Allow Bootp' (true), 'Allow Unknown Clients' (true), and 'Enable' (true). The 'Subnet Definition' section contains five rows: 'Subnet IP' (192.168.1.0), 'Subnet Mask' (255.255.255.0), 'Maximum Lease Time' (86400 seconds), 'Default Lease Time' (83200 seconds), and 'Use local host address as DNS server' (true). Below this are three more rows: 'Use local host address as default gateway' (true), 'Use subnet from IF interface' (WAN), and 'IP Range 192.168.1.1 - 192.168.1.20'. At the bottom, there is a row for 'WAN Address 192.168.1.254'.

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

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

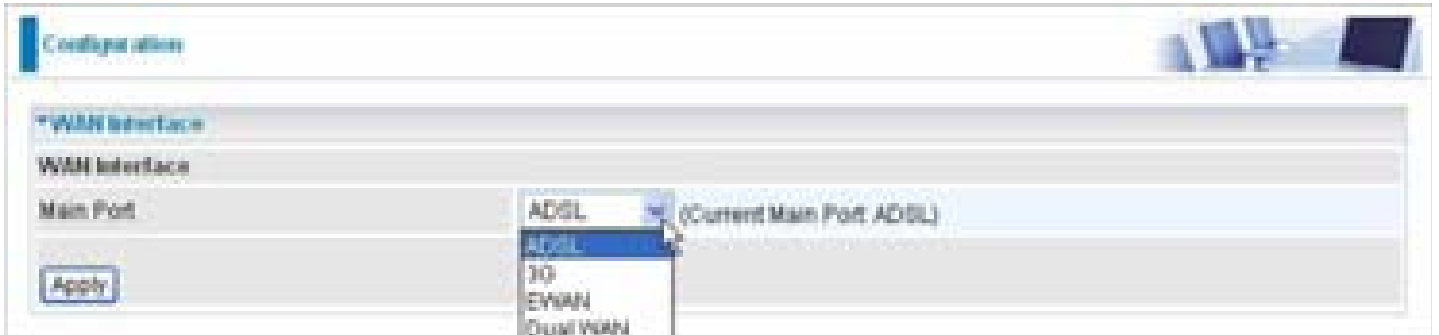
If you check DHCP Relay Agent and click Next, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

Click Apply to enable this function.

WAN - Wide Area Network

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

WAN Interface



ADSL Mode

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



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.



EWAN

EWAN is another way of getting connected to the Internet, the router offers its Ethernet port 1 as a WAN port to be used to connect to Cable Modems and fiber optic lines. This alternative, yet faster method to connect to the internet will provide users more flexibility to get online. When the above two mode is not valid, the way can be adopted.



Dual WAN



Main Port: Select **Dual WAN**.

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

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

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

Time Schedule: A self defined time period. You may specify a time schedule for your prioritization 66 policy. For setup and detail, refer to Time Schedule section.

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

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

Failover Probe Cycle: Set the time duration for the **Failover Probe Cycle** to determine when the

router will switch to the backup connection (backup port) once the main connection (main port) fails.

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




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

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

Detect Rule:

Rule 1. ADSL Down

Rule 2. Ping Fail

-  **No Ping:** It will not send any ping packet to determine the connection. It means to disable the ping fail detection.
-  **Ping Gateway:** It will send ping packet to gateway and wait response from gateway in every "Probe Cycle".
-  **Ping Host:** It will send ping packet to specific host and wait response in every "Probe Cycle".

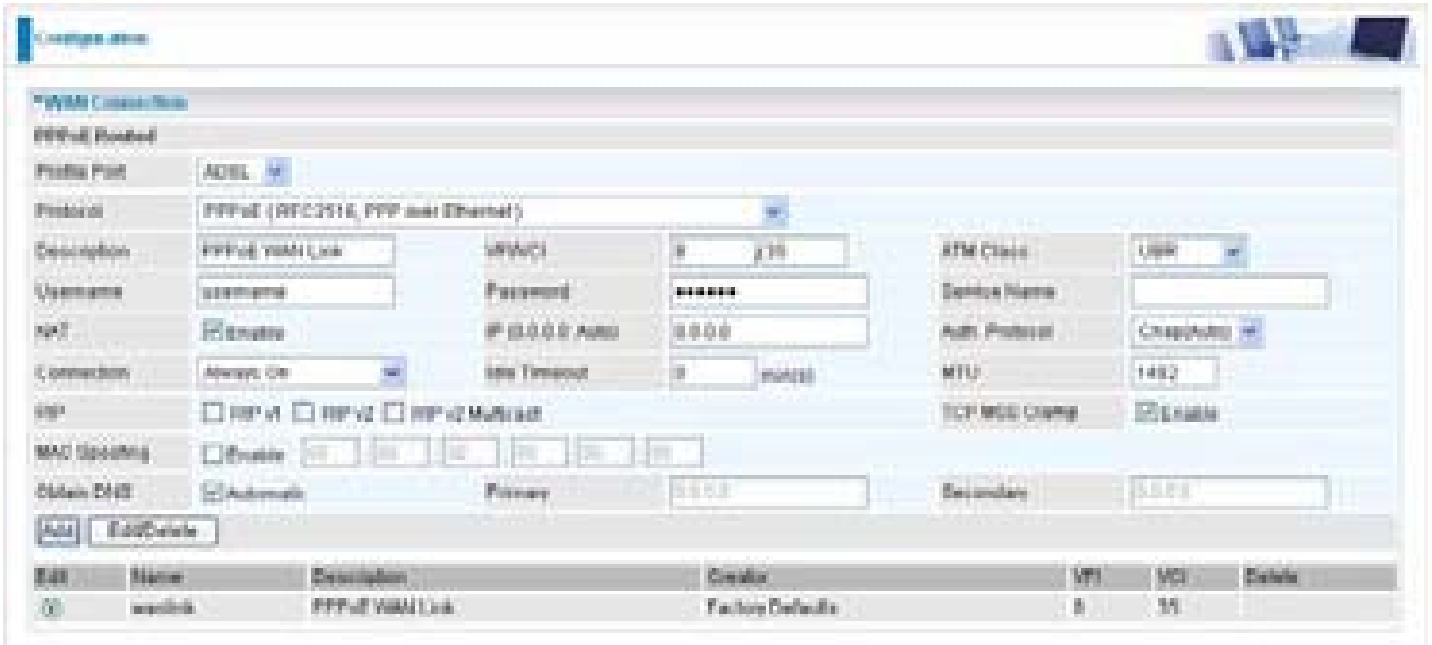
The host must be an IP address.

WAN Profile

ADSL

PPPoE Connection

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



Profile Port: Select the profile port as ADSL.

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

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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



Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is 15 alphanumeric characters.

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


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

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

Connection:

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

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

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

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

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

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

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

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS

PPPoA Connection

PPPoA Configuration

PPPoA Profile

Profile Port: ADSL

Protocol: PPPoA (RFC2364, PPP over ATM)

Destination: PPPoA-Enabled

VPI/VC: 8 / 35

ATM Class: VBR

Username: [Empty]

Password: [Empty]

NAT: Enable

IP (0.0.0.0:Auto): 0.0.0.0

Auth Protocol: CHAPv2

Connection: Always On

Idle Timeout: 0 min

MTU: 1492

TCP MSS Limit: Private

Domain DNS: Automatic

Primary: 0.0.0.0

Apply | Reset Defaults

ID	Name	Description	Creator	VPI	VCI	Delete
0	wan0	PPPoA WAN Line	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

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

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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


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


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

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


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

Connection:

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

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

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

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

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

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

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

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

MPoA Connection

Line	Name	Description	Creator	MTU	VCI	State
(1)	mpoa	MPoA WAN Link	Factory Defaults	0	25	Up

Profile Port: Select the profile port as ADSL.

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

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

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

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

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

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

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

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

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

IPoA Connection

Configuration

IPoA Connection

Profile Port: ADSL

Protocol: IPoA (RFC 2521, Class IP and ARP over ATM)

Description: IPoA mated VPI/VCI: 8/35 ATM Class: UBR

NAT: Enable MTU: 1500

IP (0.0.0.0:Auto): 0.0.0.0 Netmask: 0.0.0.0 Gateway:

RIP: RIP v1 RIP v2 RIP v2 Multicast TCP MSS Clamp: Enable

Obtain DNS: Automatic Primary: 0.0.0.0 Secondary: 0.0.0.0

Edit	Name	Description	Create	VPI	VCI	Delete
(0)	wan0	IPoA WAN Link	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

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

Description: A given name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

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

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

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

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

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

Profile Port: ADSL

Protocol: Pure Bridge

Description: RFC 1483 bridged mode

VPI/VCI: 8 / 35

ATM Class: UBR

Encap. Method: LLC Bridge

Acceptable Frame Type: acceptall

Filter Type: All

ID	Name	Description	Created	VPI	VCI	Delete
1	wan0	PPPoE WAN Line	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

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

Description: A given name for this connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

Multiple Session with PPPoE pass-through

ID	Name	Description	Create	VPI	VCI	Delete
0	wan0	PPPoE WAN Line	Factory Defaults	8	35	

Profile Port: Select the profile port as ADSL.

Protocol: The Multiple Session protocol will be used in the device.

Description: A given name for this connection.

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

ATM Class: The Quality of Service for ATM layer.

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

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

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

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

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

Connection:

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

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

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined 76 period of time.

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

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

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

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

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

The screenshot shows a configuration window titled "3G Configuration". It contains a list of parameters for configuring a 3G connection. The parameters and their values are as follows:

Parameter	Value
Profile Port	3G
iBurst	<input type="checkbox"/> Enable
Mode	UMTS GPRS
TEL No.	*99**1*
APN	internet
Username	
Password	
Auth Protocol	CHAP (Auto)
MTU	1500
PIN	
Connection	Always On
Save Alive	<input type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable
Enable DNS automatically	<input checked="" type="checkbox"/> Enable
Primary DNS/Secondary DNS	1.1.1.1 / 1.1.1.1

At the bottom of the window, there is a "Warning" message: "Warning: Entering the wrong PIN code three times will lock the SIM." and an "Apply" button.

Profile mode: select the profile port as 3G

iBurst: check the check box to determine whether to enable the iBurst function.

Mode: select your wanted mode of 3G operation from the drop-down menu.

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

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

Username: Enter the username provided by your service provider.

Password: Enter the password provided by your service provider.

Authentication Type: Default is None. 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.

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 authenticate. 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 you will require a PUK code from your network/service provider.

Connection: select the connection method you want.

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



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

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



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

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

Obtain DNS: Select Automatic to use DNS.

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

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

EWAN

WAN Configuration

Profile Port: EWAN

WAN Port: Ethernet Port 1

Protocol: Obtain an IP Address Automatically (selected)

Username: _____ Password: _____ Service Name: _____

Idle Timeout: 0 min MTU: 1482

Obtain DNS: Automatic Primary: _____ Secondary: _____

Apply

Obtain an IP Address Automatically

WAN Configuration

Obtain an IP Address Automatically

Profile Port: EWAN

WAN Port: Ethernet Port 1

Obtain DNS: Automatic Primary: _____ Secondary: _____

Apply

Profile Port: Select the profile port as EWAN.

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

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

Obtain DNS: Select Automatic to use DNS.

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

Fixed IP Address

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



The screenshot shows a router's configuration interface for the WAN connection. The 'Fixed IP Address' option is selected. The configuration fields are as follows:

Field	Value
Profile Port	EWAN
WAN Port	Ethernet Port 1
Protocol	Fixed IP Address
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	
Obtain DNS	<input type="checkbox"/> Automatic
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Profile Port: Select the profile port as EWAN.

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

Protocol: Select **Fixed IP Address**.

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

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

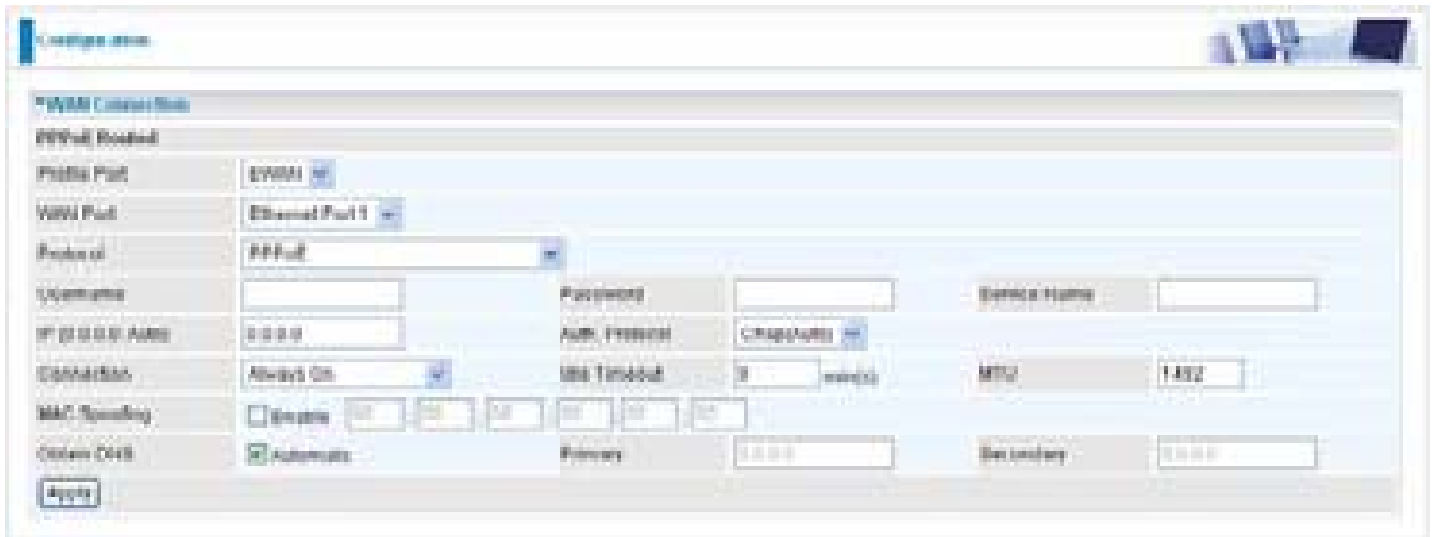
Gateway: You must specify a gateway IP address (supplied by your ISP).

Obtain DNS: Select Automatic to use DNS.

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

PPPoE

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



The screenshot shows a configuration window titled "WAN Connection Wizard". The "PPPoE Enabled" section is active. The "Profile Port" is set to "EWAN". The "WAN Port" is set to "Ethernet Port 1". The "Protocol" is set to "PPPoE". The "Username" and "Password" fields are empty. The "Auth. Protocol" is set to "CHAP/SHAP". The "Service Name" field is empty. The "IP (WAN Addr)" is set to "0.0.0.0". The "Idle Timeout" is set to "0" minutes. The "MTU" is set to "1492". The "Connection" is set to "Always On". The "MAC Spoofing" section has checkboxes for "Enable" and "Disable", both of which are unchecked. The "Clone MAC" section has a checkbox for "Automatic" which is checked. The "Primary" and "Secondary" IP addresses are both set to "0.0.0.0". An "Apply" button is located at the bottom left of the configuration area.

Profile Port: Select the profile port as EWAN.

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

Protocol: Select **PPPoE**.

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


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


Service Name: Enter a name for this connection.

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

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

Connection:

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

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

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

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific

headers) that IP will attempt to send through the interface.

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

Obtain DNS: Select Automatic to use DNS.

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

Pure Bridge



Profile Port: Select the profile port as EWAN.

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

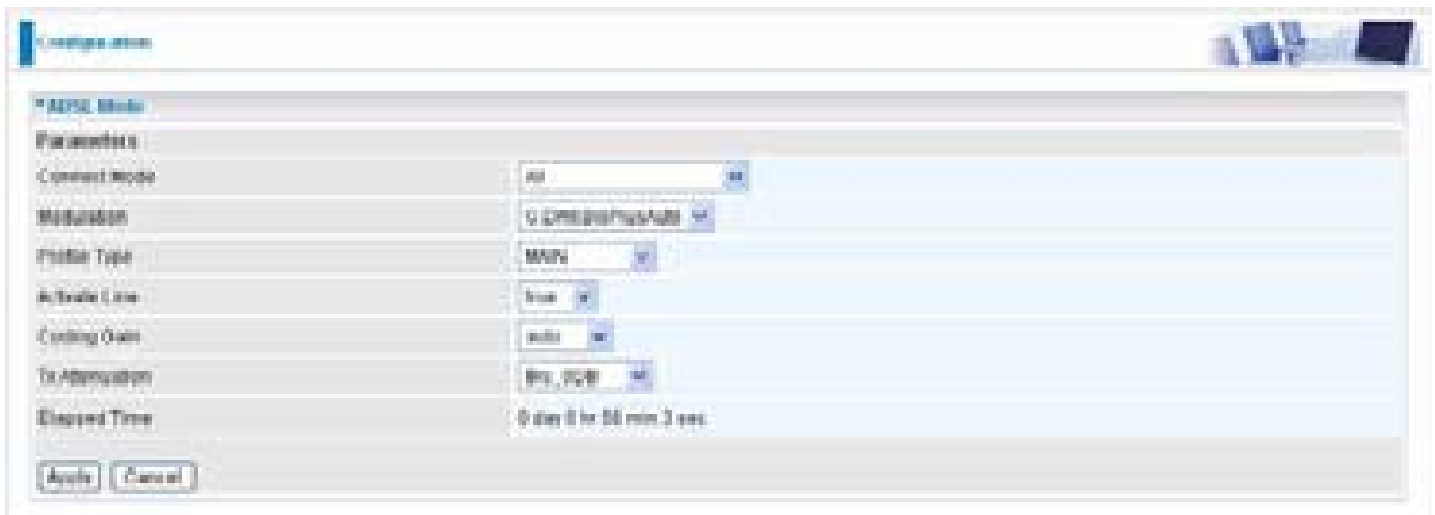
Protocol: Select **Pure Bridge**.

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

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

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

ADSL Mode



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

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

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

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

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

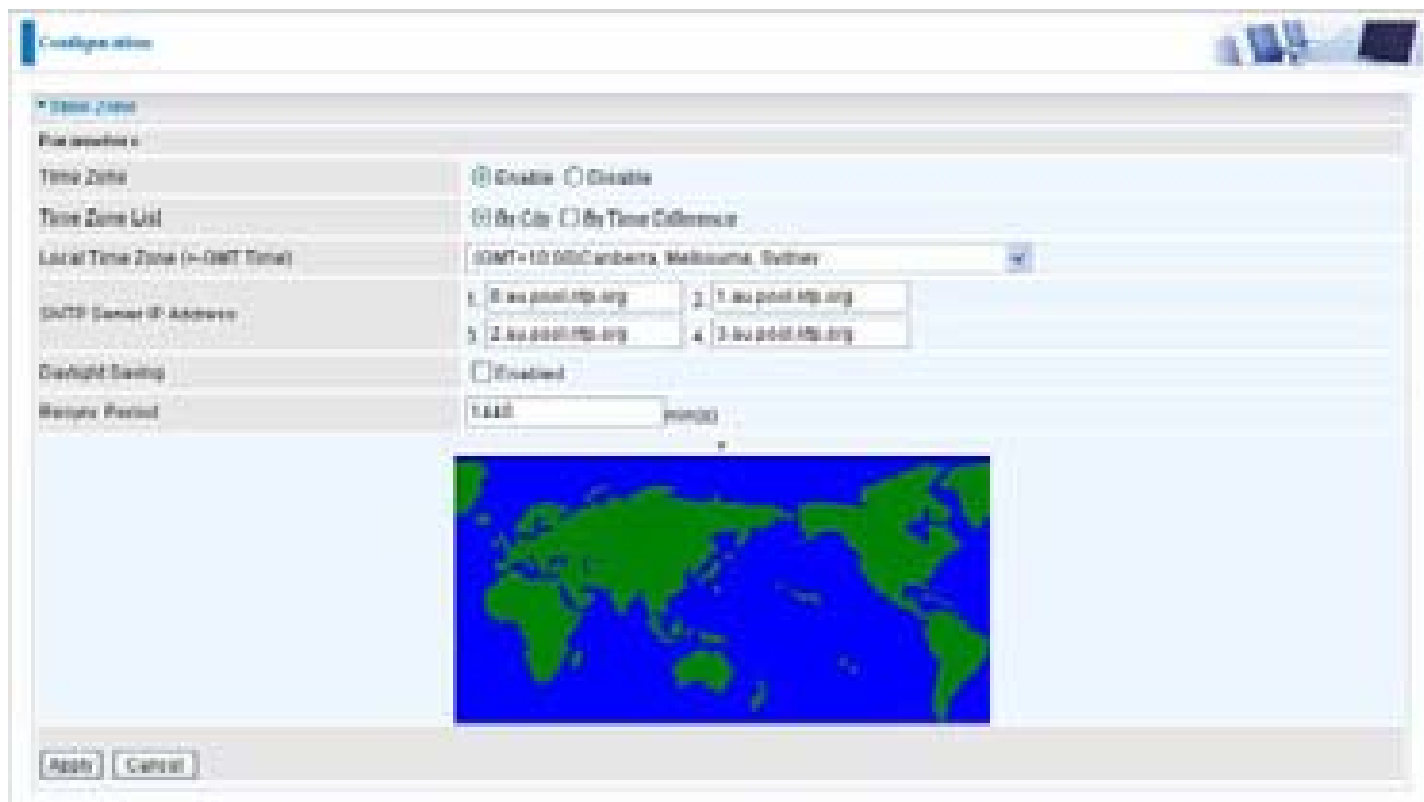
Tx Attenuation: It is the ADSL transmission power that the modem is using. The lower the power the better performance in router's upstream. Configurable value is between 0~12.

Elapsed Time: the time since ADSL connection is established.

System

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

Time Zone



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

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



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

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

Firmware Upgrade



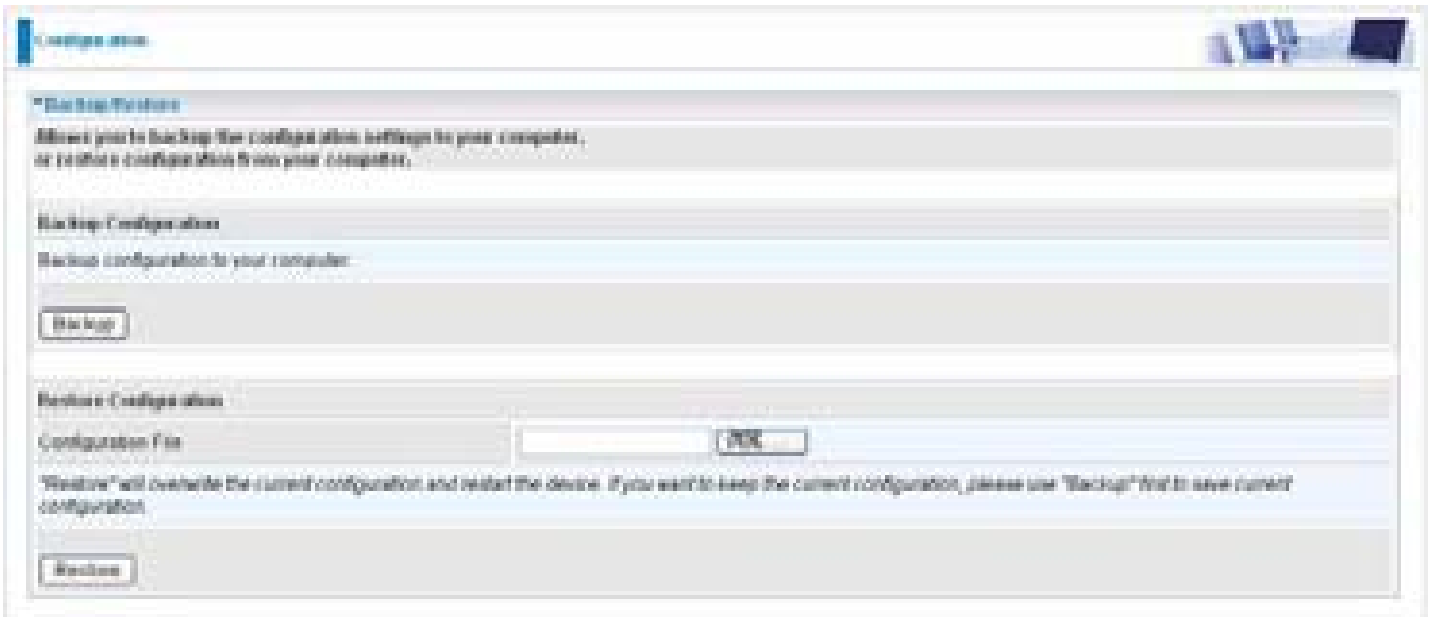
Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs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

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



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

Backup / Restore



The screenshot shows a web interface titled "Configuration" with a sub-section for "Backup/Restore". It contains two main sections: "Backup Configuration" and "Restore Configuration".

Backup Configuration: This section includes the text "Allow you to backup the configuration settings to your computer, or restore a configuration from your computer." Below this, there is a heading "Backup Configuration" and a sub-heading "Backup configuration to your computer:". A "Backup" button is located at the bottom of this section.

Restore Configuration: This section includes the text "Restore Configuration". Below this, there is a heading "Restore Configuration" and a sub-heading "Configuration File:". There is a text input field for the file name and a "Browse" button. Below the input field, there is a warning: "Restore will overwrite the current configuration and reload the device. If you wish to keep the current configuration, please use 'Backup' first to save current configuration." A "Restore" button is located at the bottom of this section.

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

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

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

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

Restart Router

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



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

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

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

User Management

Configuration

User Management

Create/Define Users

Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	

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

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

Configuration

User Management

Create/Define Users

Valid	User	Comment	Password	Confirm Password
<input checked="" type="checkbox"/>	admin	Default admin user	*****	*****

Edit	Valid	User	Comment	Delete
<input checked="" type="radio"/>	true	admin	Default admin user	

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

Configuration

User Management

Create/Define Users

Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	

When you create a user account, check Valid box and fill in the respective information for User, Comment, Password and Confirm Password in the blanks provided. Then click the Add button to add your new user account.

User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
<input checked="" type="checkbox"/>	Test	Test	****	****

Add **Edit/Delete**

Edit	Valid	User	Comment	Delete
<input type="checkbox"/>	Yes	admin	Default admin user	

To delete a user account, click on the Delete radio button on the right column of the account you wish to delete and then click the Edit/Delete button on the top to confirm your deletion.

User Management

Current Defined Users

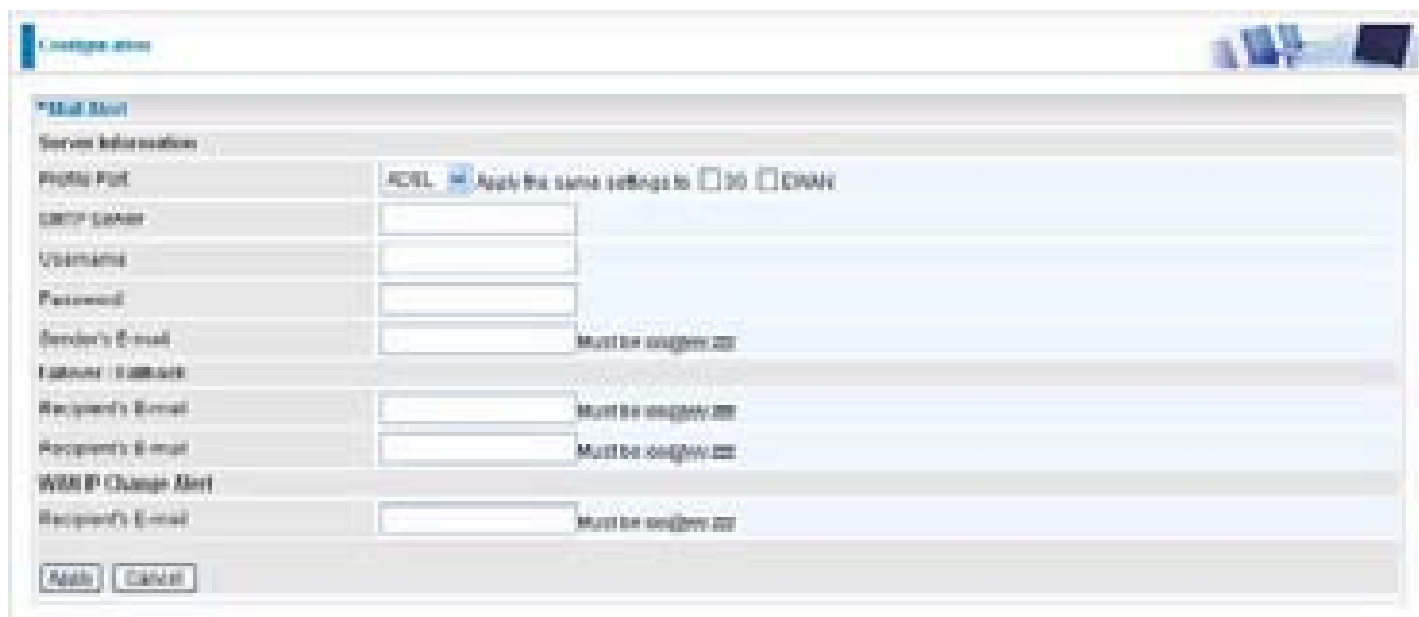
Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>				

Add **Edit/Delete**

Edit	Valid	User	Comment	Delete
<input type="checkbox"/>	Yes	admin	Default admin user	
<input type="checkbox"/>	Yes	Test	Test	

Mail Alert

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



The screenshot shows a configuration window titled "Mail Alert" with a "Server Information" section. It contains several input fields and checkboxes:

- SMTP Port:** A dropdown menu set to "SMTP" with a button "Apply the same settings to" and checkboxes for "SO" and "DMZ".
- SMTP Server:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Sender's Email:** A text input field with a validation message "Must be a valid email".
- Failover / Failback:** A section header.
- Recipient's Email:** A text input field with a validation message "Must be a valid email".
- Recipient's Email:** A second text input field with a validation message "Must be a valid email".
- WAN IP Change Alert:** A section header.
- Recipient's Email:** A text input field with a validation message "Must be a valid email".

At the bottom of the window are "Apply" and "Cancel" buttons.

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

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

Password: Enter the password of your email account.

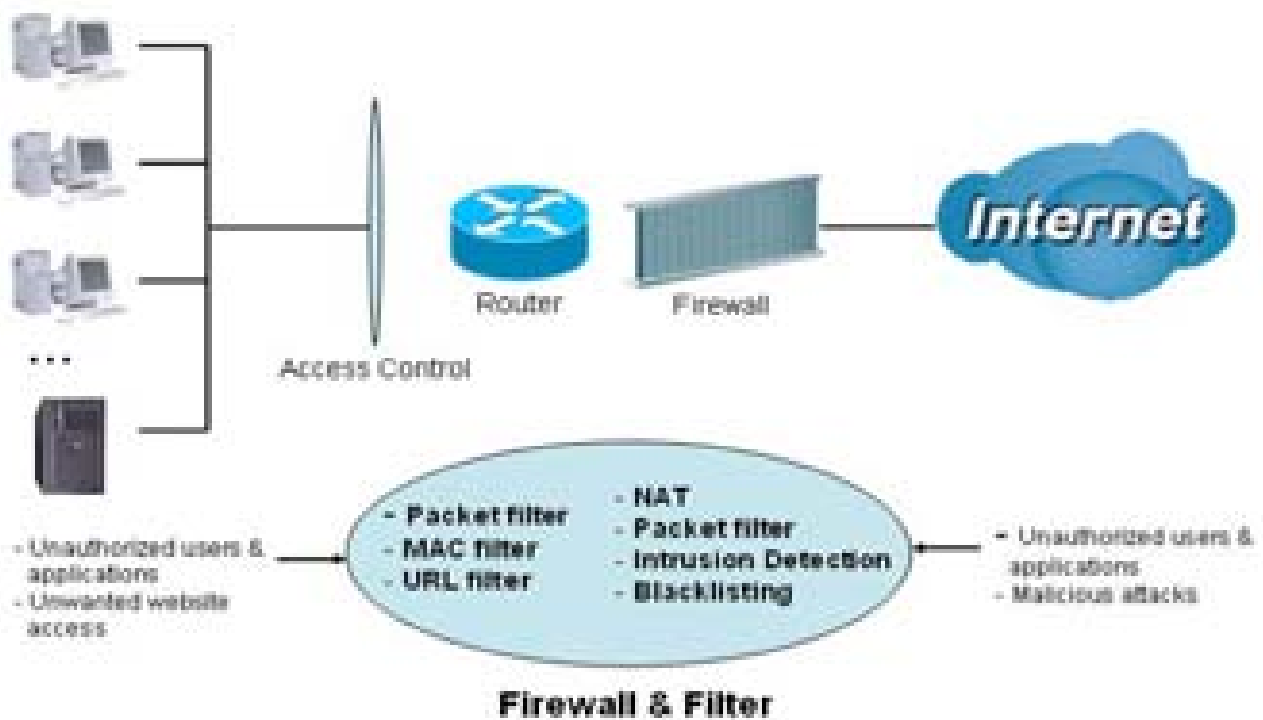
Sender's Email: Enter your email address.

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

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

Firewall and Access Control

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



Firewall: Prevent outsiders from accessing your local network. The router provides three levels of security support:



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

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

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

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

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

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

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



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

General Settings

You can choose not to enable Firewall and still able to access to URL Filter and IM/P2P Blocking or enable the Firewall using preset filter rules and modify the port filter rules as required. The Packet Filter is used to filter packets based-on Applications (Port) or IP addresses.



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

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

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

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

The “Block WAN Request” is a stand-alone function and not relate to whether security enable or

disable. Mostly it is for preventing any scan tools from WAN site by hacker.



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

Packet Filter

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

The screenshot shows the configuration page for Packet Filter rules. It includes fields for Rule Name, Time Schedule, Source/Destination IP addresses, Ports, Protocol, and Inbound/Outbound actions. Below the configuration area is a table of predefined rules.

Rule Name	Time Schedule	Source IP / Network	Destination IP / Network	Protocol	Source port(s)	Destination port(s)	Inbound	Outbound
net_mng	Always On	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	0 - 65535	80 - 80	Block	Block
net_tel	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

Example: Predefined Port Filters Rules

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

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

Table 1: Predefined Port Filter Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP /SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy (8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A
MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

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

Packet Filter – Add TCP/UDP Filter



The screenshot shows a web-based configuration interface for a packet filter. The main section is titled 'Configure Filter'. It contains several input fields and dropdown menus. The 'Rule Name Helper' field is empty, with a '-Select-' dropdown menu. The 'Time Schedule' is set to 'Always On'. The 'Source IP Address(es)' and 'Destination IP Address(es)' fields are both set to '0.0.0.0'. The 'Type' is set to 'TCP/UDP'. The 'Source Port' is set to '0' and the 'Destination Port' is set to '0'. The 'Inbound' and 'Outbound' options are both set to 'Allow'. There are also fields for 'Subnet Mask' and 'Port Number', both set to '0.0.0.0'. At the bottom, there are 'Add' and 'Edit/Delete' buttons.

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

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

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

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

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

Protocol Number: Insert the port number.

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”).

Click Add button to apply your changes.

Packet Filter – Add Raw IP Filter

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



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

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

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

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

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

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

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

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

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

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 no matter whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

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

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

The screenshot shows the configuration for a firewall rule named 'rule_http'. The rule is set to 'Always On' and applies to all source and destination IP addresses (0.0.0.0). The protocol is TCP, and it targets port 80 on both source and destination. Both inbound and outbound traffic is blocked.

Rule Name	Time Schedule	Source IP / Network	Destination IP / Network	Protocol	Source port(s)	Destination port(s)	Inbound	Outbound
rule_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	Block
rule_https	Always On	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	0 - 65535	443 - 443	Block	Block
rule_ssh	Always On	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	0 - 65535	22 - 22	Block	Block
rule_telnet	Always On	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	0 - 65535	23 - 23	Block	Block

Configuring Packet Filter:

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

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

The screenshot shows the 'Packet Filter' configuration page. The 'Parameters' section includes:

- Rule Name: Helper
- Time Schedule: Always On
- Source IP Address(es): 0.0.0.0
- Destination IP Address(es): 0.0.0.0
- Type: TCP (with a dropdown menu open showing options: TCP, UDP, TCP/UDP, Use Protocol Number)
- Source Port: (empty)
- Destination Port: (empty)
- Inbound: Allow
- Outbound: Allow

Buttons at the bottom: Add, Edit/Delete.

2. Choose the radio button you want to delete the existing HTTP rule. Click Edit/Delete button to delete the existing HTTP rule.

The screenshot shows the 'Packet Filter' configuration page with the following parameters:

- Rule Name: http
- Time Schedule: Always On
- Source IP Address(es): 0.0.0.0
- Destination IP Address(es): 0.0.0.0
- Type: TCP
- Source Port: 0 - 65535
- Destination Port: 80 - 80
- Inbound: Block
- Outbound: Allow

Buttons at the bottom: Add, Edit/Delete.

Rule Name	Time Schedule	Source IP / Netmask	Destination IP / Netmask	Protocol	Source port(s)	Destination port(s)	Inbound	Outbound	Delete
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	<input type="radio"/>
http	Always On	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	0 - 65535	80 - 80	Block	Allow	<input type="radio"/>

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

Example:

Application: Cindy_HTTP

Time Schedule: Always

On

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

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

Source Port: 0-65535 (I allow all ports to connect with the application))

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

Inbound / Outbound: Allow

Rule Name	Time Schedule	Source IP / Netmask	Destination IP / Netmask	Protocol	Source port(s)	Destination port(s)	Inbound	Outbound
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. The new port filter rule for HTTP is shown below:

<input type="radio"/>	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	<input type="radio"/>
-----------------------	------------	-----------	-----------------	-----------------	-----	-----------	---------	-------	-------	-----------------------

2. 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:



For how to configure the HTTP in Virtual Server, please refer to the Add Virtual Server sub-section under the Virtual Server section for detail.



Port Forwarding

Virtual Server Entry

Application	<input type="text"/>	to	<input type="text" value="-Select-"/>
Protocol	<input type="text" value="tcp"/>	Time Schedule	<input type="text" value="Always On"/>
External Port	from <input type="text" value="0"/> to <input type="text" value="0"/>	Redirect Port	from <input type="text" value="0"/> to <input type="text" value="0"/>
Internal IP Address	<input type="text"/>		<input type="text" value="-Select-"/>

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

Intrusion Detection






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

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

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

Block Duration:

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

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

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

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

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

ICMP Flood	Max ICMP Count (Default 100 c/ sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP

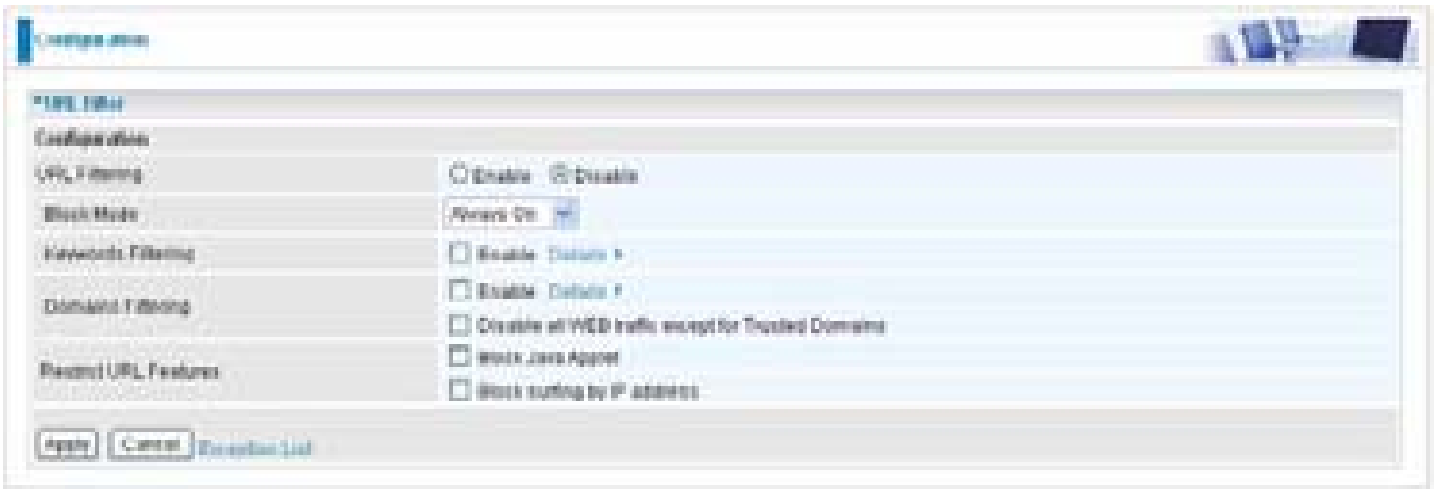
Src Port: Source Port

Dst Port: Destination Port

Dst IP: Destination IP




URL Filter

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



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

Block Mode: A list of the modes that you can choose 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 self-defined time period. You may specify the time period to check the URL filter rules, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

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

For example, if the URL is <http://www.abc.com/abcde.html>, it will be dropped as the keyword “abcde” occurs in the URL.



Domains Filtering: This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped.
3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to www.google.com.au, enter “[www.google](http://www.google.com)” 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](http://www.google.com) or www.google.com will be dropped, because [www.google](http://www.google.com) is in the forbidden list.



Example:

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

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

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

IM / P2P Blocking

IM, short for Instant Message, is required to use client program software that allows users to communicate, in exchanging text message, with other IM users in real time over the Internet. A P2P application, known as Peer-to-peer, is group of computer users who share file to specific groups of people across the Internet. Both Instant Message and Peer-to-peer applications make communication faster and easier but your network can become increasingly insecure at the same time. Billion's IM and P2P blocking helps users to restrict LAN PCs to access to the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.



Instant Message Blocking: The default is set to Disabled.

- 🌐 **Disabled:** Instant Message blocking is not triggered. No action will be performed.
- 🌐 **Always On:** Action is enabled.
- 🌐 **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer to **Time Schedule** section.

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

- 🌐 **Peer to Peer Blocking:** The default is set to Disabled.
- 🌐 **Disabled:** Instant Message blocking is not triggered. No action will be performed.
- 🌐 **Always On:** Action is enabled.

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

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

Firewall Log



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

Check the Enable box to activate the logs.

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

VPN - Virtual Private Networks

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

PPTP (Point-to-Point Tunneling Protocol)

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

Edit	Active	Name	Connection Type	Type	Delete
	<input type="checkbox"/>	Test	remoteaccess	dialout	

Name: A given name for the connection.

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

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

Connection Type: It informs your PPTP tunnel connection condition.

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

PPTP Connection - Remote Access

The screenshot shows the PPTP configuration page. The 'Parameters' section includes the following fields:

- Name: [Text Input]
- Connection Type: Remote Access (dropdown)
- Type: Dial out (dropdown)
- Server IP Address(or Domain Name): [Text Input]
- Username: [Text Input]
- Password: [Text Input]
- Auth. Type: Chap/Auto (dropdown)
- Data Encryption: Auto (dropdown)
- Key Length: Auto (dropdown)
- Mode: stateful (dropdown)
- Active as default route: Enable

Below the parameters are 'Add', 'Edit / Delete', and 'Apply' buttons. At the bottom, a table shows the current configuration:

Edit	Active	Name	Connection Type	Type	Delete
	<input type="checkbox"/>	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 VPNserver, e.g. your office server), check Dial In operates as a VPN server.

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

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

User.

Sever IP Address(or Domain Name):Enter the Server IP Adress or Domain Name.

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

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

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

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

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

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

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

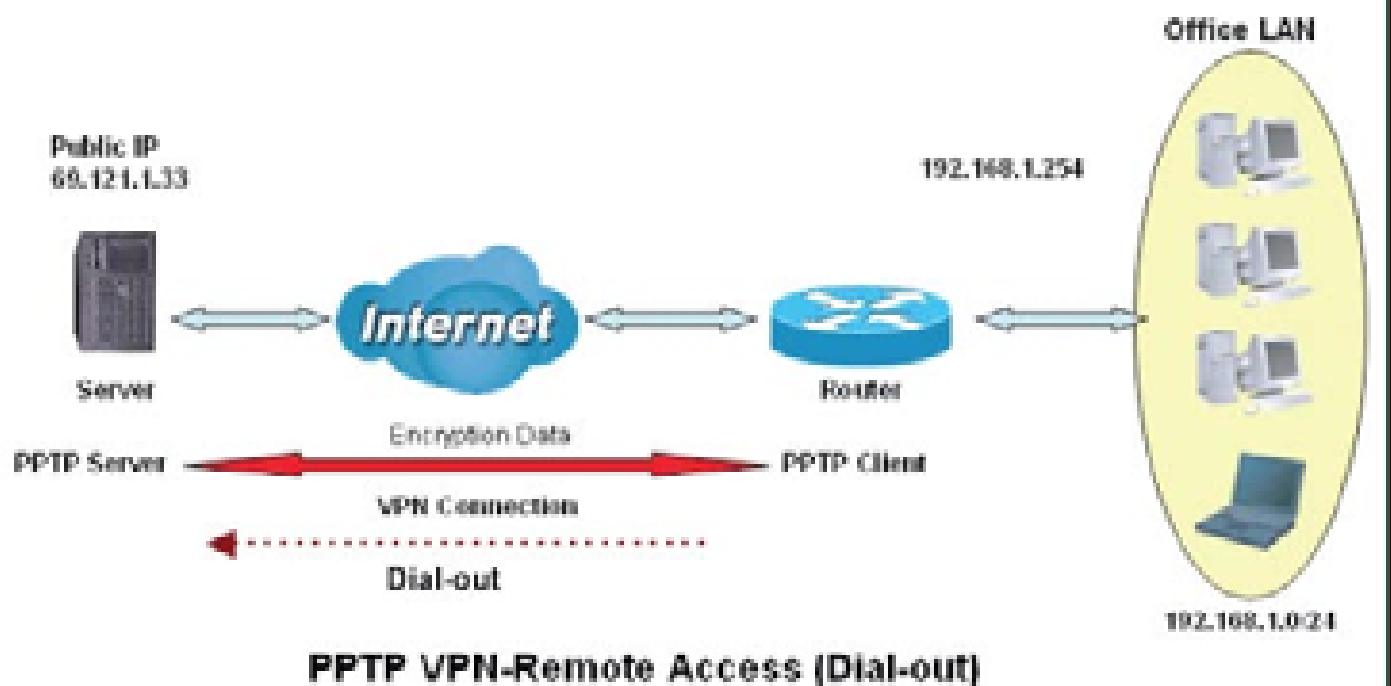
Active: This function activates or deactivates the PPTP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

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

Click Edit/Delete button to save your changes.

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

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



Configuring the PPTP VPN in the Office

Click Configuration/VPN/PPTP. Choose Remote Access from Connect Type drop-down menu. You can either input the IP address (69.1.121.33 in this case) or hostname to reach the server.

The screenshot shows the PPTP configuration window. The 'Name' field is set to 'VPN_PPTP'. The 'Connection Type' is set to 'Remote Access'. The 'Type' is set to 'Dial out'. The 'Server IP Address (or Domain Name)' is set to '69.1.121.33'. The 'Username' is 'username' and the 'Password' is '123456'. The 'Auth Type' is 'Chap(Auto)', 'Data Encryption' is 'Auto', 'Key Length' is 'Auto', and 'Mode' is 'stateful'. There is an 'Active as default route' checkbox which is currently unchecked. Below the configuration fields is a table listing the configuration:

Active	Name	Connection Type	Type	Delete
<input type="checkbox"/>	Test	remoteaccess	dialout	<input type="button" value="X"/>

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	An Dialed server IP
Username	Username	A given username & password
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 - LAN to LAN

Click Configuration/VPN/PPTP. Choose LAN to LAN from Connect Type drop-down menu.

The screenshot shows a configuration window for a PPTP connection. The 'Connection Type' is set to 'LAN to LAN'. The 'Type' is set to 'Dial out'. The 'Server IP Address (or Domain Name)' is '88.128.8.20'. The 'Auth Type' is 'CHAP/MS-CHAP v2'. The 'Mode' is 'Server'. Below the form is a table with columns: Edit, Active, Name, Connection Type, Type, and Delete. The table contains one entry: 'Test', 'enabled', 'dialout', and a delete icon.

Edit	Active	Name	Connection Type	Type	Delete
<input type="radio"/>	<input checked="" type="checkbox"/>	Test	enabled	dialout	<input type="radio"/>

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 VPNserver, e.g. your office server), check Dial In operates as a VPN server.

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

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

Sever IP Address(or Domain Name):Enter the Server IP Adress or Domain Name.

Peer Network IP: Enter Peer network IP address.

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

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

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

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

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

Key Length: The data can be encrypted by MPPE algorithm with 40 bits or 128 bits. Default is

Auto, it is negotiated when establishing a connection. 128 bit keys provide stronger encryption than 40 bit keys.

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

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

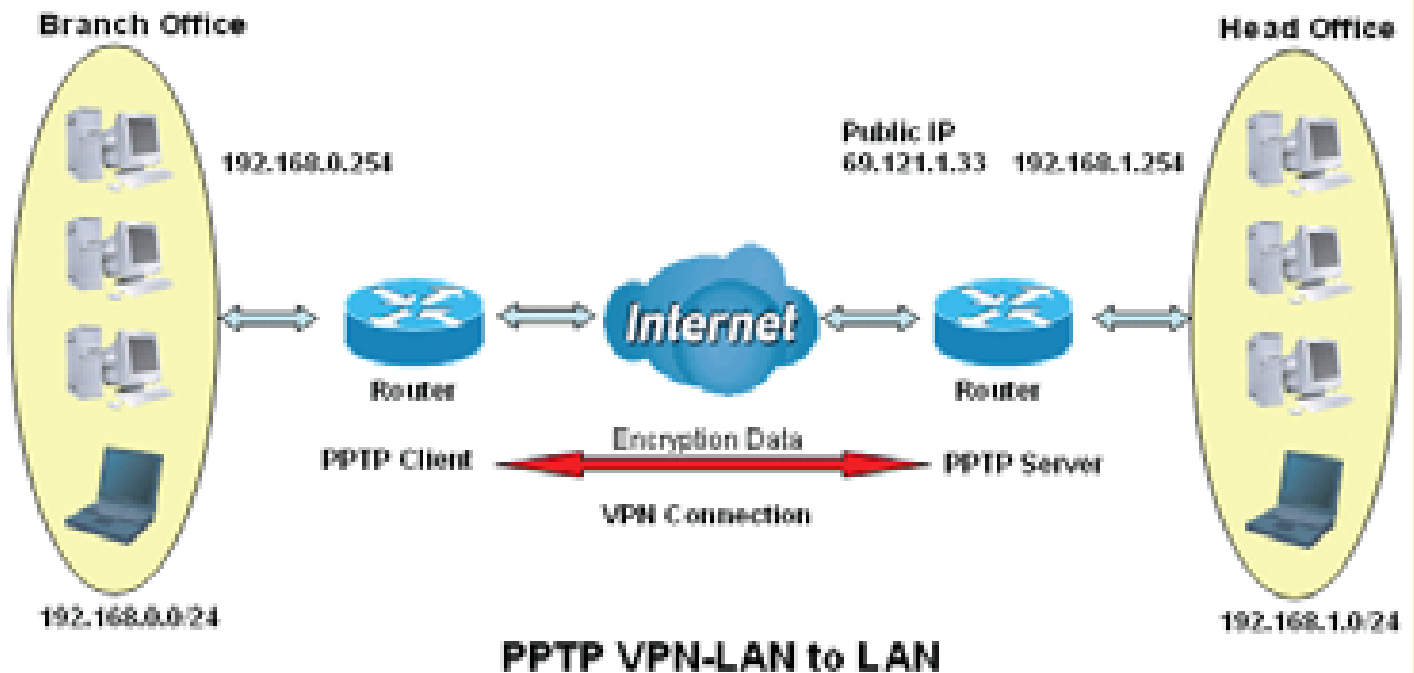
Active: This function activates or deactivates the PPTP connection. Check Active checkbox if you want the protocol of tunnel to be activated and vice versa.

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

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.



Both office LAN networks must be in different subnet with the LAN-LAN application.

Attention

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.

The screenshot shows a configuration window for a PPTP connection. The fields are as follows:

Name	HeadOffice	Connection Type	LAN to LAN
Type	Dial in	Private IP Address Assigned to Dial-in user	192.168.1.200
Peer Network IP	192.168.0.0	Netmask	255.255.255.0
Username	username	Password	*****
Data Encryption	Auto	Key Length	Auto
Active as default mode	<input type="checkbox"/> Enable	Auth. Type	Chap(Auto)
		Mode	stateful

At the bottom, there is a table with columns: Edit, Active, Name, Connection Type, Type, Delete. The first row shows: Test LAN to LAN dialout

Function		Description
Name	HeadOffice	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 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	

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.

The screenshot shows the PPTP configuration interface. The fields are as follows:

Field	Value
Name	BranchOffice
Connection Type	LAN to LAN
Type	Dial out
Server IP Address (or Domain Name)	69.121.1.30
Peer Network IP	192.168.1.0
Netmask	255.255.255.0
Username	username
Password	*****
Auth Type	Chap(Auto)
Data Encryption	Auto
Key Length	Auto
Mode	stateful
Active as default route	<input type="checkbox"/> Enable

Buttons: Add, Edit, Delete

Table Headers: Edit, Active, Name, Connection Type, Type, Delete

Function		Description
Name	HeadOffice	Given name of PPTP connection
Connection Type	LAN to LAN	Select LAN to LAN 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	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	

IPSec (IP Security Protocol)

The screenshot displays the configuration page for an IPSec tunnel. It includes a 'Parameters' section with the following fields:

- Name:** A text input field.
- Local Network:** A dropdown menu set to 'Single Address' and an 'IP Address' input field.
- Remote Secure Gateway IP:** An 'IP Address' input field.
- Remote Network:** A dropdown menu set to 'Single Address' and an 'IP Address' input field.
- IKE Mode:** A dropdown menu set to 'Main'.
- Local ID Type:** A dropdown menu set to 'Default'.
- Remote ID Type:** A dropdown menu set to 'Default'.
- Hash Function:** A dropdown menu set to 'MD5'.
- IPSec Proposal:** A list of proposals with checkboxes for ESP and AH. 'ESP' is selected.
- Perfect Forward Secrecy:** A dropdown menu set to 'NOCRYPTO1 (DH12)'.
- Phase 1 (IKE) Lifetime:** A text input field set to '300' minutes.
- Phase 2 (IPSec) Lifetime:** A text input field set to '60' minutes.
- Phase 1 to the IP (0.0.0.0/0.0.0.0):** A dropdown menu set to 'Internal' and an 'IP' input field.
- Disconnection Time after no traffic:** A text input field set to '180' minutes.
- Reconnection Time:** A text input field set to '3' minutes.

At the bottom, there is a table with columns: 'Full', 'Active', 'Name', 'Local Subnet', 'Remote Subnet', 'Remote Gateway', 'IPSec Proposal', and 'Fields'. The 'Active' column contains a checkbox.

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

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

Name: This is a given name of the connection.

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

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

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

IPSec Proposal: This is selected IPSec security method.

IPSec VPN Connection

The screenshot shows a configuration window for an IPsec VPN connection. The 'Parameters' section includes fields for Name, Local Network (with a dropdown for Single Address and an IP Address field), Remote Secure Gateway IP, Remote Network (with a dropdown for Single Address and an IP Address field), IKE Mode (Main), Pre-shared Key, Local ID Type (Default), Remote ID Type (Default), ID Content, Hash Function (MD5), Encryption (2DES), DH Group (MOCP1024 (DH2)), Authentication (MD5), and Encapsulation (2DES). There are checkboxes for Perfect Forward Secrecy, Phase 1 (ISAKMP) Lifetime (60 min), Phase 2 (IPsec) Lifetime (60 min), PFS (on/automatic), PFS to the IP (0/1/2/3/4/5/6/7/8), Interval (10 seconds), Downconnection Time after no traffic (180 seconds), and Reconnection Time (3 min). At the bottom, there is a table for VPN tunnels with columns for Edit, Active, Name, Local Subnet, Remote Subnet, Remote Gateway, IPsec Proposal, and Delete.

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

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

Single Address: The IP address of the local host.

Subnet: The subnet of the local network. For example, IP: 192.168.1.0 with netmask 255.255.255.0 specifies one class C subnet starting from 192.168.1.1 (i.e. 192.168.1.1 through to 192.168.1.254).

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

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

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

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

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

Local ID:

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

Remote ID:

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

Hash Function: It is a Message Digest algorithm which converts 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 encryption method.

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

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

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



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

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

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

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

-  **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
-  **Phase 2 (IPsec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes.

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

PING for Keep Alive:

-  **None:** The default setting is None. To this mode, it will not detect the remote IPsec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPsec will be disconnected after the time you set in this function.
-  **PING:** This mode will detect the remote IPsec peer has lost or not by pinging specify IP address.
-  **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPsec peer has lost. Please be noted, it must be enabled on the both sites.

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

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

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

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

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

is minimum time interval for this function.

Click Edit/Delete to save your changes.

Example: Configuring an IPsec LAN to LAN VPN Connection

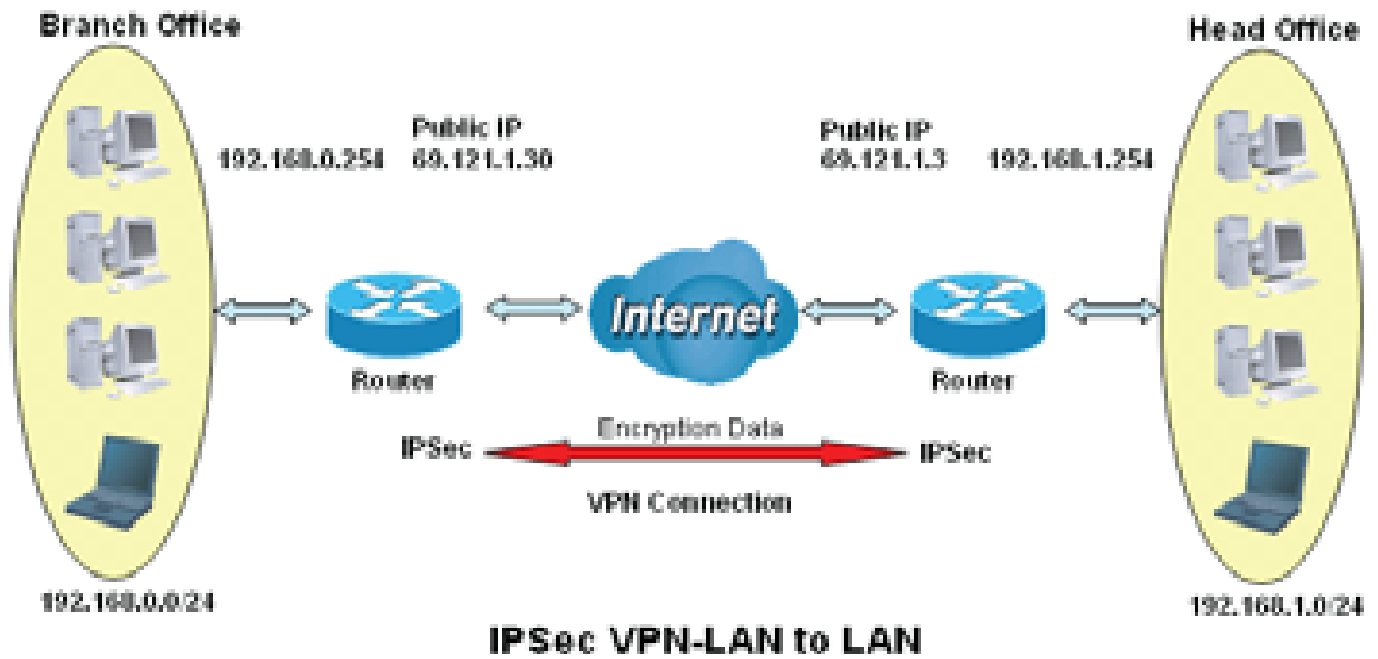


Table 3: Network Configuration and Security Plan

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



Attention

Both office LAN networks must be in different subnet with the LAN-LAN application.

Functions of Pre-shared keys, VPN Connection Type and Security Algorithm must be identically setup on both sides.

Configuring IPSec VPN in the Head Office

The screenshot shows the configuration page for an IPSec VPN connection. The configuration is as follows:

- Name:** IPSec_HeadOffice
- Local Network:** Subnet (selected), IP Address: 192.168.1.0, Netmask: 255.255.255.0
- Remote Secure Gateway IP (or Hostname):** 69.121.1.30
- Remote Network:** Subnet (selected), IP Address: 192.168.0.0, Netmask: 255.255.255.0
- Mode:** Main
- Pre-shared Key:** 12345678
- Local ID Type:** Default, ID Content: (empty)
- Remote ID Type:** Default, ID Content: (empty)
- Hash Function:** MD5
- Encryption:** 3DES
- DH Group:** MODP1024 (DHG)
- Authentication:** MD5
- Encryption:** 3DES
- IPSec Proposal:**
 - ESP
 - AH
- Authentication:** MD5
- Prefer Forward Security:** None
- Phase 1 (IKE) SA Lifetime:** 300 minutes
- Phase 2 (IPSec):** 60 minutes
- PreQ to the IP (0.0.0.0/0.0.0.0):** 1.0.0.0, Interval: 10 seconds
- PreQ for keepalive:** None
- Disconnection Time after no traffic:** 180 seconds (180 at least)
- Reconnection Time:** 3 minutes (3 at least)

Function		Description
Name	IPSec_HeadOffice	Give a name of IPSec Connection
Local Network	Subnet	Select Subnet from Local Network drop-down menu.
IP Address	192.168.1.0	Head office network
Netmask	255.255.255.0	
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 Remote Network drop-down menu
IP Address	192.168.0.0	Branch office network
Netmask	255.255.255.0	
Pre-shared Key	12345678	Security plan
Authentication	MD5	
Encryption	3DES	
Prefer Forward Security	None	

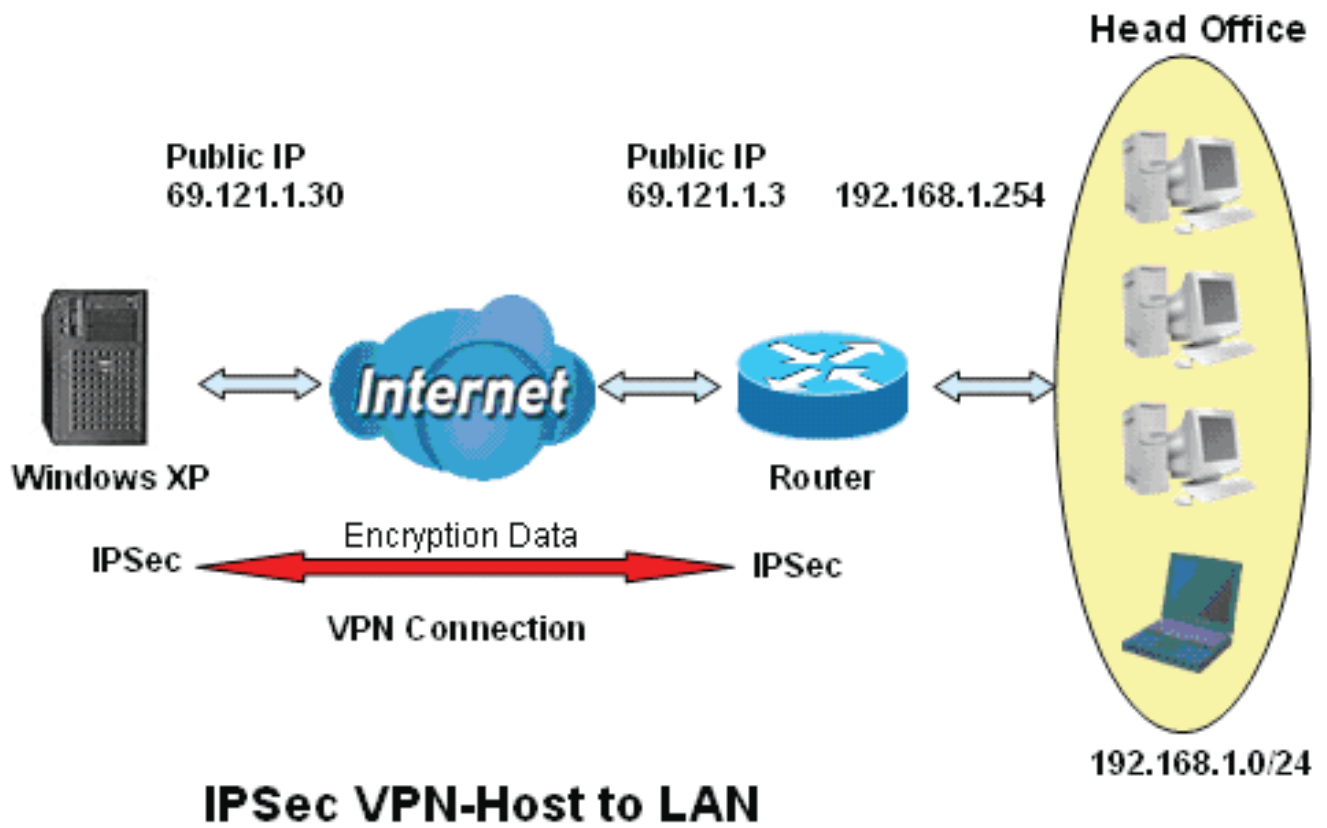
Configuring IPSec VPN in the Branch Office

The screenshot shows the configuration page for an IPSec connection named 'IPSec_BranchOffice'. The configuration is as follows:

- Name:** IPSec_BranchOffice
- Local Network:** Subnet (dropdown), IP Address: 192.168.0.0, Netmask: 255.255.255.0
- Remote Secure Gateway IP (or Hostname):** 69.121.1.3
- Remote Network:** Subnet (dropdown), IP Address: 192.168.1.0, Netmask: 255.255.255.0
- Pre-shared Key:** 12345678
- Authentication:** MD5
- Encryption:** 3DES
- Prefer Forward Security:** None
- Phase 1 (ISAKMP) Lifetime:** 480 minutes
- Phase 2 (IPsec) Lifetime:** 60 minutes
- Pre-Shared Key (MD5/3DES/SHA1):** 12345678, Label: 15 seconds
- Disconnection Time after idle:** 180 seconds (180 at least)
- Reconnection Time:** 3 minutes (3 at least)

Function		Description
Name	IPSec_BranchOffice	Give a name of IPSec Connection
Local Network	Subnet	Select Subnet from Local Network drop-down menu.
IP Address	192.168.0.0	Branch office network
Netmask	255.255.255.0	
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 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

The screenshot shows the configuration page for an IPSec VPN connection. The 'Name' field is set to 'IPSec'. The 'Local Network' is 'Subnet' with IP '192.168.1.0' and netmask '255.255.255.0'. The 'Remote Secure Gateway IP' is '69.121.1.30'. The 'Remote Network' is 'Single Address' with IP '69.121.1.30'. The 'Pre-shared Key' is '12345678'. The 'Authentication' is 'MD5' and 'Encryption' is '3DES'. The 'Phase 1 (IKE SA Lifetime)' is '480' minutes. The 'Phase 2 (IPSec)' is '60' minutes. The 'Phase 2 to the IP (IPSEC REKEY)' is '10' seconds. The 'Prefer Forward Security' is 'None'. There are 'Add' and 'Edit/Cancel' buttons at the bottom.

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

L2TP (Layer Two Tunneling Protocol)

The screenshot shows the L2TP configuration page with the 'Remote Access' connection type selected. The configuration fields are as follows:

Field	Value
Name	
Type	Default
Username	
Tunnel Authentication	<input type="checkbox"/> Enable
Remote Host Name(Optional)	
IPsec	<input type="checkbox"/> Enable
Perfect Forward Secrecy	None
Connection Type	Remote Access
Server IP Address(or Domain Name)	
Password	
Secret	
Local Host Name(Optional)	
Authentication	None
Pre-shared Key	
Auth. Type	CHAPv2
Active as default route	<input type="checkbox"/> Enable
Exception	None

Buttons: Add, Edit, Delete

Edit	Active	Name	Connection Type	Type	Delete
<input type="checkbox"/>	<input type="checkbox"/>	test	remote access	default	<input type="checkbox"/>

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

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

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

Name: This is a given name of the connection.

Connection Type: Displays the condition of your L2TP tunneling connection.

Type: This refers to your router whether it operates as a client or a server, Dial-out or Dial-in respectively.

L2TP Connection-Remote Access

The screenshot shows the L2TP configuration page with the 'Dial-out' connection type selected. The configuration fields are as follows:

Field	Value
Name	
Type	Dial-out
Username	
Tunnel Authentication	<input type="checkbox"/> Enable
Remote Host Name(Optional)	
IPsec	<input type="checkbox"/> Enable
Perfect Forward Secrecy	None
Connection Type	Remote Access
Server IP Address(or Domain Name)	
Password	
Secret	
Local Host Name(Optional)	
Authentication	None
Pre-shared Key	
Auth. Type	CHAPv2
Active as default route	<input type="checkbox"/> Enable
Exception	None

Buttons: Add, Edit, Delete

Edit	Active	Name	Connection Type	Type	Delete
<input type="checkbox"/>	<input type="checkbox"/>	test	remote access	dialout	<input type="checkbox"/>

Connection Type: Remote Access or LAN to LAN

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

Connection Type: Remote Access or LAN to LAN.

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

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

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

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

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

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

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

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

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

IPSec: Enable for enhancing your L2TP VPN security.


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

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

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

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

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

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

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

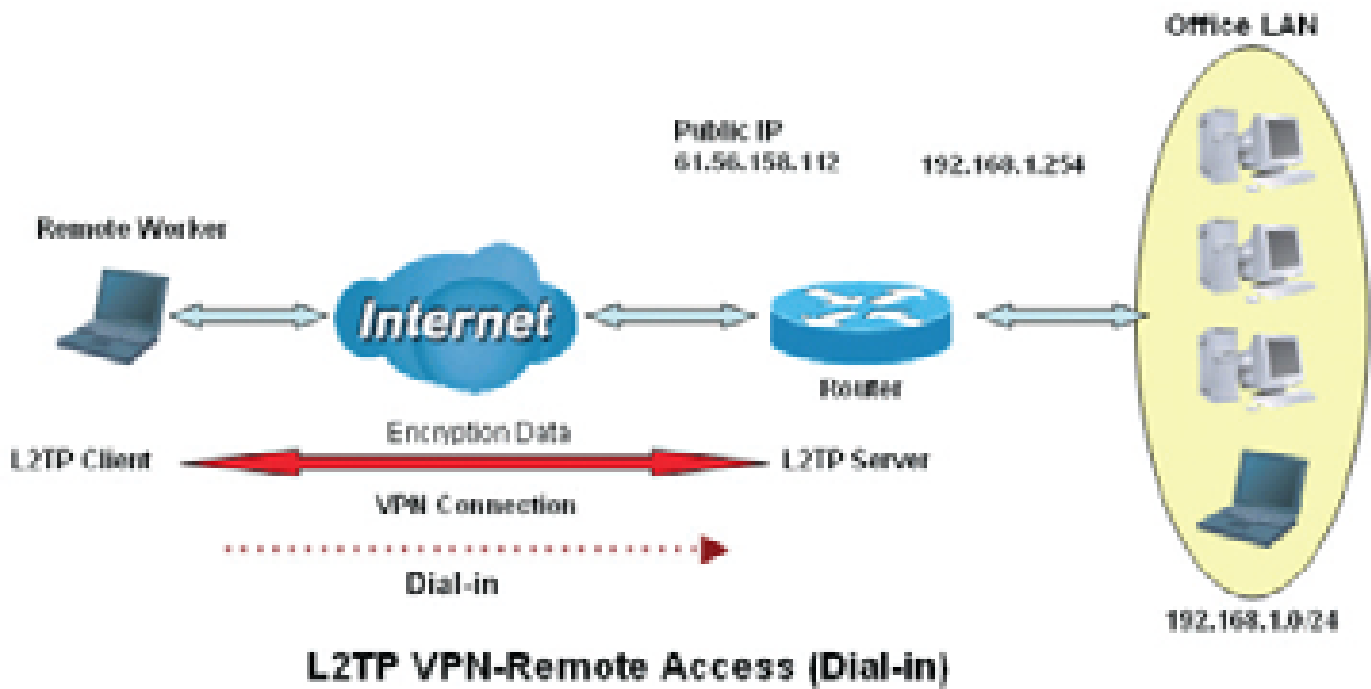
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol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

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

Click Edit/Delete to save your changes.

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

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



Configuring L2TP VPN in the Office

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

The screenshot shows the configuration page for an L2TP VPN connection. The configuration is as follows:

- Name:** VPN_L2TP
- Connection Type:** Remote Access
- Type:** Dial in
- Private IP Address Assigned to Dialin user:** 192.168.1.200
- Username:** username
- Password:** 123456
- Auth. Type:** Chap(Auto)
- Tunnel Authentication:** Enable
- Secret:** (empty)
- Active as default route:** Enable
- Remote Host Name (Optional):** (empty)
- Local Host Name (Optional):** (empty)
- IPSec:** Enable
- Authentication:** MD5
- Encryption:** 3DES
- Perfect Forward Secrecy:** None
- Pre-shared Key:** 12345678

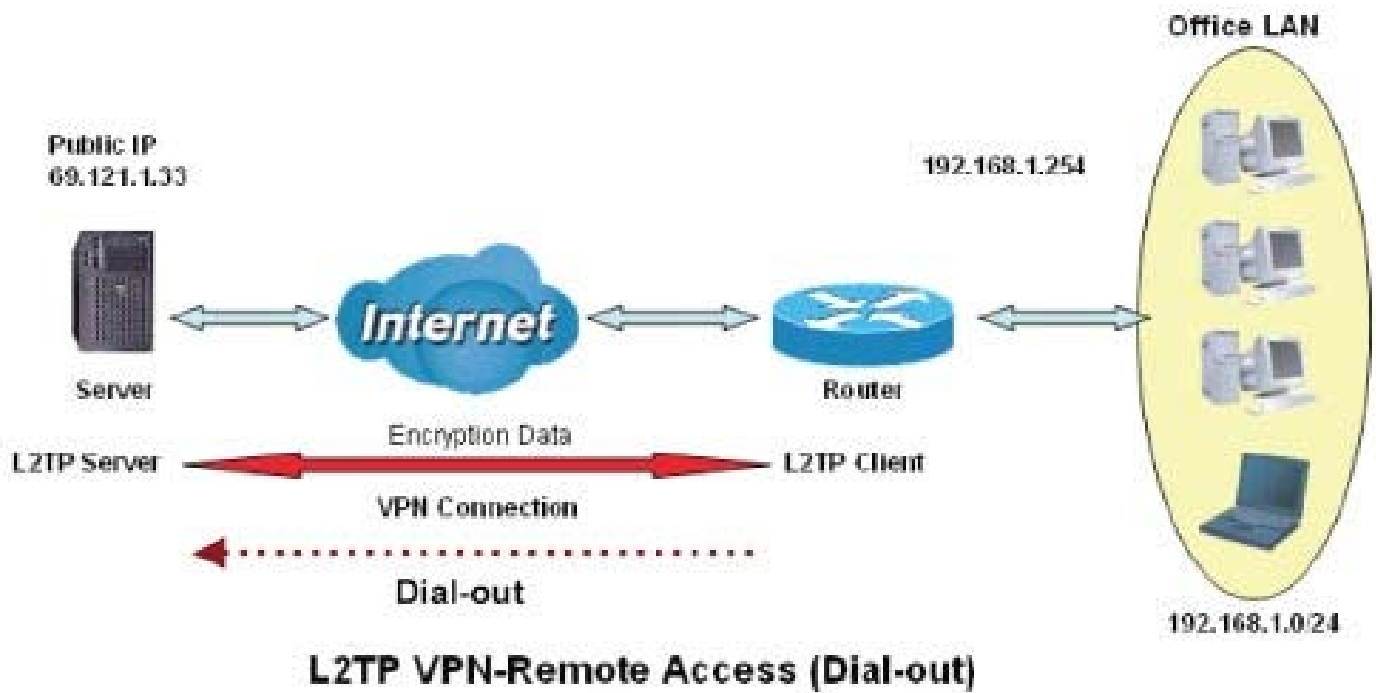
Buttons: Add, Edit / Delete

Edit	Active	Name	Connection Type	Type	Delete
------	--------	------	-----------------	------	--------

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 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 for most cases
IPSec	Enable	Both sides should use the same value
Authentication	MD5	
Encryption	3DES	
Perfect Forward Secrecy	None	
Pre-Shared Key	12345678	

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

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



Configuring 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.

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 Both sides should use the same value
Authentication	MD5	
Encryption	3DES	
Perfect Forward Secrecy	None	
Pre-Shared Key	12345678	

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

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

L2TP Connection - LAN to LAN

The screenshot shows a configuration interface for L2TP connections. The 'Parameters' section is divided into several groups of fields. The 'Name' field is empty. The 'Type' is set to 'Dial out'. The 'Peer Network IP' is empty. The 'Username' is empty. The 'Tunnel Authentication' checkbox is unchecked. The 'Remote Host Name (Optional)' is empty. The 'IPsec' checkbox is unchecked. The 'Perfect Forward Secrecy' is set to 'None'. The 'Connection Type' is set to 'LAN to LAN'. The 'Server IP Address (or Domain Name)' is empty. The 'Netmask' is empty. The 'Password' and 'Secret' fields are empty. The 'Local Host Name (Optional)' is empty. The 'Authentication' is set to 'None'. The 'Pre-shared Key' is empty. There are also buttons for 'Auth Type' (Chap/Auto), 'Add as default route' (disabled), and 'Encryption' (None). At the bottom, there is a table with columns: Edit, Active, Name, Connection Type, Type, and Delete.

L2TP VPN Connection

Name: A given name for the connection

Connection Type: Remote Access or LAN to LAN.

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

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

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

Peer Network IP: Enter Peer network IP address.

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

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

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

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

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

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

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

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

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

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

IPSec: Enable for enhancing your L2TP VPN security.

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

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

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

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

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

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

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

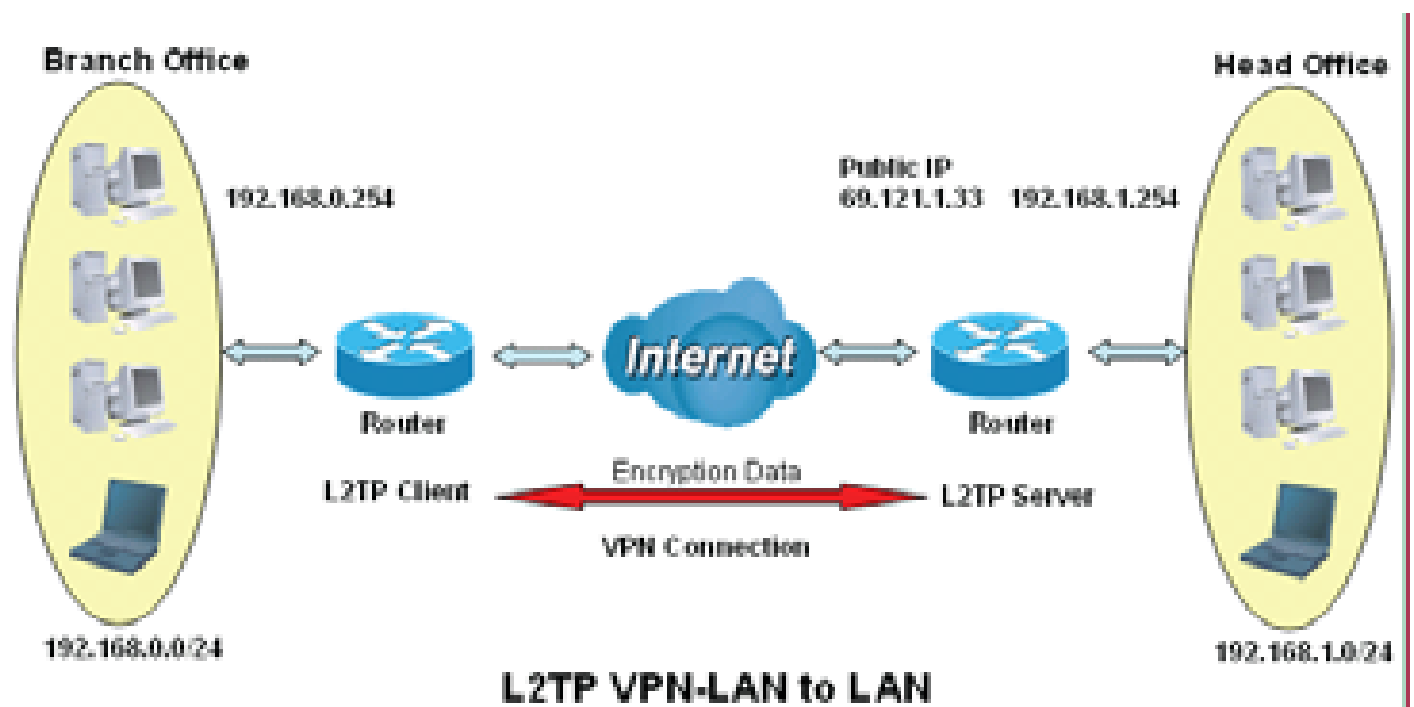
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol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

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

Click Edit/Delete to save your changes.

Example: Configuring L2TP LAN-to-LAN VPN Connection

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



Attention

Both office LAN networks must be in different subnet with the LAN-LAN application.

Functions of **Pre-shared keys**, **VPN Connection Type** and **Security Algorithm** must be identically setup on both sides.

Configuring L2TP VPN in the Head Office

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

The screenshot shows the configuration page for an L2TP connection. The 'Parameters' section includes the following fields and values:

- Name: HeadOffice
- Connection Type: LAN to LAN
- Type: Dial in
- Private IP Address Assigned to Dialin user: 192.168.1.200
- Peer Network IP: 192.168.0.0
- Network: (empty)
- Username: username
- Password: 123456
- Auth. Type: Chap(Auto)
- Tunnel Authentication: Enable
- Secret: (empty)
- Active as default route: Enable
- Remote Host Name (Optional): (empty)
- Local Host Name (Optional): (empty)
- IPSec: Enable
- Authentication: MD5
- Encryption: 3DES
- Perfect Forward Secrecy: None
- Pre-shared Key: 12345678

Buttons for 'Add', 'Edit/Details', and a table with columns 'Edit', 'Active', 'Name', 'Connection Type', 'Type', and 'Delete' are also visible.

Function		Description
Name	HeadOffice	Give a name of 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 branch office network
Peer Network IP	192.168.0.0	Branch office network
Username	username	An assigned username and password to authenticate branch office network
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 Both sides should use the same value
Authentication	MD5	
Encryption	3DES	
Perfect Forward Secrecy	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.

The screenshot shows the L2TP configuration page with the following settings:

- Name: BranchOffice
- Connection Type: LAN to LAN
- Type: Dial out
- Base IP Address (or Domain Name): 69.1.1.30
- Peer Network IP: 192.168.1.0
- Netmask: 255.255.255.0
- Username: username
- Password: 123456
- Auth. Type: Chap (Auto)
- Tunnel Authentication: Enable
- Secret:
- Action 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	BranchOffice	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN 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	IP address assigned to branch office network
Peer Network IP	192.168.1.0	Head office network
Netmask	255.255.255.0	
Username	username	An assigned username and password to authenticate branch office network
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	
Encryption	3DES	
Perfect Forward Secrecy	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.



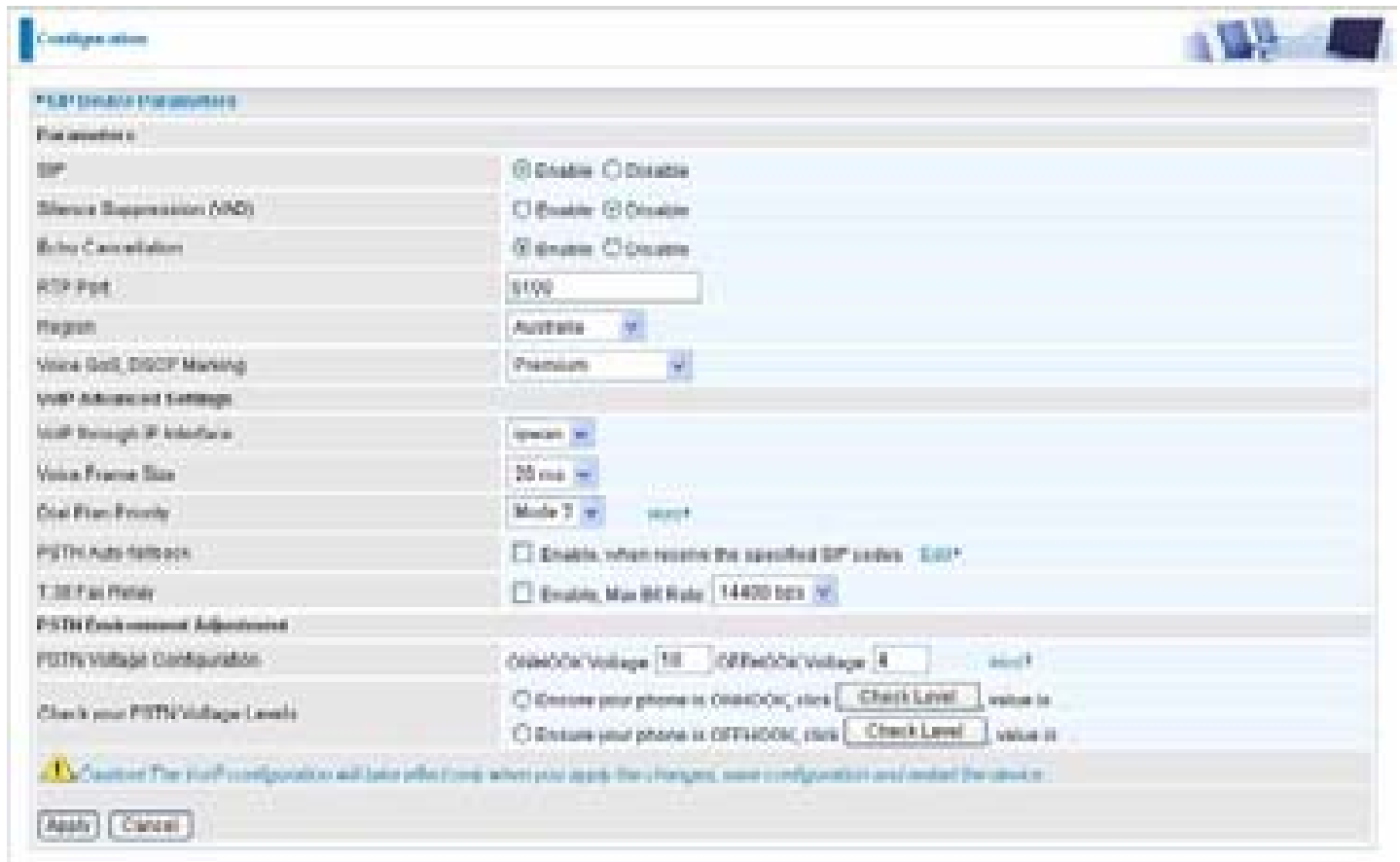
After completing VoIP configuration, remember to apply the changes. **SAVE CONFIG** and restart to activate your VoIP.

Attention

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 Provider.



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 for isolating the echo while you are on the phone. This helps you not to hear much of your own voice reflecting on the phone while you talk. Default is set to Enable.

RTP Port: Provide the based 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 user to select the country for which the VoIP device must work. 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: To be sure the router(s) in the backbones network have the capability in executing and checking the DSCP through-out the QoS network.

Advanced – Parameters



The screenshot shows the 'VoIP Advanced Settings' configuration page. It includes the following fields and options:

- VoIP through IP Interface:** A dropdown menu set to 'ipwan'.
- Voice Frame Size:** A dropdown menu set to '20ms'.
- Dial Plan Priority:** A dropdown menu set to 'Mode 1'.
- PSTN Auto-fallback:** A checkbox labeled 'Enable, when receive the specified SIP codes' with an 'Edit' link.
- T.38 Fax Relay:** A checkbox labeled 'Enable, Max BR Rate' with a dropdown menu set to '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 locates some where in 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 in both of Caller and Receiver.

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

PSTN Auto-fallback: Whenever VoIP SIP responses error and error code matching with the codes in the **Edit** section, the VoiP calls will automatically fallback to PSTN. In the other word, the call will be called via the PSTN when VoIP SIP returns an error code.

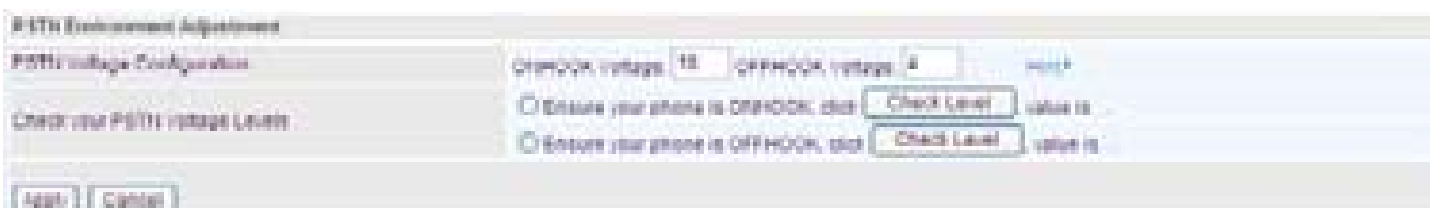
Click the Edit to add or remove the responses code. To be sure the code is separated by a comma (,).

For more information about SIP responses codes, please check [Here](#) to link to <http://voip-info.org/wiki/view/sip+response+codes> where you can get to know the meaning of each error code.

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 are support this feature and 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.



The screenshot shows the 'PSTN Environment Adjustment' configuration page. It includes the following fields and options:

- PSTN Voltage Configuration:** Two input fields for 'ONHOOK voltage' and 'OFFHOOK voltage'.
- Check your PSTN voltage level:** Two radio buttons: 'Ensure your phone is ONHOOK, click' and 'Ensure your phone is OFFHOOK, click'. Each has a 'Check Level' button and a 'value is' label.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom.

Note: ONHOOK means hung up.

To take your phone OFFHOOK, lift the receiver then press Hook/Flash until you hear your normal PSTN dialtone, not your VoIP dialtone. 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 reflects and contains basic settings for the VoIP module from selected provider in the Wizard section. Fail to provide correct information will halt making calls out to the Internet.

The screenshot shows a web-based configuration interface for SIP accounts. At the top, there's a 'SIP Accounts' section with a form containing the following fields:

- Profile Name: [text input]
- Registrar Address (or Hostname): [text input]
- Registrar Port: [text input, value: 5060]
- Expire (seconds): [text input, value: 3600]
- User Domain/Realm: [text input]
- Outbound Proxy Address: [text input]
- Outbound Proxy Port: [text input, value: 5060]
- Password: [text input]
- Phone Number: [text input]
- Username: [text input]
- Display Name: [text input]
- Direct in Dial: [dropdown menu, value: none]

Below the form, there are buttons for 'Add' and 'Edit / Delete'. Underneath is a table with the following structure:

Edit	Profile Name	Registrar Address	Phone Number	Delete
<input type="radio"/>	Phone Port 1			<input type="button" value="Delete"/>
<input type="radio"/>	Phone Port 2			<input type="button" value="Delete"/>

Profile Name: User-defined name is for identifying the Profile.

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 device.

Expire: Expire time for the registration message sending.

User Domain/Realm: Set 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 device is 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.

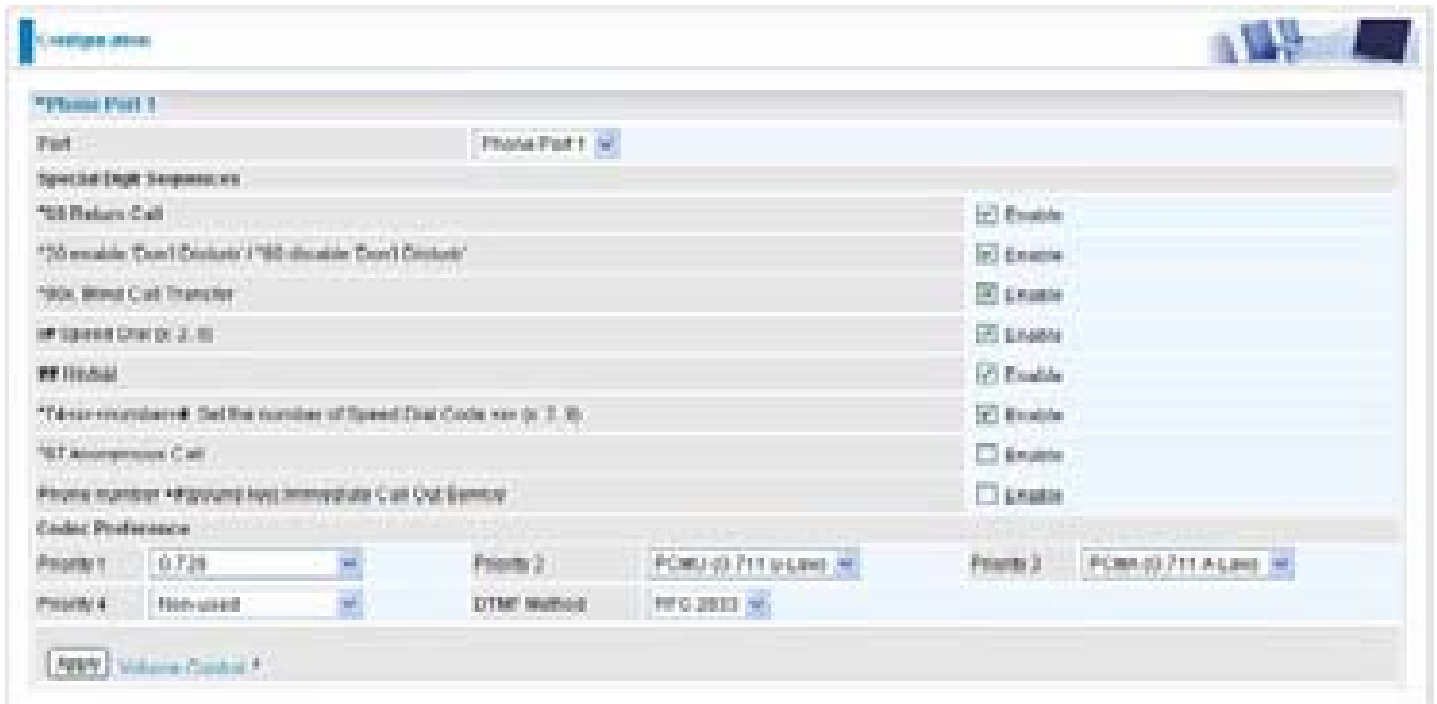
Password: This parameter holds the password used for authentication within VoIP SIP registrar.

Display Name: This parameter will be appeared on the Caller ID.

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

Phone Port

This section displays status and allows you to edit the account information of your Phones. Click Edit to update your phone information.



Port: It allows you to change the phone port setting for specify 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 set the No Disturb on. Your phone will not ring if someone calls.

***80 (Do not Disturb OFF):** Dial *80 to set the No Disturb off. Your will be able to hear ring tone when someone calls.

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

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

Redial: Press ## to redial the latest number you dialed. 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 the own phone number for each call and it will not be displayed on the remote site. 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 *Special Dial Code section in this Manual for more details.*

Codec Preference

Codec is known as Coder-Decoder used for data signal conversion. Set the priority of voice compression; Priority 1 owns the top priority.

G.729: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.

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

G.726-32: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption. Currently only supports bit rate with 32Kbps.

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

Volume Control



Volume control helps you to adjust the voice quality of telephone to the best comfortable listening level.

Press “-“, the minus sign, to reduce either microphone or/both speaker’s level of your telephone.

Press “+“, the plus sign, to increase either microphone or/both speaker’s level of your telephone.

PSTN Dial Plan (Router with LINE port only)

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

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



Edit	Prefix	Number of Digits	Action	Delete
<input type="radio"/>	000	3	Dial with Prefix	<input type="radio"/>
<input type="radio"/>	100	3	Dial with Prefix	<input type="radio"/>

Prefix: Specify number(s) for switching to a PSTN call.

Number of Digits: Specify the total number of digits wish to dial out. Maximum digit number is 15.


Action: Specify a dialing method you wish to make PSTN call(s).

 **Dial with Prefix:** The dialed number **with** prefix will be sent call through the PSTN.


Note: *The actual dialed number of valid digits length requires matching in the Number of Digits filed.*

 **Dial without Prefix:** The dialed number will be sent call through the PSTN **without** prefix.

Note: *The actual dialed number of valid digits length requires matching in the Number of Digits filed.*

 **Dial at Timeout:** The dialed number will be sent call through the PSTN **with** the prefix when timeout starts. This timeout activates when no more digits are dialed in a specific duration.

Note: *The actual dialed number of valid digits length MUST NOT exceed in the Number of Digits filed.*

 **Dial at Timeout no Prefix:** The dialed number will be sent call through the PSTN **without** prefix when timeout starts. This timeout activates when no more digits are dialed in a specific duration.

Note: *The actual dialed number of valid digits length MUST NOT exceed in the Number of Digits filed.*



Attention

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

- Power is down
- Internet service fail. i.e. lost of WAN IP address
- SIP option is disabled. See VoIP General Settings section.
- Calls match with rule(s) defined in the PSTN Digit Plan.
- SIP service is not accessible. This exclude when:
 - User manually disable Registration
 - User insert a wrong authentication username or password
 - User dials a wrong SIP number, only and if the PSTN
 - auto-fallback function is not enabled. See VoIP General Settings / Advance for more information.

PSTN Dial Plan Examples:

1. Dial with Prefix

The screenshot shows the 'Configuration' page for a PSTN Dial Plan. The 'Parameters' section is expanded to show the following settings:

Parameter	Value
Prefix	01223
Number of Digits	8 (range 8-15)
Action	Dial with Prefix

Buttons for 'Add' and 'Edit / Delete' are visible at the bottom left. A table at the bottom lists the configuration with columns for 'Edit', 'Prefix', 'Number of Digits', 'Action', and 'Delete'.

If you dial 01223 707070, number 01223707070 will be dialed out via FXO to make a regular phone call.

2. Dial without Prefix

The screenshot shows the 'Configuration' page for a PSTN Dial Plan. The 'Parameters' section is expanded to show the following settings:

Parameter	Value
Prefix	9
Number of Digits	3 (range 3-15)
Action	Dial without Prefix

Buttons for 'Add' and 'Edit / Delete' are visible at the bottom left. A table at the bottom lists the configuration with columns for 'Edit', 'Prefix', 'Number of Digits', 'Action', and 'Delete'.

If you dial 9102, the number 102 will only be dialed out via FXO port to make a regular phone call.

3. Dial at Timeout

The screenshot shows a configuration window titled "Configuration" with a sub-header "Dial at Timeout". Under the "Parameters" section, there are three fields: "Prefix" with the value "01223", "Number of Digits" with the value "7" and a range "(3-10)", and "Action" with the value "Dial at Timeout". Below the fields are two buttons: "Add" and "Edit/ Delete". At the bottom, there is a table with the following columns: "Edit", "Prefix", "Number of Digits", "Action", and "Delete".

Edit	Prefix	Number of Digits	Action	Delete
------	--------	------------------	--------	--------

If you only dial 01223 7070 and no more numbers, after the timeout activates, 012237070 will be dialed to make a regular call via FXO port.

Even though 7070 (only 4 digits) does not match with number of digits 6 defined in the filed, 7070 is still a valid phone number since it has not exceeded 6 digits.

4. Dial at Timeout no Prefix

The screenshot shows a configuration window titled 'Configuration'. Under the 'Dial Plan' section, there are three input fields: 'Prefix' (empty), 'Number of Digits' (set to 6), and 'Action' (set to 'Dial at Timeout no Prefix'). Below these fields are three buttons: 'Add', 'Edit', and 'Delete'. At the bottom of the window, there is a table header with columns: 'Edit', 'Prefix', 'Number of Digits', 'Action', and 'Delete'.

If you only dial 97070 and no more numbers, after the timeout activates, 7070 will be dialed without prefix to make a regular call via FXO port.

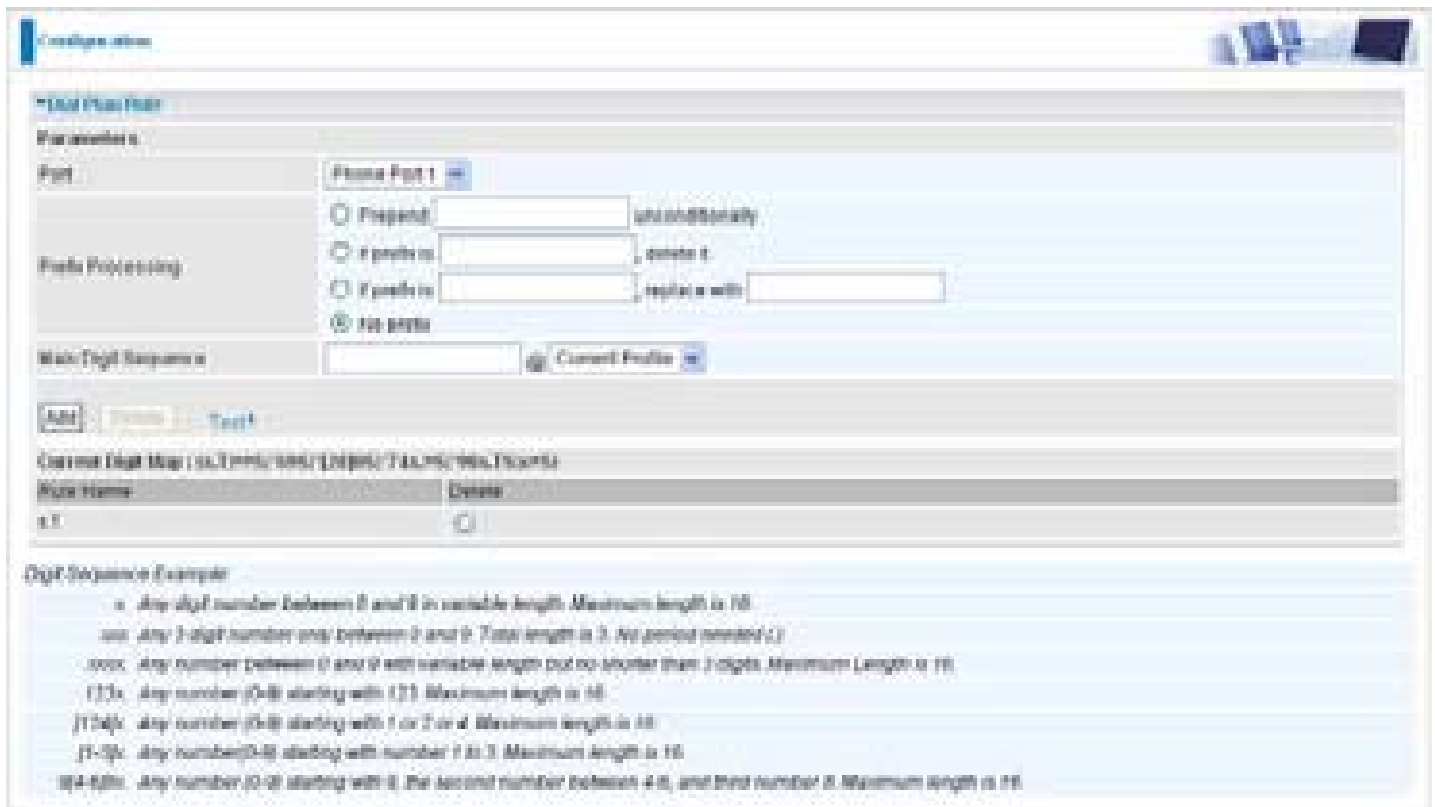
Even though 7070 (only 4 digits) does not match with number of digits 6 defined in the filed, 7070 is still a valid phone number since it has not exceed 6 digits.

VoIP Dial Plan

This section helps you to make a telephony number dialed as making a regular call via VoIP. You no longer need to memorize a long dial string of number for making a VoIP call. Go to Configuration > VoIP > VoIP Dial Plan.

Dial Plan Rules

Click the Add button to create and define a VoIP dial-plan rule(s).



Prefix Processing:

Prepend xxx unconditionally: xxx number is appended unconditionally to the front of the dialing number 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 dialing numbers before making a call.

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

No prefix: No prefix is appended to the front of the dialing numbers. It is set as in default settings.

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

x: Any numeric number between 0 and 9.

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

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

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

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

<@ PSTN>: Meaning making call(s) via the PSTN line.

<@ENUM>: Meaning making a VoIP SIP direct call via E.164 number ("ENUM") to an ENUM callee.

Electronic Number (ENUM) uses the 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 allows you to further customize their settings to suit your personal needs such as call forwarding setting, call waiting time length, conference call feature, anonymous call feature and incoming no answer timer.

The screenshot shows the 'Call Features Setting' configuration page for 'Phone Port 1'. The settings are as follows:

- Call Forwarding:** Three checkboxes are present: 'No calls forward to' (unchecked), 'Busy calls forward to' (unchecked), and 'No Answer calls forward to' (unchecked). Each checkbox is followed by an empty text input field.
- Incoming No Answer Timer:** A text input field followed by the label '(seconds)'.
- Call Waiting:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Anonymous Call:** Radio buttons for 'Enable' and 'Disable' (selected).
- Conference Call:** Radio buttons for 'Enable' and 'Disable' (selected).

Buttons for 'Apply' and 'Default' are located at the bottom left of the configuration area.

Speed Dial

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

The screenshot shows the 'Speed Dial' configuration page for 'Phone Port 1'. It features a table with three columns for speed dial entries. Each column has a 'SP' label and an empty text input field.

SP		SP		SP	

An 'Apply' button is located at the bottom left of the configuration area.

Ring & Tone

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

Ring & Tone Configuration

Country Specific Ring & Tone

Region:

Ring Parameters

	On 1	Off 1	On 2	Off 2	On 3	Off 3
Ring Cadence (in ms)	<input type="text" value="2000"/>	<input type="text" value="4000"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Tone Parameters

	Parameter		Parameter		Cadence					
	Freq 1	Power 1	Freq 2	Power 2	On 1	Off 1	Repeat 1	On 2	Off 2	Repeat 2
Dial Tone	<input type="text" value="350"/>	<input type="text" value="-13"/>	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="1000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Reconnect Tone	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="2000"/>	<input type="text" value="4000"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Busy Tone	<input type="text" value="480"/>	<input type="text" value="-24"/>	<input type="text" value="520"/>	<input type="text" value="-24"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Waiting Tone	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="2000"/>	<input type="text" value="10000"/>	<input type="text" value="1"/>	<input type="text" value="1000"/>	<input type="text" value="10000"/>	<input type="text" value="1"/>
Answer Tone	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Calling Card 'Busy' Tone	<input type="text" value="341"/>	<input type="text" value="-20"/>	<input type="text" value="1477"/>	<input type="text" value="-20"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="30"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
Call Waiting Tone	<input type="text" value="440"/>	<input type="text" value="-30"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="400"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Confuse Tone	<input type="text" value="100"/>	<input type="text" value="-13"/>	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Error Tone	<input type="text" value="300"/>	<input type="text" value="-20"/>	<input type="text" value="1379"/>	<input type="text" value="-20"/>	<input type="text" value="200"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="274"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Intercept Tone	<input type="text" value="440"/>	<input type="text" value="-24"/>	<input type="text" value="520"/>	<input type="text" value="-24"/>	<input type="text" value="200"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Message Waiting Tone	<input type="text" value="350"/>	<input type="text" value="-13"/>	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="10"/>	<input type="text" value="1000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
Remote Busy Tone	<input type="text" value="480"/>	<input type="text" value="-24"/>	<input type="text" value="520"/>	<input type="text" value="-24"/>	<input type="text" value="200"/>	<input type="text" value="200"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Remote Congestion Tone	<input type="text" value="480"/>	<input type="text" value="-24"/>	<input type="text" value="520"/>	<input type="text" value="-24"/>	<input type="text" value="200"/>	<input type="text" value="200"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Off Hook Warning Tone	<input type="text" value="1400"/>	<input type="text" value="4"/>	<input type="text" value="1080"/>	<input type="text" value="4"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Preemption Tone	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1000"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Pronged Tone	<input type="text" value="341"/>	<input type="text" value="-20"/>	<input type="text" value="1477"/>	<input type="text" value="-20"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="30"/>	<input type="text" value="0"/>	<input type="text" value="1"/>
Reorder Tone	<input type="text" value="480"/>	<input type="text" value="-24"/>	<input type="text" value="520"/>	<input type="text" value="-24"/>	<input type="text" value="200"/>	<input type="text" value="200"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Reorder Warning Tone	<input type="text" value="1400"/>	<input type="text" value="-20"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="100"/>	<input type="text" value="10000"/>	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Ringback on Connection Tone	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="2000"/>	<input type="text" value="10000"/>	<input type="text" value="1"/>	<input type="text" value="2000"/>	<input type="text" value="10000"/>	<input type="text" value="1"/>
Service Tone	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Buffer Dial Tone	<input type="text" value="350"/>	<input type="text" value="-13"/>	<input type="text" value="440"/>	<input type="text" value="-13"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="3"/>	<input type="text" value="100"/>	<input type="text" value="100"/>	<input type="text" value="1"/>

CountrySpecificRing&Tone

Region: Select a country ring-tone, from the drop-down list, where you are located. This VoIP router provides default parameter of ring tones according to different countries. The ring-tone parameters are automatically displayed after entering a specific country. If your country is not in the list, you may manually create ring-tone parameters.

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 advanced user unless you are instructed to do so.

Click **Apply** to apply the settings.




QoS - Quality of Service

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

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

Prioritization

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

-  **High**
-  **Normal** (The default is normal priority for all of traffic without setting)
-  **Low**

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

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



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

Time Schedule: Scheduling your prioritization policy.

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

Protocol: The name of supported protocol.

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

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

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

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

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

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

Table 4: DSCP Mapping Table

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

Outbound IP Throttling (LAN to WAN)

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



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

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

information.

Protocol: The name of supported protocol.

Rate Limit: To limit the speed of outbound traffic

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

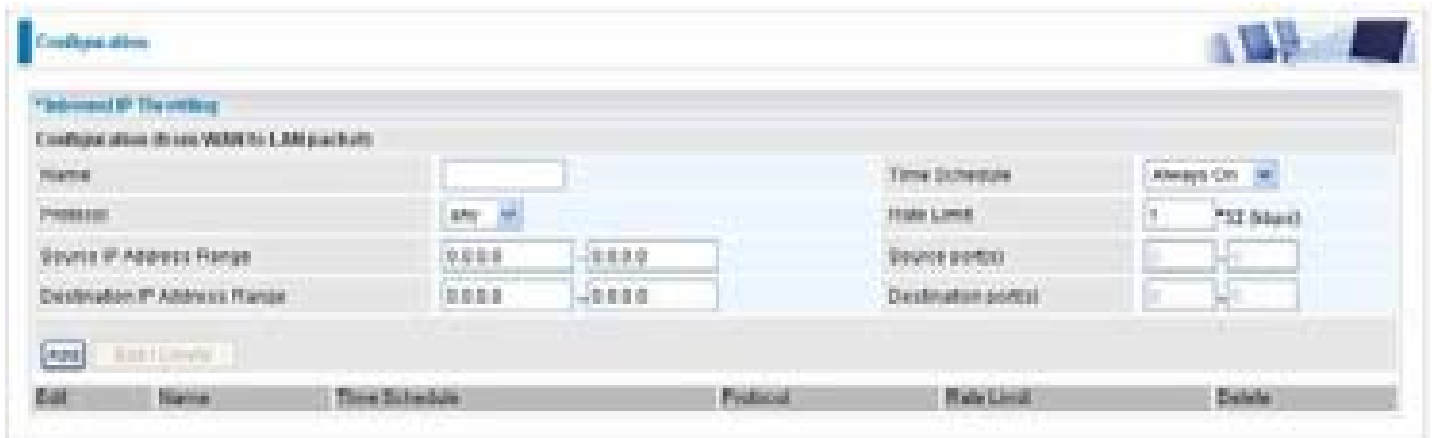
Source Port(s): The source port of packets to be monitored.

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

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

Inbound IP Throttling (WAN to LAN)

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



The screenshot shows a configuration window titled "Inbound IP Throttling" with the subtitle "Configuration (WAN to LAN packets)". The interface includes several input fields and a table at the bottom. The fields are: "Name" (text input), "Protocol" (dropdown menu), "Time Schedule" (dropdown menu set to "Always On"), "Rate Limit" (text input with a "32 kbps" multiplier), "Source IP Address Range" (two text inputs for range), "Destination IP Address Range" (two text inputs for range), "Source port(s)" (text input), and "Destination port(s)" (text input). Below the fields are "Add" and "Edit Rate Limit" buttons. At the bottom, a table lists existing configurations with columns for "Edit", "Name", "Time Schedule", "Protocol", "Rate Limit", and "Delete".

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

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

Protocol: The name of supported protocol.

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

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

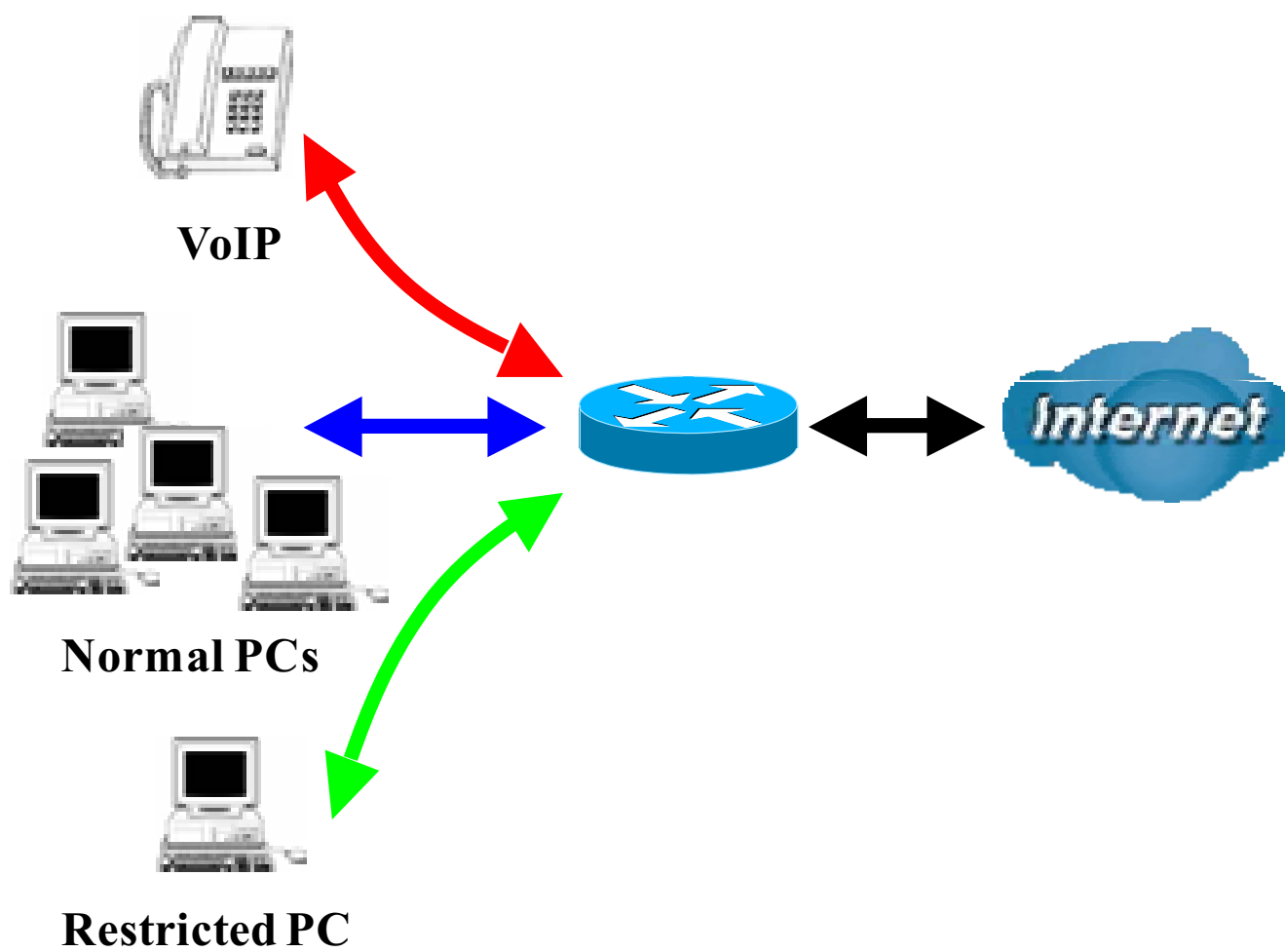
Source Port(s): The source port of packets to be monitored.

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

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

Example: QoS for your Network

Connection Diagram



Information and Settings

Upstream: 928 kbps

Downstream: 8 Mbps

VoIP User : 192.168.1.1

Normal Users : 192.168.1.2~192.168.1.5

Restricted User: 192.168.1.100

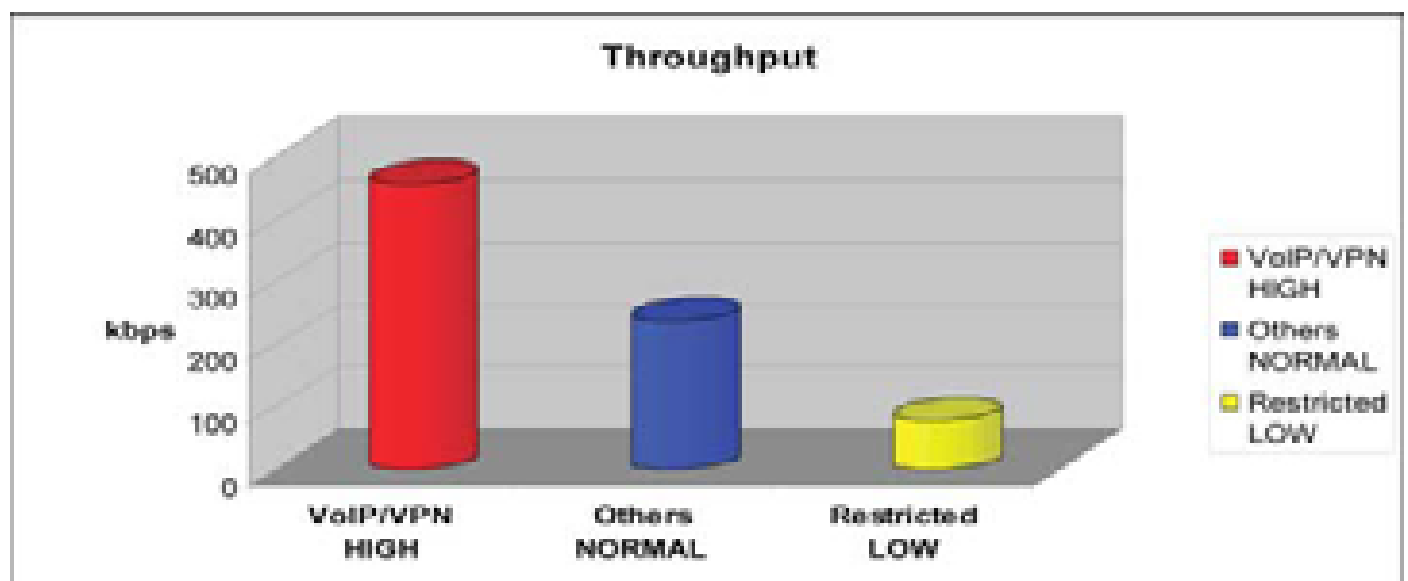
Configuration

Classification

Configuration from LAN to WAN packets

Name		Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	0.0.0.0 - 0.0.0.0	Source Port	
Destination IP Address Range	0.0.0.0 - 0.0.0.0	Destination Port	
DSCP Marking	Classified		

Lib	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input type="radio"/>	FTP	Always On	GRE	High	00110000 (0)	<input type="radio"/>
<input type="radio"/>	VoIP	Always On	Any	High	00111000 (0)	<input type="radio"/>
<input type="radio"/>	Restricted	TimeSlot	Any	High	00110000 (0)	<input type="radio"/>



Mission-critical application

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



The screenshot shows a configuration window for QoS rules. The rule is named 'FTP' and is set to 'Always On'. The priority is 'High'. The source IP address range is '0.0.0.0 - 0.0.0.0' and the destination IP address range is '0.0.0.0 - 0.0.0.0'. The DSCP marking is 'Gold service (5)'. The protocol is 'gre'. The source and destination ports are both set to '1'. Below the configuration fields are 'Add', 'Edit', and 'Delete' buttons. At the bottom, there is a table listing the configured rules.

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input checked="" type="radio"/>	FTP	Always On	GRE	High	Gold service (5)	<input type="radio"/>

The mission-critical application must be sent out smoothly without any dropping. Set priority as high level for preventing any other applications to saturate the bandwidth.

Voice application

Voice is latency-sensitive application. Most VoIP devices are use SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.



The screenshot shows a configuration window for QoS rules. The rule is named 'VoIP' and is set to 'Always On'. The priority is 'High'. The source IP address range is '192.168.1.1 - 192.168.1.1' and the destination IP address range is '0.0.0.0 - 0.0.0.0'. The DSCP marking is 'Gold service (5)'. The protocol is 'any'. The source and destination ports are both set to '1'. Below the configuration fields are 'Add' and 'Edit/Delete' buttons. At the bottom, there is a table listing the configured rules.

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input type="radio"/>	FTP	Always On	GRE	High	Gold service (5)	<input type="radio"/>
<input checked="" type="radio"/>	VoIP	Always On	Any	High	Gold service (5)	<input type="radio"/>

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

Restricted Application

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



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

Advanced setting by using IP throttling

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

Upstream: 928kbps (29*32kbps)

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

Voice Application: 128kbps (4*32kbps)

Restricted Application: 160kbps (5*32kbps)

Other Applications: 448kbps (14*32kbps)

$6+4+14+5=29$, $29*32\text{kbps}=928\text{kbps}$

Configuration

*** Outbound IP Traffic**

Configuration (From LAN to WAN packet)

Name:

Protocol:

Time Schedule:

Rate Limit: *32 (Mbps)

Source IP Address Range: -

Destination IP Address Range: -

Source port(s):

Destination port(s):

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
<input type="radio"/>	FTP	Always On	GRE	8	<input type="radio"/>
<input type="radio"/>	VoIP	Always On	Any	4	<input type="radio"/>
<input type="radio"/>	Restricted	TimeSlot	Any	4	<input type="radio"/>
<input type="radio"/>	Others	TimeSlot	Any	14	<input type="radio"/>

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

Configuration

*** Outbound IP Traffic**

Configuration (From LAN to WAN packet)

Name:

Protocol:

Time Schedule:

Rate Limit: *32 (Mbps)

Source IP Address Range: -

Destination IP Address Range: -

Source port(s):

Destination port(s):

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
<input checked="" type="radio"/>	Restricted	TimeSlot	Any	64	<input type="radio"/>

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



The screenshot displays a web-based configuration interface for a router, specifically the 'Port Forwarding' section. The interface is titled 'Configuration' and includes a 'Port Forwarding' tab. Below the tab is a 'Virtual Server Entry' form. The form contains the following fields:

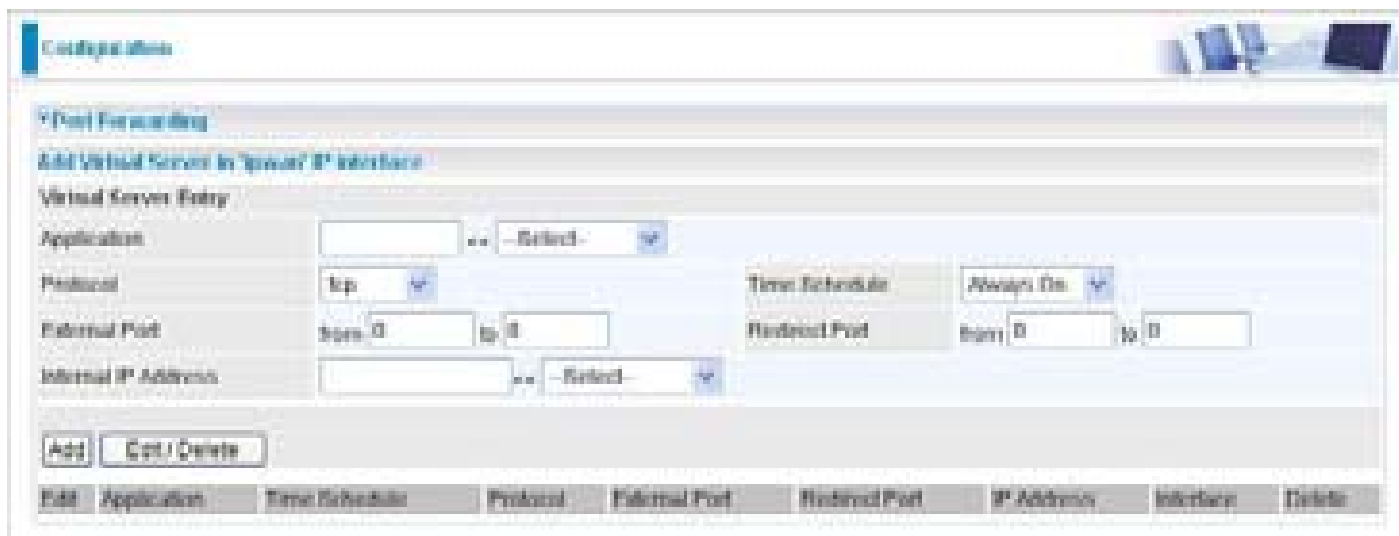
- Application:** A dropdown menu with a '- Select -' option.
- Protocol:** A dropdown menu with 'tcp' selected.
- Time Schedule:** A dropdown menu with 'Always On' selected.
- External Port:** Two input fields for 'from' and 'to' ports, both currently empty.
- Redirect Port:** Two input fields for 'from' and 'to' ports, both currently empty.
- Internal IP Address:** A dropdown menu with a '- Select -' option.

Below the form are two buttons: 'Add' and 'Edit/Delete'. At the bottom of the page is a table with the following columns: 'App', 'Application', 'Time Schedule', 'Protocol', 'External Port', 'Redirect Port', 'IP Address', 'Interface', and 'Delete'.

Porting Forwarding

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

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



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

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

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

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

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

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

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

Example:

If you like to remote accessing your Router through the Web/HTTP at all time, you would need to

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

Application: *HTTP_Server*

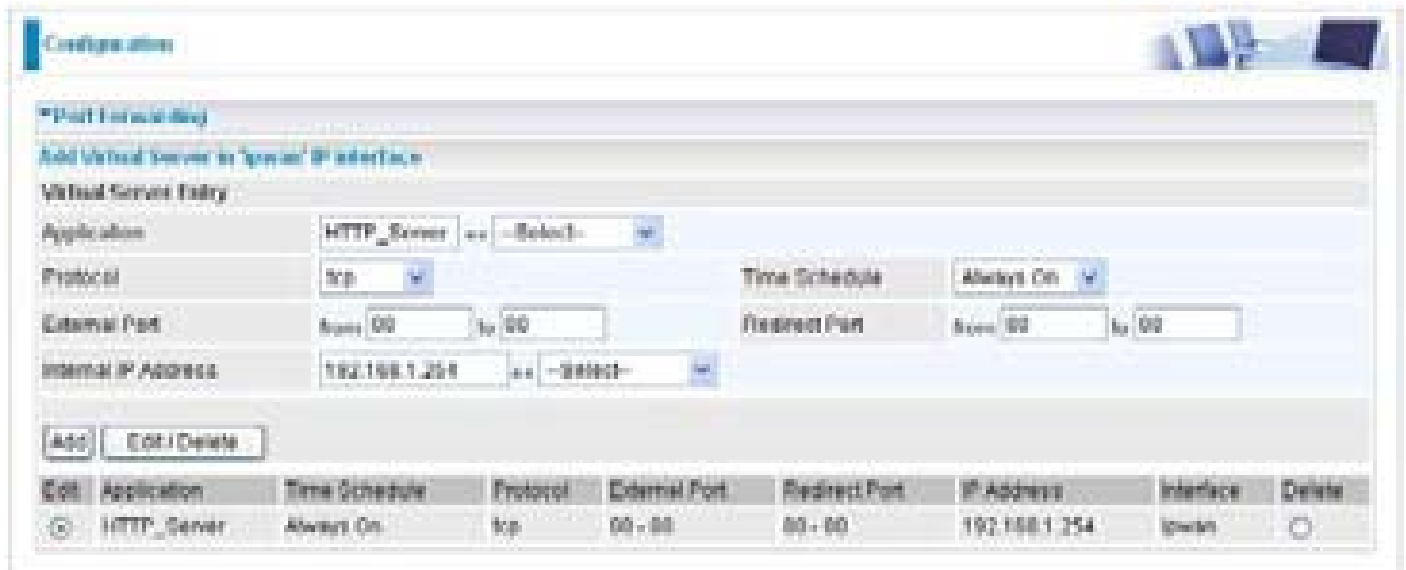
Time Schedule: *Always On*

Protocol: *tcp*

External Port: *80-80*

Redirect Port: *80-80*

IP Address: *192.168.1.254*



Configuration

Port Forwarding

Add Virtual Server to 'wan' IP Interface

Virtual Server Entry

Application: HTTP_Server

Protocol: tcp

Time Schedule: Always On

External Port: 80 - 80

Redirect Port: 80 - 80

Internal IP Address: 192.168.1.254

Buttons: Add, Edit/Delete

Icon	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
⊙	HTTP_Server	Always On	tcp	80 - 80	80 - 80	192.168.1.254	wan	⊙

Add: Click it to apply your settings.

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



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



Attention

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

Edit DMZ Host

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

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

Go to Configuration > Virtual Server > Edit DMZ Host



Enabled: It activates your DMZ function.

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

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

-Select- List all existing PCs connecting to the network. You may assign a PC with 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 for One-to-One NAT to utilize these IP addresses.

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



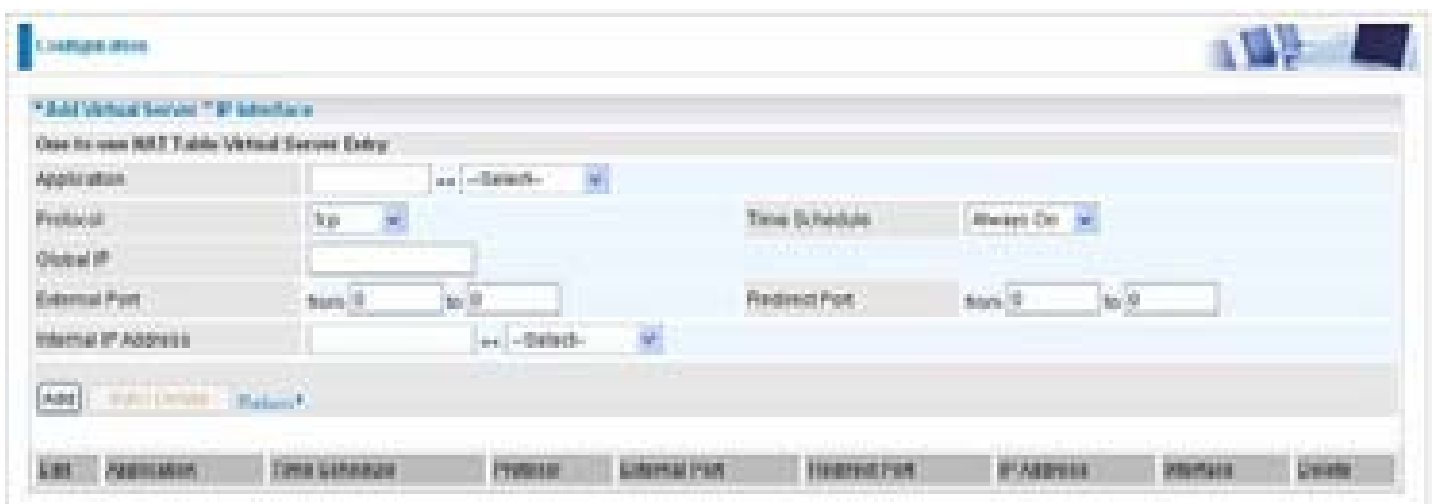
NAT Type: Select desired NAT type. As set in default setting, it disables the One-to-One NAT function.


Global IP Address:


- Subnet:** The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.
- IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 192.168.1.1, end IP: 192.168.1.10

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

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



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

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

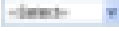
Protocol: It is the supported protocol for the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP;

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

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

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

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

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

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

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

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

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

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

Table 5: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Wake on LAN

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



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

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

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

Ready:

“Yes” indicating the remote computer is ready for your waking up.

“No” indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.

Time Schedule

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

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

Configuration

New Schedule

Name:

Day: Sun Mon Tue Wed Thu Fri Sat

Start Time: 00:00

End Time: 18:00

Time Slot

ID	Name	Day of a week	Start Time	End Time	On/Off
<input type="checkbox"/>	TimeSlot0	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot1	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot2	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot3	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot4	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot5	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot6	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot7	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot8	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot9	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot10	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot11	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot12	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot13	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot14	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot15	uBTWTFs	00:00	18:00	<input type="checkbox"/>
<input type="checkbox"/>	TimeSlot16	uBTWTFs	00:00	18:00	<input type="checkbox"/>

Configuration of Time Schedule

Edit a Time Slot

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

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
<input checked="" type="radio"/>	1	TimeSlot1	Mon Tue Wed Thu	08:00	18:00	<input type="radio"/>
<input type="radio"/>	2	TimeSlot2	Mon Tue Wed Thu	08:00	18:00	<input type="radio"/>
<input type="radio"/>	3	TimeSlot3	Mon Tue Wed Thu	08:00	18:00	<input type="radio"/>

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

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

Edit	ID	Name	Day in a week	Start Time	End Time	Delete
<input checked="" type="radio"/>	1	TimeSlot1	Mon Tue Wed Thu	08:00	18:00	<input type="radio"/>
<input type="radio"/>	2	TimeSlot2	Mon Tue Wed Thu	08:00	18:00	<input type="radio"/>
<input type="radio"/>	3	TimeSlot3	Mon Tue Wed Thu	08:00	18:00	<input type="radio"/>

ID: This is the index of the time slot.

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

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

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

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

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

Delete a Time Slot

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

Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the Advanced section: [Static Route](#), [Static ARP](#), [Dynamic DNS](#), [Device Management](#), [IGMP](#) and [VLAN Bridge](#).

Static Route

Go to Configuration > Advanced > Static Route.



The screenshot shows the 'Static Routing' configuration page. It includes a 'Static Routing' section with input fields for 'Destination', 'Netmask', 'Gateway', 'Interface', and 'Cost'. Below these fields are 'Add' and 'Edit/Delete' buttons. A table below the form lists the configured static routes.

ID	State	Destination	Netmask	Gateway/Interface	Cost
1	+	0.0.0.0	0.0.0.0	0.0.0.0/gig0/0	1

Destination: This is the destination subnet IP address.

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

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

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

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

Static ARP

Go to Configuration > Advanced > Static ARP.



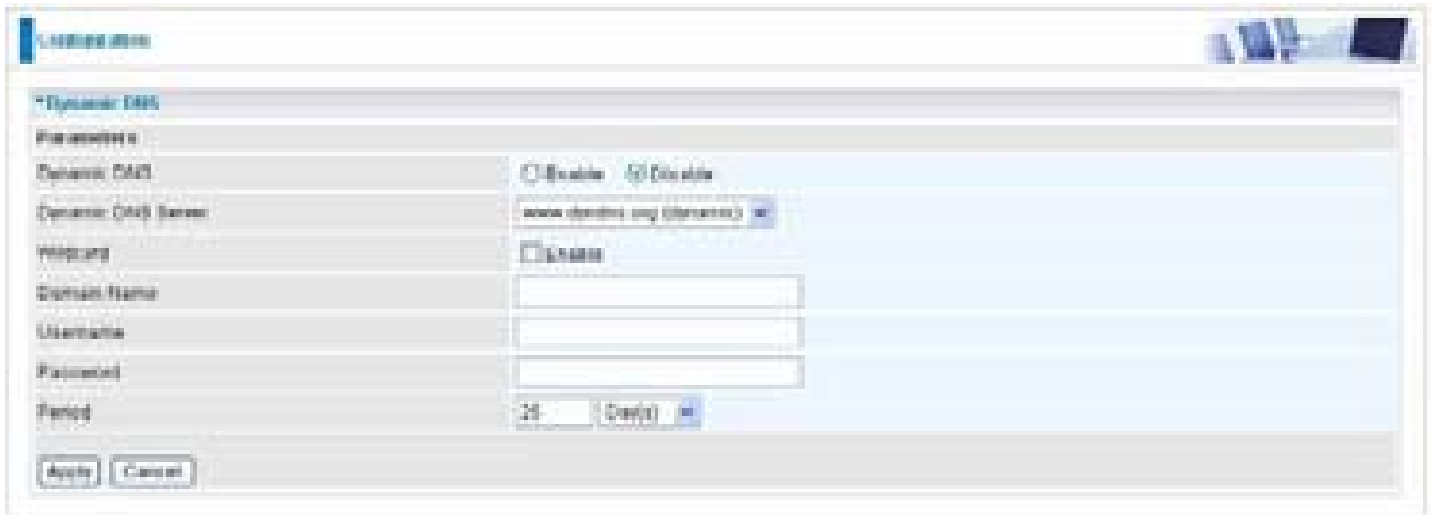
The screenshot shows a web-based configuration interface for Static ARP. At the top, there is a navigation bar with the text "Configuration" and a small image of a server rack. Below this, the main content area is titled "Static ARP". Underneath, there is a section labeled "Parameters". This section contains two input fields: "IP Address" and "MAC Address". Below these fields are two buttons: "Add" and "Remove". At the bottom of the form, there is a table with four columns: "ID", "IP Address", "MAC Address", and "Delete".

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

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

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



The screenshot shows a configuration window titled "Dynamic DNS" with a "Parameters" section. The "Dynamic DNS" checkbox is checked, and the "Dynamic DNS Server" is set to "www.dyndns.org (dyndns)". The "Period" is set to "24" hours. There are input fields for "Domain Name", "Username", and "Password". The "Apply" and "Cancel" buttons are at the bottom left.

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

There are more than 5 DDNS services supported.

Dynamic DNS:

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

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

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

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

Device Management

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

*Device Management			
Device Host Name			
Host Name	home.gateway		
Embedded Web Server			
* HTTP Port	80	(80 is default HTTP port)	
Management IP Address	0.0.0.0	(0.0.0.0 means Any)	
Management IP Netmask	255.255.255.255		
Management IP Address(2)	0.0.0.0		
Management IP Netmask(2)	255.255.255.255		
Expires to auto-logout	180	seconds	
Universal Plug and Play (UPnP)			
UPnP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
* UPnP Port	3900		
SNMP Access Control			
SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> 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	<input checked="" type="radio"/> Read <input type="radio"/> ReadWrite	IP Address	

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

Apply

Device Host Name

Host Name: Assign it a name.

(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.

Example:

Host Name: homegateway ==> Incorrect

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

Embedded Web Server (2 Management IP Accounts)

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

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


Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.


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

Universal Plug and Play (UPnP)

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

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

 **Disable:** Check to disable the router's UPnP functionality.

 **Enable:** Check to enable the router's UPnP functionality.

UPnP Port: Its default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports already being used you may wish to change the port.

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

SNMP V1 and V2:

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

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

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

SNMP V3:

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

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is the combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm

for “security”, but is widely accepted as the SNMPv2 standard.

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

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II)System group

- System group
- Interface group
- Address Translation group
- IP group

From RFC 1472 (PPP/Security MIB)

- PPP security group

From RFC 1473 (PPP/IP MIB)

- PPP IP group

ICMP Group

- TCP group
- UDP group
- EGP (not applicable)
- Transmission
- SNMP group

From RFC 1474 (PPP/Bridge MIB)

- PPP Bridge group

From RFC 1573 (IfMIB)

- ifMIBObjects group

From RFC 1650 (EtherLike-MIB)

- dot3stats

From RFC 1695 (atmMIB)

- atmMIBObjects

From RFC 1493 (Bridge MIB)

- dot1 dBase group
- dot1 dTp group
- dot1 dStp group (if configured as spanning tree)

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 management hosts from multicast group.

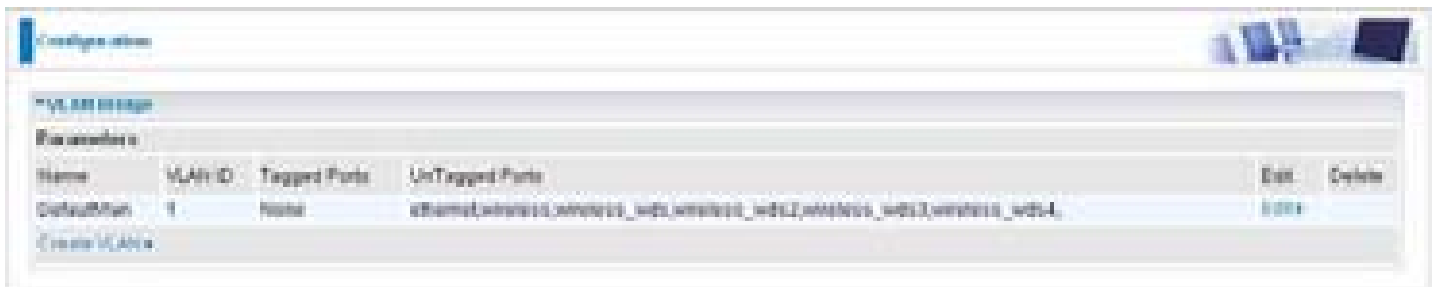


IGMP Forwarding: Accepting multicast packet. Default is set to Enable.

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

VLAN Bridge

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



Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

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

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

Chapter 5: Troubleshooting

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

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on.	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds

Problems with WAN interface

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

Problem with LAN interface

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

Appendix: Product Support & Contact

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

Contact Billion

Worldwide:

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/ 98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.

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

*Federal Communications Commission (FCC) Statement

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

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

FCC Caution:

1. This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference, and
 - (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

IMPORTANT NOTE :**FCC Radiation Exposure Statement:**

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

IC Radiation Exposure Statement:

This device complies with the exemption from the routine evaluation limits in Section 2.5 of RSS 102.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.