BiPAC 7404V Series

VoIP/(802.11g) ADSL2+

(VPN) Firewall Router

User's Manual

Table of Contents

Chapter 1: Introduction

Introduction to your Router

Welcome to the VoIP/(802.11g) ADSL2+ (VPN) Firewall Router. The router is an "all-in-one" VoIP ADSL router, combining an ADSL modem, ADSL router, Ethernet network switch and 2 ports for Voice over IP 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

● **Voice over IP Compliance with SIP Standard**
The router supports cost-effective, toll-quality voice calls over the Internet. It complies with the most popular industrial standard, SIP protocol, to ensure the interoperability with SIP devices and major VoIP Gateways. The VoIP ADSL router supports call waiting, silence suppression, voice activity detection (VAD), comfort noise generation (CNG), line echo cancellation, caller ID (Bell 202, V3) and so on.

● **Fixed-Line Support (Router with LINE port only)**
The router integrates RJ-11 FXO port for inbound and outbound calls transmitted through PSTN. Users can receive phone calls from PSTN while enjoying VoIP call service at the same time. In addition, the device automatically fallbacks to lifeline POTS to enable making normal phone calls when there is power outage, or when the Internet connection is down.

● **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)).

● **Virtual Private Network (VPN) (BiPAC 7404VGO 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.

● **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 Wireless Protected Access (WPA1 and WPA2) and Wireless Encryption Protocol (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.

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

directly for auto detection.

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

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

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

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

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

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

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

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

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

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

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

● **Static and RIP1/2 Routing**
It has routing capability and supports easy static routing table or RIP1/2 routing protocol.

● **Simple Network Management Protocol (SNMP)**
It is an easy way to remotely manage the router via SNMP.

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

● **Firmware Upgradeable**
Device can be upgraded to the latest firmware through the WEB based GUI.

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

Chapter 2: Installing the Router

Important note for using this router

<table>
<tr>
<td>Warning</td>
<td>
✓   **Do not use this router in high humidity or high temperatures.**

✓   **Do not use the same power source for this router as other equipment.**

✓   **Do not open or repair the case yourself.   If this router is too hot, turn off the power immediately and have it repaired at a qualified service center.**

✓   **Avoid using this product and all accessories outdoors.**
</td>
</tr>
</table>

<table>
<tr>
<td>Attention</td>
<td>
✓   **Place this router on a stable surface.**

✓   **Only use the power adapter that comes with the package.   Using a different voltage rating power adaptor may damage this router.**
</td>
</tr>
</table>

Package Contents

- VoIP/(802.11g) ADSL2+ (VPN) Firewall Router
- CD-ROM containing the online manual
- RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5 LAN) Cable
- Console tool kit
- AC-DC power adapter (12VDC, 1.2A)
- A detachable antenna
- Quick Start Guide

The Front LEDs
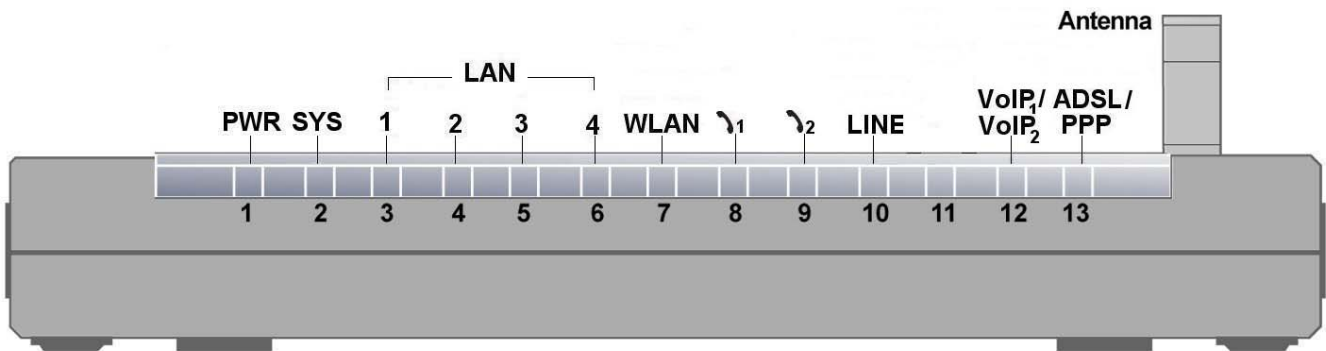
LED		Meaning
1	**PWR**	Lit when power is ON.
2	**SYS**	Lit when the system is ready.
3 – 6	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps. Blinking when data is Transmitted / Received.
7	**WLAN** **(Wireless Router only)**	Lit green when the wireless connection is established. Flashes when sending/receiving data.
8 – 9	**Phone** **1X — 2X** (RJ-11 connector)	Lit green when the phone is off-hook.
10	**LINE** **(Router with LINE port only)**	Lit when the inbound and outbound calls transmitted through PSTN.
12	**VoIP Port** **1X — 2X** (RJ-11 connector)	Lit when the SIP Registration is OK. Green for Phone 1; Orange for Phone 2. Note: Orange also referring to when both Phone 1 and 2 are registered OK at the same time.
13	**ADSL/PPP**	Lit Green when successfully connected to an ADSL DSLAM, ("line synch"). Lit Orange when there is a PPPoA / PPPoE connection.

Chapter 2: Installing the router

The Rear Ports
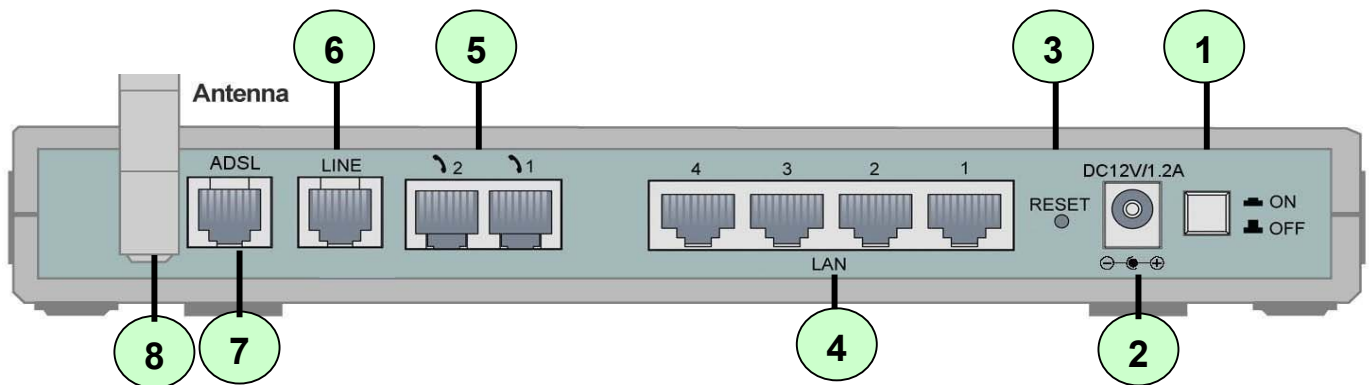
> **NOTE:** The Ethernet Port # 4 can be used as a console port. You need a special console tool which already includes in the package to connect with LAN port 4 and PC's RS-232 port (9-pin serial port).

	Port	leaning
1	**Power Switch**	Power ON/OFF switch
2	**PWR**	Connect the supplied power adapter to this jack.
3	**RESET**	To be sure the device is being turned on → press RESET button for: **1-3 seconds**: quick reset the device. **6 seconds above, and power off, power on the device**: restore to factory default settings. (Cannot login to the router or forgot your Username/Password. Press the button for more than 6 seconds). **Caution**: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.
4	**LAN** **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.
4	**Console Port (as LAN port 4)** (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.
5	**Phone** **1X — 2X** (RJ-11 connector)	Connect RJ-11 cable to this port when connecting to an analog phone set.
6	**LINE** **(Router with LINE port only)**	Connect RJ-11 cable to this port when connecting to the telephone wall jack.

7	**ADSL**	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the ADSL/telephone network.
8	**Antenna** **(Wireless Router only)**	Connect the detachable antenna to this port.

Cabling

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

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Chapter 3: Basic Installation

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

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

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

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

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

Connecting Your Router

1. Connect this router to a **LAN** (Local Area Network) and the ADSL/telephone (**ADSL**) network.
2. Power on the device.
3. Make sure the **PWR** and **SYS** LEDs are lit steadily and that the **LAN** LED is lit.
4. Connect an RJ11 cable to VoIP port when connecting to an analog phone set.
5. Connect RJ-11 cable to LINE Port when connecting to the telephone wall jack.
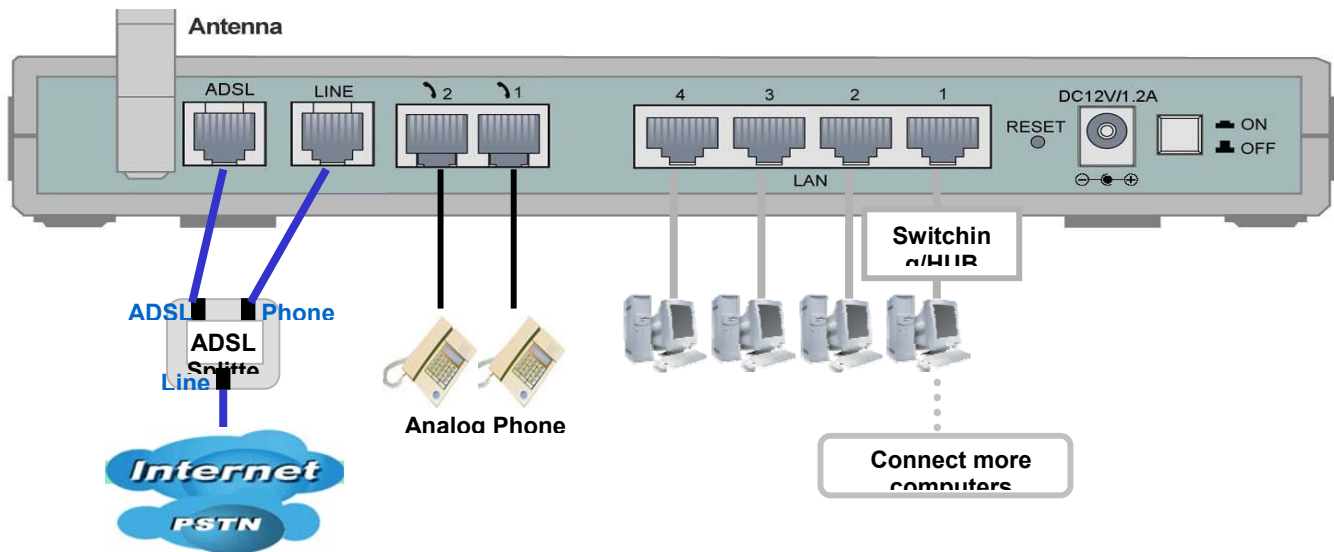
Configuring PCs in Windows in Window XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click **Network Connections**.

2. Double-click **Local Area Connection**. **(See Figure 3.1)**

Figure 3.1: LAN Area Connection

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

Figure 3.2: LAN Connection Status

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

Figure 3.3: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (**See Figure 3.4**)

6. Click **OK** to finish the configuration.

Figure 3.4: IP Address & DNS Configuration

Chapter 3: Basic Installation

Configuring PCs in Windows 2000

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

Figure 3.5: LAN Area Connection

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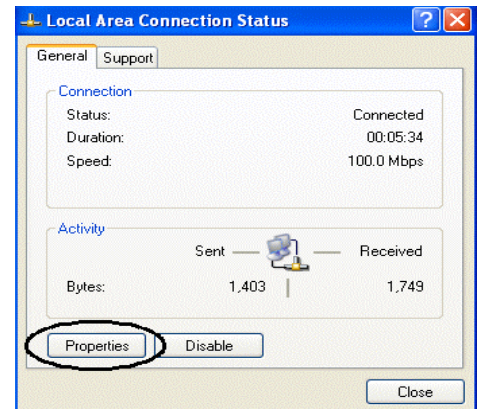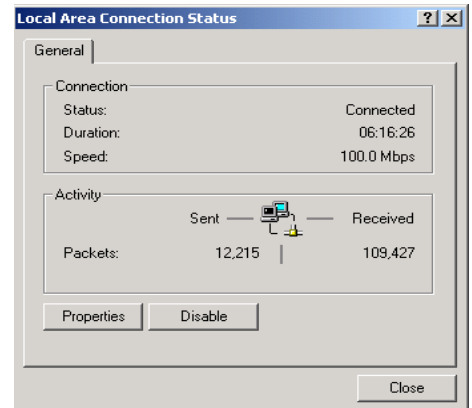
Figure 3.6: LAN Connection Status

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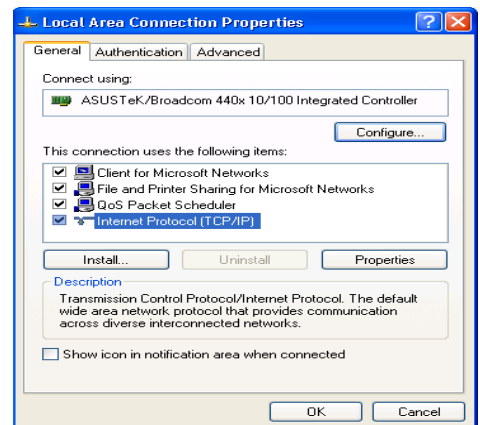
Figure 3.7: TCP / IP

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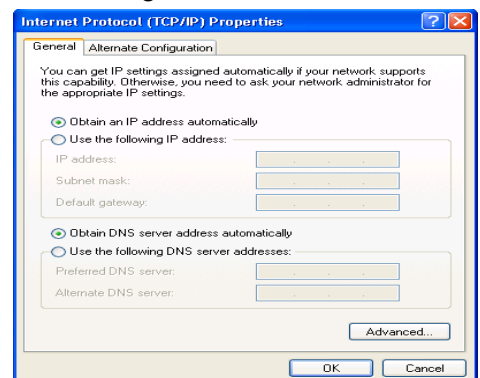6. Click **OK** to finish the configuration.
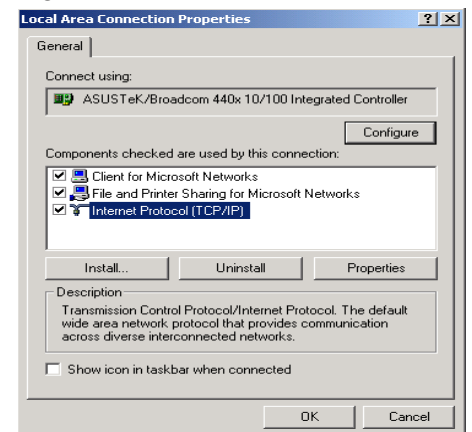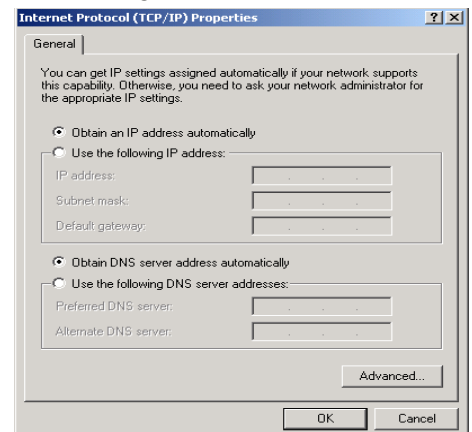
Figure 3.8: IP Address & DNS Configuration

Configuring PC in Windows 95/98/ME

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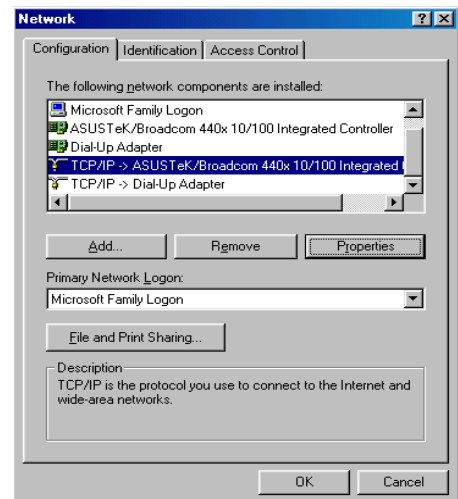
Figure 3.9: TCP / IP

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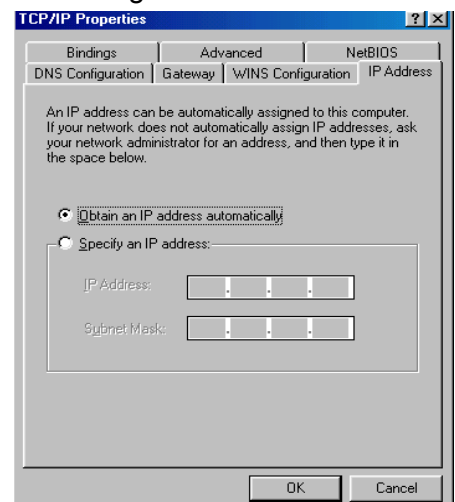
Figure 3.10: IP Address

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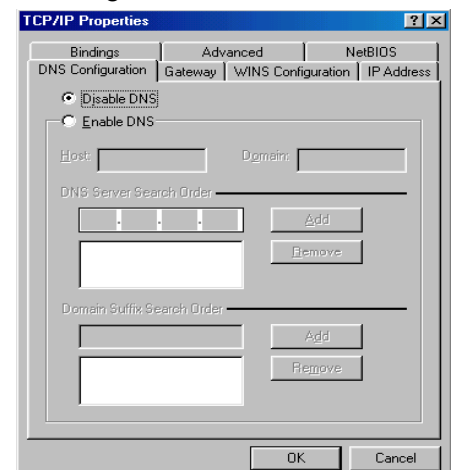
Figure 3.11: DNS Configuration

Configuring PC in Windows NT4.0

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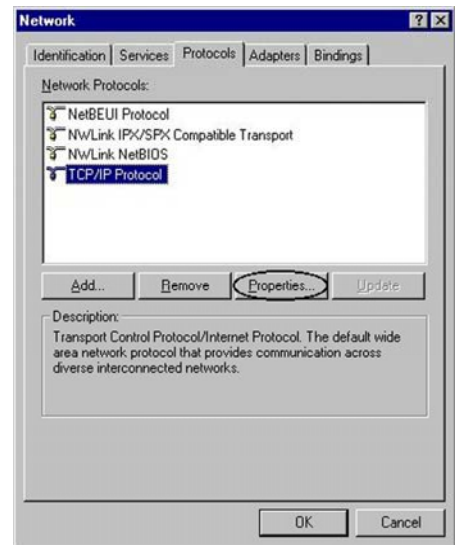
Figure 3.12: TCP / IP

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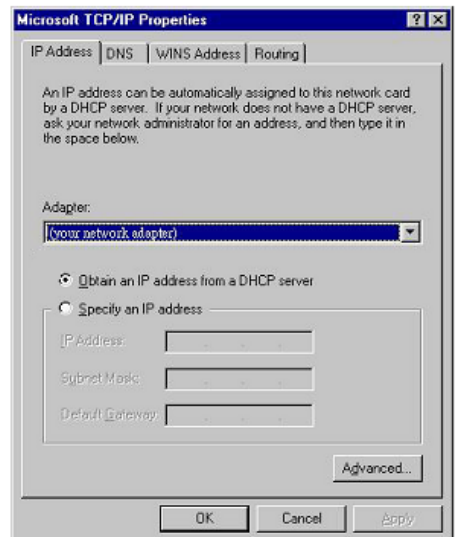
Figure 3.13: IP Address

Factory Default Settings

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

Web Interface (Username and Password)

▶ Username: admin

▶ Password: admin

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

⚠️ **If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds to restore the factory default settings.**
Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.

Attention

Device LAN IP settings

▶ IP Address: 192.168.1.254

▶ Subnet Mask: 255.255.255.0

ISP setting in WAN site

▶ PPPoE

DHCP server

▶ DHCP server is enabled.

▶ Start IP Address: 192.168.1.100

▶ IP pool counts: 100

LAN and WAN Port Addresses

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

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

Information from your ISP

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

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

PPPoE	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually).
PPPoE / PPPoE with Pass-through	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually). In addition, additional WAN address can be assigned using PPPoE dialer.
PPPoA	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it ca be automatically assigned by your ISP when you connect or be set manually).
RFC 1483 Bridged	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.
RFC 1483 Routed	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA Routed (IP over ATM)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **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)**
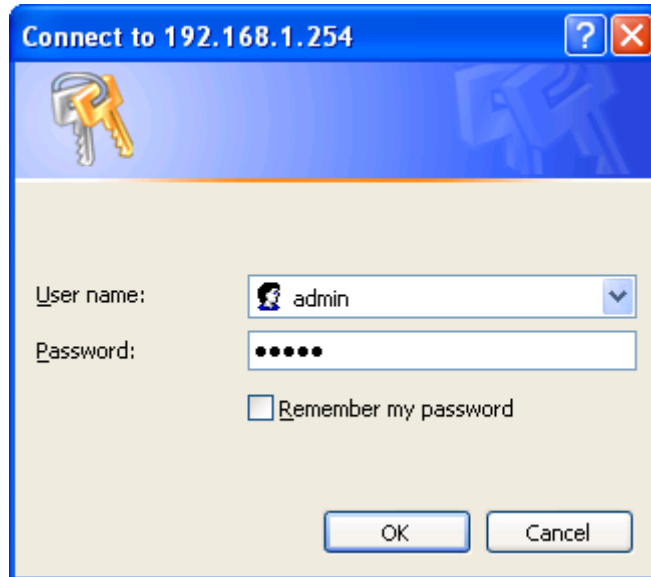
Figure 3.14: User name & Password Prompt Widonw

Congratulation! You are now successfully logon to the VoIP/(802.11g) ADSL Router!

Chapter 4: Configuration

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

⬤ **Status**
  - ARP Table
  - Wireless Association
  - Routing Table
  - DHCP Table
  - PPTP Status
  - IPSec Status
  - L2TP Status
  - Email Status
  - VoIP Status
  - Event Log
  - Error Log
  - NAT Sessions
  - Diagnostic
  - UPnP Portmap

⬤ **Quick Start**

⬤ **Configuration**
  - LAN
  - WAN
  - System
  - Firewall
  - VPN
  - VoIP
  - QoS
  - Virtual Server
  - Time Schedule
  - Advanced

⬤ **Save Config to FLASH**

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

⬤ **Logout**

Please click the links to see the relevant sections of this manual for detailed instructions on how to configure the VoIP Router.

Status

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

IP <> MAC List

IP Address	MAC Address	Interface	Static
192.168.1.187	00:0c:6e:bd:11:6d	iplan	no

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.

Wireless Association Table (Wireless Router only)

Wireless Association Table

Wireless client's MAC address and the corresponding IP address

IP Address	MAC
192.168.1.100	00:04:23:73:9a:86

IP Address: It is IP address of wireless client that joins this network.

MAC: The MAC address of wireless client.

Routing Table

Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost
✓	0.0.0.0	0.0.0.0	192.168.21.1	1

RIP Routing Table

Destination	Netmask	Gateway	Cost

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination Netmask address.

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

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

RIP Routing Table

Destination: The IP address of the destination network.

Netmask: The destination Netmask address.

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

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

DHCP Table

DHCP Table

Type		
Leased ◉	Expired ◉	Permanent ◉

Leased: The DHCP assigned IP addresses information.

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

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

Leased Table

Leased Table

IP Address	MAC Address	Client Host Name	Expiry

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.

Expired Table

Expired Table

IP Address	MAC Address	Client Host Name	Expiry

Please refer the **Leased Table**.

Permanent Table

Permanent Table

Name	IP Address	MAC Address	Maximum Lease Time

Name: The name you assigned to the Permanent configuration.

IP Address: The fixed IP address for the specify client.

MAC Address: The MAC Address that you want to assign the fixed IP address.

Maximum Lease Time: The maximum lease time interval you allow to clients.

PPTP Status (Only the 7404VGO has VPN features)

This shows details of your configured PPTP VPN Connections.

PPTP Status

VPN/PPTP for Remote Access Application						
Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/PPTP for LAN-to-LAN Application						
Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

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

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

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

Tunnel Connected: Whether the VPN Tunnel is currently connected.

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

Encryption: The encryption type used for this VPN connection.

IPSec Status (Only the 7404VGO has VPN features)

This shows details of your configured IPSec VPN Connections.

IPSec Status

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

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

Active: Whether the VPN Connection is currently Active.

Connection State: Whether the VPN is Connected or Disconnected.

Statistics: Statistics for this VPN Connection.

Local Subnet: The local IP Address or Subnet used.

Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

L2TP Status (Only the 7404VGO has VPN features)

This shows details of your configured L2TP VPN Connections.

L2TP Status

VPN/L2TP for Remote Access Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

VPN/L2TP for LAN-to-LAN Application

Name	Type	Enable	Active	Tunnel Connected	Call Connected	Encryption

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

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

Enable: Whether the connection is currently enabled.

Active: Whether the connection is currently active.

Tunnel Connected: Whether the VPN Tunnel is currently connected.

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

Encryption: The encryption type used for this VPN connection.

Email Status

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

Email Status

Email Account

Account Name	username
POP3 Mail Server	pop3.mail.com
Email Status	No mail

[Reset Status] [Check Now]

VoIP Status

Here you can check details and status of VoIP Account you have configured. Please see the **VoIP Configuration** section for more details.

VoIP Status

Phone Port

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

[Refresh]

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.

```
Event Log

----------- system log buffer head --------------
Jan 01 00:00:11 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 01 22:00:20 home.gateway:im:none: Reset SNMP community to factory default
settings

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




  [Refresh]  [Clear]
```

Error Log

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

Error Log

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

NAT Sessions

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

```
NAT Sessions

Active NAT sessions between interface of types external and internal:

Prot | Local IP: Port local/public | Remote IP: Port      | Idle (sec.)
-----|-----------------------------|----------------------|-------
TCP  | 192.168.  1.201: 1110/ 1110 |  64. 94.110. 12:   80 | 29
TCP  | 192.168.  1. 99: 1982/ 1982 | 210.184.108.126:   80 | 729
TCP  | 192.168.  1. 99: 1979/ 1979 | 207. 68.178.239:   80 | 542
TCP  | 192.168.  1.202: 2011/ 2011 | 207. 46.107. 27: 1863 | 21
TCP  | 192.168.  1.100: 1166/ 1166 | 207. 46.106. 90: 1863 | 18
TCP  | 192.168.  1. 99: 1969/ 1969 | 207. 46.107. 22: 1863 | 673
ICMP | 192.168.  1.201:  512/  512 | 168. 95.  4.211:  512 | 0

    TCP :     6 sessions
    UDP :     0 sessions
Others :     1 sessions
 Total :     7 sessions
```

Refresh

Diagnostic

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

Diagnostic

LAN Connection	
Testing Ethernet LAN connection	PASS

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

Refresh

UPnP Portmap

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

UPnP Portmap

UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address
emwebigd1024	udp	35324 ~ 35324	15852 ~ 15852	192.168.1.205
emwebigd1025	tcp	48888 ~ 48888	14811 ~ 14811	192.168.1.205
emwebigd1063	udp	9210 ~ 9210	15169 ~ 15169	192.168.1.202
emwebigd1064	tcp	50937 ~ 50937	14500 ~ 14500	192.168.1.202

Quick Start

Quick Start

Connection

Encapsulation	PPPoE ⌄ Auto Scan
VPI	0
VCI	33
NAT	⊙ Enable ○ Disable

Optional Settings

IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
SubNetmask	0.0.0.0
Default Gateway	0.0.0.0

DNS

Obtain DNS automatically	☐ Enable
Primary DNS	
Secondary DNS	

PPP

|	
Username	
Password	

Apply   Cancel

For detailed instructions on configuring your WAN settings, please see the **WAN** section of this manual.

Usually, the only details you will need for the Quick Start wizard to get you online are your login (often in the form of *username@ispname*), your password and the encapsulation type.   In additional, you have the option to provide specific DNS as your desire, or check the **Enable** box to get the DNS automatically from your ISP.

Your ISP will be able to supply all the details you need, alternatively, if you have deleted the current WAN Connection in the **WAN – ISP** section of the interface, you can use the router's PVC Scan feature to attempt to determine the Encapsulation types offered by your ISP.

Auto Scan

Before you scan the PVCs, please DELETE all the WAN interfaces.

IP Address		if provided by ISP
Gateway		if provided by ISP

Start

Click **Start** to begin scanning for encapsulation types offered by your ISP. If the scan is successful you will then be presented with a list of supported options:
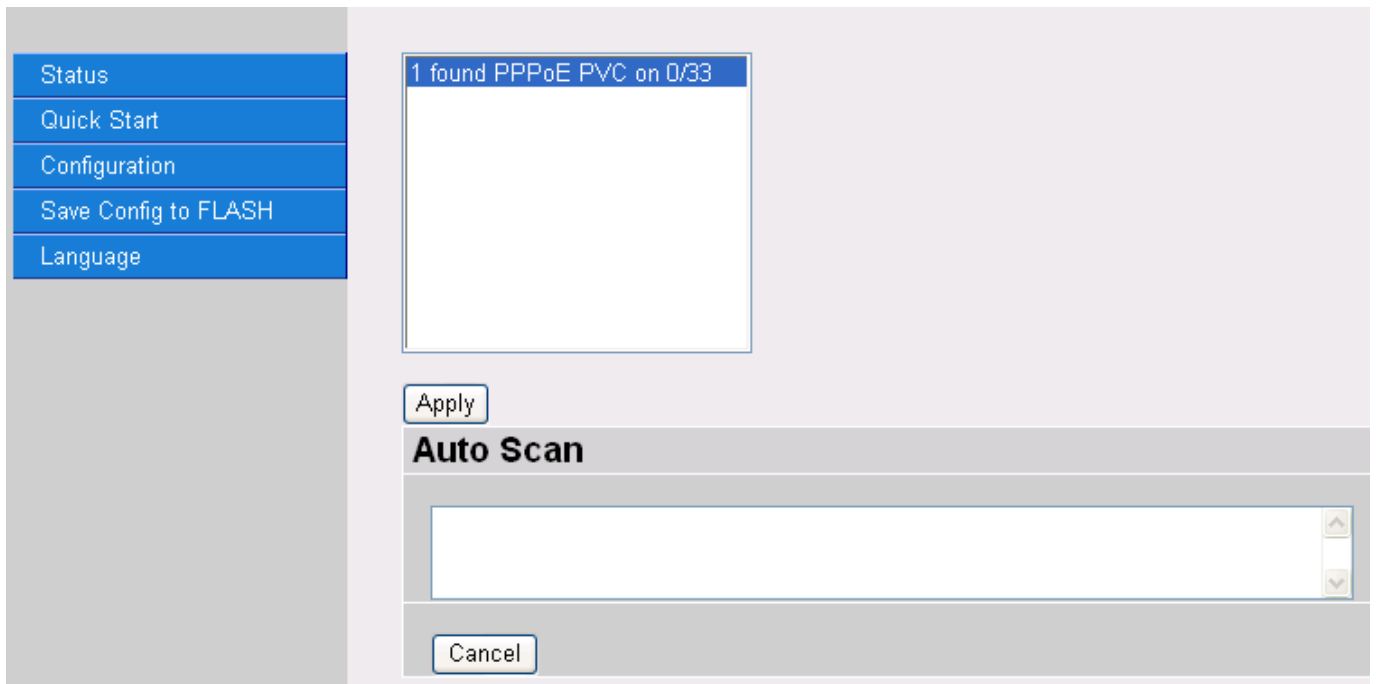
Select the desired option from the list and click **Apply** to return to the Quick Start interface to continue configuring your ISP connection. Please note that the contents of this list will vary, depending on what is supported by your ISP.

Chapter 4: Configuration

Configuration

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

- **LAN, Wan, System, Firewall, VPN, VoIP, QoS, Virtual Server, Time Schedule** and **Advanced**

These functions are described below in the following sections.

LAN - Local Area Network

Here are the items within the LAN section: **Bridge Interface, Ethernet, IP Alias, Ethernet Client Filter, Wireless, Wireless Security, Wireless Client Filter, Port Settings** 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

Ethernet

Primary IP Address				
IP Address	192	168	1	254
SubNetmask	255	255	255	0
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast			

[Apply]

Primary IP Address

IP Address: The default IP on this router.

SubNetmask: 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 supports to create 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 Alias

Parameters	
IP Address	. . .
SubNetmask	. . .
Security Interface	⦿ Internal ◯ External ◯ DMZ

[Apply] [Cancel]

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.

Chapter 4: Configuration

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

Filtering Rules

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

Apply

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

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

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

The maximum client is 16.   The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters.   The number **0** - **9** and letters **a** - **f** are acceptable.
Note: Follow the MAC Address Format xx:xx:xx:xx:xx:xx.   Semicolon (:) must be included.

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

Candidates ▶ → **Active PC in LAN**

http://192.168.1.254 - Active PC in LAN - Micro...

Active PC in LAN

IP Address	MAC Address
☐ 192.168.1.218	00:11:2f:0b:56:07

Add

Chapter 4: Configuration

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 (Wireless Router only)

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 propose, change the default **wlan-ap** to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.
Note: It is case sensitive and must not excess 32 characters.

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

    ◉   **Disable: I**f 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) in

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

Channel ID: Select the wireless connection ID channel that you would like to use.   Use the *Scan Channel Usage* to help to select non-occupied wireless channel.

    ◉   **Scan Channel Usage:** Wireless channel scan takes up to 14 seconds to survey the channel ID in the network area.   The result will show all ID channel is being occupied or not occupied.
        Note: Wireless performance may degrade if select ID channel is already being occupied by other AP(s).

Chapter 4: Configuration

TX PowerLevel: It is function that enhances the wireless transmitting signal strength. User may adjust this power level from minimum 0 up to maximum 255.

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.

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 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.

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.

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.

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

Wireless Security (Wireless Router only)

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

Wireless Security

Parameters	
Security Mode	Disable ▼

[Apply] [Cancel]

WPA-PSK (TKIP) / WPA-PSK (AES) Pre-Shared Key

Wireless Security

Parameters			
Security Mode	WPA1 Pre-Shared Key ▼	or	WPA2 Pre-Shared Key ▼
WPA Algorithms	TKIP	or	AES
WPA Shared Key			
Group Key Renewal	3600		seconds
Idle Timeout	3600		seconds (120~65535)

[Apply] [Cancel]

WPA Algorithms: There are two types of the WPA-PSK, WPA1 and WPA2.   The WPA1 adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2 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 **3600** seconds.

Idle Timeout: The default idle timeout is **3600** seconds.   A Timeout value base on the case of no data traffic is send or received. If Router detects no traffic in the wireless, it will start timing the clock and drop the session as it reaches to the defined timeout value. New session will be re-established after the old session.

Chapter 4: Configuration

WEP

Wireless Security

Parameters	
Security Mode	WEP
WEP Authentication	Open System
WEP Encryption	⦿ WEP64 ◯ WEP128 Hex
Passphrase	[ ] Generate
Default Used WEP Key	1 (1~4)
Key 1	00-00-00-00-00
Key 2	00-00-00-00-00
Key 3	00-00-00-00-00
Key 4	00-00-00-00-00

(WEP 64 - Hex): 5 Hex code, (1~9, a~z, A~Z), separated by hyphen, - ,are required. Either use the Passphrase or manually insert your WEP key. EX: 11-aa-22-cc-33.

* : WDS uses Key1 for WEP encryption.

[Apply] [Cancel]

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, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is "-". For example, using WEP64, 11-22-33-44-55 is a valid key, whilst 1122334455 is invalid.

Wireless Client / MAC Address Filter (Wireless Router only)

The MAC Address supports up to 16 wireless network machines and helps you to 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.

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

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

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

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

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

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

Candidates ▶ →**Associated Wireless Clients**
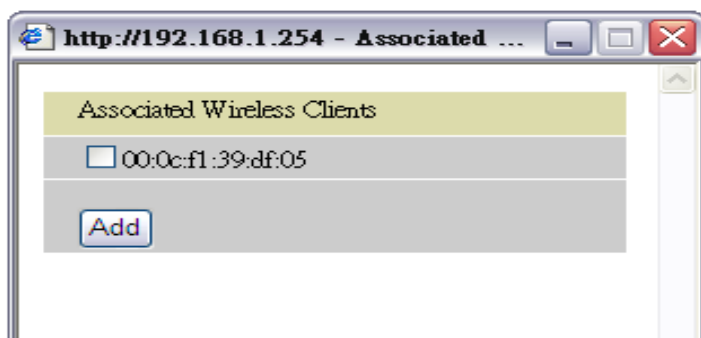
Associate Wireless Client displays a list of individual wireless device's MAC Address that currently connects to the router.

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.

Port Setting

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

Port Setting

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

Set High Priority TOS

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

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

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

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

Apply

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.

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.

DHCP Server

Configuration

DHCP Server Mode	○ Disable
	⦿ DHCP Server
	○ DHCP Relay Agent

[Next]

DHCP Server Status

Allow Bootp	true
Allow Unknown Clients	true
Enable	true

Subnet Definitions

Subnet Value	192.168.1.0
SubNetmask	255.255.255.0
Maximum Lease Time	86400 seconds
Default Lease Time	43200 seconds
Use local host address as DNS server	true
Use local host address as default gateway	true
Get subnet from IP interface	iplan

IP Range *192.168.1.100- 192.168.1.199*

Option *domain-name-servers= 0.0.0.0*

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

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

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

Click **Apply** to enable this function.

WAN - Wide Area Network

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

ISP

Name	Description	Creator	VPI	VCI		
wanlink	PPPoE WAN Link	Factory Defaults	8	35	Edit ▶	Change ▶

WAN Connection

WAN Services Table

Create ▶

The factory default is PPPoE. If your ISP uses this access protocol, click **Edit** to input other parameters as below. If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

Some of ISP may provide more service via different WAN connection. In case, you can create more connections by clicking **Create**. The device can support maximum up to 8 WAN connections.

Note: The application of multiple WAN connections is depend on your Service Provider.

A simpler alternative is to select **Quick Start** from the main menu on the left. Please see the Quick Start section of the manual for more information.

RFC 1483 Routed Connections

WAN Connection

RFC 1483 Routed

Description	RFC 1483 routed mode
VPI	0
VCI	0
ATM Class	UBR
NAT	⊙ Enable ○ Disable
Encapsulation Method	LLC Bridged
IP Assignment	⊙ Obtain an IP address automatically via DHCP client ○ Use the following IP address IP Address _____ Netmask _____ Gateway _____
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast
MTU	1500

[Apply]

Description: User-definable name for the connection.

VPI and 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 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.

Encapsulation method: Selects the encapsulation format, the default is LLC Bridged. Select the one provided by your ISP.

IP Assignment

⊙ **Obtain an IP address automatically via DHCP client:** specify if the Router can get an IP address from the ISP (Internet Service Provider) automatically.

⊙ **Use the following IP Address:** Specify the IP address manually; the IP should be given by you our ISP.

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

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

RFC 1483 Bridged Connections

WAN Connection

RFC 1483 Bridged

Description	RFC 1483 bridged mode
VPI	0
VCI	33
ATM Class	UBR
Encapsulation Method	LLC Bridged
Acceptable Frame Type	acceptall
Filter Type	All
PVID for Utagged Frames	1

Apply

Description: User-definable name for the connection.

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

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

Acceptable Frame Type: Specify what kind of traffic can 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.

PVID for Untagged Frames: PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID. The valid value range for PVID is 1~4094.

PPPoA Routed Connections

WAN Connection

PPPoA Routed

Description	PPPoA Routed
VPI	0
VCI	0
ATM Class	UBR
NAT	⊙ Enable ○ Disable
Username	
Password	
IP Address	('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast
MTU	1500

[Apply]

Description: User-definable 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.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be 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).

IP Address: 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.

Authentication Protocol Type: Default is Chap (Auto). Your ISP will advise you 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.

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

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

Advanced Options (PPPoA)

LLC Header: Selects encapsulation mode, true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can equest a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

IPoA Routed Connections

Description: User-definable 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.

IP Assignment

⊙ **Obtain an IP address automatically via DHCP client:** specify if the Router can get an IP address from the ISP (Internet Service Provider) automatically.

⊙ **Use the following IP Address:** Specify the IP address manually; the IP should be given by you our ISP.

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

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

Chapter 4: Configuration

PPPoE Connections

WAN Connection

PPPoE Routed

Description	PPPoE Routed
VPI	0
VCI	0
ATM Class	UBR
NAT	⊙ Enable ○ Disable
Username	
Password	
Service Name	
IP Address	('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast
MTU	1492

[Apply]

Description: User-definable name for this 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 ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be 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 will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

Authentication Protocol: Default is Chap(Auto). Your ISP will advise you whether to use Chap or Pap.

Connection

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

Chapter 4: Configuration

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

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

⊙ **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.

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

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

Advanced Options (PPPoE)

LLC Header: Selects encapsulation mode, true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

PPPoE with Pass-through Connections

PPPoE with pass-through adapts the following method: PPPoE Routed mode + 1483 Bridge Mode. With pure PPPoE connection, the router can get one WAN address to the router. With the PPPoE and PPPoE pass-through, concurrently, it allows user to have a WAN address assigned to the router but also able to get another WAN IP from ISP using PPPoE dialer (e.g WinPoETor Windows XP PPPoE Dialer) at the same time.

WAN Connection

PPPoE Routed

Description	PPPoE with Pass-through
VPI	0
VCI	33
ATM Class	UBR
NAT	○ Enable ◉ Disable
Username	
Password	
Service Name	
IP Address	
	('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast
MTU	1492

[Apply]

Description: User-definable name for this 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 ISP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be 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 will provide you the information. Maximum input is **20** alphanumeric characters.

IP Address: specify if the Router can get an IP address from the Internet Server Provider (ISP) automatically or not. Please click Obtain an IP address automatically via DHCP client to enable the DHCP client function or click Specify an IP address to disable the DHCP client function, and specify the IP address manually. The setting of this item is specified by your ISP.

Authentication Protocol: Default is Chap(Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

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

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

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

⊙ **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.

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

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

Advanced Options (PPPoE)

LLC Header: Selects encapsulation mode, true for using LLC or false for using VC-Mux.

Create Route: This setting specifies whether a route is added to the system after IPCP (Internet Protocol Control Protocol) negotiation is completed. If set to *enabled*, a route will be created which directs packets to the remote end of the PPP link.

Specific Route: Specifies whether the route created when a PPP link comes up is a specific or default route. If set to *enabled*, the route created will only apply to packets for the subnet at the remote end of the PPP link. The address of this subnet is obtained during IPCP negotiation.

Subnet Mask: sets the subnet mask used for the local IP interface connected to the PPP transport. If the value *0.0.0.0* is supplied, the netmask will be calculated from the class of the IP address obtained during IPCP negotiation.

Route Mask: Sets the subnet mask used by the route that is created when a PPP link comes up. If it is set to *0.0.0.0*, the subnet mask is determined by the IP address of the remote end of the link. The class of the IP address is obtained during IPCP (Internet Protocol Control Protocol) negotiation.

MRU: Maximum Receive Unit. This is negotiated during the LCP protocol stage.

Discover Primary / Secondary DNS: This setting enables/disables whether the primary/secondary DNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is *enabled*.

Give DNS to Relay: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request the DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS relay so that a connection can be established.

Give DNS to Client: Controls whether the PPP Internet Protocol Control Protocol (IPCP) can request a DNS server IP address for a remote PPP peer. Once IPCP has discovered the DNS server IP address, it automatically gives the address to the local DNS client so that a connection can be established.

Give DNS to DHCP Server: Similar to the above, but gives the DNS server address to the DHCP server.

Discover Primary NBNS / Discover Secondary NBNS: This setting enables/disables whether the primary/secondary NBNS server address is requested from a remote PPP peer using IPCP. The default setting for this command is disabled.

Discover Subnet Mask: Specifies if the subnet mask given by IPCP negotiation process is to be used.

Give Subnet Mask To DHCP Server: Enable to change your DHCP Server settings by using the given information in IPCP negotiation process.

DNS

DNS

Parameters

Obtain DNS automatically	☑ Enable
Primary DNS	
Secondary DNS	

[Apply] [Cancel]

A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com and an IP address. An IP address is a 32-bit number in the form of *xxx.xxx.xxx.xxx*, for example 192.168.1.254. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP has provided it when you logon, check the **Enable** box. Usually when you choose PPPoE or PPPoA as your WAN - ISP protocol, the ISP will provide the DNS IP address automatically. You may leave the configuration field blank.

Alternatively, your ISP may provide you with an IP address of their DNS. If this is the case, you must enter the DNS IP address manually.

If you choose one of the other three protocols ─ RFC1483 Routed/Bridged and IPoA check with your ISP, it may provide you with an IP address for their DNS server. You must enter the DNS IP address if you set the DNS of your PC to the LAN IP address of this router.

Chapter 4: Configuration

ADSL

ADSL

Parameters

Connect Mode	ADSL2+, auto-fallback
Modulation	G.Dmt.BisPlusAuto
Profile Type	MAIN
Activate Line	true
Coding Gain	auto
Tx Attenuation	Bis_0DB
DSP Firmware Version	E.38.2.12
Connected	false
Operational Mode	Inactive
Annex Type	ADSL2
Upstream	0
Downstream	0
CO Vendor	
Elaspsed Time	

Apply   Cancel   Advanced Options ▶

Connect Mode: This mode will automatically detect your ADSL line code, ADSL2+, ADSL2, G.dmt, G.lite, T1.413, AnnexM2 and AnnexM2+. But in some area, multimode cannot detect the ADSL line code well. If it is the case, please adjust the ADSL line code to G.dmt or T1.413 first. If it still fails, please try the other values such as ALCTL, ADI, etc.   If you still having trouble with the line, please check with your ISP for line connect information.

Note: If you have subscribed ADSL1 T1.413 mode line, you may go to the Advanced Options for more connection module combinations.

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.

DSP Firmware Version: Current ADSL line code firmware version.

Connected: Display current ADSL line sync status.

Operational Mode: Display current ADSL mode standard (Operational Mode) your Router is using when ADSL line has sync.

Annex Type: ADSL Annex A, which works over a standard telephone line. Annex B, which works over an ISDN line.

Upstream: Display current upstream rate of your ADSL line.

Downstream: Display current downstream rate of your ADSL line.

Chapter 4: Configuration

Advanced Options

ADSL Parameters help to interpret your ADSL line statistics.

ADSL		
Parameters		
	Downstream	Upstream
SNR Margin	0.0 dB	0 dB
Line Attenuation	0.0 dB	0.0 dB
CRC Errors	0	0
Latency		

Refresh Return ▶

SNR Margin: It is known as Signal to Noise Ration Margin. It is the relative of DSL strength to Noise ratio. This margin is measured in decibels (dB). Higher the dB figures better the DSL strength and better chance to get faster speed. THE HIGHER THE BETTER

Line Attenuation: it measures the signal loss in decibel (dB) between the CO DSLAM. Lower the attenuation dB figures better the DSL strength/speed. THE LOWER THE BETTER.

CRC Errors: It is known as Cyclic Redundancy Check Error. Its checksum is to detect the transmission error.

Latency: It includes two channels, Fast and Interleaved. It displays the channel adapted by your ISP.

ADSL Advanced setting	
Parameters	
Capability	BIS+/BIS/A/MULTIMODE ▾
s=1/2 Mode	○ Enable ⊙ Disable

Apply Cancel

Capability: There are more combinational ADSL modulation modes to be selected.

⊙ **GDMT:** ADSL connection will be limited to ADSL1 (G.DMT / G.Lite) only.

⊙ **BIS+:** ADSL connection will be limited to ADSL2+ only. (If you are ADSL1 subscriber DO NOT select this option).

⊙ **BIS+/T1413:** ADSL connection will be limited to ADSL2+ and ADSL1 T1.413 only.

⊙ **BIS+/BIS:** ADSL connection will be limited to ADSL2+ and ADSL2 only.

⊙ **BIS+/BIS/GDMT/T1413:** ADSL connection will be limited to ADSL2+, ADSL2 and ADSL1 G.DMT & G.Lite & T1.413.

⊙ **BIS+/BIS/T1413:** ADSL connection will be limited to ADSL2+, ADSL2 and T1.413.

⊙ **BIS+/BIS/GDMT:** ADSL connection will be limited to ADSL2+, ADSL2 and ADS1 (G.DMT/G.Lite) only.

⊙ **DISABLE:** This disable function will disconnect your ADSL synch. Select it with cautious.

S=1/2 Mode: It is ADSL1 protocols which can increase the downstream speed up to 12Mpb. Please check further with your ISP about this option is being enabled or not.

System

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

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 **Automatic** box to auto set your local time.

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

Chapter 4: Configuration

Remote Access

Remote Access

You may temporarily permit remote administration of this network device

| Allow Access for | 30 | minutes. |

[Enable]

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 <u>**0**</u> minute.

Firmware Upgrade

Firmware Upgrade

You may upgrade the system software on your network device

New Firmware Image		Browse...

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 modified, 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

Backup/Restore

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

Backup Configuration

Backup configuration to your computer.

[Backup]

Restore Configuration

| Configuration File | [   ] [Browse...] |

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

[Restore]

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.

Chapter 4: Configuration

Restart Router

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

Restart Router

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

| Restart Router with | ⦿ Current Settings |
| | ○ Factory Default Settings |

Restart

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 on the back of your router in for more than 6 seconds whilst the router is turned on.

User Management

User Management

Current Defined Users

Valid	User	Comment		
true	*admin*	Default admin user	Edit ◯	

Create ◯

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

User Management

Edit

Username	**admin**
Password	•••••
Confirm	•••••
Valid	true
Comment	Default admin user

[Apply] [Reset]

You can change the user's **password**, whether their account is active and **valid**, as well as add a comment to each user account. These options are the same when creating a user account, with the exception that once created you cannot change the username. You cannot delete the default admin account; 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.

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. In addition to this, when using NAT, the router acts as a "natural" Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.
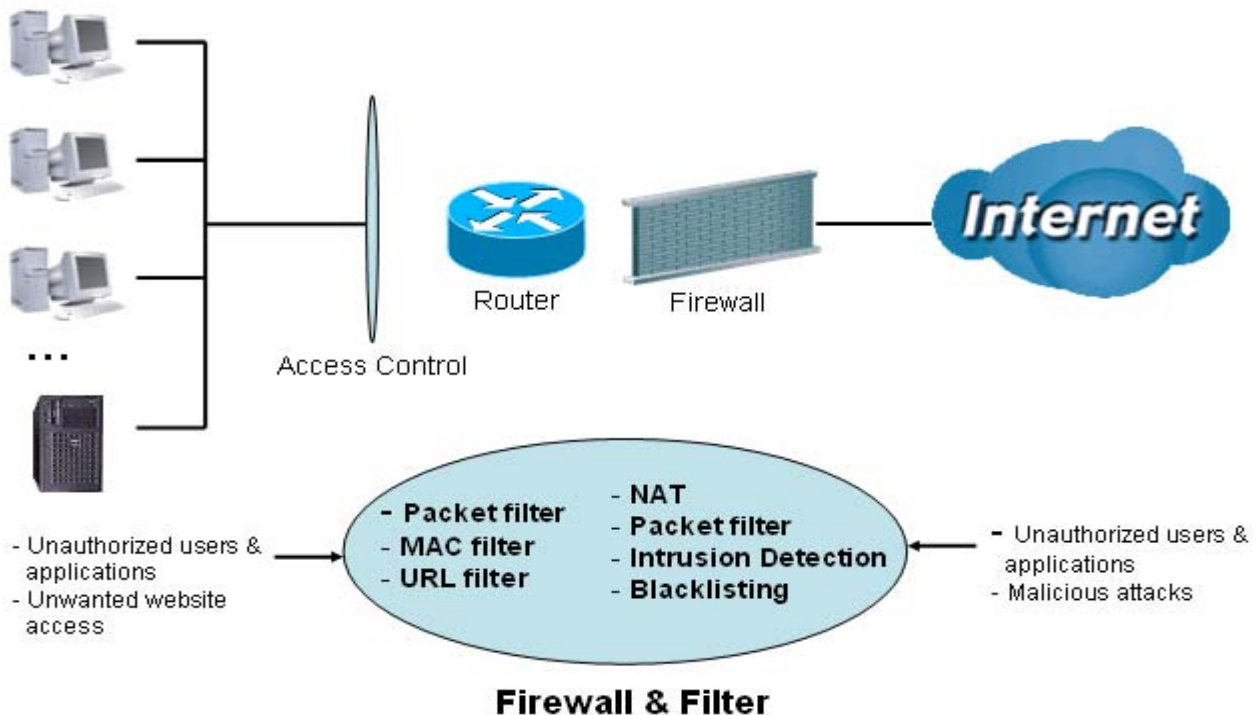
Firewall: Prevents access from outside your network. The router provides three levels of security support:

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

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

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

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

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

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

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

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

General Settings

You can choose not to enable Firewall and still able to access to URL Filter 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.

General Settings

Firewall Security

Security	○ Enable ⊙ Disable
Policy	○ All blocked/User-defined
	○ High security level
	• Medium security level
	○ Low security level

(⚠️*If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.*)

Block WAN Request	○ Enable ⊙ Disable

(⚠️*Enable for preventing any ping test from Internet, such as hacker attack.*)

[Apply]

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

Packet Filter

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

Packet Filter

Add TCP/UDP Filter ▶   Add Raw IP Filter ▶

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask	Protocol	Source port(s)	Inbound		
		Destination IP / Netmask		Destination port(s)	Outbound		
lei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		
lei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
lei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
lei_ftp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		21 ~ 21	Allow		
lei_tnet	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		23 ~ 23	Allow		
lei_smtp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		25 ~ 25	Allow		
lei_pop3	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		110 ~ 110	Allow		

Chapter 4: Configuration

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

Chapter 4: Configuration

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

Chapter 4: Configuration

Packet Filter – Add TCP/UDP Filter

Packet Filter

Add TCP/UDP Filter

Rule Name Helper ◉	[ ]		
Time Schedule	Always On ▾		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Type	TCP ▾		
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Allow ▾		
Outbound	Allow ▾		

[Apply] Return ◉

Rule Name: Users-define description to identify this entry or click **Helper ◉** 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 form; set IP address and Subnet Mask to **0.0.0.0** to inactive the Address-Filter rule.

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

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

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 **Apply** button to apply your changes.

Packet Filter – Add Raw IP Filter

Packet Filter

Add Raw IP Filter

Rule Name Helper ▶	[ ]
Time Schedule	Always On ▼
Protocol Number	[ ]
Inbound	Allow ▼
Outbound	Allow ▼

Apply   Return ▶

Rule Name: Users-define description to identify this entry or click Helper ▶ 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

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

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

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

Example: Configuring your firewall to allow for 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.

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask / Destination IP / Netmask	Protocol	Source port(s) / Destination port(s)	Inbound / Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		
mei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
mei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
mei_ftp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		21 ~ 21	Allow		
mei_tnet	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		23 ~ 23	Allow		
mei_smtp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		25 ~ 25	Allow		
mei_pop3	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		110 ~ 110	Allow		
mei_nntp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		119 ~ 119	Allow		

Configuring Packet Filter:

1. Click **Port 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.

Packet Filter

Add TCP/UDP Filter ▶	Add Raw IP Filter ▶

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask / Destination IP / Netmask	Protocol	Source port(s) / Destination port(s)	Inbound / Outbound		Click Delete
mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		
mei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
mei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
mei_ftp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		21 ~ 21	Allow		
mei_tnet	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		23 ~ 23	Allow		

2. Click **Delete** to delete the existing HTTP rule.

3. Click **Add TCP/UDP Filter**.

Click Add TCP/UDP Filter

Packet Filter

Add TCP/UDP Filter ▶	Add Raw IP Filter ▶

4. 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*

Packet Filter

Add TCP/UDP Filter

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

[Apply] Return ▶

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

Cindy_HTTP	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Allow Allow	Edit ▶	Delete ▶

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

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

Virtual Server (Port Forwarding)

Add Virtual Server ▶	Edit DMZ Host ▶	Edit One-to-one NAT ▶

Virtual Server Table

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address		
HTTP_Server	Always On	tcp	80 - 80	80 - 80	192.168.1.254	Edit ▶	Delete ▶

Intrusion Detection

Intrusion Detection

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

Apply

Clear Blacklist

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

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

Chapter 4: Configuration

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

_____ 72

Chapter 4: Configuration

dropped.

3. If the packet does not match either of the above two items, it is sent to the remote web server.

4. Please be note that the completed URL, "www" + domain name shall be specified. For example to block traffic to www.google.com.au, enter "www.google" or "www.google.com"

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

Domains Filtering

Domain Name

Domain Name	www.google
Type	Forbidden Domain ▾

Apply

Trusted Domain

Name	Domain	
item0	www.abc	Delete ▶

Forbidden Domain

Name	Domain	
item1	www.google	Delete ▶

Return ▶

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.

IM/P2P Blocking

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

[Apply] [Cancel]

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 <u>enabled</u> 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 <u>enabled</u> the *Peer to Peer Blocking* first.

Firewall Log

Firewall Log

Event will be shown in the Status - Event Log

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

[Apply]

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.

Chapter 4: Configuration

VPN - Virtual Private Networks (BiPAC 7404VGO Only)

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

PPTP (Point-to-Point Tunneling Protocol)

PPTP

VPN/PPTP for Remote Access Application

Enable	Disable	Name	Type	Status		

VPN/PPTP for LAN-to-LAN Application

Enable	Disable	Name	Type	Status		

Create ◐

Apply

There are two types of PPTP VPN supported; **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to configure a new VPN connection.

PPTP

VPN/PPTP for Remote Access Application

Enable	Disable	Name	Type	Status		
○	◉	Testing	dialout	Inactive	Edit ◐	Delete ◐

VPN/PPTP for LAN-to-LAN Application

Enable	Disable	Name	Type	Status		

Create ◐

Apply

After you have created PPTP connection, account status will be displayed. (See example above).

⊙ **Enable / Disable:** This function activates or deactivates the PPTP connection.   To wish interrupting the tunnel, check **Disable** radio button and click **Apply** button to deactivate the connection.

Name: User-defined name of the connection.

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

Status: It informs your PPTP tunnel connection condition.

PPTP Connection - Remote Access

PPTP

Remote Access Connection

Connection Name						
Type	⦿ Dial out,	Server IP Address (or Domain Name)				
	○ Dial in,	Private IP Address Assigned to Dialin User				
Username						
Password						
Auth. Type	Chap(Auto) ▾					
Data Encryption	Auto ▾	Key Length	Auto ▾	Mode	stateful ▾	
Idle Timeout	0 minutes					
Active as default route	☐ Enable					

Apply

Connection Name: User-defined name for the connection (e.g. "connection to office").

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

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

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

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

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

PPP 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.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

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

Click **Apply** button to apply 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.

PPTP VPN-Remote Access (Dial-out)
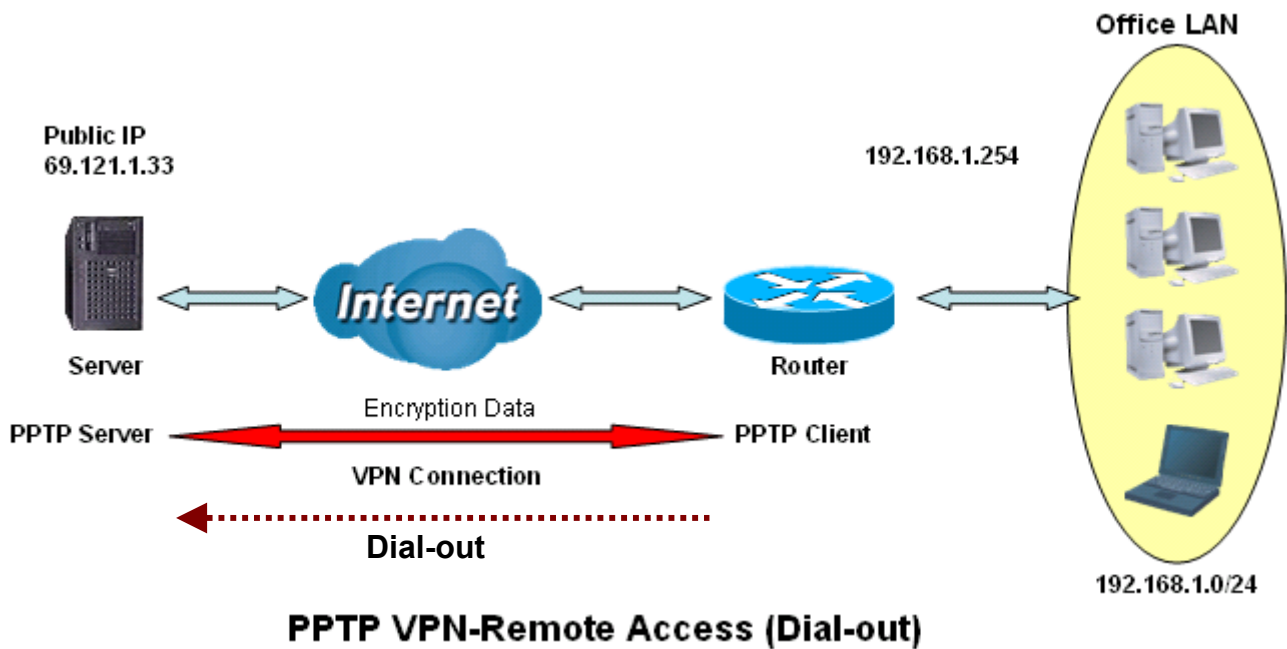
Configuring the PPTP VPN in the Office

You can either input the IP address (69.1.121.33 in this case) or hostname to reach the server.

PPTP

Remote Access Connection

Connection Name	VPN_PPTP ①		
Type	○ Dial out,	Server IP Address (or Domain Name)	69.121.1.33 ②
	○ Dial in,	Private IP Address Assigned to Dialin User	
Username	username ③		
Password	******		
Auth. Type	Chap(Auto) ▼		④
Data Encryption	Auto ▼	Key Length Auto ▼ Mode stateful ▼	
Idle Timeout	0 minutes ⑤		
Active as default route	☐ Enable		

[Apply]

Item	Function		Description
1	Connection Name	VPN_PPTP	Given name of PPTP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	An Dialed server IP
3	Username	username	A given username & password
	Password	123456	
4	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	
5	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time **0** means the connection is always on.

PPTP Connection - LAN to LAN

PPTP

LAN to LAN

Connection Name			
Type	⊙ Dial out,	Server IP Address (or Hostname)	
	○ Dial in,	Private IP Address Assigned to Dialin User	
Peer Network IP		Netmask	
Username			
Password			
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾	Mode	stateful ▾
Idle Timeout	0 minutes		

[Apply]

Connection Name: User-define description of the connection.

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

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

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

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

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

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

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

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

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

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

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

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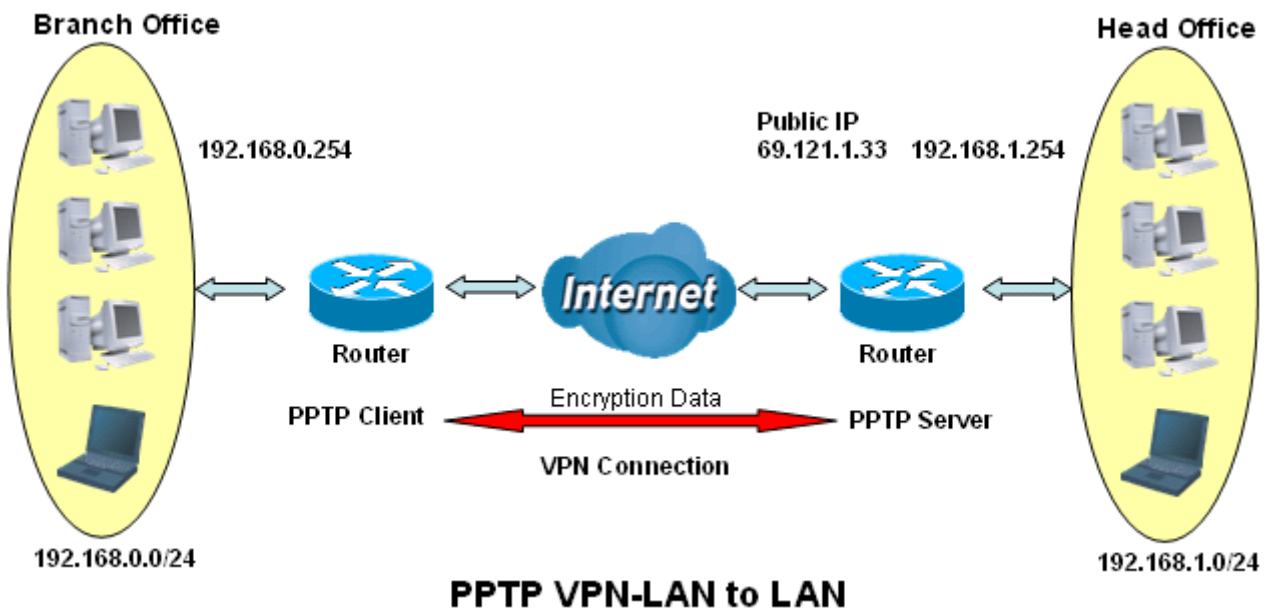
PPTP VPN-LAN to LAN

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

Chapter 4: Configuration

Configuring PPTP VPN in the Head Office

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

Item	Function		Description
1	Connection Name	HeadOffice	Given a name of PPTP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	IP address assigned to branch office network
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.

Configuring PPTP 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.

PPTP

LAN to LAN

Connection Name	BranchOffice ①		
Type	⊙ Dial out,	Server IP Address (or Hostname)	69.121.1.33 ②
	○ Dial in,	Private IP Address Assigned to Dialin User	
Peer Network IP	192.168.1.0	Netmask	255.255.255.0 ③
Username	username		
Password	•••••• ④		
Auth. Type	Chap(Auto) ▾		
Data Encryption	Auto ▾	Key Length	Auto ▾	Mode	stateful ▾ ⑤
Idle Timeout	0 minutes ⑥		

[Apply]

Item	Function		Description
1	Connection Name	BranchOffice	Given a name of PPTP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases, PPTP server & client will determine the value automatically. Refer to manual for details if you want to change the setting.
	Data Encryption	Auto	
	Key Length	Auto	
	Mode	stateful	
6	Idle Time	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.

IPSec (IP Security Protocol)

IPSec

VPN Tunnels

Enable	Disable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal		

Create ◐

[Apply]

Click **Create** to create a new IPSec VPN connection account.

IPSec

VPN Tunnels

Enable	Disable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal		
○	⊙	cindy	192.168.3.0 /255.255.255.0	192.168.4.0 /255.255.255.0	testing.no-ip.info	AH:none ESP:md5,3des	Edit ◐	Delete ◐

Create ◐

[Apply]

After you have created the IPSec connection, account information will be displayed. (See example above).

◉ **Enable / Disable:** This function activates or deactivates the IPSec connection.   To wish interrupting the tunnel, check **Disable** radio button and click **Apply** button to deactivate the connection.

Name: This is the user-defined 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

Connection Name: User-defined 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.

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 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).

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

Advanced Option

This function is only available after completed creating an IPSec account. Click **Advanced Option** to change the following settings:

IPSec	
IKE Mode	Main
IKE Proposal	
Hash Function	MD5
Encryption	3DES
Diffie-Hellman Group	MODP 1024 (Group 2)
Local ID	
Type	Default
Content	
Remote ID	
Type	Default
Identifier	
SA Lifetime	
Phase 1 (IKE)	480 minutes
Phase 2 (IPSec)	60 minutes
PING for keepalive	
PING to the IP	0.0.0.0 (0.0.0.0 means NEVER)
Interval	10 seconds (0-3600, 0 means NEVER)
Disconnection Time after no traffic	180 seconds (180 at least)
Reconnection Time	3 minutes (3 at least)

Apply   Reset

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

IKE Proposal:

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

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

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

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

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

Local ID:

⊙ **Type:** Specify local ID type.

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

Remote ID:

⊙ **Type:** Specify Remote ID type.

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

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

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

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

A short SA time increases security by forcing the two parties to update the keys. However, every

time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Ping to Keep Alive:

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

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

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

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

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

Select the **Apply** button to update the settings.

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

IPSec VPN-LAN to LAN
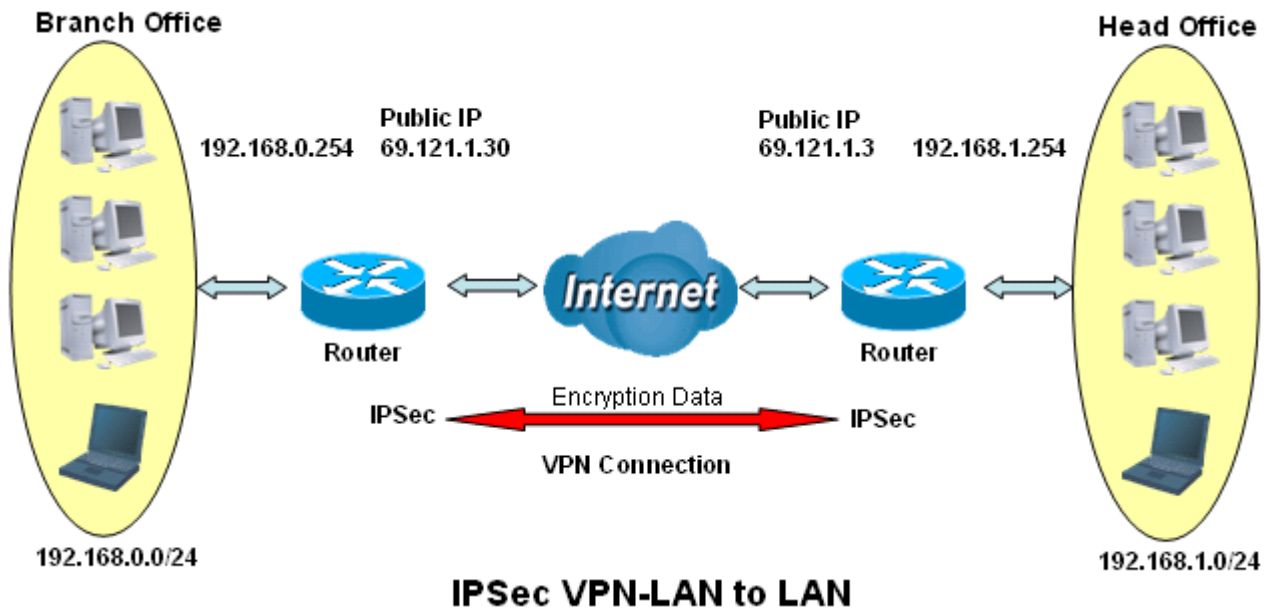
Table 3: Network Configuration and Security Plan

	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

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

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

Attention

Configuring IPSec VPN in the Head Office

IPSec						
Create						
Connection Name	IPSec_HeadOffice ①					
Local						
Network	○ Single Address	IP Address				
	⦿ Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0 ②	
	○ IP Range	IP Address		End IP		
Remote						
Secure Gateway Address(or Hostname)		61.121.1.30 ③				
Network	○ Single Address	IP Address				
	⦿ Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0 ④	
	○ IP Range	IP Address		End IP		
Proposal						
⦿ ESP	Authentication	MD5			⑤	
	Encryption	3DES				
○ AH	Authentication	MD5				
Perfect Forward Secrecy	None					
Pre-shared Key	12345678					

Apply

Item	Function		Description
1	Connection Name	IPSec_HeadOffice	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
4	Subnet		Check Subnet radio button
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	ESP		Check ESP radio button
	Authentication	MD5	
	Encryption	3DES	Security plan
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

Chapter 4: Configuration

Configuring IPSec VPN in the Branch Office

IPSec					
Create					
Connection Name	IPSec_BranchOffice ①				
Local					
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0 ②
	○ IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)		61.121.1.3 ③			
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0 ④
	○ IP Range	IP Address		End IP	
Proposal					
● ESP	Authentication	MD5 ▼			⑤
	Encryption	3DES ▼			
○ AH	Authentication	MD5 ▼			
Perfect Forward Secrecy	None ▼				
Pre-shared Key	12345678				
Apply					

Item	Function		Description	
1	Connection Name	IPSec_Branch Office	Given a name of IPSec connection	
2	Subnet		Check Subnet radio button	
	IP Address	192.168.0.0	Branch office network	
	Netmask	255.255.255.0		
3	Secure Gateway Address (or Hostname)	69.121.1.3	IP address of the head office router (in WAN side)	
4	Subnet		Check Subnet radio button	
	IP Address	192.168.1.0	Head office network	
	Netmask	255.255.255.0		
5	ESP		Check ESP radio button	
	Authentication	MD5	Security plan	
	Encryption	3DES		
	Prefer Forward Security	None		
	Pre-shared Key	12345678		

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

Configuring IPSec VPN in the Office

Item	Function		Description
1	Connection Name	IPSec	Given a name of IPSec connection
2	Subnet		Check Subnet radio button
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
3	Secure Gateway Address (or Hostname)	69.121.1.30	IP address of the head office router (in WAN side)
4	Single Address		Check Single Address radio button
	IP Address	69.121.1.30	Remote worker's IP address
5	ESP		Check ESP radio button
	Authentication	MD5	
	Encryption	3DES	Security plan
	Prefer Forward Security	None	
	Pre-shared Key	12345678	

L2TP (Layer Two Tunneling Protocol)

Two types of L2TP VPN are supported **Remote Access** and **LAN-to-LAN** (please refer below for more information.). Click **Create** to create a new VPN connection account.

After you have created L2TP connection, account status will be displayed. (See example above).

⊙ **Enable / Disable:** This function activates or deactivates the L2TP connection.   To wish interrupting the tunnel, check **Disable** radio button and click **Apply** button to deactivate the connection.

Name: This is the user-defined name of the connection.

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

Status: It informs your L2TP tunnel connection condition.

Chapter 4: Configuration

L2TP Connection - Remote Access

L2TP

Remote Access Connection

Connection Name			
Type	⊙ Dial out,	Server IP Address (or Domain Name)	
	○ Dial in,	Private IP Address Assigned to Dialin User	
Username			
Password			
Auth. Type	Chap(Auto) ▾		
Idle Timeout	0 minutes		
Active as default route	☐ Enable		
IPSec	☐ Enable		
Authentication	None ▾		
Encryption	NULL ▾		
Perfect Forward Secrecy	None ▾		
Pre-shared Key			
Remote Host Name		(Optional)	
Local Host Name		(Optional)	
Tunnel Authentication	☐ Enable		
Secret			

[Apply]

L2TP VPN Connection

Connection Name: User-defined name for the connection (e.g. "connection to office").

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

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

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

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

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

PPP 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.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a pre-determined period of time. 0 means this connection is always on.

Active as default route: Commonly used by the *Dial-out* connection which all packets will route through

the VPN tunnel to the Internet; therefore, active the function may degrade the Internet performance.

Click **Apply** after changing settings.

L2TP over IPSec (L2TP/IPSec) VPN Connection

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 **NONE**. NONE 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).

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.**

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.

Click **Apply** after changing settings.

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.

L2TP VPN-Remote Access (Dial-in)
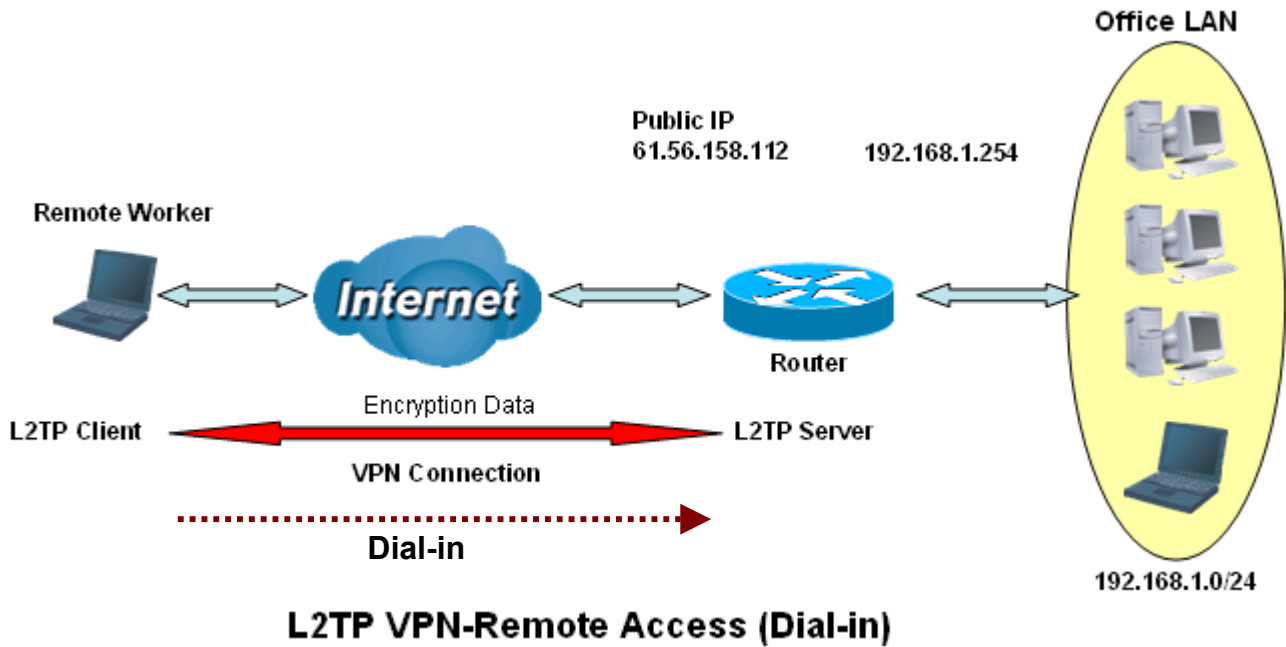
Configuring L2TP VPN in the Office

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.

Item	Function		Description
1	Connection Name	VPN_L2TP	Given a name of L2TP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	An assigned IP address for the remote worker
3	Username	username	Input username & password to authenticate remote worker
	Password	123456	
4	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
5	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time.　Idle time 0 means the connection is always on.
6	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	
	Encryption	3DES	Both sites should use the same value.
	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.

L2TP VPN-Remote Access (Dial-out)
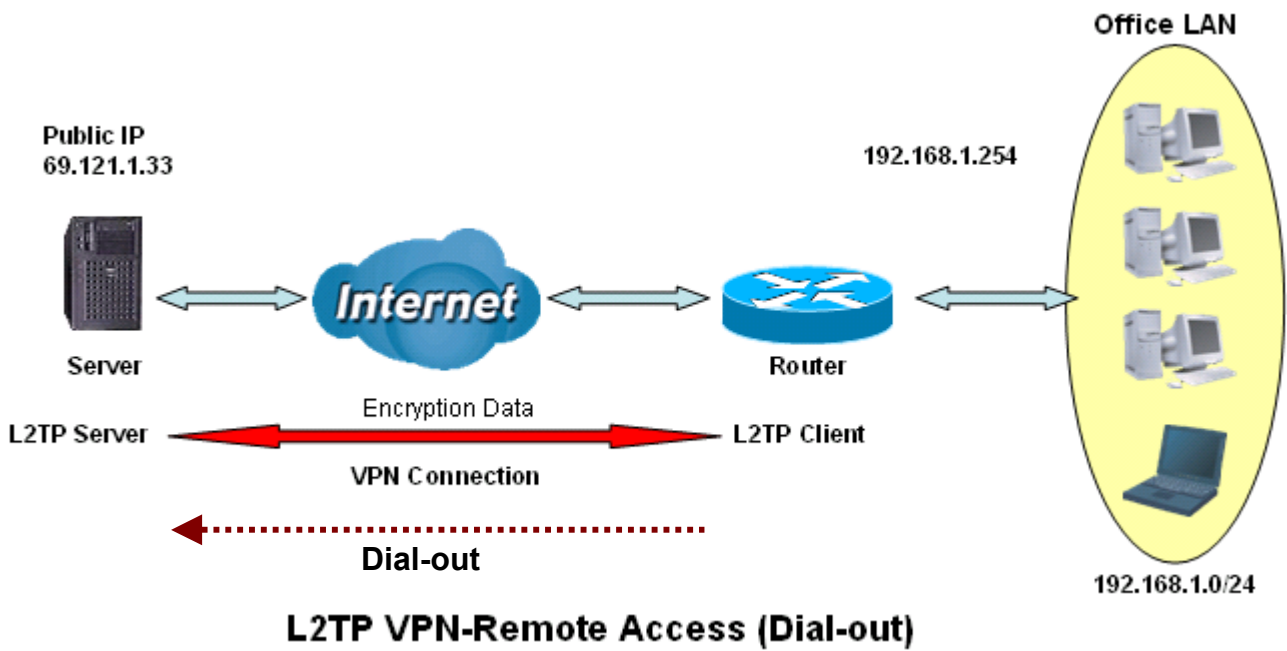
Configuring the L2TP VPN in the Office

Item	Function		Description
1	Connection Name	VPN_L2TP	Given name of L2TP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	An Dialed server IP
3	Username	username	A given username & password
	Password	123456	
4	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
5	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
6	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

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

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

Chapter 4: Configuration

L2TP Connection - LAN to LAN

L2TP VPN Connection

Connection Name: User-define description of the connection.

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

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

Peer Network IP: Enter Peer network IP address.

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

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

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

PPP 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.

Idle Time: Auto-disconnect the VPN connection when there is no activity on the connection for a

predetermined period of time. 0 means this connection is always on.

Click **Apply** after changing settings.

L2TP over IPSec (L2TP/IPSec) VPN Connection

IPSec: Enable for enhancing your L2TP VPN security.

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

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

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

Encryption: Select the encryption method from the pull-down menu. There are four options, **DES**, **3DES**, **AES** and **NONE**. NONE 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).

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.**

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.

Click **Apply** after changing settings.

Example: Configuring L2TP LAN-to-LAN VPN Connection

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

	Both office LAN networks **MUST in different subnet** with LAN to LAN application.
	Functions of **Pre-shared Key, VPN Connection Type and Security Algorithm MUST BE** identically set up on both sides.
Attention	

Configuring L2TP VPN in the Head Office

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

Item	Function		Description
1	Connection Name	HeadOffice	Given a name of L2TP connection
2	Dial in		Check Dial in
	Private IP Address Assigned to Dialing User	192.168.1.200	IP address assigned to branch office network
3	Peer Network IP	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
7	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	
	Encryption	3DES	Both sites should use the same value.
	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.

Item	Function		Description
1	Connection Name	BranchOffice	Given a name of L2TP connection
2	Dial out		Check Dial out
	Server IP Address (or Hostname)	69.121.1.33	IP address of the head office router (in WAN side)
3	Peer Network IP	192.168.1.0	Head office network
	Netmask	255.255.255.0	
4	Username	username	Input username & password to authenticate branch office network
	Password	123456	
5	Auth.Type	Chap(Auto)	Keep as default value in most of the cases.
6	Idle Timeout	0	The connection will be disconnected when there Is no traffic in a predefined period of time. Idle time 0 means the connection is always on.
7	IPSec		Enable for enhancing your L2TP VPN security.
	Authentication	MD5	Both sites should use the same value.
	Encryption	3DES	
	Perfect Forward Secrecy	None	
	Pre-shared Key	12345678	

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: **Wizard**, **General Settings**, **Phone Port, PSTN Dial Plan, VoIP Dial Plan** and **Ring &Tone**.

Wizard

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

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.

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.

Setting for Phone Port 1

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

Select Profile: It allows you to select a desired VoIP provider whom is not defined already in the *SIP Service Provider.*   You may manually setup the SIP accounts by entering VoIP SIP information to *User-defined Profile.*   See below for details.

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

Authentication 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.

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

Setting for Phone Port 2

Click box of **Same as Phone Port 1** to set phone port 2 be identical as phone port 1.

Please refer to descriptions in "Setting for Phone Port 1".

User-defined Profiles

Note: User defined profiles are limited to 8 only.

VoIP User-defined Profiles

Profile List

Name	Registrar Address	Phone Number		

Create ◉   Return ◉

Create VoIP User-defined Profile

SIP Setting

Profile Name		
Registrar Address(or Hostname)		
Registrar Port	5060	
Expire	3600	seconds
User Domain/Realm		(If empty, it is the same as Registrar Address.)
Outbound Proxy Address		(If empty, it is the same as Registrar Address.)
Outbound Proxy Port	5060	
Phone Number		
Authentication Username		
Authentication Password		
Display Name		

[Apply] [Cancel] Return ◉

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.

Authentication Username: Same as Phone Number.

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

Chapter 4: Configuration

Confirm Password: Re-enter the password for confirmation.

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

General Settings

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.

<u>**SIP Device Parameters**</u>

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,: 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.

Setting for Phone Port 1

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.

Setting for Phone Port 2

Please refer to descriptions in "Setting for Phone Port 1".

How to register to SIP Server

1)   In Wizard Section, select your VoIP Service Provider and input information in the filed of *Phone Number, Authentication Username* and *Authentication Password.*

2)   In Wizard Section, click Apply button to apply the settings.

3)   In General Settings, make sure general VoIP SIP information are correctly inserted.

4)   In General Settings, click Apply button to apply the settings.

5)   In General Settings, click Synch Now button to register the account(s) with your VoIP server.

Advanced – Parameters

VoIP Advanced Settings

Parameters	
VoIP through IP Interface	ipwan ▾
Voice Frame Size	20 ms ▾
PSTN Auto-fallback	☐ Enable, when receive the specified SIP codes Edit ▶

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.

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.

Advanced – PSTN Environment Adjustment

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

PSTN Environment Adjustment		
PSTN Voltage Configuration	ONHOOK Voltage: 18 OFFHOOK Voltage: 4	Hint ●
Check your PSTN Voltage Levels	○ Ensure your phone is ONHOOK, click [Check Level] , value is . ○ Ensure your phone is OFFHOOK, click [Check Level] , value is .	
[Apply] [Cancel] Return ●		

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.

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

Phone Configuration

Phone Port

Index	Phone Number	Display Name	Registered	
1			unknown	Edit ◉
2			unknown	Edit ◉

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

Phone Port 1

Login Account Configuration

Phone Number	
Authentication Username	
Authentication Password	
Confirm Password	
Display Name	

Codec Preference

Priority 1	G.729
Priority 2	PCMU (G.711 u-Law)
Priority 3	PCMA (G.711 A-Law)

Speed Dial

2#	
3#	
4#	
5#	
6#	
7#	
8#	
9#	

[Apply] [Cancel] Volume Control ◉

Login Account Configuration

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

Authentication Username: Same as Phone Number.

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

Chapter 4: Configuration

Confirm Password: Re-enter the password for confirmation.

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

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. 8kbps bandwidth is needed.

G.711µ-LAW: It is a basic non-compressed encoder and decoder technique. µ-LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample. 64kbps bandwidth is needed.

G.711A-LAW: It is a basic non-compressed encoder and decoder technique. µ-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample. 64kbps bandwidth is needed.

Non-used: Only available in Priority 2 and 3. It is selected if codec is not to be used.

Note: Codec priority is assigned in the order as G.729 > G.711µ-LAW > G.711A-LAW**.**

Speed Dial

Speed Dial comes 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.

For examples:

If your friend Tim gives you a SIP URL as sip: 89755@192.246.69.223 then you can fill in as 89755@192.246.69.223.

If your friend Felix gives you a SIP URL as sip: felix@iptel.org then you can fill in as felix@iptel.org.

If your friend Greg gives you an IP address "192.246.56.56" only, then you can fill in as "192.246.56.56". In case, some of users may use DDNS, you can fill in with domain name as well.

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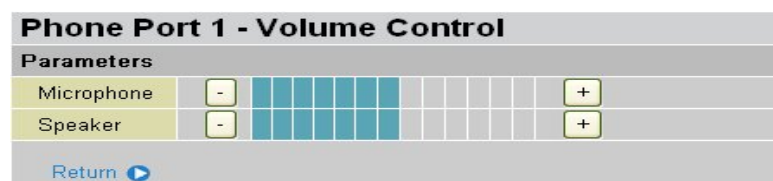
Volume control helps you to adjust the voice quality of telephone to the best comfortable listening level.

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.*

PSTN Dial Plan

Add Entry ◐

PSTN Dial Plan

Prefix	Number of Digits	Action		

Add PSTN Dial Plan Entry

Parameters

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

[Apply] [Cancel] Return ◐

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 and 2 will automatically rely to PSTN line when:
- **Power Down**
- **Internet Service Fail**, i.e., lost of WAN IP Address
- **SIP option is disabled.** See *VoIP General Setting* section.
- **Calls match with rule(s) defined in the** *PSTN Digit Plan.*
- **SIP service is not accessible.** This excludes when:
  - User manually disables Registration.
  - User inserts a wrong authentication username or password.
  - User dials a wrong SIP number, only and if, the *PSTN Auto-Fallback* function is <u>not</u> enabled. See *VoIP General Setting / Advanced* for information.

Chapter 4: Configuration

PSTN Dial Plan Examples:

1) Dial with Prefix

Add Dial Plan Entry

Parameters

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

[Apply] [Cancel] Return ▶

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

2) Dial without Prefix

Add Dial Plan Entry

Parameters

Prefix	9
Number of Digits	3 (0..15)
Action	Dial without Prefix ▾

[Apply] [Cancel] Return ▶

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

Add Dial Plan Entry

Parameters

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

[Apply] [Cancel] Return ▶

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 exceed 6 digits.

4) Dial at Timeout no Prefix

Add PSTN Dial Plan Entry

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

[Apply] [Cancel] Return ►

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.

VoIP Dial Plan 1

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

Apply   Test ▶

Dial Plan Rules List

Rule Name	
x.T	Delete ▶

Add

Parameters

A listed of special dial feature comes handy when you have a miss call or need to transfer a call to a third party. Details please refer to the section **Special dial codes** below.

*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.

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.

Test: It is a tool to help to identify the call number is being properly being processed prior to making an actual call.

Click **Apply** to apply the settings.

Dial Plan Rules List

Click **Add** to create and define 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 it is provided by your VoIP Service Provider or Local Telephone Service Provider for special service(s).

 # (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.

<@SIPgateway> / Intelligent Call Routing Example:

VoIP Gateway let you use 3 VoIP/SIP providers at the same time.　VoIP/SIP providers are *localcheap.com, longdischeap.com* and *mobilecheap.com.*　Each provider has its price for different type of calls and I can set the following rule for each providers.

1) Phone 1: For Local calls: I use *localcheap.com* that charges $0.01 per minute to all local calls.　I set a dial rule, **<:03>[123]x.T**, on my phone port 1.

Create Rule

Parameters

Prefix Processing	● Prepend `03`	unconditionally
	○ If prefix is ` `	, delete it
	○ If prefix is ` `	, replace with ` `
	○ No prefix	
Main Digit Sequence	`[123]x.` @ `Current Profile ▼`	

[Apply] Return ○

Localcheap.com is the default VoIP provider I set on phone port 1.   When I call out any number start with 1 or 2 or 3 and plus rest of the phone number for local call, 03 is always prepended in front of these number.   If **2**3295 are dialed, 03-2-32935 is the actual phone number called out via localcheap.com provider.

2) Phone 1: For International calls: I use *longdischeap.com* that charges $0.05 per minute to all International long distance calls.   I set a dial rule, **0[2456]x.T<@LongdisCheap>**, on my phone port 1.

Create Rule

Parameters

Prefix Processing	○ Prepend ` `	unconditionally
	○ If prefix is ` `	, delete it
	○ If prefix is ` `	, replace with ` `
	● No prefix	
Main Digit Sequence	`0[2456]x.` @ `LongdisCheap ▼`	

[Apply] Return ○

Longislcheap.com is one of the VoIP providers I set in the User-defined profile.   No prefix is attached to the dialed number when I call out number 0 plus any following number 2 or 4 or 5 or 6 and plus rest of the phone number for an international call.   If **02**016148513295 are dialed, 0-2-016148513295 is the actual phone number called out via longdischeap.com provider.

3) Phone 2: For Mobile calls: I use *mobilecheap.com* that charges $0.25 per minute to all local calls.   I set a dial rule, **<123:09>39x.T**, on my phone port 2.

Create Rule

Parameters

Prefix Processing	○ Prepend ` `	unconditionally
	○ If prefix is ` `	, delete it
	● If prefix is `123`	, replace with `09`
	○ No prefix	
Main Digit Sequence	`39x.` @ `Current Profile ▼`	

[Apply] Return ○

Mobilecheap.com is the default VoIP provider I set on phone port 2.   When I call out 123-39-45678 for a mobile call, 123 is replaced with 09.   Therefore, 09-39-45678 is the actual phone number called out via Mobilecheap.com provider.

The Intelligent Call Gateway not only saves time from changing VoIP settings to different provider to make call get routed to specific gateway(s) automatically but also taking advantage of different call rate.

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	UK

Ring Parameters

	On 1	Off 1	On 2	Off 2	On 3	Off 3	
Ring Cadence (in ms)	400	200	400	2000	0	0	

Tone Parameters

Country Specific Ring & 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 an advanced user, unless you are instructed to do so.

Click **Apply** to apply the settings.

Special Dial Codes

The following table lists the special dial codes that are built-in to the system:

Option	Description
Flash-hook (Wireless Router with LINE port only)	Switch to PSTN line Note: A quick press of the hook. On some phones a button is provided which provides Flash-hook functionality. The button is marked "FLASH" or "RECALL".
*69	Return the last missed call for SIP service only Note: Entering this on a phone will call the last number which made a call to the phone. For example A makes a call to B, but hangs up before B answers. If B enters *69, A will be called.
##	Last number redial
*20	Set do not disturb on Note: It is possible to set a Do-Not-Disturb feature on a phone such that any phone which calls the phone will receive an engaged tone and the phone called will not ring. For example, B enters *20 and hangs up. A makes a call to B, and receives the engaged tone and phone B does not ring.
*80	Set do not disturb off
*74<x><number>#	Set the number for Speed dial code 'x', where 'x' is a number between 2 and 9. Note: Where <x> is a number between 2 and 9, and <number> is the number to dial. The code needed to dial a speed dial from a phone connected to a VoIP Router is: <x>#, where **<x>** is a number between 2 and 9. The settings will infect to your setting in Speed Dial on WEB GUI.
*90<phone-number>	Set the number for performing **Blind Call Transfer**, where <phone-number> is the number that you wish to transfer the call to. It's for SIP service only. Note: In **Blind Call Transfer**, you have a call in progress (incoming or outgoing) and decide you wish to transfer the call to another phone. To transfer the call, perform the following steps: 1. Hook-flash to get a dial tone. 2. Dial *90<phone-number> (e.g. *907401), there will be a confirmation tone then hang up. The other end will hear ring back and the called third-party phone will ring. When the third-party phone is picked up the two calls will be connected. If the third-party phone does not answer then the caller being transferred can hang up to cancel the connect attempt.

QoS - Quality of Service

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

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

Prioritization

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

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

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

Prioritization

Configuration (from LAN to WAN packet)

Application	Time Schedule	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)		DSCP Marking
PPTP	Disabled ▼	High ▼	GRE	none / none	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼
[__] 🗑	Always On ▼	High ▼	any ▼	0 ~0 / 0 ~0	0.0.0.0 ~0.0.0.0 / 0.0.0.0 ~0.0.0.0		Disabled ▼

Click Clear

You can click **Clear** to delete the existing Application.

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

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

125

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

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

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

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

Table 4: DSCP Mapping Table

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

Outbound IP Throttling (LAN to WAN)

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

Click Clear — You can click **Clear** to delete the existing Application.

Application: 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.

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

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

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

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

Outbound Rate Limit: To limit the speed of outbound traffic

Chapter 4: Configuration

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.

Click Clear | You can click **Clear** to delete the existing Application.

Application: 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.

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

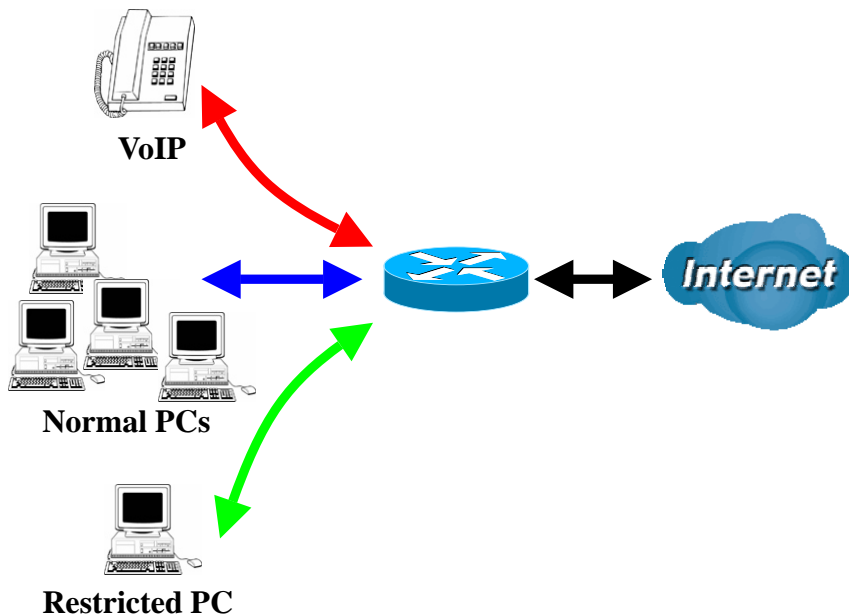**Destination Port**: The destination port of packets to be monitored.

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

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

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

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

Prioritization

Configuration (from LAN to WAN packet)

Application	Time Schedule	Priority	Protocol	Source Port / Destination Port	Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)		DSCP Marking
PPTP	Always On	High	GRE	none	0.0.0.0	~ 0.0.0.0	Gold service (L)
				none	0.0.0.0	~ 0.0.0.0	
VoIP	Always On	High	any	0 ~ 0	192.168.1.1	~ 192.168.1.1	Gold service (L)
				0 ~ 0	0.0.0.0	~ 0.0.0.0	
Restricted	TimeSlot1	Low	any	0 ~ 0	192.168.1.100	~ 192.168.1.100	Gold service (L)
				0 ~ 0	0.0.0.0	~ 0.0.0.0	

Chapter 4: Configuration

Mission-critical application

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

PPTP	Always On	High	GRE	none	0.0.0.0	~ 0.0.0.0		Gold service (L)	
				none	0.0.0.0	~ 0.0.0.0			

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.

VoIP	Always On	High	any	0	~ 0	192.168.1.1	~ 192.168.1.1		Gold service (L)	
				0	~ 0	0.0.0.0	~ 0.0.0.0			

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.

Restricted	TimeSlot1	Low	any	0	~ 0	192.168.1.100	~ 192.168.1.100		Gold service (L)	
				0	~ 0	0.0.0.0	~ 0.0.0.0			

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

Advanced setting by using IP throttling

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

Upstream: 928kbps (29*32kbps)
Mission-critical Application: 192kbps (6*32kbps)
Voice Application: 128kbps (4*32kbps)
Restricted Application: 160kbps (5*32kbps)
Other Applications: 448kbps (14*32kbps)

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

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Application	Time Schedule	Protocol	Source Port / Destination Port		Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)		Rate Limit
PPTP	Always On	gre	0 ~ 0		0.0.0.0 ~ 0.0.0.0		6 *32 (kbps)
			0 ~ 0		0.0.0.0 ~ 0.0.0.0		
VoIP	Always On	any	0 ~ 0		0.0.0.0 ~ 0.0.0.0		4 *32 (kbps)
			0 ~ 0		0.0.0.0 ~ 0.0.0.0		
Restricted	TimeSlot1	any	0 ~ 0		192.168.1.100 ~ 192.168.1.100		5 *32 (kbps)
			0 ~ 0		0.0.0.0 ~ 0.0.0.0		
Others	TimeSlot1	any	0 ~ 0		192.168.1.2 ~ 192.168.1.5		14 *32 (kbps)
			0 ~ 0		0.0.0.0 ~ 0.0.0.0		

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.

Inbound IP Throttling

Configuration (from WAN to LAN packet)

Application	Time Schedule	Protocol	Source Port / Destination Port		Source IP Address Range ('0.0.0.0' means Any) / Destination IP Address Range ('0.0.0.0' means Any)		Rate Limit
Restricted	TimeSlot1	any	0 ~ 0		0.0.0.0 ~ 0.0.0.0		64 *32 (kbps)
			0 ~ 0		192.168.1.100 ~ 192.168.1.100		

Chapter 4: Configuration

Virtual Server (known as Port Forwarding)

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

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

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

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

Virtual Server (Port Forwarding)

| Add Virtual Server ▶ | Edit DMZ Host ▶ | Edit One-to-one NAT ▶ |

Virtual Server Table

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address		

Add Virtual Server

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

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

Virtual Server (Port Forwarding)

Add Virtual Server ▶	Edit DMZ Host ▶	Edit One-to-one NAT ▶

Virtual Server Table

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	

Add Virtual Server in 'ipwan' IP Interface

Virtual Server Entry

Time Schedule	Always On
Application Helper ▶	
Protocol	tcp
External Port	from 0 to 0
Redirect Port	from 0 to 0
Internal IP Address Candidates ▶	

[Apply] Return ▶

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

Application: Users-define description to identify this entry or click Helper ▶ to select existing predefined rules.

Helper ▶ : 20 predefined rules are available. Click the Radio button to select the rule; 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.

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

Example:

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

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

Virtual Server (Port Forwarding)

Add Virtual Server ▶	Edit DMZ Host ▶	Edit One-to-one NAT ▶

Virtual Server Table

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address		
HTTP_Server	Always On	tcp	80 - 80	80 - 80	192.168.1.254	Edit ▶	Delete ▶

Edit: Click it to edit this virtual server application.

Delete: Click it to delete this virtual server application.

NOTE: Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention

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

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Edit DMZ Host

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

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

Virtual Server (Port Forwarding)

Add Virtual Server ▶	Edit DMZ Host ▶	Edit One-to-one NAT ▶

Virtual Server Table

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address		

Edit DMZ Host

DMZ Host for 'ipwan' IP Interface

○ Enabled ⊙ Disabled

Internal IP Address Candidates ▶	[ ]

[Apply] Return ▶

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

⊙ **Enabled:** It activates your 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.

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

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

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

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

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

Virtual Server (Port Forwarding)

| Add Virtual Server ▶ | Edit DMZ Host ▶ | Edit One-to-one NAT ▶ |

Virtual Server Table

| Application | Time Schedule | Protocol | External Port | Redirect Port | IP Address | | |

Global IP Pool in 'ipwan' IP interface

Global Address Pool

NAT Type	⦿ Disable	◯ Public to Private Subnet		◯ Public to DMZ Zone		
Global IP Addresses	⦿ Subnet	IP Address		Netmask		
	◯ IP Range	IP Address		End IP		

[Apply] Return ▶

One-to-one NAT Table Add Entry ▶

| Application | Time Schedule | Protocol | External Port | Redirect Port | IP Address | | |

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 Add Entry ▶ to create a new One-to-One NAT rule:

Add Virtual Server in 'ipwan' IP interface

Virtual Server Entry

Time Schedule	Always On
Application Helper ⦿	
Protocol	tcp
Global IP	
External Port	from 0 to 0
Redirect Port	from 0 to 0
Internal IP Address Candidates⦿	

Apply   Return⦿

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

Application: Users-defined description to identify this entry or click Helper ⦿ to select existing predefined rules.

Helper ⦿**:** 20 predefined rules are available. Click the Radio button to select the rule; 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;

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

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

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

Time Schedule

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

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

Time Schedule

Time Slot

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

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, Dynamic DNS**, **Check Email, Device Management, IGMP** and **VLAN Bridge.**

Static Route

Click on **Routing Table** and then choose **Create Route** add a routing table.

Static Route			
Create			
Destination			
Netmask			
via Gateway		or Interface	⌄
Cost	1		

Apply   Cancel

Destination: This is the destination subnet IP address.

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

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

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

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

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/

There are more than 5 DDNS services supported.

- ⊙ **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.

Chapter 4: Configuration

Check Email

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

Check Email

Parameters

Check Email	○ Enable ⊙ Disable
Account Name	
Password	
POP3 Mail Server	
Period	60 minutes
Dial-out for Checking Emails	☐ Automatic

[Apply]

Check Email:

⊙ **Disable:** Check to disable the router's Email checking function.

⊙ **Enable:** Check to enable the routers email checking function. The following fields will be activated and required:

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

Password: Enter the account's password.

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

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

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

Device Management

The Device Management advanced configuration 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	
Expire to auto-logout	180	seconds

Universal Plug and Play (UPnP)

UPnP	○ Enable ⊙ Disable
* UPnP Port	2800

SNMP Access Control

SNMP V1 and V2

Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	

SNMP V3

Username		Password	
Access Right	⊙ Read ○ Read/Write	IP Address	

*: This setting will become effective after you save to flash and restart the router.

[Apply]

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. 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
- ☑ Interfaces group
- ☑ Address Translation group

Chapter 4: Configuration

- ☑ IP group
- ☑ ICMP group
- ☑ TCP group
- ☑ UDP group
- ☒ EGP (not applicable)
- ☑ Transmission
- ☑ SNMP group

From RFC1650 (EtherLike-MIB):

- ☑ dot3Stats

From RFC 1493 (Bridge MIB):

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

From RFC 1471 (PPP/LCP MIB):

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

From RFC 1472 (PPP/Security MIB):

- ☑ PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- ☑ PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- ☑ PPP Bridge Group

From RFC1573 (IfMIB):

- ☑ ifMIBObjects Group

From RFC1695 (atmMIB):

- ☑ atmMIBObjects

From RFC 1907 (SNMPv2):

- ☑ only snmpSetSerialNo OID

IGMP

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

IGMP

Parameters

IGMP Forwarding	⦿ Enable ○ Disable
IGMP Snooping	○ Enable ⦿ Disable

Apply

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.

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,	Edit ◉	
Create VLAN ◉					

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Advanced VLAN Setup Example (Triply Play)

VLAN_data:
Ethernet Port 1, Wireless and Wireless WDS are reserving for Internet
- On Ethernet port 1 I also need VC 0/40 bridged.

VLAN_Vedio
Ethernet ports: 2, 3 and 4:
- 0/33 Bi-directional IP
- 0/34   Video
- 0/35   Video
- 0/36   Video Subscriber Services (EPG, EAS, etc.)
- 0/37   Video
- 0/38   Video
- 0/39   Spare

Step 1: Setup Member Ports

Go to **Configuration → LAN → 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) Please 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

Step 2: Create WAN Interface

Go to **Configuration → WAN→ ISP**

wanlink is the factory default WAN interface which in service for data/internet access. If your ISP uses this access protocol, click **Edit** to input other parameters if needed.   If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking **Change**.

From the example, 0/40 is used for data/internet and assumes PPPoE is used; click the **Edit** to change the VPI/VCI to 0/40.

Click **Create** to setup up additional WAN interface for video applications. Total of 8 VLAN is support; therefore, only 8 WAN interfaces can be created in the table.

From the example, PVC 0/33 to 0/39 is assigned for video using 1483 Bridged mode.   Check **RFC 1483 Bridged** and click **Next** to continue the setup.

Spaces next to VPI and VCI, type 0 and 33 in respectively. Select appropriate ATM Class, Encapsulation Method, Acceptable Frame Type, Filter Type and PVID for Untagged Frames.

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

ATM Class: The Quality of Service for ATM layer.

Encapsulation method: Select the encapsulation format, this is provided by your ISP.

Acceptable Frame Type: Specify what kind of traffic can 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.

PVID for Untagged Frames: PVID is known as Port VLAN Identifier. When an untagged packet is received by input port(s), this packet will be tagged with specified PVID.

From the example, VPI and VCI only section need to be filled-in and just leave the rest as is. Repeat the same procedure by clicking **Create** → select **RFC1483 Bridged** → fill-in the rest of PVC 0/34 to 0/39.

WAN Connection

WAN Services Table

Name	Description	Creator	VPI	VCI		
wanlink	PPPoE WAN Link	QuickStart	0	40	Edit ▶	Change ▶
rfc1483-0	RFC 1483 bridged mode	WebAdmin	0	33	Edit ▶	Delete ▶
rfc1483-1	RFC 1483 bridged mode	WebAdmin	0	34	Edit ▶	Delete ▶
rfc1483-2	RFC 1483 bridged mode	WebAdmin	0	35	Edit ▶	Delete ▶
rfc1483-3	RFC 1483 bridged mode	WebAdmin	0	36	Edit ▶	Delete ▶
rfc1483-4	RFC 1483 bridged mode	WebAdmin	0	37	Edit ▶	Delete ▶
rfc1483-5	RFC 1483 bridged mode	WebAdmin	0	38	Edit ▶	Delete ▶
rfc1483-6	RFC 1483 bridged mode	WebAdmin	0	39	Edit ▶	Delete ▶

Step 3: Setup VLAN Service

Go to **Configuration → Advanced → VLAN Bridge**

DefaultVlan lists all member ports.　It is necessary to group specific member ports for each VLAN.

From the example, two VLAN groups are requested: Data and Video.

To create another VLAN group for Video by clicking **Create VLAN.**

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit ▶	

Create VLAN ▶

Given a name and ID (PVID) to identify the Video group and the valid value range for PVID is 1 ~ 4094.

From the example:

VLAN untagged ports for Data/Internet: ethernet, wireless and wireless_wds.

VLAN untagged ports for Video: ethernet1, rfc-1483-0 ~ rfc-1483-6.

Click **Apply** to made change effective immediately.

Create VLAN

Parameters

| VLAN Name | Video_VLAN | VLAN ID | 2 | (2~4094) |

Tagged Member Port(s)
- [ ] ethernet [ ] wireless [ ] wireless_wds
- [ ] ethernet1 [ ] rfc1483-0 [ ] rfc1483-1 [ ] rfc1483-2
- [ ] rfc1483-3 [ ] rfc1483-4 [ ] rfc1483-5 [ ] rfc1483-6

Untagged Member Port(s)
- [ ] ethernet [ ] wireless [ ] wireless_wds
- [x] ethernet1 [x] rfc1483-0 [x] rfc1483-1 [x] rfc1483-2
- [x] rfc1483-3 [x] rfc1483-4 [x] rfc1483-5 [x] rfc1483-6

[Apply] [Cancel] Return ●

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	Untagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,	Edit ●	
Video_VLAN	2	None	ethernet1,rfc1483-0,rfc1483-1,rfc1483-2,rfc1483-3,rfc1483-4,rfc1483-5,rfc1483-6,	Edit ●	Delete ●

Create VLAN ●

Mapping the **VLAN Bridge** with **Bridge Interface** created in Step1, you will see the conformable relationship in these two screenshots.

Step 4: IGMP Snooping Enable

Go **Configuration → Advanced → IGMP**.

IGMP Snooping must be enabled in order to allow video stream forwarding correctly.

IGMP

Parameters

| IGMP Forwarding | ⦿ Enable ○ Disable |
| IGMP Snooping | ⦿ Enable ○ Disable |

[Apply]

Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid them being lost after turning off or resetting your router. Click **Save** to write your new configuration to FLASH.

Save Config to FLASH

Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to FLASH chips.

Apply

Logout

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

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

Chapter 5: Troubleshooting

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

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds.

Problems with the WAN Interface

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

Problems with the LAN Interface

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

APPENDIX A: Product Support and Contact Information

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

Contact Billion

AUSTRALIA

http://www.billion.com.au/

©2006 Billion Electric Co., Ltd. PC Range P/L. All Rights Reserved.

WORLDWIDE

http://www.billion.com/

Mac OS is a registered Trademark of Apple Computer, Inc.
Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered Trademarks of Microsoft Corporation.