BILLION™

BiPAC 8500/8520

SHDSL VPN Firewall Bridge/ Router

BiPAC 8501/8501 R2/8521

SHDSL.bis (VPN) Firewall Bridge/Router

User Manual

Firmware Version 5.75 Last Revised on September 2010

Table of Contents

Chapter 1: Product

Introduction to your Router

Thank you for purchasing Billion BiPAC 8500/ 8520/ 8501/ 8501 *R2*/ 8521 SHDSL (bis) Router. Your SHDSL (bis) router is an “all-in-one” unit, combining an SHDSL (bis) modem, SHDSL (bis) router and Ethernet network switch, providing everything you need to get the machines on your network connected to the Internet over your SHDSL (bis) broadband connection. With features such as an SHDSL (bis) Quick-Start wizard and DHCP Server, you can be online in no time at all and with minimum fuss and configuration, catering for both first-time users and professionals who require advanced features to control their Internet connection and network.

Features

SHDSL (bis) Multi-Mode Standard

BiPAC 8500 / 8520 SHDSL supports downstream and upstream transmission rates of up to 2.3 / 4.6 Mbps, respectively, and BiPAC 8501 R2 SHDSL bis can support up to 5.7 Mbps on 2-wire and 8521 SHDSL.bis can support up to 11.4 Mbps on 4-wire. BiPAC 85xx series also supports rate management that allows SHDSL (bis) subscribers to select an Internet access speed suiting their needs and budgets. BiPAC 8500/ 8520 and 8501 R2/ 8521 follows ITU standard PAM16 Line Code complies with G.991.2 and G.994.1 standards, and BiPAC 8501 R2 follows PAM 32 Line code with G.991.2 and G.991.2.bis standards. These models can support Annex A and B operating mode.

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 not only can enter the information they get from their ISP easily, it also enables immediate internet suffing.

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 networking simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to controling data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.

Network Address Translation (NAT)

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

SOHO Firewall Security with DoS and SPI

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

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 IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS of an 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 type 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 speed fast, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed of different types of outgoing data passing through the router to ensure P2P users don’t saturate the upload bandwidth, or office browsing doesn’t bring client web serving to a halt. Alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds of each data transmission.

Virtual Private Network (VPN) (BiPAC 8500 /8520 /8501 Only)

It allows user to establish a virtual network with a remote computer. In this way data can be transmitted securedly through the virtual tunnel formed within the network. User can use embedded PPTP and L2TP client/server, IKE and IPSec which are supported by this router to make a VPN connection or run the PPTP client in PC and the router which 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.

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 specific local computer for handling. 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. It 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 including IP address, subnet mask as well as DNS IP address and distribute them 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

Package Contents

- **SHDSL Firewall Bridge/Router (BiPAC 8500/8520) or SHDSL.bis Firewall Bridge/Router (BiPAC 8501/ 8501 *R2*/ 8521)**

- **CD-ROM containing the online manual**

- **RJ-11 SHDSL/telephone Cable (One Cable for BiPAC 8500/ 8501/ 8501 *R2*) (Two Cables for BiPAC 8520/8521)**

- **Ethernet (CAT-5 LAN) Cable**

- **Console (PS2-RS232) Cable**

- **Power Adapter**

- **Quick Start Guide**

Important note for using this router

Warning

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

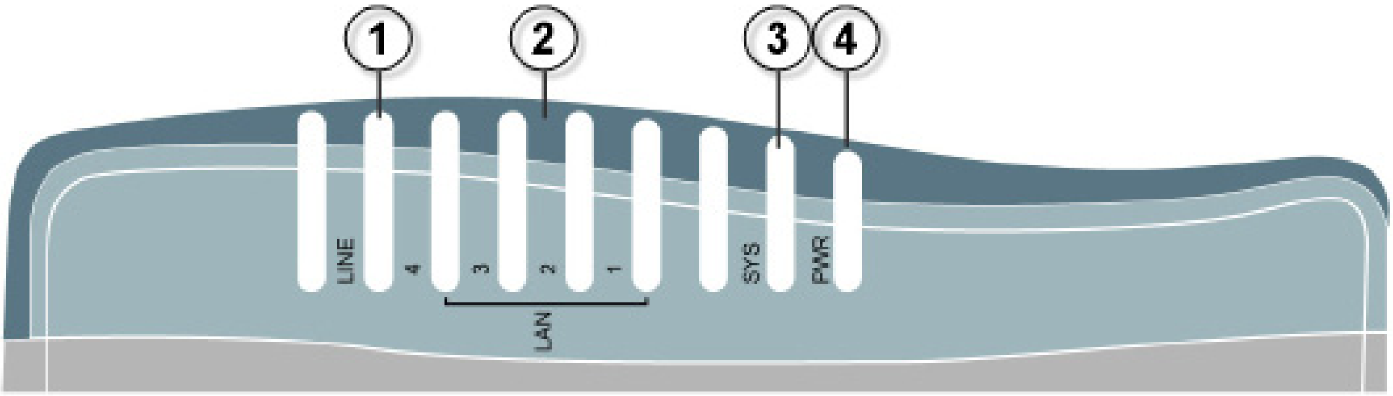
Attention

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

Device Description

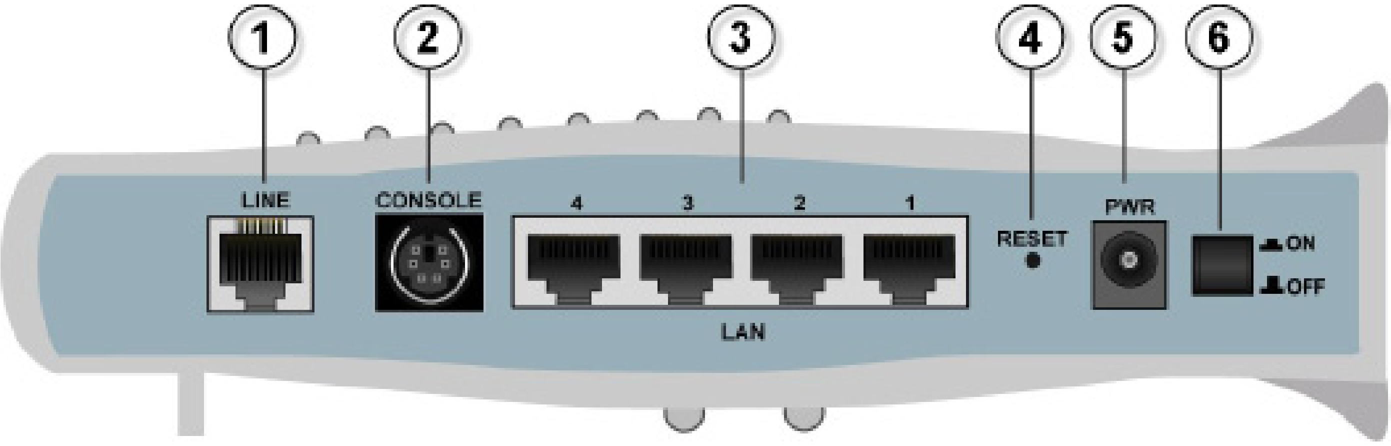
BiPAC 8500

Front Panel LED



LED		Meaning
1	**LINE**	Lit when the device is successfully connected to SHDSL line and synchronized.
2	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an Ethernet device of 100Mbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an 100Mbps of 10Mbps. Blinking when data is transmitted/received.
3	**SYS**	Lit when the system is ready.
4	**Power**	Lit when power is turned on.

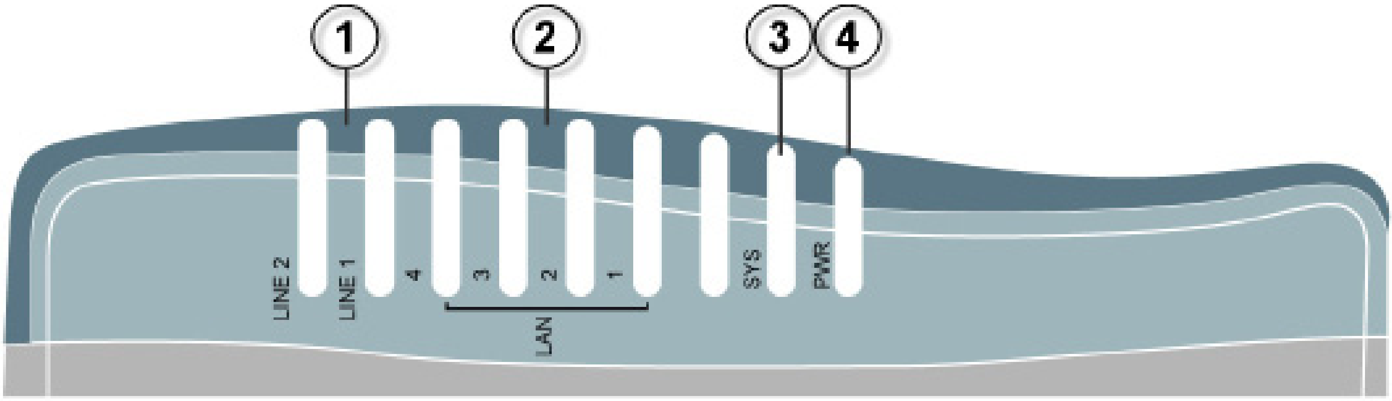
Rear Ports



Port		Meaning
1	**LINE** (RJ-11 connector)	Connect the supplied RJ-11 (“telephone”) cable to this port when connecting to the SHDSL line.
2	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC’s RS-232 port (9-pin serial port).
3	**LAN** **1X - 4X** (RJ-45 connector)	Connect an UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/ home network of 10Mbps or 100Mbps.
4	**RESET**	Press this button for 1-3 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
5	**PWR**	Connect it with the supplied power adapter.
6	**Power Switch**	Power ON/OFF switch.

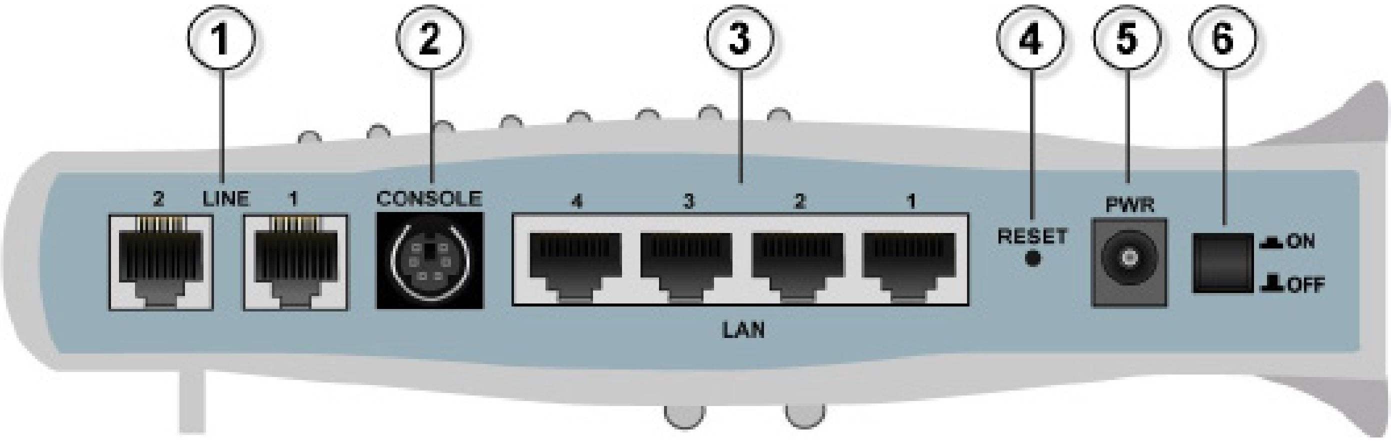
BiPAC 8520

Front Panel LED



LED		Meaning
1	**LINE 1 & 2**	Lit when the device is successfully connected to SHDSL line and synchronized.
2	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an Ethernet device of 100Mbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an 100Mbps of 10Mbps. Blinking when data is transmitted/received.
3	**SYS**	Lit when the system is ready.
4	**Power**	Lit when power is turned on.

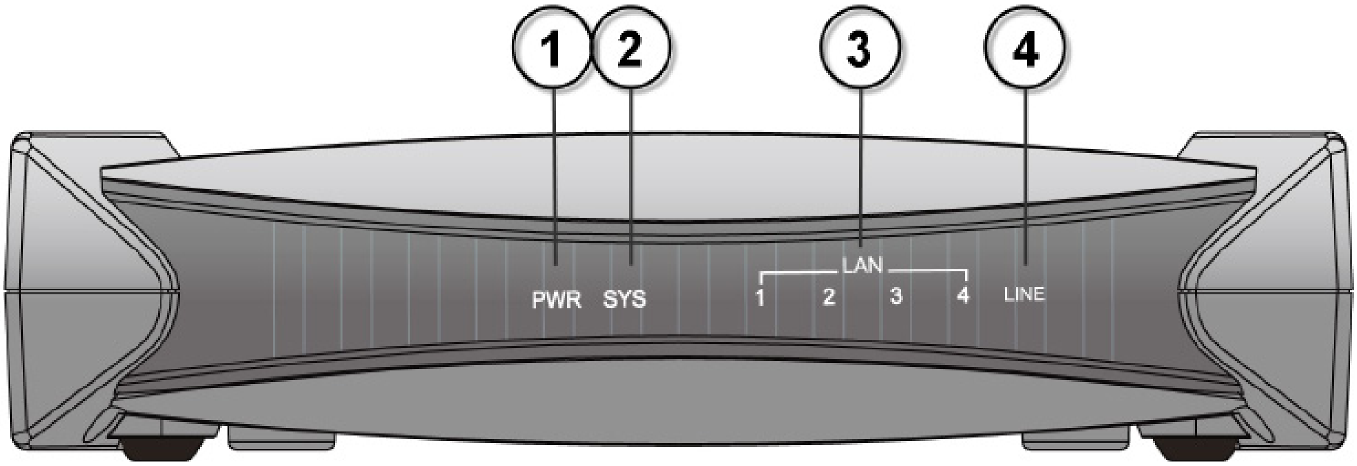
Rear Ports



Port		Meaning
1	**LINE** **1X - 2X** (RJ-11 connector)	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the SHDSL line.
2	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
3	**LAN** **1X - 4X** (RJ-45 connector)	Connect an UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/ home network of 10Mbps or 100Mbps.
4	**RESET**	Press this button for 1-3 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
5	**PWR**	Connect it with the supplied power adapter.
6	**Power Switch**	Power ON/OFF switch.

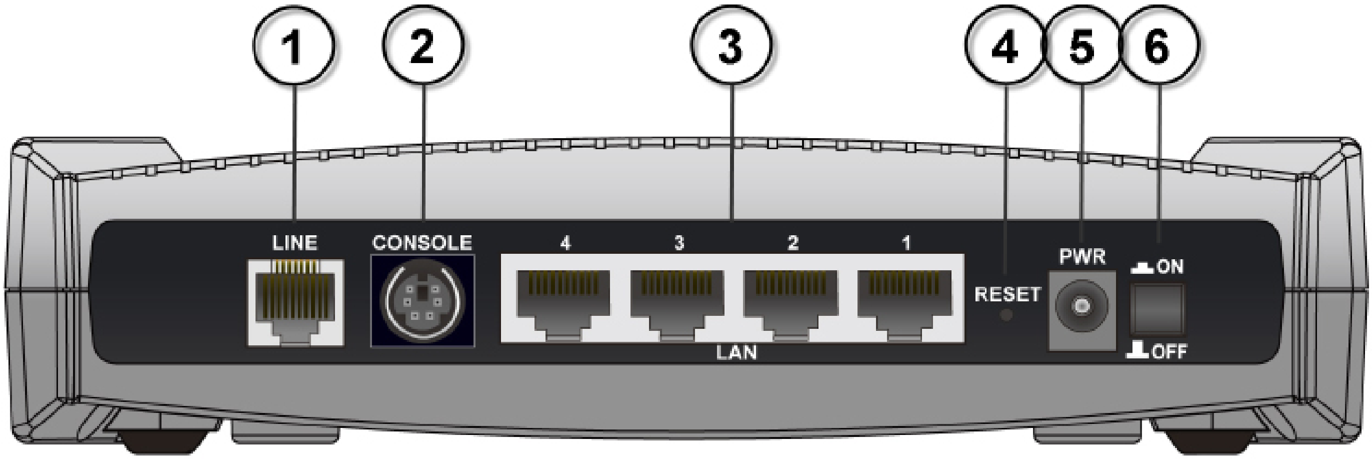
BiPAC 8501

Front Panel LED



LED		Meaning
1	**LINE**	Lit when the device is successfully connected to SHDSL line and synchronized.
2	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an Ethernet device of 100Mbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an 100Mbps of 10Mbps. Blinking when data is transmitted/received.
3	**SYS**	Lit when the system is ready.
4	**Power**	Lit when power is turned on.

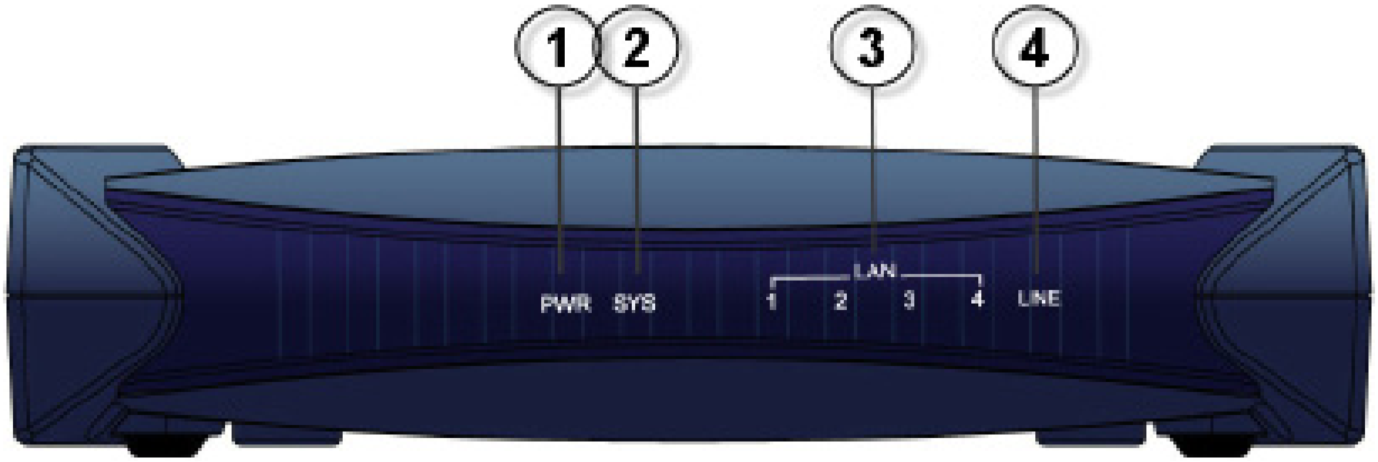
Rear Ports



Port		Meaning
1	**LINE** **1X - 2X** (RJ-11 connector)	Connect the supplied RJ-11 (“telephone”) cable to this port when connecting to the SHDSL line.
2	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC’s RS-232 port (9-pin serial port).
3	**LAN** **1X - 4X** (RJ-45 connector)	Connect an UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/ home network of 10Mbps or 100Mbps.
4	**RESET**	Press this button for 1-3 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
5	**PWR**	Connect it with the supplied power adapter.
6	**Power Switch**	Power ON/OFF switch.

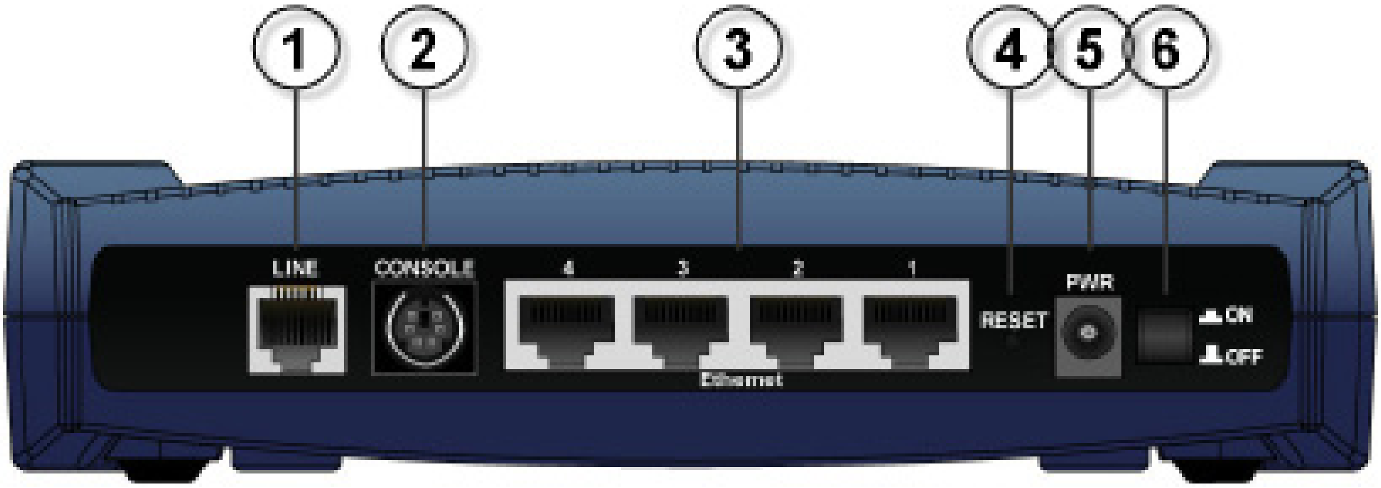
BiPAC 8501 *R2*

Front Panel LED



LED		Meaning
1	**LINE**	Lit when the device is successfully connected to SHDSL line and synchronized.
2	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an Ethernet device of 100Mbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an 100Mbps of 10Mbps. Blinking when data is transmitted/received.
3	**SYS**	Lit when the system is ready.
4	**Power**	Lit when power is turned on.

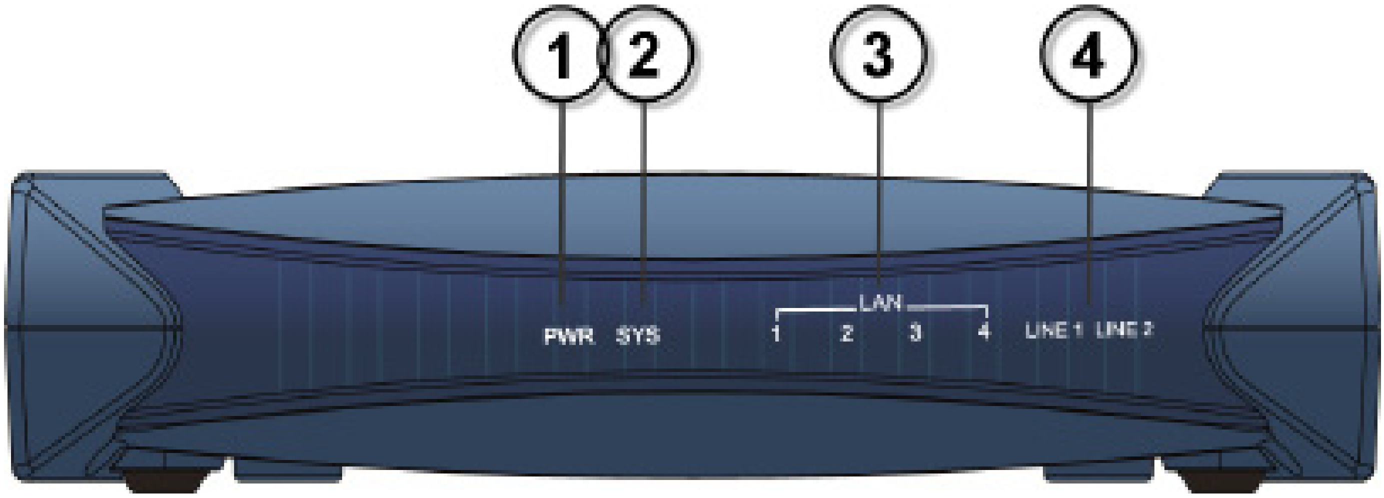
Rear Ports



Port		Meaning
1	**LINE** **1X - 2X** (RJ-11 connector)	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the SHDSL line.
2	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
3	**LAN** **1X - 4X** (RJ-45 connector)	Connect an UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/ home network of 10Mbps or 100Mbps.
4	**RESET**	Press this button for 1-3 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
5	**PWR**	Connect it with the supplied power adapter.
6	**Power Switch**	Power ON/OFF switch.

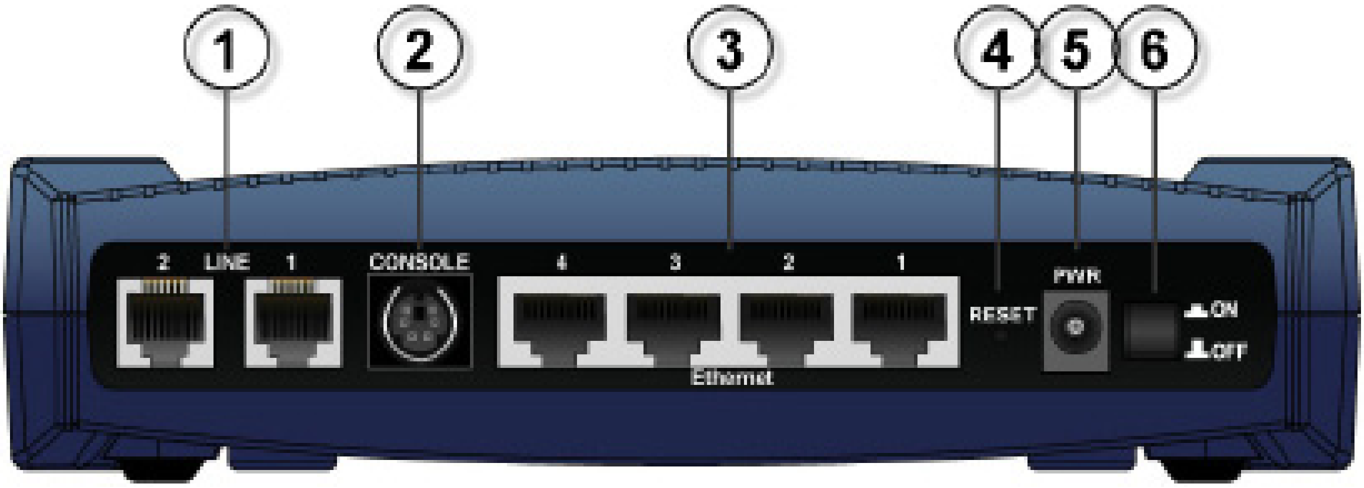
BiPAC 8521

Front Panel LED



LED		Meaning
1	**LINE**	Lit when the device is successfully connected to SHDSL line and synchronized.
2	**LAN Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an Ethernet device of 100Mbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an 100Mbps of 10Mbps. Blinking when data is transmitted/received.
3	**SYS**	Lit when the system is ready.
4	**Power**	Lit when power is turned on.

Rear Ports



Port		Meaning
1	**LINE** **1X - 2X** (RJ-11 connector)	Connect the supplied RJ-11 ("telephone") cable to this port when connecting to the SHDSL line.
2	**CONSOLE**	Connect a PS2/RS-232 cable to this port when connecting to a PC's RS-232 port (9-pin serial port).
3	**LAN** **1X - 4X** (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
4	**RESET**	Press this button for 1-3 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
5	**PWR**	Connect it with the supplied power adapter.
6	**Power Switch**	Power ON/OFF switch.

Chapter 3: Basic Network Installation

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

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

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

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

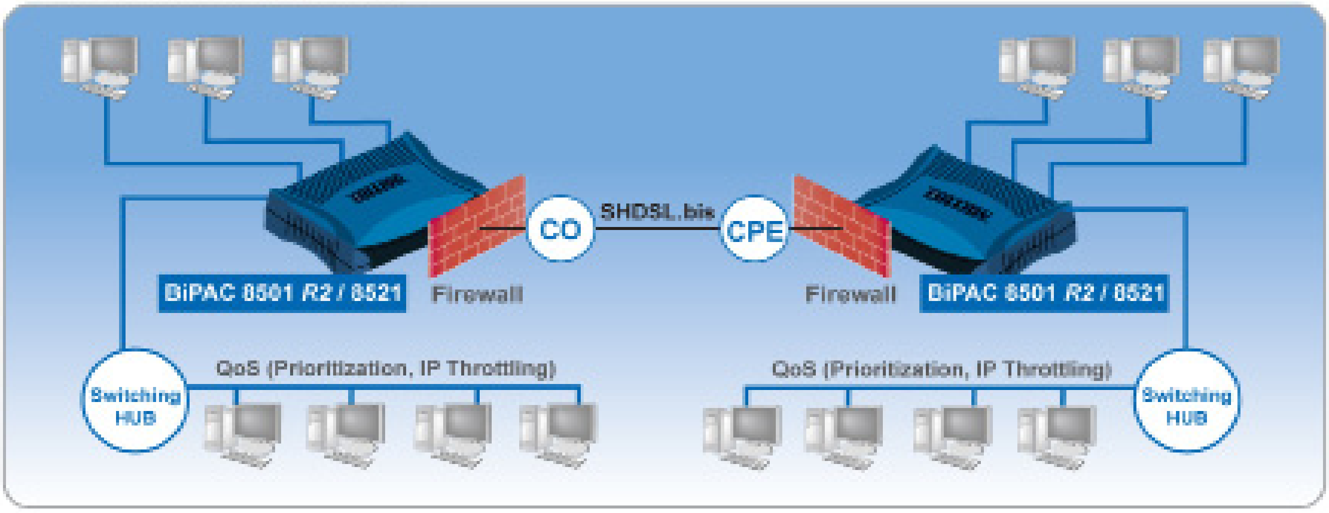
NOTE:

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

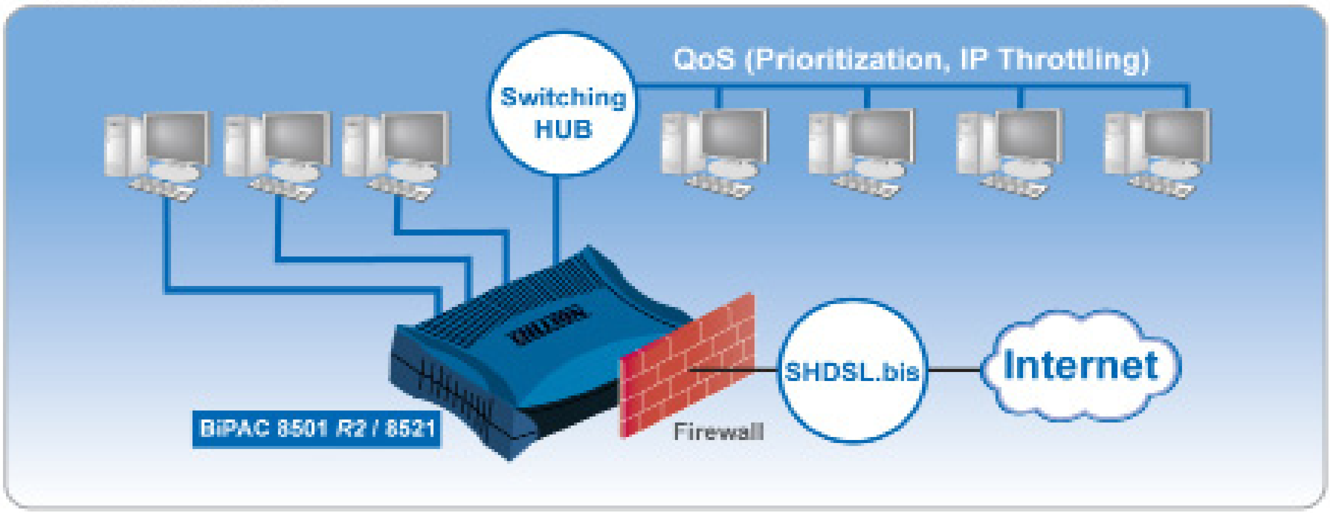
Applications of the device

1. Connect the Router to a LAN (Local Area Network) and the SHDSL LINE.
2. Power on the device.
3. Make sure the PWR and SYS LEDs are lit steadily and that the relevant LAN LED are lit.

Back-to-back Application



Internet Access

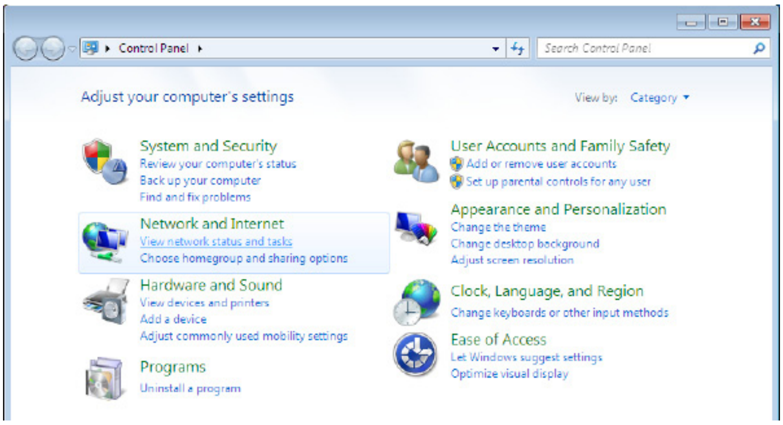


Network Configuration

Configuring PC in Windows 7

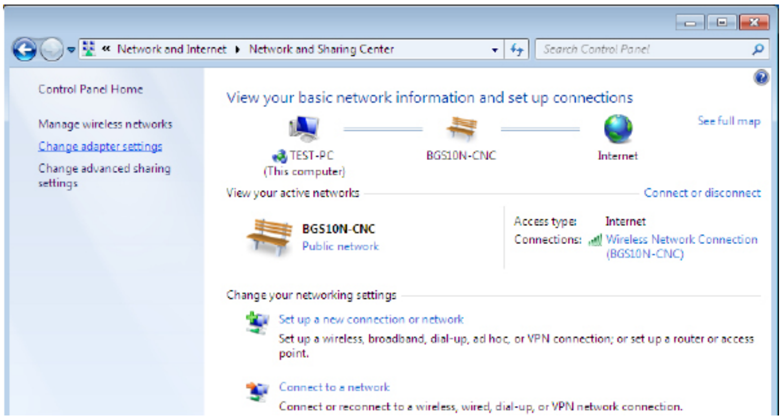
1. Go to Start. Click on Control Panel.
1. Then click on Network and Internet.

1.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

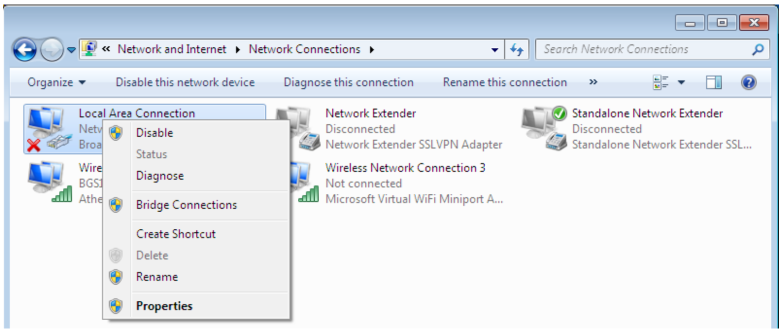
1. When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

1.


Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

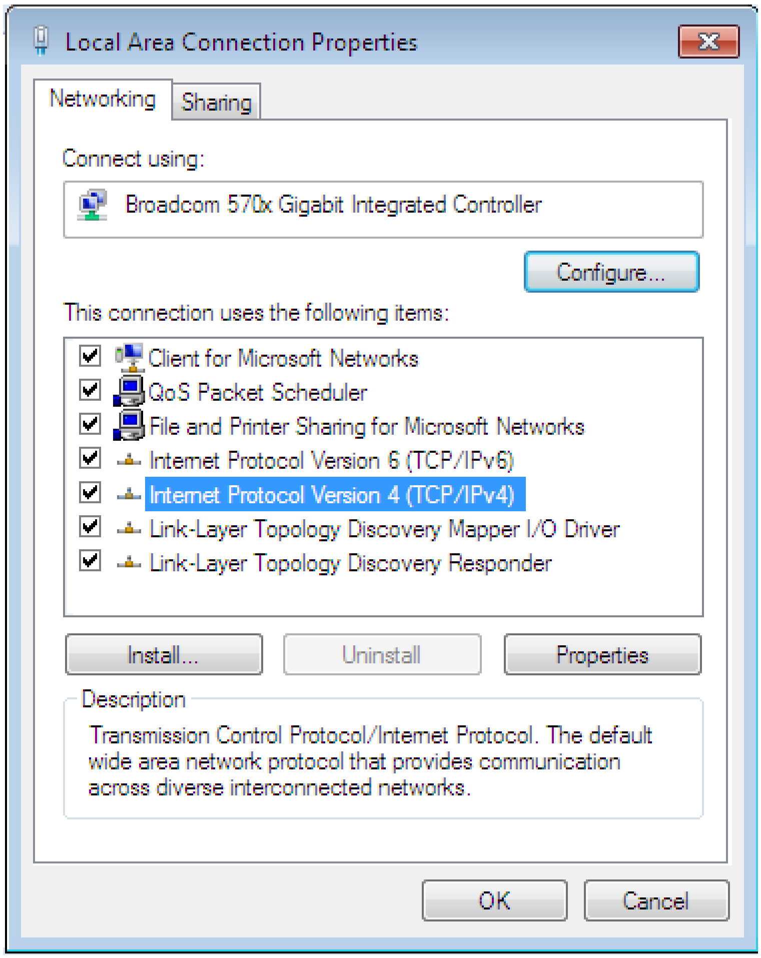
1. Select the Local Area Connection, and right click the icon to select Properties.

1.


Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Local Area Connection
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Network Extender
Disconnected
Network Extender SSLVPN Adapter
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...
Standalone Network Extender
Disconnected
Standalone Network Extender SSL...

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

1.



Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

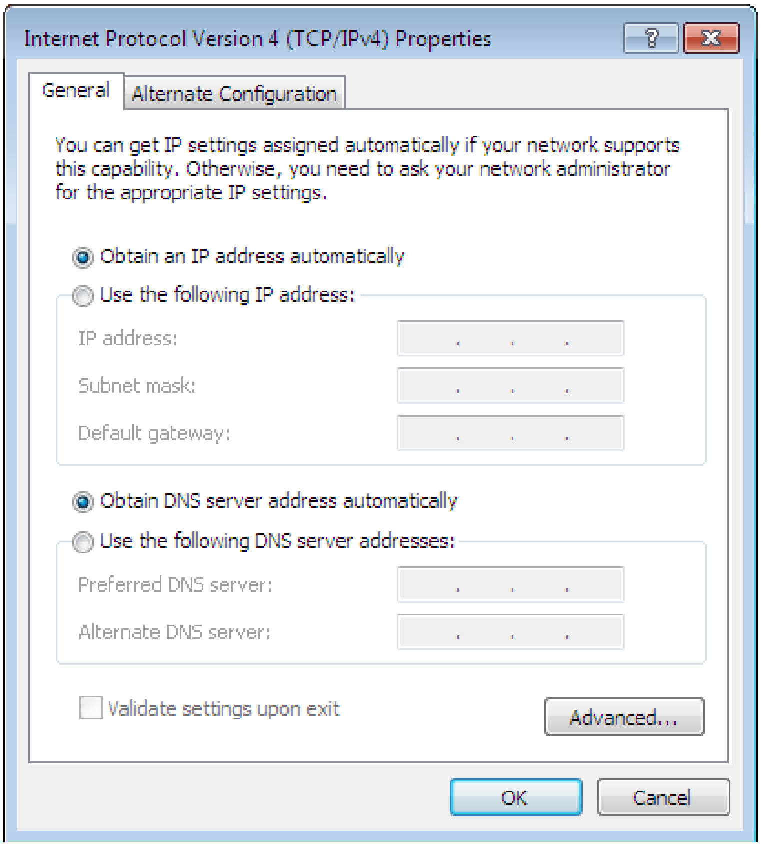
Description

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

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

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

1.



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

- ● Obtain an IP address automatically
- ○ Use the following IP address:
  - IP address: . . .
  - Subnet mask: . . .
  - Default gateway: . . .
- ● Obtain DNS server address automatically
- ○ Use the following DNS server addresses:
  - Preferred DNS server: . . .
  - Alternate DNS server: . . .

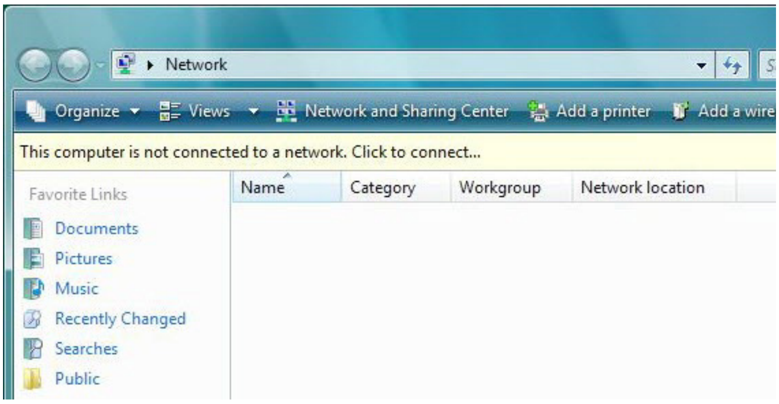
☐ Validate settings upon exit

Configuring PC in Windows Vista

1. Go to Start. Click on Network.

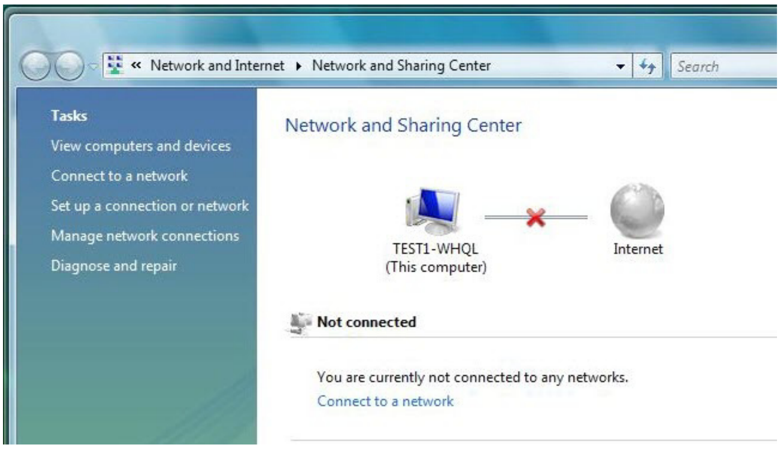
1. Then click on Network and Sharing Center at the top bar.

1.


This computer is not connected to a network. Click to connect...

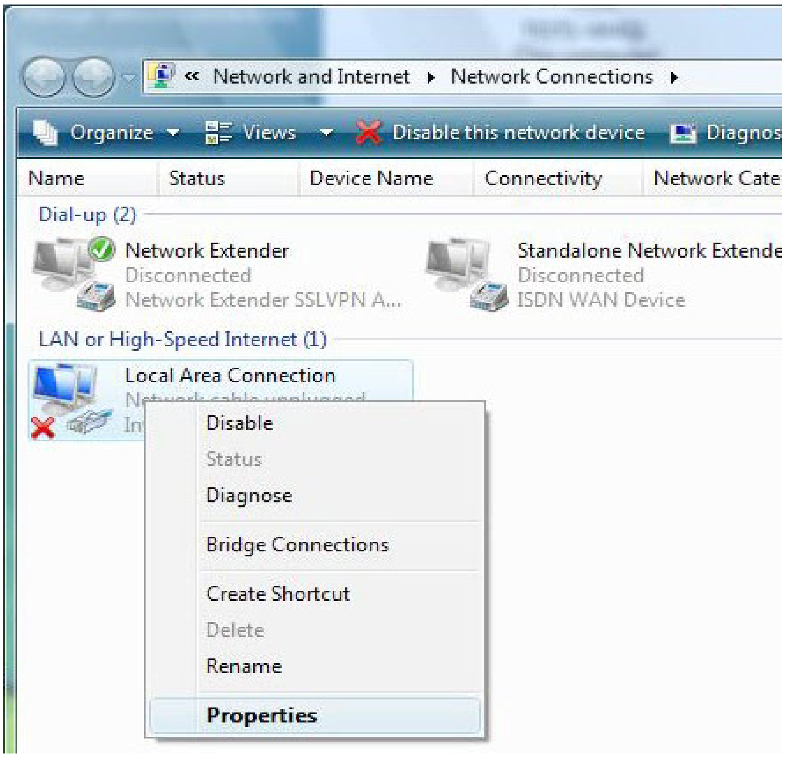
1. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.

1.


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

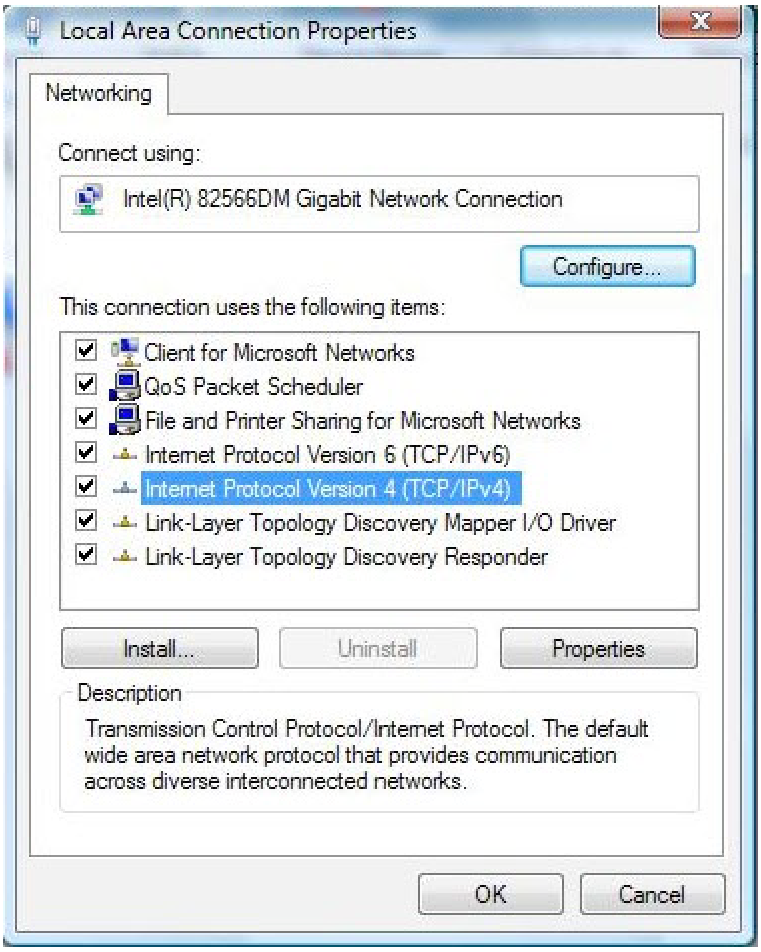
1. Select the Local Area Connection, and right click the icon to select Properties.

1.



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

1.


Local Area Connection Properties

Networking

Connect using:

Intel(R) 82566DM Gigabit Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

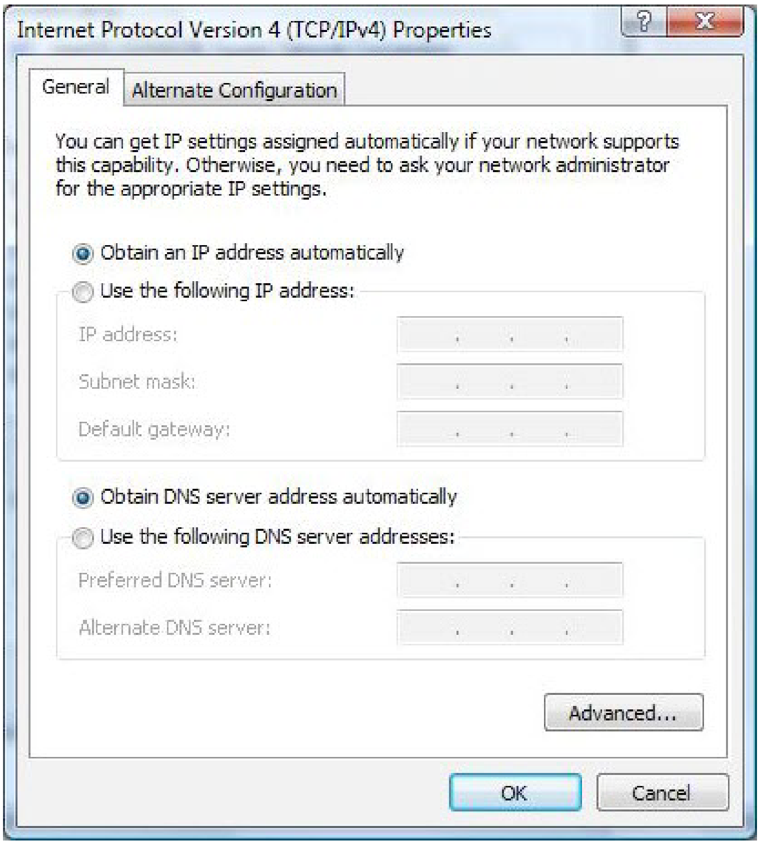
Description

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

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

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

1.


Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

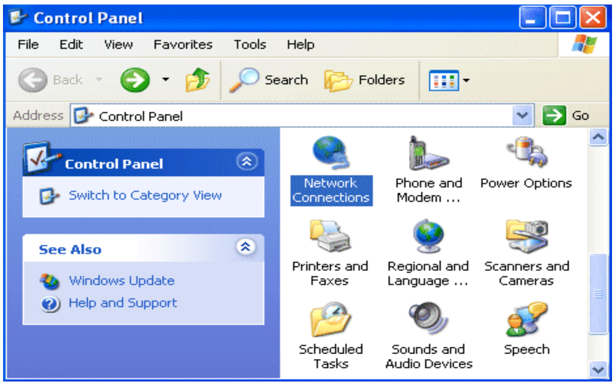
Preferred DNS server: . . .

Alternate DNS server: . . .

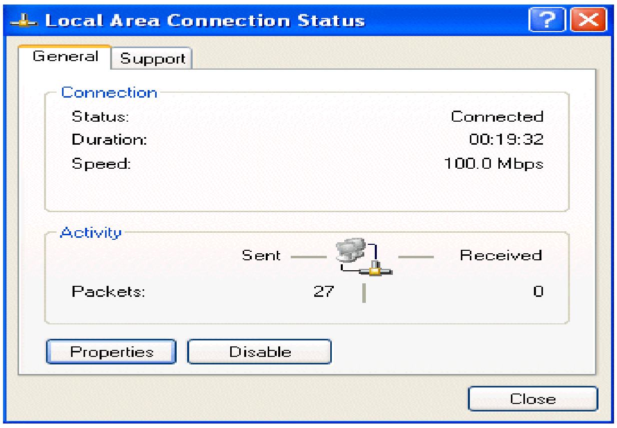
Configuring PC in Windows XP

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

1. Double-click Local Area Connection.



1. In the Local Area Connection Status window, click Properties.



Connection

Status: Connected

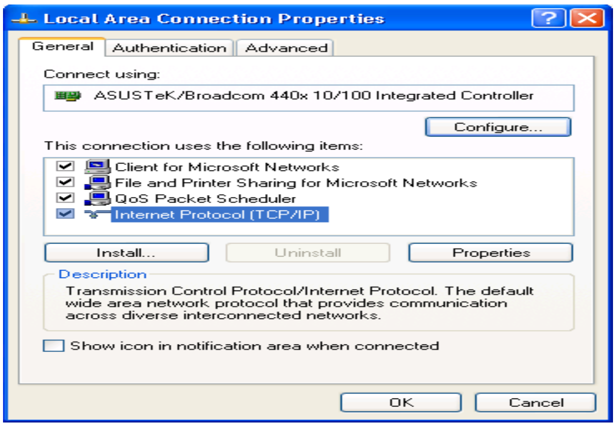
Duration: 00:19:32

Speed: 100.0 Mbps

Activity

	Sent	Received
Packets:	27	0

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



Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

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

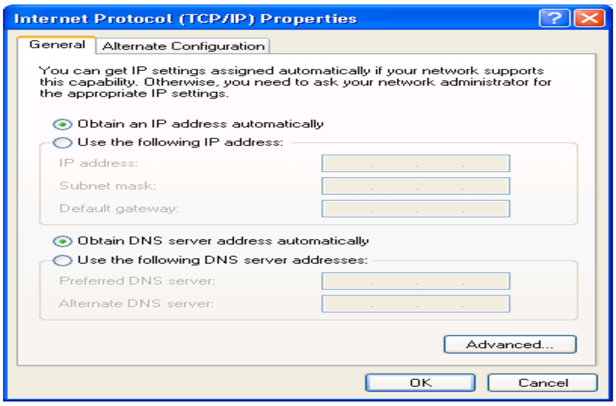
Description

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

☐ Show icon in notification area when connected

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

1. Click OK to finish the configuration.



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

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

IP address:
Subnet mask:
Default gateway:

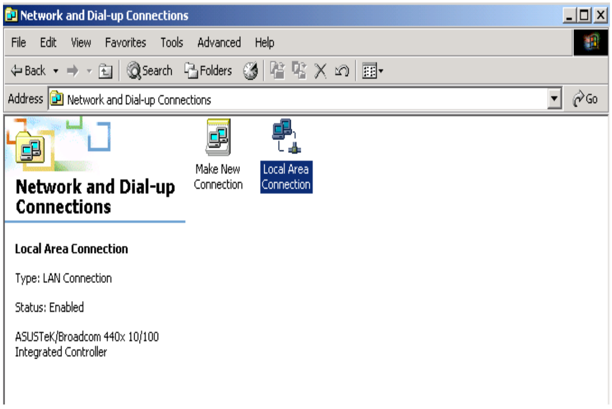
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

Configuring PC in Windows 2000

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

1. Double-click Local Area Connection.


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

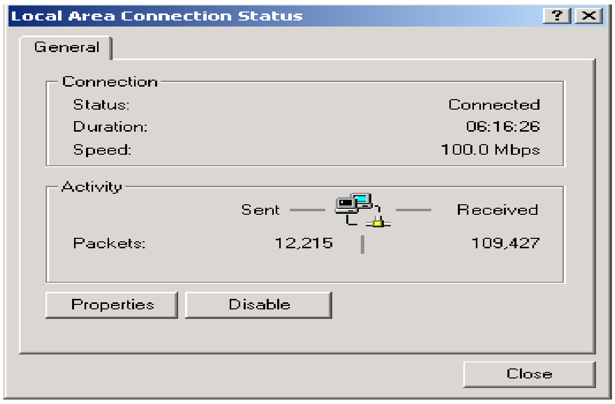
Local Area Connection

Type: LAN Connection

Status: Enabled

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

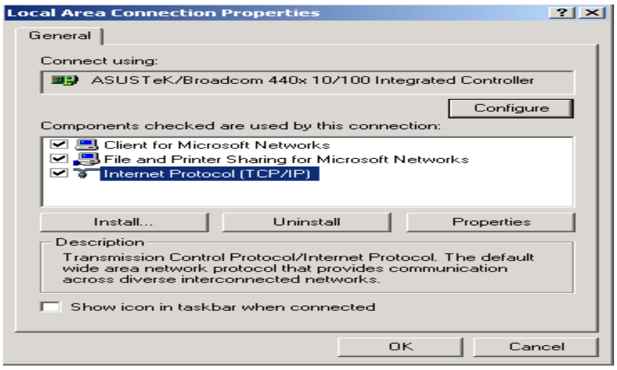
1. In the Local Area Connection Status window click Properties.



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

	Sent	Received
Packets:	12,215	109,427

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



Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller

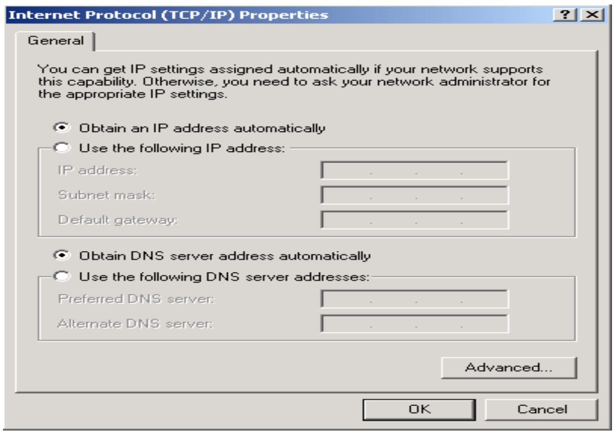
Components checked are used by this connection:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

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

☐ Show icon in taskbar when connected

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

1. Click OK to finish the configuration.



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

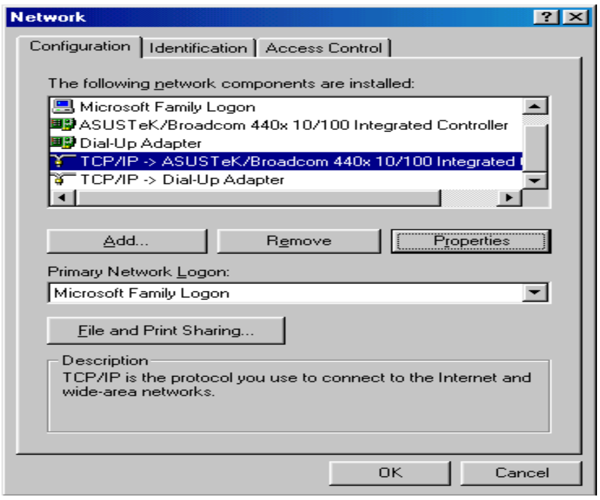
● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

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

Configuring PC in Windows 95/98/Me

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.

1. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



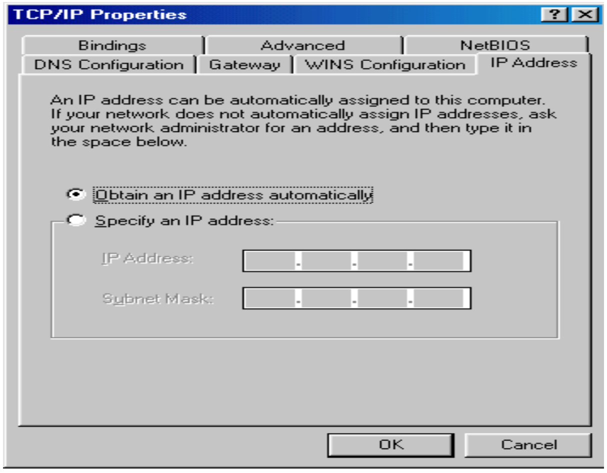
The following network components are installed:

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

Primary Network Logon: Microsoft Family Logon

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

1. Select the Obtain an IP address automatically radio button.

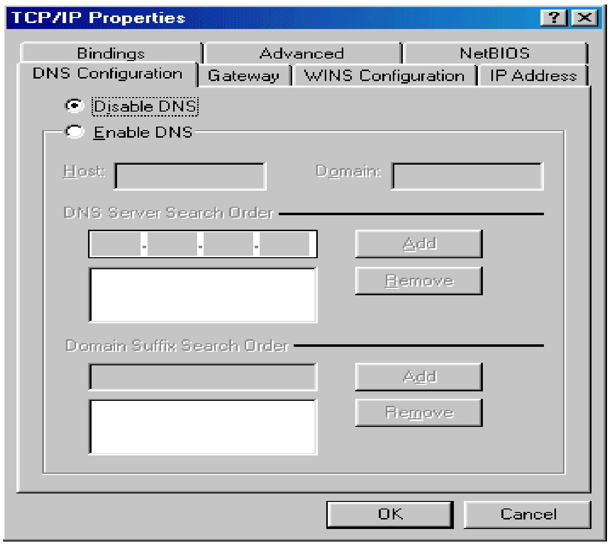


An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically
○ Specify an IP address:

1. Then select the DNS Configuration tab.

1. Select the Disable DNS radio button and click OK to finish the configuration.

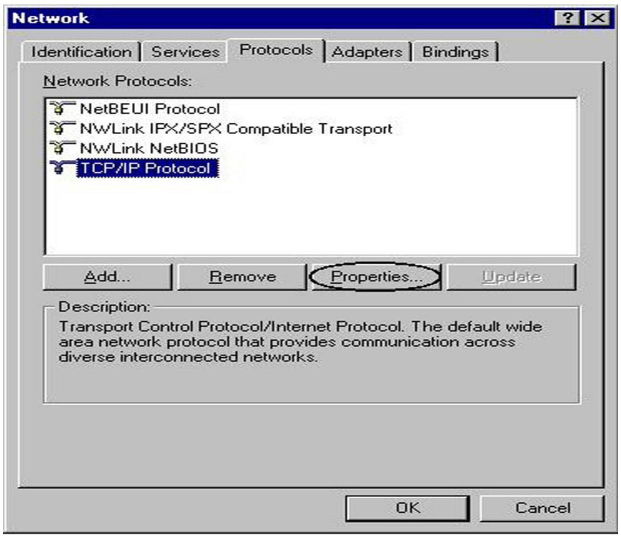


● Disable DNS
○ Enable DNS

Configuring PC in Windows NT4.0

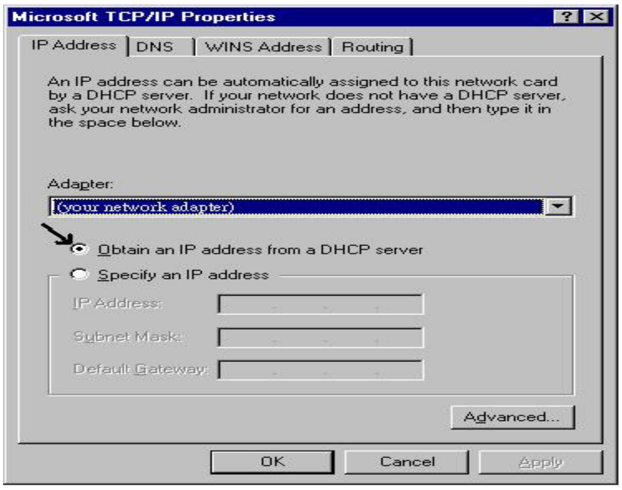
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.

1. Select TCP/IP Protocol and click Properties.



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

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



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

Adapter: (your network adapter)

● Obtain an IP address from a DHCP server

○ Specify an IP address

Factory Default Settings

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

Web Interface (Username and Password)

- Username: admin
- Password: admin

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

Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

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

LAN and WAN Port Addresses

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

LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP. However, you have to set the username and password first.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Information from your ISP

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

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

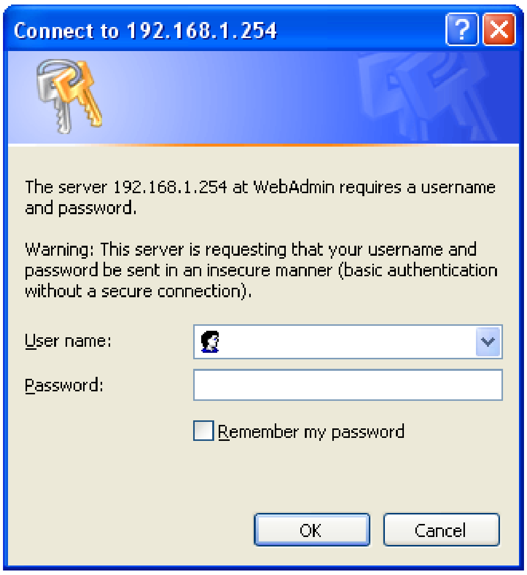
PPPoE	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
PPPoE / PPPoE with Pass-through	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name,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

Easy Internet Access Configuration

To easily configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There is basically one way to configure your router before you are able to connect to the internet: **Web Interface**. Configuration of this method will be discussed in detail in the following section.

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.



The server 192.168.1.254 at WebAdmin requires a username and password.

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

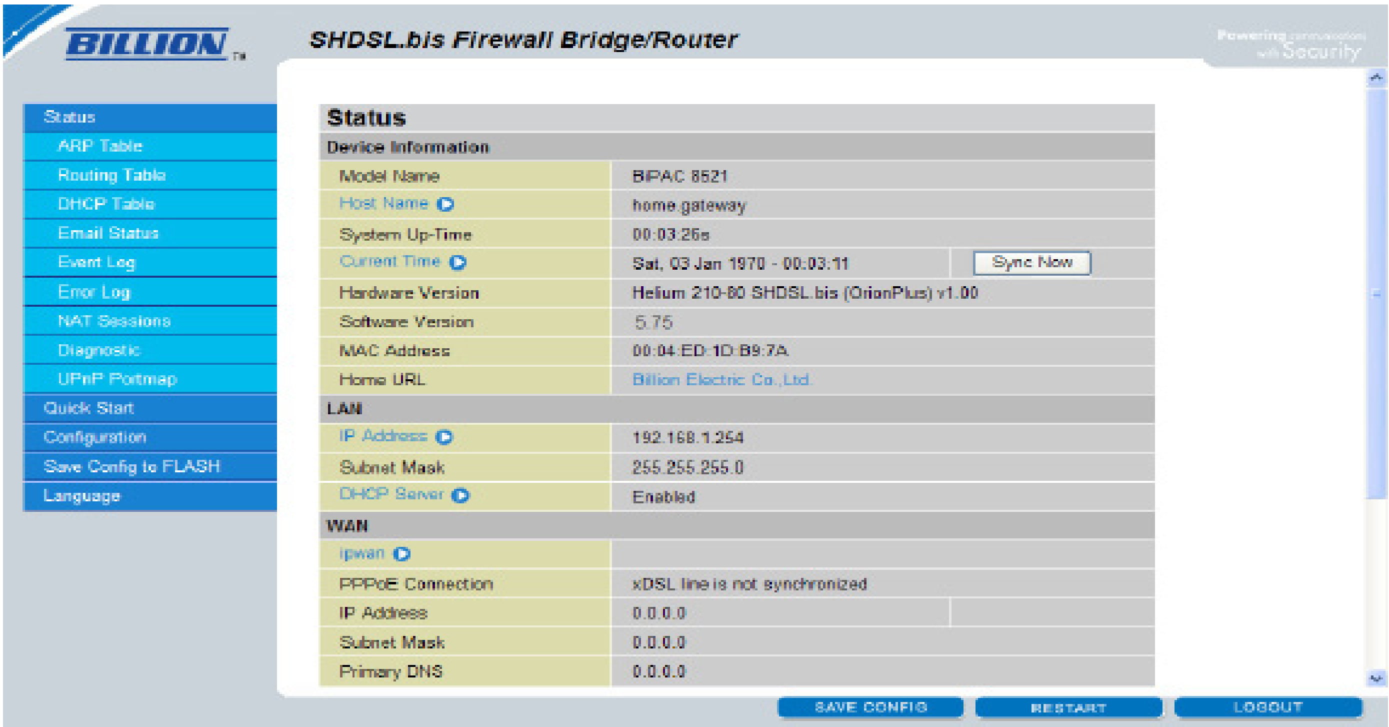
User name:

Password:

☐ Remember my password

Congratulations! You are now successfully logon to the Gateway Router!

If the authentication succeeds, the homepage Status will appear on the screen.



Status

Device Information	
Model Name	BiPAC 8521
Host Name	home.gateway
System Up-Time	00:03:26s
Current Time	Sat, 03 Jan 1970 - 00:03:11
Hardware Version	Helium 210-80 SHDSL.bis (OrionPlus) v1.00
Software Version	5.75
MAC Address	00:04:ED:1D:B9:7A
Home URL	Billion Electric Co.,Ltd.
LAN	
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server	Enabled
WAN	
ipwan	
PPPoE Connection	xDSL line is not synchronized
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Primary DNS	0.0.0.0

Chapter 4: Configuration

Once you have logged on to your router GUI via your web browser, you can begin to configure the router according to your needs. On the configuration homepage, the left navigation pane provides the links to different setup pages.

Status:

- **ARP Table**
- **Routing Table**
- **DHCP Table**
- **PPTP Status (BiPAC 8500 /8520 Only)**
- **IPSec Status (BiPAC 8500 /8520 Only)**
- **L2TP Status (BiPAC 8500 /8520 Only)**
- **Email Status**
- **Event Log**
- **Error Log**
- **NAT Sessions**
- **Diagnostic**
- **UPnP Portmap**

Quick Start

Configuration:

- **LAN**
- **WAN**
- **System**
- **Firewall**
- **VPN (BiPAC 8500/ 8520/ 8501 Only)**
- **QoS**
- **Virtual Server**
- **Time Schedule**
- **Advanced**

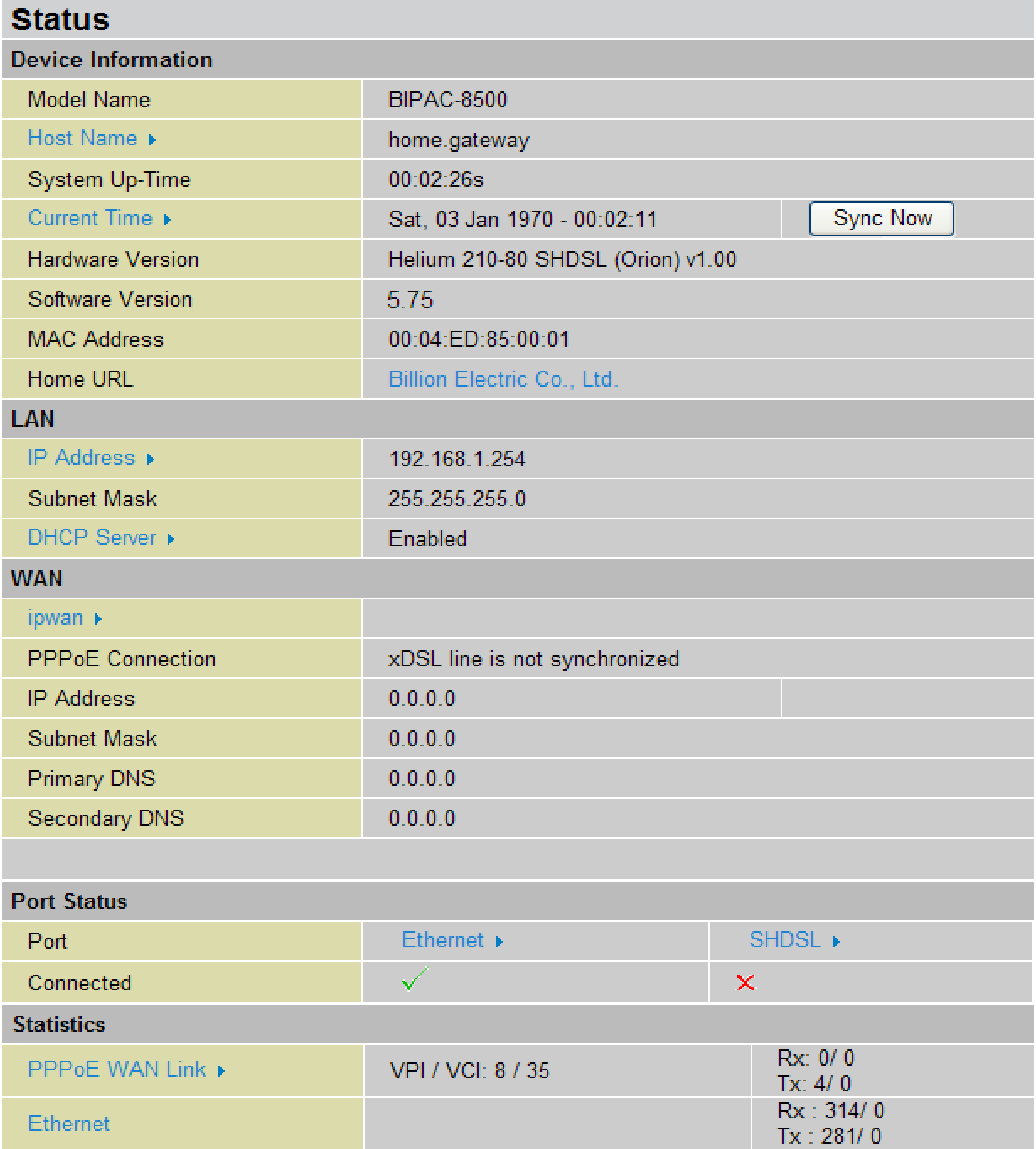
Save Config to FLASH

Language

Each of these setup pages will be discussed in detail in sections that follow ahead.

Status

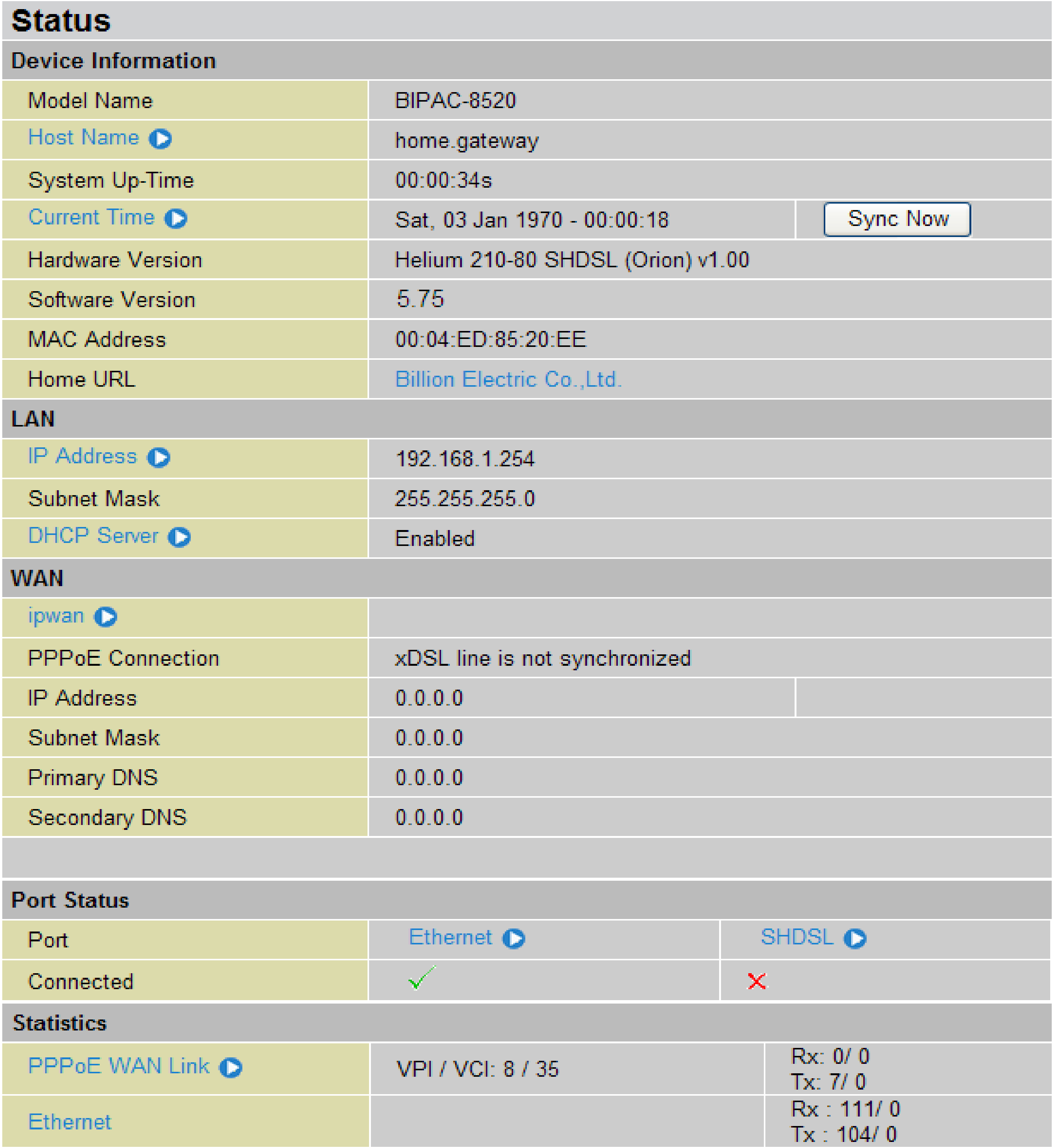
8500



Status

Device Information		
Model Name	BIPAC-8500	
Host Name ▸	home.gateway	
System Up-Time	00:02:26s	
Current Time ▸	Sat, 03 Jan 1970 - 00:02:11	Sync Now
Hardware Version	Helium 210-80 SHDSL (Orion) v1.00	
Software Version	5.75	
MAC Address	00:04:ED:85:00:01	
Home URL	Billion Electric Co., Ltd.	
LAN		
IP Address ▸	192.168.1.254	
Subnet Mask	255.255.255.0	
DHCP Server ▸	Enabled	
WAN		
ipwan ▸		
PPPoE Connection	xDSL line is not synchronized	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0	
Port Status		
Port	Ethernet ▸	SHDSL ▸
Connected	✓	✗
Statistics		
PPPoE WAN Link ▸	VPI / VCI: 8 / 35	Rx: 0/ 0 Tx: 4/ 0
Ethernet		Rx : 314/ 0 Tx : 281/ 0

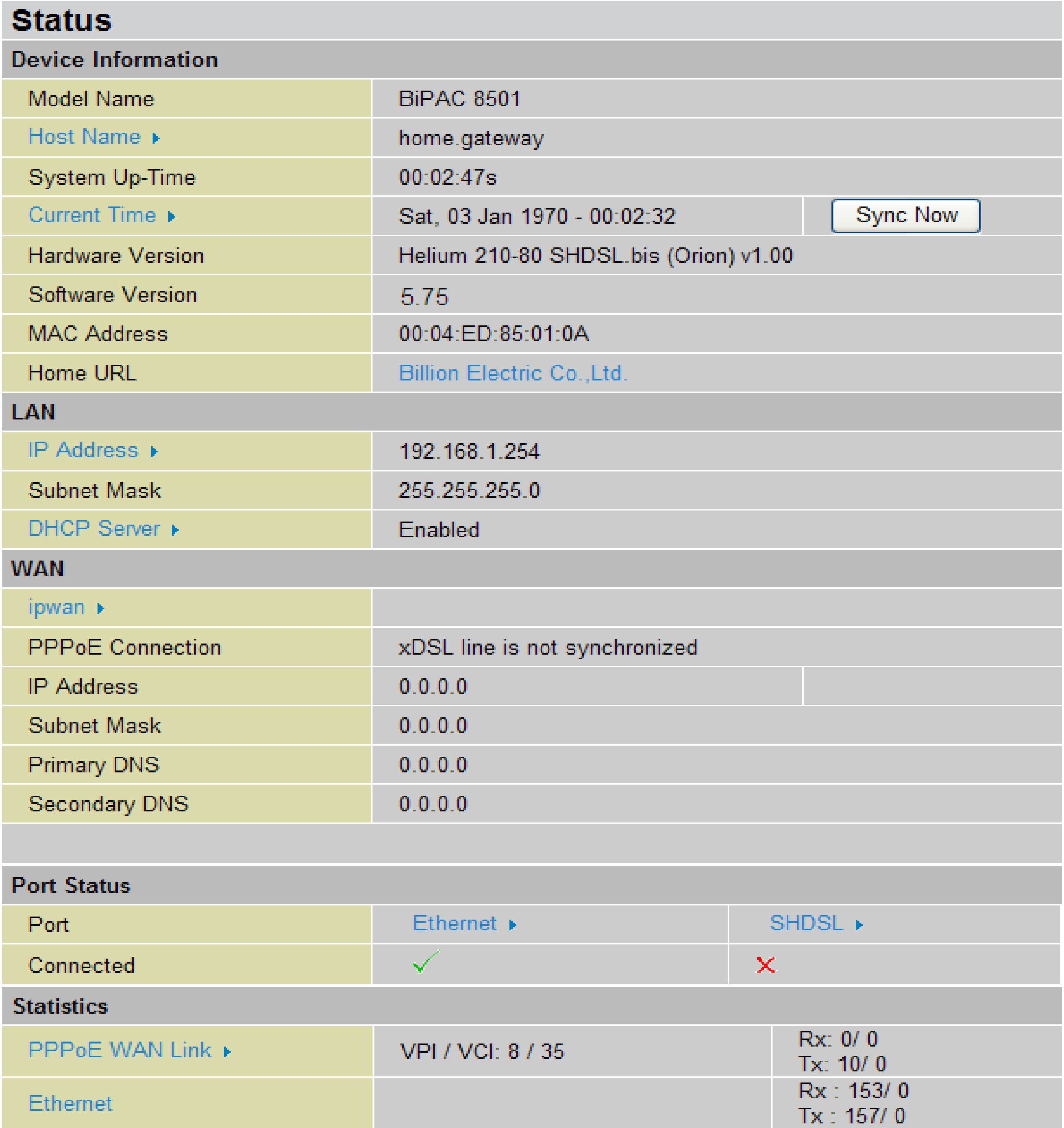
8520



Status

Device Information		
Model Name	BIPAC-8520	
Host Name	home.gateway	
System Up-Time	00:00:34s	
Current Time	Sat, 03 Jan 1970 - 00:00:18	Sync Now
Hardware Version	Helium 210-80 SHDSL (Orion) v1.00	
Software Version	5.75	
MAC Address	00:04:ED:85:20:EE	
Home URL	Billion Electric Co.,Ltd.	
LAN		
IP Address	192.168.1.254	
Subnet Mask	255.255.255.0	
DHCP Server	Enabled	
WAN		
ipwan		
PPPoE Connection	xDSL line is not synchronized	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0	
Port Status		
Port	Ethernet	SHDSL
Connected	✓	✗
Statistics		
PPPoE WAN Link	VPI / VCI: 8 / 35	Rx: 0/ 0 Tx: 7/ 0
Ethernet		Rx : 111/ 0 Tx : 104/ 0

8501



Status

Device Information

Model Name	BiPAC 8501
Host Name ▸	home.gateway
System Up-Time	00:02:47s
Current Time ▸	Sat, 03 Jan 1970 - 00:02:32
Hardware Version	Helium 210-80 SHDSL.bis (Orion) v1.00
Software Version	5.75
MAC Address	00:04:ED:85:01:0A
Home URL	Billion Electric Co.,Ltd.

LAN

IP Address ▸	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server ▸	Enabled

WAN

ipwan ▸	
PPPoE Connection	xDSL line is not synchronized
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

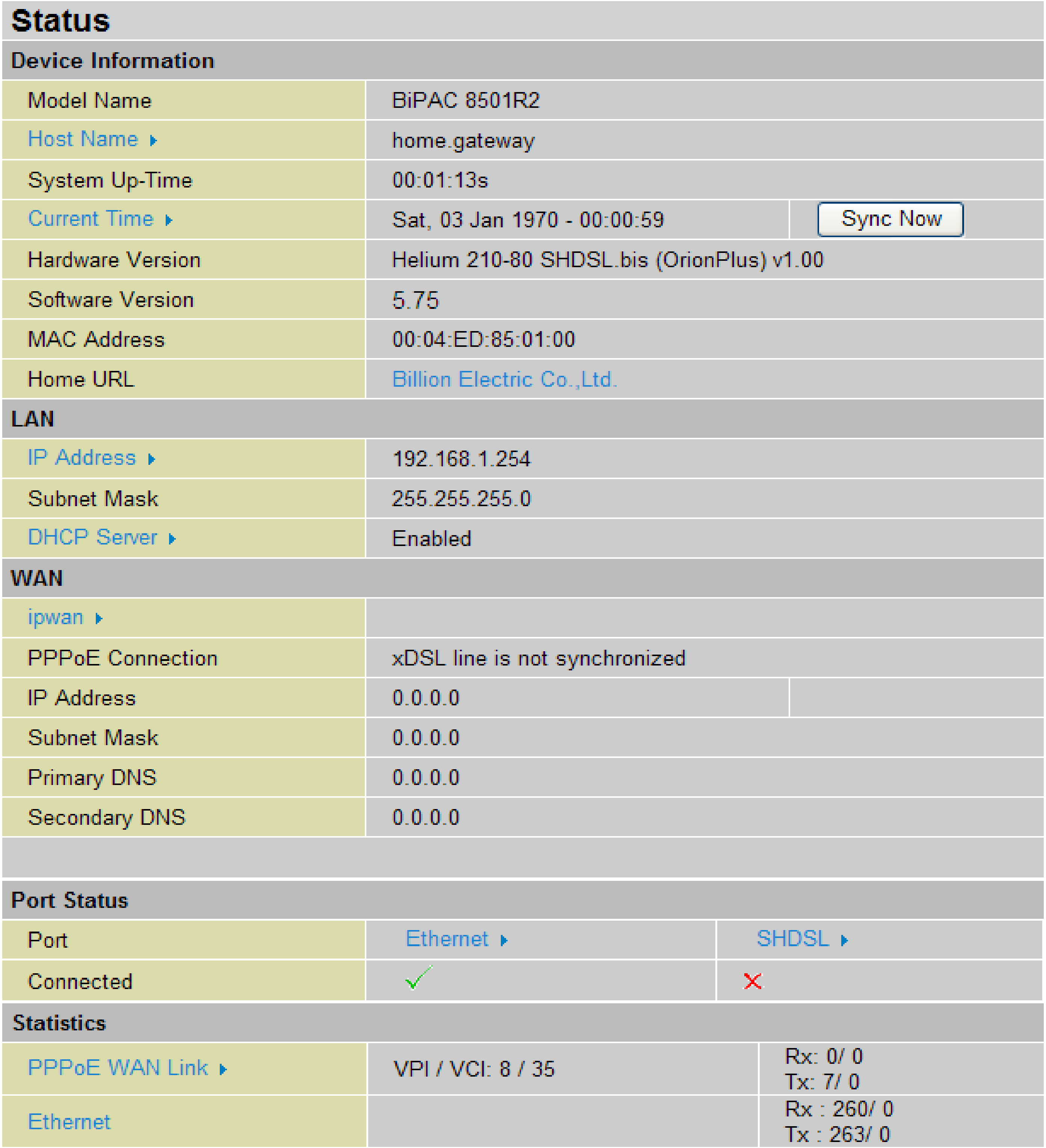
Port Status

Port	Ethernet ▸	SHDSL ▸
Connected	✓	✗

Statistics

PPPoE WAN Link ▸	VPI / VCI: 8 / 35	Rx: 0/ 0 Tx: 10/ 0
Ethernet		Rx : 153/ 0 Tx : 157/ 0

8501 R2



Status

Device Information

Model Name	BiPAC 8501R2	
Host Name ▸	home.gateway	
System Up-Time	00:01:13s	
Current Time ▸	Sat, 03 Jan 1970 - 00:00:59	
Hardware Version	Helium 210-80 SHDSL.bis (OrionPlus) v1.00	
Software Version	5.75	
MAC Address	00:04:ED:85:01:00	
Home URL	Billion Electric Co.,Ltd.	

LAN

IP Address ▸	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server ▸	Enabled

WAN

ipwan ▸	
PPPoE Connection	xDSL line is not synchronized
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

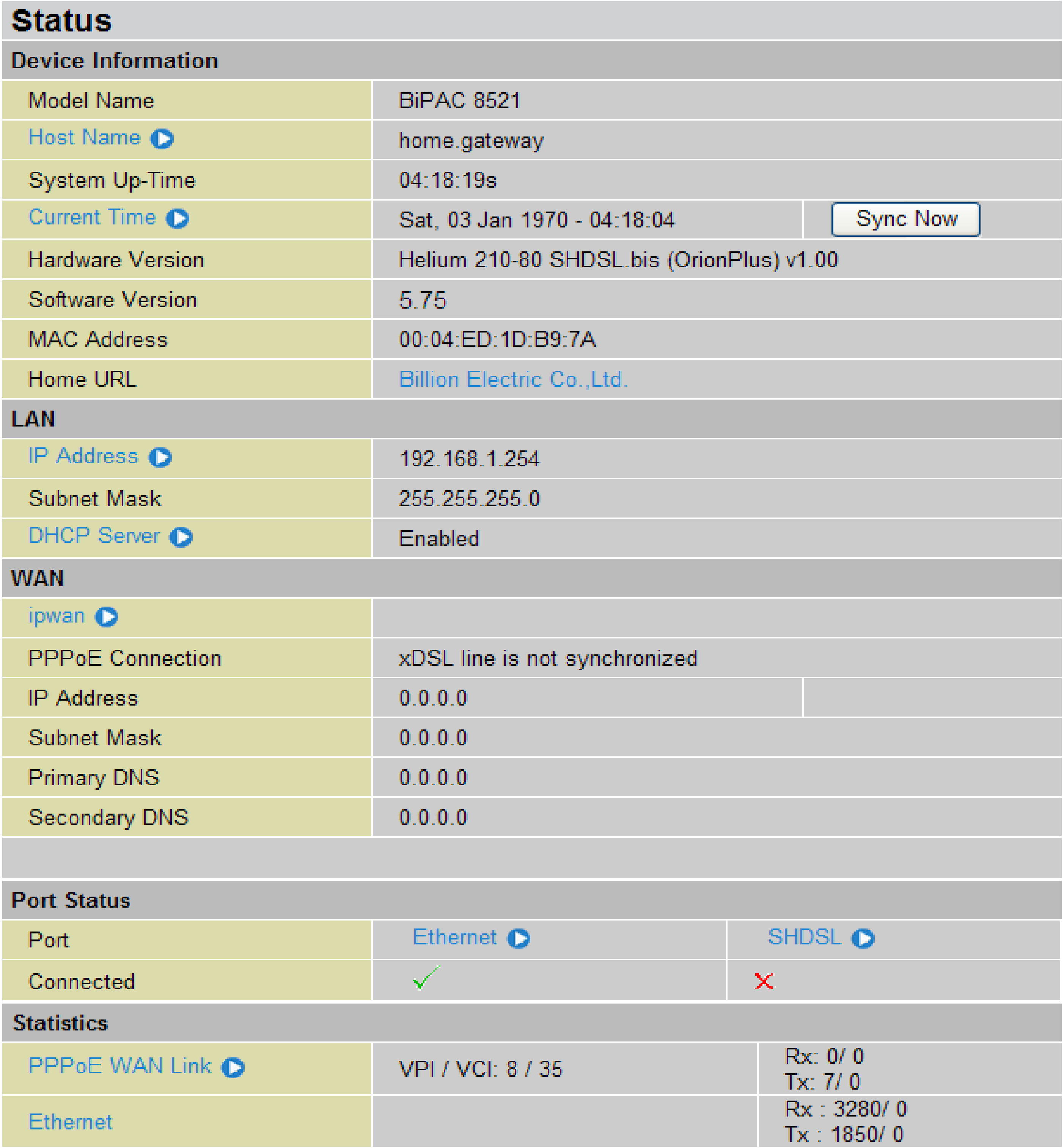
Port Status

Port	Ethernet ▸	SHDSL ▸
Connected	✓	✗

Statistics

PPPoE WAN Link ▸	VPI / VCI: 8 / 35	Rx: 0/ 0 Tx: 7/ 0
Ethernet		Rx : 260/ 0 Tx : 263/ 0

8521



Status

Device Information

Model Name	BiPAC 8521	
Host Name ▶	home.gateway	
System Up-Time	04:18:19s	
Current Time ▶	Sat, 03 Jan 1970 - 04:18:04	Sync Now
Hardware Version	Helium 210-80 SHDSL.bis (OrionPlus) v1.00	
Software Version	5.75	
MAC Address	00:04:ED:1D:B9:7A	
Home URL	Billion Electric Co.,Ltd.	

LAN

IP Address ▶	192.168.1.254
Subnet Mask	255.255.255.0
DHCP Server ▶	Enabled

WAN

ipwan ▶	
PPPoE Connection	xDSL line is not synchronized
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Port Status

Port	Ethernet ▶	SHDSL ▶
Connected	✓	✗

Statistics

PPPoE WAN Link ▶	VPI / VCI: 8 / 35	Rx: 0/ 0 Tx: 7/ 0
Ethernet		Rx : 3280/ 0 Tx : 1850/ 0

Device Information

Model Name: Displays the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name.

System Up-Time: Records system up-time enabling a user to determine how long has the system being online or the time that an unexpected restart or fault occured.The system up-time is restarted when there is a power failure or upon software or hardware reset.

Current Time: Set the current time. See the **Time Zone** section for more information.

Software Version: The version number of firmware on the flash.

MAC Address: The LAN MAC address.

Home URL: Displays the manufacturer's website.

LAN

IP Address: Displays the IP address for the LAN.

Subnet Mask: Displays the subnet mask for the LAN.

DHCP Server: Displays DHCP server status for the LAN (Disable / DHCP Server / DHCP Relay Agent).

WAN

PPPoE Connection: The current connection status for the WAN.

IP Address: WAN port IP address.

Subnet Mask: WAN port IP subnet mask.

Primary DNS: The IP address of the primary DNS server.

Secondary DNS: The IP address of the secondary DNS server.

LAN

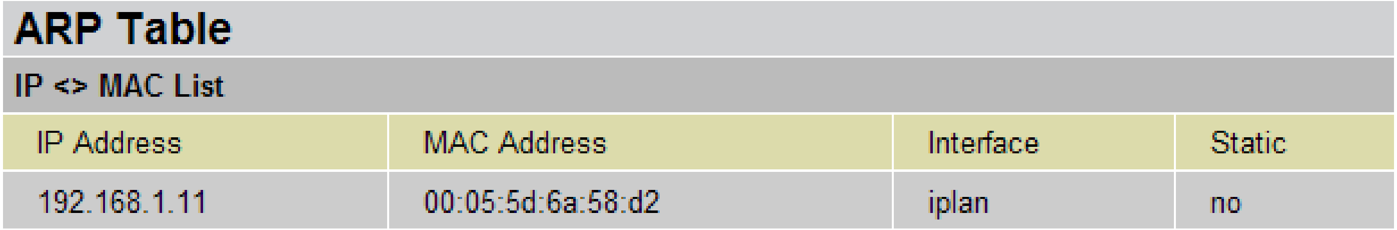
Port Status: User can look up to see if they are connected to Ethernet and SHDSL.

Statistics

Displays the Ethernet and SHDSL connection statistics (eg. sent and received data).

ARP Table

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



ARP Table

IP <> MAC List

IP Address	MAC Address	Interface	Static
192.168.1.11	00:05:5d:6a:58:d2	iplan	no

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

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

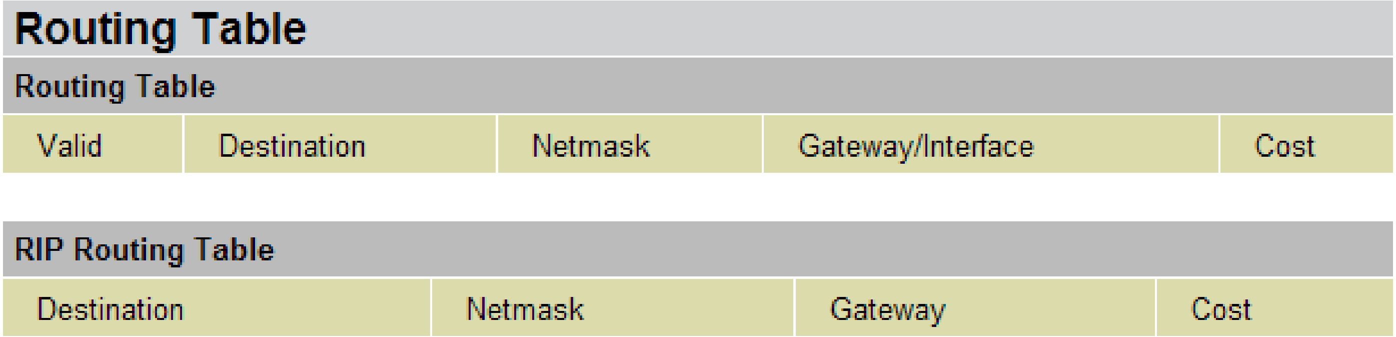
Interface: Shows the interface for the ARP item.

Static ARP: Shows the state of the static ARP item:

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

Routing Table

The Routing Table provides administrators with a database in the router that contains current network topology such as current paths for transmitted packets.



Routing Table

Routing Table

Valid	Destination	Netmask	Gateway/Interface	Cost

RIP Routing Table

Destination	Netmask	Gateway	Cost

Routing Table

Valid: Indicates a successful routing status.

Destination: Displays the IP address of the destination network.

Netmask: Displays the destination subnet mask address.

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

Gateway/Interface: Displays the IP address of the gateway or existing interface that this route uses.

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

RIP Routing Table

Destination: Displays the IP address of the destination network.

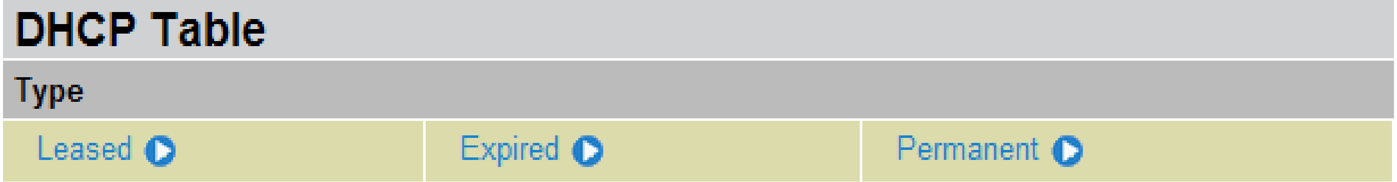
Netmask: Displays the destination subnet mask address.

Gateway: Displays the IP address of the gateway or existing interface that this route uses.

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

DHCP Table

The DHCP Table lists the DHCP lease information for all IP addresses assigned by the DHCP server in the device.



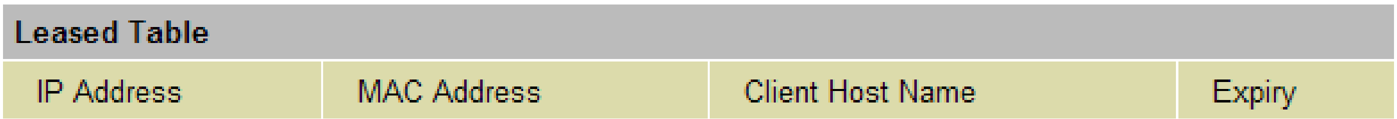
DHCP Table		
Type		
Leased	Expired	Permanent

Leased: The DHCP assigned IP addresses information.

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information.

Leased Table



Leased Table			
IP Address	MAC Address	Client Host Name	Expiry

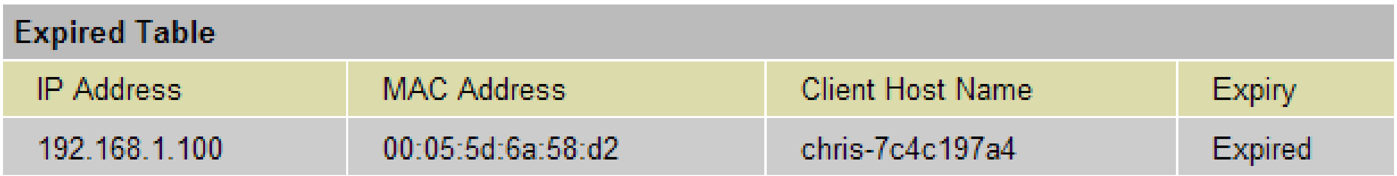
IP Address: The current corresponding DHCP-assigned dynamic IP address of the device.

MAC Address: The MAC Address of internal dhcp client host.

Client Host Name: The Host Name of the internal dhcp client.

Expiry: The current lease time of client.

Expired Table



Expired Table			
IP Address	MAC Address	Client Host Name	Expiry
192.168.1.100	00:05:5d:6a:58:d2	chris-7c4c197a4	Expired

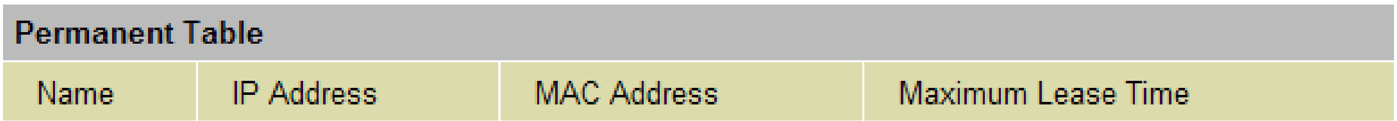
IP Address: The current corresponding DHCP-assigned dynamic IP address of the device.

MAC Address: The MAC Address of internal dhcp client host.

Client Host Name: The Host Name of the internal dhcp client.

Expiry: The current lease time of client.

Permanent Table



Permanent Table			
Name	IP Address	MAC Address	Maximum Lease Time

Name: The name you assigned to the Permanent configuration.

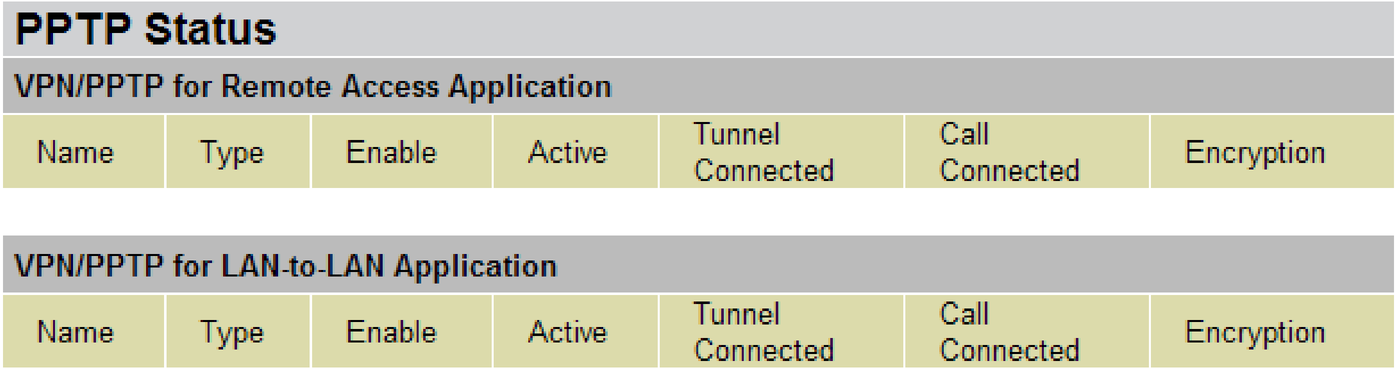
IP Address: The fixed IP address for the specific client.

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

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

PPTP Status (BiPAC 8500/ 8501/ 8520 Only)

This screen 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 activate.

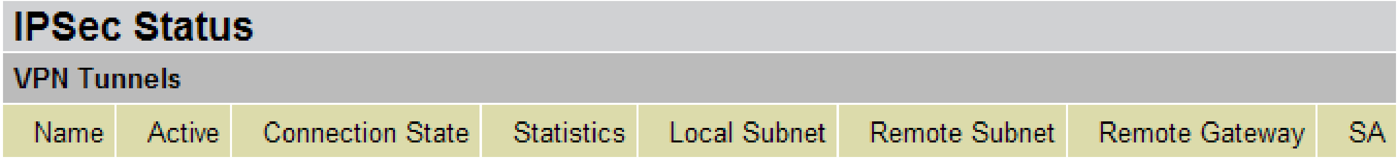
Tunnel Connected: Whether the VPN Tunnel is currently connected.

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

Encryption: The encryption type used for this VPN connection.

IPSec Status (BiPAC 8500/ 8501/ 8520 Only)

This screen 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.

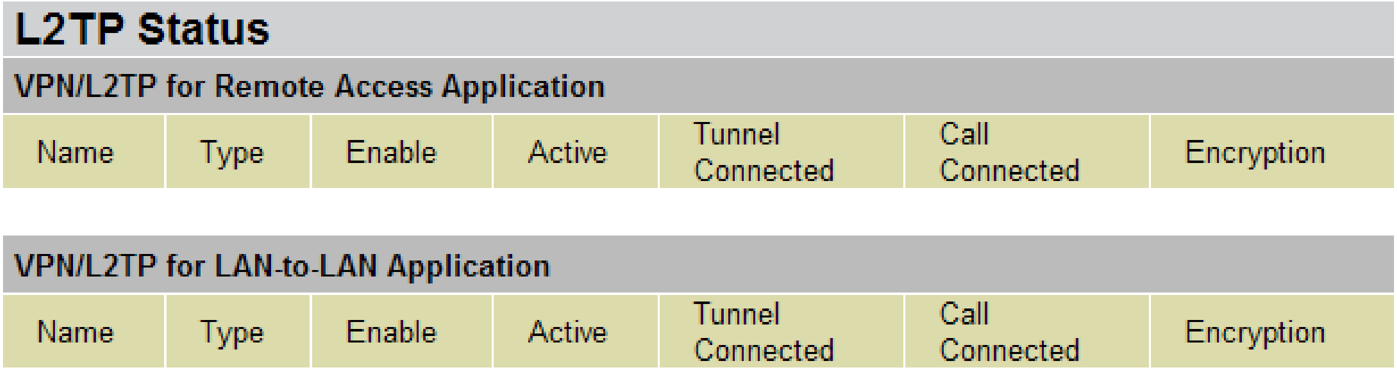
Remote Subnet: The Subnet of the remote site.

Remote Gateway: The Remote Gateway IP address.

SA: The Security Association for this VPN entry.

L2TP Status (BiPAC 8500/ 8501/ 8520 Only)

This screen 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 activate.

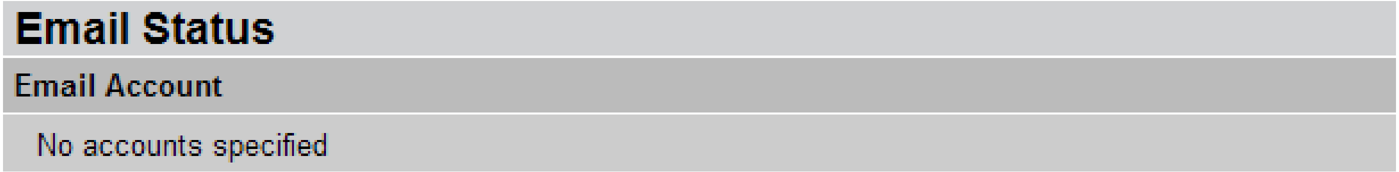
Tunnel Connected: Whether the VPN Tunnel is currently connected.

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

Encryption: The encryption type used for this VPN connection.

Email Status

This screen shows the details and status for the Email Account you have configured. Please refer to the Advanced section of this manual for the detail information.



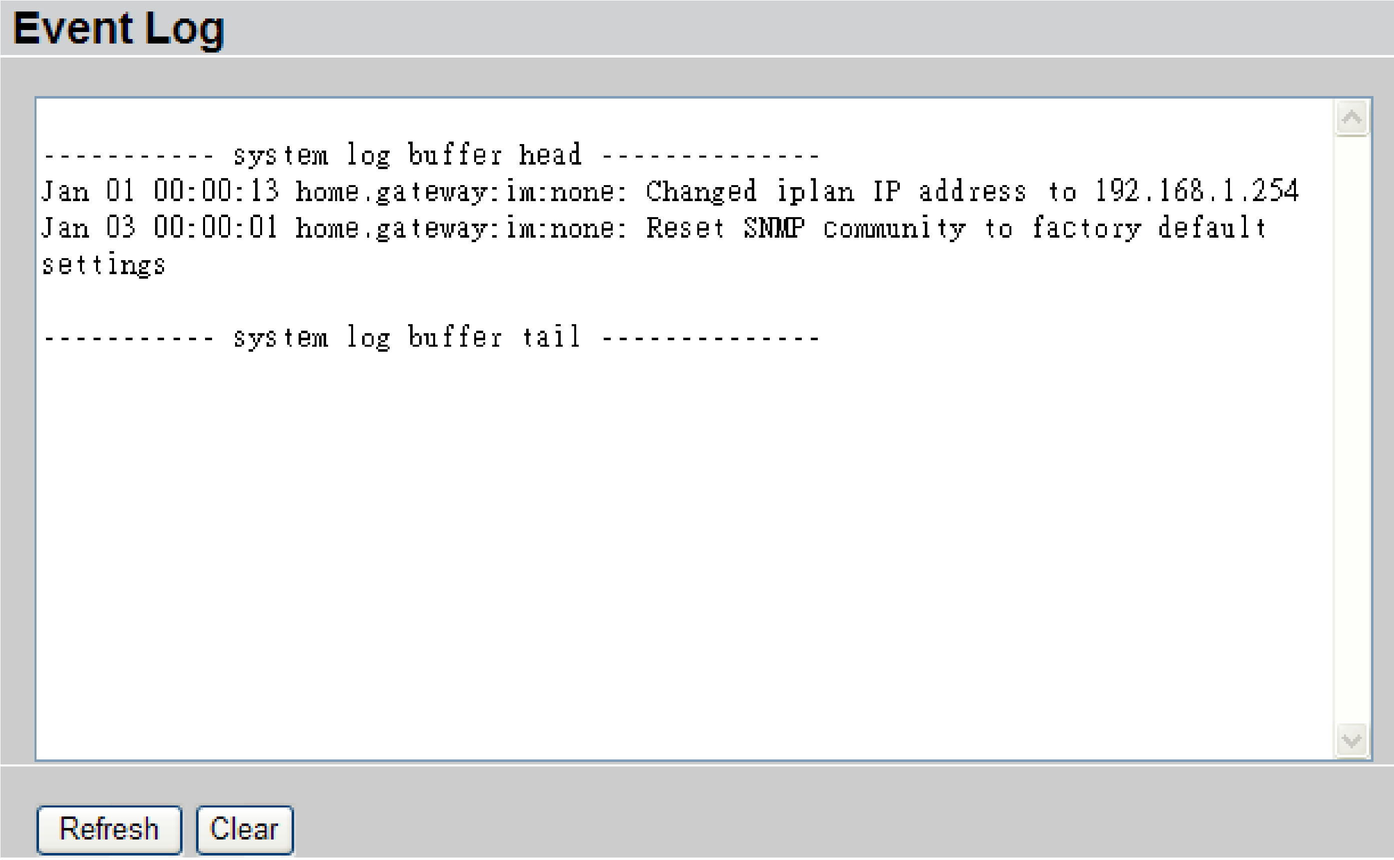
Email Status

Email Account

No accounts specified

Event Log

Event Log displays the log information of any unexpected events that occurs to your setting. This page displays the router Event Log entries which have been recorded when you have enabled Intrusion Detection or Block WAN PING on the Firewall screen. Please see the **Firewall** section of this manual for more detail informtaion.



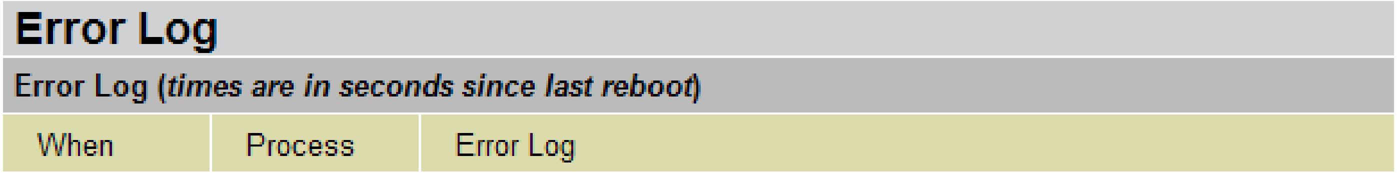
```
----------- system log buffer head --------------
Jan 01 00:00:13 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 03 00:00:01 home.gateway:im:none: Reset SNMP community to factory default
settings

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

Refresh: Click to update the event log.

Clear: Click to clear the current log from the screen.

Error Log

Displays any error encountered by the router (e.g. invalid names given to entries) accumulated up to the present time. You can trace its historical information with this function.



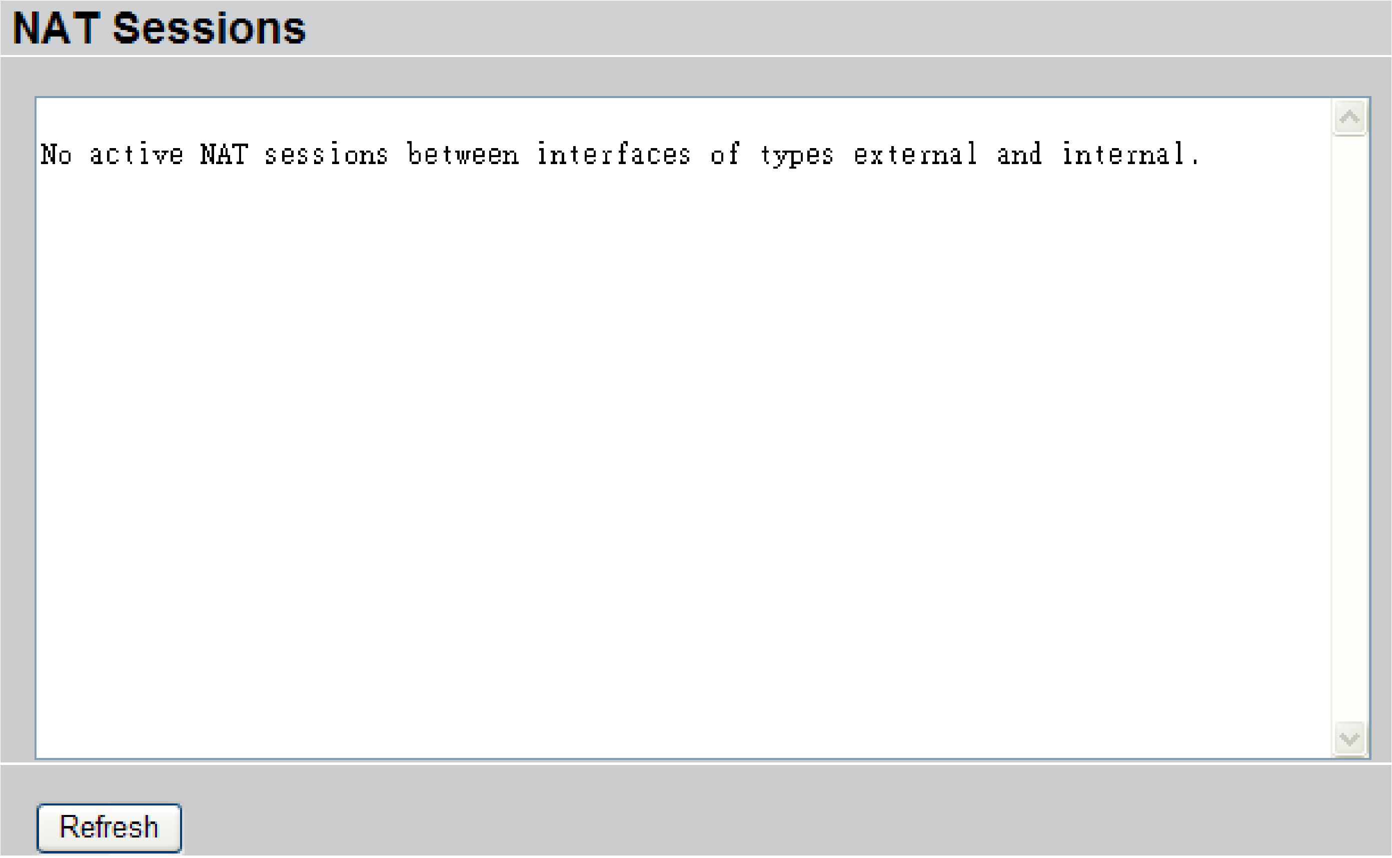
Error Log

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

When	Process	Error Log

NAT Sessions

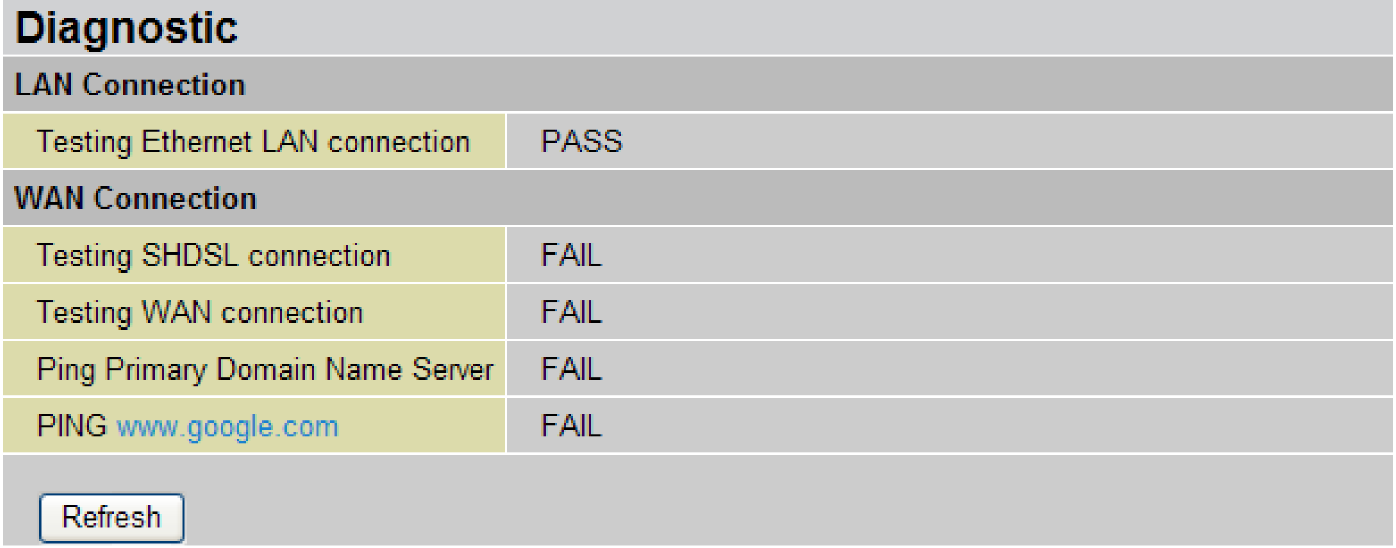
This section lists all current NAT sessions between interface of types external (WAN) and internal (LAN).



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

Diagnostic

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



Diagnostic

LAN Connection

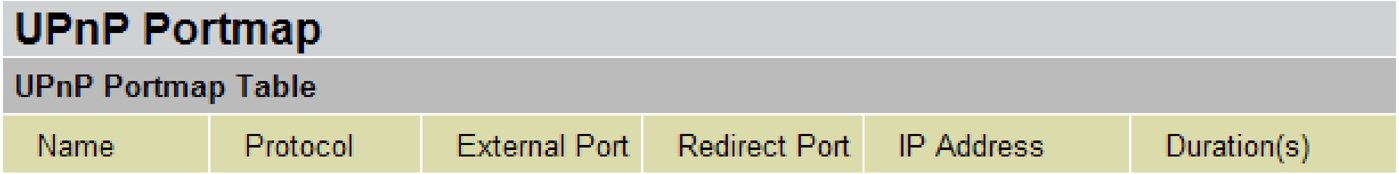
Testing Ethernet LAN connection	PASS

WAN Connection

Testing SHDSL connection	FAIL
Testing WAN connection	FAIL
Ping Primary Domain Name Server	FAIL
PING www.google.com	FAIL

UPnP Portmap

The section lists all established port-mapping using UPnP (Universal Plug and Play). Please see the **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	Duration(s)

Name: The Host Name of the internal UPnP client.

Protocol: The connection protocol of the UPnP client.

External Port: The external port for this connection.

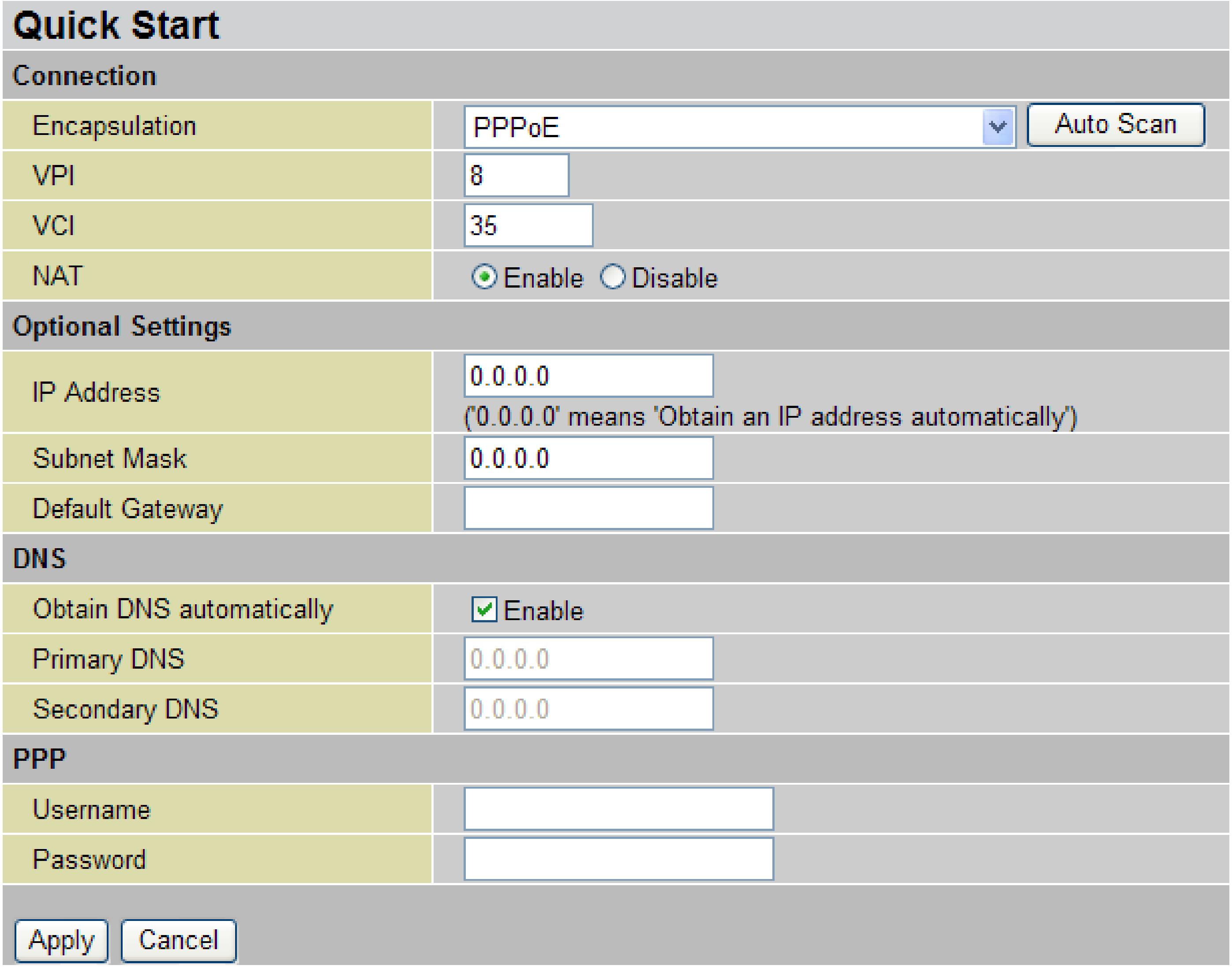
Redirect Port: The internal port for this connection.

IP Address: IP of the internal UPnP client.

Duration(s): Time (in seconds) of port mapping session that exists in UPnP Portmap.

Quick Start

Click Quick Start link to WAN Port setup pages. Please see the **WAN** section for detailed instructions on configuring your WAN settings.

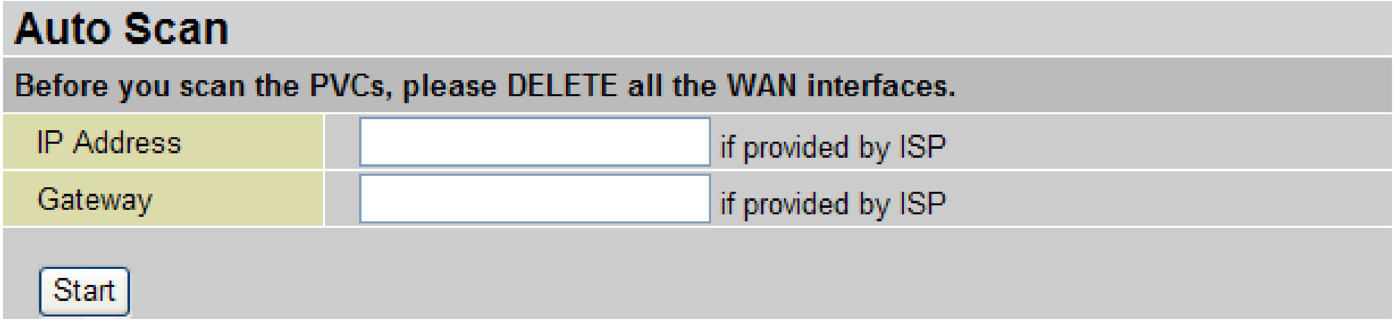


Quick Start

Connection	
Encapsulation	PPPoE
VPI	8
VCI	35
NAT	● Enable ○ Disable
Optional Settings	
IP Address	0.0.0.0 ('0.0.0.0' means 'Obtain an IP address automatically')
Subnet Mask	0.0.0.0
Default Gateway	
DNS	
Obtain DNS automatically	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
PPP	
Username	
Password	

Usually, the information you will need for the Quick Start wizard to configure the connection is your login name (often in the form of username@ispname), password and the encapsulation type. In addition, you can provide a specific DNS or check the Enable box to get the DNS automatically from your ISP.

Your ISP will be able to provide all the information you need. Alternatively, if you have deleted the current WAN Connection through WAN > ISP page, you are allowed to use the router's PVC Scan feature to determine the Encapsulation types offered by your ISP.

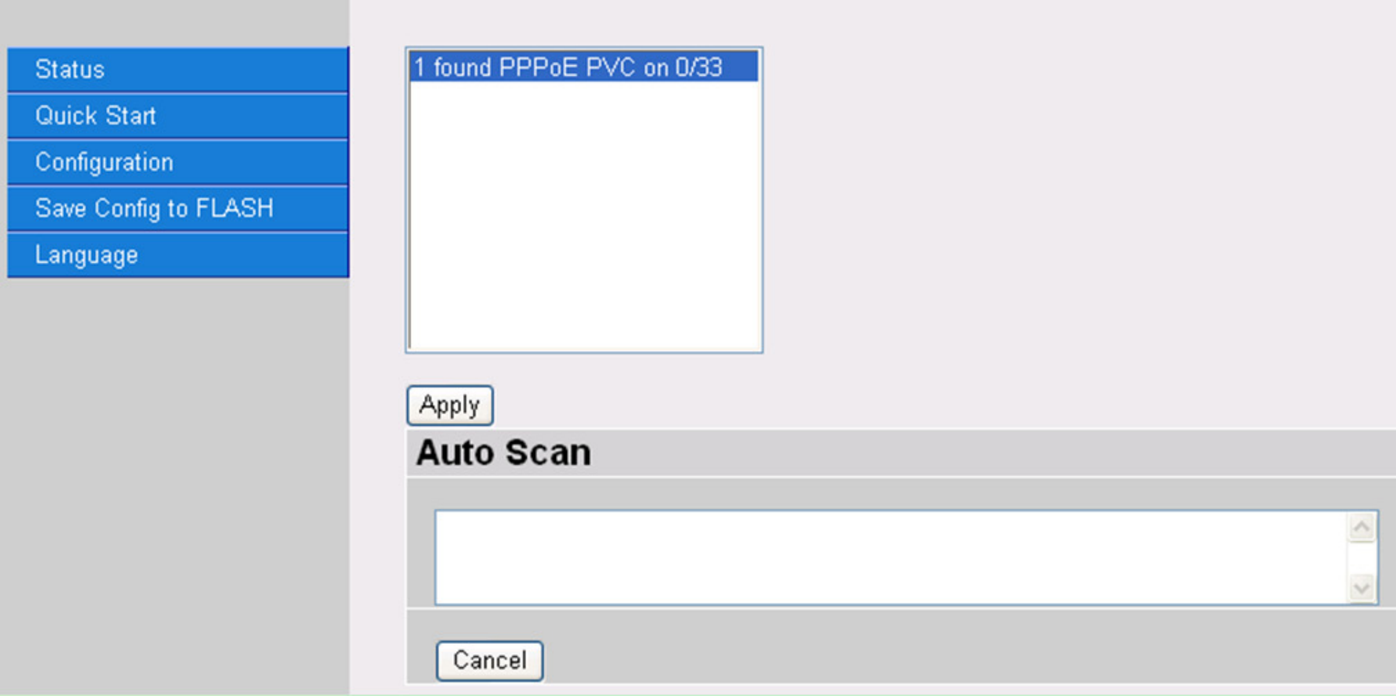


Auto Scan

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

IP Address	if provided by ISP
Gateway	if provided by ISP

Click Start to start scanning. If the scan is successful, you will be presented with a list of supported options:



1 found PPPoE PVC on 0/33

Select the desired option from the list and click Apply to return to the Quick Start screen to continue configuring your ISP connection. Please note that the contents of this list will vary depending on what is supported by your ISP.

Configuration

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

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

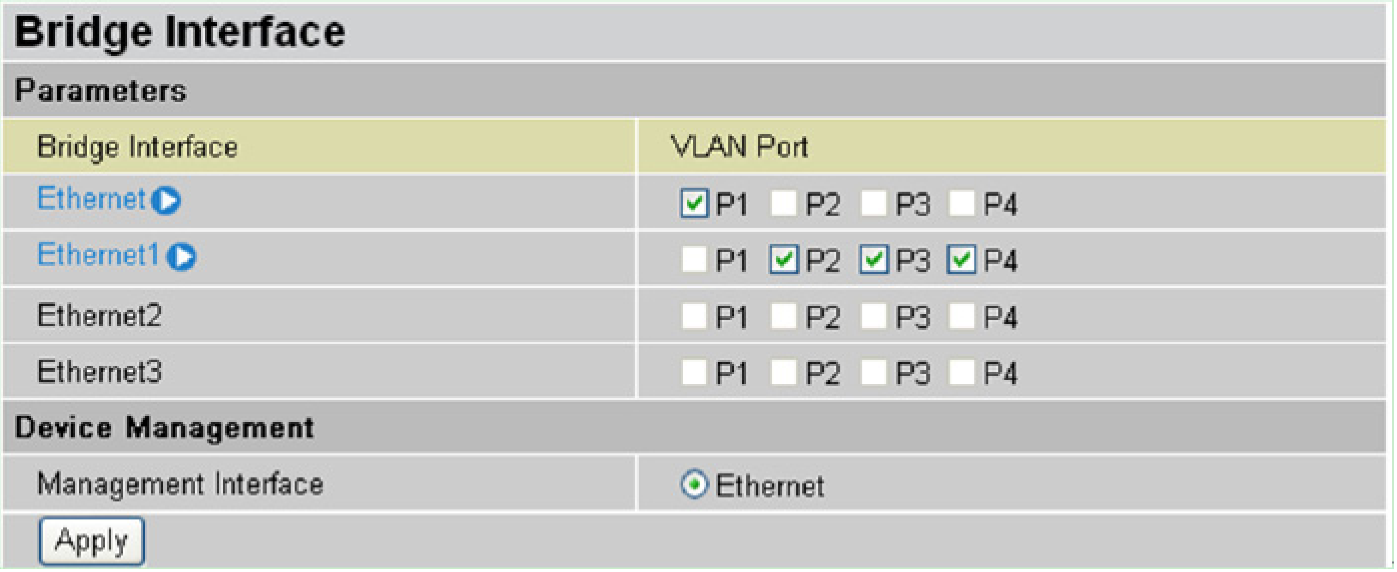
The function of each configuration sub-item is described in the following sections.

LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system to which many computers are attached together and is limited to the immediate area, usually within the same building or storey of a building.

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

Bridge Interface



Bridge Interface

Parameters

Bridge Interface	VLAN Port
Ethernet	☑ P1 ☐ P2 ☐ P3 ☐ P4
Ethernet1	☐ P1 ☑ P2 ☑ P3 ☑ P4
Ethernet2	☐ P1 ☐ P2 ☐ P3 ☐ P4
Ethernet3	☐ P1 ☐ P2 ☐ P3 ☐ P4

Device Management

Management Interface: ● Ethernet

You can setup member ports for each VLAN group under Bridge Interface section. For example shown as above, 2 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.

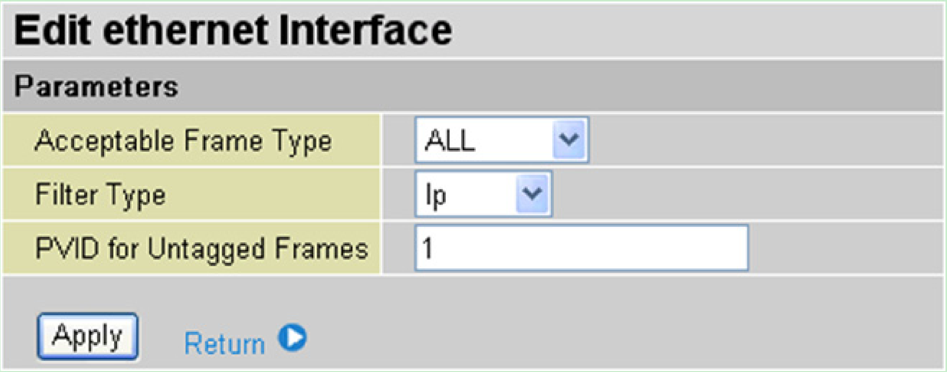
Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

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

Edit Ethernet Interface Parameter

Click on a specific Ethernet you that you wish to edit its interface parameter under the Bridged Interface section.

You can also edit the Ethernet Interface parameter such as its Acceptable Frame Type; Filter Type or PVID for Untagged Frames. When the editing is complete, click Apply to save the changes and then click Return to go back to the Bridged Interface page.



Acceptable Frame Type: ALL

Filter Type: Ip

PVID for Untagged Frames: 1

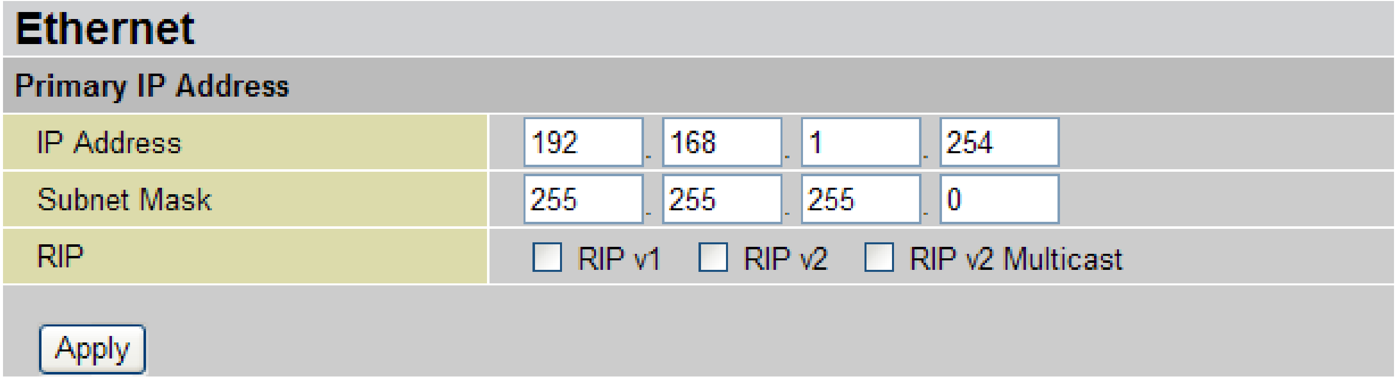
Management Interface: To specify which VLAN group is responsible for device management, like doing web management.

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

Click Apply to confirm the settings.

Ethernet

The router supports more than one Ethernet IP addresses in the LAN that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



IP Address: 192 . 168 . 1 . 254

Subnet Mask: 255 . 255 . 255 . 0

RIP: ☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast

IP Address: The default IP address of this router.

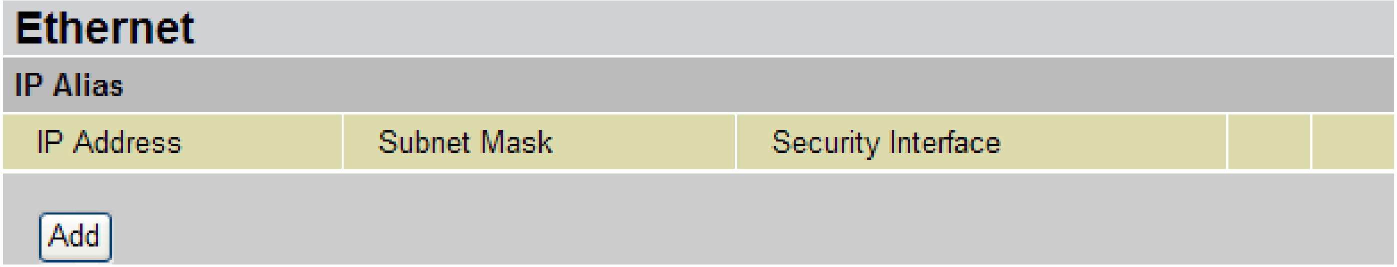
Netmask: The default subnet mask of this router.

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

Click Apply to confirm the settings.

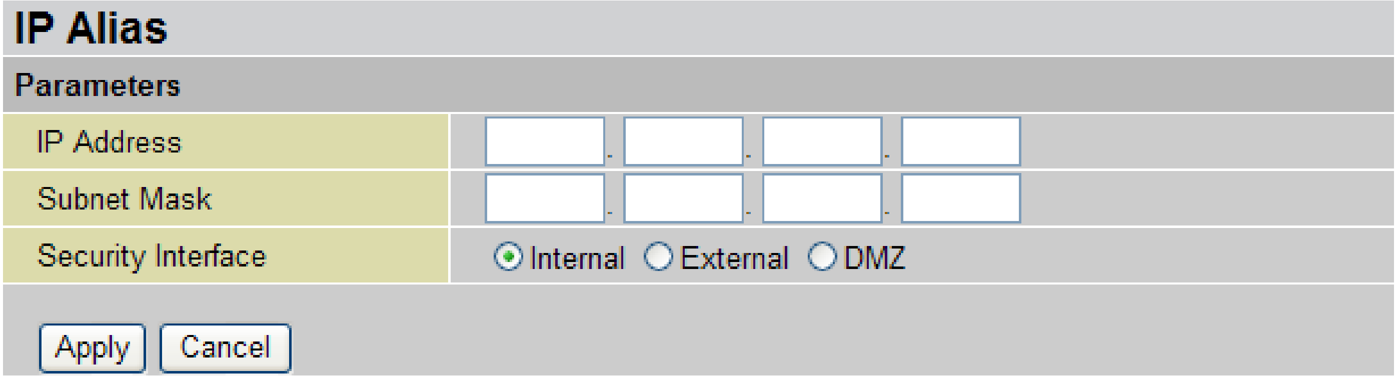
IP Alias

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



IP Address	Subnet Mask	Security Interface		

Click Add to add a new IP alias.



Security Interface ● Internal ○ External ○ DMZ

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

SubNetmask: Specify a subnet mask for this virtual interface.

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

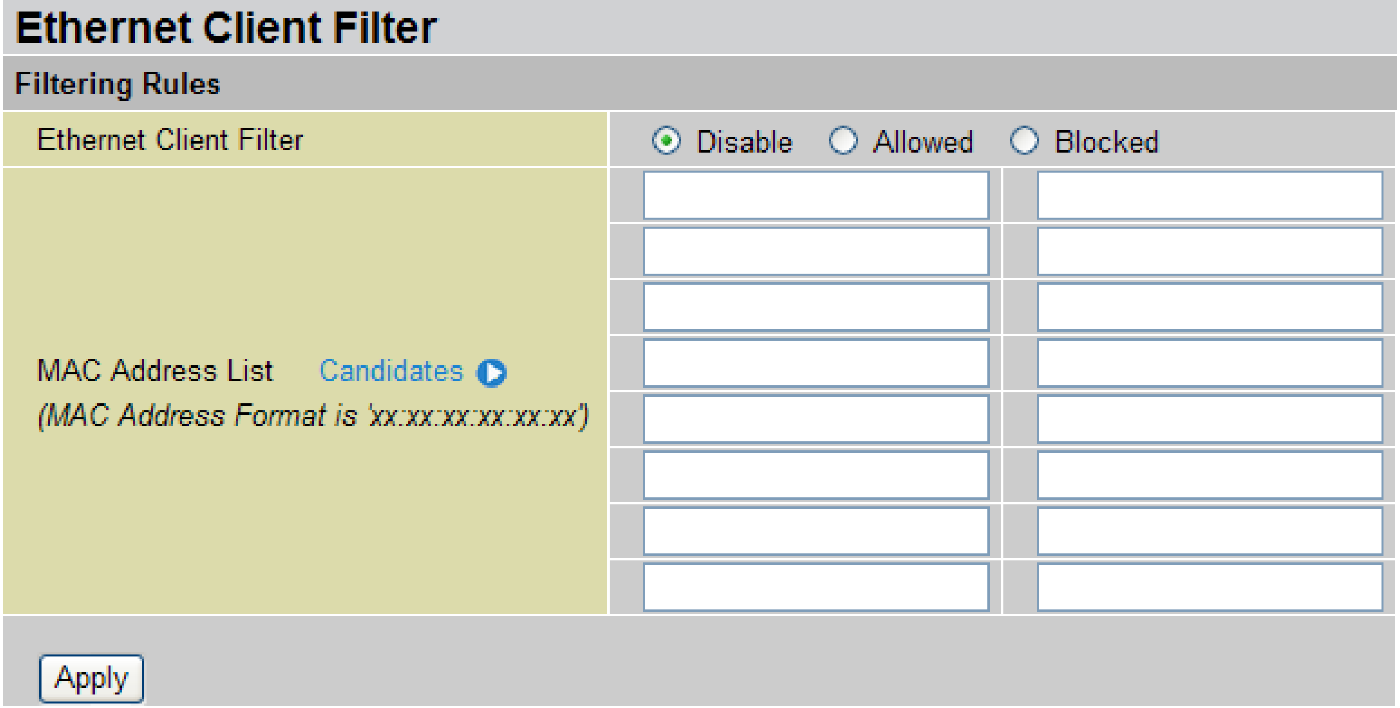
- **Internal:** The network is behind NAT. All traffic will translate network address when being sent out to the Internet if NAT is enabled.
- **External:** There is no NAT for this IP interface and it is connecting to the Internet directly. It is used when provided with multiple public IP addresses by ISP. In this case, you allow to use the public IP address in the local network with gateway IP address point to the IP address for this interface.
- **DMZ:** Specify the network to the DMZ area. There is no NAT for this interface.

Click Apply to confirm the settings.

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 to restrict unwanted machine(s) to access your LAN.

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



Ethernet Client Filter ● Disable ○ Allowed ○ Blocked

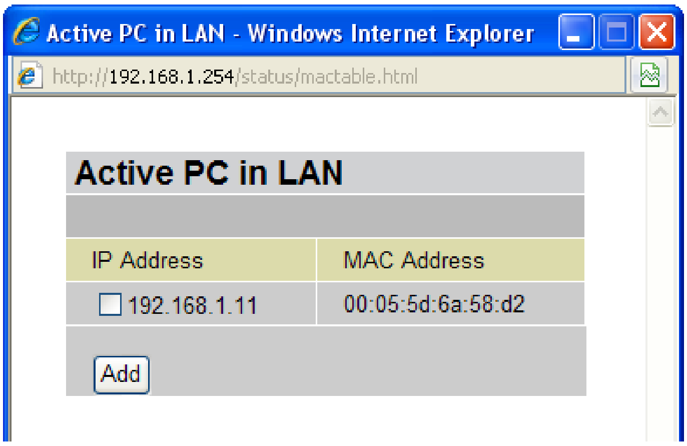
Ethernet Client Filter: Default setting is Disable.

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

MAC Address List: You are allowed to set up to 16 entries for MAC Address Filter. The length of MAC address is 6 bytes and can be input by number 0 - 9 or letter a - f.

Note: Mac address is presented only in hexadecimal characters. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. Semicolon (:) must be included.

Candidates: Click the link to automatically detect devices connected to the router through the Ethernet.


Active PC in LAN - Windows Internet Explorer
http://192.168.1.254/status/mactable.html
Active PC in LAN
Add

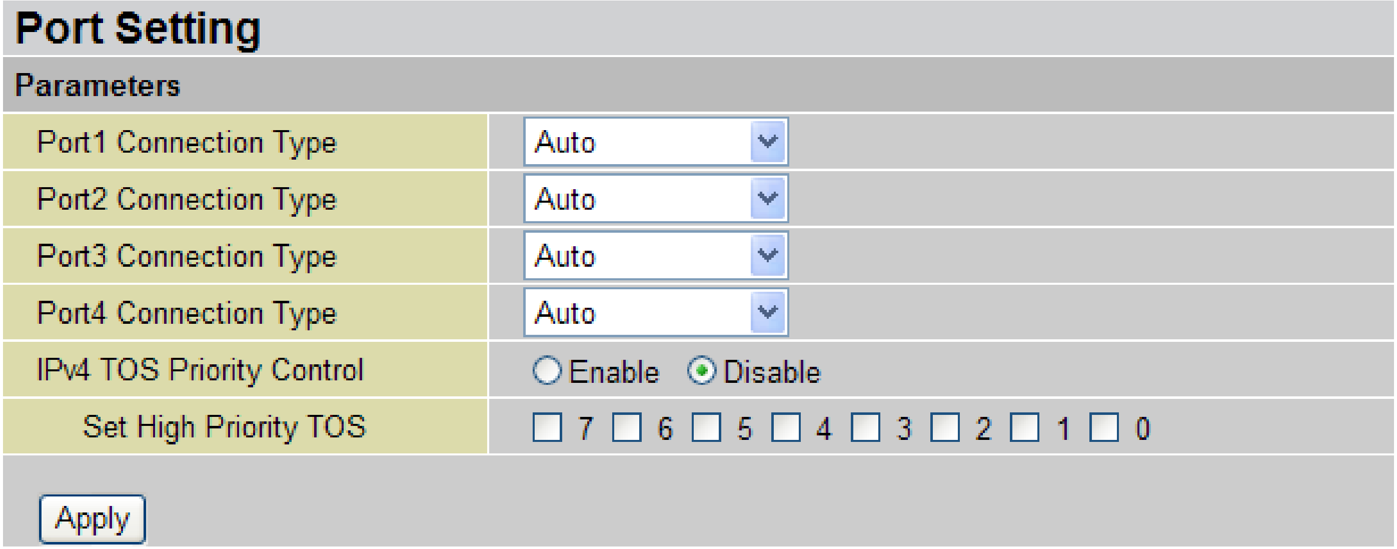
IP Address	MAC Address
☐ 192.168.1.11	00:05:5d:6a:58:d2

Active PC in LAN displays a list of IP Address & MAC Address of each individual Ethernet device which is connected to the router. You can check the box next to the IP address to block or allow and then click Add to add the entry to the Ethernet Client Filter table.

Click Apply to confirm the settings.

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.



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	☐ 7 ☐ 6 ☐ 5 ☐ 4 ☐ 3 ☐ 2 ☐ 1 ☐ 0

Port # Connection Type: There are 6 options to choose: Auto, 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. Default setting is Auto, which users should keep it unless there is specific problem occured with PCs and you cannot access your LAN.

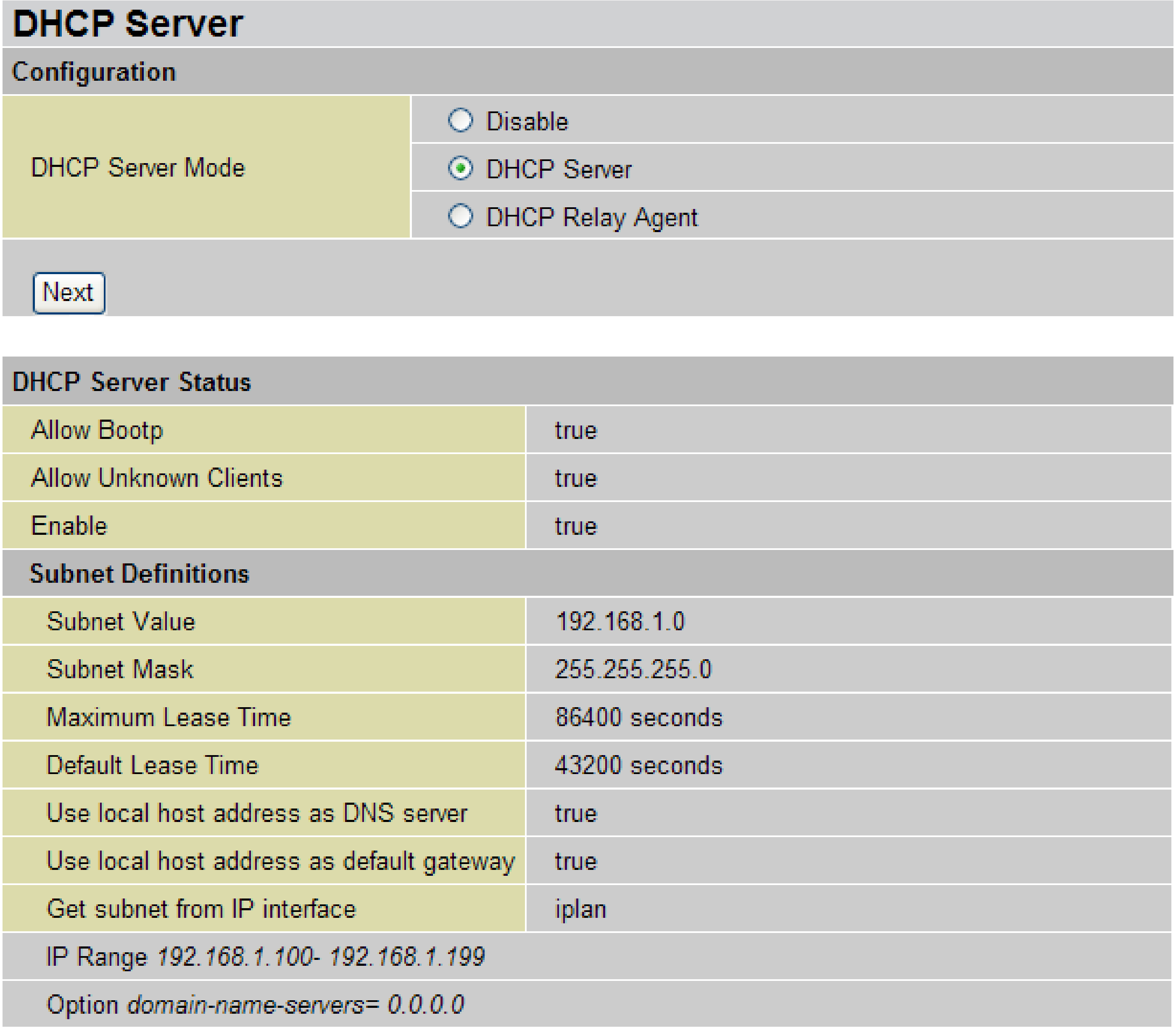
IPv4 TOS priority Control (Advanced users)**:** TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

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.

Click Apply to confirm the settings.

DHCP Server

The device enables to act as a DHCP server for your network. You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. Disable this function if the stations that connect to the device's LAN ports using static IP addresses.



DHCP Server

Configuration

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

DHCP Server Status

Allow Bootp	true
Allow Unknown Clients	true
Enable	true
Subnet Definitions	
Subnet Value	192.168.1.0
Subnet Mask	255.255.255.0
Maximum Lease Time	86400 seconds
Default Lease Time	43200 seconds
Use local host address as DNS server	true
Use local host address as default gateway	true
Get subnet from IP interface	iplan

IP Range *192.168.1.100- 192.168.1.199*

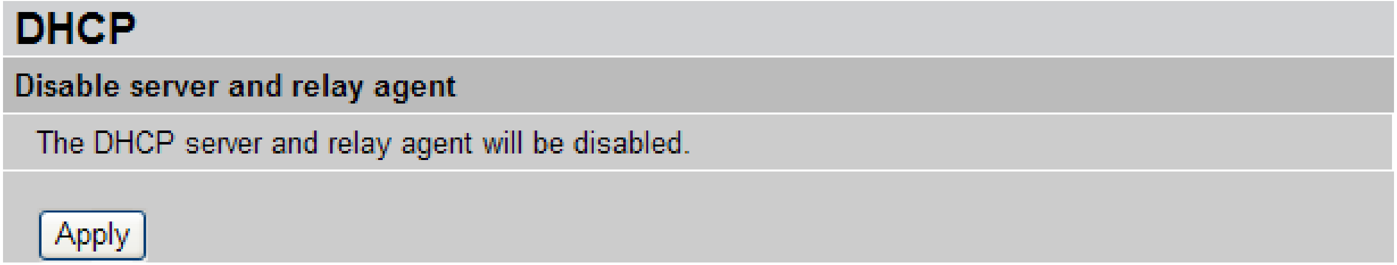
Option *domain-name-servers= 0.0.0.0*

DHCP Server Mode:

- **Disable:** Choose Disable if IP addresses are assigned manually to stations on your network.
- **DHCP Server:** Choose DHCP Server to have the BiPAC 85xx series devices assign IP addresses automatically to stations on your network.
- **DHCP Relay Agent:** Choose DHCP Relay Agent if you want to place DHCP servers and clients on different networks, making DHCP management easier when there is more than one subnet on the network.

Disabling DHCP Server

Click the Disable radio button and then click Next to display the confirmation screen.



DHCP

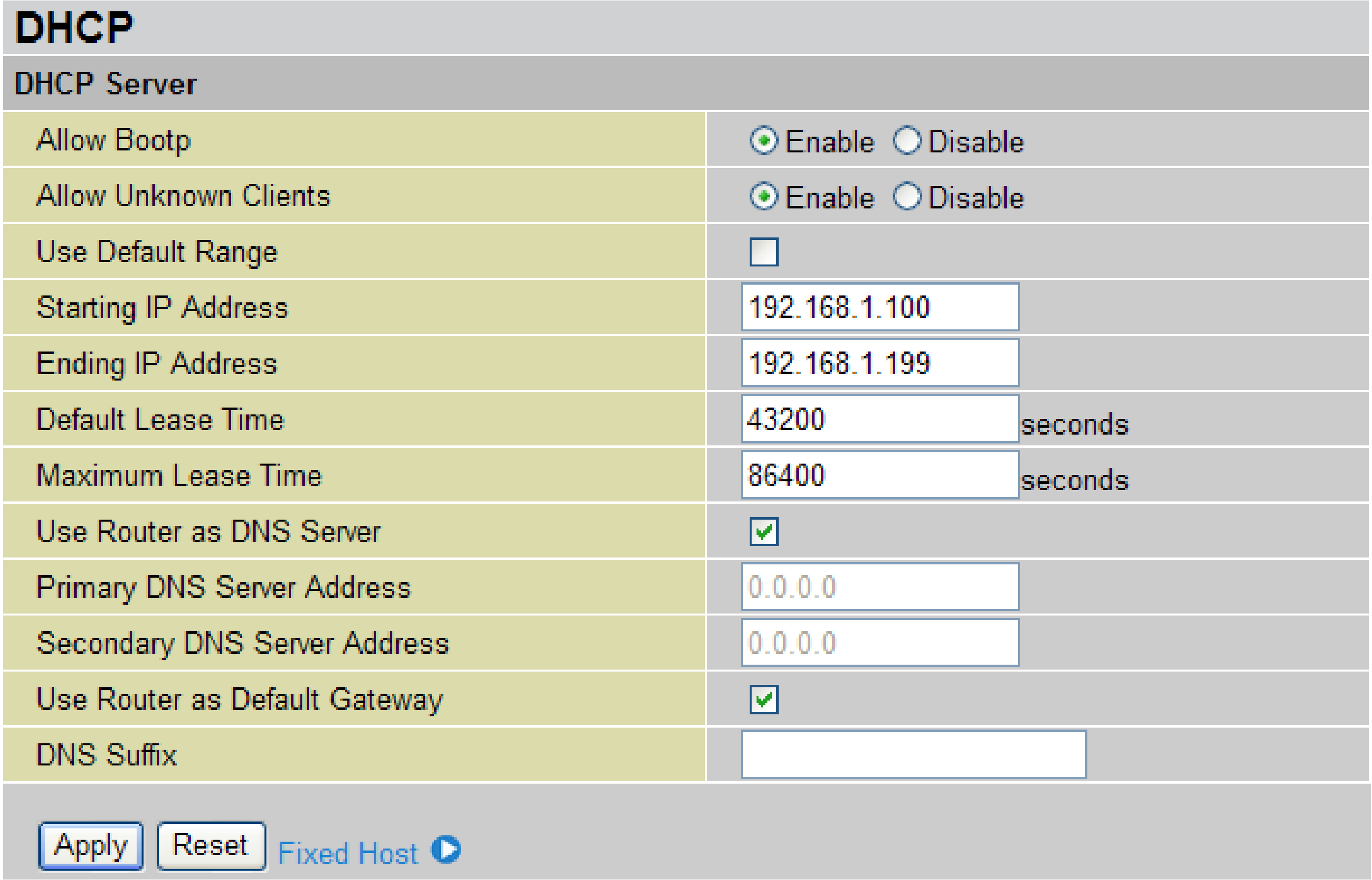
Disable server and relay agent

The DHCP server and relay agent will be disabled.

Click Apply to disable the DHCP server and relay agent.

Configuring DHCP Server

To configure the router's DHCP Server, select DHCP Server from DHCP Server Mode and click Next.

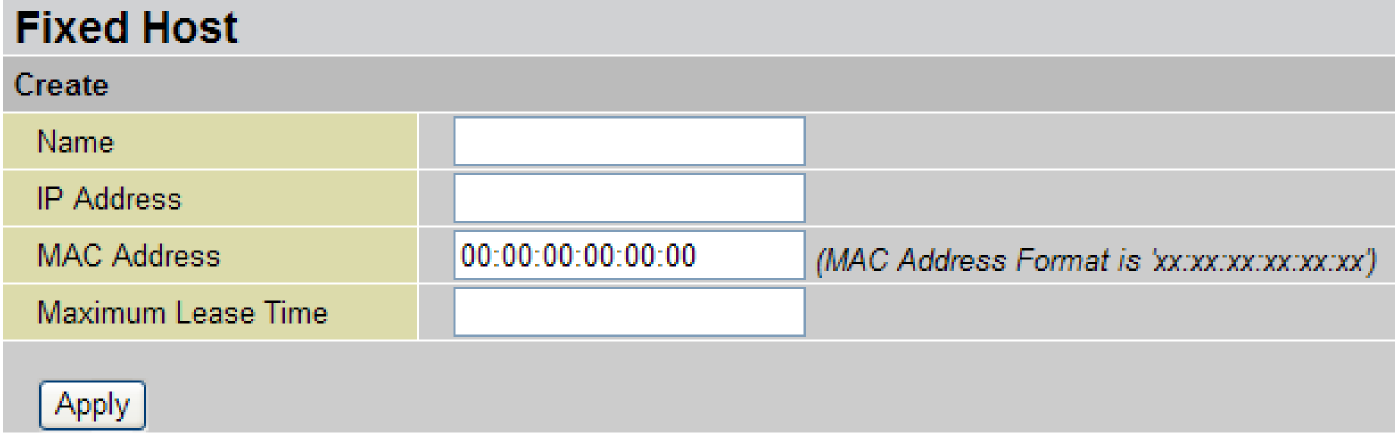


DHCP

DHCP Server

Allow Bootp	● Enable ○ Disable
Allow Unknown Clients	● Enable ○ Disable
Use Default Range	☐
Starting IP Address	192.168.1.100
Ending IP Address	192.168.1.199
Default Lease Time	43200 seconds
Maximum Lease Time	86400 seconds
Use Router as DNS Server	☑
Primary DNS Server Address	0.0.0.0
Secondary DNS Server Address	0.0.0.0
Use Router as Default Gateway	☑
DNS Suffix	

You can then configure parameters of the DHCP Server. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. If you check "Use Router as a DNS Server", the 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).

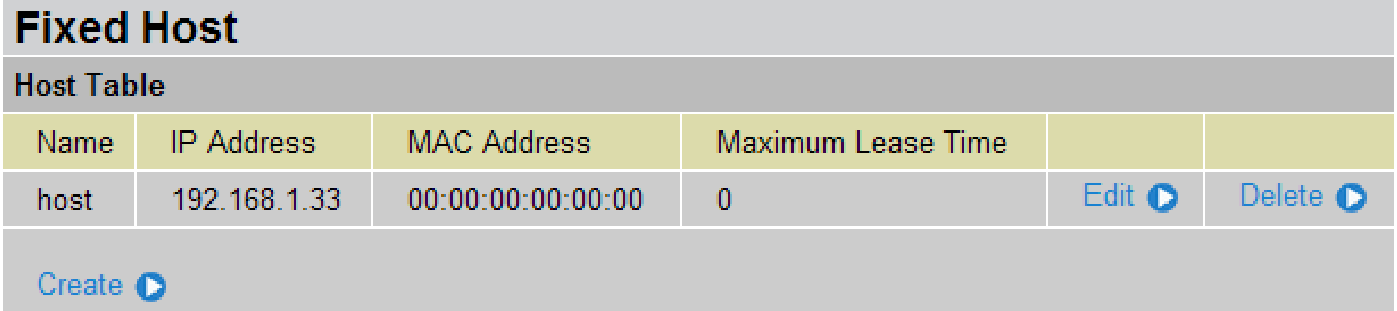


Fixed Host

Create

Name		
IP Address		
MAC Address	00:00:00:00:00:00	(MAC Address Format is 'xx:xx:xx:xx:xx:xx')
Maximum Lease Time		

Fixed Host: Click this link to add a specific fixed MAC Address Mapping to a fixed Address.



Fixed Host

Host Table

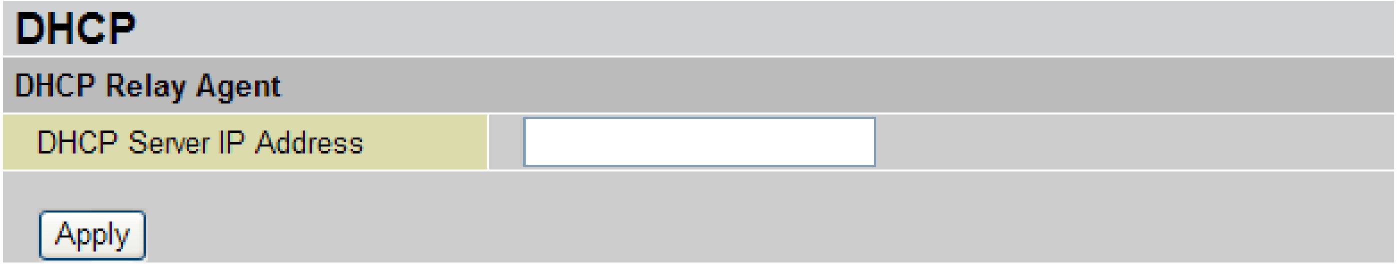
Name	IP Address	MAC Address	Maximum Lease Time		
host	192.168.1.33	00:00:00:00:00:00	0	Edit	Delete

Fill in the Host Name, MAC Address and IP Address fields. After clicking Apply, the new entry is listed.

You can edit or delete the MAC Address by clicking Edit or Delete next to the item you want to modify/remove.

Configuring the DHCP Relay Agent

Choose DHCP Relay Agent if you want to place DHCP servers and clients on different networks. Click Next to display the screen as below.



DHCP

DHCP Relay Agent

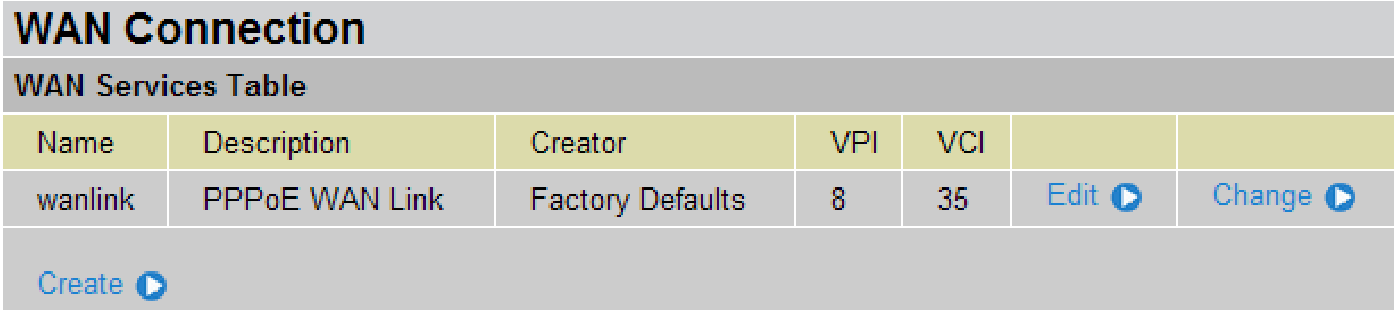
DHCP Server IP Address	

You must enter the IP address of the DHCP server that assigns an IP address 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. There are 2 items within the WAN section: **ISP** and **SHDSL**.

ISP



WAN Connection

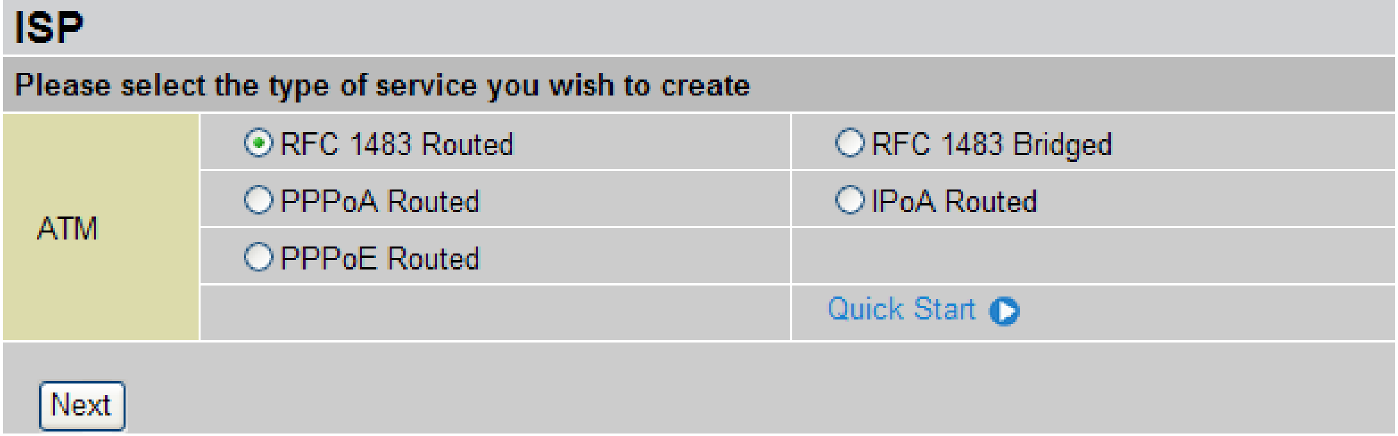
WAN Services Table

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

Default setting is PPPoE. If your ISP uses this access protocol, click Edit to input other parameters. (On the Edit screen, click Advanced Options to modify the associated parameters.) If your ISP does not use PPPoE, you can change the default WAN connection entry by clicking Change.

Some ISP may provide more service via different WAN connection. In this case, you can create more connections by clicking Create to go to the configuration page to setup the type of sevice from the list and then press Next to continue with the configuration. There are 5 types of ISP service to choose from: **RFC 1483 Routed**, **RFC 1483 Bridged**, **PPPoA Routed**, **IPoA Routed** and **PPPoE Routed**. The device can support maximum of up to 8 WAN connections.

Note: The application of multiple WAN connections depends on your Internet Service Provider.



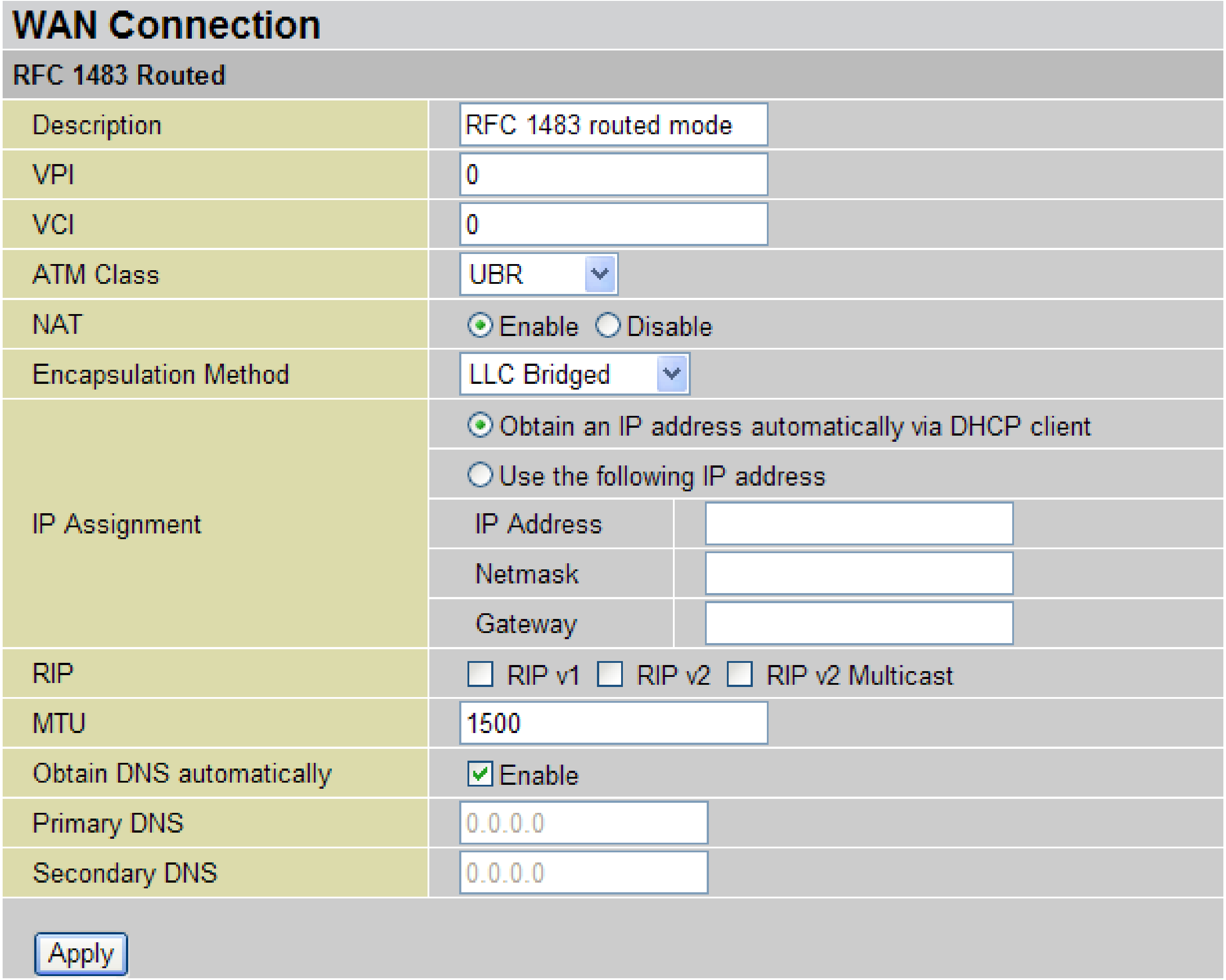
ISP

Please select the type of service you wish to create

ATM	● RFC 1483 Routed	○ RFC 1483 Bridged
	○ PPPoA Routed	○ IPoA Routed
	○ PPPoE Routed	
		Quick Start

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

RFC 1483 Routed



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
Obtain DNS automatically	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Description: User-definable name for the connection.

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

ATM Class: Select thehe 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 by sharing the single IP address. If users on your LAN have their own public IP addresses for accessing Internet directly, the NAT function can be disabled.

Encapsulation method: Select 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.

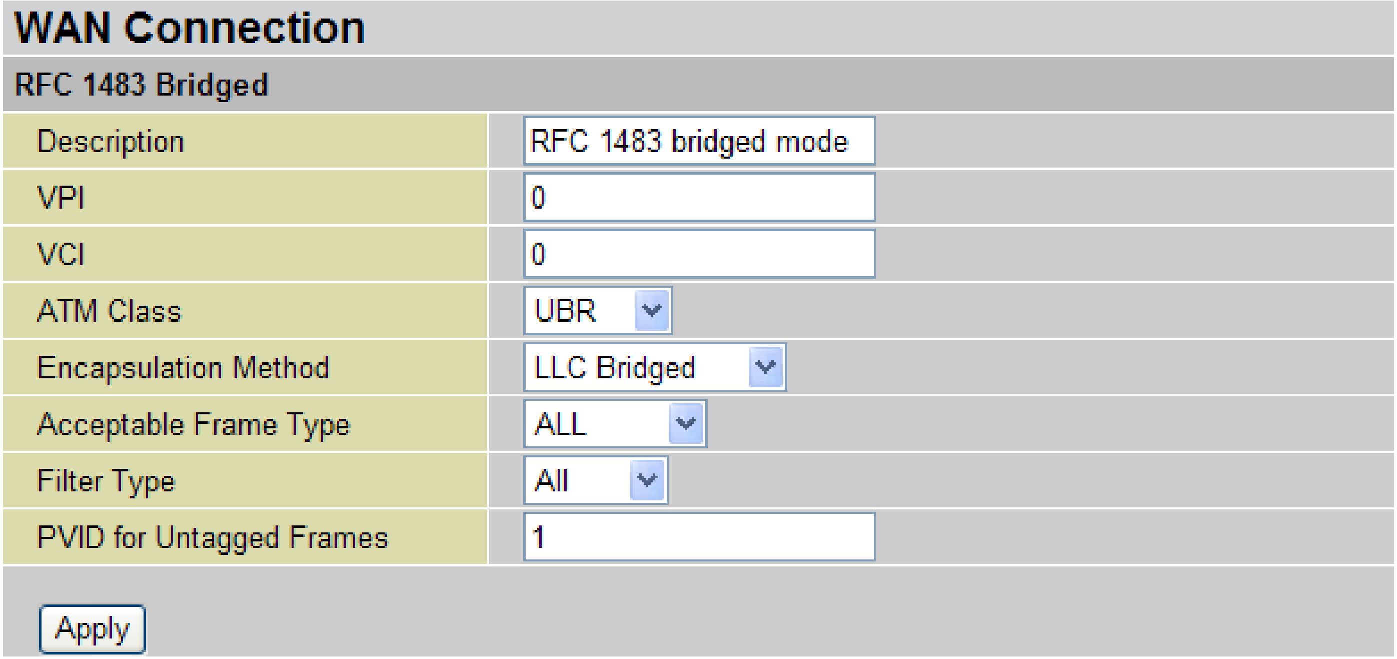
MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

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

MAC Address Spoofing: This option is required by Service Providers. You must fill in the MAC address that is specified by your Service Provider if this is required. Default is disabled.

Click Apply to confirm the settings.

RFC 1483 Bridged



WAN Connection

RFC 1483 Bridged

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

Description: User-definable name for the connection.

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

ATM Class: Select thehe 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 pass through this connection, all traffic or only VLAN tagged.

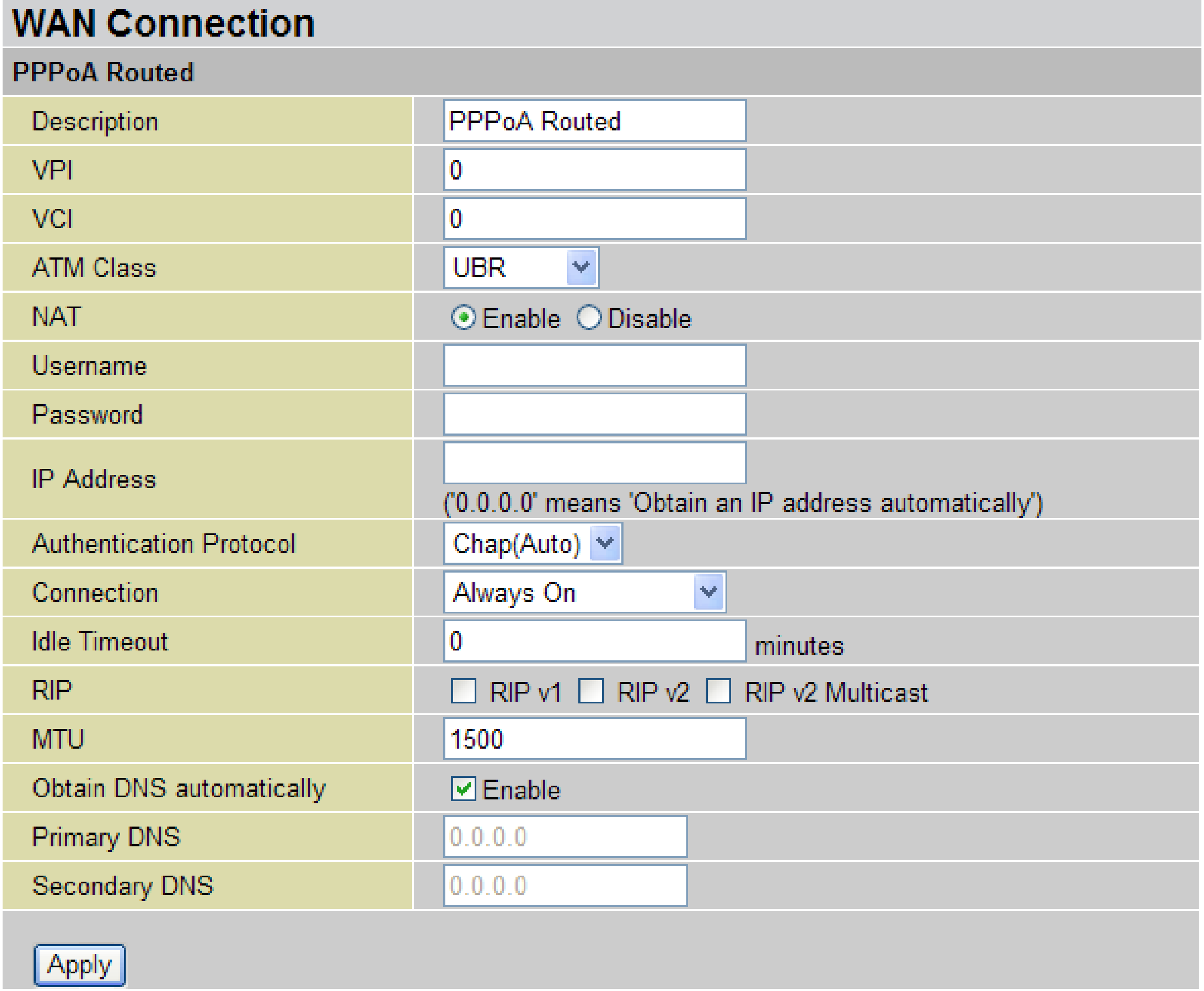
Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

- **All:** Allow all types of ethernet packets through the port.
- **Ip:** Allow only IP/ARP types of ethernet packets through the port.
- **Pppoe:** Allow 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 a specific PVID. The valid value range for PVID is 1~4094.

Click Apply to confirm the settings.

PPPoA Routed



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
Obtain DNS automatically	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Description: User-definable name for the connection.

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

ATM Class: Select thehe 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 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 PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

- **Connect to Demand:** If you want to establish a PPPoA session only when there is a packet requesting to access 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 being checked by the 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.

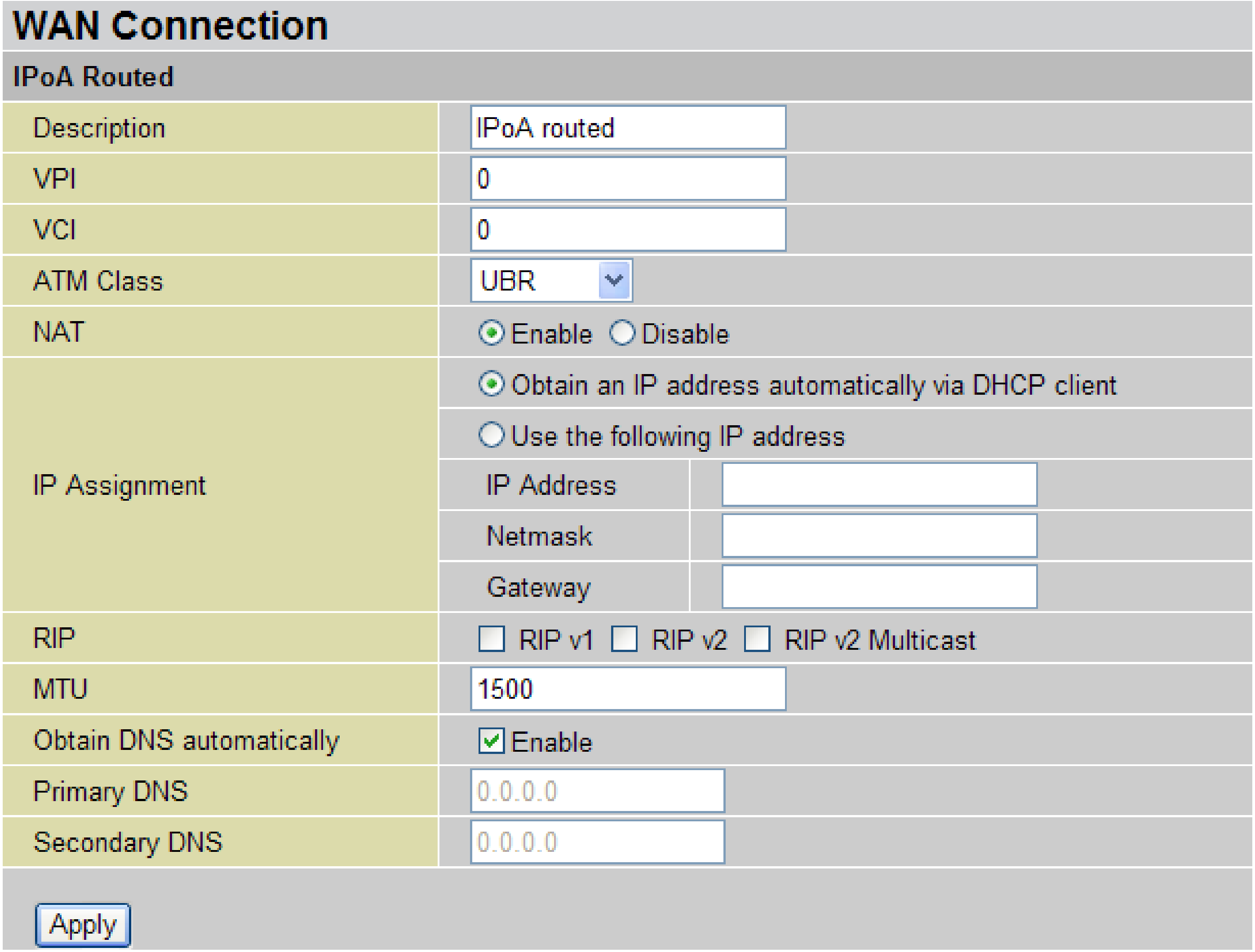
Obtain DNS automatically: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Click Apply to confirm the settings.

IPoA Routed



WAN Connection

IPoA Routed

Description	IPoA routed	
VPI	0	
VCI	0	
ATM Class	UBR	
NAT	● Enable ○ Disable	
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	
Obtain DNS automatically	☑ Enable	
Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0	

Description: User-definable name for the connection.

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

ATM Class: Select thehe 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.

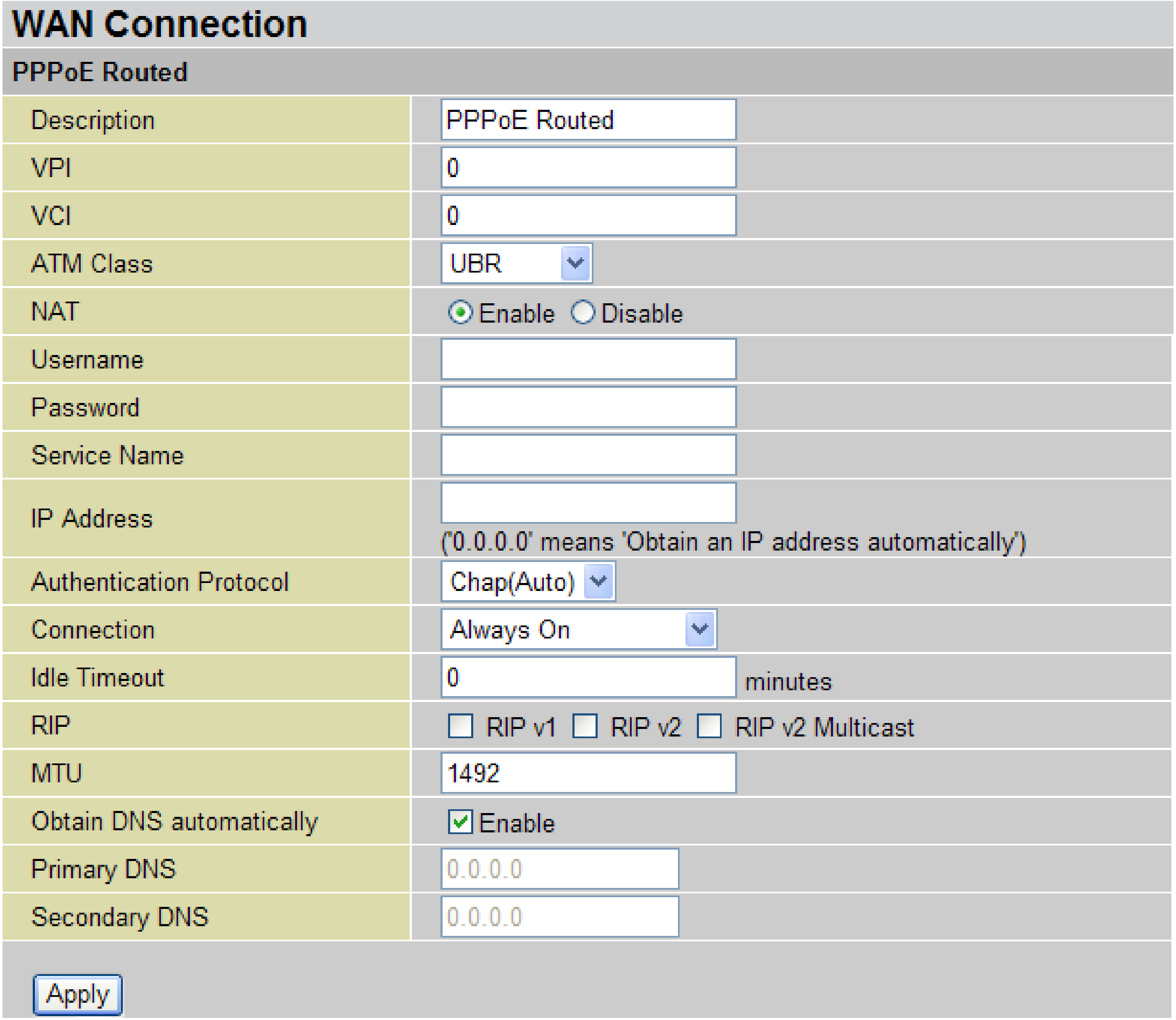
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Click Apply to confirm the settings.

PPPoE Routed



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
Obtain DNS automatically	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

Description: User-definable name for the connection.

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

ATM Class: Select 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).

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 PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.
- **Connect to Demand:** If you want to establish a PPPoA session only when there is a packet requesting to access 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 being checked by the 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.

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

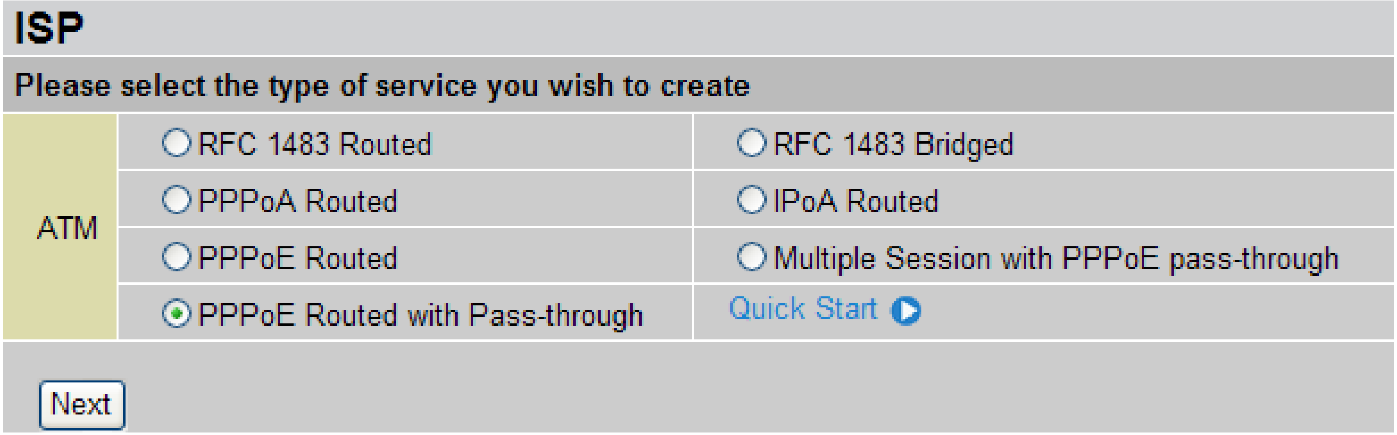
Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Click Apply to confirm the settings.

PPPoE Routed with Pass-through

To access PPPoE with Pass-through Connection, press Change > PPPoE Routed with Pass-through.

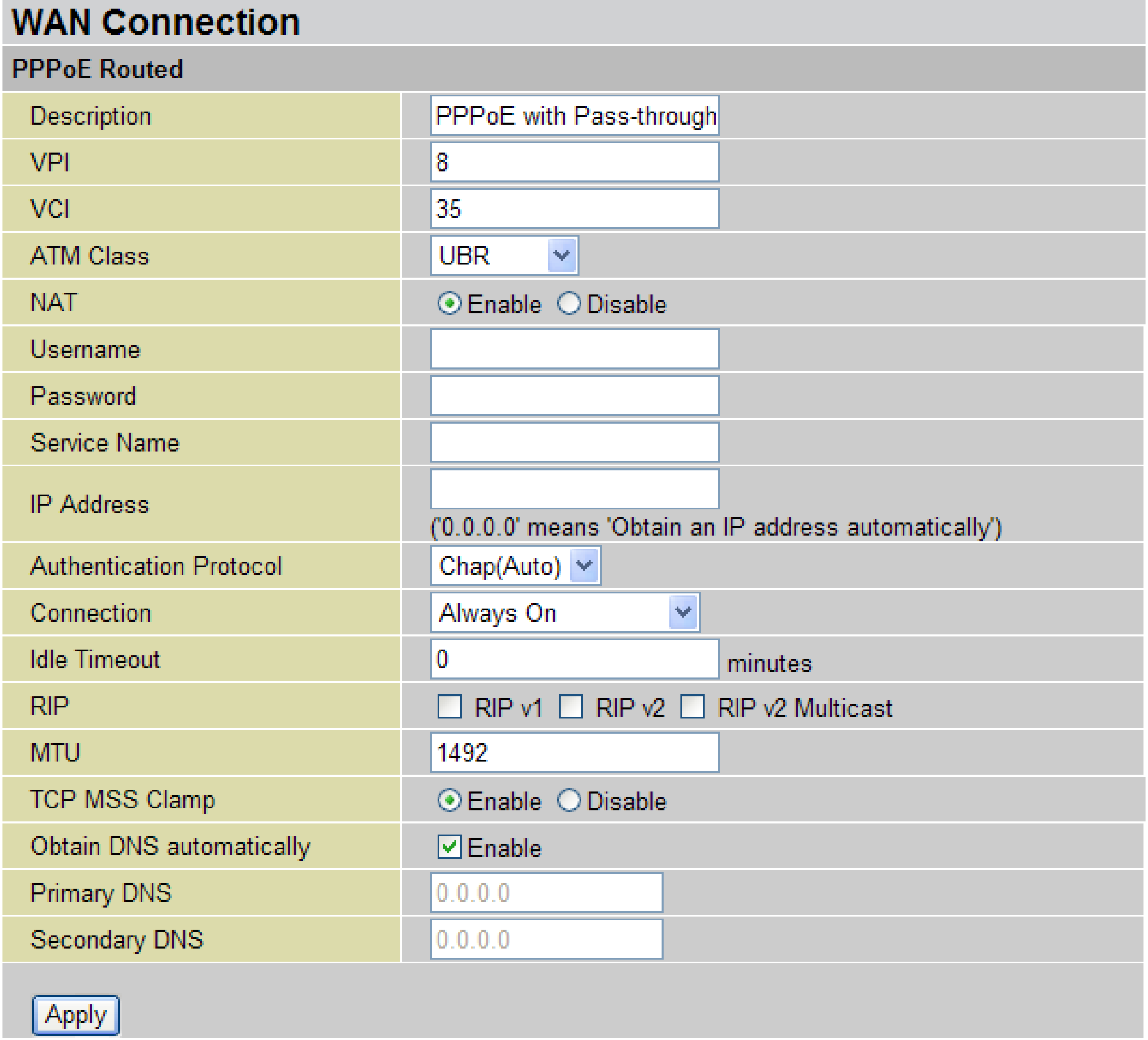


ISP

Please select the type of service you wish to create

ATM
- ○ RFC 1483 Routed
- ○ RFC 1483 Bridged
- ○ PPPoA Routed
- ○ IPoA Routed
- ○ PPPoE Routed
- ○ Multiple Session with PPPoE pass-through
- ● PPPoE Routed with Pass-through

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

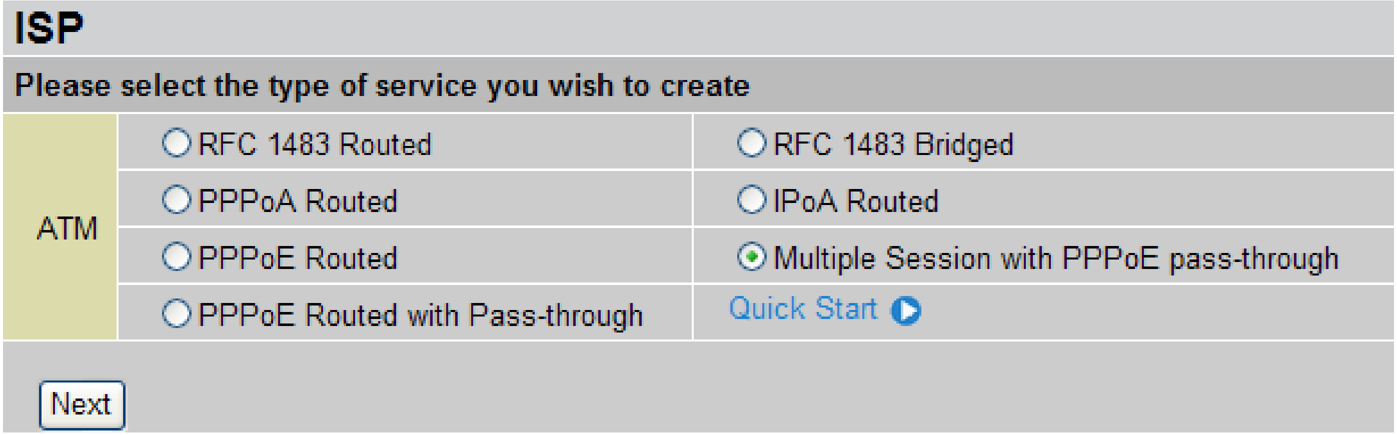
Description	PPPoE with Pass-through
VPI	8
VCI	35
ATM Class	UBR
NAT	● Enable ○ Disable
Username	
Password	
Service Name	
IP Address	('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast
MTU	1492
TCP MSS Clamp	● Enable ○ Disable
Obtain DNS automatically	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

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

Click Apply to confirm the settings.

Multiple Session with PPPoE Pass-through Connection

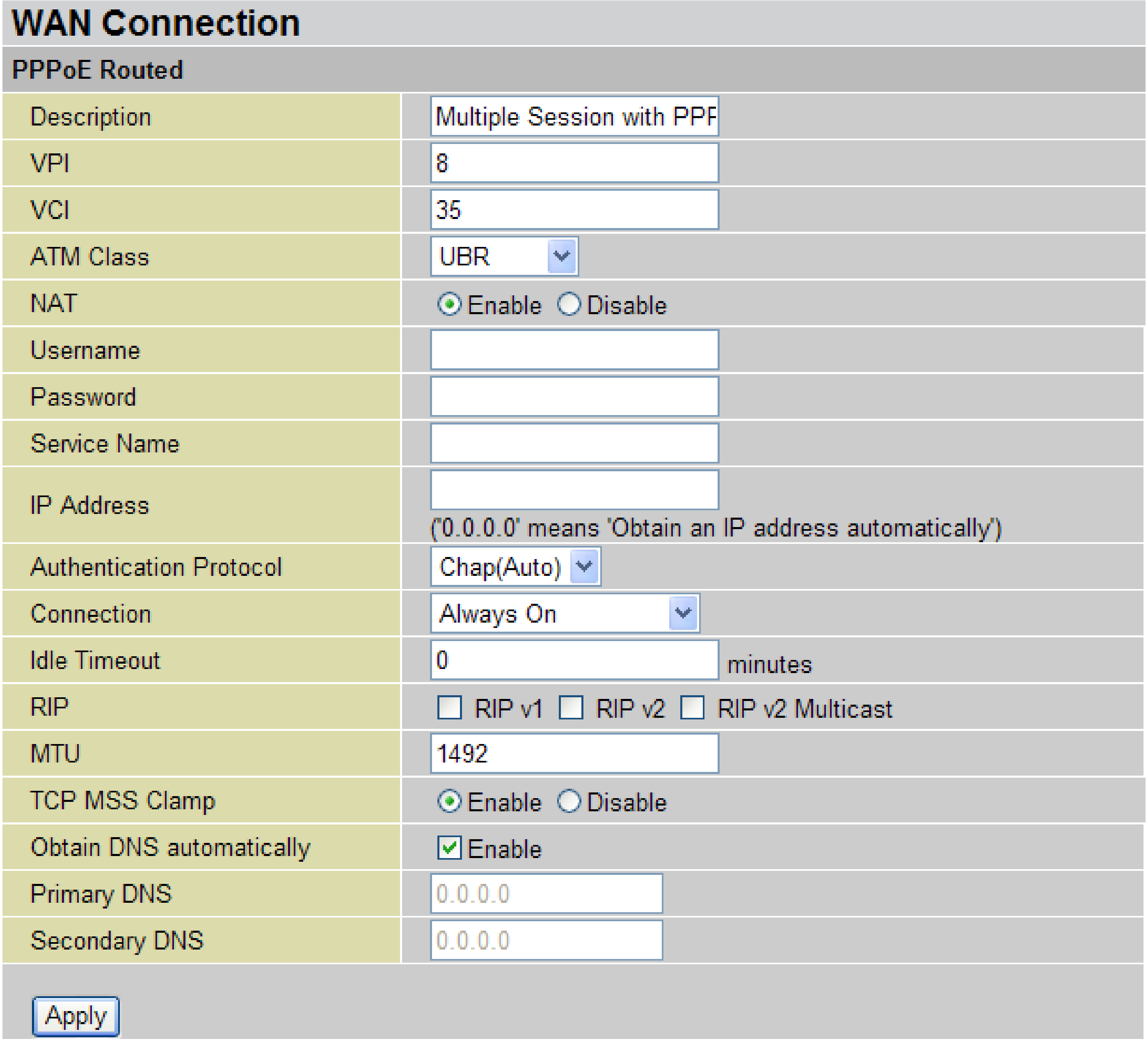
To access Multiple Session with PPPoE Pass-through Connection, press Change > Multiple Session with PPPoE pass-through.



ISP

Please select the type of service you wish to create

ATM	○ RFC 1483 Routed	○ RFC 1483 Bridged
	○ PPPoA Routed	○ IPoA Routed
	○ PPPoE Routed	● Multiple Session with PPPoE pass-through
	○ PPPoE Routed with Pass-through	Quick Start



WAN Connection

PPPoE Routed

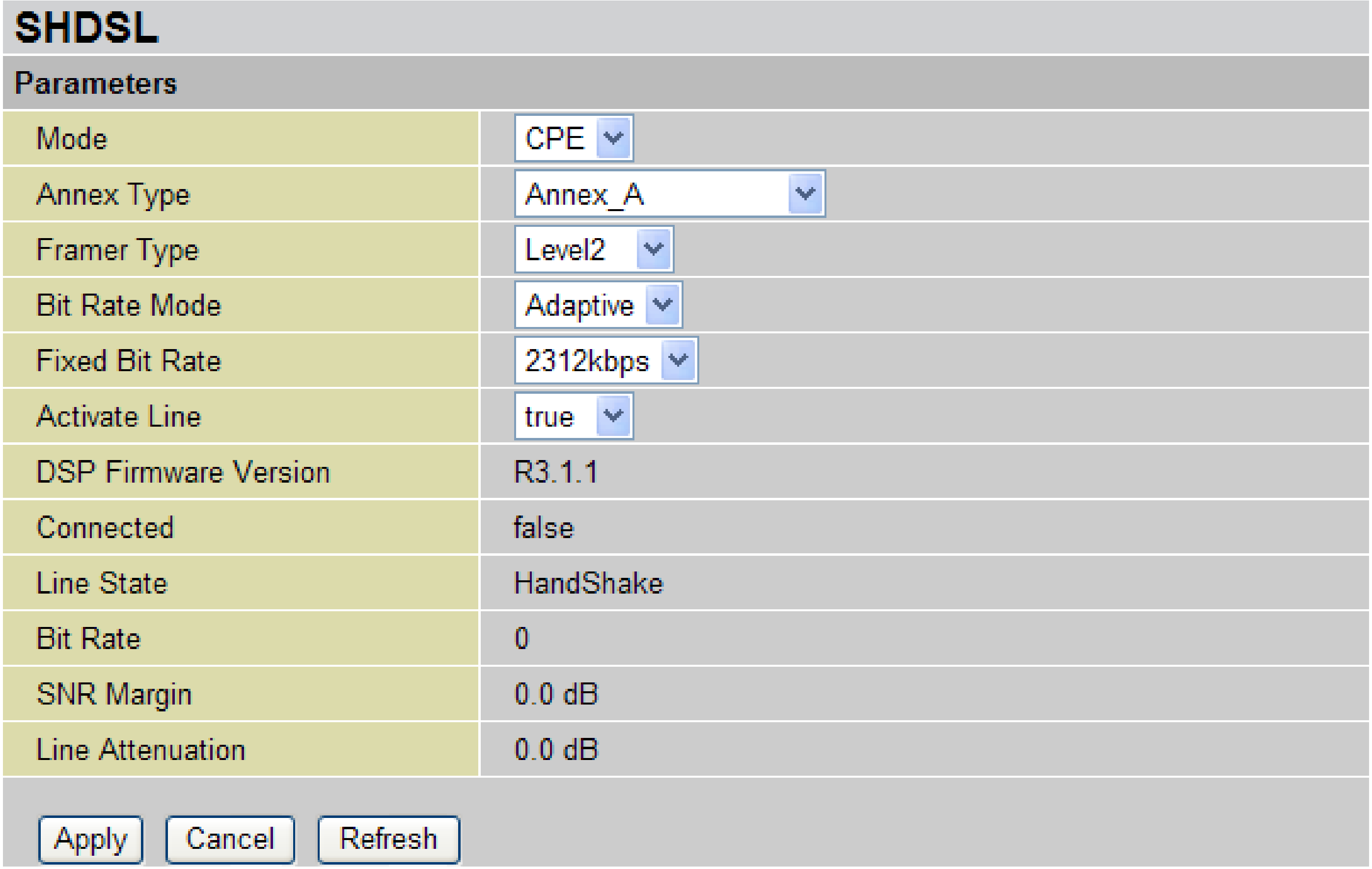
Description	Multiple Session with PPF
VPI	8
VCI	35
ATM Class	UBR
NAT	● Enable ○ Disable
Username	
Password	
Service Name	
IP Address	('0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Chap(Auto)
Connection	Always On
Idle Timeout	0 minutes
RIP	☐ RIP v1 ☐ RIP v2 ☐ RIP v2 Multicast
MTU	1492
TCP MSS Clamp	● Enable ○ Disable
Obtain DNS automatically	☑ Enable
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0

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

Click Apply to confirm the settings.

SHDSL

BiPAC 8500



Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	2312kbps
Activate Line	true
DSP Firmware Version	R3.1.1
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

Mode: The SHDSL device can operate as a CPE (Customer Premises Equipment) or CO (Central Office). Select CPE mode when the BiPAC 8500 is connected to your ISP.

Note: Back-to-back feature is a direct connection between two SHDSL devices that one is set to be CPE and the other CO by using a standard RJ-11 telephone cable.

Annex Type: It is the DSL operating mode standard. Select Annex A or Annex B to support up to 2.3Mpbs SHDSL function.

Note: Make sure that the Annex type is the same for the BiPAC 8500 and the remote router. Consult with your ISP to set the same annex for the other device.

Framer Type: The mode

Bit Rate Mode: The mode selections are Adaptive and Fixed. Selecting the Adaptive mode, the best connection rate will be automatically negotiated with the CO / ISP. Selecting the Fixed mode, the connection rate will be fixed to the specific fixed bit rate selected with the CO / ISP.

Fixed Bit Rate: Specify the fix transfer rate when Fixed Mode is selected. Specify the maximum transfer rate when Adaptive Mode is selected. Bit Rate range is 72kbps ~ 5704kbps.

Activate Line: Line active true is set by default. Select false to disable and true to enable SHDSL SHDSL connection

Note: Once Active Line is selected as false, you have to enable the Active Line to true again and click the Apply button to reactivate SHDSL connection.

DSP Firmware Version: Displays the SHDSL line code firmware version.

Connected: Displays current SHDSL line sync status.

Line State: Displays current SHDSL line status.

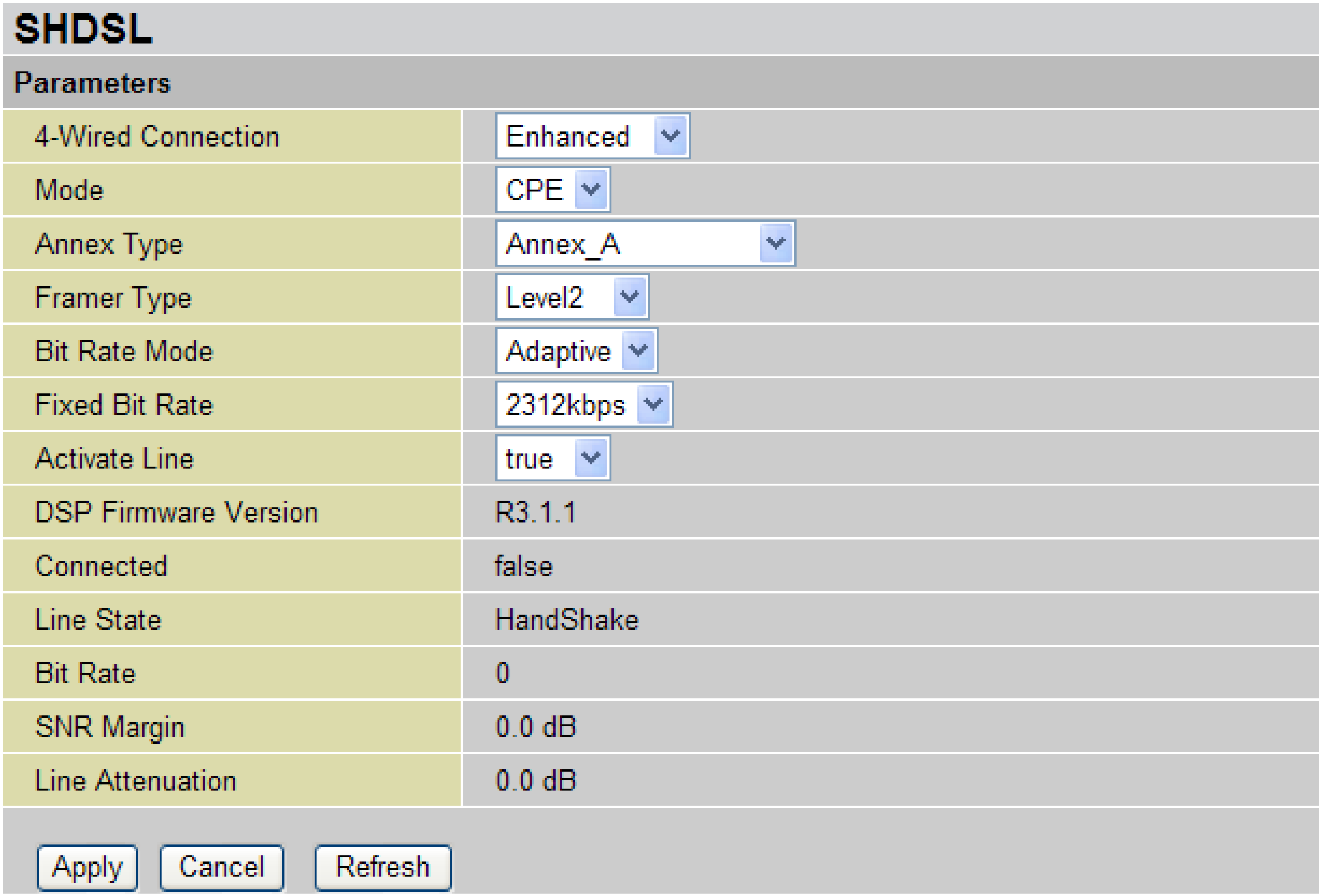
Bit Rate: Displays SHDSL line synch speed rate.

SNR Margin: Displays

Line Attenuation: Displays

Click Apply to confirm the settings.

BiPAC 8520



SHDSL

Parameters

4-Wired Connection	Enhanced
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	2312kbps
Activate Line	true
DSP Firmware Version	R3.1.1
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

4-Wired Connection: BiPAC 8520 supports 4 types of SHDSL.bis connection: **false**, **Enahnced**, **Standard** & **Sustain2W**. Select the type of SHDSL.bis connection from the 4-wired connection drop-down menu, and then press Apply to activate the configuration page.

Note: When select 2-wired mode, only Port 1 settings need to be configured and the SHDSL (RJ-11 cable) must be connected to LINE 1 on the back of the device.

Mode: The SHDSL device can function as a CPE (Customer Premises Equipment) or CO (Central Office). Select CPE mode when the BiPAC 8520 is connected to your ISP.

Note: Back-to-back feature is a direct connection between two SHDSL devices that one is set to be CPE and the other CO by using a standard RJ-11 telephone cable.

Annex Type: It is the DSL operating mode standard. Select Annex A or Annex B to support up to 2.3Mpbs SHDSL function.

Note: Make sure that the Annex type is the same for the BiPAC 8520 and the remote router. Consult with your ISP to set the same annex for the other device.

Framer Type: Packet Framing format. There are 3 types: Level2, Level1A and Level1B . Level2 is the same as ATM framing.

Bit Rate Mode: The mode selections are Adaptive and Fixed. Selecting the Adaptive mode, the best connection rate will be automatically negotiated with the CO / ISP. Selecting the Fixed mode, the connection rate will be fixed to the specific fixed bit rate selected with the CO / ISP.

Fixed Bit Rate: Specify the fix transfer rate when Fixed Mode is selected. Specify the maximum transfer rate when Adaptive Mode is selected. Bit Rate range is 72kbps ~ 5704kbps.

Activate Line: Line active true is set by default. Select false to disable and true to enable SHDSL SHDSL connection

Note: Once Active Line is selected as false, you have to enable the Active Line to true again and click the Apply button to reactivate SHDSL connection.

DSP Firmware Version: Displays the SHDSL line code firmware version.

Connected: Displays current SHDSL line sync status.

Line State: Displays current SHDSL line status.

Bit Rate: Displays SHDSL line synch speed rate.

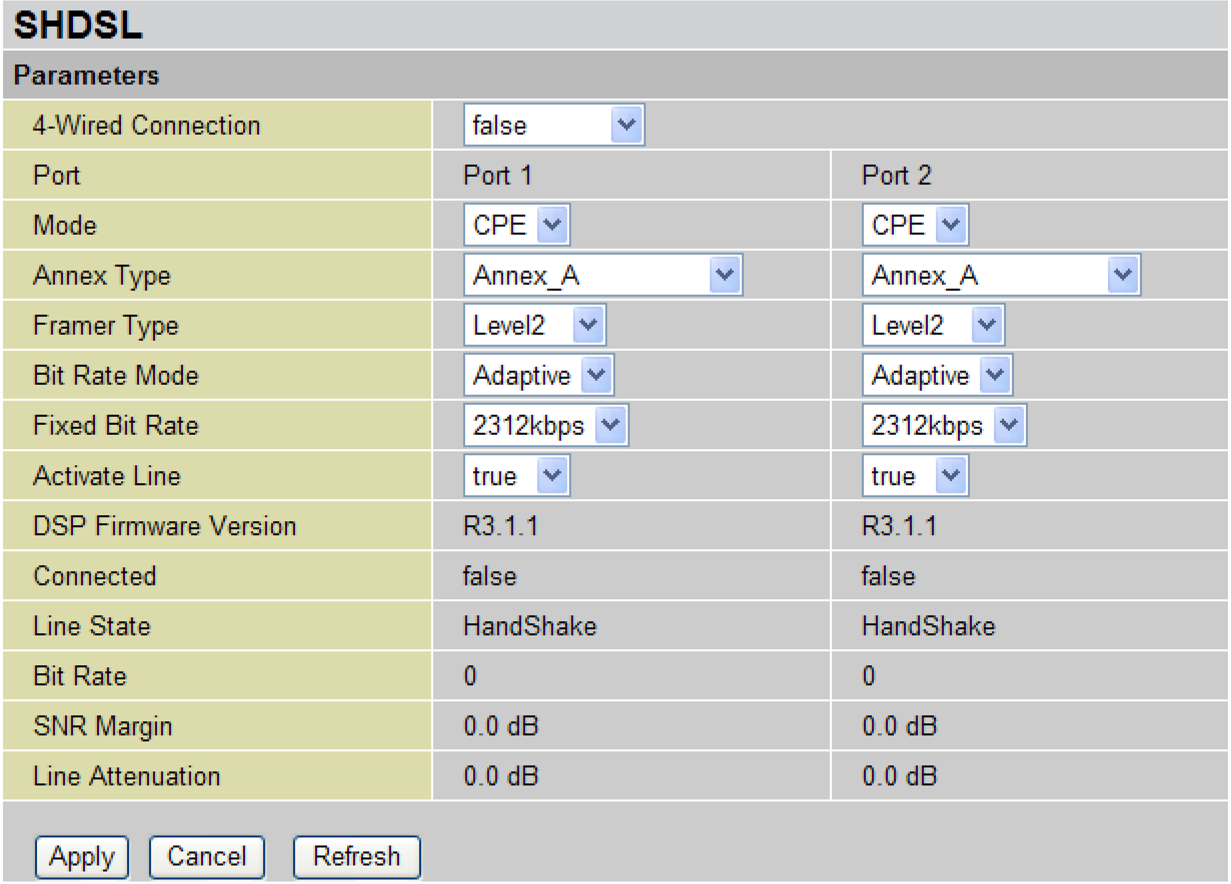
SNR Margin: Displays SNR value when line is synchronized. It indicates the signal quality; the higher the ratio, the higher signal quality it has.

Line Attenuation: Displays signal attenuation. The longer loop dostance, the larger line attenuation value is.

Click Apply to confirm the settings.

False 4-wired Connection

This mode is used when 4-wired connection is disabled.



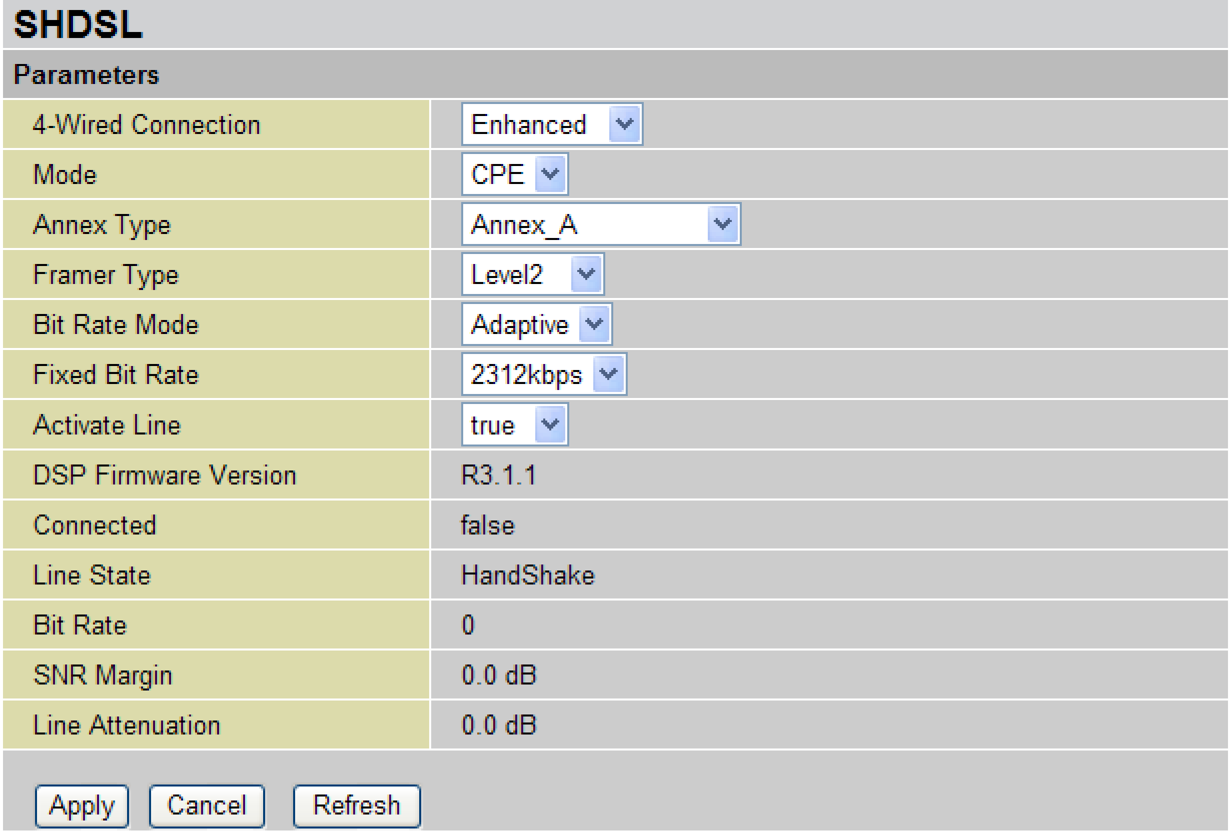
SHDSL

Parameters

4-Wired Connection	false	
Port	Port 1	Port 2
Mode	CPE	CPE
Annex Type	Annex_A	Annex_A
Framer Type	Level2	Level2
Bit Rate Mode	Adaptive	Adaptive
Fixed Bit Rate	2312kbps	2312kbps
Activate Line	true	true
DSP Firmware Version	R3.1.1	R3.1.1
Connected	false	false
Line State	HandShake	HandShake
Bit Rate	0	0
SNR Margin	0.0 dB	0.0 dB
Line Attenuation	0.0 dB	0.0 dB

Enhanced 4-wired Connection

Conexant enhanced 4-wired mode and compliant with Conexant Legacy codes.



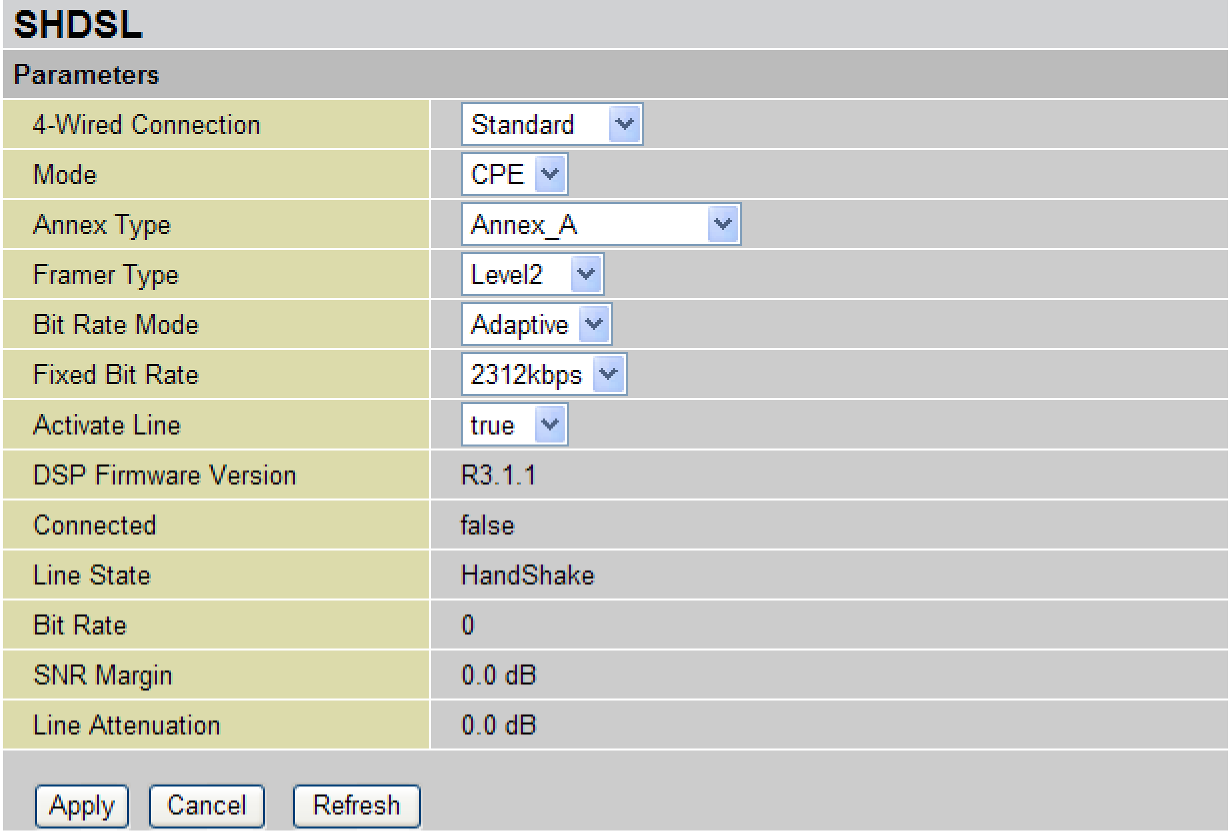
SHDSL

Parameters

4-Wired Connection	Enhanced
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	2312kbps
Activate Line	true
DSP Firmware Version	R3.1.1
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

Standard 4-wired Connection

The 4-wired handshaking procedure that is compliant with ITU-T standard.



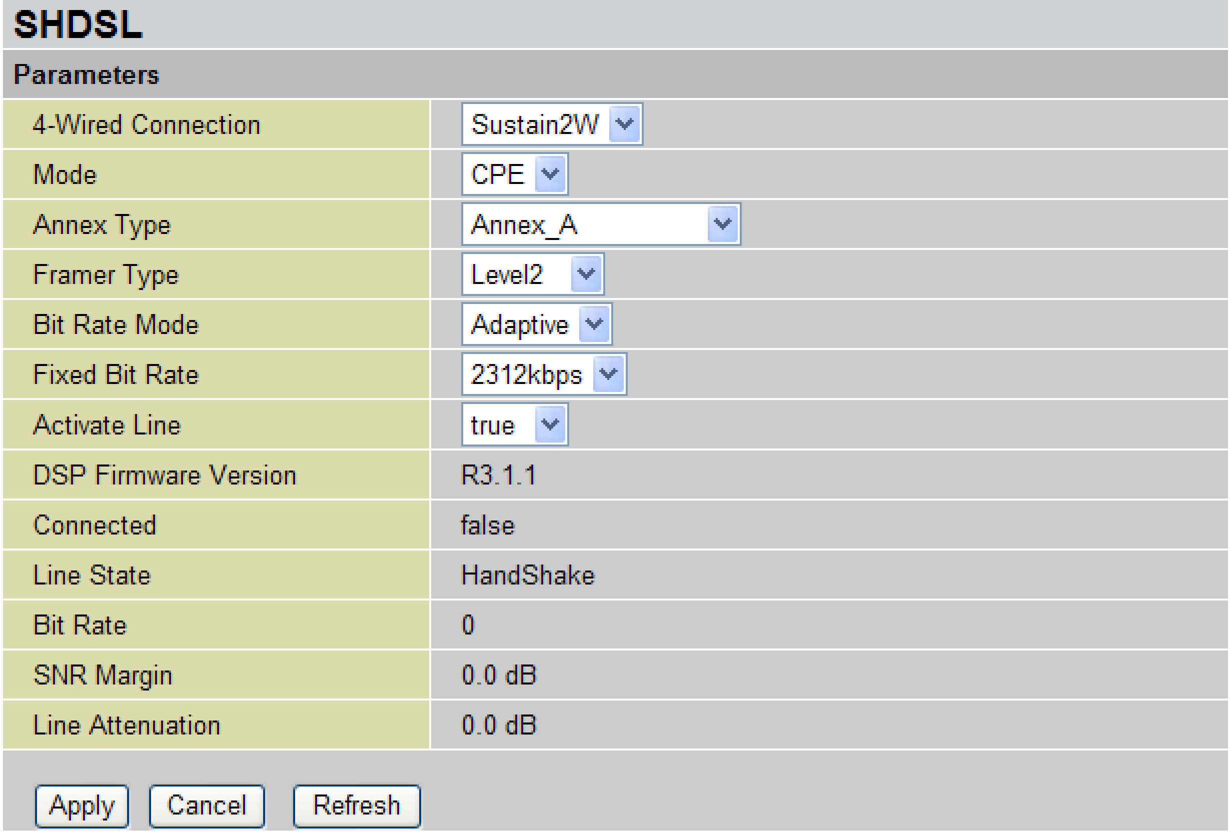
SHDSL

Parameters

4-Wired Connection	Standard
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	2312kbps
Activate Line	true
DSP Firmware Version	R3.1.1
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

Sustain2W 4-wired Connection

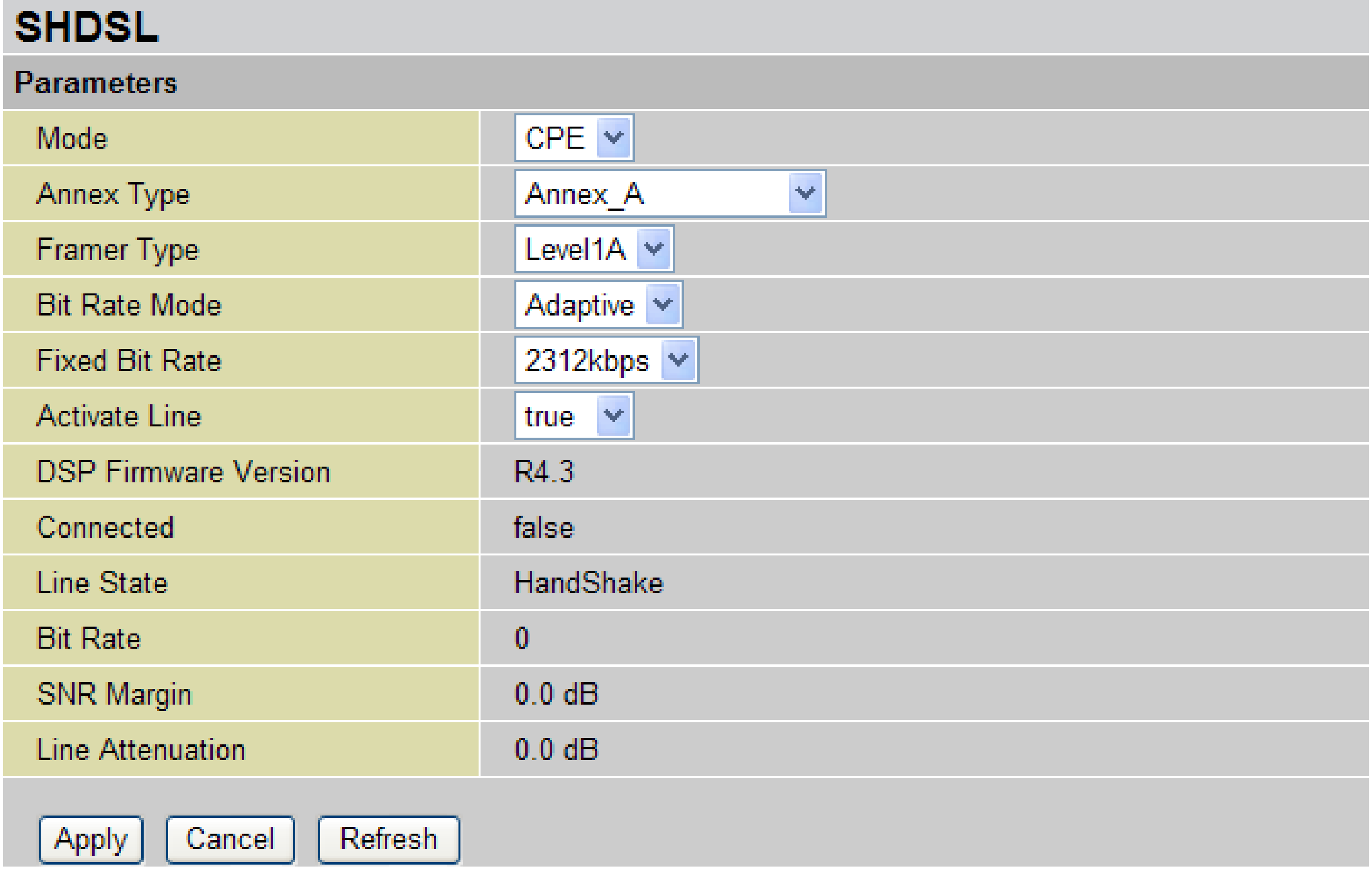
This mode is used to auto detect whether the device uses 2-wired connection or 4-wired connection.



SHDSL

Parameters

4-Wired Connection	Sustain2W
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	2312kbps
Activate Line	true
DSP Firmware Version	R3.1.1
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB



SHDSL

Parameters

Mode	CPE
Annex Type	Annex_A
Framer Type	Level1A
Bit Rate Mode	Adaptive
Fixed Bit Rate	2312kbps
Activate Line	true
DSP Firmware Version	R4.3
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

Mode: The SHDSL device can operate as a CPE (Customer Premises Equipment) or CO (Central Office). Select CPE mode when the BiPAC 8500 is connected to your ISP.

Note: Back-to-back feature is a direct connection between two SHDSL devices that one is set to be CPE and the other CO by using a standard RJ-11 telephone cable.

Annex Type: It is the DSL operating mode standard. Select Annex A or Annex B to support up to 2.3Mpbs SHDSL function.

Note: Make sure that the Annex type is the same for the BiPAC 8501 and the remote router. Consult with your ISP to set the same annex for the other device.

Framer Type: Packet Framing format. There are 3 types: Level2, Level1A and Level1B. Level2 is the same as ATM framing.

Bit Rate Mode: The mode selections are Adaptive and Fixed. Selecting the Adaptive mode, the best connection rate will be automatically negotiated with the CO / ISP. Selecting the Fixed mode, the connection rate will be fixed to the specific fixed bit rate selected with the CO / ISP.

Fixed Bit Rate: Specify the fix transfer rate when Fixed Mode is selected. Specify the maximum transfer rate when Adaptive Mode is selected. Bit Rate range is 72kbps ~ 5704kbps.

Activate Line: Line active true is set by default. Select false to disable and true to enable SHDSL SHDSL connection

Note: Once Active Line is selected as false, you have to enable the Active Line to true again and click the Apply button to reactivate SHDSL connection.

DSP Firmware Version: Displays the SHDSL line code firmware version.

Connected: Displays current SHDSL line sync status.

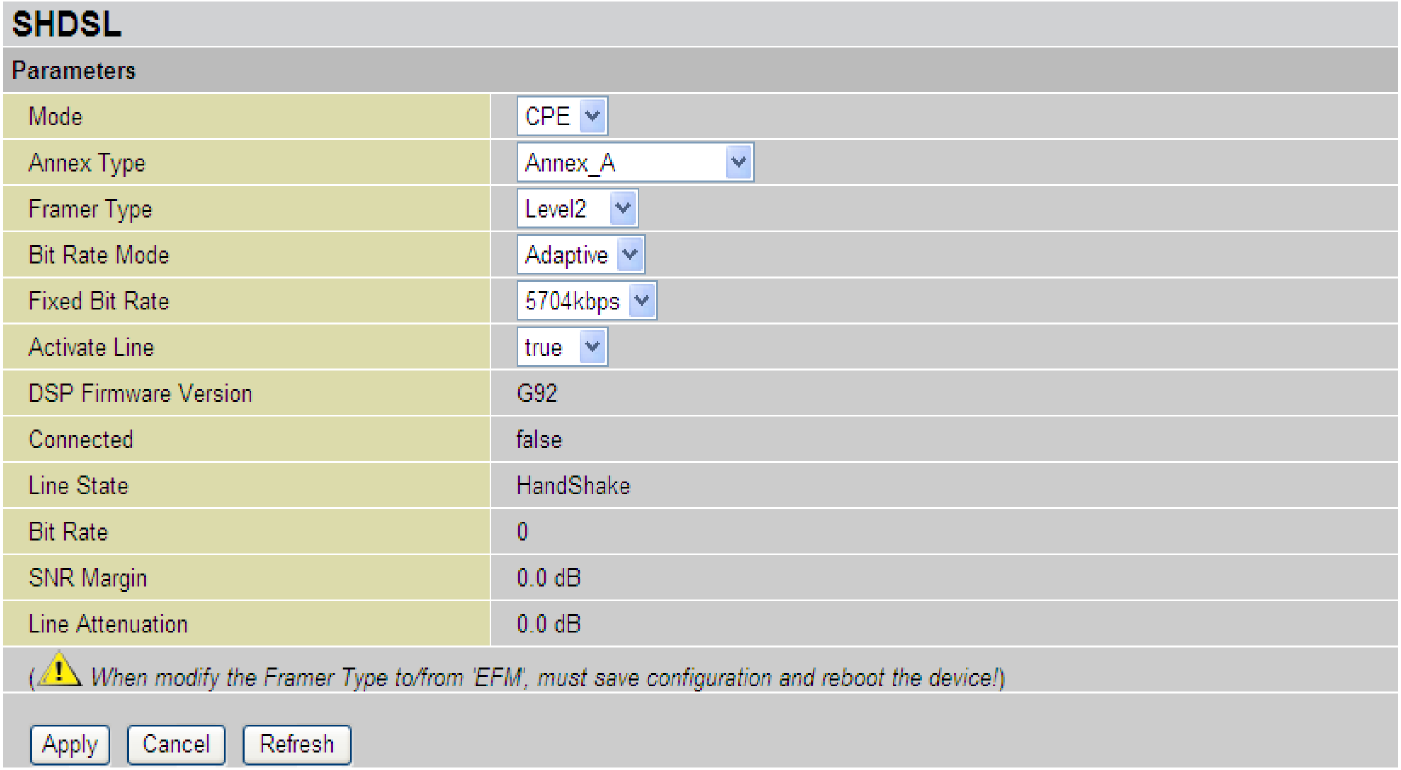
Line State: Displays current SHDSL line status.

Bit Rate: Displays SHDSL line synch speed rate.

SNR Margin: Displays SNR value when line is synchronized. It indicates the signal quality; the higher the ratio, the higher signal quality it has.

Line Attenuation: Displays signal attenuation. The longer loop dostance, the larger line attenuation value is.

Click Apply to confirm the settings.



SHDSL

Parameters

Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	5704kbps
Activate Line	true
DSP Firmware Version	G92
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

(⚠ *When modify the Framer Type to/from 'EFM', must save configuration and reboot the device!*)

Mode: The SHDSL device can operate as a CPE (Customer Premises Equipment) or CO (Central Office). Select CPE mode when the BiPAC 8500 is connected to your ISP.

Note: Back-to-back feature is a direct connection between two SHDSL devices that one is set to be CPE and the other CO by using a standard RJ-11 telephone cable.

Annex Type: It is the DSL operating mode standard. Select Annex A or Annex B to support up to 2.3Mpbs SHDSL function.

Note: Make sure that the Annex type is the same for the BiPAC 8501R2 and the remote router. Consult with your ISP to set the same annex for the other device.

Framer Type: Packet Framing format. There are 4 types: Level2, Level1A , Level1B and EFM. Level2 is the same as ATM framing.

Bit Rate Mode: The mode selections are Adaptive and Fixed. Selecting the Adaptive mode, the best connection rate will be automatically negotiated with the CO / ISP. Selecting the Fixed mode, the connection rate will be fixed to the specific fixed bit rate selected with the CO / ISP.

Fixed Bit Rate: Specify the fix transfer rate when Fixed Mode is selected. Specify the maximum transfer rate when Adaptive Mode is selected. Bit Rate range is 72kbps ~ 5704kbps.

Activate Line: Line active true is set by default. Select false to disable and true to enable SHDSL SHDSL connection

Note: Once Active Line is selected as false, you have to enable the Active Line to true again and click the Apply button to reactivate SHDSL connection.

DSP Firmware Version: Displays the SHDSL line code firmware version.

Connected: Displays current SHDSL line sync status.

Line State: Displays current SHDSL line status.

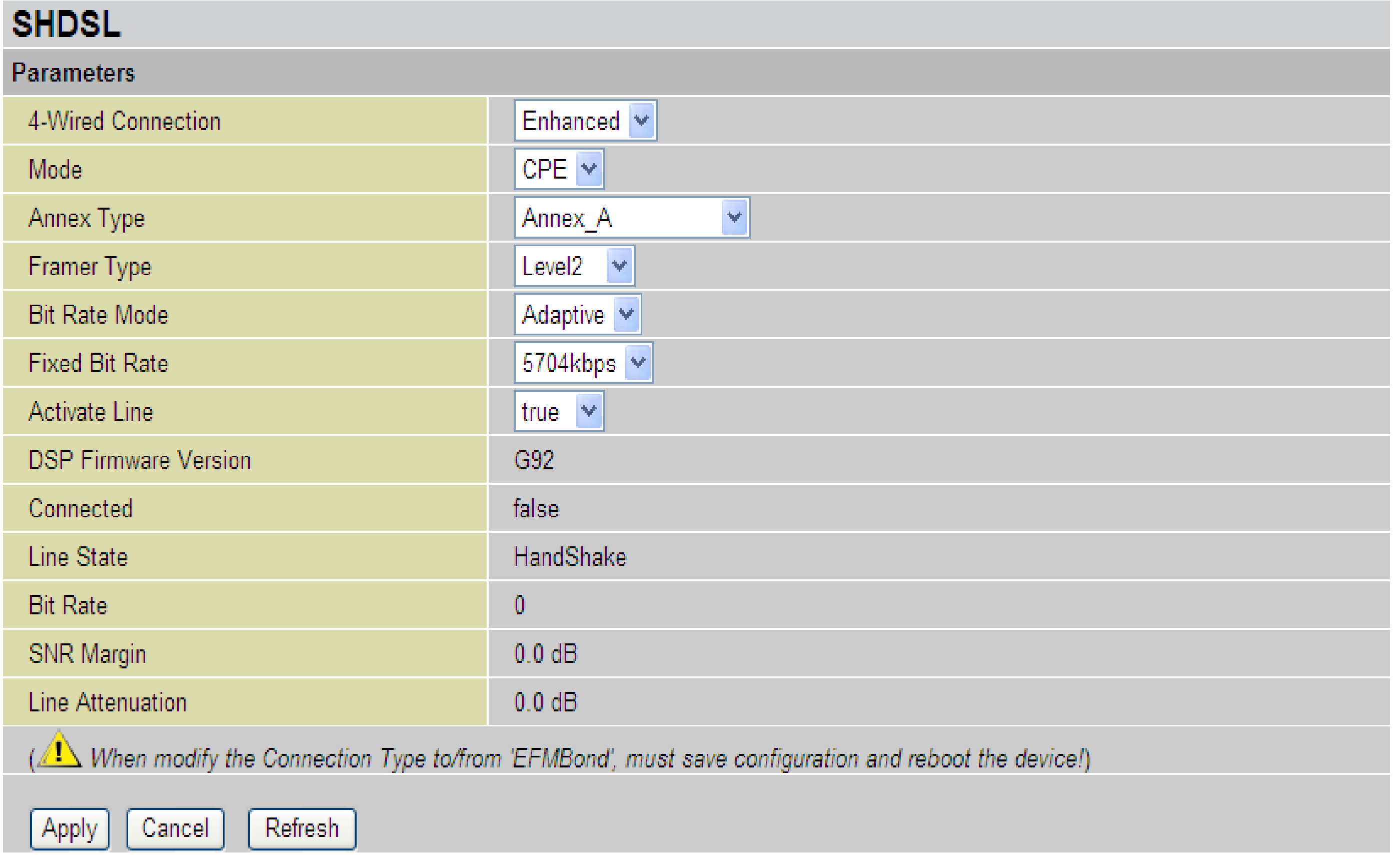
Bit Rate: Displays SHDSL line synch speed rate.

SNR Margin: Displays SNR value when line is synchronized. It indicates the signal quality; the higher the ratio, the higher signal quality it has.

Line Attenuation: Displays signal attenuation. The longer loop dostance, the larger line attenuation value is.

Click Apply to confirm the settings.

BiPAC 8521



SHDSL

Parameters

4-Wired Connection	Enhanced
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	5704kbps
Activate Line	true
DSP Firmware Version	G92
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

(⚠ *When modify the Connection Type to/from 'EFMBond', must save configuration and reboot the device!*)

Standard 4-wired connection: BiPAC 8521 supports 4 types of SHDSL.bis connection: **False, Enahnced, Standard&EFMBond**. Select the type of SHDSL.bis connection from the 4-wired connection drop-down menu, and then press Apply to activate the configuration page.

Note: When select 2-wire mode, only Port 1 settings need to be configured and the SHDSL (RJ-11 cable) must be connected to LINE 1 on the back of the device.

Mode: The SHDSL device can operate as a CPE (Customer Premises Equipment) or CO (Central Office). Select CPE mode when the BiPAC 8500 is connected to your ISP.

Note: Back-to-back feature is a direct connection between two SHDSL devices that one is set to be CPE and the other CO by using a standard RJ-11 telephone cable.

Annex Type: It is the DSL operating mode standard. Select Annex A or Annex B to support up to 2.3Mpbs SHDSL function.

Note: Make sure that the Annex type is the same for the BiPAC 8521 and the remote router. Consult with your ISP to set the same annex for the other device.

Framer Type: Packet Framing format. There are 4 types: Level2, Level1A, Level1B and EFM. Level2 is the same as ATM framing; EFM is EFM framing.

Bit Rate Mode: The mode selections are Adaptive and Fixed. Selecting the Adaptive mode, the best connection rate will be automatically negotiated with the CO / ISP. Selecting the Fixed mode, the connection rate will be fixed to the specific fixed bit rate selected with the CO / ISP.

Fixed Bit Rate: Specify the fix transfer rate when Fixed Mode is selected. Specify the maximum transfer rate when Adaptive Mode is selected. Bit Rate range is 72kbps ~ 5704kbps.

Activate Line: Line active true is set by default. Select false to disable and true to enable SHDSL SHDSL connection

Note: Once Active Line is selected as false, you have to enable the Active Line to true again and click the Apply button to reactivate SHDSL connection.

DSP Firmware Version: Displays the SHDSL line code firmware version.

Connected: Displays current SHDSL line sync status.

Line State: Displays current SHDSL line status.

Bit Rate: Displays SHDSL line synch speed rate.

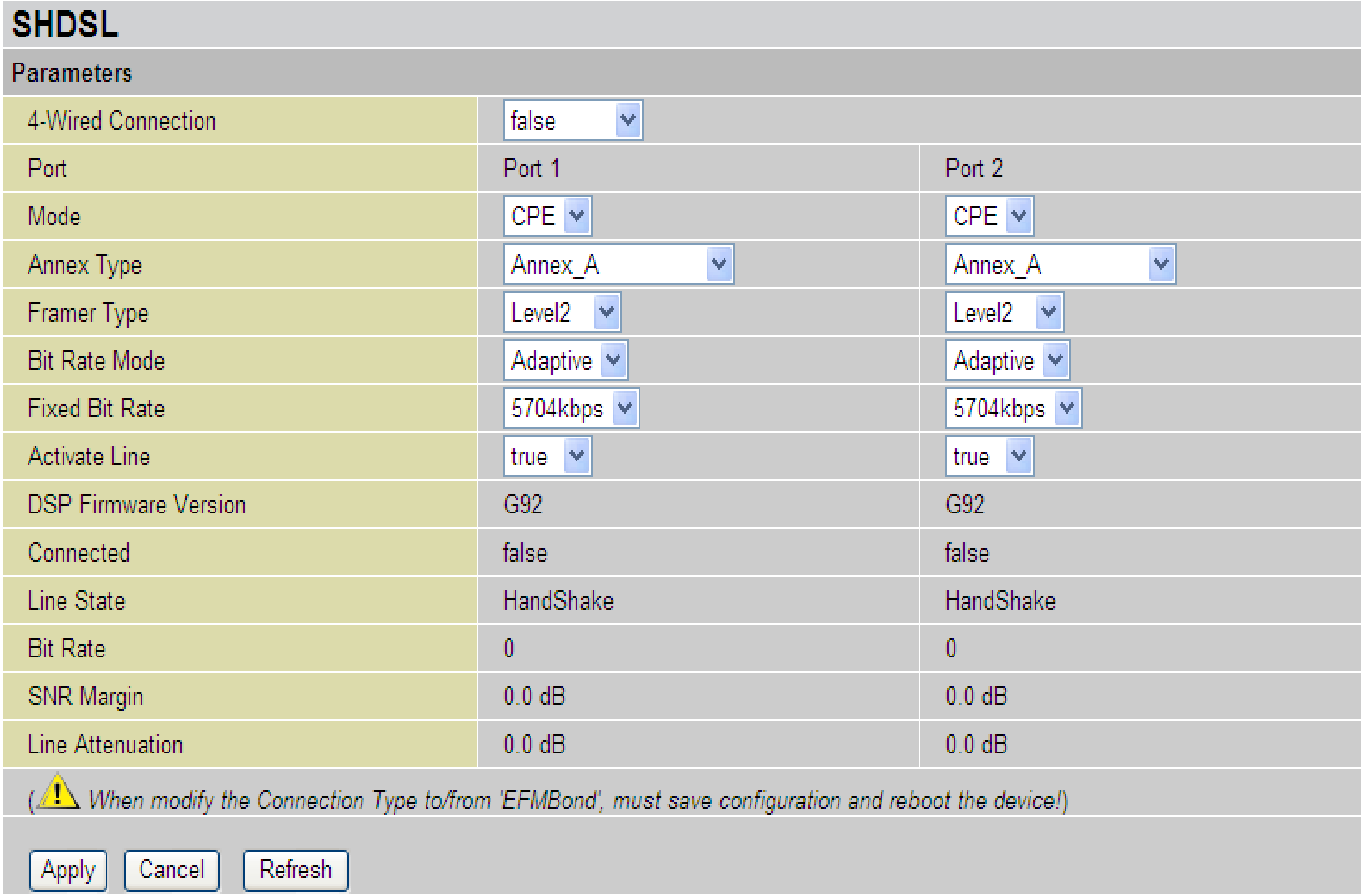
SNR Margin: Displays SNR value when line is synchronized. It indicates the signal quality; the higher the ratio, the higher signal quality it has.

Line Attenuation: Displays signal attenuation. The longer loop dostance, the larger line attenuation value is.

Click Apply to confirm the settings.

False 4-wired Connection

This mode is used when 4-wired connection is disabled.



SHDSL

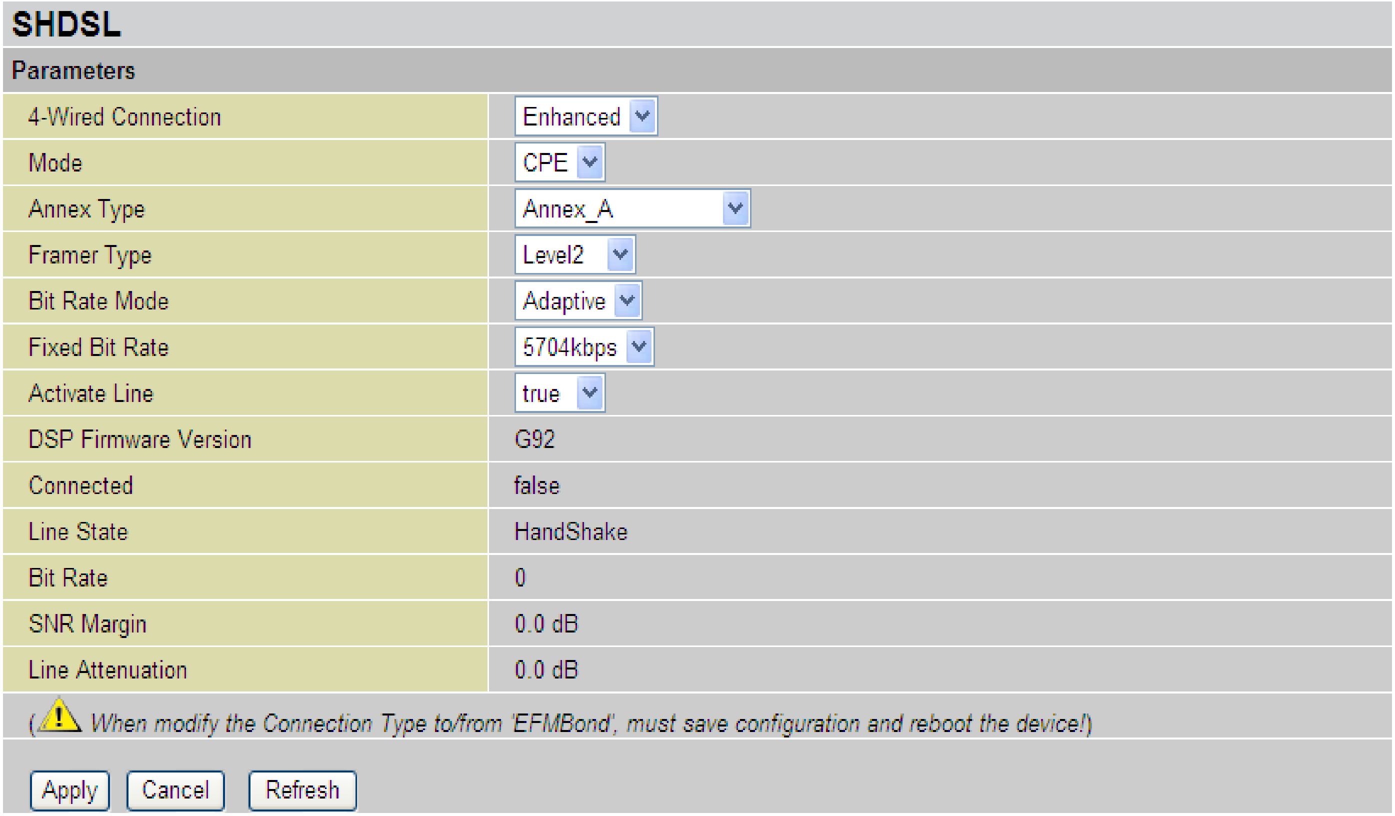
Parameters

4-Wired Connection	false	
Port	Port 1	Port 2
Mode	CPE	CPE
Annex Type	Annex_A	Annex_A
Framer Type	Level2	Level2
Bit Rate Mode	Adaptive	Adaptive
Fixed Bit Rate	5704kbps	5704kbps
Activate Line	true	true
DSP Firmware Version	G92	G92
Connected	false	false
Line State	HandShake	HandShake
Bit Rate	0	0
SNR Margin	0.0 dB	0.0 dB
Line Attenuation	0.0 dB	0.0 dB

(⚠ *When modify the Connection Type to/from 'EFMBond', must save configuration and reboot the device!*)

Enhanced 4-wired Connection

Conexant enhanced 4-wired mode and compliant with Conexant Legacy codes.



SHDSL

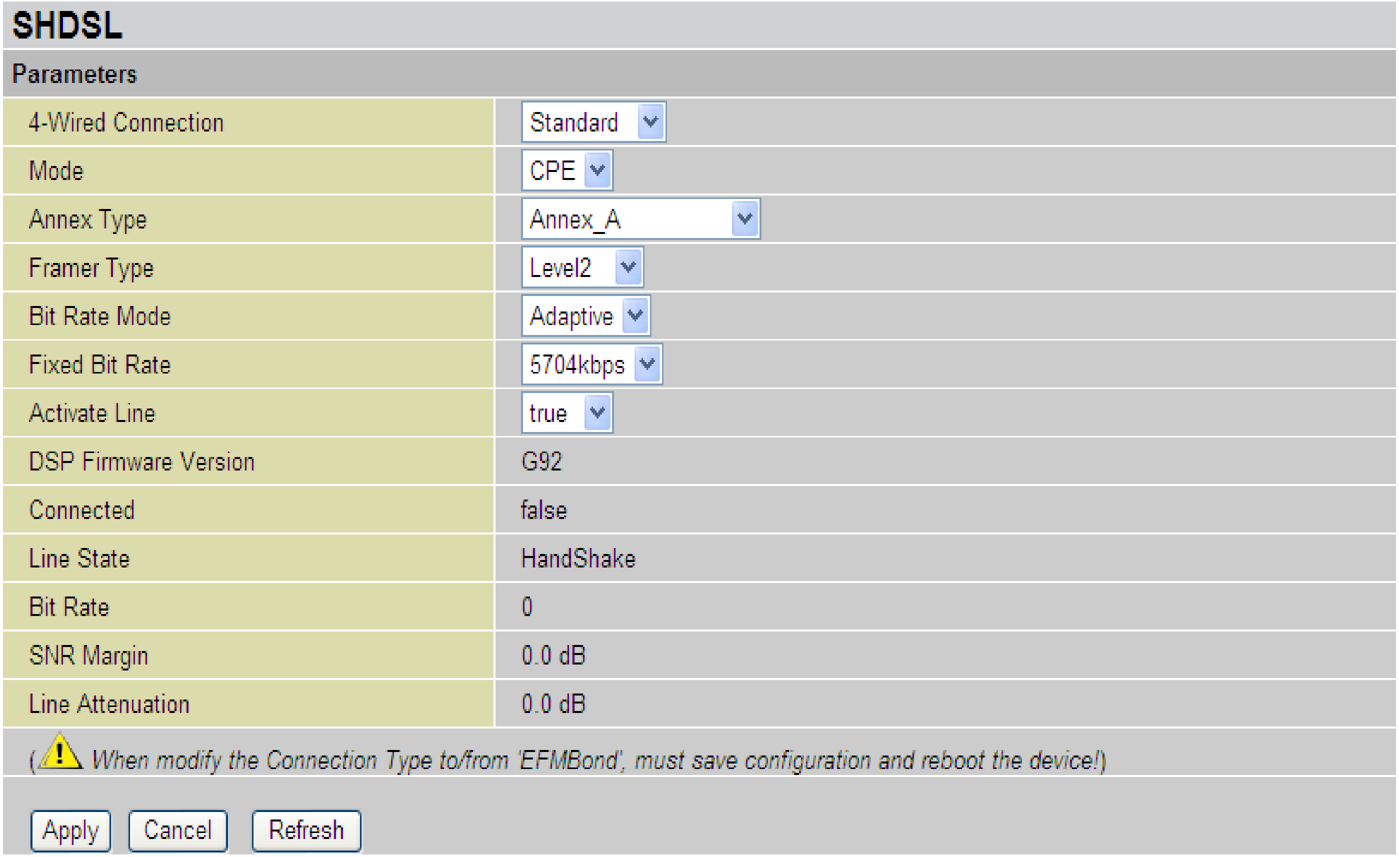
Parameters

4-Wired Connection	Enhanced
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	5704kbps
Activate Line	true
DSP Firmware Version	G92
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

(⚠ *When modify the Connection Type to/from 'EFMBond', must save configuration and reboot the device!*)

Standard 4-wired Connection

The 4-wired handshaking procedure that is compliant with ITU-T standard.



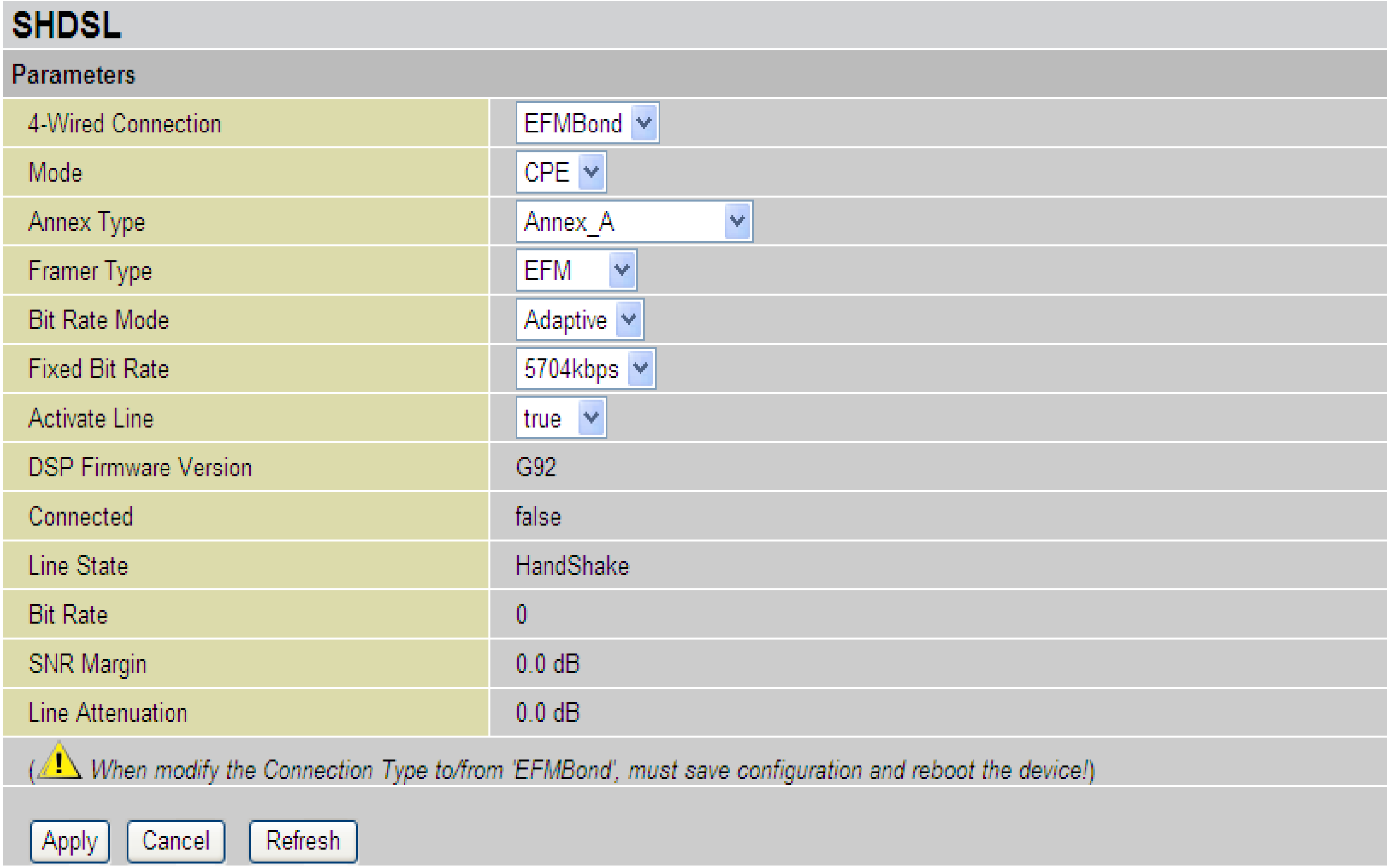
SHDSL

Parameters

4-Wired Connection	Standard
Mode	CPE
Annex Type	Annex_A
Framer Type	Level2
Bit Rate Mode	Adaptive
Fixed Bit Rate	5704kbps
Activate Line	true
DSP Firmware Version	G92
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

(⚠ *When modify the Connection Type to/from 'EFMBond', must save configuration and reboot the device!*)

EFMBond 4-wired Connection



SHDSL

Parameters

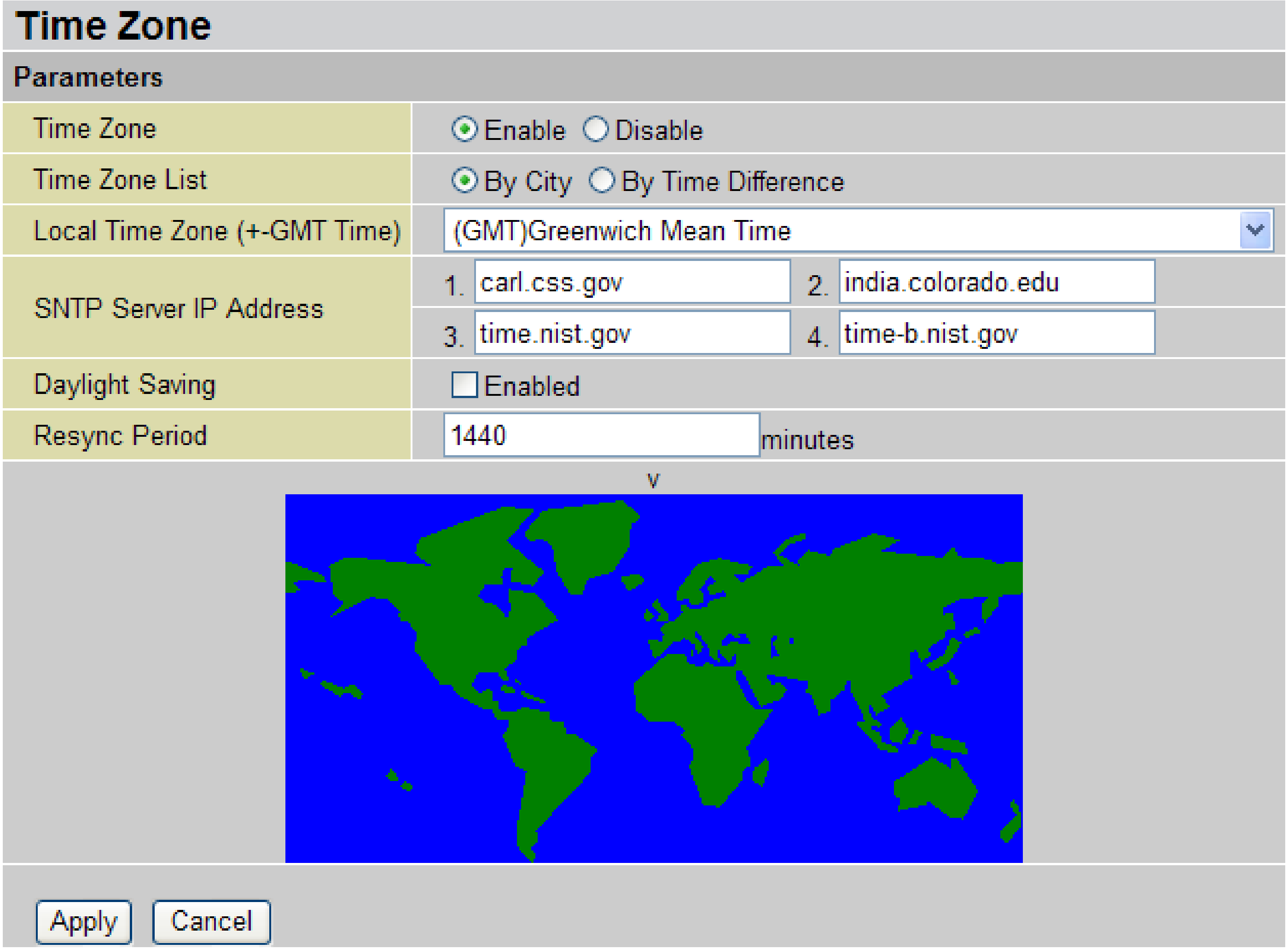
4-Wired Connection	EFMBond
Mode	CPE
Annex Type	Annex_A
Framer Type	EFM
Bit Rate Mode	Adaptive
Fixed Bit Rate	5704kbps
Activate Line	true
DSP Firmware Version	G92
Connected	false
Line State	HandShake
Bit Rate	0
SNR Margin	0.0 dB
Line Attenuation	0.0 dB

(⚠ When modify the Connection Type to/from 'EFMBond', must save configuration and reboot the device!)

System

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

Time Zone



Time Zone

Parameters

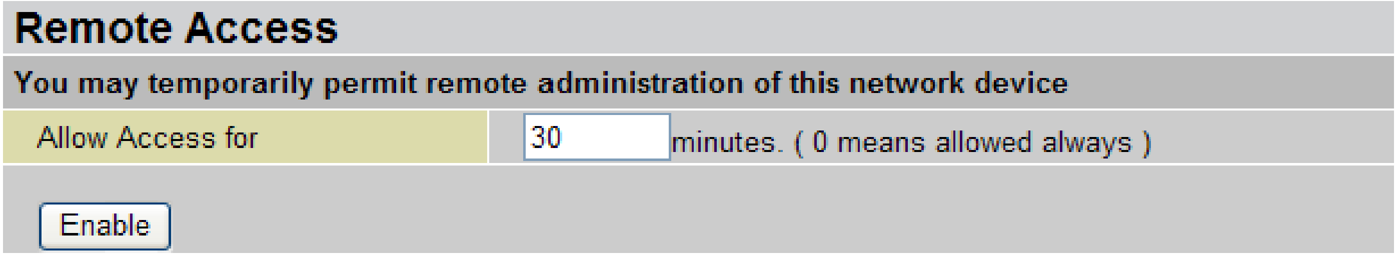
Time Zone	● Enable ○ Disable
Time Zone List	● By City ○ By Time Difference
Local Time Zone (+-GMT Time)	(GMT)Greenwich Mean Time
SNTP Server IP Address	1. carl.css.gov 2. india.colorado.edu 3. time.nist.gov 4. time-b.nist.gov
Daylight Saving	☐ Enabled
Resync Period	1440 minutes

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 from the drop down menu. To apply the selected local time zone, check 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 drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

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

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days. The default value is set at 1440 minutes.

Remote Access



Remote Access

You may temporarily permit remote administration of this network device

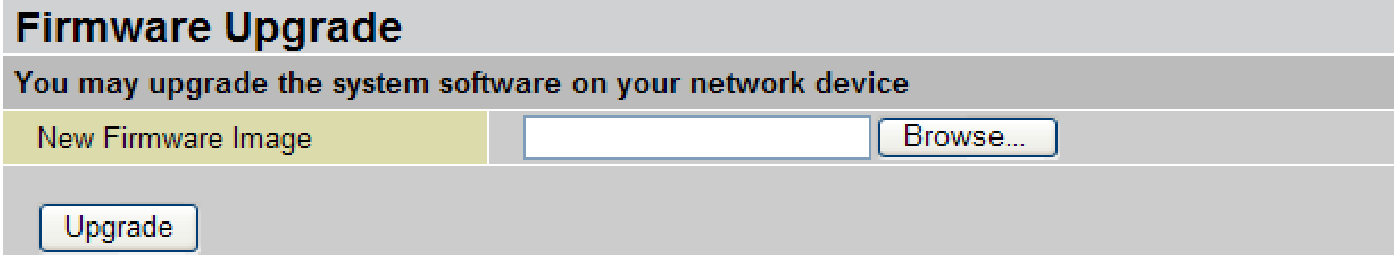
Allow Access for 30 minutes. (0 means allowed always)

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

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

Firmware Upgrade

Your router’s firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.



Firmware Upgrade

You may upgrade the system software on your network device

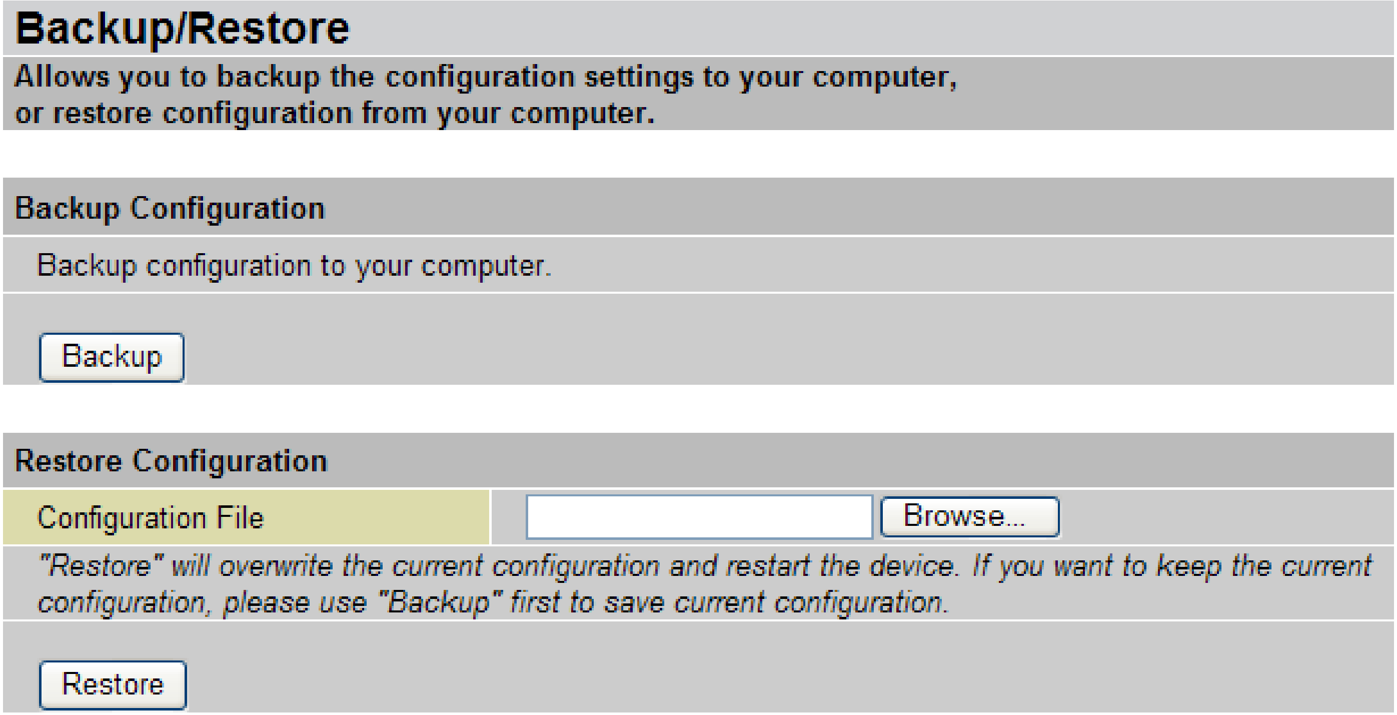
New Firmware Image: Click on Browse button to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware to your router.

Warning

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

Backup / Restore

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



Backup/Restore

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

Backup Configuration

Backup configuration to your computer.

Restore Configuration

Configuration File

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

Backup Configuration

Press Backup to select where on your local PC you want to store your setting file. You may also change the name of the file if you wish to keep multiple backups.

Restore Configuration

Press Browse to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router firmware. Settings files saved to your PC should not be manually edited in any way.

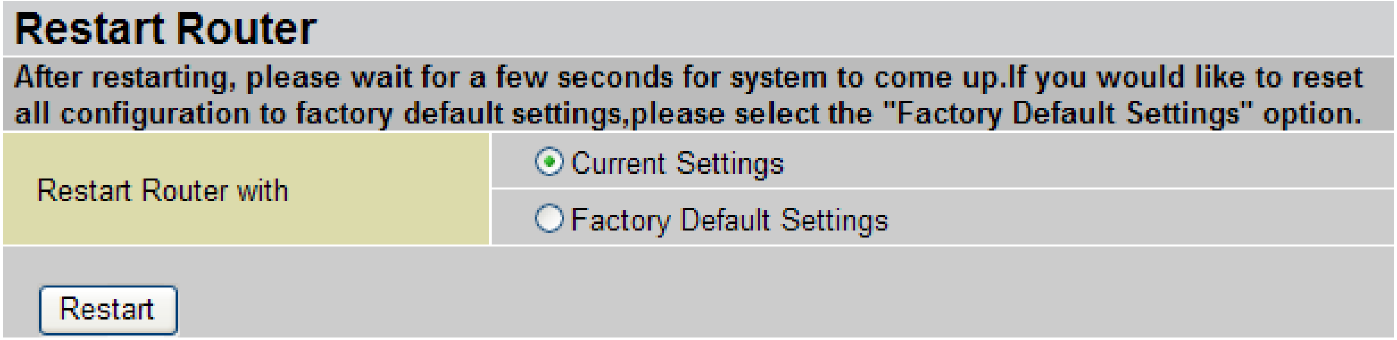
After selecting the settings file you wish to use, press Restore will load those settings into the router.

Note: Do NOT perform any more actions while the device is restoring.

Restart

There are two options for you to choose from before restarting the your 85xx devices. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.

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.



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

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

After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait for several minutes to let the selected setting applied to the system.

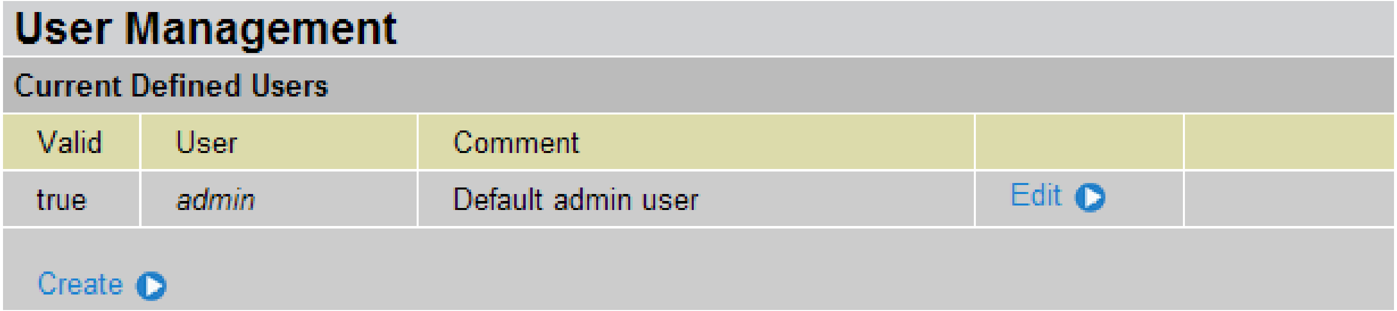
Note: Do NOT perform any more actions while the device is being restarted.

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

User Management

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system.

This feature allows you to set up multiple user accounts which contains a unique password of its own. In addition, you can also edit any existing user accounts or add new users to allow access to the device configuration interface.



User Management

Current Defined Users

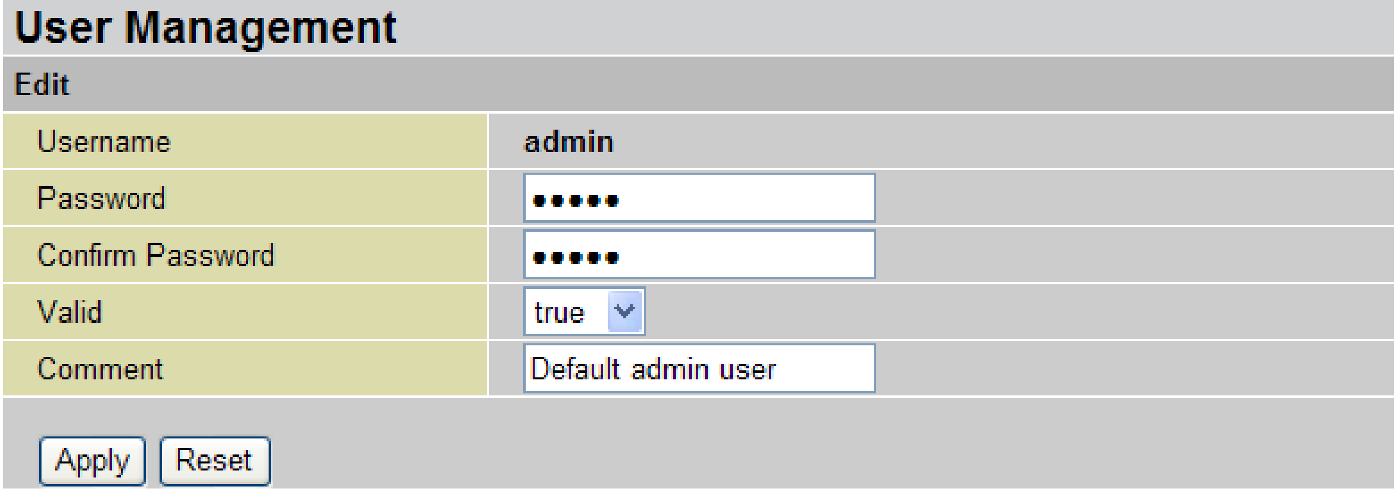
Valid	User	Comment		
true	*admin*	Default admin user	Edit	

Screen1

Edit Account Information

You can change the informations of any account whether the account is active or valid.

1. To edit an account, click on the Edit radio button of the account you want to edit.
2. On the Edit screen, delete the information to be edited and replace it with the new one.



User Management

Edit

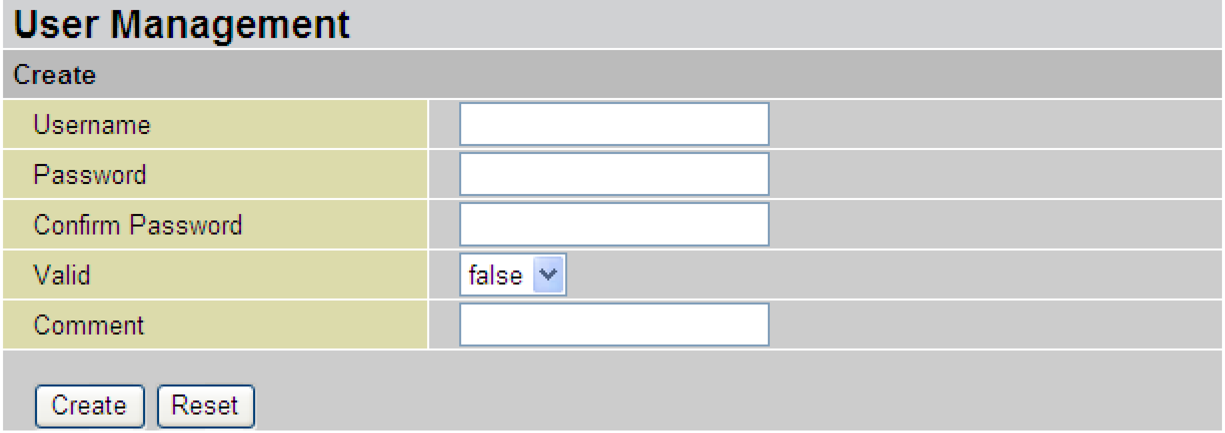
Username	admin
Password	●●●●●
Confirm Password	●●●●●
Valid	true
Comment	Default admin user

3. When it is done, simply click on the Apply button to save your changes.

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

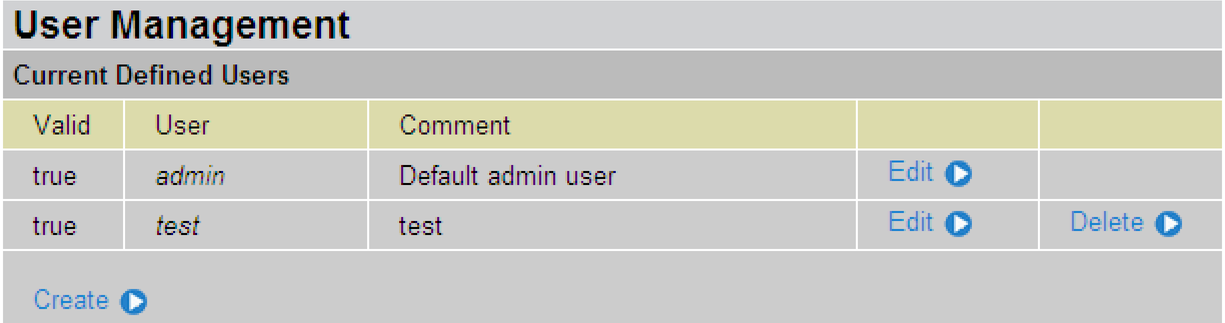
Add an Account

1. In Screen 1, click Create, then the user creating page appears. In this page select true or false from the Valid drop-down menu, fill in all the information: User name, Comment (optional), Password, Confirm Password.



Username	
Password	
Confirm Password	
Valid	false
Comment	

2. When it is done, click the Create button.

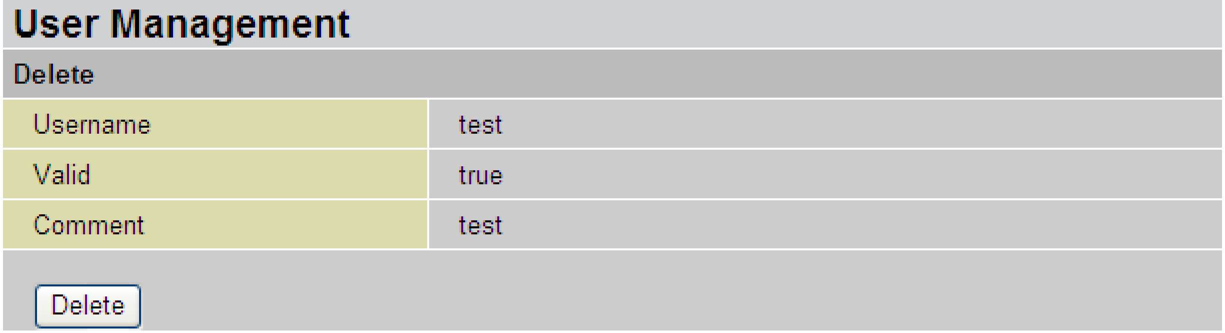


Valid	User	Comment		
true	*admin*	Default admin user	Edit	
true	*test*	test	Edit	Delete

Delete a user account

1. Check the Delete beside the account you want to delete.

2. Then click the Delete button to confirm the deletion.



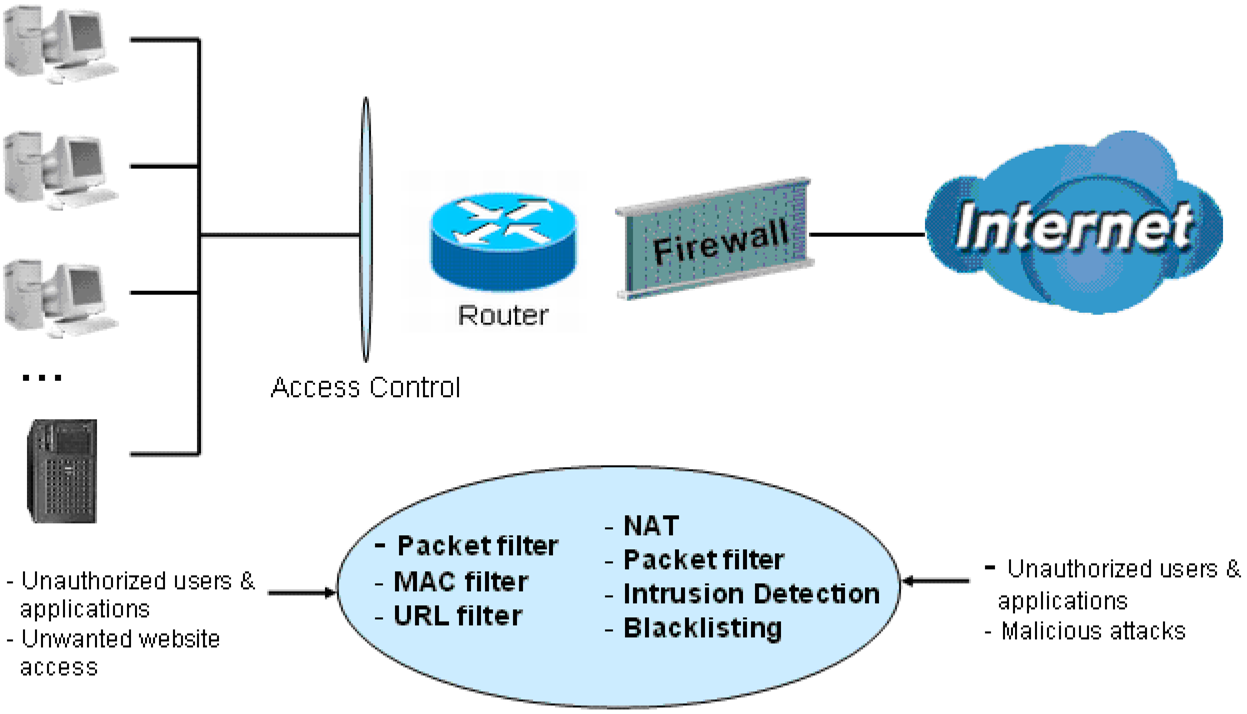
Username	test
Valid	true
Comment	test

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

Firewall

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 (Network Address Translation) the router acts as a "natural" Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet. See the WAN configuration section for more details on NAT.



Firewall & Filter

Firewall: Prevents access from outside your network.

NAT natural firewall: This masks LAN users' IP addresses, which are 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 the NAT function is enabled.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules 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: Allow the filtering of unauthorized users from other networks or WAN, unwanted websites & malicious programs from accessing the local network.

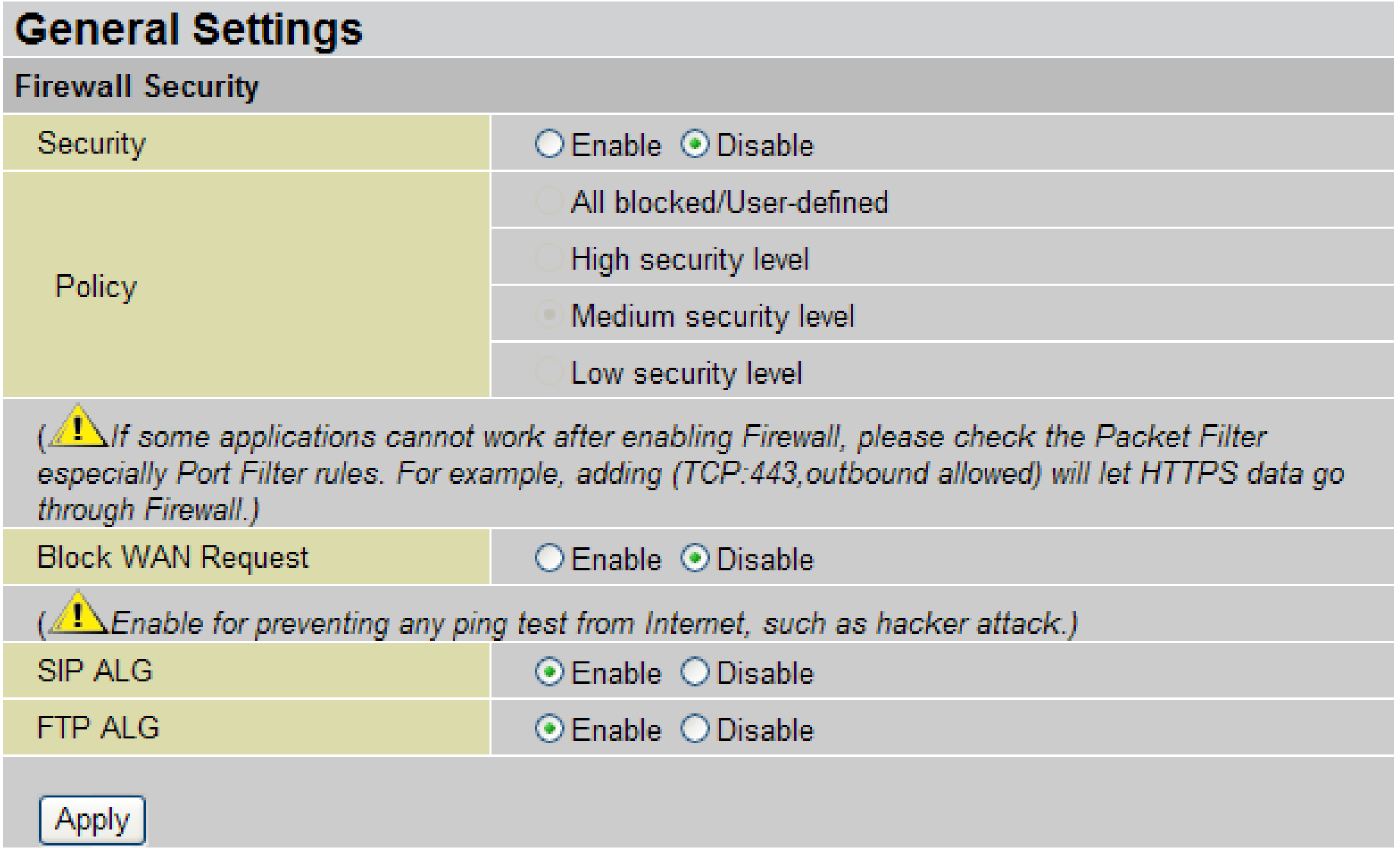
MAC Filter rules: Prevents unauthorized computers accessing the Internet.

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

A detailed explanation of each of the following items appears in the Firewall section below: **General Settings**, **Packet Filter**, **Intrusion Detection**, **URL Filter**, **IM/P2P Blocking** and **Firewall Log**.

General Settings

You can choose enable or disable Firewall. If you disable this function, you will not able to add filter rules by yourself in the Packet Filter. If you enable this function using preset filter rules, you are allowed to modify the packet filter rules as required. The Packet Filter is used to filter packets based-on Applications (Port) or IP addresses.



General Settings

Firewall Security

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

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

Block WAN Request	○ Enable ● Disable

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

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

There are 4 options to choose when you enable Firewall:

- **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 the Packet Filter.

Select either High, Medium or Low security level to enable 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.

Note: The changes or added custom filters on a previous security level will be remembered whenever newer security level is selected. There is no need to reconfigure all settings again if switching back to the previous level.

The "Block WAN Request" is a stand-alone function and is not affected by whether security is enabled or disabled. Mostly this is for preventing any scan tools from the hacker from WAN site.

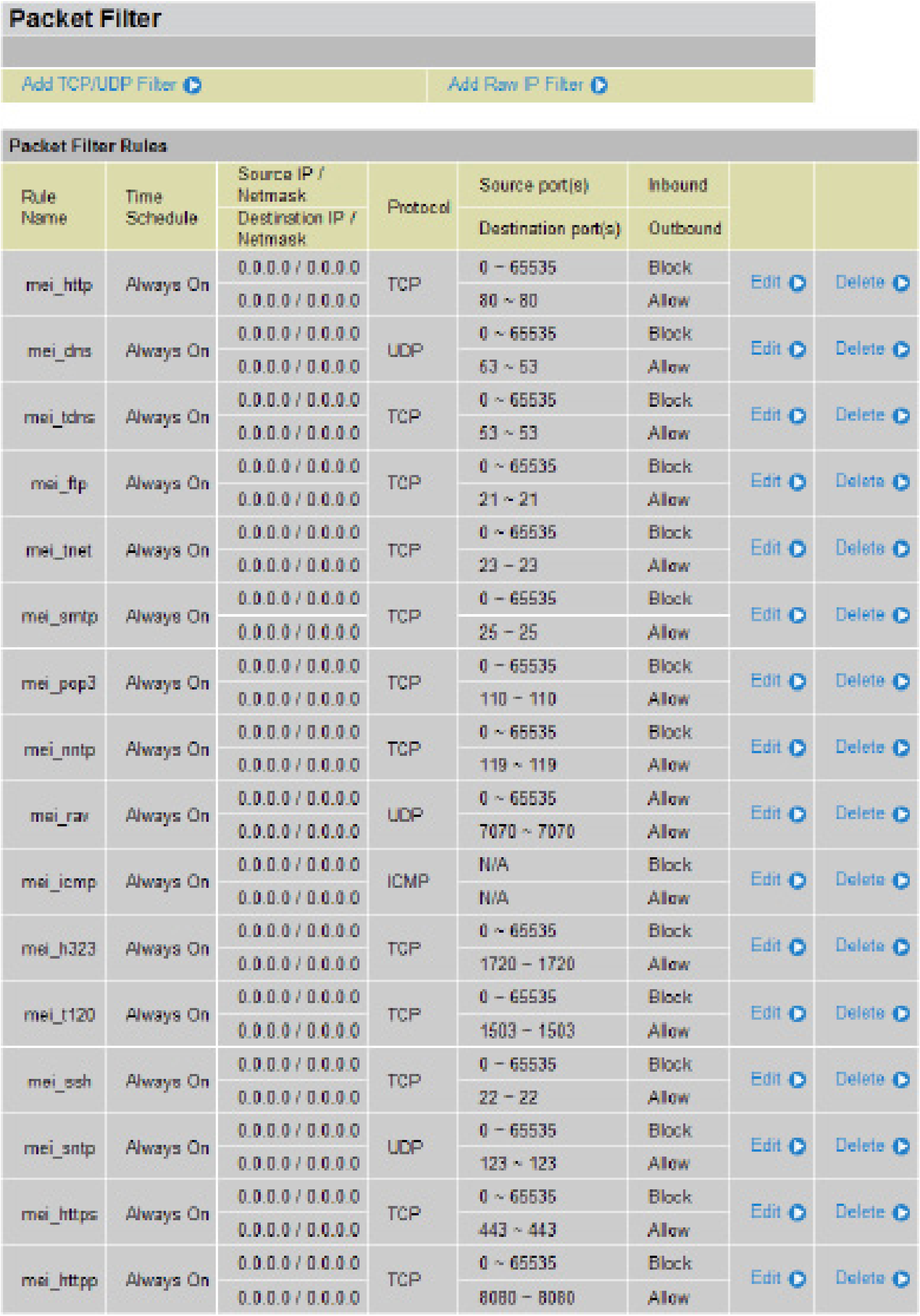
NOTE:

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

Packet Filter

Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet.

This function is only available when Firewall is enabled and one of these four security levels is chosen (All blocked, High, Medium and Low). The predefined port filter rules in the Packet Filter must modify according to the level of Firewall, which is selected. See Table1: Predefined Port Filter for more detailed 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		
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		
mei_rav	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Allow	Edit	Delete
		0.0.0.0 / 0.0.0.0		7070 ~ 7070	Allow		
mei_icmp	Always On	0.0.0.0 / 0.0.0.0	ICMP	N/A	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		N/A	Allow		
mei_h323	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		1720 - 1720	Allow		
mei_t120	Always On	0.0.0.0 / 0.0.0.0	TCP	0 - 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		1503 - 1503	Allow		
mei_ssh	Always On	0.0.0.0 / 0.0.0.0	TCP	0 - 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		22 - 22	Allow		
mei_sntp	Always On	0.0.0.0 / 0.0.0.0	UDP	0 - 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		123 ~ 123	Allow		
mei_https	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		443 ~ 443	Allow		
mei_httpp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit	Delete
		0.0.0.0 / 0.0.0.0		8080 - 8080	Allow		

Example: Predefined Port Filters Rules

The predefined port filter rules for High, Medium and Low security levels are listed. See **Table: Predefined Port Filter** as below.

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

Table: Predefined Port Filter

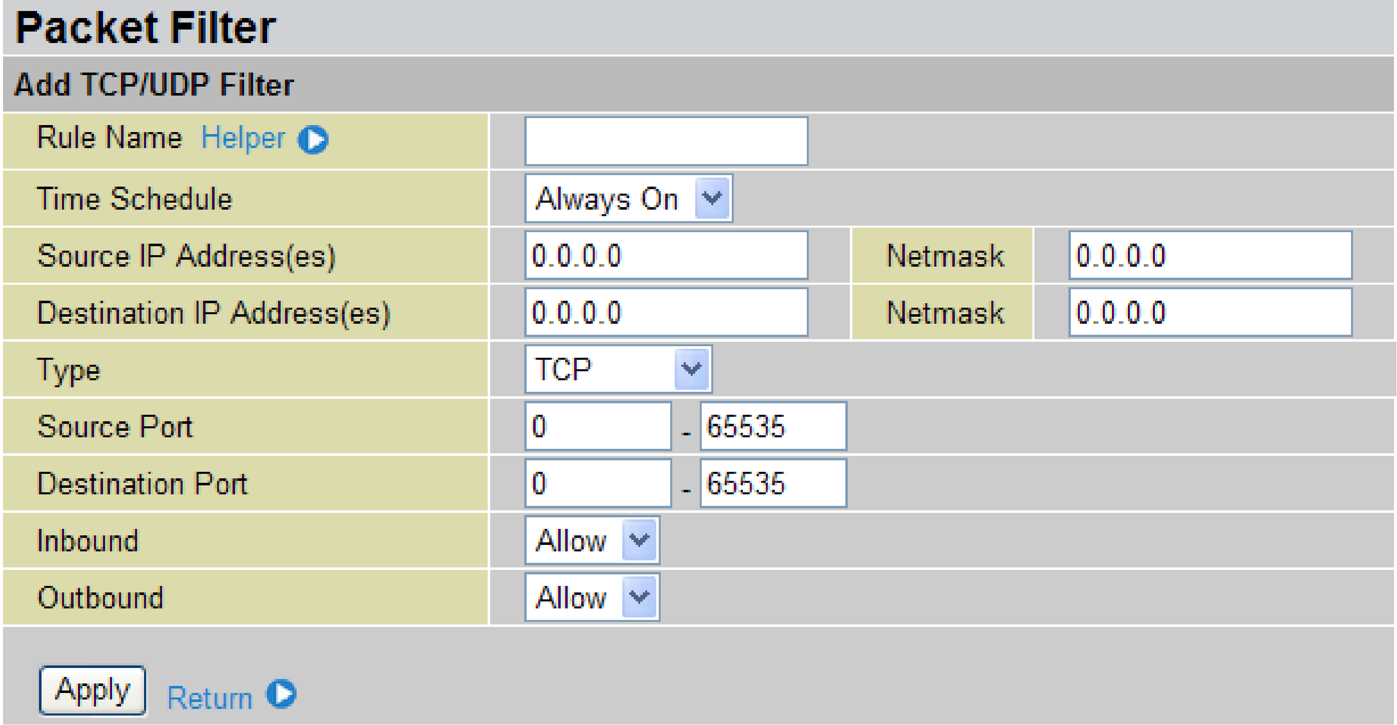
Application	Protocol	Port Number		Firewall - High		Firewall - Medium		Firewall – Low	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	YES	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	YES	YES
FTP(21)	TCP(6)	21	21	NO	NO	NO	YES	NO	YES
Telnet(23)	TCP(6)	23	23	NO	NO	NO	YES	NO	YES
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(119)	TCP(6)	119	119	NO	NO	NO	YES	NO	YES
RealAudio(7070)	UDP(17)	7070	7070	NO	NO	YES	YES	YES	YES
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	NO	NO	NO	YES	YES	YES
T.120(1503)	TCP(6)	1503	1503	NO	NO	NO	YES	YES	YES
SSH(22)	TCP(6)	22	22	NO	NO	NO	YES	YES	YES
NTP(123)	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTPS(443)	TCP(6)	443	443	NO	NO	NO	YES	NO	YES
ICQ (5190)	TCP(6)	5190	5190	NO	NO	NO	NO	YES	YES

Inbound: Internet to LAN ; **Outbound:** LAN to Internet.

YES: Allowed ; **NO:** Blocked ; **N/A:** Not Applicable.

Add TCP/UDP Filter

On the Packet Filter Rules screen, click Add TCP/UDP Filter link to add TCP/UDP filter rule.



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		

Rule Name: User-define description to identify this entry or click Helper link to select existing predefined rules. The maximum name length is 32 characters.

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

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

Note: 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 either TCP or UDP or both of 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.

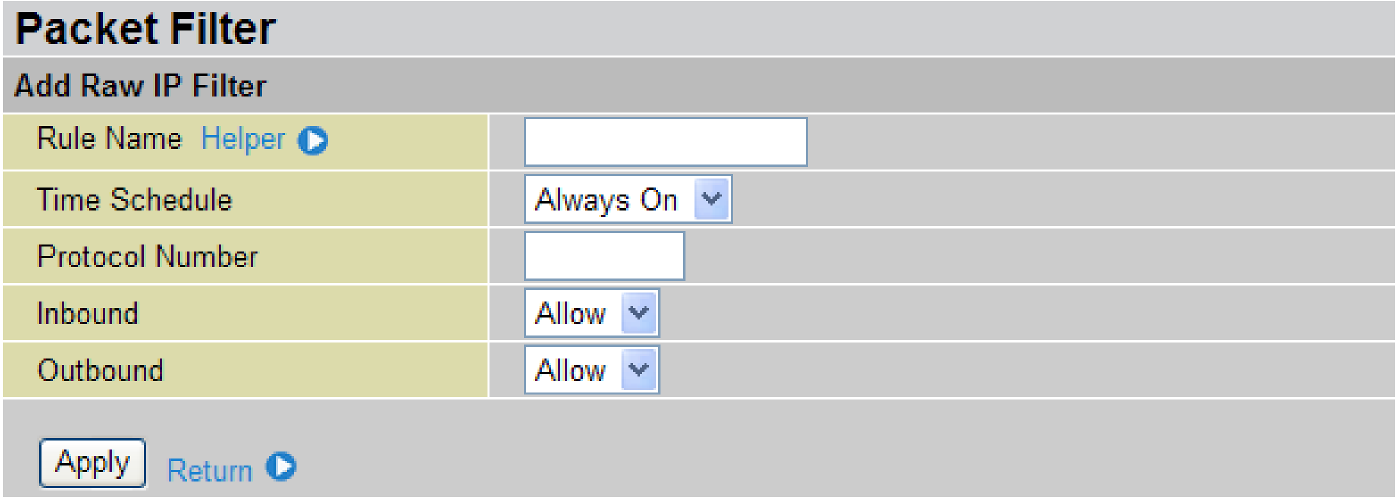
Destination Port: This is the Port or Port Ranges that defines the application.

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

Click Apply to apply the settings.

Add Raw IP Filter

On the Packet Filter Rules screen, click Add Raw IP Filter link to add raw IP filter rule.



Packet Filter

Add Raw IP Filter

Rule Name	
Time Schedule	Always On
Protocol Number	
Inbound	Allow
Outbound	Allow

Rule Name: A user-defined name for identifying the rule.

Time Schedule: It is a 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 to apply the settings.

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

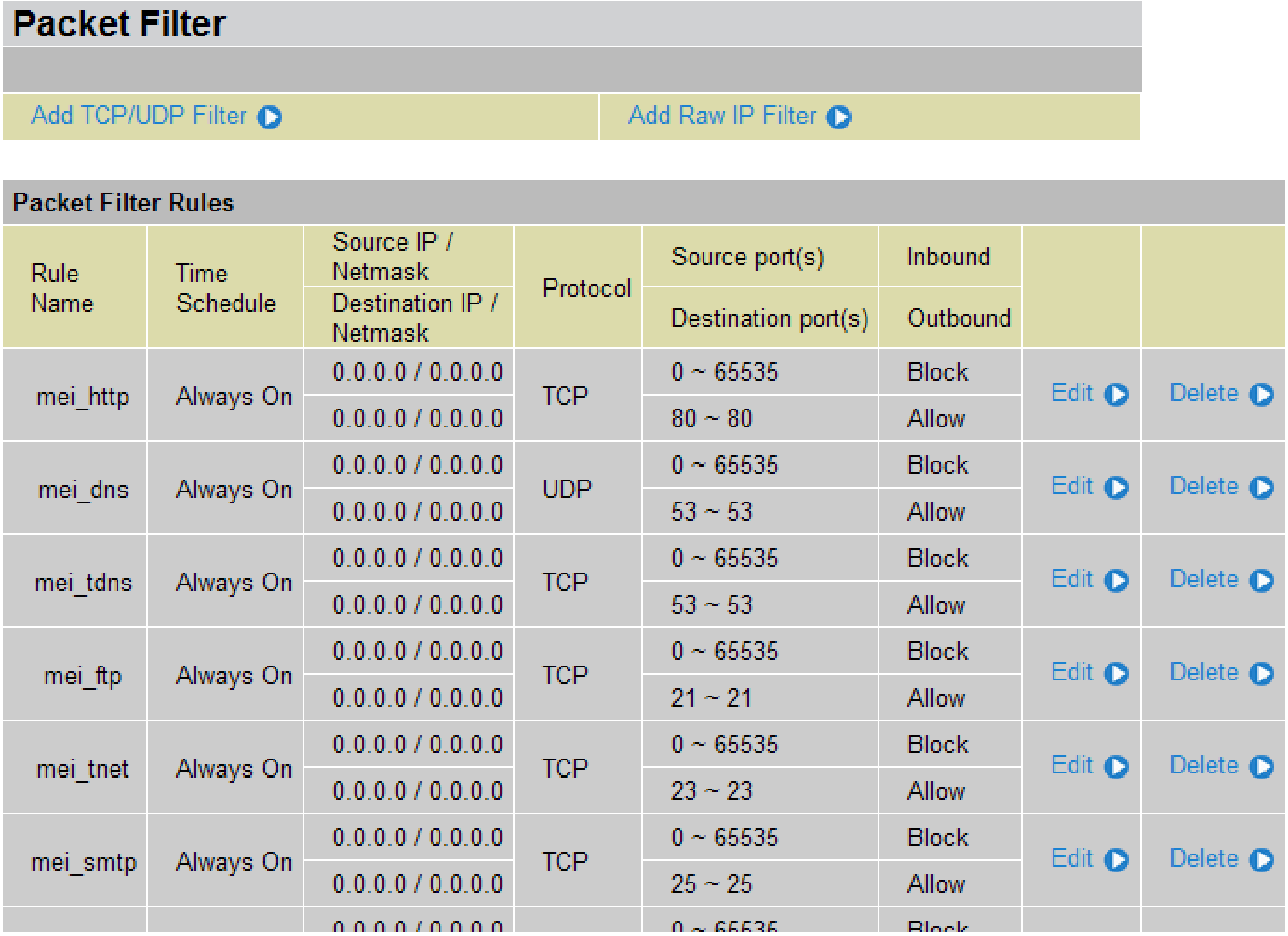
The predefined port filter rule for HTTP (TCP port 80) is the same whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.
As you can see from the diagram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

Configuring Packet Filter

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

Note: You can click Edit the predefined rule instead of Delete it. This example shows you how to add a filter.



Packet Filter

Packet Filter Rules

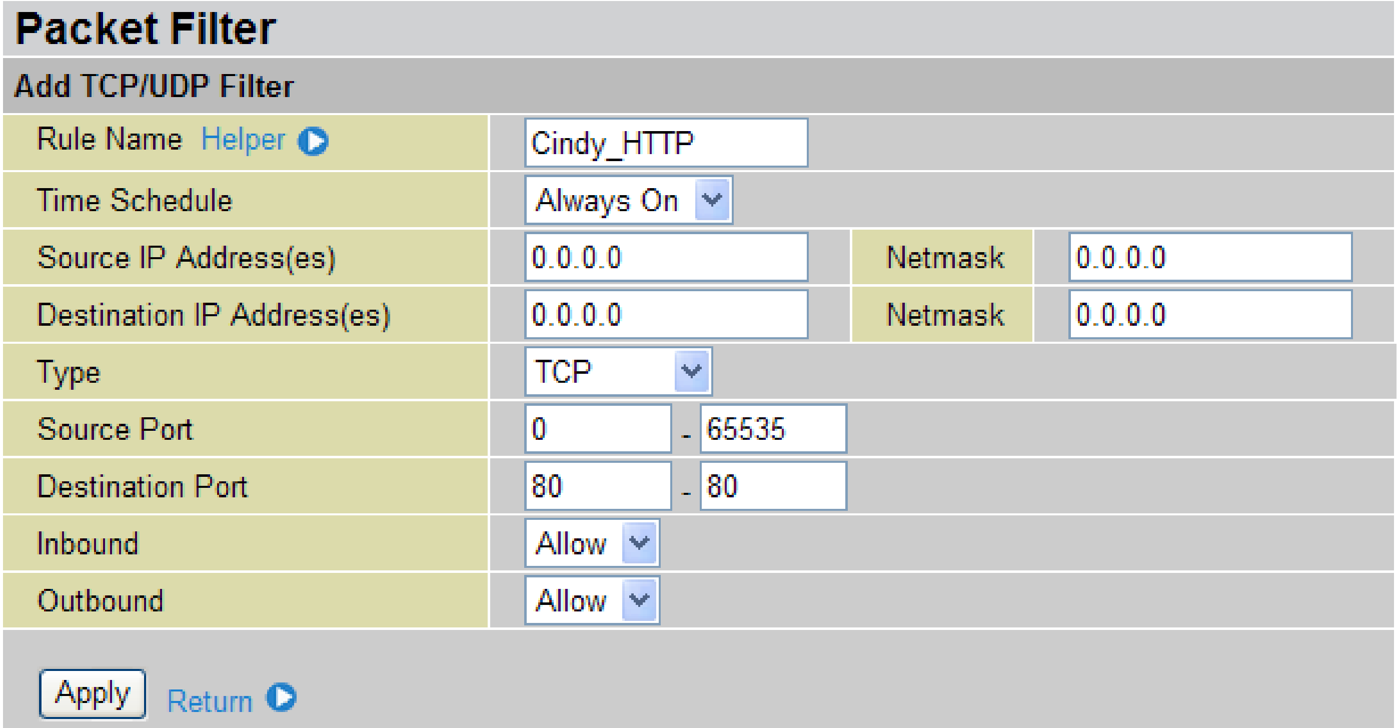
Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	Edit	Delete
mei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535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

2. Click Delete to delete the existing HTTP rule.
3. Click Add TCP/UDP Filter.
4. Enter 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 activate the address-filter, instead I use the port-filter.)
Type: *TCP* (Please refer to Table: 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*

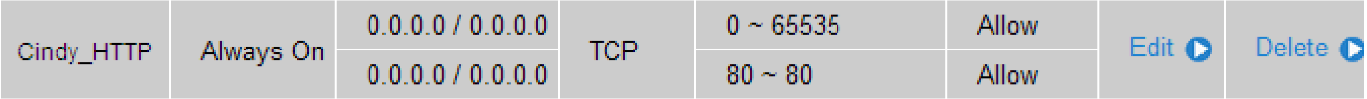


Packet Filter

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		

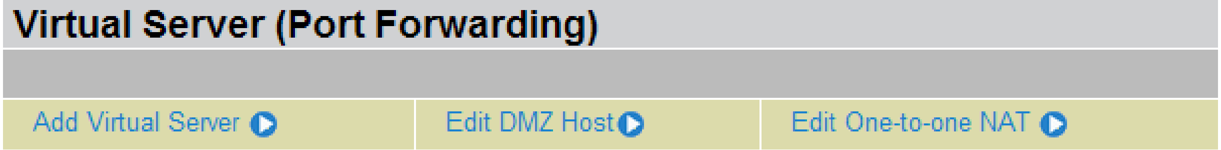
5. Click Apply to save the settings. The new port filter rule for HTTP will be added to the Port Filter Rules table.



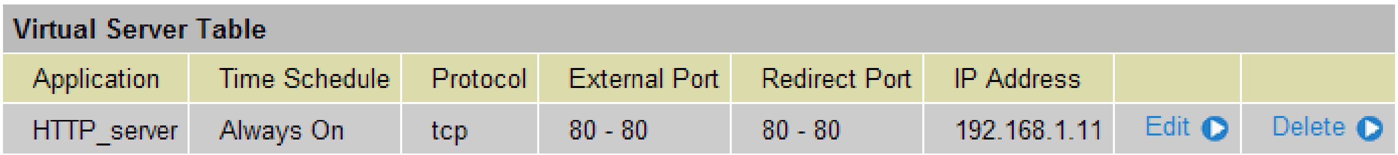
Cindy_HTTP	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Allow	Edit	Delete
		0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		

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: To configure the HTTP in Virtual Server, please refer to Add Virtual Server in Virtual Server section for more details.



Virtual Server (Port Forwarding)

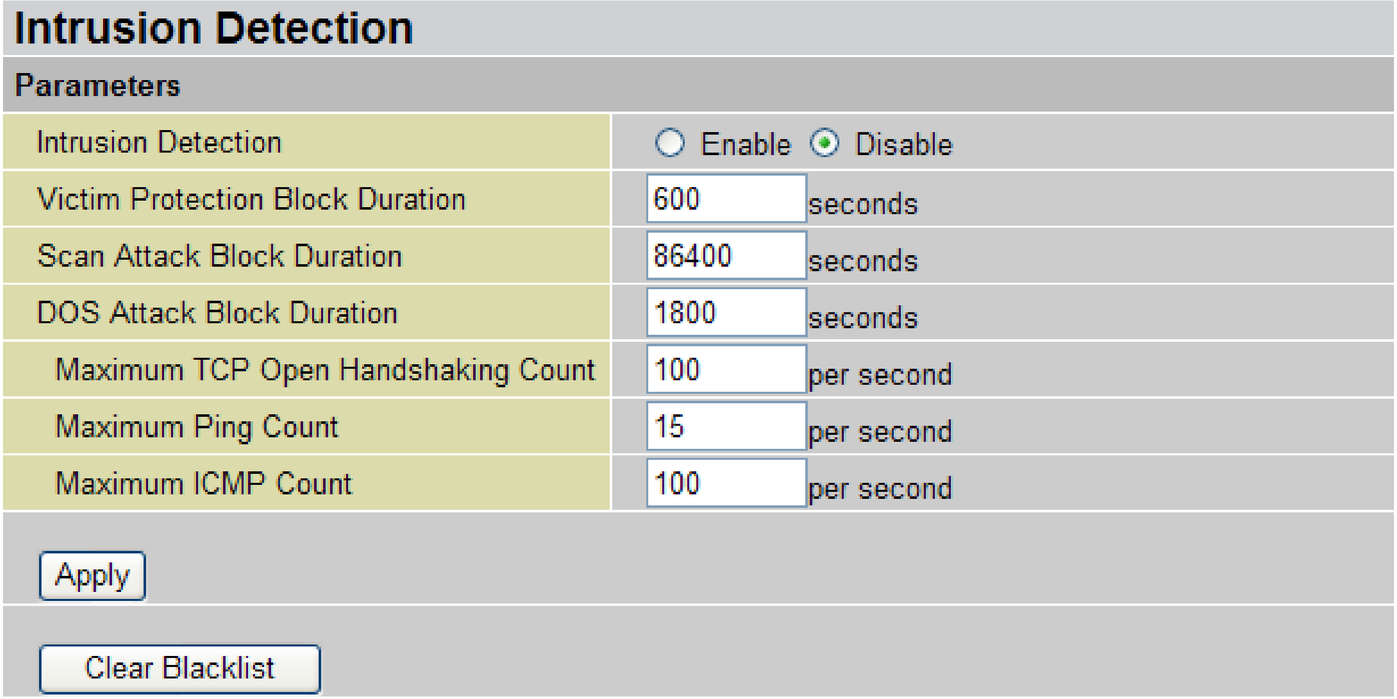


Virtual Server Table

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address		
HTTP_server	Always On	tcp	80 - 80	80 - 80	192.168.1.11	Edit	Delete

Intrusion Detection

The router Intrusion Detection System (IDS) is used to detect hacker's attack 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.



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

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 **Block Duration**. 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: Check Enable if you wish to detect intruders accessing your computer without permission.

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.

Maximum 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.

Maximum 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.

Maximum 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.

Click Apply to confirm the settings.

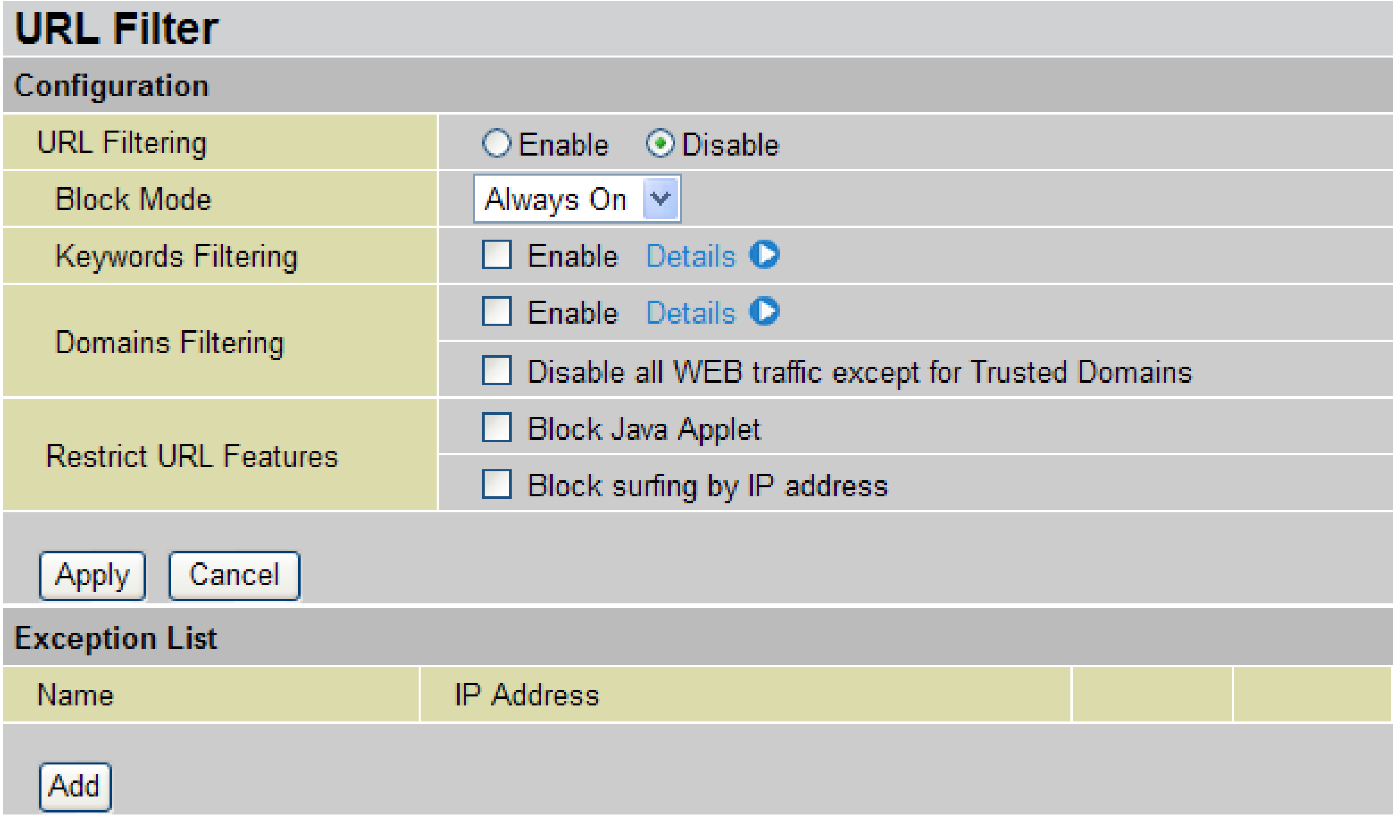
Table: Hacker attack types recognized by the IDS

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

URL Filter

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



URL Filter

Configuration

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

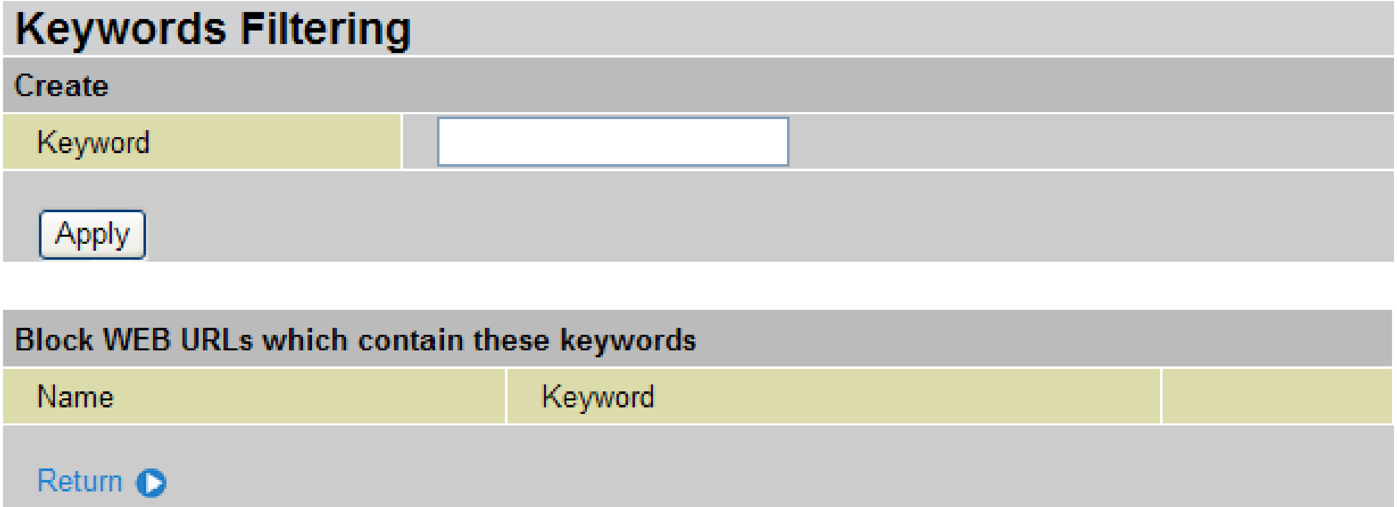
Exception List

Name	IP Address		

URL Filtering: Click Enable to activate URL Filter feature.

Block Mode: A list of modes that you can choose from to check the URL filter rules.

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



Keywords Filtering

Create

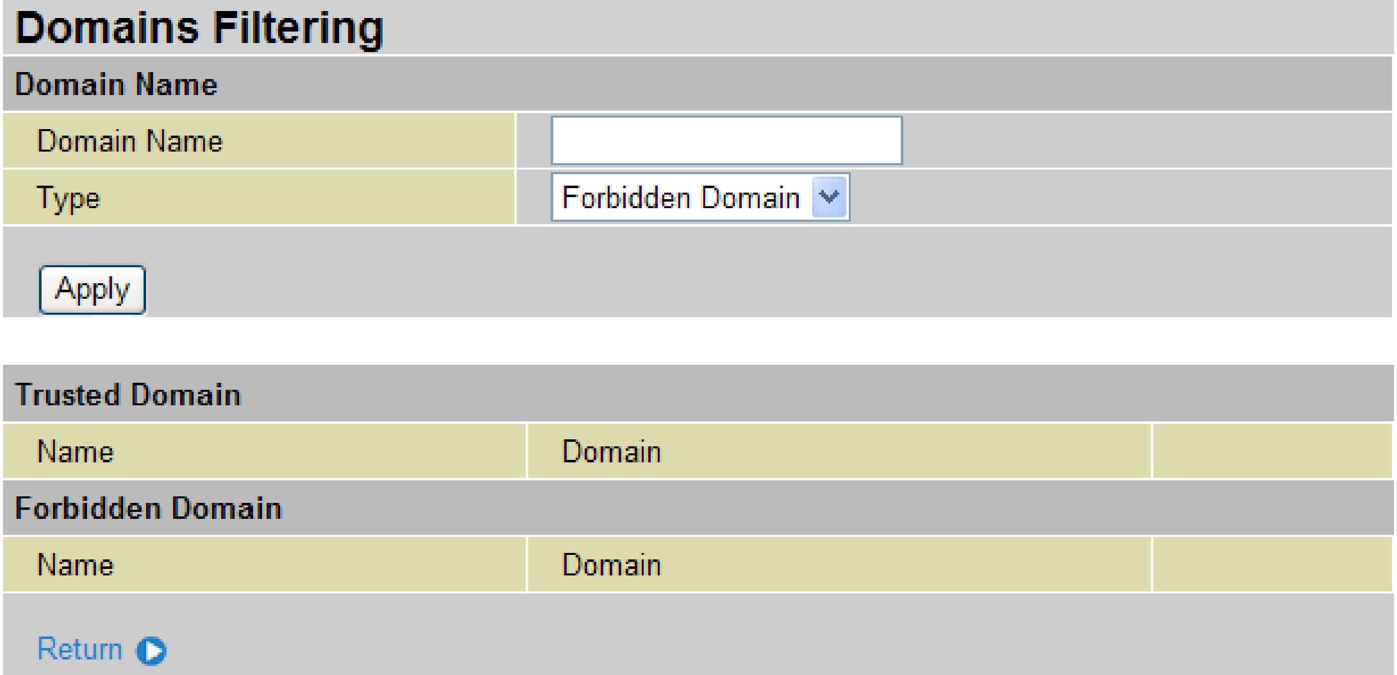
Keyword	

Block WEB URLs which contain these keywords

Name	Keyword	

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:



Domains Filtering

Domain Name

Domain Name	
Type	Forbidden Domain

Trusted Domain

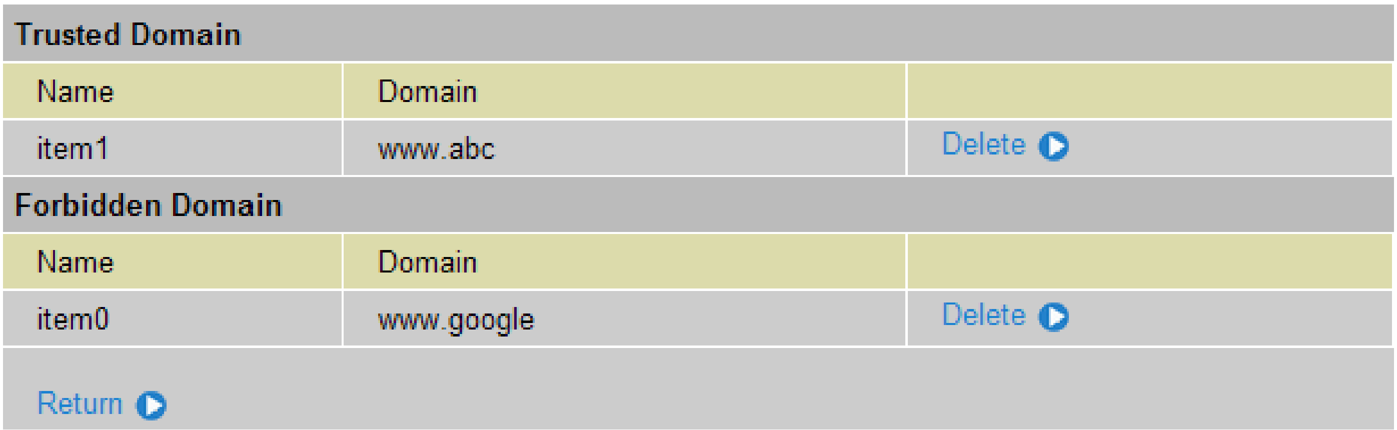
Name	Domain	

Forbidden Domain

Name	Domain	

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

In this example, 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.



Trusted Domain

Name	Domain	
item1	www.abc	Delete

Forbidden Domain

Name	Domain	
item0	www.google	Delete

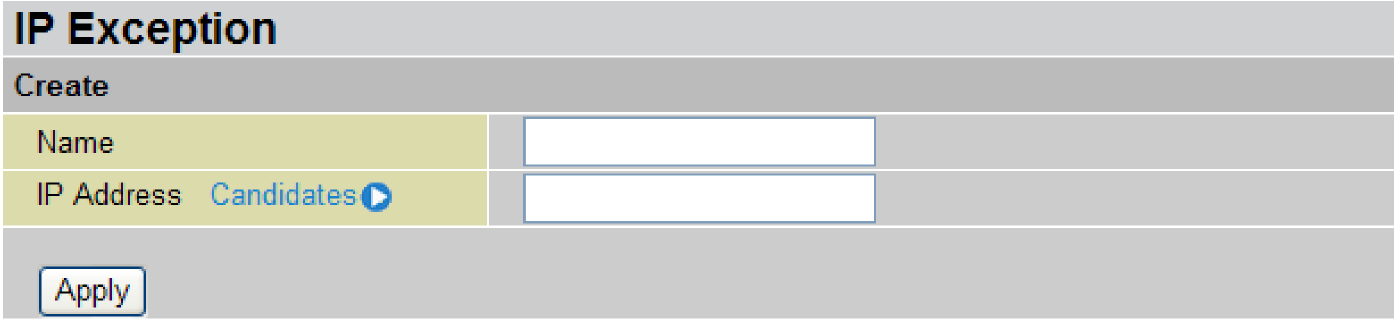
Example:

Andy wishes to disable all WEB traffic except for the ones listed in the trusted domain list, which would prevent Bobby from accessing other web sites. Andy selects both functions in the Domain Filtering and thinks that it will stop Bobby. Nevertheless, Bobby knows that Domain Filtering will ONLY disable all WEB traffic except for the one in the 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. With this feature, Andy can prevent Bobby from accessing unwanted websites.

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

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

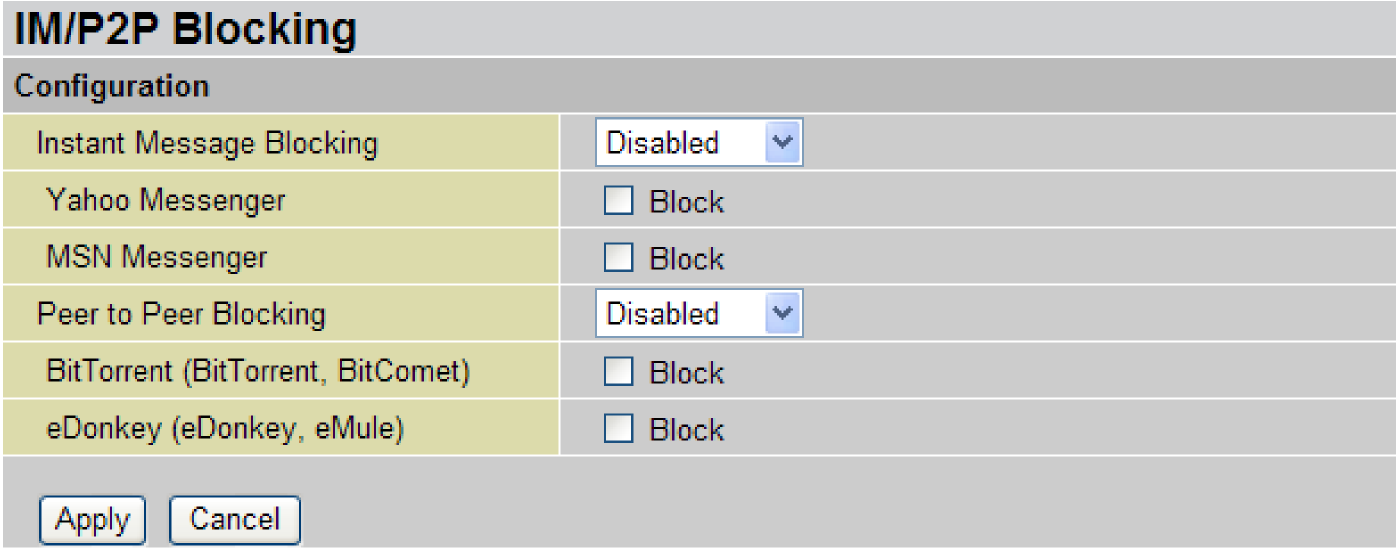
Except IP Address: The except IP address list. Enter the Name and IP Address and then click Apply to save the configuration.



Click Apply to confirm the settings.

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 a group of computer users who share files with 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 to restrict LAN PCs from accessing the commonly used IM such as 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

Instant Message Blocking: Default is set to Disable.

- **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: Tick the checking box to block either or both Yahoo or/and MSN Messenger. Be sure you enabled the Instant Message Blocking first.

Peer to Peer Blocking: Default setting is Disable.

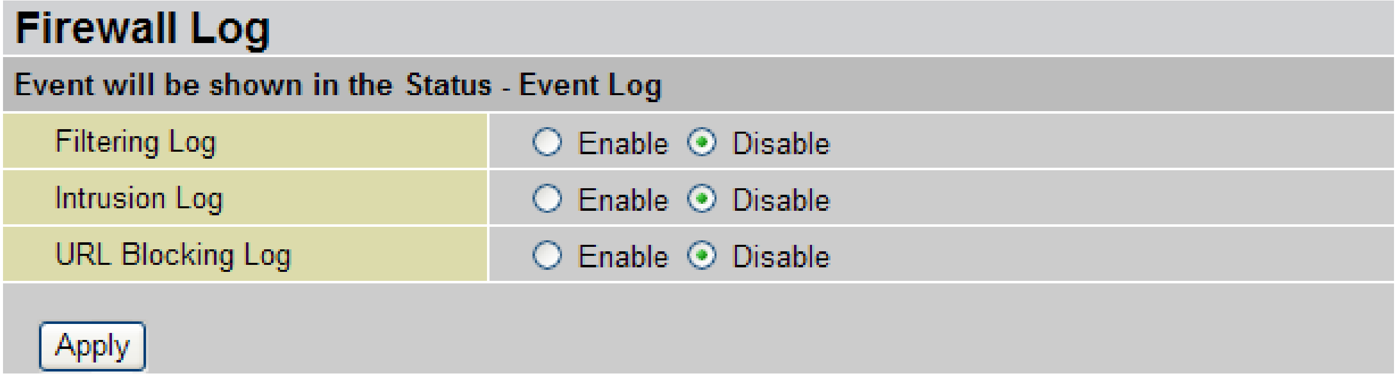
- **Disabled:** Instant Message blocking is not triggered. No action will be performed.
- **Always On:** Action is enabled.
- **TimeSlot1 ~ TimeSlot16:** This is the self-defined time period. You may specify the time period to trigger the blocking, i.e. during working hours. For setup and detail, refer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

BitTorrent / eDonkey: Tick the checking box to block either or both Bit Torrent or/and eDonkey. Be sure you enabled the Peer to Peer Blocking first.

Click Apply to confirm the settings.

Firewall Log

Firewall Log displays log information of all unexpected action taken by your firewall settings.



Firewall Log

Event will be shown in the Status - Event Log

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

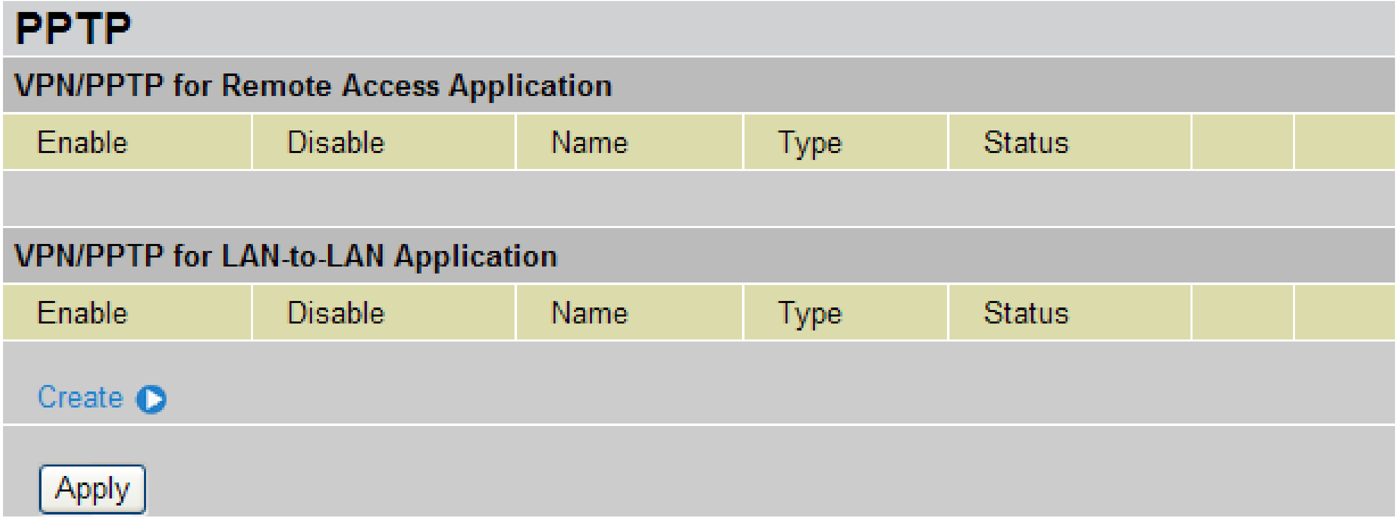
This feature is disabled by default. To activate the logs, check the Enable box then click the Apply button.

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

VPN (Virtual Private Networks) (BiPAC 8500/ 8501/ 8520 Only)

Virtual Private Networks is a way to establish a secured communication tunnel 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		

If you have created a PPTP connection, the account information will be shown.

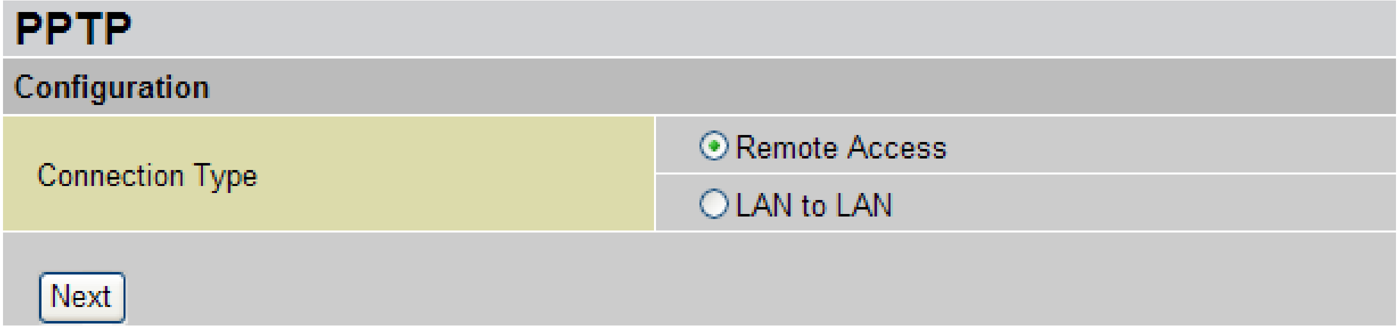
Enable / Disable: This function activates or inactivates the PPTP connection. To interrupt the tunnel, check the Disable radio button and click the Apply button to inactivate the connection.

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

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

Status: Shows the condition of your PPTP tunnel connection.

Click Create to configure a new VPN connection. There are 2 types of PPTP VPN supported: **Remote Access** and **LAN-to-LAN**.

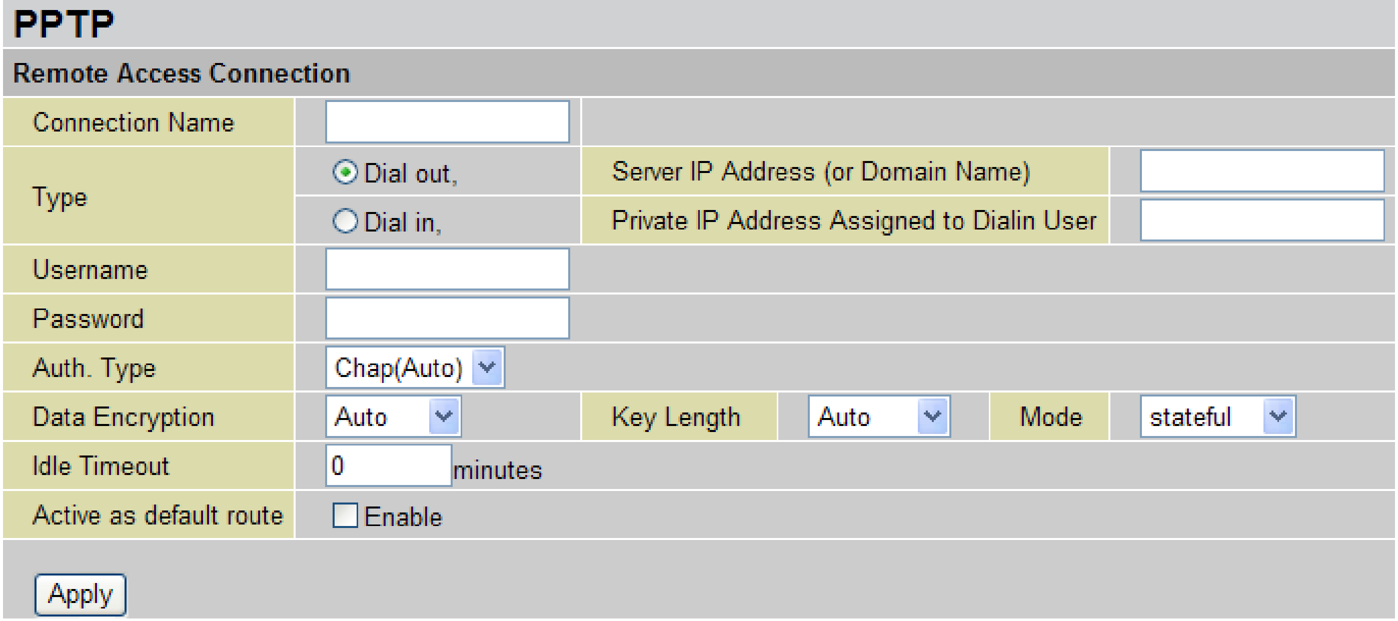


PPTP

Configuration

Connection Type	● Remote Access ○ LAN to LAN

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				

Connection Name: A 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 if you want the router to operate as a VPN server.

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

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.

Auth. Type: Default is Auto, allows the router to determine which the type of authentication to use. You can also 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 the authentication type you want clients to use (when acting as a server). When using PAP, the password is sent unencrypted, CHAP encrypts the password before sending. This presents 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 a MPPE algorithm. Default is Auto, which means this setting is negotiated when establishing a connection. You can also 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.

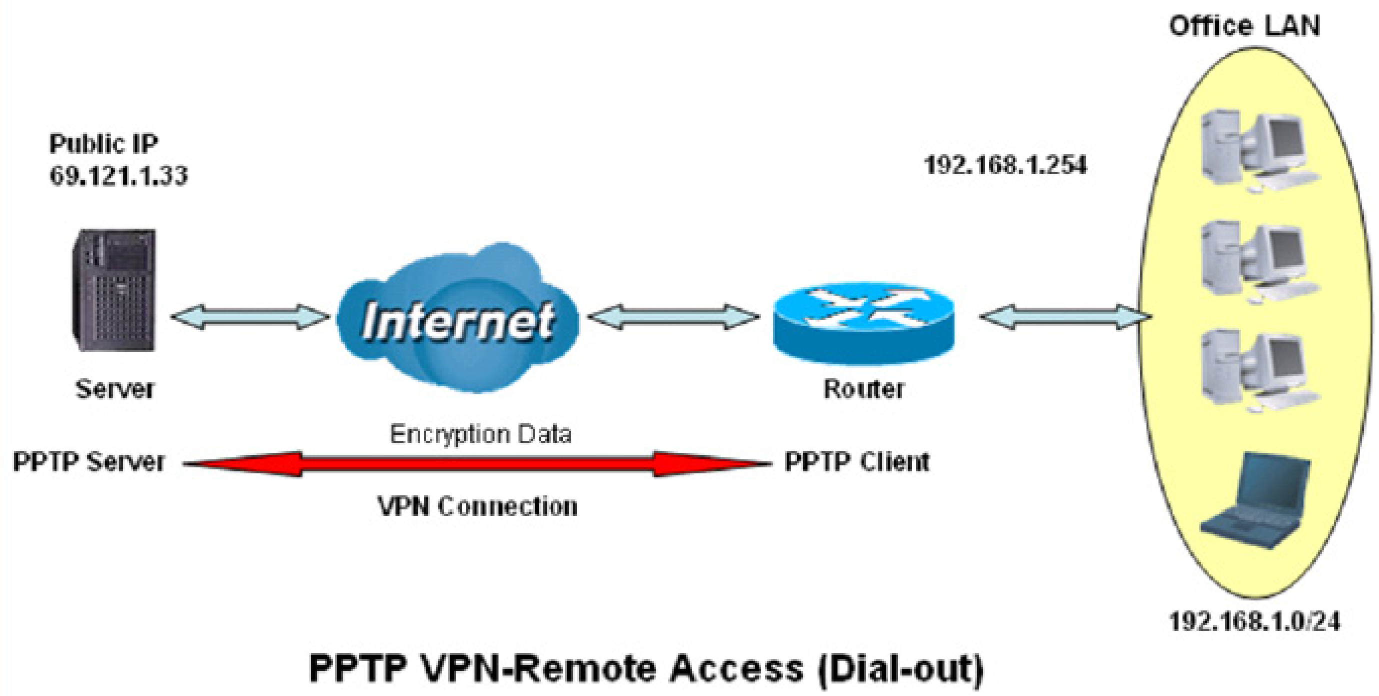
Idle Timeout: Auto-disconnect the VPN connection when there is no activity on the connection for a predetermined period of time. 0 means this connection is always on.

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

Click the Apply button to apply your changes.

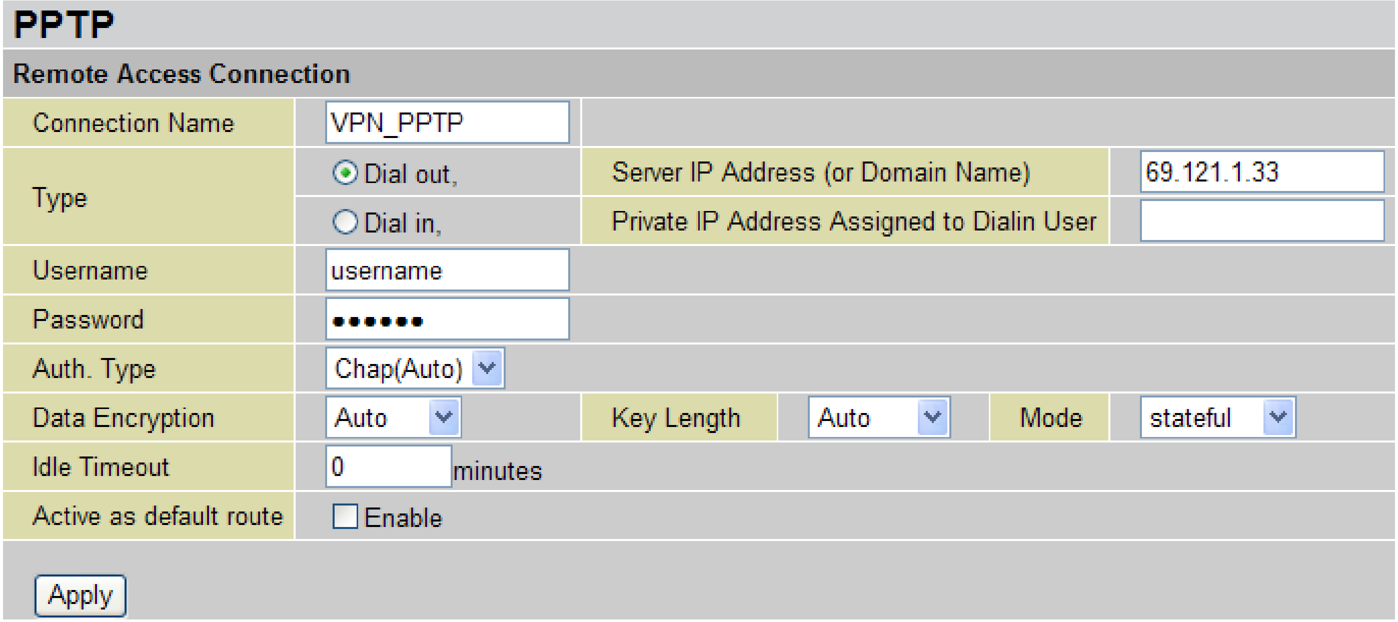
Example: Configuring a Remote Access PPTP VPN Dial-out Connection

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



Configuring the PPTP VPN in the Office

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



PPTP

Remote Access Connection

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

Connection Name: Specify a name for the PPTP connection (**VPN_PPTP**).

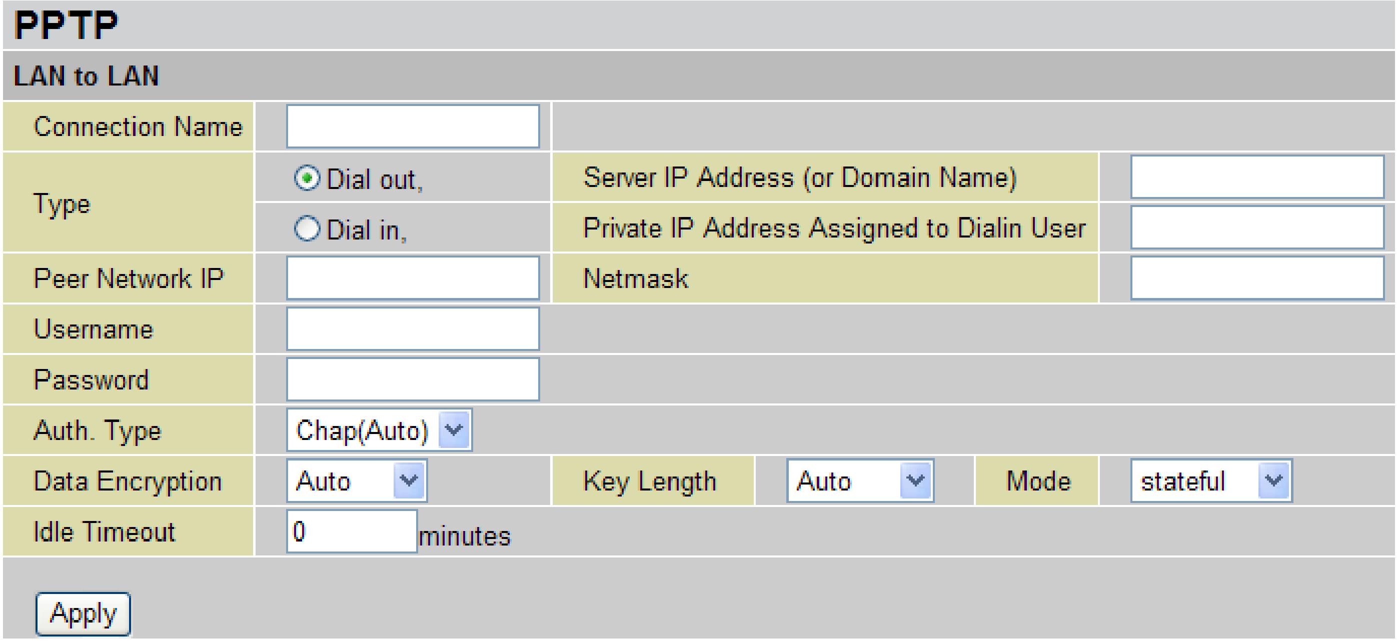
Dial out: Check **Dial out** and enter a Dialed server IP (**69.121.1.33**) on the Server IP Address (or Hostname) field.

Username / Password: Specify the username (**username**) & password (**123456**).

Auth.Type/Data Encryption/Key Length/Mode: 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.

Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

PPTP Connection - LAN to LAN



PPTP

LAN to LAN

Connection Name					
Type	● Dial out,	Server IP Address (or Domain Name)			
	○ 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				

Connection Name: A user-defined name for 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 if you want it to operate as a VPN server.

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

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

Peer Network IP: Enter the Peer network IP address.

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

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

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

Authentication Type: Default is Auto, allows the router to determine which authentication type to use. You can also 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 the authentication type you want clients to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending. This presents 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 a MPPE algorithm. Default is Auto, which means this setting is negotiated when establishing a connection. You can also 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.

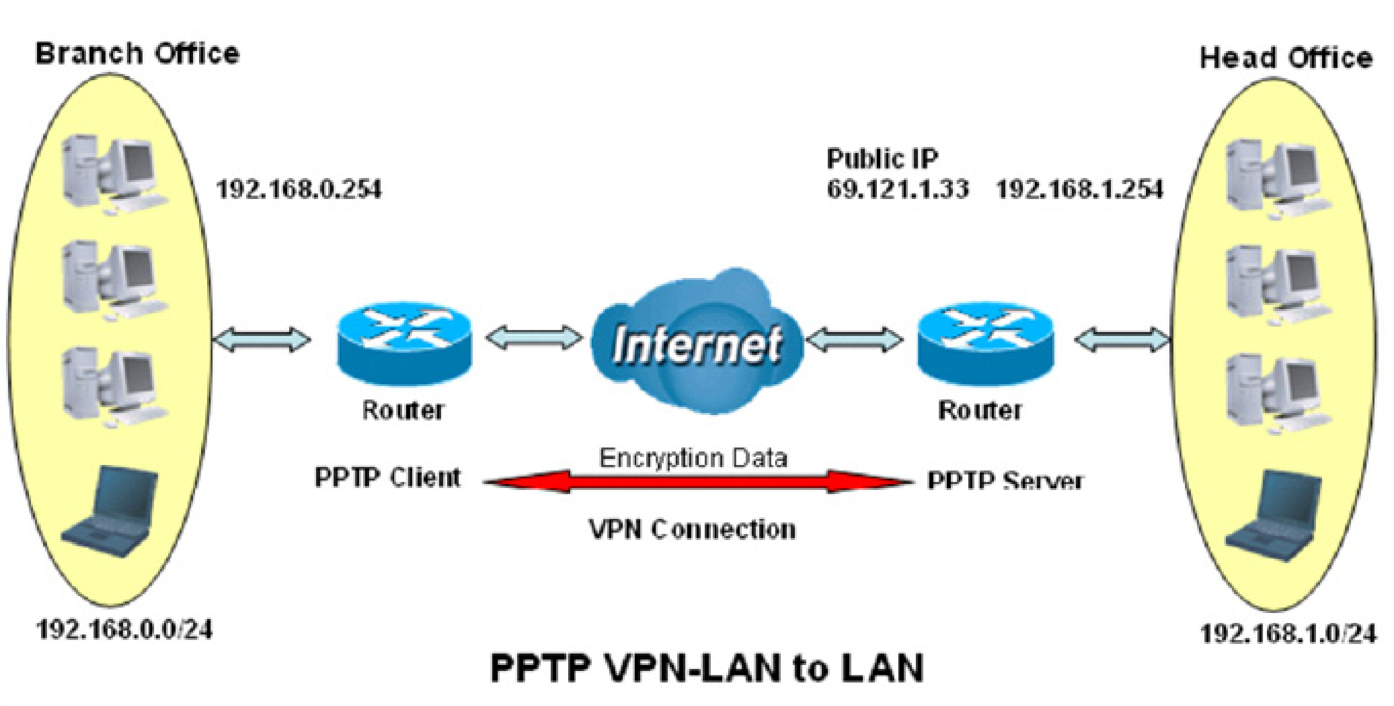
Mode: You may select Stateful or Stateless mode. The key will be changed every 256 packets when you select Stateful mode. If you select Stateless mode, the key will be changed in each packet.

Idle Timeout: 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 the Apply button to apply your changes.

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

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

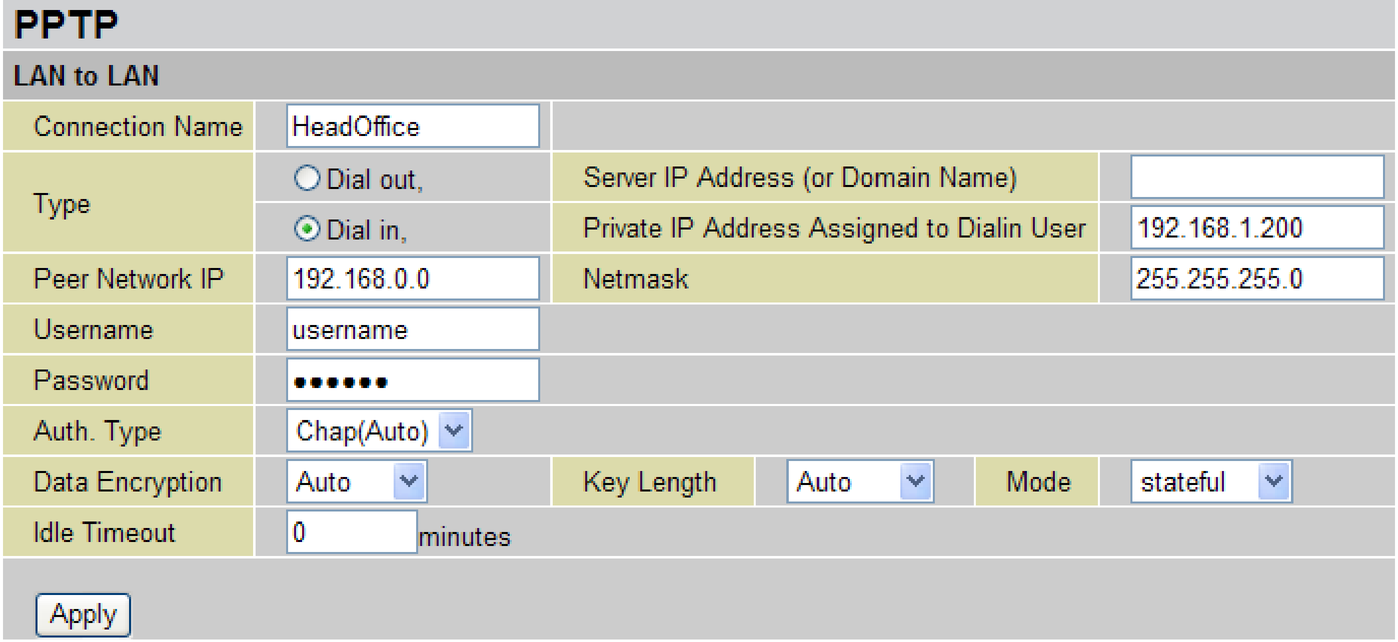


Attention

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

Configuring PPTP VPN in the Head Office

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



PPTP

LAN to LAN

Connection Name	HeadOffice				
Type	○ Dial out,	Server IP Address (or Domain Name)			
	● Dial in,	Private IP Address Assigned to Dialin User			192.168.1.200
Peer Network IP	192.168.0.0	Netmask			255.255.255.0
Username	username				
Password	••••••				
Auth. Type	Chap(Auto)				
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Idle Timeout	0 minutes				

Connection Name: Specify a name for the PPTP connection (**HeadOffice**).

Type: Check **Dial in** and enter an IP address assigned to branch office network (**192.168.1.200**).

Peer Network IP and **Netmask:** Enter the IP address (**192.168.0.0**) & subnet mask (**255.255.255.0**) of branch office network.

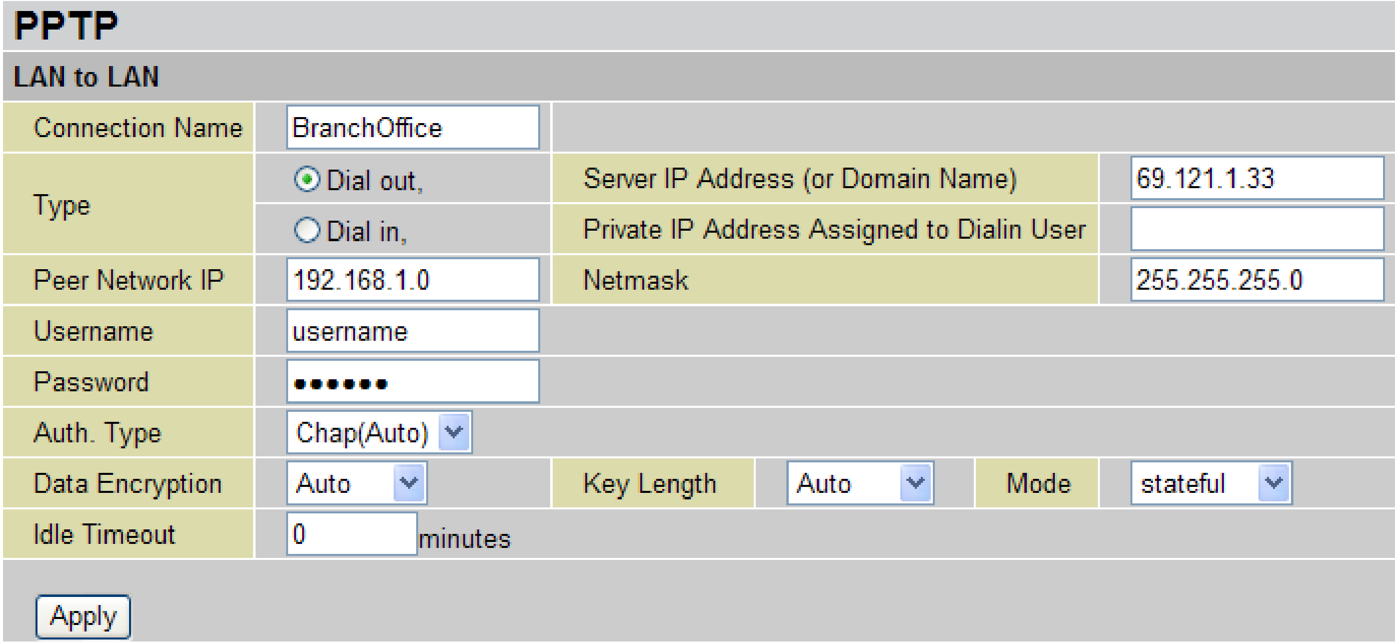
Username / Password: Specify the username (**username**) & password (**123456**) to authenticate branch office network.

Auth.Type/Data Encryption/Key Length/Mode: 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.

Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

Configuring PPTP VPN in the Head Office

The IP address 69.1.121.30 is the Public IP address of the router located in the 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				
Type	● Dial out,	Server IP Address (or Domain Name)	69.121.1.33		
	○ Dial in,	Private IP Address Assigned to Dialin User			
Peer Network IP	192.168.1.0	Netmask	255.255.255.0		
Username	username				
Password	••••••				
Auth. Type	Chap(Auto)				
Data Encryption	Auto	Key Length	Auto	Mode	stateful
Idle Timeout	0 minutes				

Connection Name: Specify a name for the PPTP connection (**BranchOffice**).

Type: Check **Dial out** and enter the IP address (**69.121.1.33**) of the head office router (in WAN side).

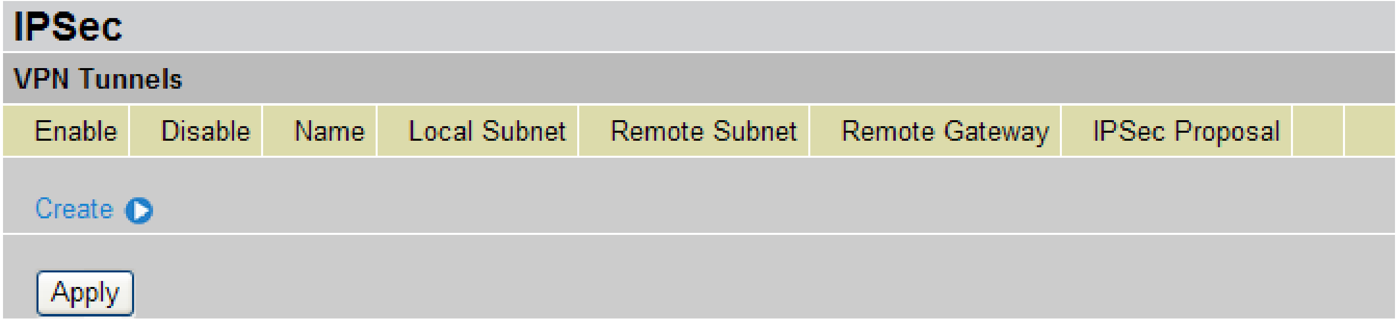
Peer Network IP and **Netmask:** Enter the IP address (**192.168.1.0**) & subnet mask (**255.255.255.0**) of head office network.

Username / Password: Specify the username (**username**) & password (**123456**) to authenticate branch office network.

Auth.Type/Data Encryption/Key Length/Mode: 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.

Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

IPSec (IP Security Protocol)



IPSec

VPN Tunnels

Enable	Disable	Name	Local Subnet	Remote Subnet	Remote Gateway	IPSec Proposal		

If you have created an IPSec connection, the account information will be shown.

Enable / Disable: This function activates or inactivates the IPSec connection. To interrupt the tunnel, check the Disable radio button and click the Apply button to inactivate the connection.

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

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

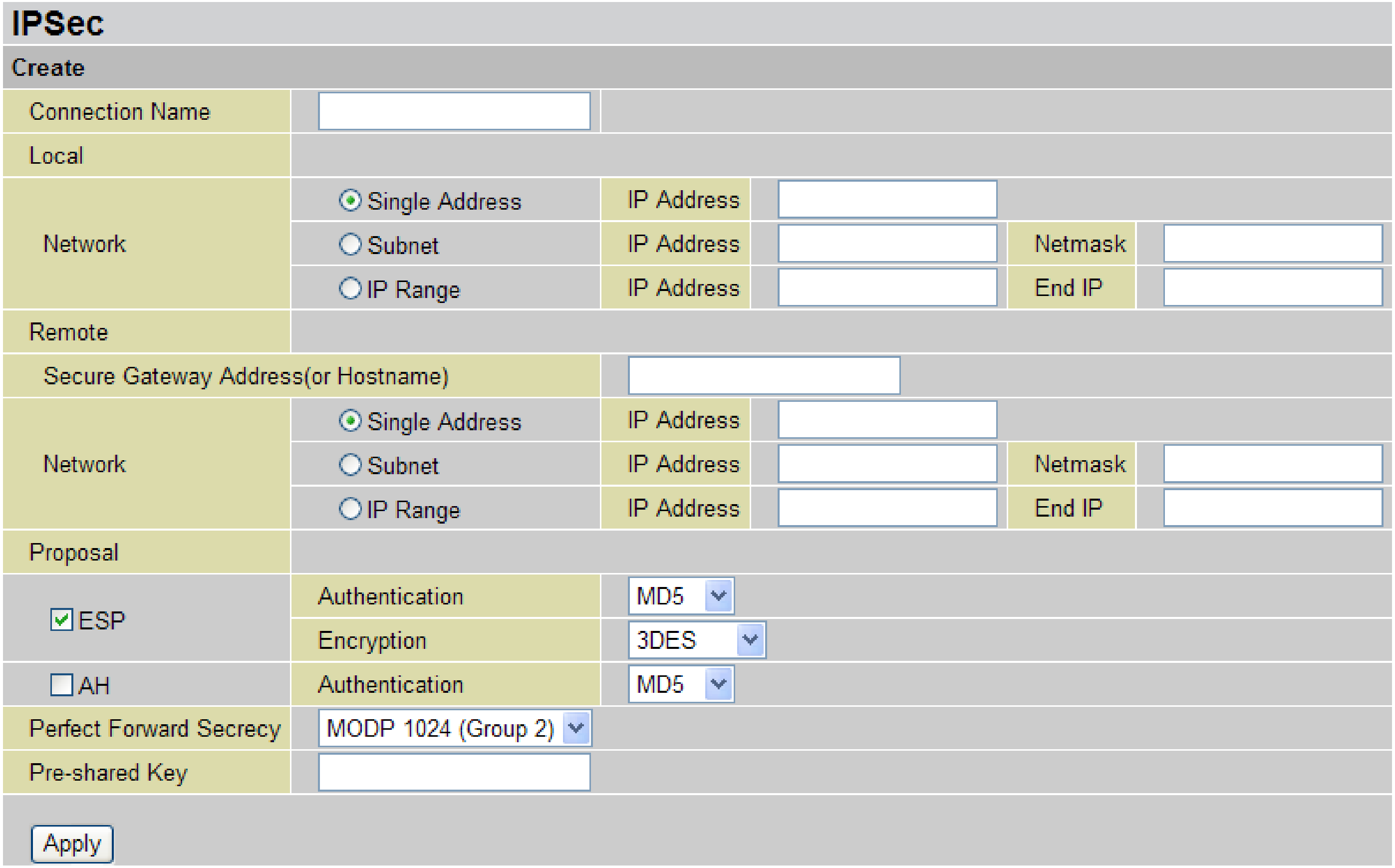
Remote Subnet: Displays IP address and subnet of the remote network.

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

IPSec Proposal: This is the selected IPSec security method.

Click Create to configure a new IPSec VPN connection account.

IPSec VPN Connection



IPSec

Create

Connection Name					
Local					
Network	● Single Address	IP Address			
	○ Subnet	IP Address		Netmask	
	○ IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)					
Network	● Single Address	IP Address			
	○ Subnet	IP Address		Netmask	
	○ IP Range	IP Address		End IP	
Proposal					
☑ ESP	Authentication	MD5			
	Encryption	3DES			
☐ AH	Authentication	MD5			
Perfect Forward Secrecy	MODP 1024 (Group 2)				
Pre-shared Key					

Connection Name: A user-defined name for the connection.

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

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

Remote Secure Gateway Address (or Domain Name): The IP address or hostname of the remote VPN device that is connected and is used to establishe 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 that it is not tampered with during transmission. There are three options, Message Digest 5 (**MD5**), Secure Hash Algorithm (**SHA1**) or **NONE**. SHA1 is more resistant to brute-force attacks than MD5, however it is slower.

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

Encryption: Select the encryption method from the pull-down menu. There are 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 the latency.

- **DES:** Stand for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stand for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stand for Advanced Encryption Standards, you can use 128, 192 or 256 bits encryption method.

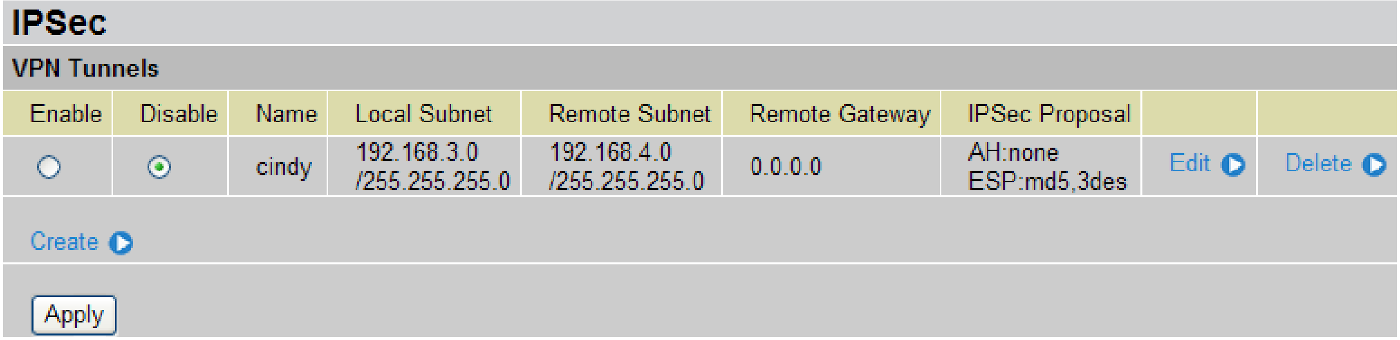
Perfect Forward Secrecy: Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change the encryption keys during second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol 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 to the router or hosts at both ends.

Click the Apply button to save your setting.

Edit IPSec VPN Tunnels

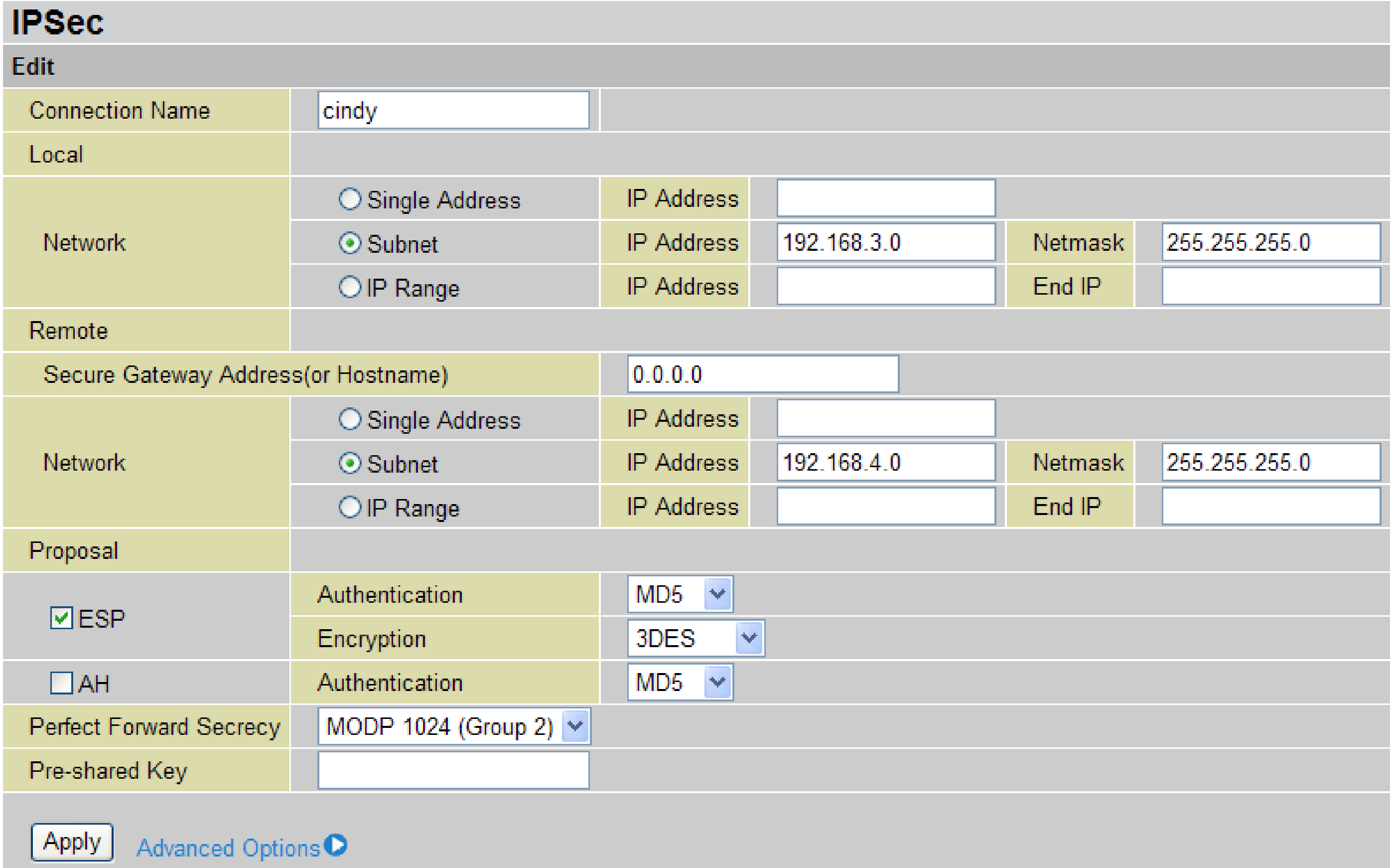
To change the information of IPSec VPN Tunnels, click Edit.



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	0.0.0.0	AH:none ESP:md5,3des	Edit	Delete



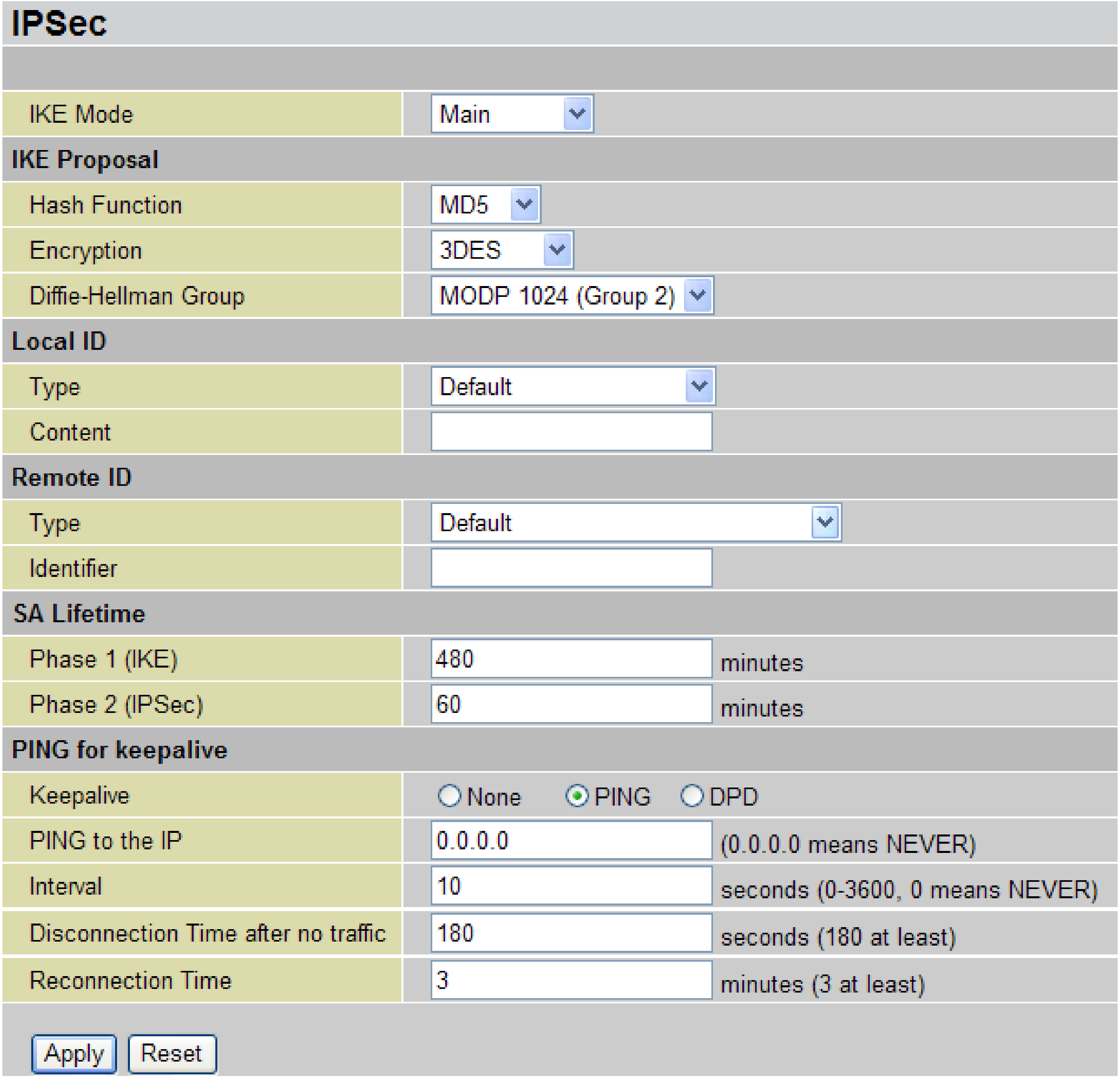
IPSec

Edit

Connection Name	cindy				
Local					
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.3.0	Netmask	255.255.255.0
	○ IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)		0.0.0.0			
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.4.0	Netmask	255.255.255.0
	○ IP Range	IP Address		End IP	
Proposal					
☑ ESP	Authentication	MD5			
	Encryption	3DES			
☐ AH	Authentication	MD5			
Perfect Forward Secrecy	MODP 1024 (Group 2)				
Pre-shared Key					

Advanced Options

On the IPSec Edit screen, click **Advanced Options** link to change the 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	
Keepalive	○ None ● PING ○ DPD
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)

IKE Mode: Set IKE (Internet key Exchange) 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. 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 drop-down menu. There are several options, DES, 3DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase the latency.

- **DES:** Stands for Data Encryption Standard and uses 56 bits encryption method.

- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits 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 3 modes, MODP 768-bit, MODP 1024-bit and MODP 1536-bit. MODP stands for Modular Exponentiation Groups.

Local ID

Type: Specify a local ID type.

Content: Input ID information, such as domain name www.ipsectest.com.

Remote ID

Type: Specify a Remote ID type.

Identifier: Input remote ID information, like domain name www.ipsectest.com.

SA Lifetime

Specify the number of minutes that a Security Association (SA) will stay active before a new encryption and an 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. Default is 240 minutes.

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

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

PING to Keepalive

Keepalive: It is used to detect IPSec tunnel connection failure. Connection failure is defined as abort or in NO response state. In such event Ping to Keepalive takes proper action to ensure the connection quality of IPSec.

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

Interval: This sets the time interval of 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 seconds; 0 indicates disabing the function.

Ping to the IP	Internal (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 seconds.

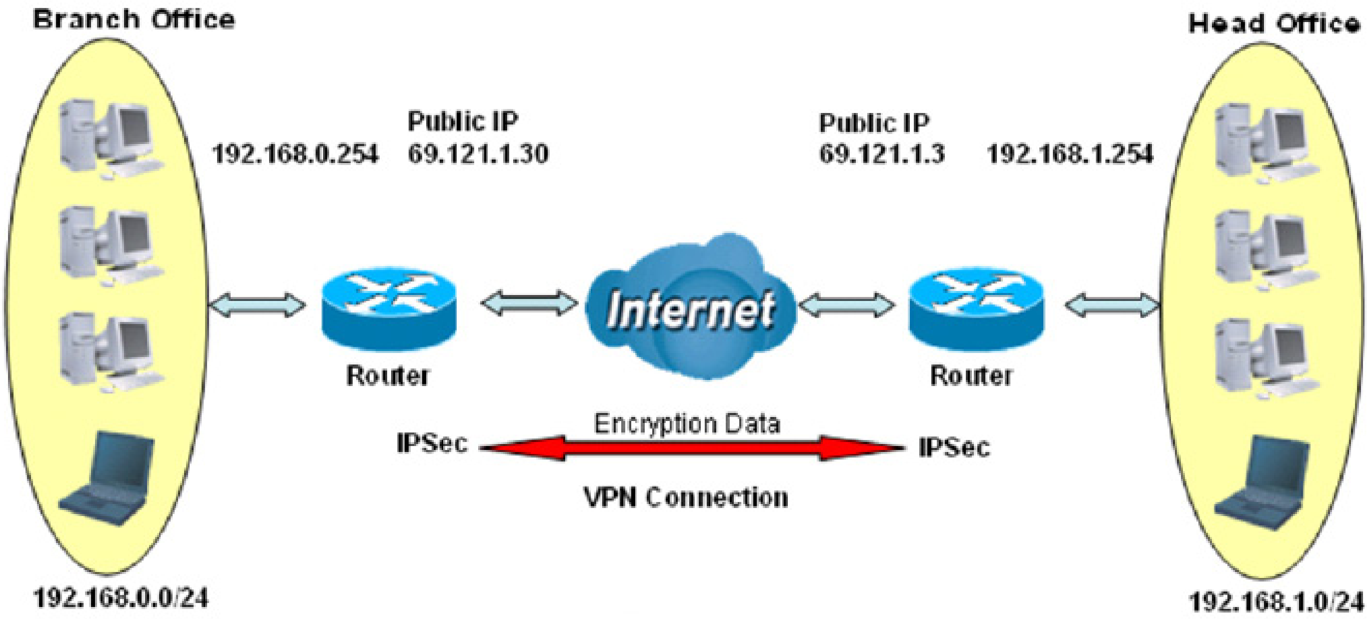
Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the Reconnection Time set. Default setting is 1200 seconds; 180 seconds is the minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. Default setting is 15 minutes; 3 minutes is the minimum time interval for this function.

Click the Apply button to update the settings.

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

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



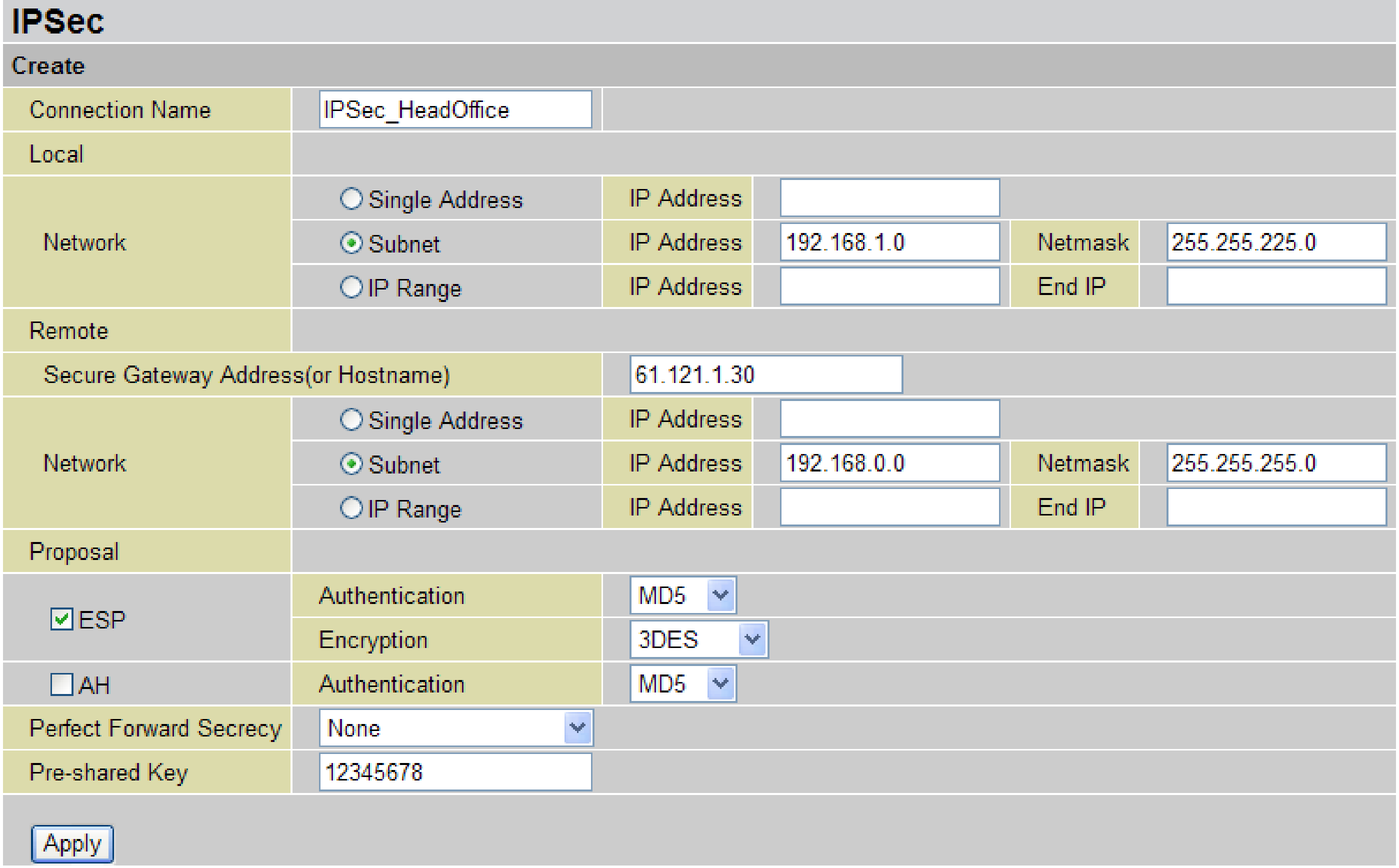
IPSec VPN-LAN to LAN

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

Attention

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

Configuring IPSec VPN in the Head Office



IPSec

Create

Connection Name	IPSec_HeadOffice				
Local					
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.1.0	Netmask	255.255.225.0
	○ IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)		61.121.1.30			
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
	○ IP Range	IP Address		End IP	
Proposal					
☑ ESP	Authentication	MD5			
	Encryption	3DES			
☐ AH	Authentication	MD5			
Perfect Forward Secrecy	None				
Pre-shared Key	12345678				

Connection Name: Specify a name for the PPTP connection (**IPSec_HeadOffice**).

Local Network: Check the Subnet radio button and enter the IP address (**192.168.1.0**) and subnet mask (**255.255.255.0**) of head office network.

Remote Secure Gateway Address (or Hostname): Enter the IP address (**69.121.1.30**) of the head office router (in WAN side).

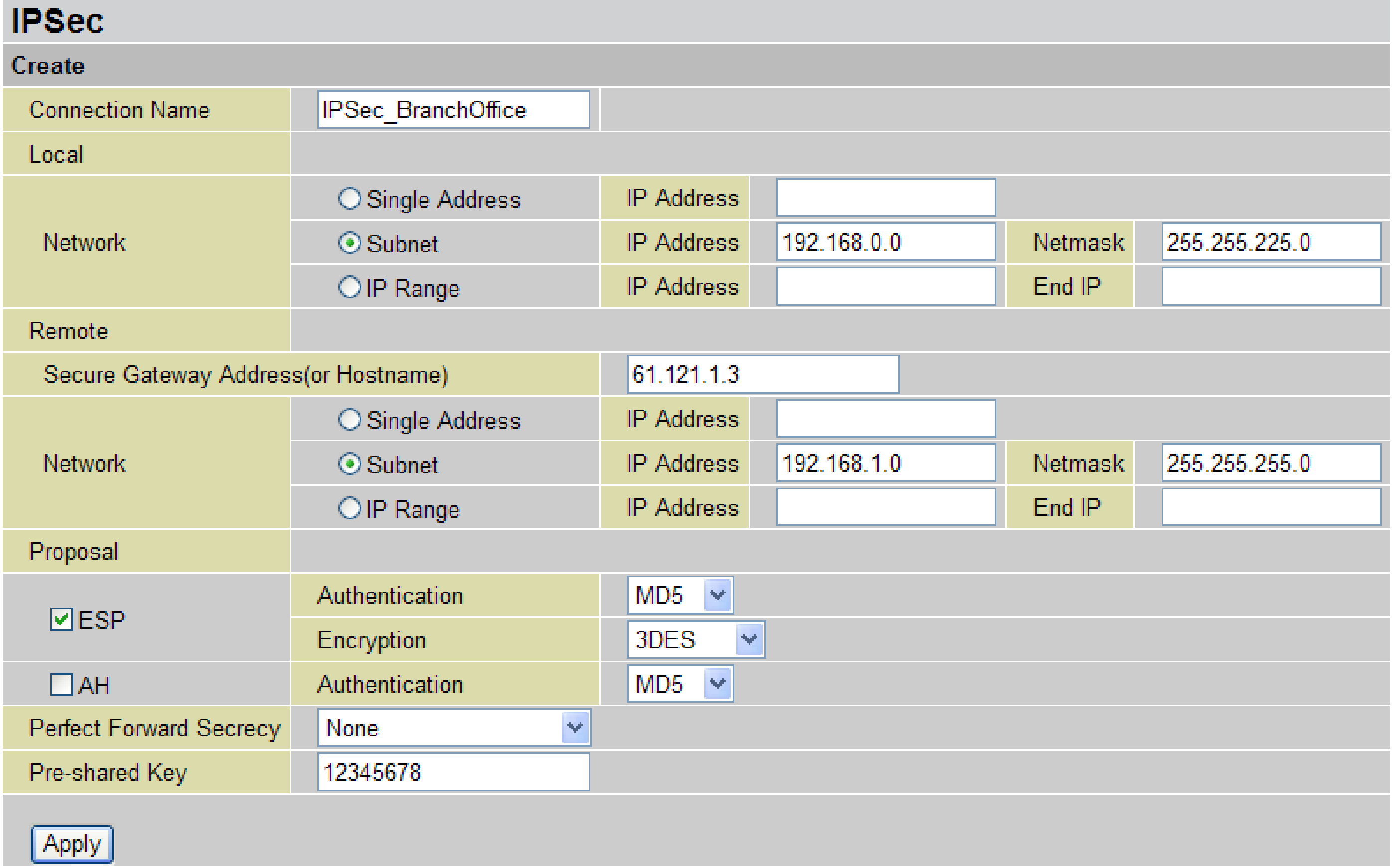
Remote Network: Check the Subnet radio button and enter the IP address (**192.168.0.0**) and subnet mask (**255.255.255.0**) of branch office network.

Proposal: Check the ESP radio button. Select **MD5** from the Authentication drop-down menu and **3DES** from the Encryption drop-down menu.

Prefer Forward Security and **Pre-shared Key**: Select the prefer forward security (**None**) and enter the pre-shared key (**12345678**) for security policy.

Click Apply to confirm the settings.

Configuring IPSec VPN in the Branch Office



IPSec

Create

Connection Name	IPSec_BranchOffice				
Local					
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.0.0	Netmask	255.255.225.0
	○ IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)		61.121.1.3			
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
	○ IP Range	IP Address		End IP	
Proposal					
☑ ESP	Authentication	MD5			
	Encryption	3DES			
☐ AH	Authentication	MD5			
Perfect Forward Secrecy	None				
Pre-shared Key	12345678				

Connection Name: Specify a name for the PPTP connection (**IPSec_BranchOffice**).

Local Network: Check the Subnet radio button and enter the IP address (**192.168.0.0**) and subnet mask (**255.255.255.0**) of branch office network.

Remote Secure Gateway Address (or Hostname): Enter the IP address (**69.121.1.3**) of the head office router (in WAN side).

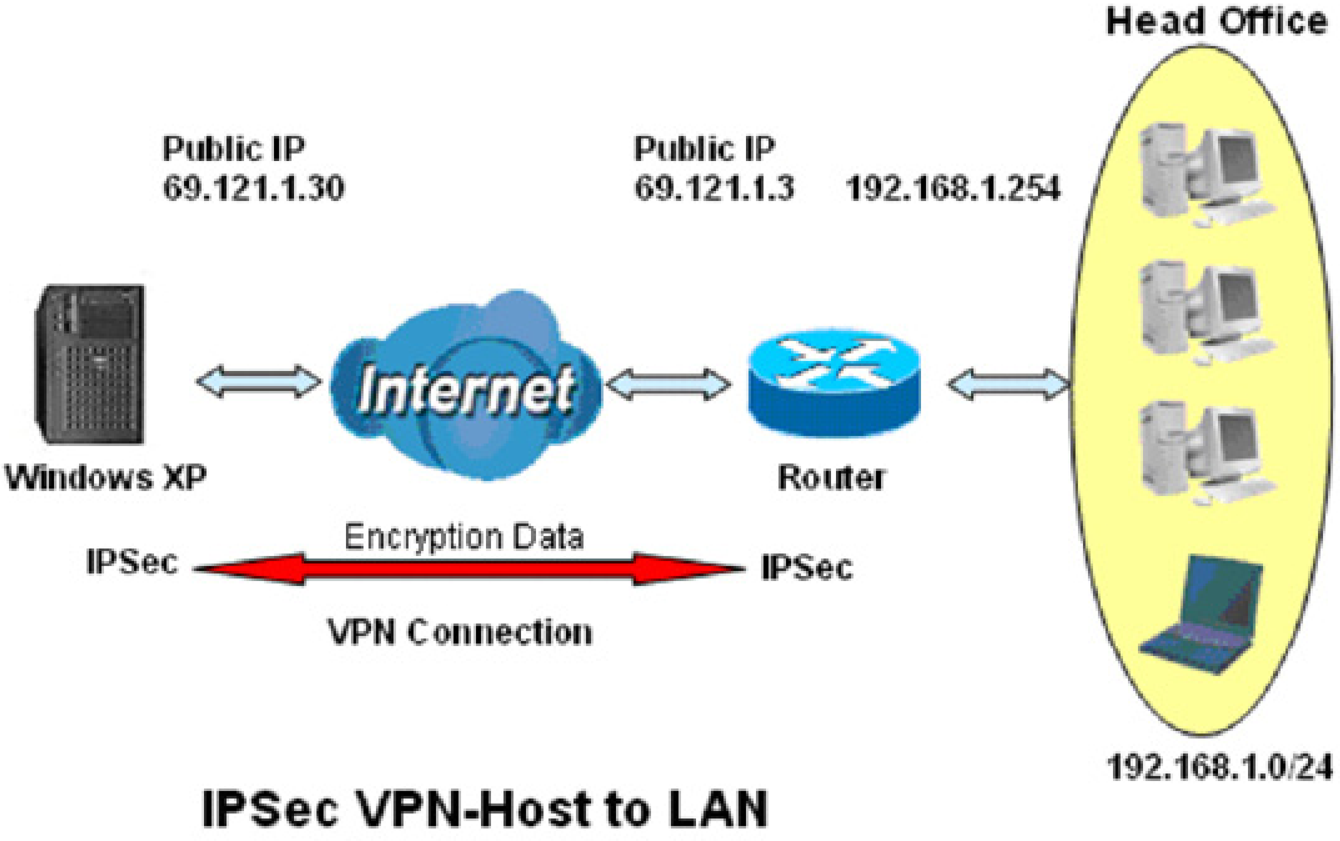
Remote Network: Check the Subnet radio button and enter the IP address (**192.168.1.0**) and subnet mask (**255.255.255.0**) of head office network.

Proposal: Check the ESP radio button. Select **MD5** from the Authentication drop-down menu and **3DES** from the Encryption drop-down menu.

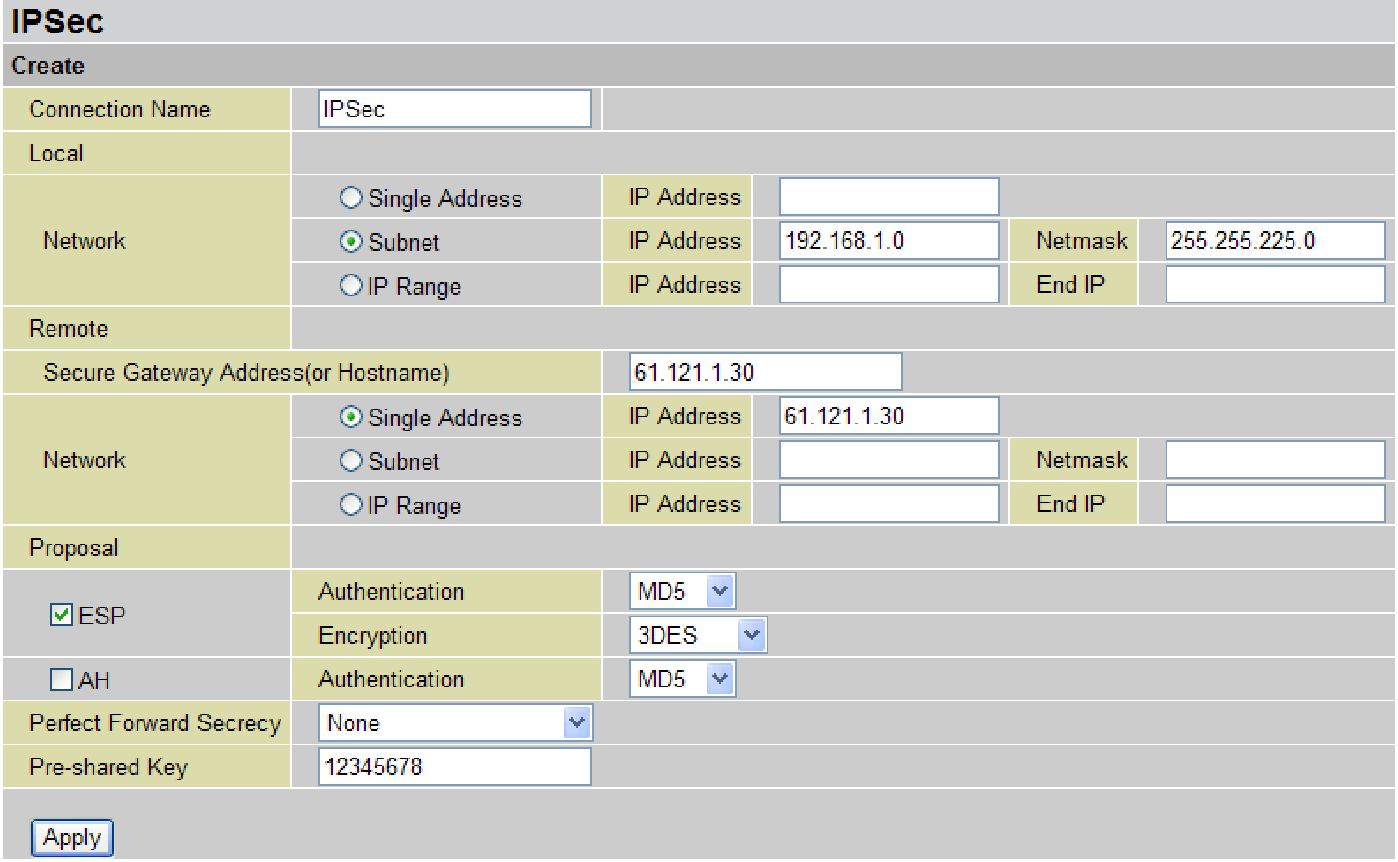
Prefer Forward Security and **Pre-shared Key**: Select the prefer forward security (**None**) and enter the pre-shared key (**12345678**) for security policy.

Click Apply to confirm the settings.

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



Configuring IPSec VPN in the Office



IPSec

Create

Connection Name	IPSec				
Local					
Network	○ Single Address	IP Address			
	● Subnet	IP Address	192.168.1.0	Netmask	255.255.225.0
	○ IP Range	IP Address		End IP	
Remote					
Secure Gateway Address(or Hostname)		61.121.1.30			
Network	● Single Address	IP Address	61.121.1.30		
	○ Subnet	IP Address		Netmask	
	○ IP Range	IP Address		End IP	
Proposal					
☑ ESP	Authentication	MD5			
	Encryption	3DES			
☐ AH	Authentication	MD5			
Perfect Forward Secrecy	None				
Pre-shared Key	12345678				

Connection Name: Specify a name for the PPTP connection (**IPSec**).

Local Network: Check the Subnet radio button and enter the IP address (**192.168.1.0**) and subnet mask (**255.255.255.0**) of head office network.

Remote Secure Gateway Address (or Hostname): Enter the IP address (**69.121.1.30**) of the head office router (in WAN side).

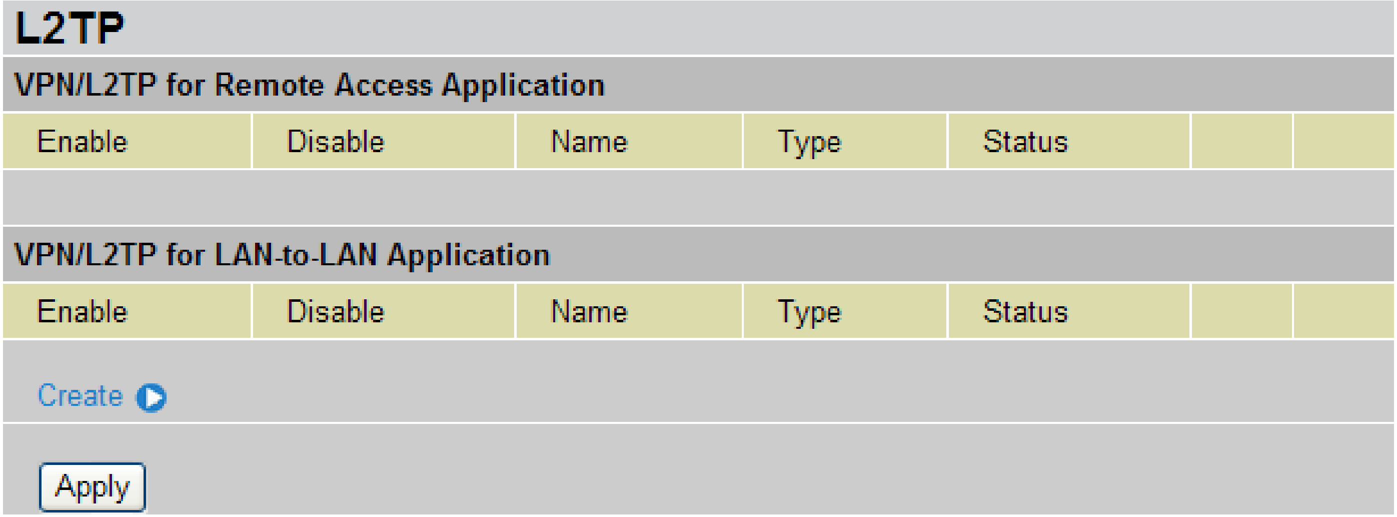
Remote Network: Check the Single Address radio button and enter the Remote worker's IP address (**69.121.1.30**).

Proposal: Check the ESP radio button. Select **MD5** from the Authentication drop-down menu and **3DES** from the Encryption drop-down menu.

Prefer Forward Security and **Pre-shared Key**: Select the prefer forward security (**None**) and enter the pre-shared key (**12345678**) for security policy.

Click Apply to confirm the settings.

L2TP (Layer Two Tunneling Protocol)



L2TP

VPN/L2TP for Remote Access Application

Enable	Disable	Name	Type	Status		

VPN/L2TP for LAN-to-LAN Application

Enable	Disable	Name	Type	Status		

If you have created a L2TP connection, the account information will be displayed.

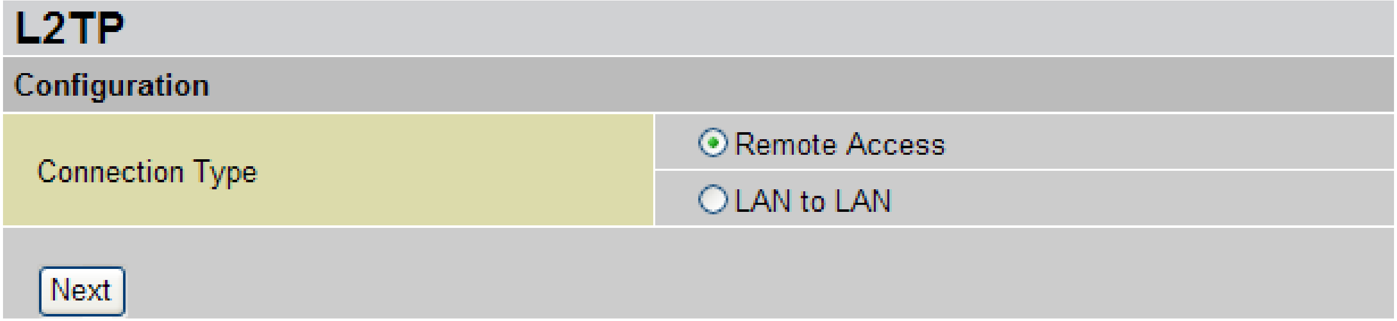
Enable / Disable: This function activates or inactivates the L2TP connection. To interrupt the tunnel, check the Disable radio button and click the Apply button to inactivate the connection.

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

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

Status: Shows the condition of your L2TP tunnel connection.

Click Create to configure a new VPN connection. There are 2 types of L2TP VPN supported: **Remote Access** and **LAN-to-LAN**.

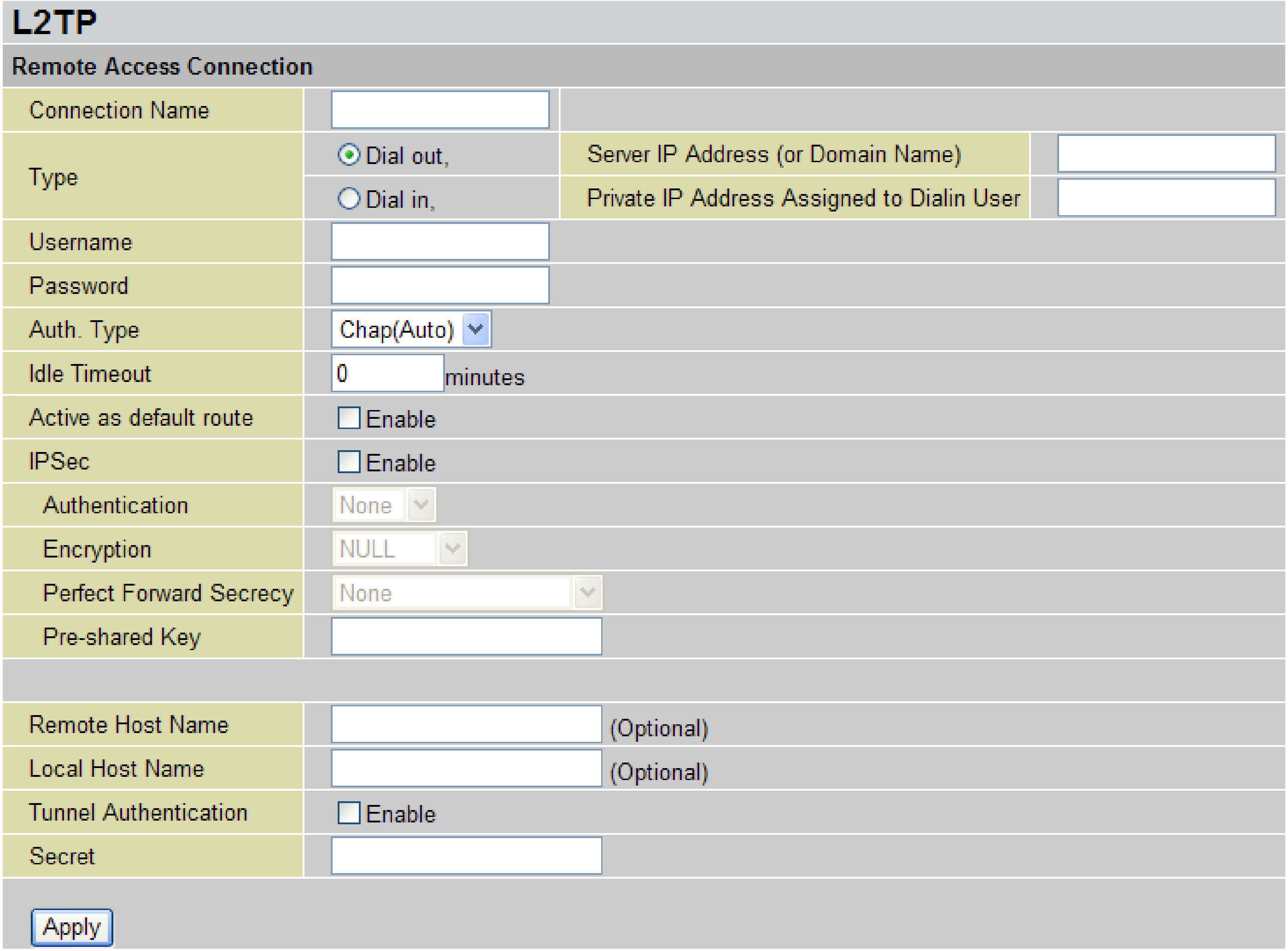


L2TP

Configuration

Connection Type	● Remote Access ○ LAN to LAN

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			

Connection Name: A 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 if you want the router to operate as a VPN server.

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

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

Auth. Type: Default is Auto, allows the router to determine which the type of authentication to use. You can also 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 the authentication type you want clients to use (when acting as a server). When using PAP, the password is sent unencrypted, CHAP encrypts the password before sending. This presents challenges at different periods to ensure that an intruder has not replaced the client.

Idle Timeout: 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, activate the function may degrade the Internet performance.

IPSec: Enable for enhancing your L2TP VPN security. (L2TP over IPSec (L2TP/IPSec) VPN Connection)

Note: Authentication, Encryption, Perfect Forward Secrecy and Pre-shared Key will only be available for selection after IPSec is enabled.

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

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

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

- **Encryption:** Select the encryption method from the pull-down menu. There are four options, DES, 3DES, AES and None. None indicates that it is only a tunnel with no encryption. 3DES and AES are more powerful but increase the 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 the encryption keys during 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 consists of 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 the router or host at both ends.

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

Note: This is used 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 default Hostname is home.gateway.

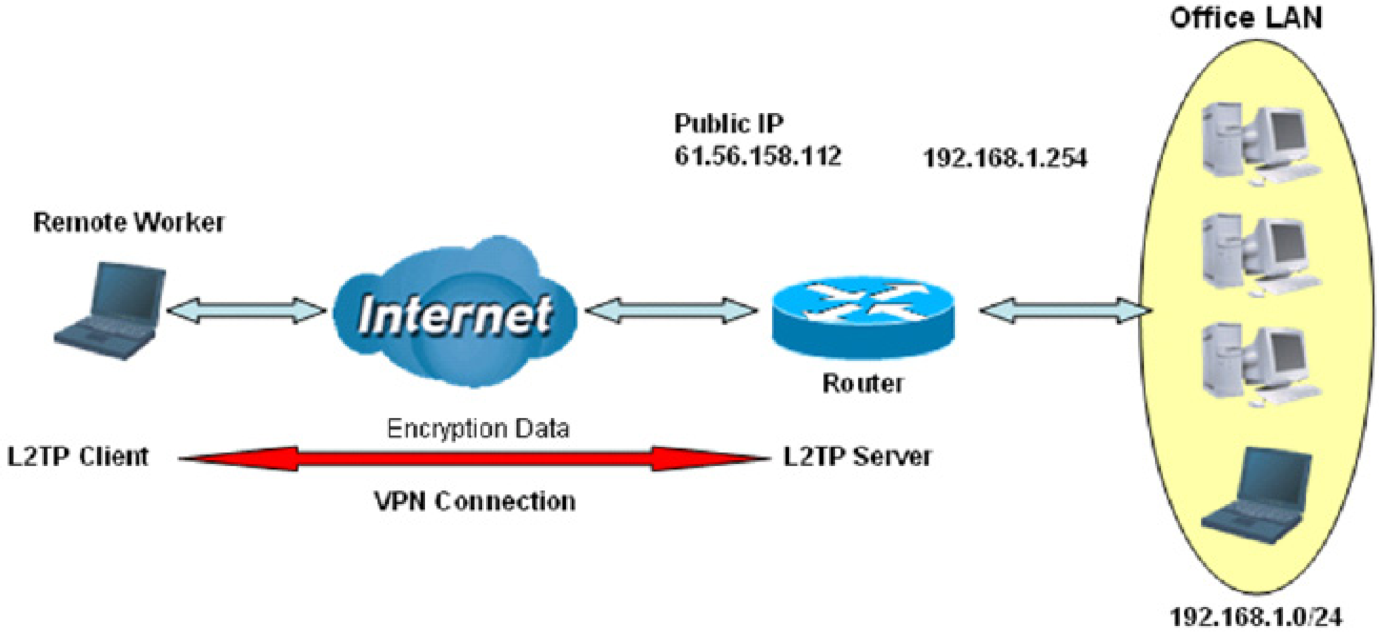
Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

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

Click the Apply button to save your changes.

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

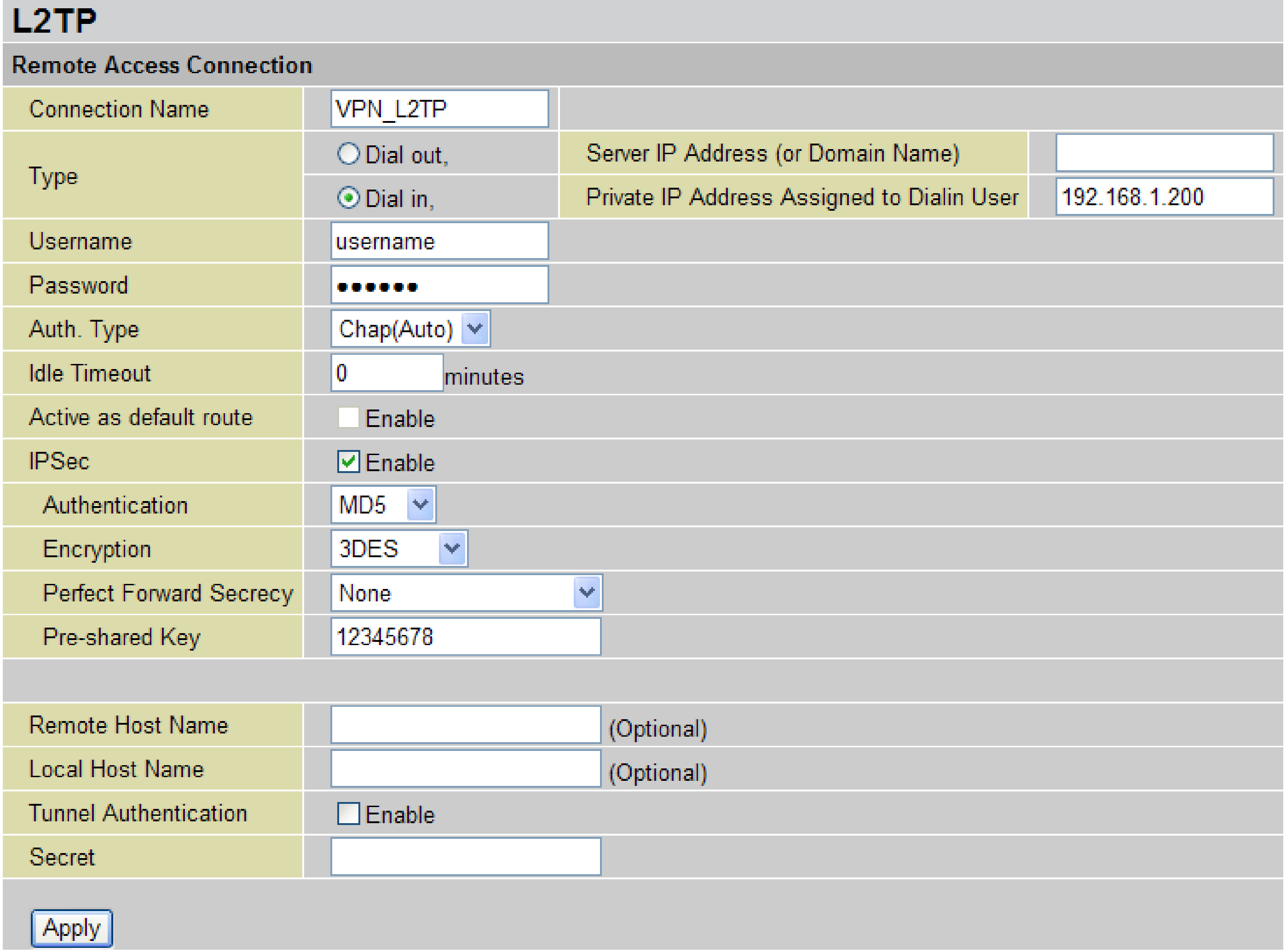
A remote worker establishes a L2TP VPN connection with the head office using Microsoft VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office, connecting to a couple of PCs and Servers.



L2TP VPN-Remote Access (Dial-in)

Configuring L2TP VPN in the Office-Dial In

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



L2TP

Remote Access Connection

Connection Name	VPN_L2TP		
Type	○ Dial out,	Server IP Address (or Domain Name)	
	● Dial in,	Private IP Address Assigned to Dialin User	192.168.1.200
Username	username		
Password	••••••		
Auth. Type	Chap(Auto)		
Idle Timeout	0 minutes		
Active as default route	☐ Enable		
IPSec	☑ Enable		
Authentication	MD5		
Encryption	3DES		
Perfect Forward Secrecy	None		
Pre-shared Key	12345678		
Remote Host Name	(Optional)		
Local Host Name	(Optional)		
Tunnel Authentication	☐ Enable		
Secret			

Connection Name: Specify a name for the L2TP connection (**VPN_L2TP**).

Type: Check **Dial in** and enter an assigned IP address (**192.168.1.200**) for the remote worker on the Private IP Address Assigned to Dialing User field.

Username / Password: Enter the username (**username**) & password (**123456**) to authenticate remote worker.

Auth.Type: Keep as default value in most of the cases.

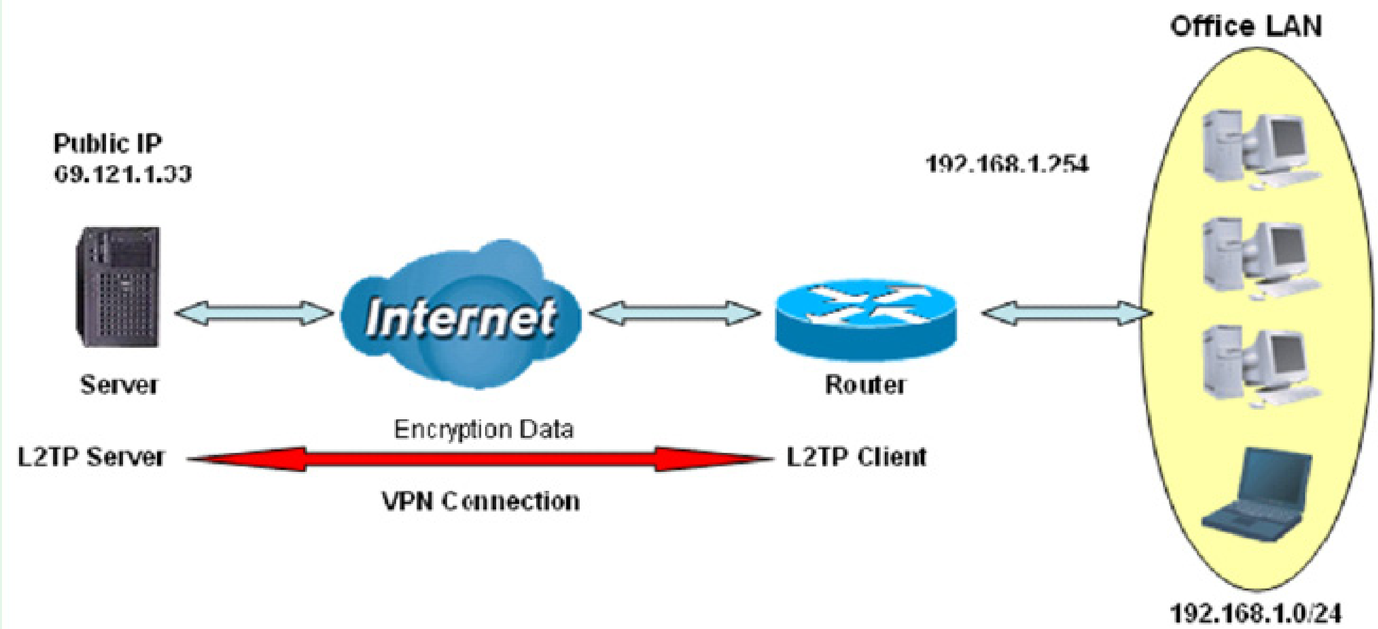
Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

IPSec: Enabled for enhancing your L2TP VPN security and then set the Authentication/Encryption/ Perfect Forward Secrecy/Pre-shared Key parameters. Both sites should use the same value.

Click Apply to save your settings.

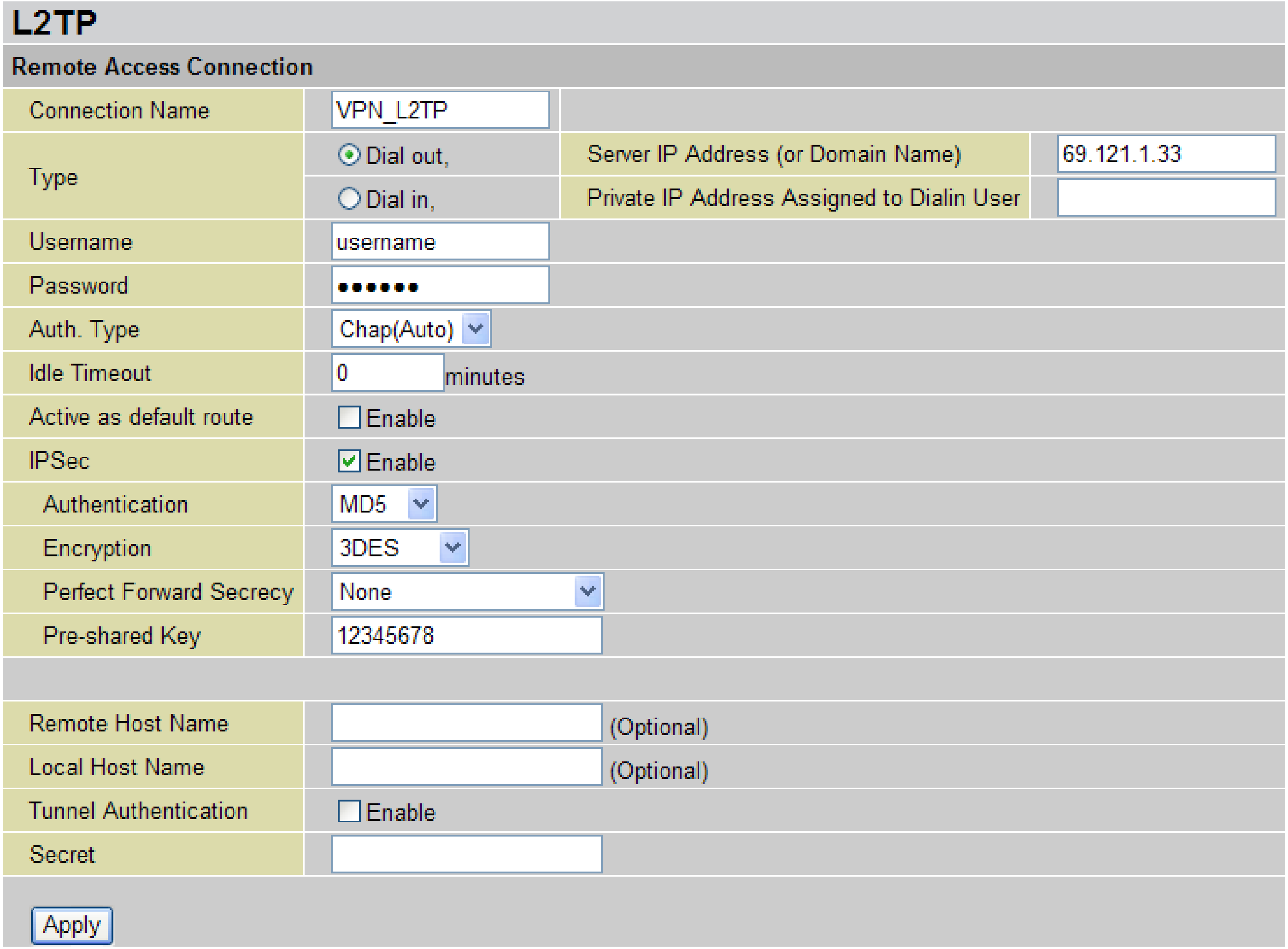
Example: Configuring a Remote Access L2TP VPN Dial-out Connection

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



L2TP VPN-Remote Access (Dial-out)

Configuring L2TP VPN in the Office-Dial Out



L2TP

Remote Access Connection

Connection Name	VPN_L2TP		
Type	● Dial out,	Server IP Address (or Domain Name)	69.121.1.33
	○ Dial in,	Private IP Address Assigned to Dialin User	
Username	username		
Password	••••••		
Auth. Type	Chap(Auto)		
Idle Timeout	0 minutes		
Active as default route	☐ Enable		
IPSec	☑ Enable		
Authentication	MD5		
Encryption	3DES		
Perfect Forward Secrecy	None		
Pre-shared Key	12345678		
Remote Host Name	(Optional)		
Local Host Name	(Optional)		
Tunnel Authentication	☐ Enable		
Secret			

Connection Name: Specify a name for the L2TP connection (**VPN_L2TP**).

Type: Check **Dial out** and enter a Dialed server IP (**69.121.1.33**) on the Server IP Address (or Hostname) field.

Username / Password: Enter the username (**username**) & password (**123456**).

Auth.Type: Keep as default value in most of the cases.

Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

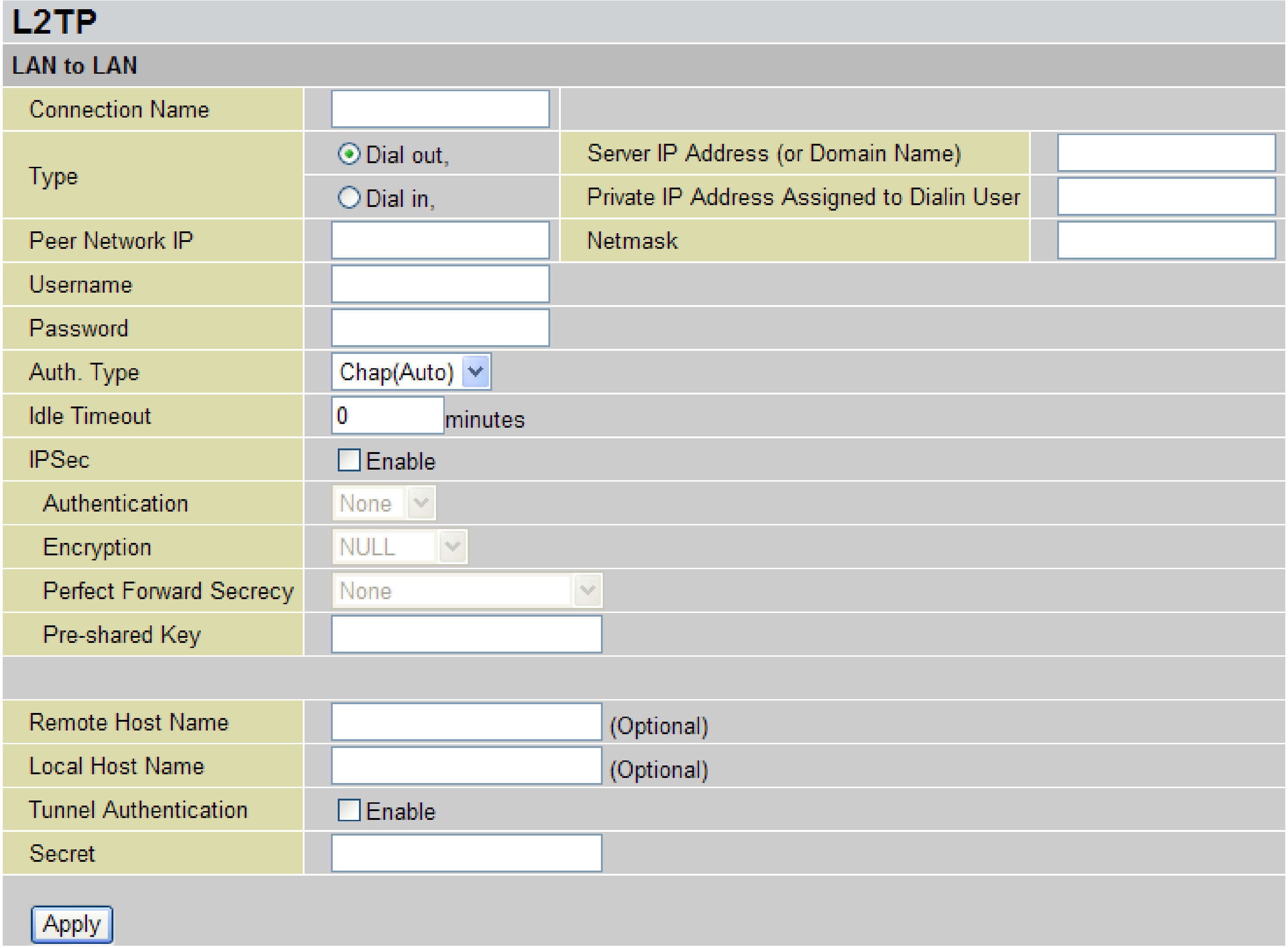
IPSec: Enabled for enhancing your L2TP VPN security and then set the Authentication/Encryption/ Perfect Forward Secrecy/Pre-shared Key parameters. Both sites should use the same value.

Click Apply to save your settings.

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

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

L2TP Connection - LAN to LAN



L2TP

LAN to LAN

Connection Name			
Type	● Dial out,	Server IP Address (or Domain Name)	
	○ Dial in,	Private IP Address Assigned to Dialin User	
Peer Network IP		Netmask	
Username			
Password			
Auth. Type	Chap(Auto)		
Idle Timeout	0 minutes		
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			

Connection Name: A user-defined name for 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 if you want it to operate as a VPN server.

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

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

Peer Network IP: Enter the Peer network IP address.

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

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

Authentication Type: Default is Auto, allows the router to determine which authentication type to use. You can also 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 the authentication type you want clients to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending. This presents challenges at different periods to ensure that an intruder has not replaced the client.

Idle Timeout: 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.

IPSec: Enabled for enhancing your L2TP VPN security. (L2TP over IPSec (L2TP/IPSec) VPN Connection)

Note: Authentication, Encryption, Perfect Forward Secrecy and Pre-shared Key will only be available for selection after IPSec is enabled.

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

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

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

- **Encryption:** Select the encryption method from the pull-down menu. There are four options, DES, 3DES, AES and None. None indicates that it is only a tunnel with no encryption. 3DES and AES are more powerful but increase the 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 the encryption keys during 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 consists of 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 the router or host at both ends.

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

Note: This is used 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 default Hostname is home.gateway.

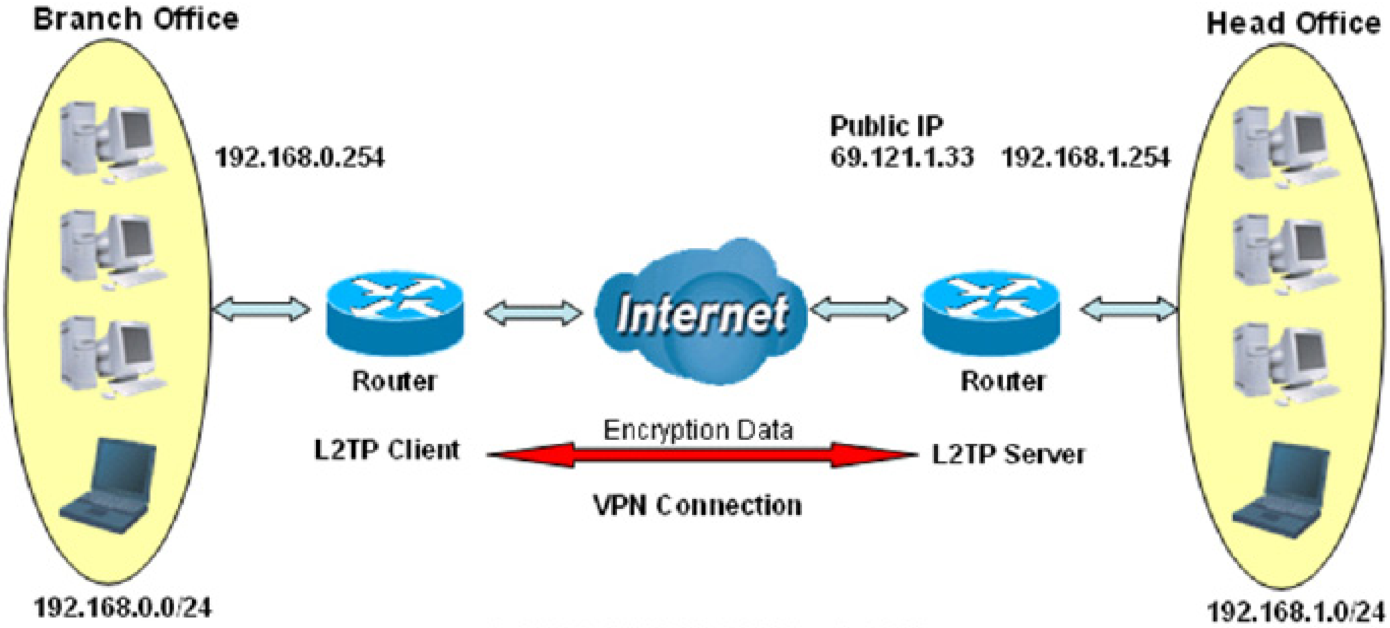
Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

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

Click the Apply button to save your settings.

Example: Configuring L2TP LAN-to-LAN VPN Connection

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



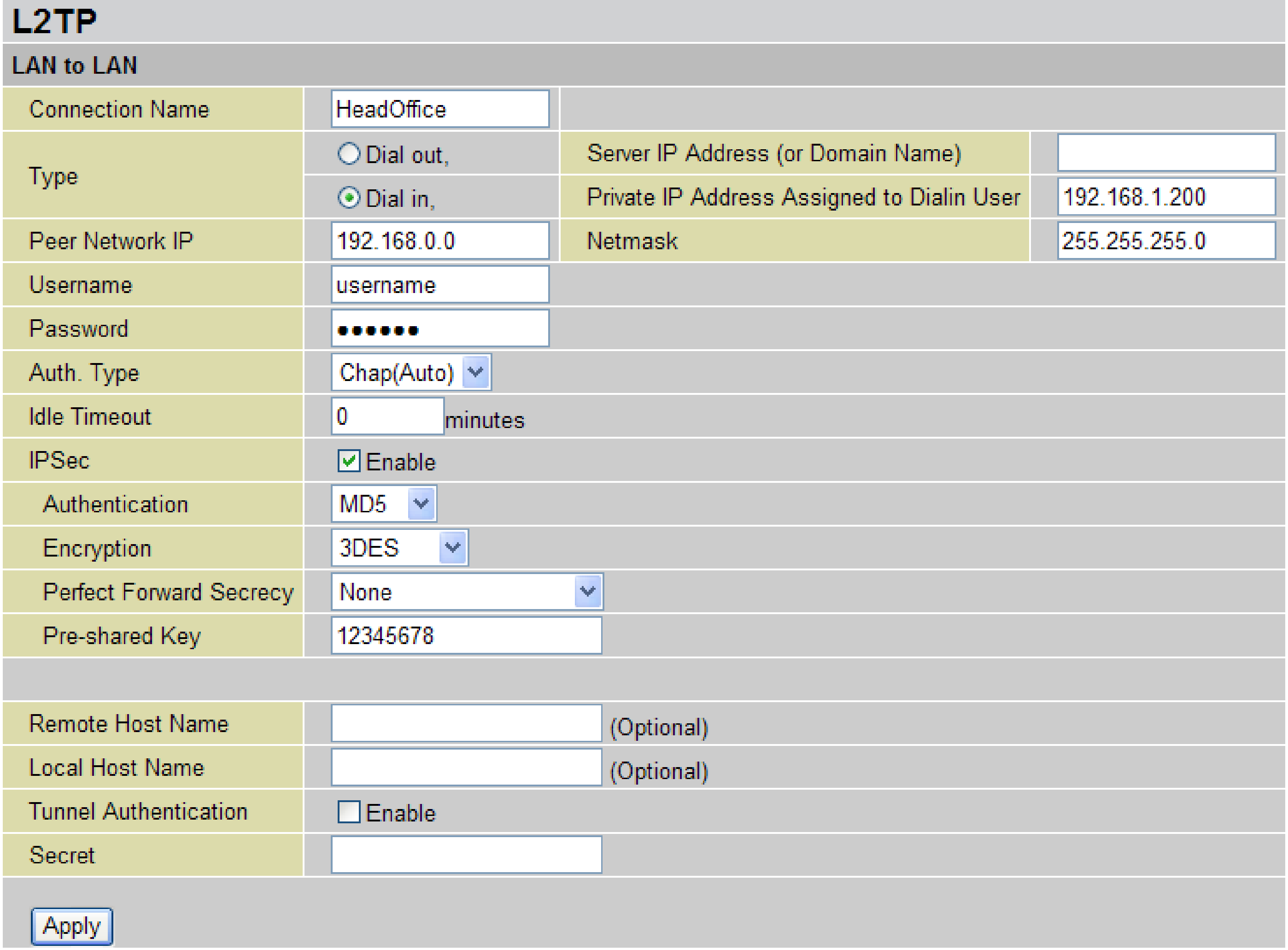
L2TP VPN-LAN to LAN

Attention

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

Configuring L2TP VPN in the Head Office

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



L2TP

LAN to LAN

Connection Name	HeadOffice		
Type	○ Dial out,	Server IP Address (or Domain Name)	
	● Dial in,	Private IP Address Assigned to Dialin User	192.168.1.200
Peer Network IP	192.168.0.0	Netmask	255.255.255.0
Username	username		
Password	●●●●●●		
Auth. Type	Chap(Auto)		
Idle Timeout	0 minutes		
IPSec	☑ Enable		
Authentication	MD5		
Encryption	3DES		
Perfect Forward Secrecy	None		
Pre-shared Key	12345678		
Remote Host Name	(Optional)		
Local Host Name	(Optional)		
Tunnel Authentication	☐ Enable		
Secret			

Connection Name: Specify a name for the L2TP connection (**HeadOffice**).

Type: Check **Dial in** and enter the IP address (**192.168.1.0**) assigned to the branch office network on the Private IP Address Assigned to Dialing User field.

Peer Network IP: Enter the IP address (**192.168.0.0**) and subnet mask (**255.255.255.0**) of branch office network.

Username / Password: Enter the username (**username**) & password (**123456**) to authenticate remote worker.

Auth.Type: Keep as default value in most of the cases.

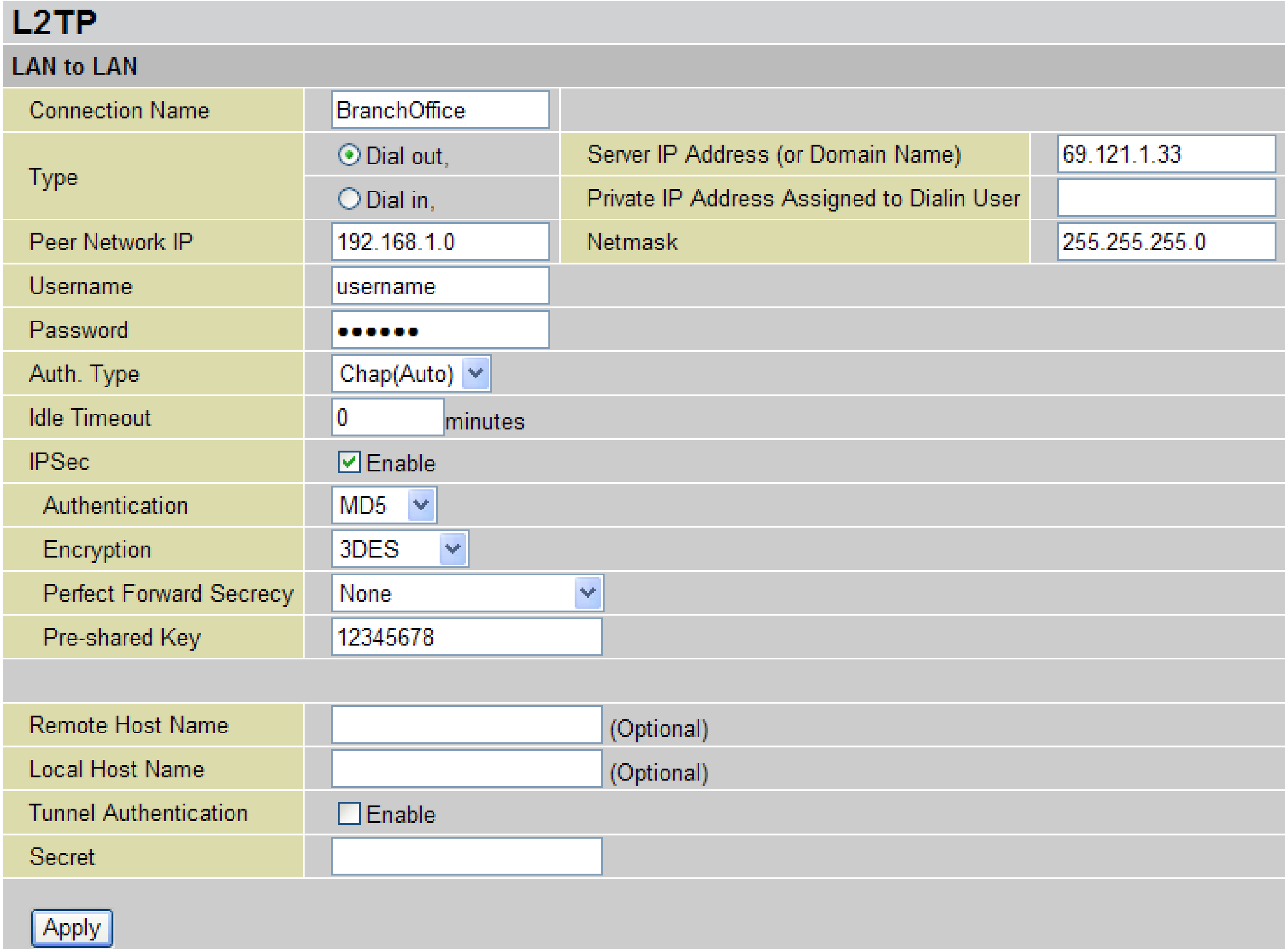
Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

IPSec: Enabled for enhancing your L2TP VPN security and then set the Authentication/Encryption/ Perfect Forward Secrecy/Pre-shared Key parameters. Both sites should use the same value.

Click Apply to confirm the settings.

Configuring L2TP VPN in the Branch Office

The IP address 69.1.121.30 is the Public IP address of the router located at 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.



L2TP

LAN to LAN

Connection Name	BranchOffice		
Type	● Dial out,	Server IP Address (or Domain Name)	69.121.1.33
	○ Dial in,	Private IP Address Assigned to Dialin User	
Peer Network IP	192.168.1.0	Netmask	255.255.255.0
Username	username		
Password	••••••		
Auth. Type	Chap(Auto)		
Idle Timeout	0 minutes		
IPSec	☑ Enable		
Authentication	MD5		
Encryption	3DES		
Perfect Forward Secrecy	None		
Pre-shared Key	12345678		
Remote Host Name	(Optional)		
Local Host Name	(Optional)		
Tunnel Authentication	☐ Enable		
Secret			

Connection Name: Specify a name for the L2TP connection (**BranchOffice**).

Type: Check **Dial out** and enter the IP address (**69.121.1.33**) of the head office router (in WAN side).

Peer Network IP: Enter the IP address (**192.168.1.0**) and subnet mask (**255.255.255.0**) of head office network.

Username / Password: Enter the username (**username**) & password (**123456**) to authenticate branch office network.

Auth.Type: Keep as default value in most of the cases.

Idle Timeout: The connection will be disconnected when there is no traffic in a predefined period of time. **0** means always on.

IPSec: Enabled for enhancing your L2TP VPN security and then set the Authentication/Encryption/ Perfect Forward Secrecy/Pre-shared Key parameters. Both sites should use the same value.

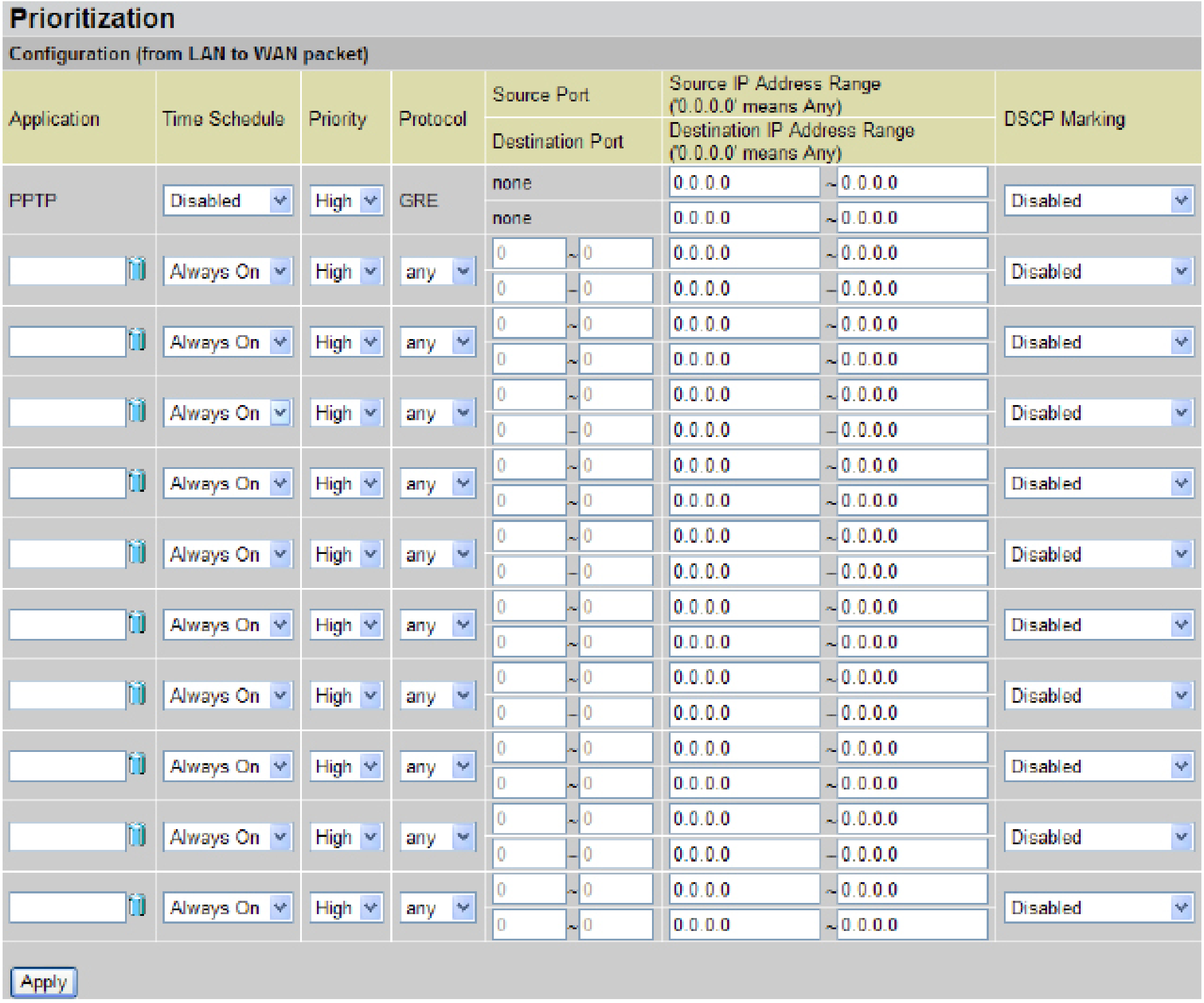
Click Apply to confirm the settings.

QoS - Quality of Service

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

You can find three items under the QoS section: **Prioritization** and **Outbound / Inbound IP Throttling** (bandwidth management).

Prioritization



Prioritization

Configuration (from LAN to WAN packet)

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

Application: Assign a name that identifies the new QoS application rule.

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: Select the supported protocol from the drop down list. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

any: No protocol type is specified.

tcp

udp

icmp

gre: For PPTP VPN Connections.

Source/Destination Port: The packet source/destination port to be monitored.

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

Priority: The priority given to each policy/application. You may adjust this setting to fit your policy / application. For examples, you are allowed to specify two different QoS policies for different applications. Both applications need minimal or higher bandwidth, besides the assigned one, if there is any available/non-used one available, you can specify which application can have higher priority by acquiring the non-used bandwidth. Average utilization of each priority type: High (60%), Normal (30%) and Low (10%).

High

Normal: The default is set to normal.

Low

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

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

Note: Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.

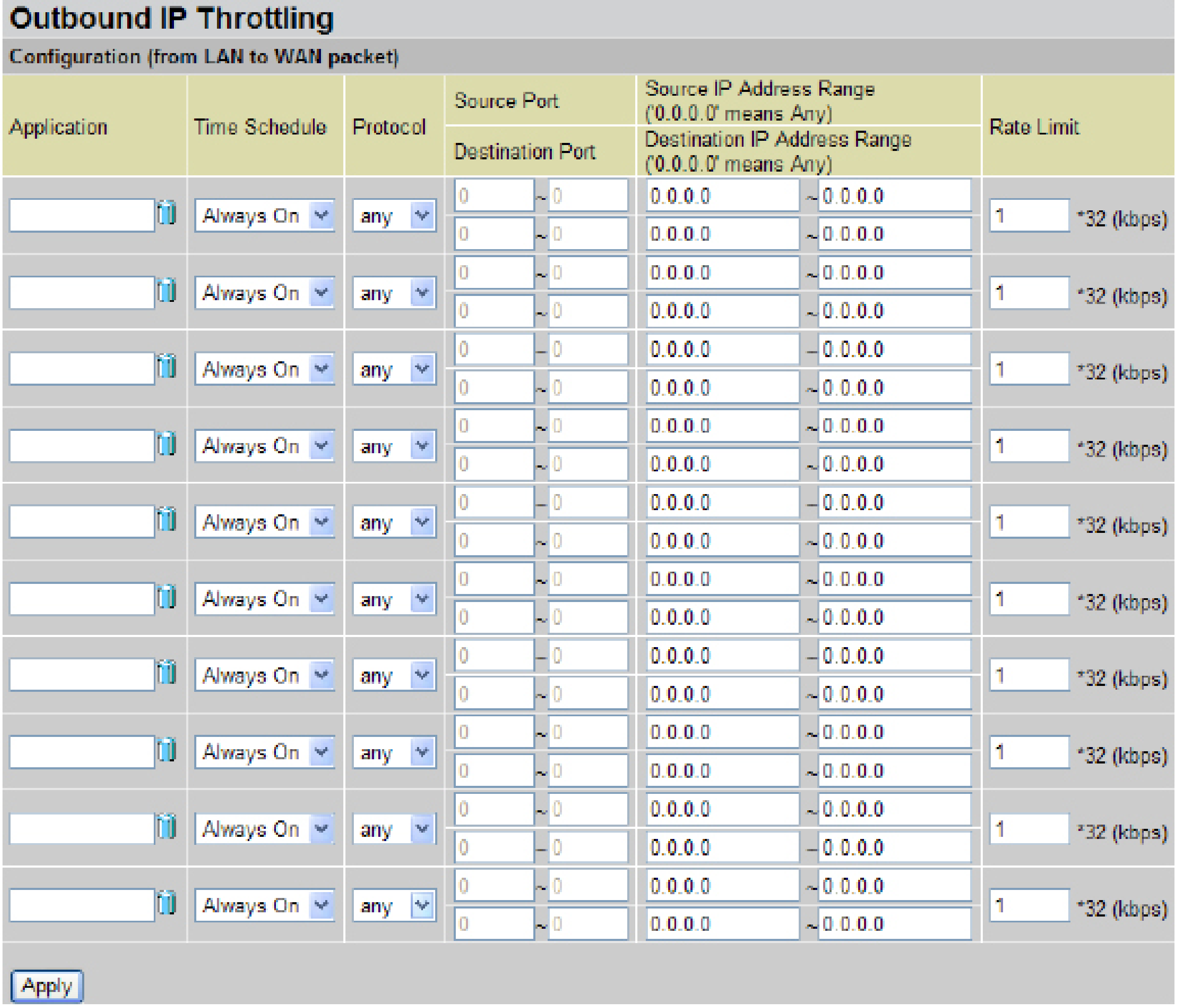
DSCP Mapping Table

DSCP Mapping Table	
(Wireless) GPON 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)

Remember clicking Apply to save your settings.

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 multiple of 32kbps.



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
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)

Application: Assign a name that identifies the new QoS application rule.

Time Schedule: Scheduling your prioritization policy.

Protocol: Select the supported protocol from the drop down list.

Source/Destination Port: The packet source/destination port to be monitored.

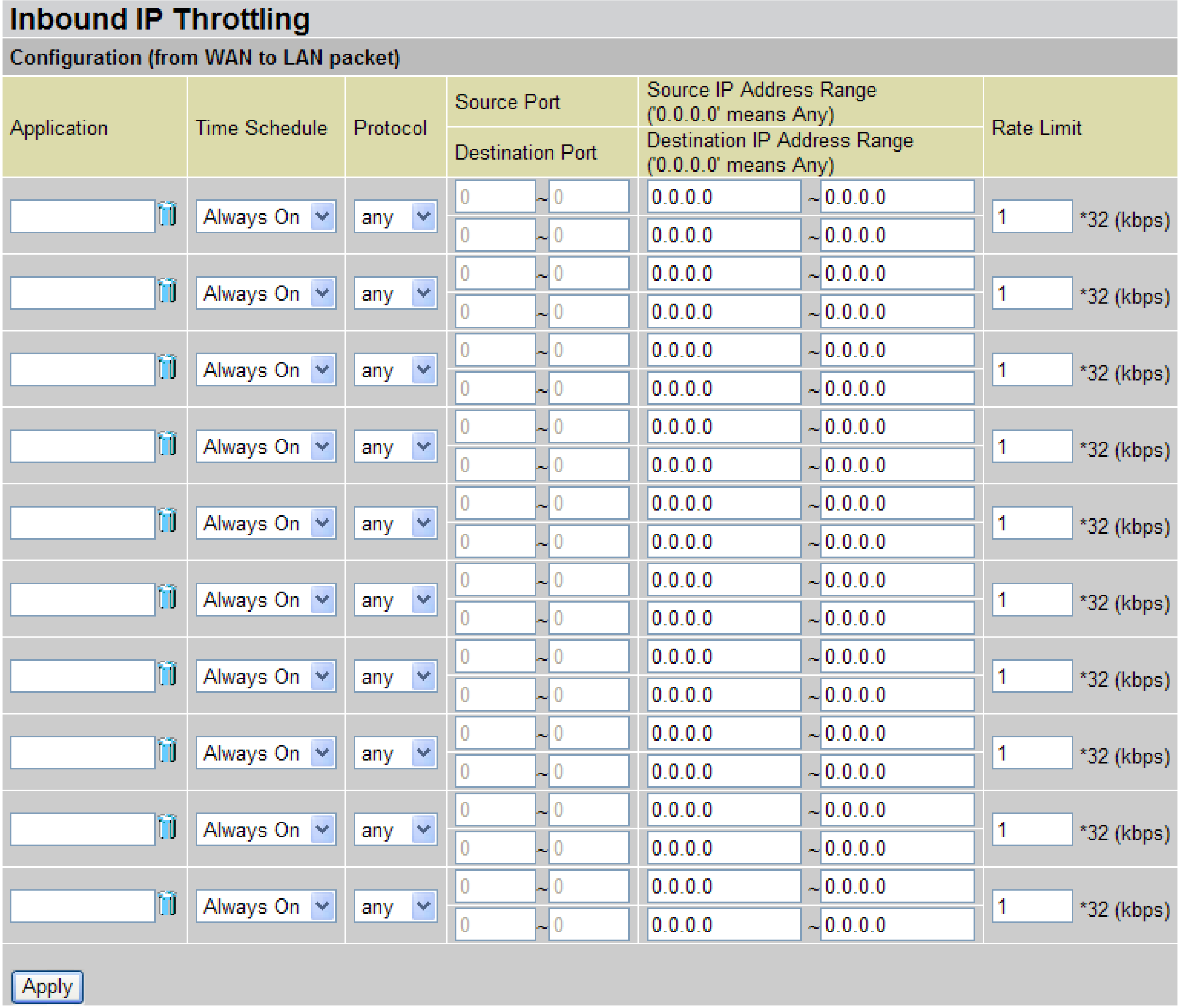
Source/Destination IP Address Range: The source/destination IP address or range of packets to be monitored.

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

Click Apply to confirm the settings.

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 multiple of 32kbps.



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
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)
	Always On	any	0 ~ 0 0 ~ 0	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	1 *32 (kbps)

Application: Assign a name that identifies the new QoS application rule.

Time Schedule: Scheduling your prioritization policy.

Protocol: Select the supported protocol from the drop down list.

Source/Destination Port: The packet source/destination port to be monitored.

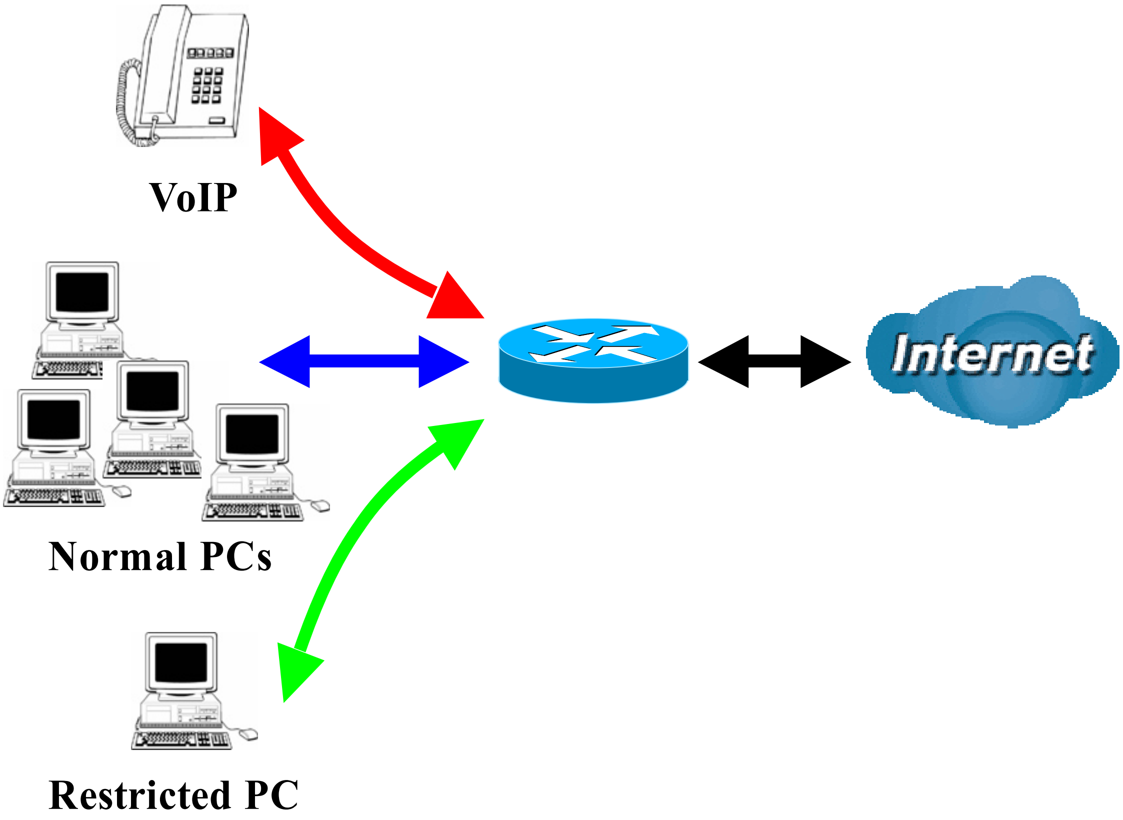
Source/Destination IP Address Range: The source/destination IP address or range of packets to be monitored.

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

Click Apply to confirm the settings.

Example: QoS for your Network

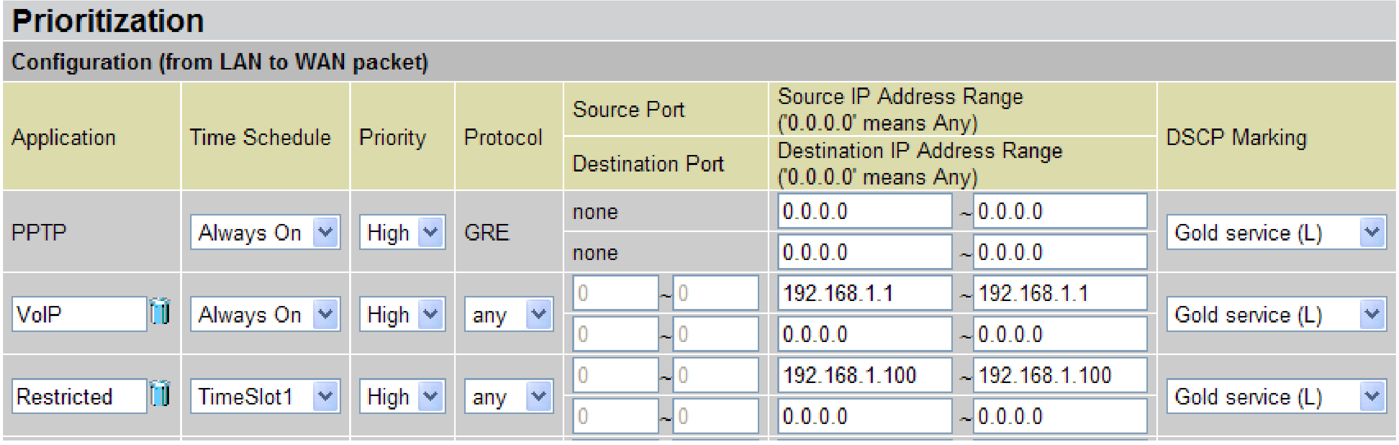
Connection Diagram



Information and Settings

Upstream: 928 kbps
Downstream: 8 Mbps

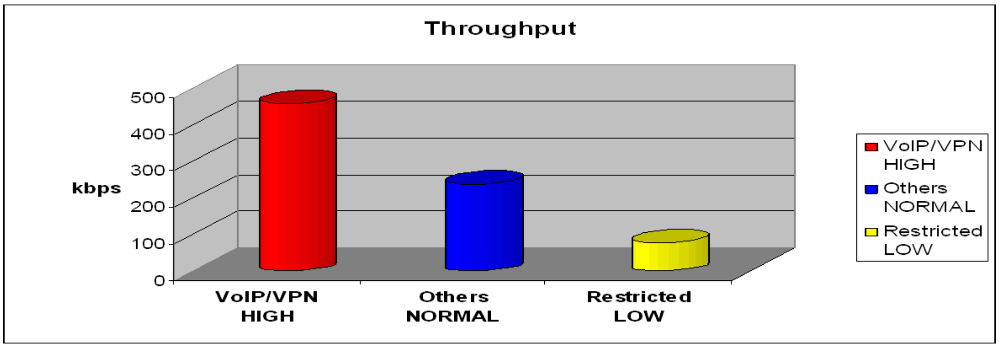
VoIP User : 192.168.1.1
Normal Users : 192.168.1.2~192.168.1.5
Restricted User: 192.168.1.100



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 none	0.0.0.0 ~ 0.0.0.0 0.0.0.0 ~ 0.0.0.0	Gold service (L)
VoIP	Always On	High	any	0 ~ 0 0 ~ 0	192.168.1.1 ~ 192.168.1.1 0.0.0.0 ~ 0.0.0.0	Gold service (L)
Restricted	TimeSlot1	High	any	0 ~ 0 0 ~ 0	192.168.1.100 ~ 192.168.1.100 0.0.0.0 ~ 0.0.0.0	Gold service (L)



Mission-critical application

VPN connection is a mission-critical application used for data exchange between head office and branch office. This mission-critical application must be sent out smoothly without any dropping. Set this application as high priority to prevent other applications to saturate the bandwidth.

Voice application

Voice is latency-sensitive application. Most VoIP devices use SIP protocol and the port number will be assigned by SIP module automatically. It is recommended to set a high priority for catching VoIP packets with a fixed IP address. The settings will help to improve the quality of your VoIP service when the traffic loading is full.

Restricted Application

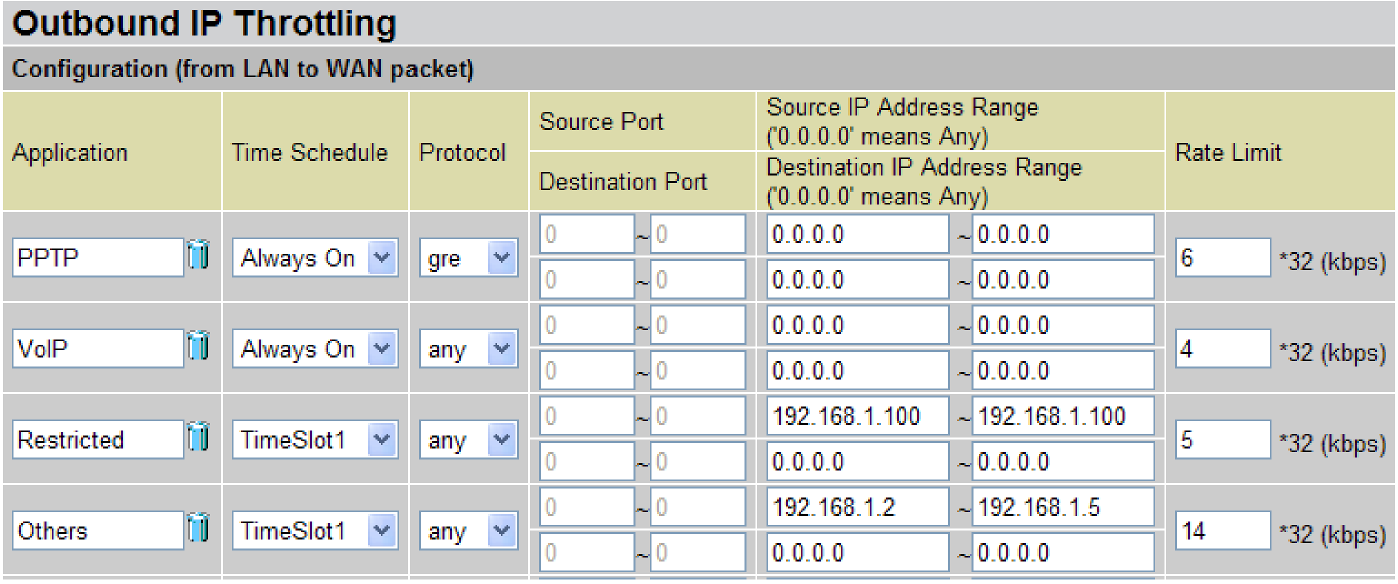
Some companies will setup a FTP server for customers to download files or home users to share their files via FTP. The settings help to limit upstream utilization of the FTP. Time schedule feature also helps to limit daytime utilization.

Advanced setting by using IP throttling

With IP throttling you can set more detailed parameters to manage bandwidth allocation even when the applications are located on the same level.

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

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

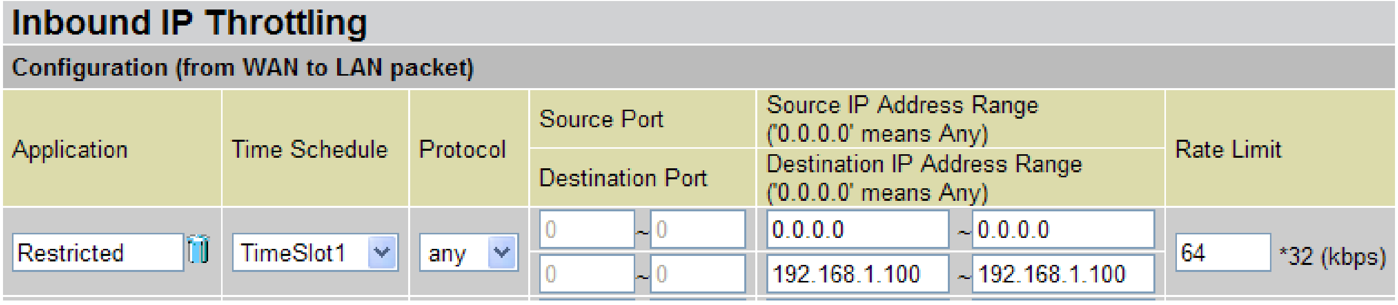


Outbound IP Throttling

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 saturate your downstream bandwidth. The settings below can help you to limit the 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	

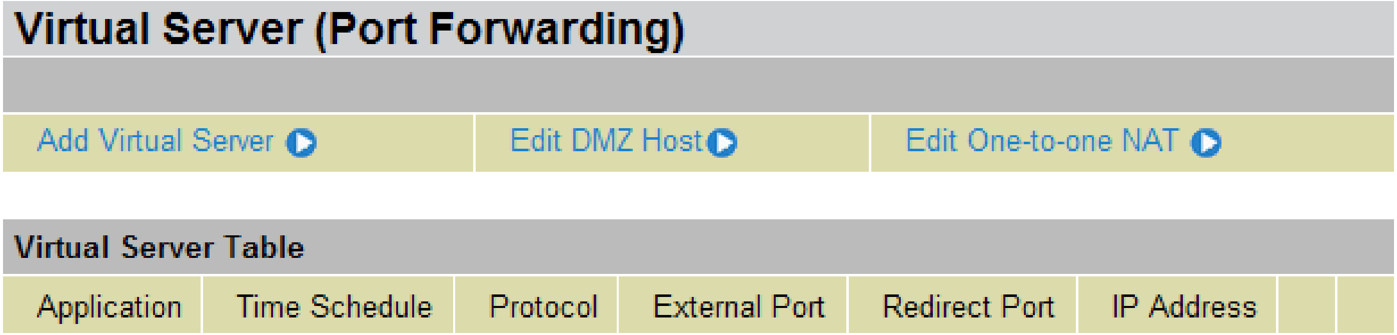
Virtual Server (Port Forwarding)

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

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.

In TCP 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 need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.



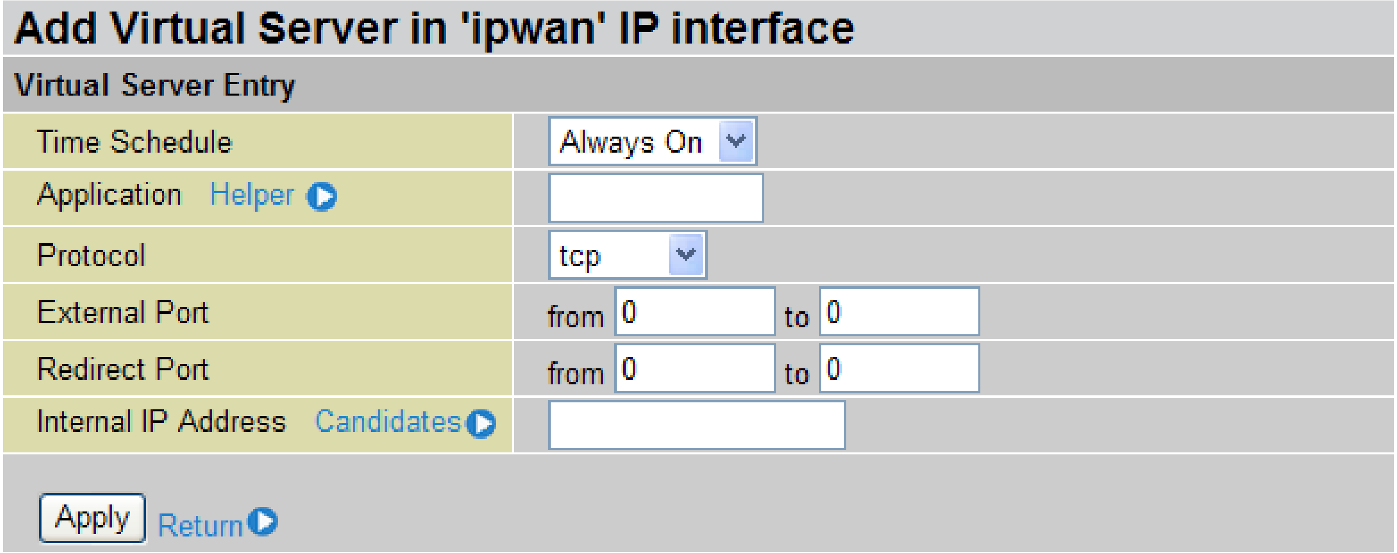
Virtual Server Table

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 new 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.


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	

Time Schedule: A self-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. There are 20 predefined rules. 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 being used. The protocol used is determined by a particular application. Most applications will use TCP or UDP.

External Port: The Port number which will be used by the Remote/WAN client when accessing the virtual server.

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

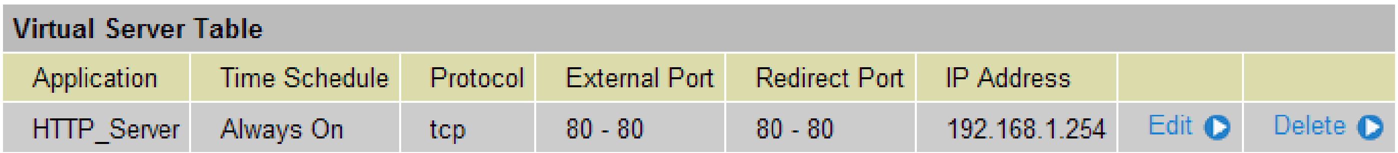
Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application. **Candidates** list all the existing PCs connecting to the network. You can assign a PC a specific IP address and MAC from this list.

Example:

If you like to access your Router remotely through the Web/HTTP at all time, you would need to enable port number 80 (Web/HTTP) and map to the Router IP Address. Then all incoming HTTP requests from you (Remote side) will be forwarded to the Router with the IP address of 192.168.1.254. Since port number 80 has already been predefined, next to the Application click Helper. When a predefined rule window pops up, select HTTP_Sever from the rule list.

Application: *HTT_Sever*
Time Schedule: *Always On*
Protocol: *tcp*
External Port: *80-80*
Redirect Port: *80-80*

IP Address: *192.168.1.254*



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 to change virtual server application parameters.

Delete: Click to remove virtual server application entry.

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.

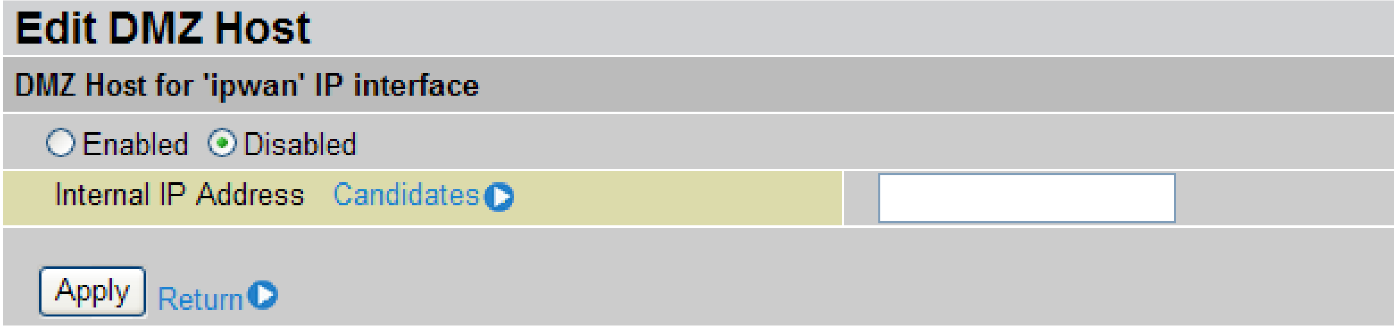
Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP addresses 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 that use the port number different from the one used by other Virtual Server entries will be checked by the Firewall and NAT algorithms before being passed to the DMZ host.

Note: The local computer exposing to the Internet may face various security risks.



Edit DMZ Host

DMZ Host for 'ipwan' IP interface

○ Enabled ● Disabled

Internal IP Address

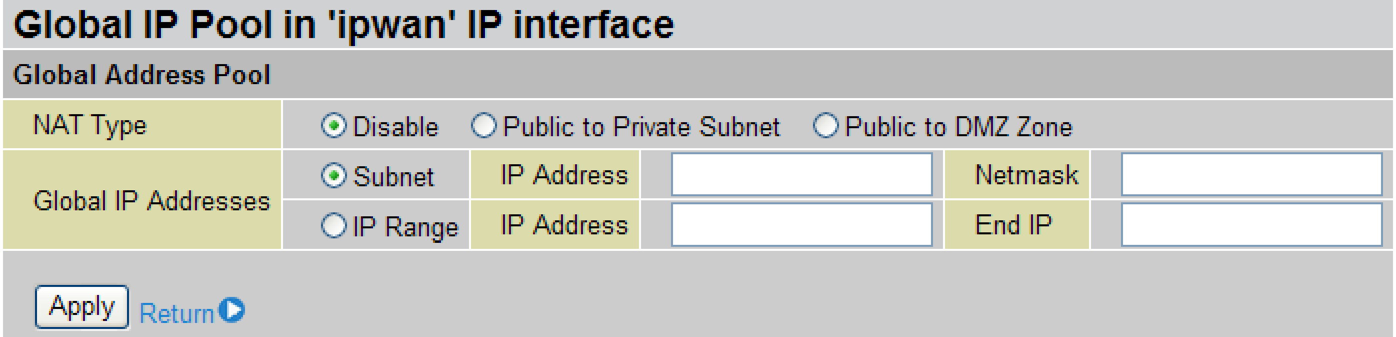
- **Disabled:** As set in default setting, it disables the DMZ function.
- **Enabled:** Select to activate your DMZ function.

Internal IP Address: Specify a static IP address to the DMZ Host when the Enabled radio button is checked. Be aware that this IP will be exposed to the WAN/Internet. **Candidates** list all the existing PCs connecting to the network. You can assign a PC a specific IP address and MAC from this list.

Click Apply to confirm the change.

Edit One-to-one NAT

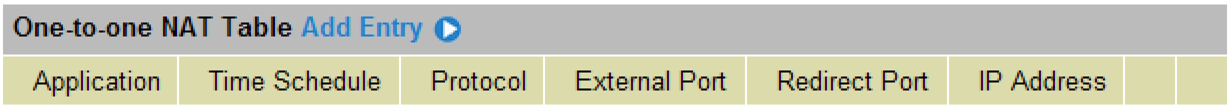
One-to-One NAT maps a specific private/local IP address to a global/public IP address. If you have multiple public/WAN IP addresses from you ISP, you are eligible for One-to-One NAT to utilize these IP addresses.



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	



One-to-one NAT Table Add Entry

Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address		

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

Global IP Address:

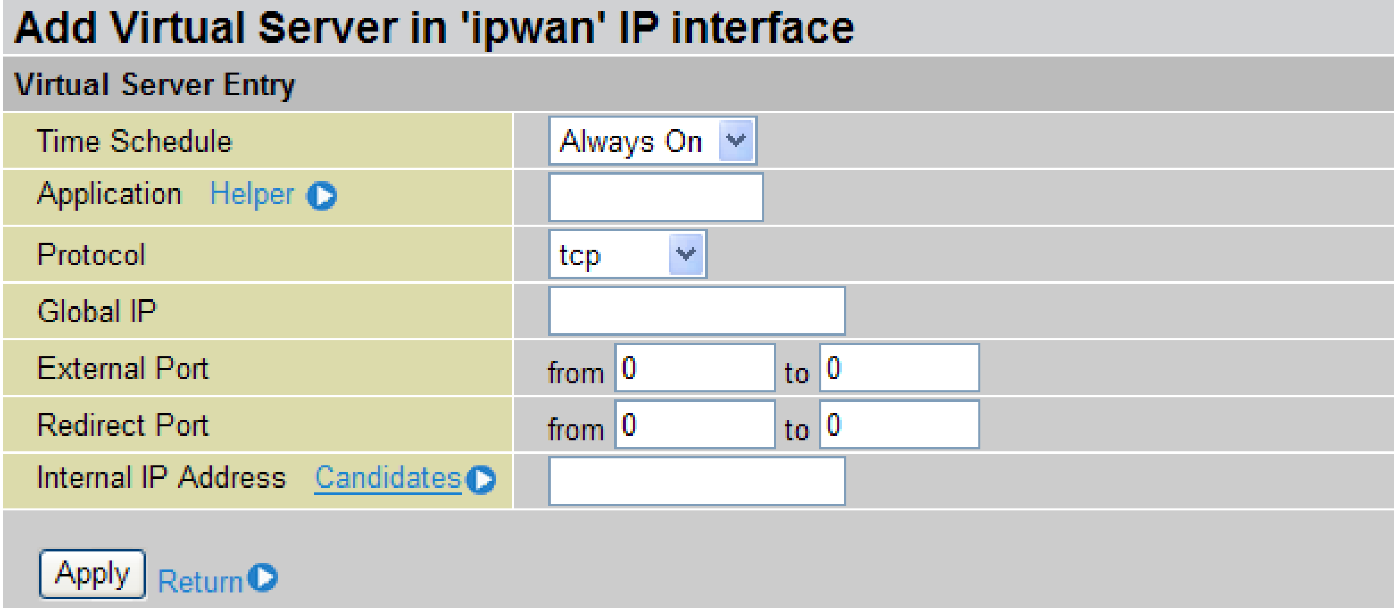
- **Subnet:** The subnet of the public/WAN IP address given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use IP Range method.
- **IP Range:** The IP address range of your public/WAN IP addresses. For example, IP address: 192.168.1.1, End IP: 192.168.1.10.

Click Apply to confirm the settings.

Add a new rule

Check Add Entry to create a new One-to-One NAT rule. Please refer to **Add Virtual Server** section.

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



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	

Click Apply to confirm the settings.

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 below). 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.

Examples of well-known and registered port numbers are shown below, 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**.

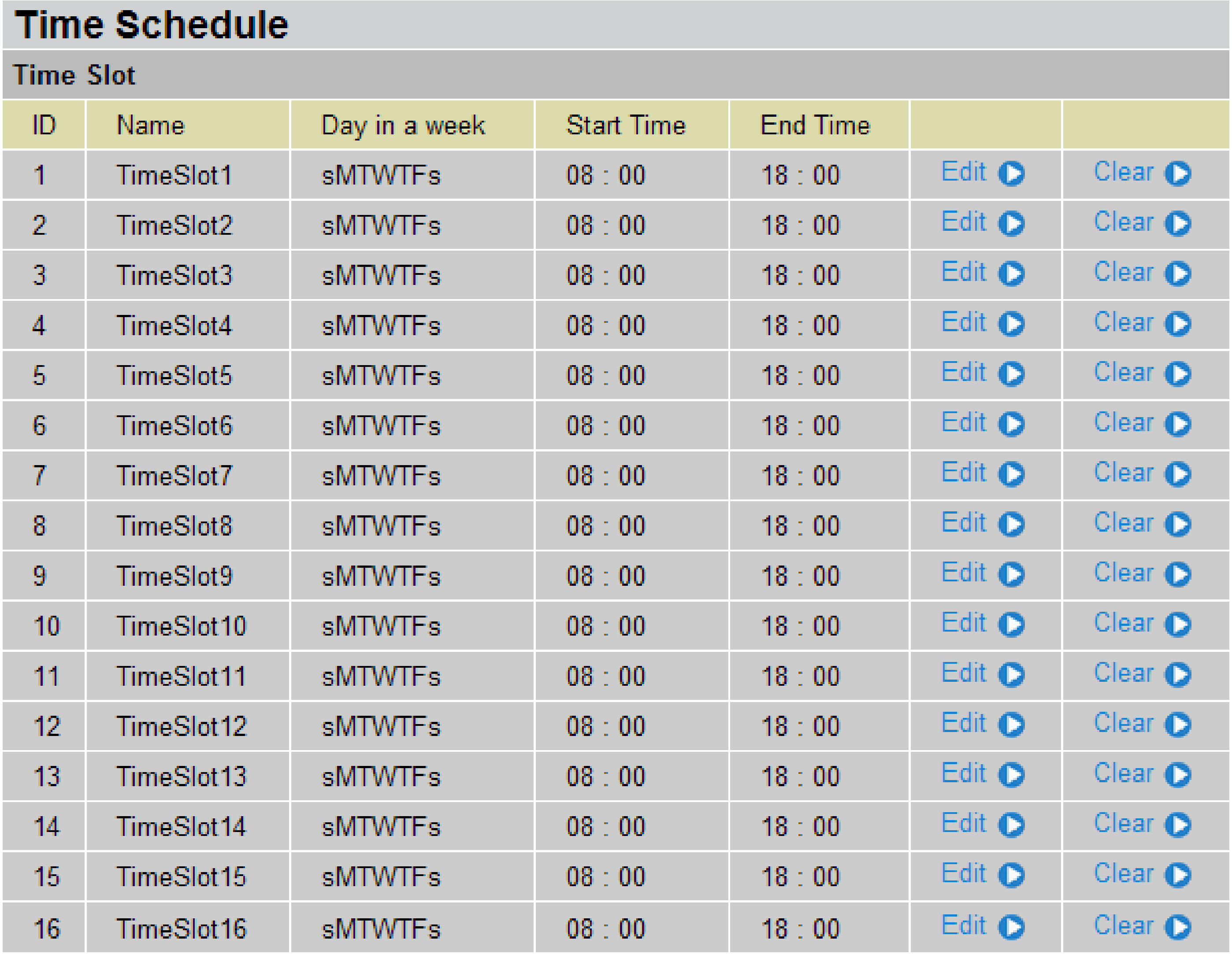
Table: Well-known and registered Ports

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	Real Audio

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

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

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

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

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

Click the Edit/Clear button to save your changes.

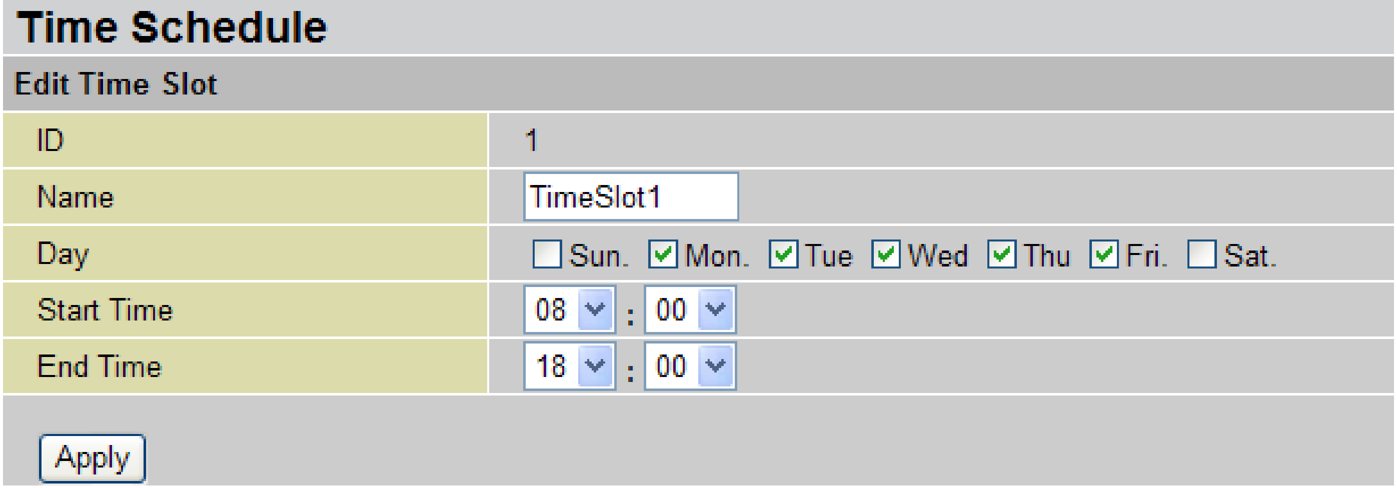
Configuration of Time Schedule

Edit a Time Slot

1. To edit a time schedule, click on the Edit link of the schedule slot you want to edit.

Note: The days you have selected will be shown with a capital letter.

2. On the Edit screen, delete the information to be edited and replace it with the new one.



Time Schedule

Edit Time Slot

ID	1
Name	TimeSlot1
Day	☐ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. ☐ Sat.
Start Time	08 : 00
End Time	18 : 00

ID: This is the index of the time slot.

Name: A user-define description to identify the time profile.

Day: Default is set from Monday through Friday. You may specify the days for the schedule to be applied.

Start Time: Default is set at 8:00 AM. You may specify the schedule starting time.

End Time: Default is set at 18:00 (6:00PM). You may specify the schedule ending time.

3. When it is done, simply click on the Apply button to save your changes.

Delete a Time Slot

Click Clear to delete the existing Time profile, i.e. erase the Day and reset it to the default setting for the Start Time / End Time.

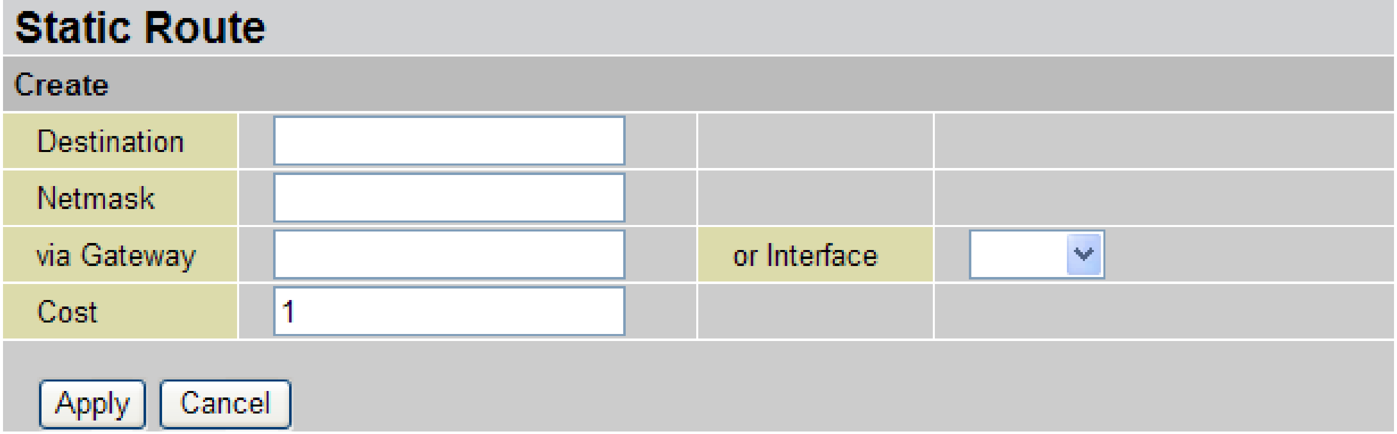
Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the Advanced section: **Static Route**, **Dynamic DNS**, **Check Email**, **Device Management**, **IGMP** and **Remote Access**.

Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed to.



Static Route

Create

Destination			
Netmask			
via Gateway		or Interface	
Cost	1		

Destination: Enter the destination IP where the traffic is to be forwarded.

Netmask: Enter the netmask of the destination.

via Gateway: Enter the gateway address for the traffic.

or Interface: Select an appropriate interface for the new routing rule from the drop down menu.

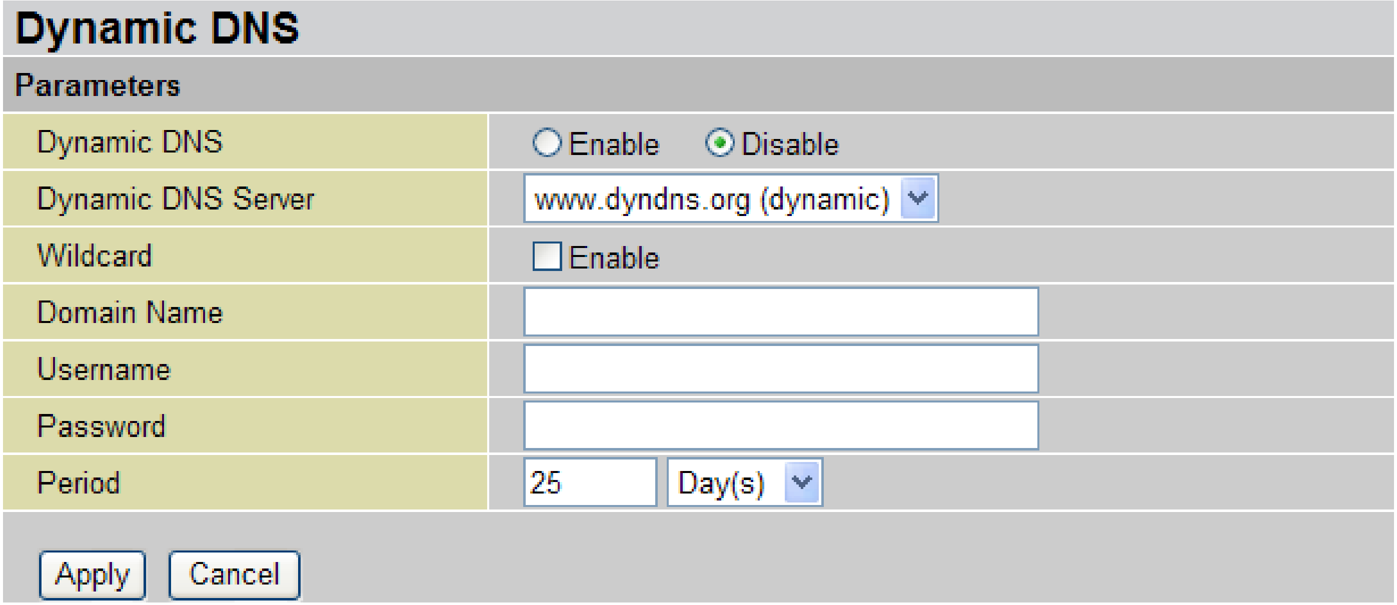
Cost: This is the same meaning as Hop and represents the cost of transmission for routing purposes. The number needs not be precise, but it must between 0 and 65535; usually be left at 1.

Click Apply to confirm the settings.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful when hosting servers via your GPON connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

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



Dynamic DNS

Parameters

Dynamic DNS	○ Enable ● Disable
Dynamic DNS Server	www.dyndns.org (dynamic)
Wildcard	☐ Enable
Domain Name	
Username	
Password	
Period	25 Day(s)

Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The following fields will be activated and required.

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

Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

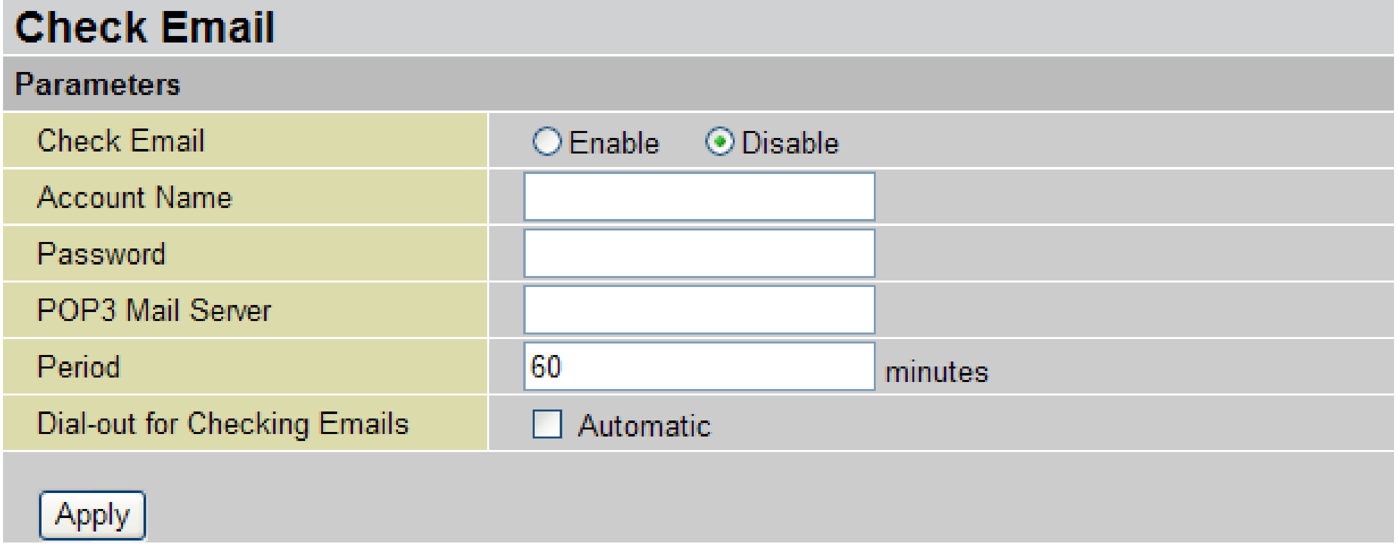
Domain Name, **Username** and **Password:** Enter your registered domain name and your username and password for this service.

Period: Enter the length of the period in the blank, you can set the period unit in day (d), hour (H) or minute (M). In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Click Apply to confirm the settings.

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 Status section of the web interface, which also provides details on the number of new messages await for download.



Check Email

Parameters

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

Check Email: Choose to Enable or Disable the router Email checking function. The following fields will be required when this function is enabled.

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

Password: Enter the account password.

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

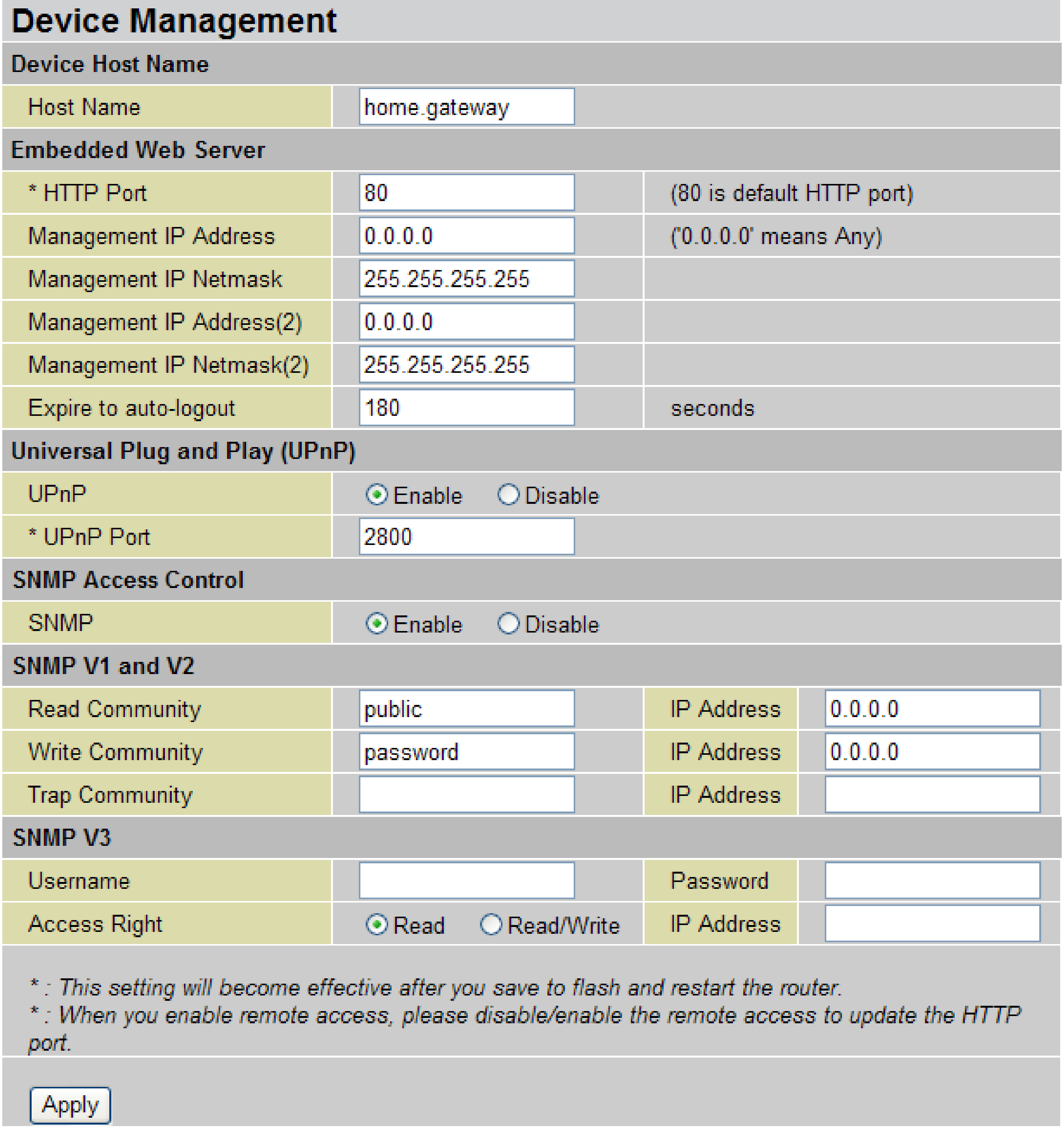
Period: Enter the value in minutes between each mail checking interval.

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

Click Apply to confirm the settings.

Device Management

The Device Management advanced configuration settings allows 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	● Enable ○ Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	● Read ○ Read/Write	IP Address	

** : This setting will become effective after you save to flash and restart the router.*
** : When you enable remote access, please disable/enable the remote access to update the HTTP port.*

Device Host Name

Host Name: Assign it a name.

(The Host Name cannot be used with one word only. There are two words should be connected with a ‘.’ at least.
Example:
Host Name: homegateway ==> Incorrect
Host Name: home.gateway or my.home.gateway ==> Correct)

Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You can specify an IP address used to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, and allowing users to login from any IP address.

Expire to auto-logout: Specify a time length for the system to auto-logout user from the configuration session.

Example: User A enters 100 for HTTP port number, specifies 192.168.1.55 for his/hser own IP address, and sets the logout time to 100 minutes. The router will allow User A to access only from the IP address 192.168.1.55 to logon to the Web GUI by typing: http://192.168.1.254:100 in their web browser. After 100 minutes, User A is logged out by the device automatically.

Universal Plug and Play (UPnP)

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

Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UpnP feature. Windows 2000 does not support UPnP.

- **Disable:** Check to inactive the router's UPnP functionality.
- **Enable:** Check to active the router's UPnP functionality.

UPnP Port: Default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports that have been used, you are allowed to change the port number.

SNMP Access Control

(Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol

Click to enable or disable this function.

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 who 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, user 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, user from this IP address will be sent to SNMP Traps.

SNMP V3

Specify a name and password for authentication. And define the access right from an identified IP address. Once the authentication has succeeded, user 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, authorizing with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

- From RFC 1213 (MIB-II):

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

- From RFC1650 (EtherLike-MIB):

  dot3Stats

- From RFC 1493 (Bridge MIB):

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

- From RFC 1471 (PPP/LCP MIB):

  pppLink group
  pppLqr group

- 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):

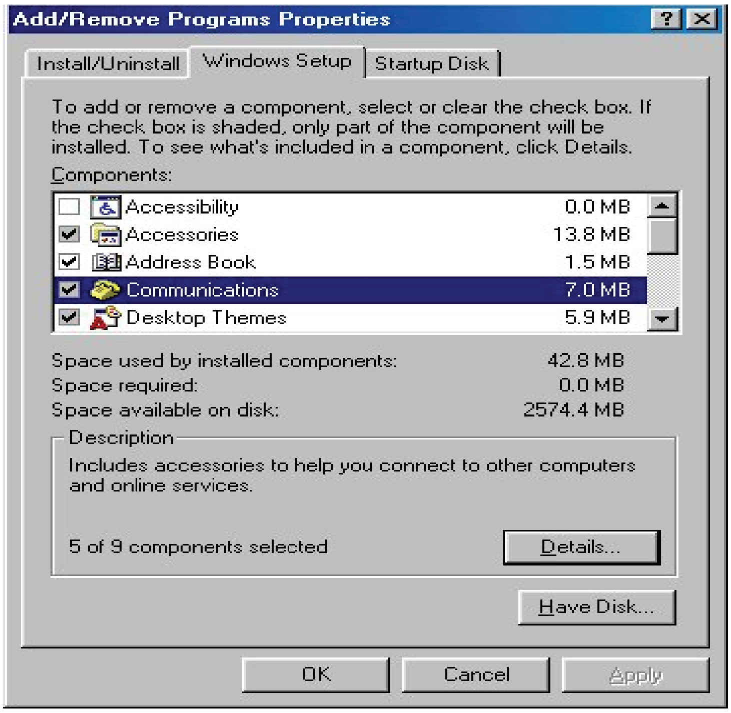
only snmpSetSerialNo OID

Installing UPnP in Windows Example

Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐	Accessibility	0.0 MB
☑	Accessories	13.8 MB
☑	Address Book	1.5 MB
☑	Communications	7.0 MB
☑	Desktop Themes	5.9 MB

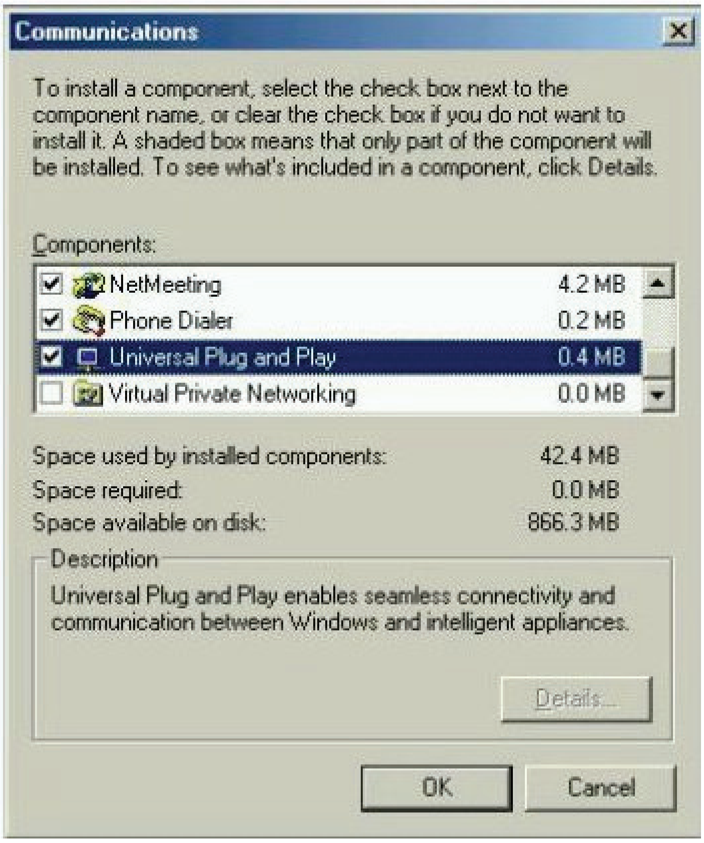
Space used by installed components: 42.8 MB
Space required: 0.0 MB
Space available on disk: 2574.4 MB

Description

Includes accessories to help you connect to other computers and online services.

5 of 9 components selected

Step 3: In the Communications window, select the Universal Plug and Play check box in the Components selection box.



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
☐	Virtual Private Networking	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

Step 4: Click OK to go back to the Add/Remove Programs Properties window. Click Next.

Step 5: Restart the computer when prompted.

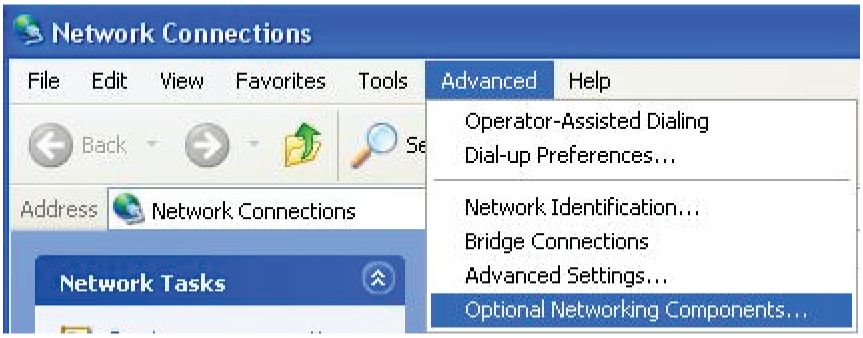
Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

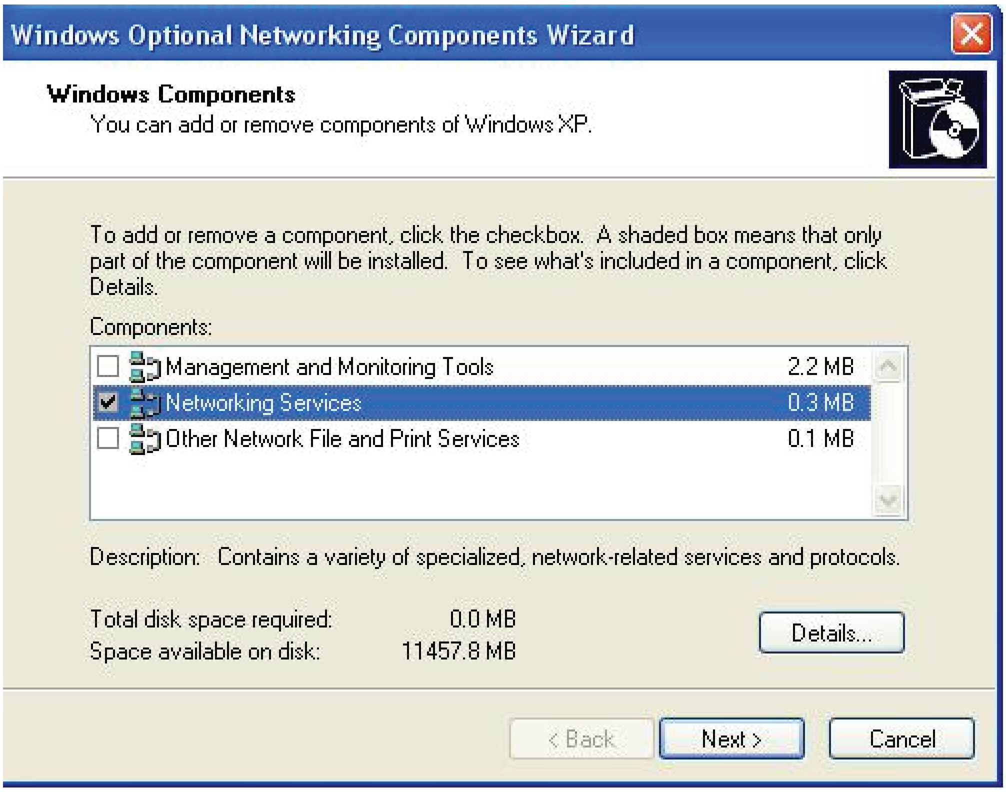
Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….

Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.



Windows Components
You can add or remove components of Windows XP.

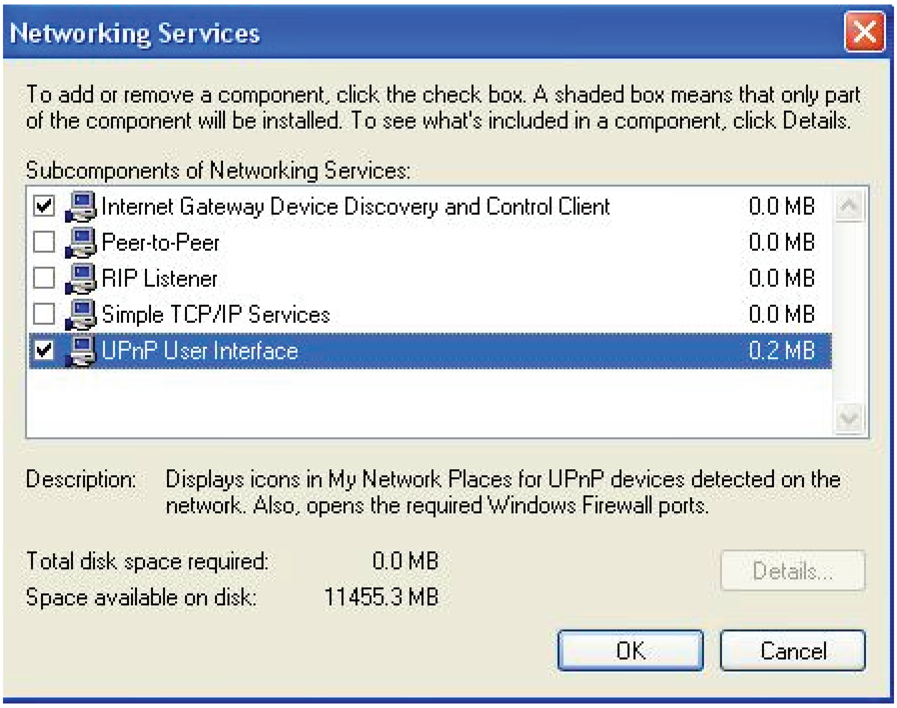
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☐ Management and Monitoring Tools 2.2 MB
☑ Networking Services 0.3 MB
☐ Other Network File and Print Services 0.1 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 11457.8 MB



To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☑	Internet Gateway Device Discovery and Control Client	0.0 MB
☐	Peer-to-Peer	0.0 MB
☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	UPnP User Interface	0.2 MB

Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.

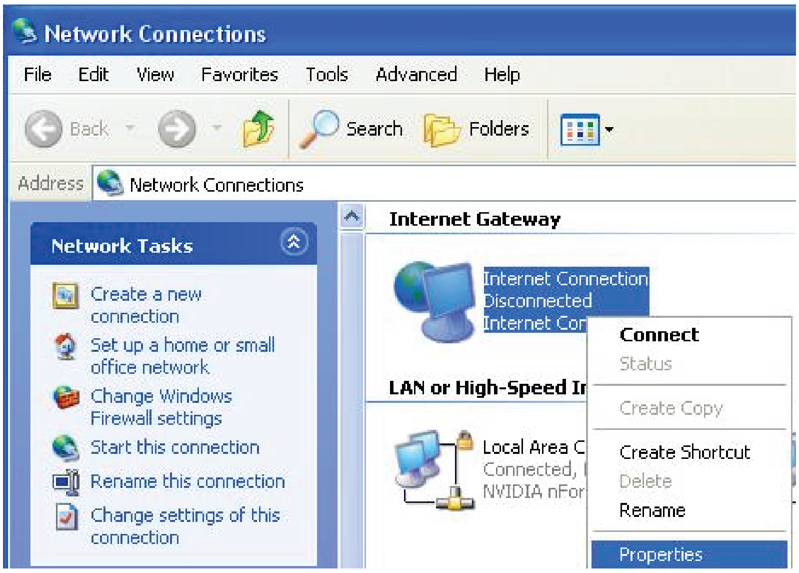
Total disk space required: 0.0 MB

Space available on disk: 11455.3 MB

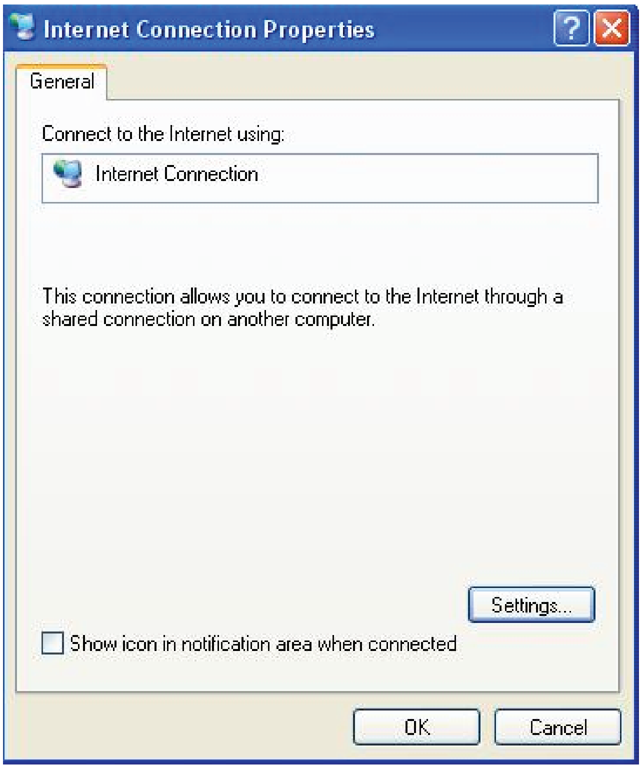
Auto-discover Your UPnP-enabled Network Device

Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2: Right-click the icon and select Properties.



Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



Internet Connection Properties

General

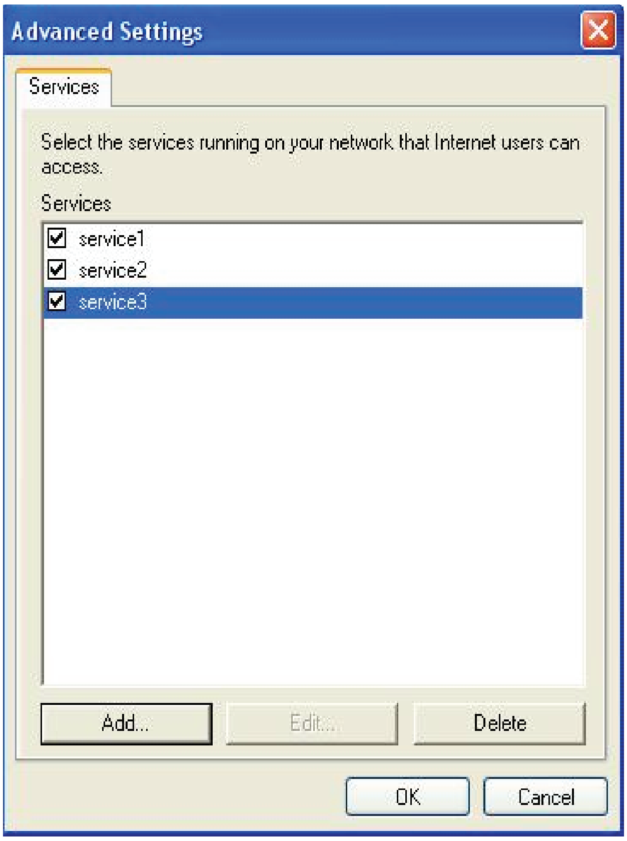
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☐ Show icon in notification area when connected

Step 4: You may edit or delete the port mappings or click Add to manually add port mappings.



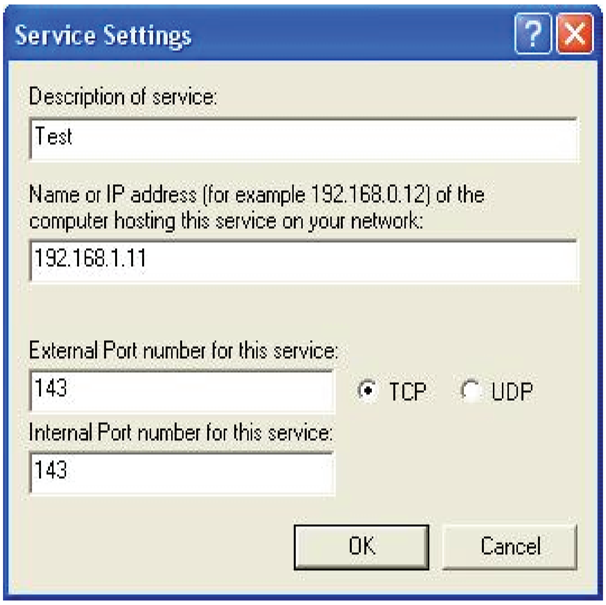
Advanced Settings

Services

Select the services running on your network that Internet users can access.

Services

☑ service1
☑ service2
☑ service3



Service Settings

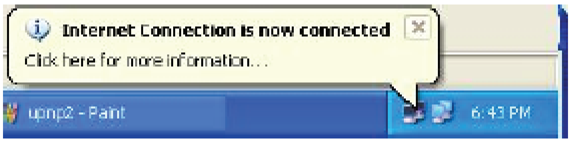
Description of service:
Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

External Port number for this service:
143
● TCP ○ UDP

Internal Port number for this service:
143

Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.

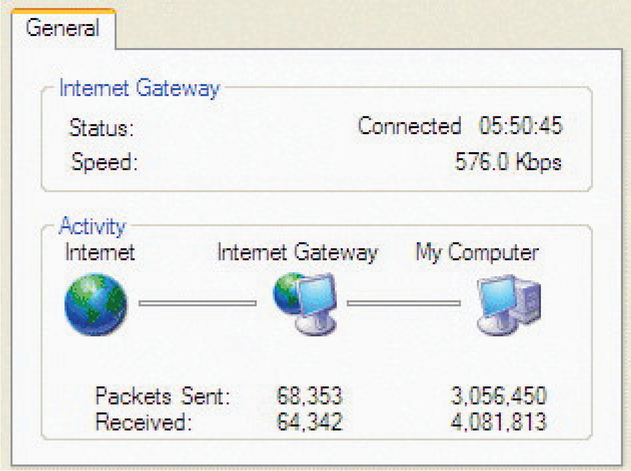


Internet Connection is now connected

Click here for more information...

Step 6: Double-click on the icon to display your current Internet connection status.

Step 6: Double-click on the icon to display your current Internet connection status.



Internet Gateway

Status: Connected 05:50:45

Speed: 576.0 Kbps

Activity

	Internet Gateway	My Computer
Packets Sent:	68,353	3,056,450
Received:	64,342	4,081,813

Web Configurator Easy Access

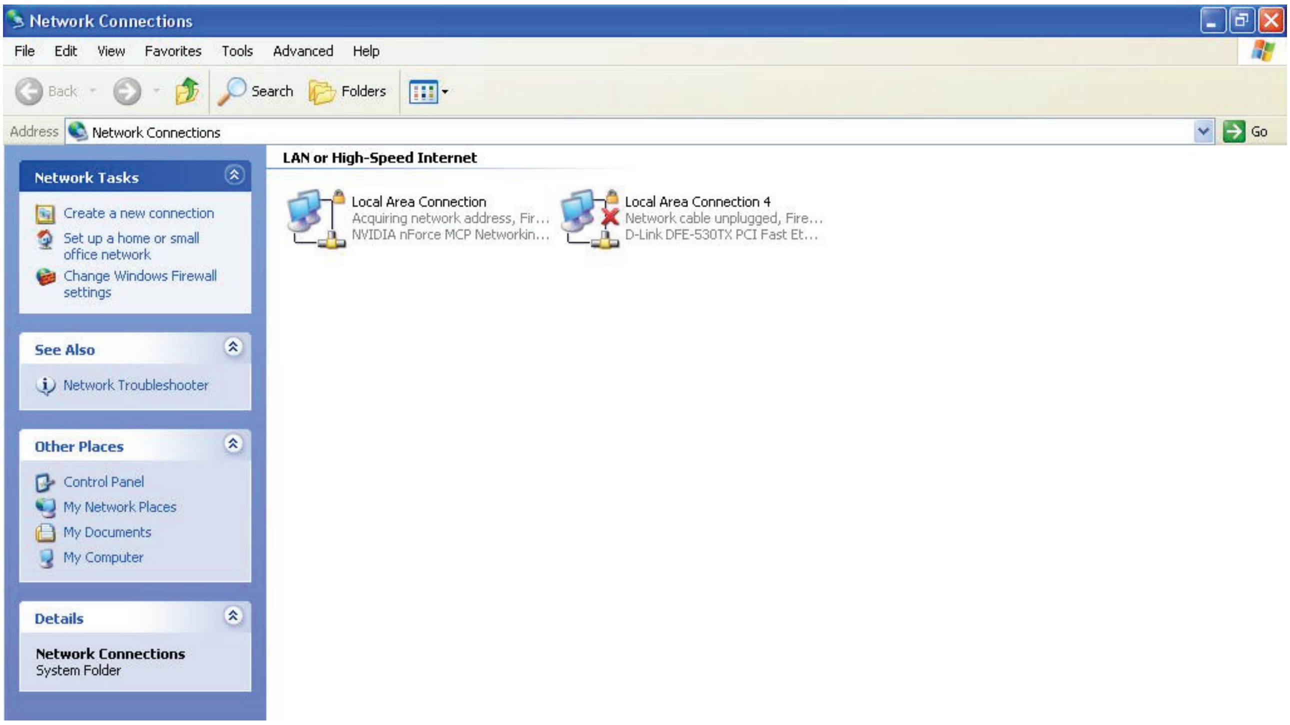
With UPnP, you can access web-based configuration for the BiPAC 9300(V)NX without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



Network Connections
System Folder

LAN or High-Speed Internet

Local Area Connection
Acquiring network address, Fir...
NVIDIA nForce MCP Networkin...

Local Area Connection 4
Network cable unplugged, Fire...
D-Link DFE-530TX PCI Fast Et...

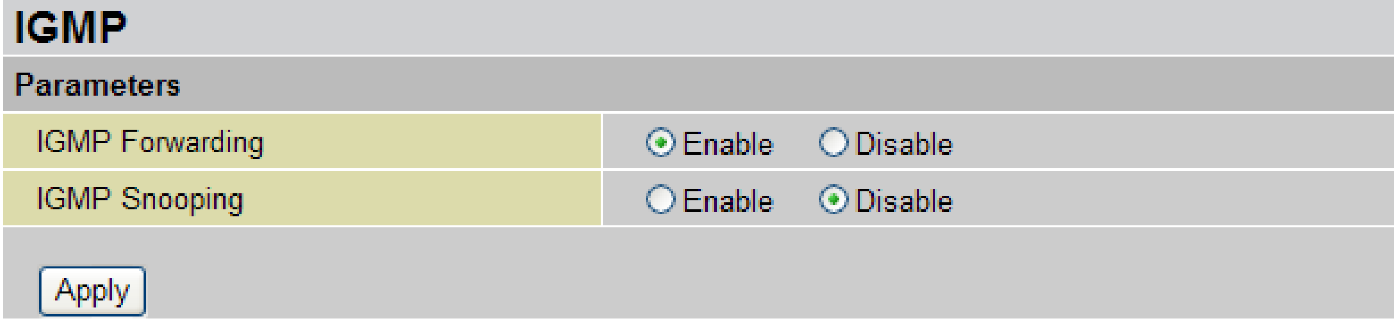
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 85xx and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 85xx and select Properties. A properties window displays basic information about the BiPAC85xx.

IGMP

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



IGMP

Parameters

IGMP Forwarding	● Enable ○ Disable
IGMP Snooping	○ Enable ● Disable

IGMP Forwarding: Accept multicast packet. Default is Enable.

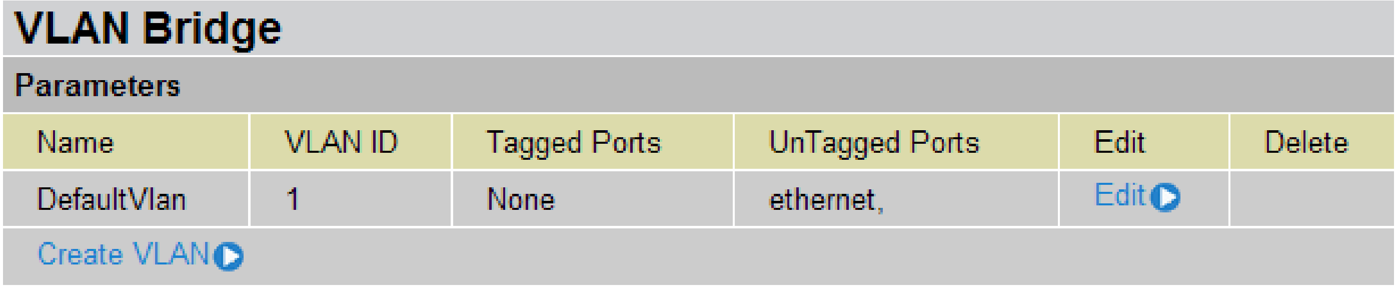
IGMP Snooping: Allows a layer 2 switch to manage the transmission of any incoming IGMP multicast packet groups between the host and the router. Default is set to Disable.

Click Apply to confirm the changes.

Example:
When IGMP snooping is enabled, the feature will analyze all incoming IGMP packets between the hosts that are connected to the switch and the multicast routers in the network. When the layer 2 switch receives an IGMP report from a host requesting for a given multicast group, the switch will add the host's port number to the multicast list for that multicast group to be forwarded to. And, when the layer 2 switch has detected that an IGMP has left, it will remove the host's port from the table entry.

VLAN Bridge

This section allows you to create a VLAN group and specify the members of the VLAN group..



VLAN Bridge

Parameters

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

Edit: Edit your member ports in selected VLAN group.

Create VLAN: Click to create another VLAN group.

Advanced VLAN Setup Example (Triply Play)

VLAN_data

Ethernet Port 1, Wireless and Wireless WDS are reserved 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

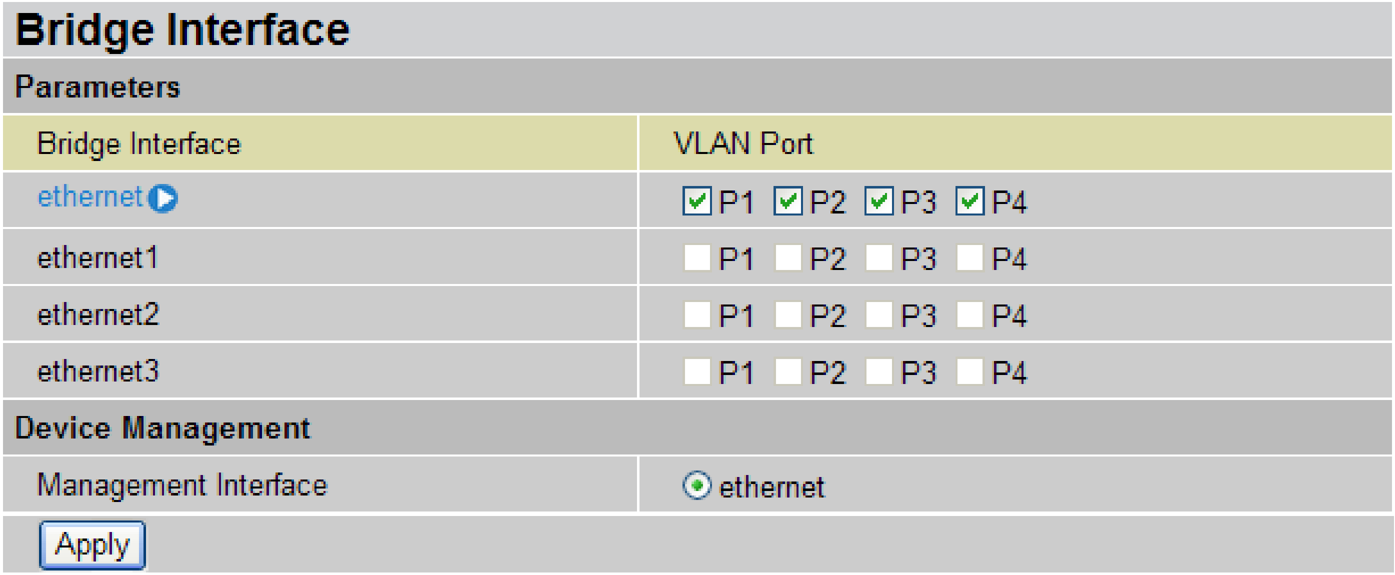
Go to Configuration > LAN > Bridge Interface.

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

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

Parameters

Bridge Interface	VLAN Port
ethernet	☑ P1 ☑ P2 ☑ P3 ☑ P4
ethernet1	☐ P1 ☐ P2 ☐ P3 ☐ P4
ethernet2	☐ P1 ☐ P2 ☐ P3 ☐ P4
ethernet3	☐ P1 ☐ P2 ☐ P3 ☐ P4

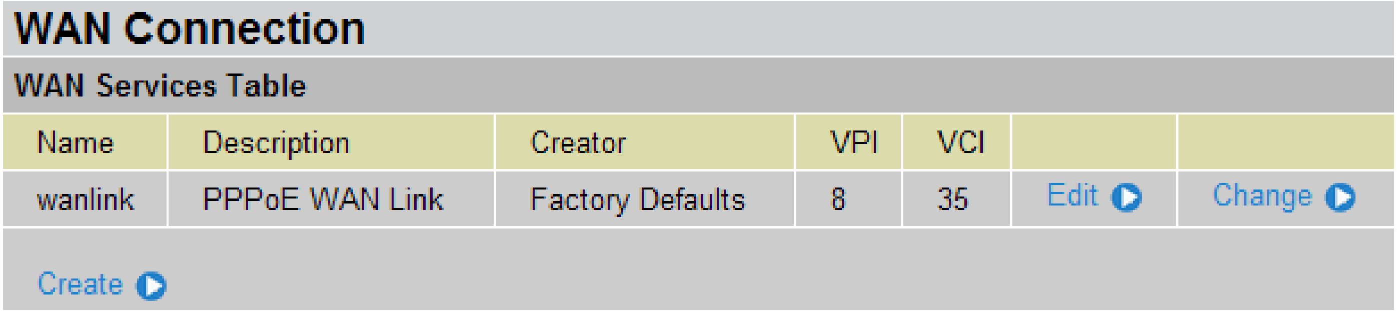
Device Management

Management Interface ● ethernet

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.

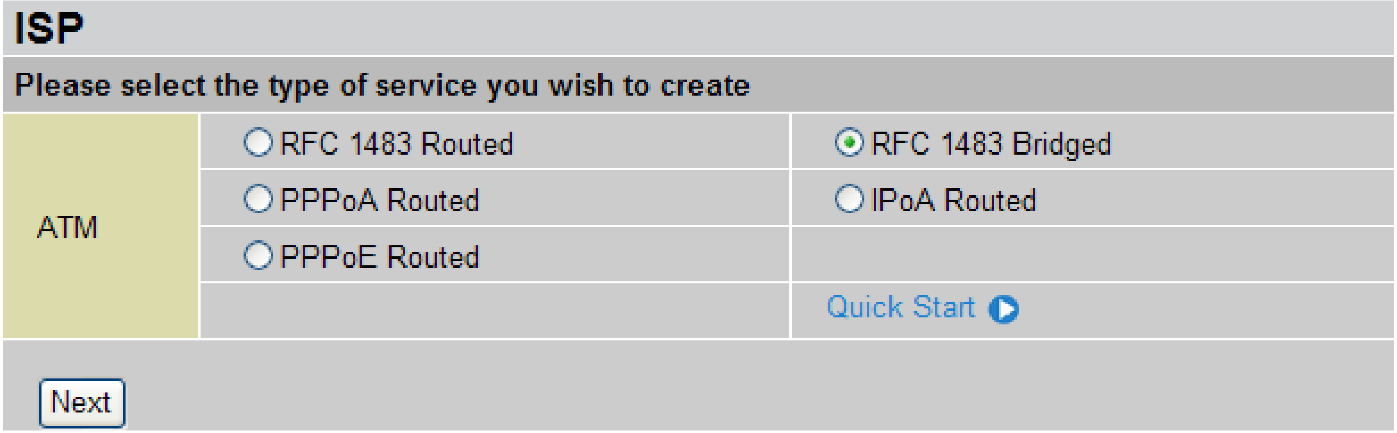


WAN Connection

WAN Services Table

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

wanlink is the factory default WAN interface which provides 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.

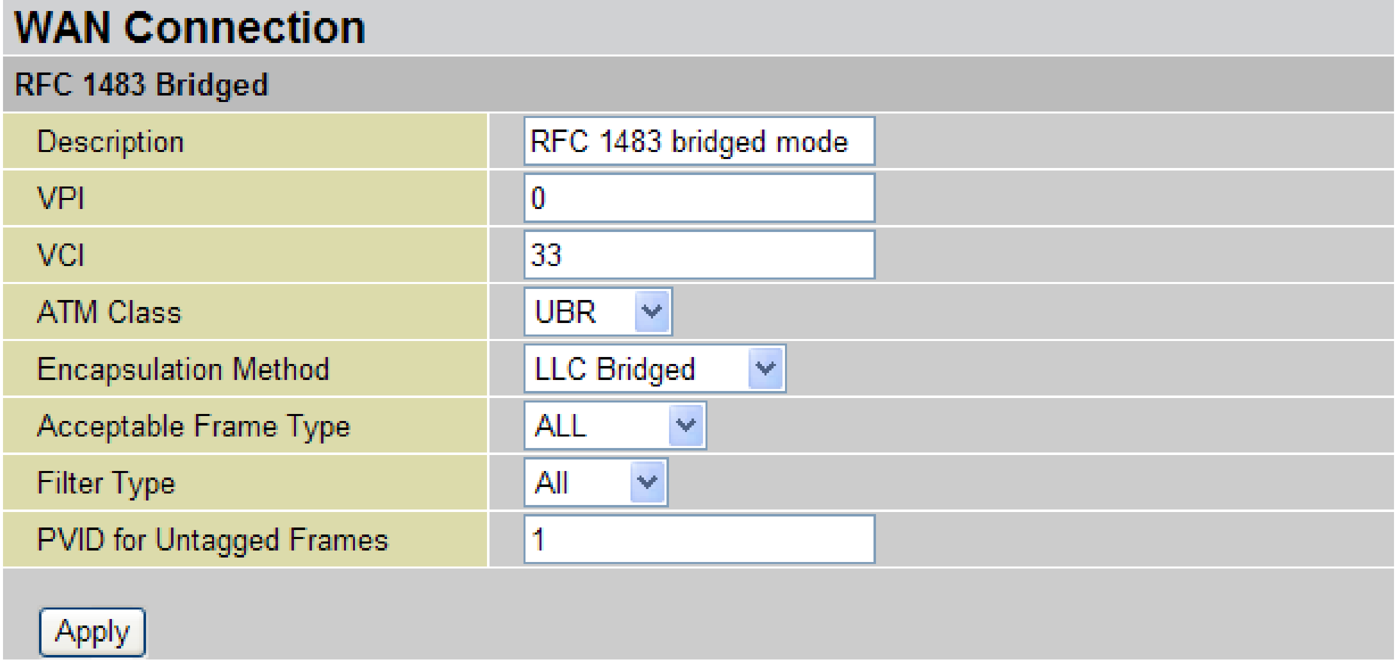


ISP

Please select the type of service you wish to create

ATM	○ RFC 1483 Routed	● RFC 1483 Bridged
	○ PPPoA Routed	○ IPoA Routed
	○ PPPoE Routed	
		Quick Start

From the example, 0/40 is used for data/internet and with the assumption that PPPoE is used; click the Edit button to change the VPI/VCI to 0/40.

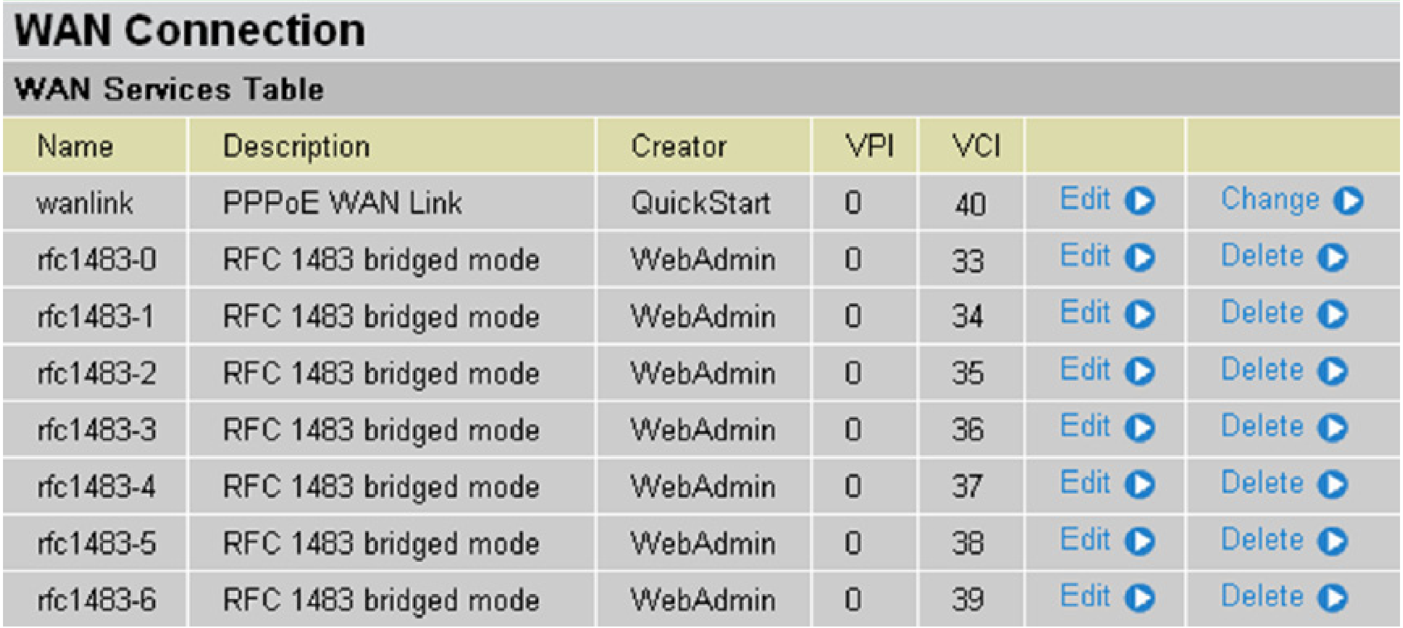


WAN Connection

RFC 1483 Bridged

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

Click Create to setup up an additional WAN interface for video applications. A total of 8 VLAN is supported; therefore, only 8 WAN interfaces can be created in the table.



WAN Connection

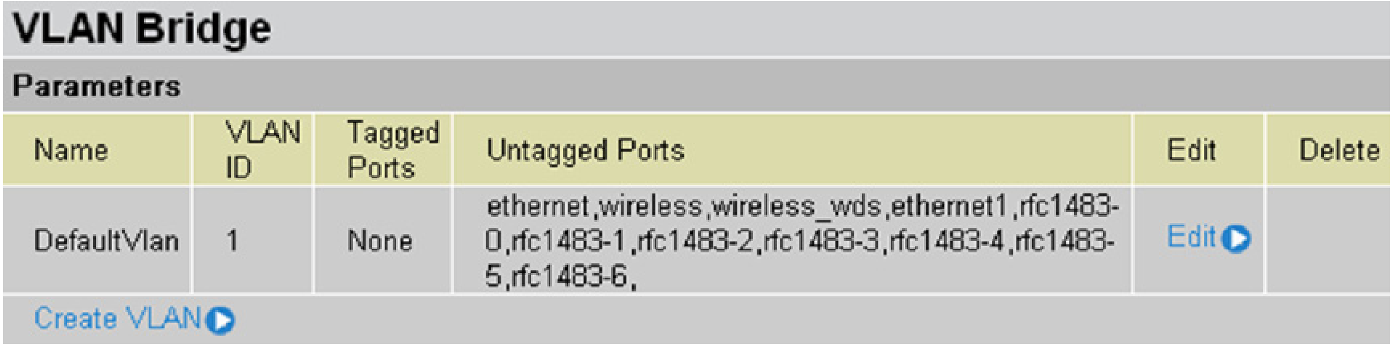
WAN Services Table

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

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

Enter 0 for VPI and 33 for VCI in their respective blanks provided. Select an appropriate ATM Class, Encapsulation Method, Acceptable Frame Type and Filter Type from their drop down menus and enter the correct PVID for Untagged Frames in the blank. When all information has been entered, press Apply to save changes.

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



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

Step 3: Setup Member Ports

Go to Configuration > Advanced > VLAN Bridge.

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

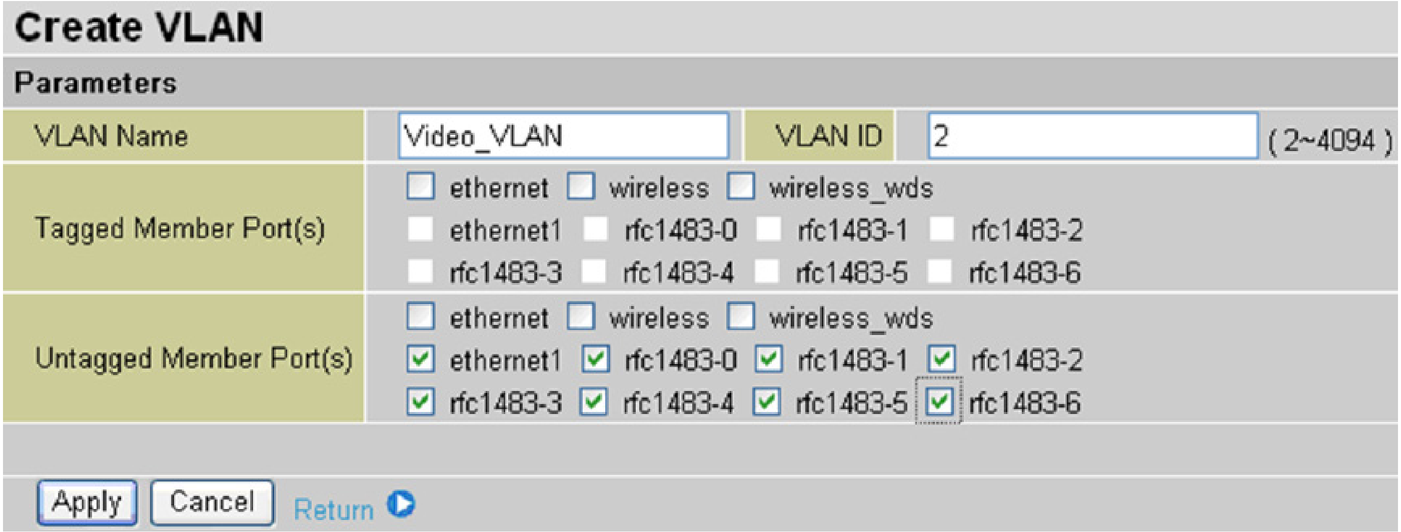
In the example, 2 VLAN groups are requested: Data and Video. To create another VLAN group for Video, click Create VLAN.

Give a name and ID (PVID) to identify the Video group. 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.

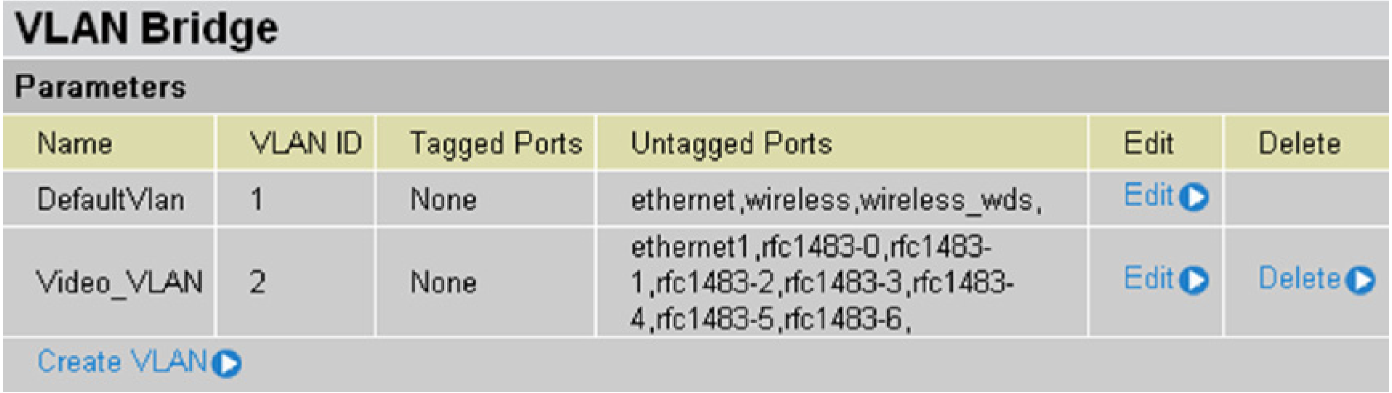
Click Apply to made changes effective immediately.



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 ☑ ethernet1 ☑ rfc1483-0 ☑ rfc1483-1 ☑ rfc1483-2 ☑ rfc1483-3 ☑ rfc1483-4 ☑ rfc1483-5 ☑ rfc1483-6		



VLAN Bridge

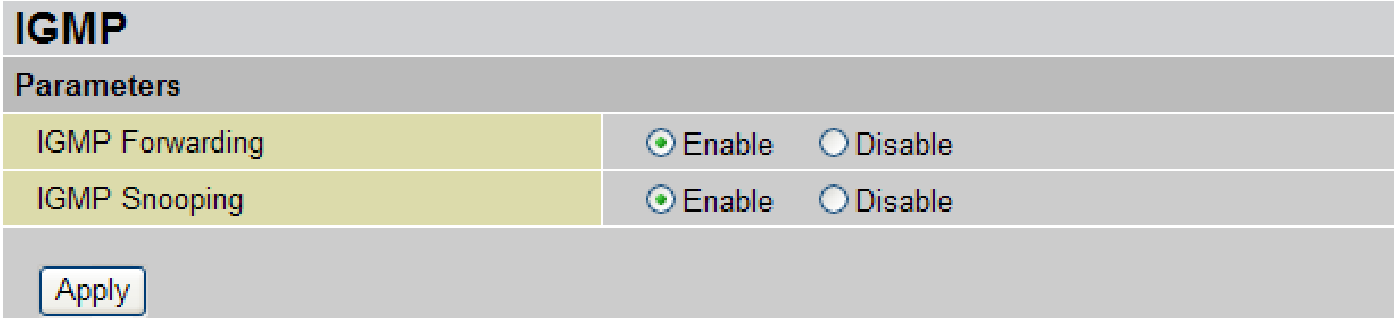
Parameters

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

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

Step 4: Enable IGMP Snooping

Go to Configuration > Advanced > IGMP.



IGMP

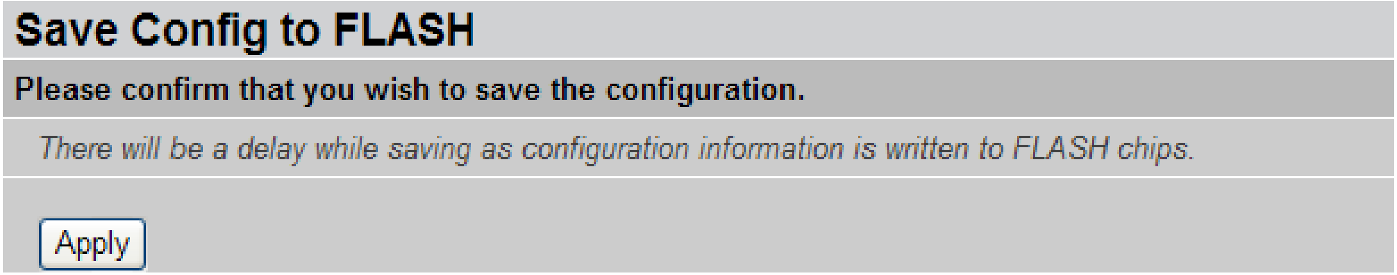
Parameters

IGMP Forwarding	● Enable ○ Disable
IGMP Snooping	● Enable ○ Disable

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

Save Configuration to Flash

After changing the router’s configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click “Save Config“ and click “Apply” to write your new configuration to FLASH.



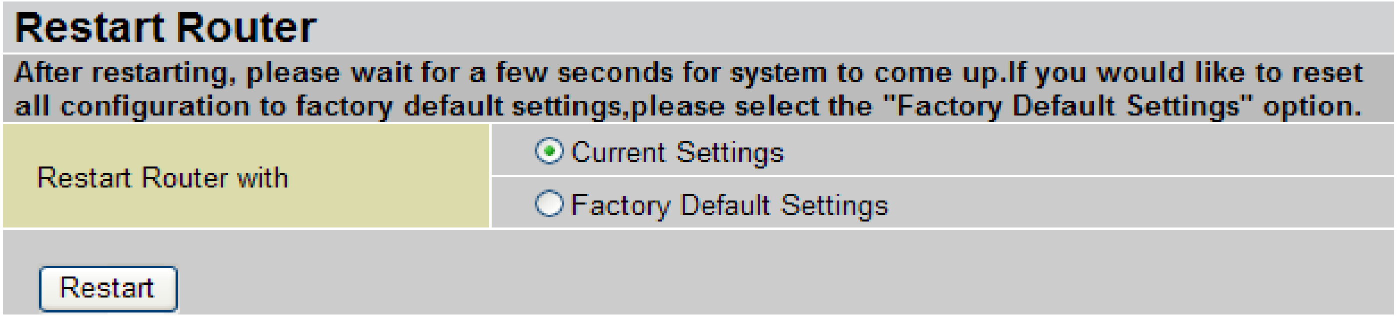
Save Config to FLASH

Please confirm that you wish to save the configuration.

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

Restart

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



Restart Router

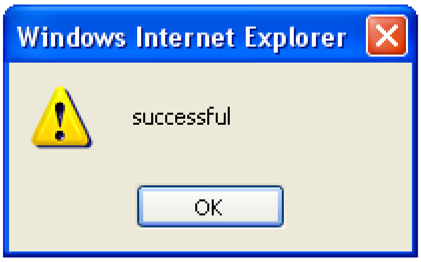
After restarting, please wait for a few seconds for system to come up.If you would like to reset all configuration to factory default settings,please select the "Factory Default Settings" option.

Restart Router with ● Current Settings ○ Factory Default Settings

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

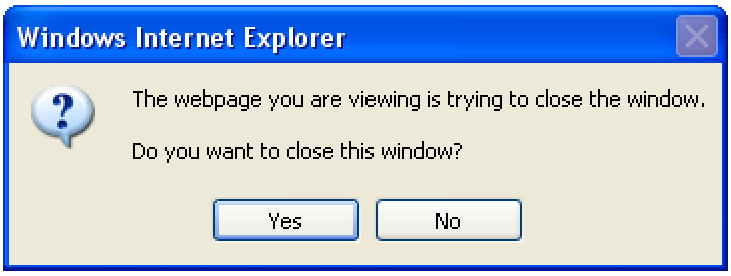
Logout

To exit the router web interface, click “Logout”. Please save your configuration setting before logging out of the system. A Warning screen will appear as below.



successful

Click OK and a message displays. Click Yes to close the window.



The webpage you are viewing is trying to close the window.

Do you want to close this window?

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the Reset button for more than 6 seconds.

Problems with WAN interface

Problem	Suggested Action
Initialization of SHDSL connection (linesync) fail	Make sure that telephone cable is properly connected between the SHDSL port and the wall jack. When the SHDSL LED on the front panel does not light, check your VPI, VCI, encapsulation type and the multiplexing settings type to see if thet are as same as those provided by your ISP and then reboot the router. If you still have problems, please verify these settings with your ISP.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not light, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
Verify that the IP address and the subnet mask are consistent between the router and the workstations.	

Appendix: Product Support & Contact

Following the suggestions listed in the Troubleshooting section of the user manual can help you to solve most of your problems. However, if your problems persist or you come across other technical issues that are not listed in the Troubleshooting section, please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.