BILLION™

BiPAC 7800VDP(O)X

Dual-band Wireless-N 3G/4G LTE VoIP (VPN) ADSL2+ Router

User Manual

Version Released: 2.32d

Last revised date: February 18, 2014

Table of Contents

Chapter 1: Introduction

Introduction to your Router

The BiPAC 7800VDP(O)X is a dual-band wireless network device, it utilizes two wireless bands for wireless communications, and offers maximum performance in setting up a network. Users can choose the most economical rate of VoIP calls provided by different Internet Technology Service Provider (ITSP). The device integrates two FXS ports which allows for simultaneous VoIP calls. The extra FXO port enables you to make & receive calls via PSTN Fixed-line while sharing a high-speed internet connection. Its built-in 4-port Gigabit Ethernet Switch, supporting high-speed data transfer including a Gigabit WAN port for Broadband connectivity. The Quality of Service (QoS) feature ensures a smooth net connection for inbound and outbound data transmission with minimal traffic congestion. With the BiPAC 7800VDP(O)X, you can create your own mobile hotspot for Wi-Fi access.

Dual-band

A Dual-band Router utilizes two different wireless bands that support connections on both 2.4GHz and 5GHz simultaneously. The BiPAC 7800VDP(O)X is a dual-band router which transmits on two frequency bands-2.4GHz and 5GHz simultaneously. The two wireless bands are fully independent. One band can be used for downloading while the other is used for uploading; or one is used for online gaming, video streaming and music downloading while the other takes care of accessing email, file sharing and regular internet surfing. With an integrated 802.11 wireless access point, the router can deliver up to 6 times the speed of an 802.11b/g wireless device. It supports a date rate of up to 300 Mbps with each band and is also compatible with 802.11b/g devices in 2.4GHz and 802.11a in 5GHz.

Cost saving

Making VoIP calls is extremely simple; just connect the router to your existing telephones. The BiPAC 7800VDP(O)X complies with the most popularly adopted VoIP standard, SIP protocol, to ensure interoperability with SIP devices and major VoIP Gateways. One RJ-11 FXO port is integrated to transmit inbound and outbound calls through PSTN Fixed-line, so that users may still be able to receive phone calls through PSTN, while enjoying VoIP service at the same time. In addition, outgoing calls will be automatically redirected to PSTN when the Internet or VoIP service is not available. The router also supports a wider range of telephony features, such as call waiting, silence suppression, line echo cancellation, caller ID, etc.

IPv6 supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2^{128} (about 3.4×10^{38}) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements new features that simplify aspects of address assignment (stateless address autoconfiguration) and network renumbering (prefix and router announcements) when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from Link Layer media addressing information (MAC address).

Network security is integrated into the design of the IPv6 architecture. Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread optional deployment first in IPv4 (into which it was back-engineered). The IPv6 specifications mandate IPsec implementation as a fundamental interoperability requirement.

Jumbo frames supported

Jumbo frames are Ethernet frames with more than 1500 bytes (standard Ethernet frame) of payload. Conventionally, jumbo frames can carry up to 9720 bytes of payload to enjoy a high-efficiency communication in Gigabit Ethernet. Jumbo frames increase the frame size so that a certain large amount of date can be transported with less effort, reducing CPU utilization and increasing throughput by reducing the number of frames needing to be processed and reducing the total overhead byte count of all frames sent.

3G/LTE

With 3G/LTE-based Internet connection (requires an additional 3G/LTE USB modem), user can access internet through 3G/LTE, whether you are seated at your desk or taking a cross-country trip.

Virtual AP

A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Web Based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with online 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.

Features

- IPv6 ready (IPv4/IPv6 dual stack)
- Flexible WAN approach – ADSL2+, 3G/LTE mobile connection, and Ethernet WAN for Broadband Connectivity
- Dual-band (2.4GHz / 5GHz) wireless access point (300 + 300) Mbps
- Auto fail-over
- High-speed Internet Access via ADSL2 / 2+; Backward Compatible with ADSL
- Jumbo frames
- IEEE 802.11 a/b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS), Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization and Bandwidth management
- Secured IPSec VPN with powerful DES/ 3DES/ AES (BiPAC7800VDOX only)
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication (BiPAC7800VDOX only)
- Pure L2TP and L2TP over IPSec (BiPAC7800VDOX only)
- GRE tunnel (BiPAC7800VDOX only)
- Universal Plug and Play (UPnP) Compliance
- Supports IPTV Application[*2]
- Supports Storage Service
- Ease of Use with Quick Installation Wizard (EZSO)
- Make phone calls via Internet as well as PSTN Fixed-line
- Gain control to reduce bad PSTN quality issue
- Voice over IP compliant with SIP standard
- Two FXS ports for connecting to regular telephones
- One FXO port for voice calls via PSTN Fixed-line
- Answering machine and voice mail for flexible phone answering and message recording
- Fax over IP network
- Call Waiting, 3-Way Conference, and “Don’t Disturb (DND)”
- Call Forward, Call Through and Call Block
- Phone Book for speed dial

ADSL Compliance

- Compliant with ADSL Standard
  - Full-rate ANSI T1.413 Issue 2
  - G.dmt (ITU G.992.1)
  - G.lite (ITU G.992.2)
  - G.hs (ITU G.994.1)
- Compliant with ADSL2 Standard
  - G.dmt.bis (ITU G.992.3)
  - ADSL2 Annex M (ITU G.992.3 Annex M)
- Compliant with ADSL2+ Standard
  - G.dmt.bis plus (ITU G.992.5)
  - ADSL2+ Annex M (ITU G.992.5 Annex M)

Network Protocols and Features

- IPv4 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- IPv6 Stateless / Stateful Address Auto-configuration
- IPv6 Router Advertisement
- IPv6 over PPP
- DHCPv6
- IP Tunnel IPv6 in IPv4(6RD)
- IP Tunnel IPv4 in IPv6(DS-Lite)
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ and one-to-one NAT
- SNTP, DNS relay, IGMP snooping and IGMP proxy for video service
- MLD snooping and MLD proxy for video service
- Management based-on IP protocol, port number and address

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- Packet Filtering (v4/v6) - port, source IP address, destination IP address, MAC address
- URL Content Filtering (v4/v6) – string or domain name detection in URL string
- MAC Filtering

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IPv4/IPv6 protocol, port number and address

VOIP

- Two RJ-11 FXS ports for connecting to regular phones
- One RJ-11 FXO port for PSTN Fixed-line
- Compliant with SIP standard (RFC 3261)
- Supports G.711 A/μ law, G.711Mu-Law, G.726_32, G.722and G.729 Audio Codec standards
- Supports Telephony Features – calling waiting, silence suppression, voice activity detection (VOD), comfort noise generation (CNG). G.168 line echo cancellation, caller ID (bell 202, V23), three-way conference
- Dialing rules for individual use of Internet and fixed line telephony
- Answering machine and voice mail for flexible phone answering and message recording
- Fax over IP network
- Don’t Disturb (DND)
- Call Forward, Call Through, Call Block
- Phone Book for speed dial

ATM, PTM and PPP Protocols

- ATM Adaptation Layer Type 5 (AAL5)
- Multiple Protocol over ALL5 (RFC 268, formerly RFC 1483)
- Bridged or routed Ethernet encapsulation
- VC and LLC based multiplexing
- PPP over Ethernet (PPPoE)
- PPP over ATM (RFC 2364)
- Classical IP over ATM (RFC 1577)
- MAC Encapsulated Routing (RFC 1483 MER)
- OAM F4 / F5

IPTV Applications*2

- IGMP Snooping and IGMP Proxy
- MLD Snooping and MLD Proxy
- Virtual LAN (VLAN)
- Quality of Service (QoS)

Wireless LAN

- Compliant with IEEE 802.11 a/ b/ g/ n standards
- 2.4 GHz and 5GHz radio band for wireless
- Up to (300 + 300) Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Supports WPS v2
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support

USB Application Server

- 3G/LTE dongle support
- Storage: FTP server, Samba server，DLNA
- Printer Server

Virtual Private Network (VPN) (7800VDOX only)

- IKE key management
- DES, 3DES and AES encryption for IPSec
- L2TP over IPSec
- Pap/ Chap/ MS-CHAPv2 authentication for PPTP
- IPSec pass-through
- GRE tunnel

Management

- Easy Sign-on (EZSO)
- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Supports DHCP server / client / relay
- Supports SNMP v1,v2, MIB-I and MIB-II
- TR-069[*1] supports remote management
- Available Syslog
- Mail alert for WAN IP changed
- Auto failover and fallback
- Push Service

NOTE:

1. On request for Telco / ISP projects
2. IPTV application may require subscription to IPTV services from a Telco / ISP.
3. Specifications on this datasheet are subject to change without prior notice.

Hardware Specifications

Physical Interface

- WLAN: 2 x 2dbi fixed antennas
- DSL: ADSL port
- Telephone:

  1-port FXO (For PSTN Fixed-line)

  2-port FXS (For connecting to phones)
- USB 2.0 port for storage service and printer server
- Ethernet: 4-port 10 / 100 / 1000Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: Ethernet port #4 can be configured as a WAN interface for Broadband connectivity.
- Factory default reset button
- WPS push button
- Power jack
- Power switch

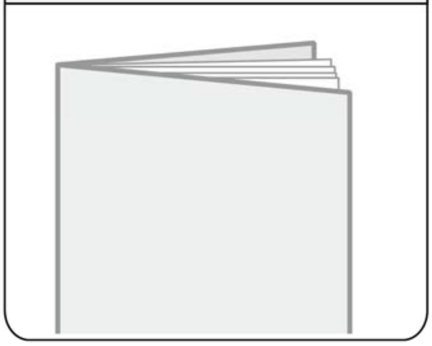
Chapter 2: Installing the Router

Package Contents

- **BiPAC 7800VDP(O)X Dual-band Wireless-N VoIP ADSL2+ (VPN) Router**
- **Quick Start Guide**
- **CD containing the on-line manual**
- **Two fixed dual-band antennas**
- **RJ-45 Cat. 5e STP Ethernet cable**
- **RJ-11 ADSL/ telephone cable**
- **Power adapter**
- **Splitter / Micro-filter (Optional)**

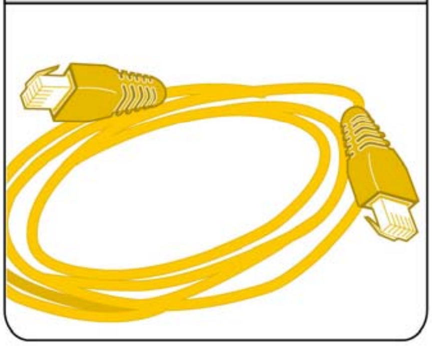
ADSL2+ Router

Quick Start Guide

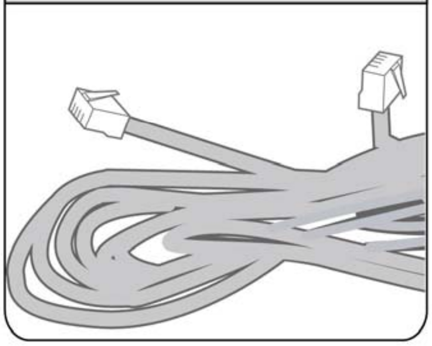


CD

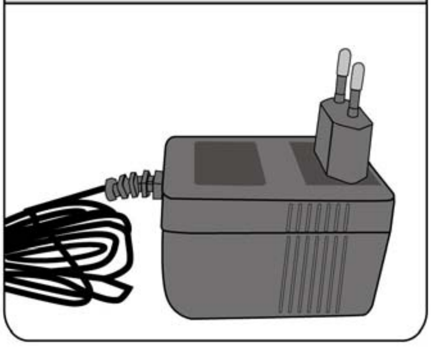
RJ-45 Cat. 5e STP Ethernet cable



RJ-11 Phone cable



Power Adapter (The type may differ by different country)



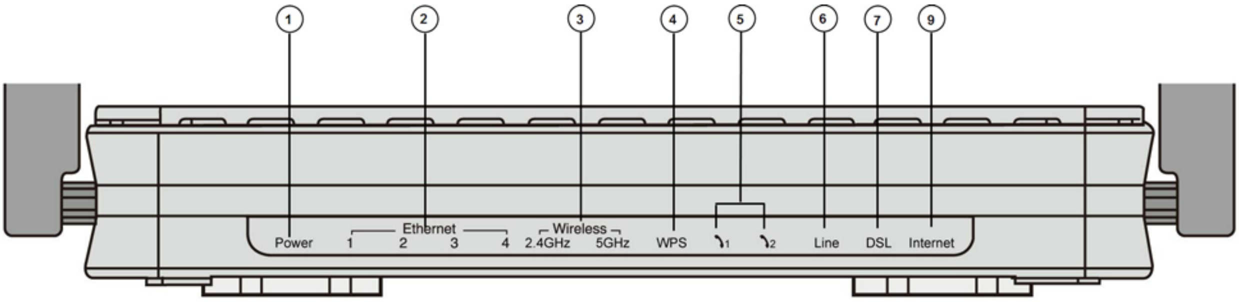
Important note for using this router

Warning	1. Do not use the router in high humidity or high temperatures. 2. Do not use the same power source for the router as other equipment. 3. 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. 4. Avoid using this product and all accessories outdoors.

Attention	1. Place the router on a stable surface. 2. Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

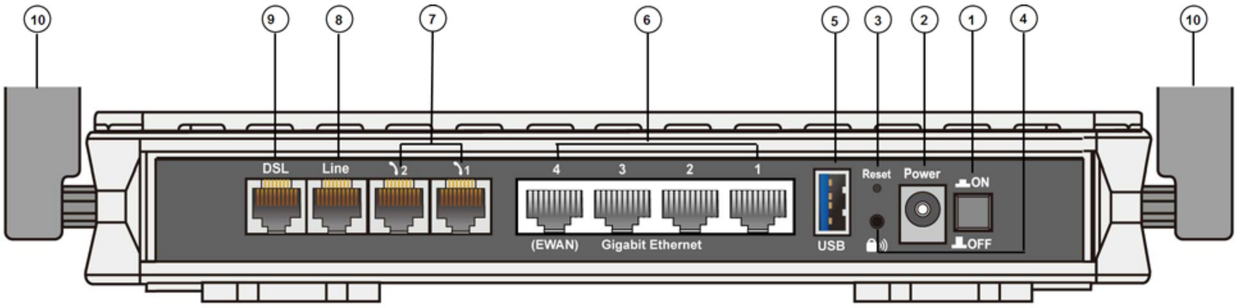
Device Description

The Front LEDs



LED		Status	Meaning
1	**Power**	Red	Boot failure or in emergency mode
		Green	System ready
2	**Ethernet Port 1-4 (EWAN)**	Green	Transmission speed hitting 1000Mbps
		Orange	Transmission speed hitting 10/100Mbps
		Blinking	Data being transmitted/received
3	**Wireless**	Green	Wireless connection established
		Green blinking	Sending/receiving data
4	**WPS**	Green blinking	WPS configuration being in progress
		Off	WPS process completed or WPS is off
5	**Phone (1X-2X) (RJ-11 connector)**	Green	Phone off-hook
6	**Line**	Green	Inbound or outbound calls are being transmitted through PSTN
7	**DSL**	Green Blinking	DSL synchronizing or waiting for DSL synchronizing
		Green	Successfully connected to an ADSL DSLAM (Line Sync).
		Off	DSL cable unplugged
8	**Internet**	Red	Obtaining IP failure
		Green	Having obtained an IP address successfully
		Off	Router in bridge mode or DSL connection not present.

The Rear Ports



Port		Meaning
1	Power Switch	Power ON / OFF switch.
2	Power	Connect the supplied power adapter to this jack.
3	RESET	After the device is powered on, press it **5 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password)
4	WPS	1 WPS button: Push WPS button to trigger Wi-Fi Protected Setup function. 2. Wireless on/off: When WPS is disabled, WPS button can act as wireless on/off button and is applied to both WLAN 2.4G and WLAN 5G. Press WPS button more than 2 seconds to switch on/off the whole wireless connectivity, including wireless 2.4G and wireless 5G. Pease Note that the action is based the status of wireless 2.4G, if now the wireless 2.4G is on, then you press the WPS button more than 2 seconds to switch off both wireless mode.
5	USB	Connect the USB device (Printer, USB 2.0 storage, 3G/LTE 3G USB modem) to this port.
6	Ethernet	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 /100Mbps /1000Mbps. **Note:** Port #4 can be configured as a WAN Interface for Broadband connectivity.
7	Phone (1X-2X)	Connect your analog phone set to this port with the RJ-11 cable.
8	Line (PSTN)	Connect this port with an RJ-11 cable to the telephone jack on the wall.
9	DSL	Connect this port to the DSL network with the RJ-11 cable (telephone) provided.
10	Antenna	The fixed dual-band antennas.

Cabling

One of the most common causes of problems is bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front panel of your router is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are all lit. If they are not, verify if you are using the proper cables. If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Make sure you have a line filter with all devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Chapter 3: Basic Installation

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

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

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

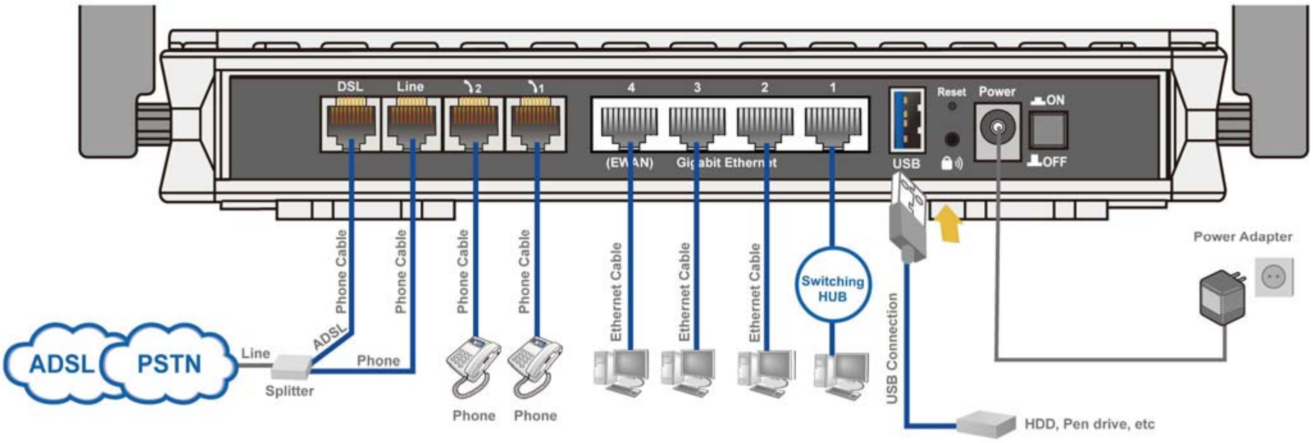
Please follow the following steps to configure your PC network environment.

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

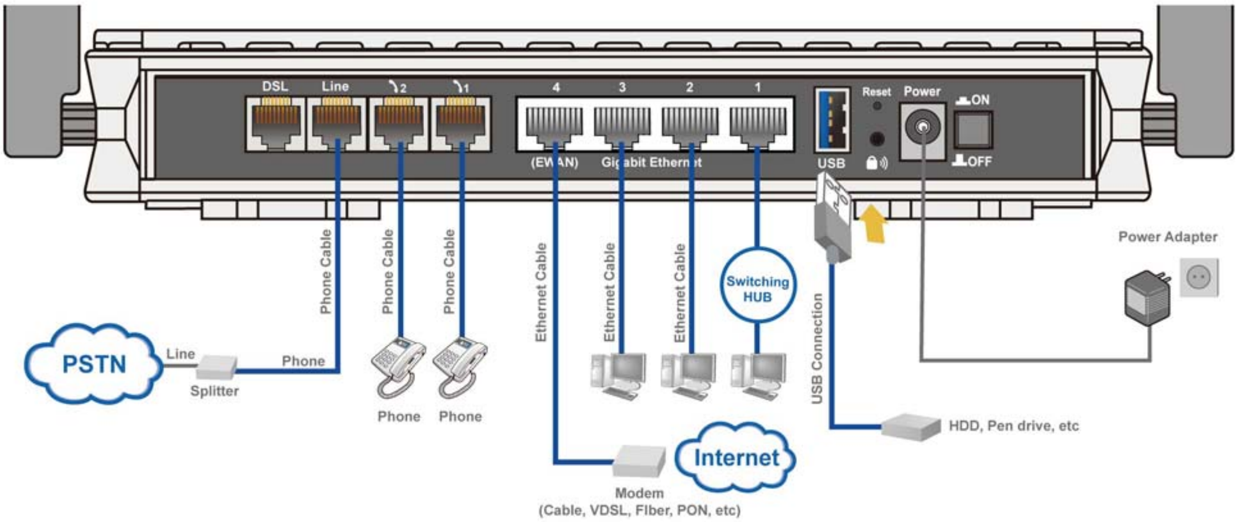
Connecting Your Router

Users can connect the ADSL2+ router as the following.

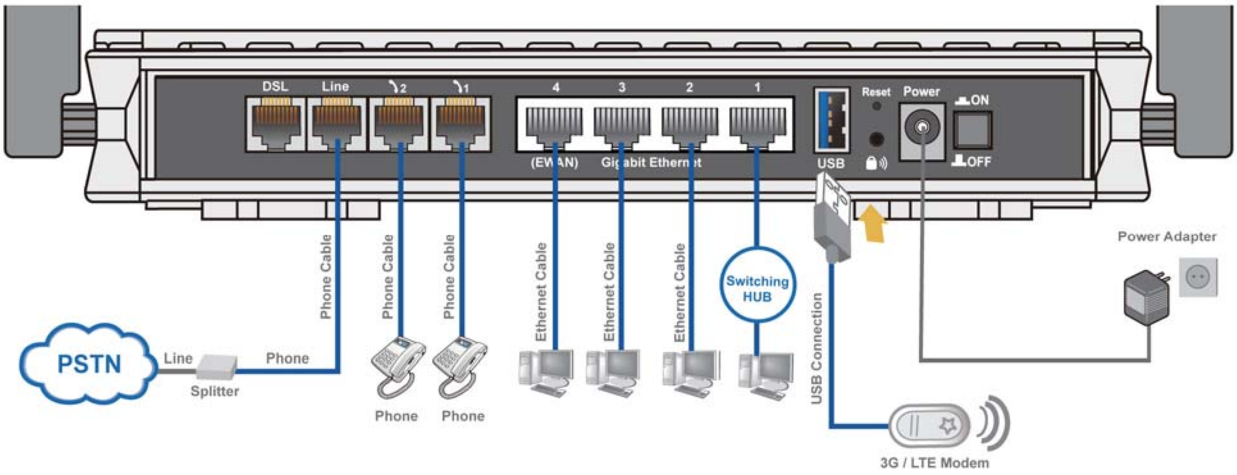
ADSL Router mode:



Broadband Router mode:



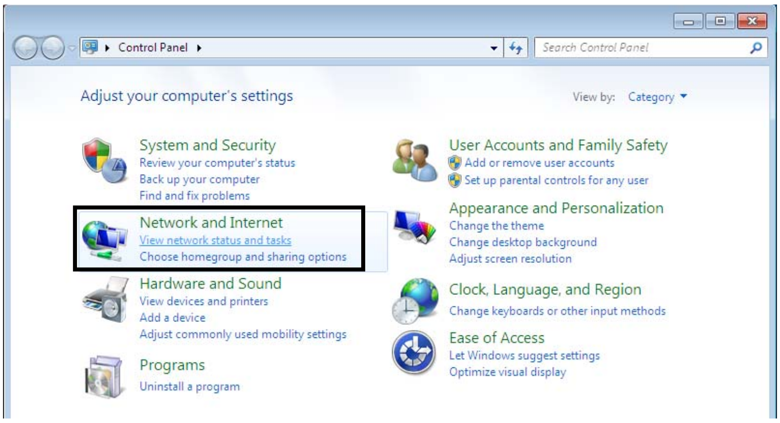
3G/LTE Router mode



Network Configuration

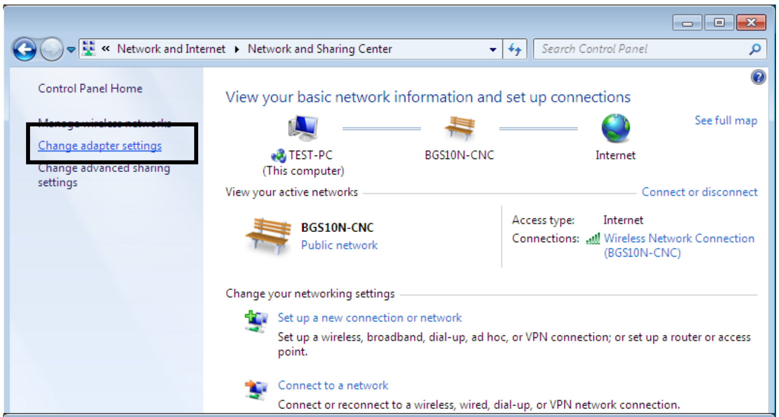
Configuring a PC in Windows 7

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



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
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display
Programs
Uninstall a program

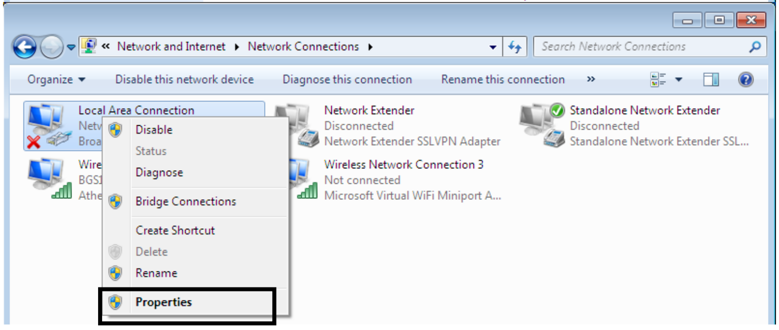
2. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.



Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

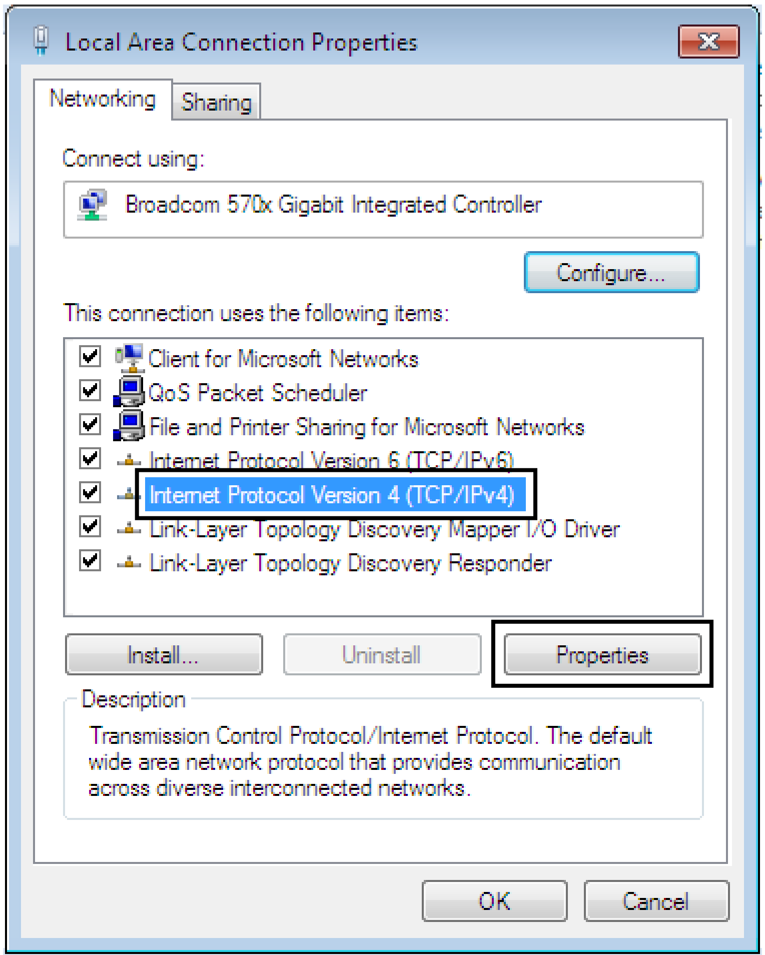
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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



IPv4:

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



Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

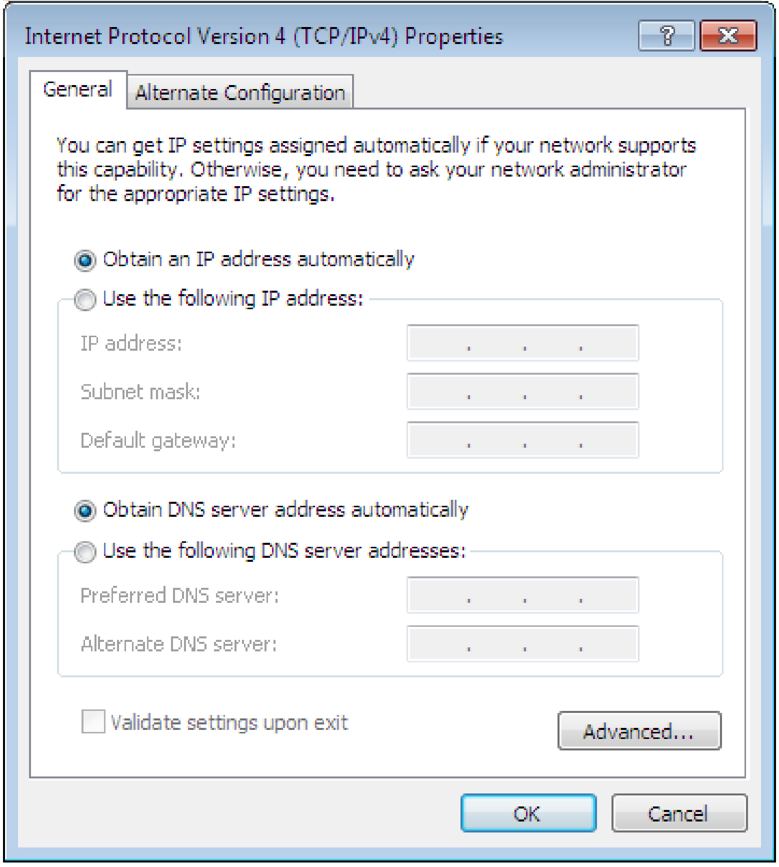
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

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

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

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



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: . . .

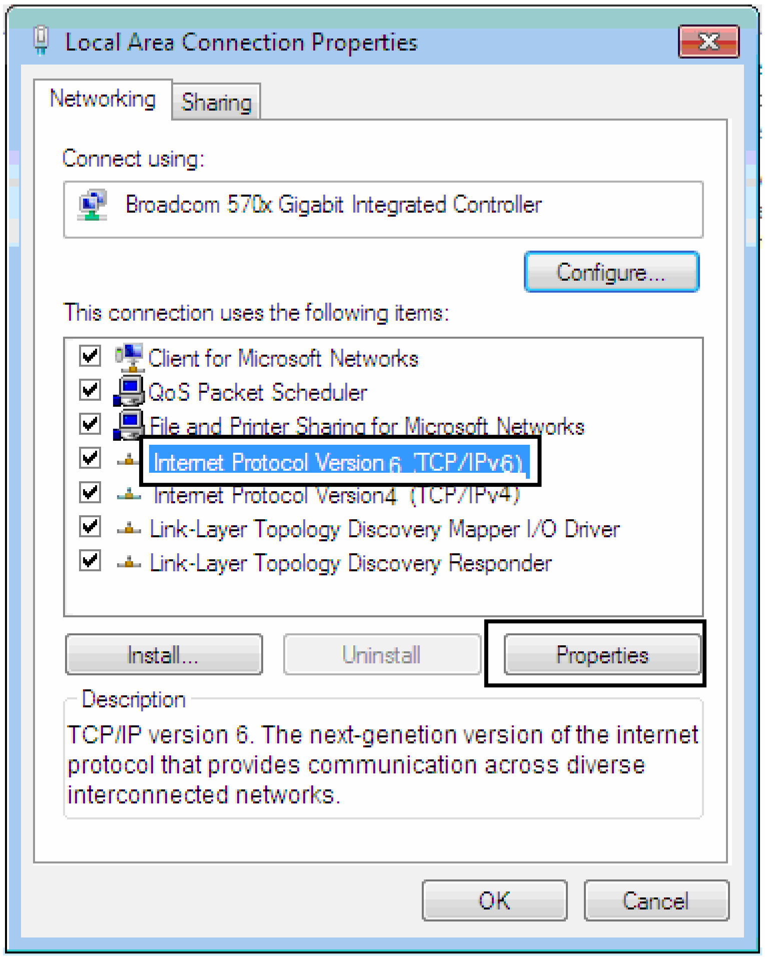
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

IPv6:

4. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

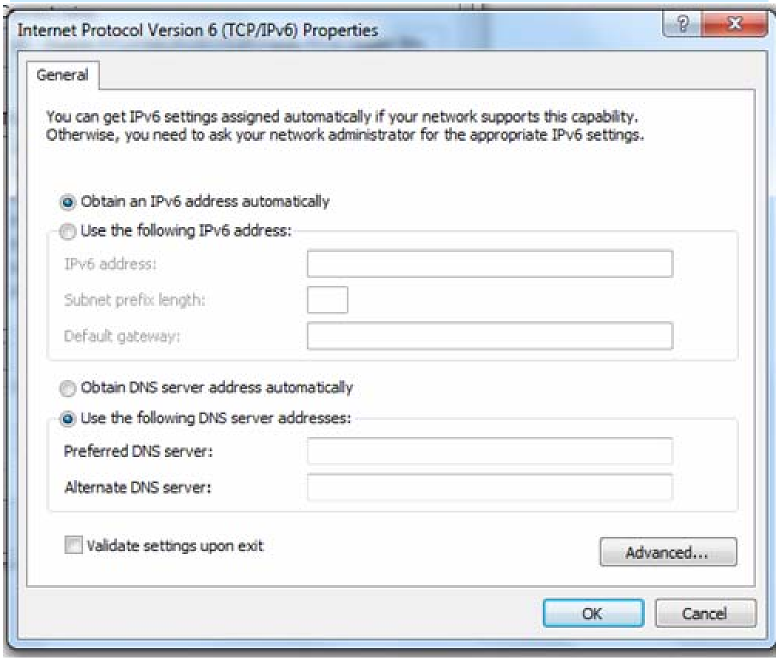
Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

OK | Cancel

5. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

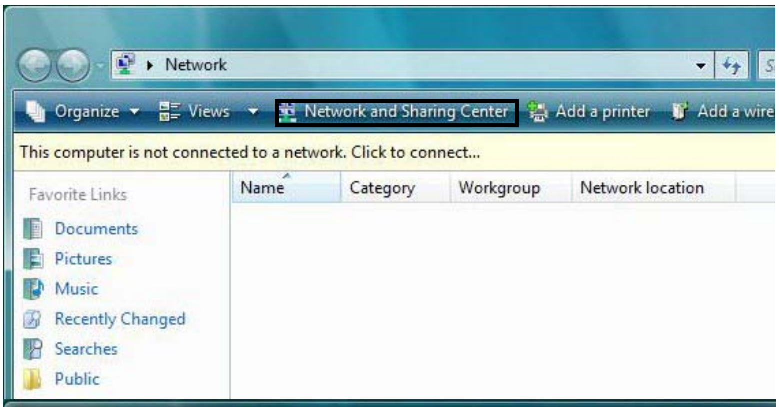
Advanced...

OK | Cancel

Configuring a PC in Windows Vista

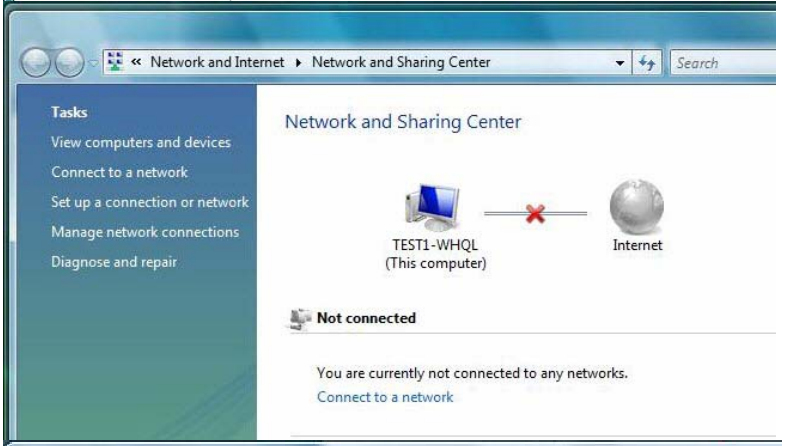
1. Go to **Start**. Click on **Network**.

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



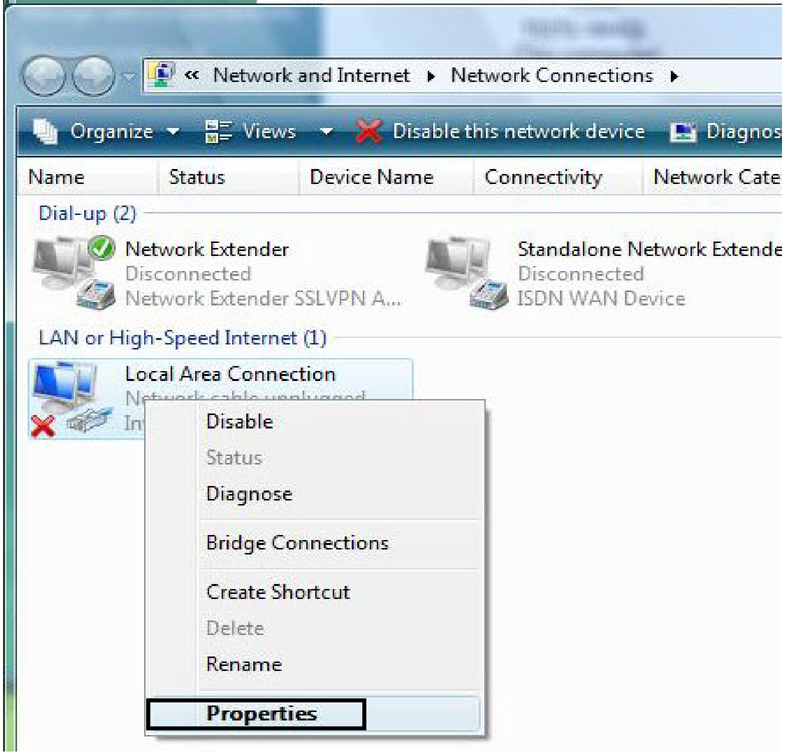
This computer is not connected to a network. Click to connect...

3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.


« 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

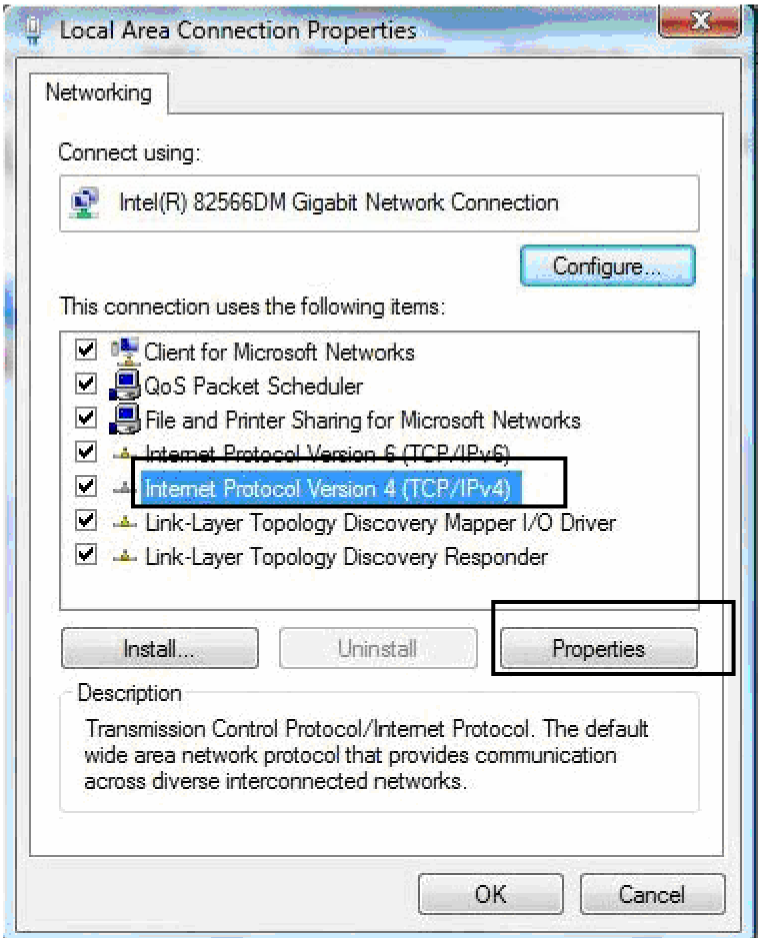
You are currently not connected to any networks.

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



IPv4:

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82566DM Gigabit Network Connection

Configure...

This connection uses the following items:

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

Install... Uninstall Properties

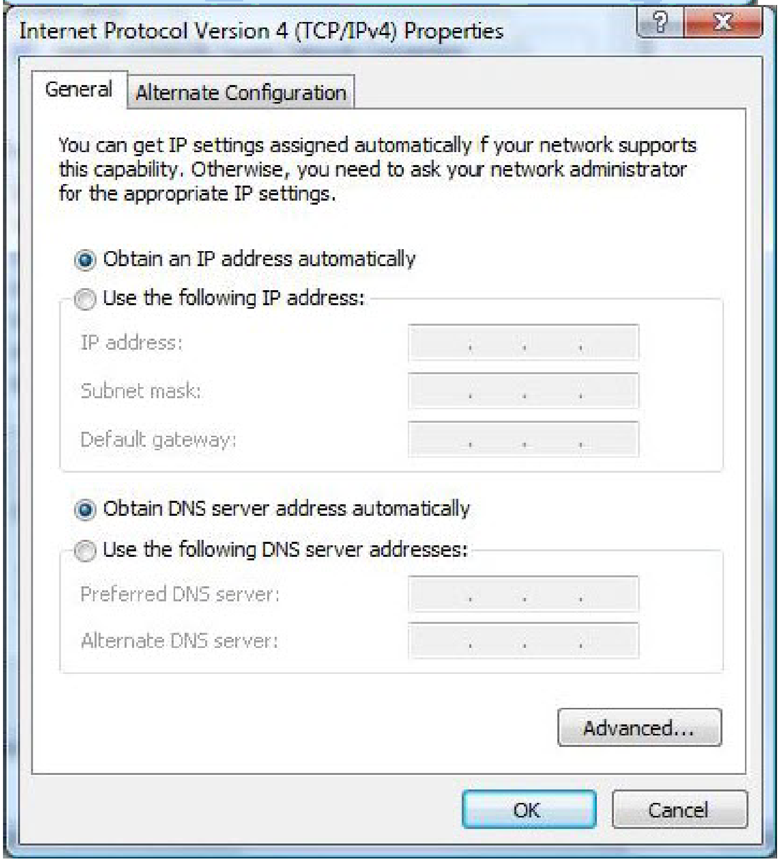
Description

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

OK Cancel

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

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

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

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

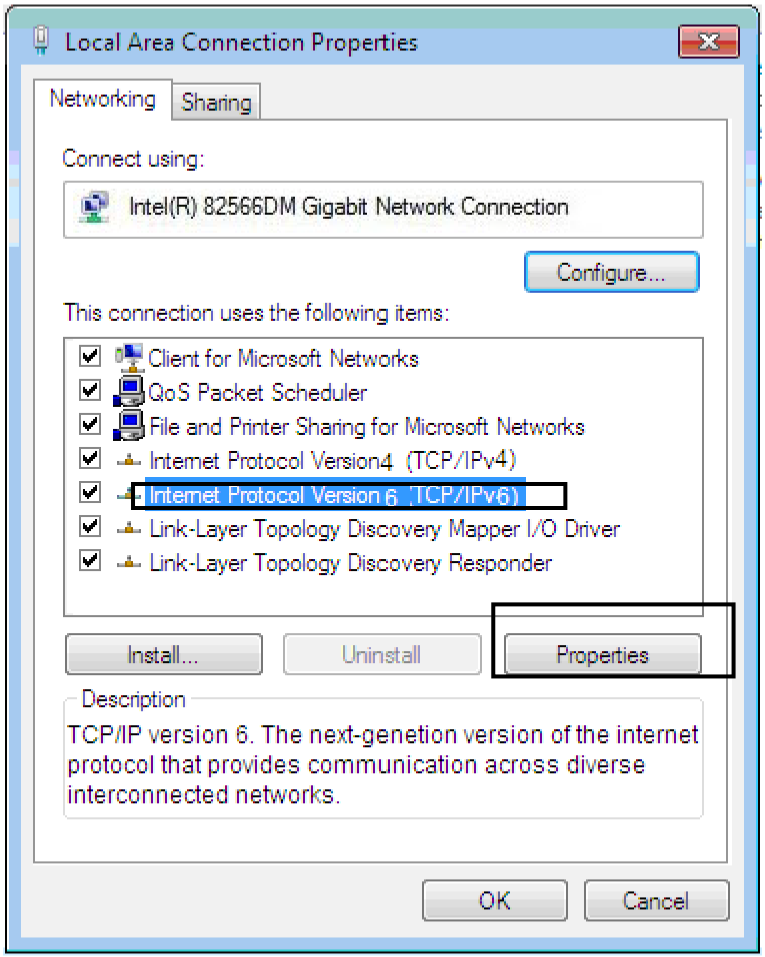
Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK Cancel

IPv6:

8. Select **Internet Protocol Version 6 (TCP/IPv6)** then click **Properties**.



Local Area Connection Properties

Connect using:

Intel(R) 82566DM Gigabit Network Connection

This connection uses the following items:

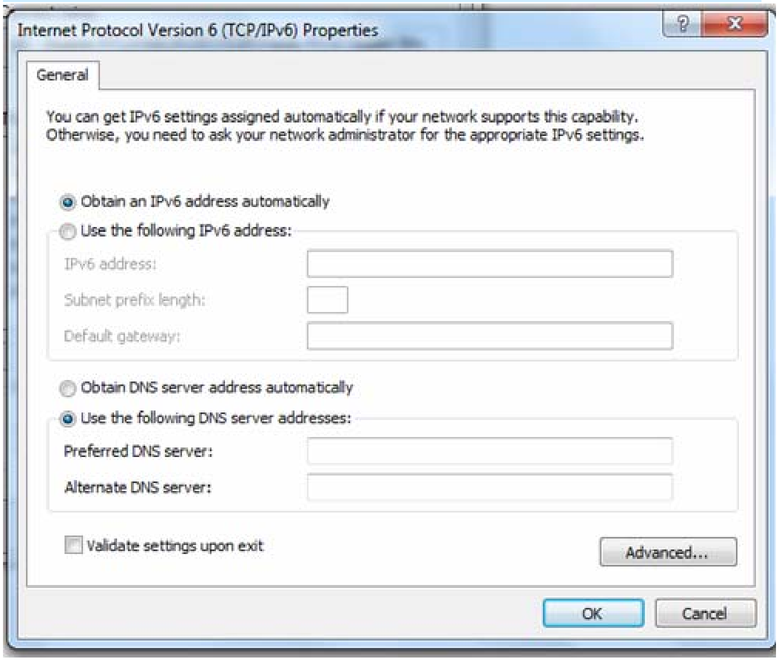
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version4 (TCP/IPv4)
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

9. In the **TCP/IPv6 properties** window, select the Obtain an **IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



Internet Protocol Version 6 (TCP/IPv6) Properties

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically
○ Use the following IPv6 address:

IPv6 address:
Subnet prefix length:
Default gateway:

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

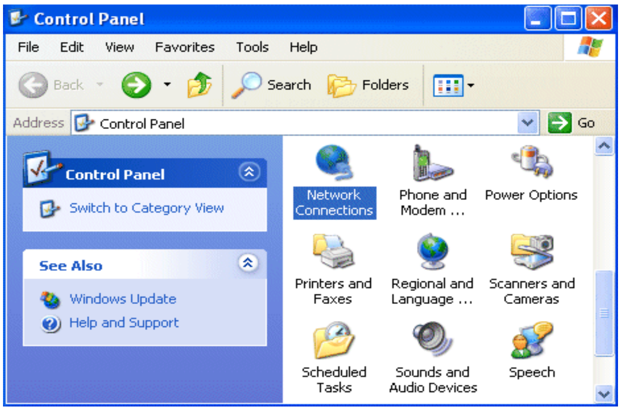
Preferred DNS server:
Alternate DNS server:

□ Validate settings upon exit

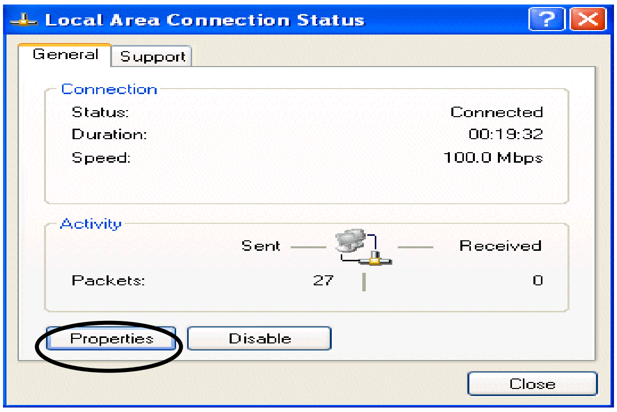
Configuring a PC in Windows XP

IPv4:

1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



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



Connection

Status: Connected

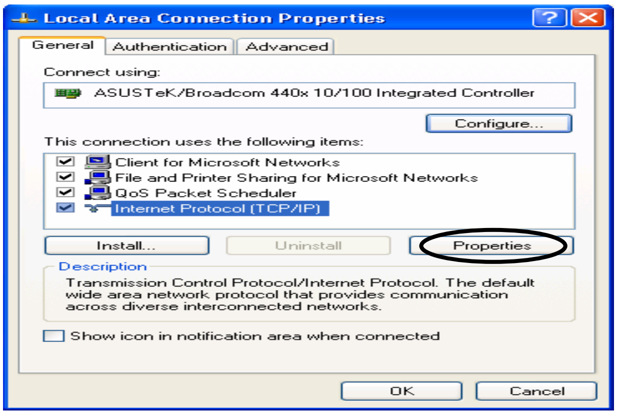
Duration: 00:19:32

Speed: 100.0 Mbps

Activity

	Sent	Received
Packets:	27	0

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


Local Area Connection Properties
General Authentication Advanced
Configure...
Install... Uninstall Properties
OK Cancel

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)

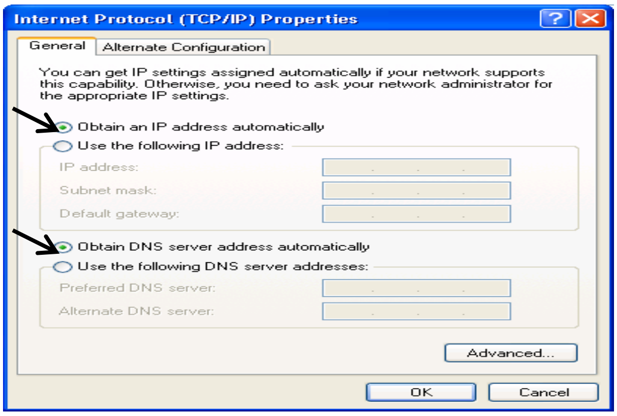
Description

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

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

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


Internet Protocol (TCP/IP) Properties
General Alternate Configuration
Advanced...
OK Cancel

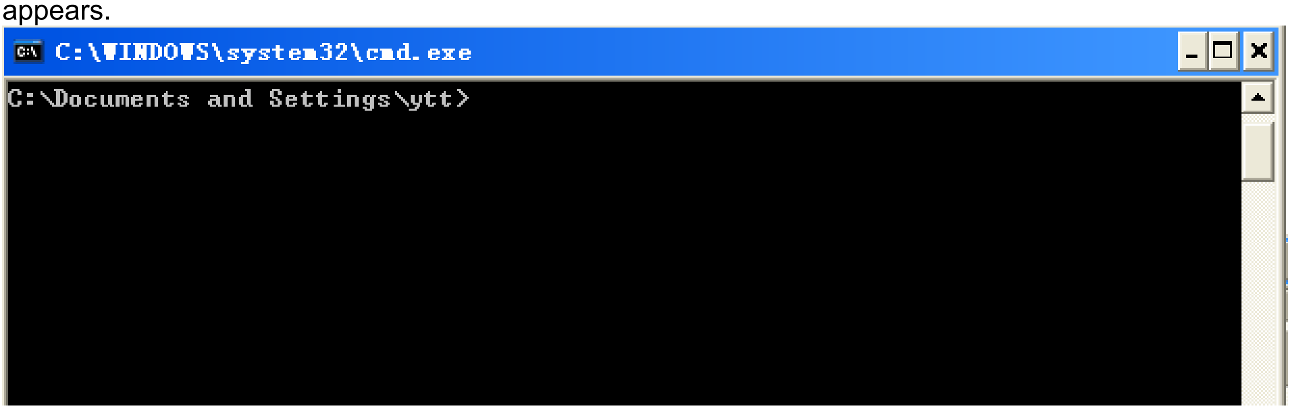
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● 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:

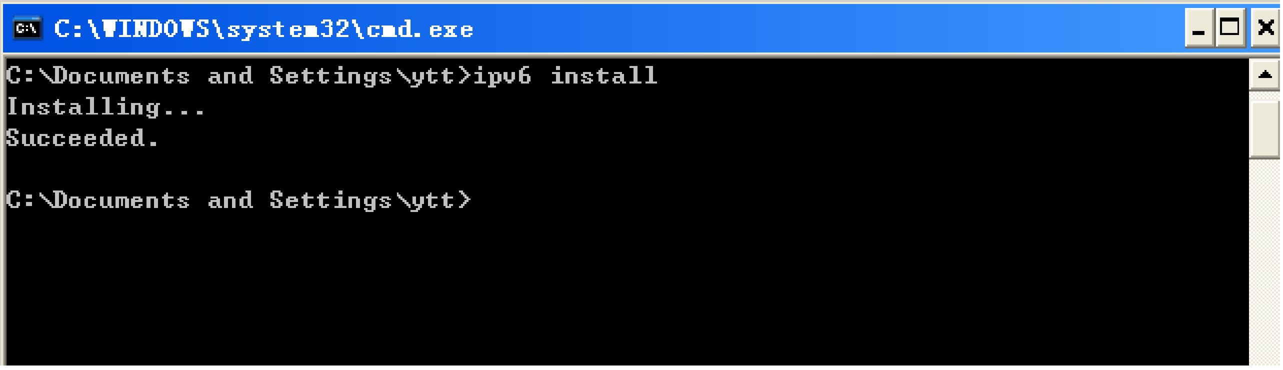
IPv6:

IPv6 is supported by Windows XP, but you should install it first.
Act as shown below:
1. On the desktop, Click Start > Run, type cmd, then press Enter key in the keyboard, the following screen appears.



```
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



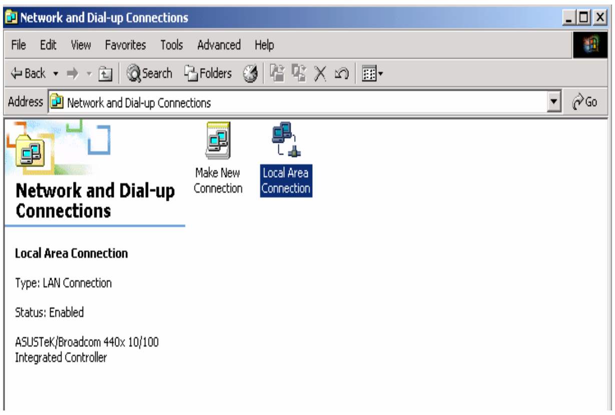
```
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.

C:\Documents and Settings\ytt>
```

Configuration is OK now, you can test whether it works ok.

Configuring a PC in Windows 2000

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

2. Double-click Local Area Connection.


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

Network and Dial-up Connections

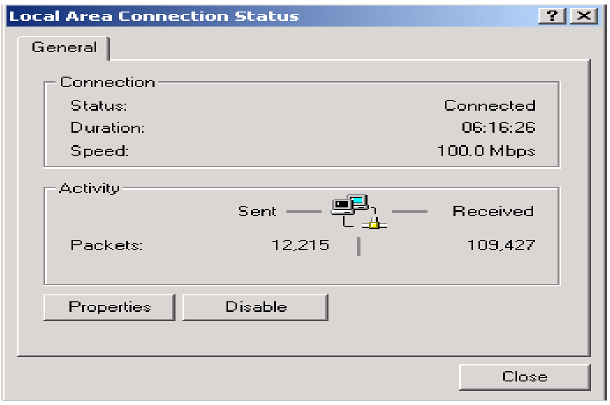
Local Area Connection

Type: LAN Connection

Status: Enabled

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

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



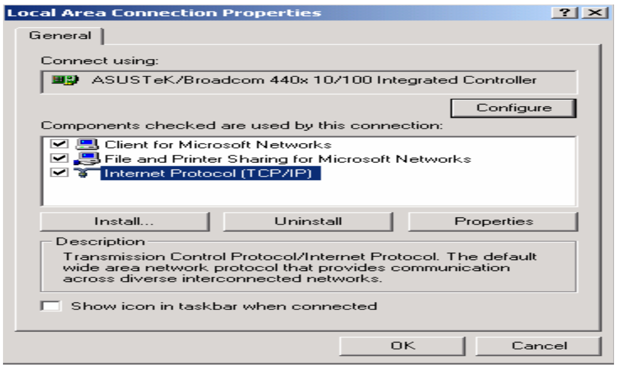
Connection

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

Activity

	Sent	Received
Packets:	12,215	109,427

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



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

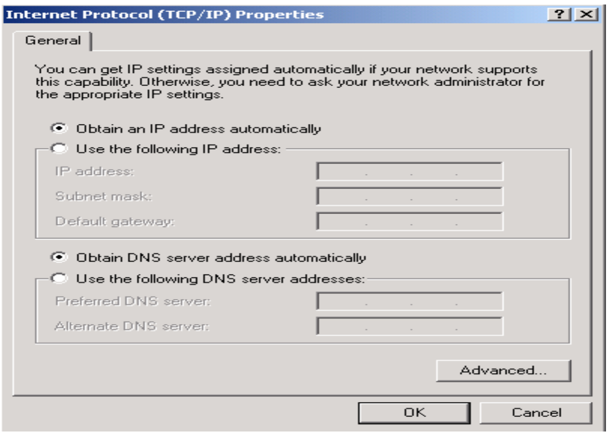
Components checked are used by this connection:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

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

□ Show icon in taskbar when connected

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

6. 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.

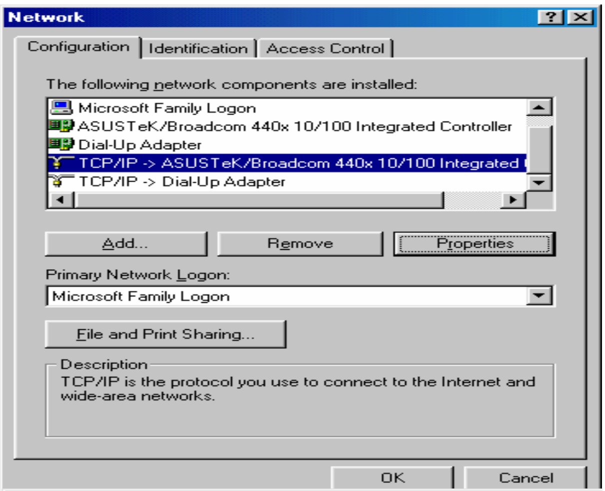
● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

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

Configuring a PC in Windows 95/98/Me

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

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



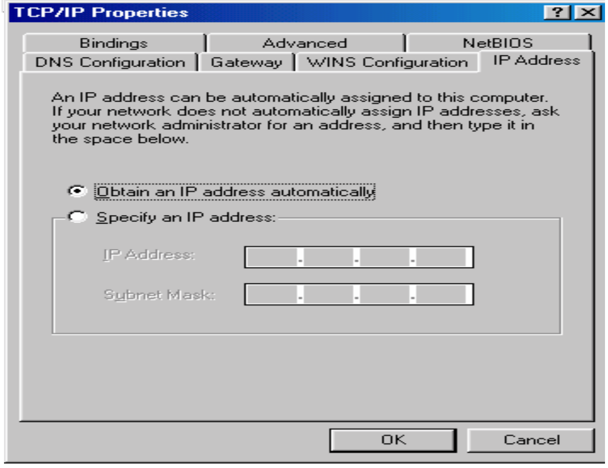
The following network components are installed:

- 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.

3. 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

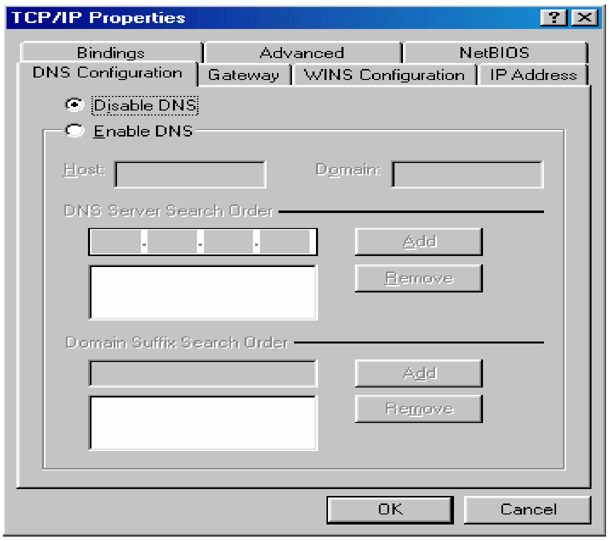
○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

4. Then select the DNS Configuration tab.

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



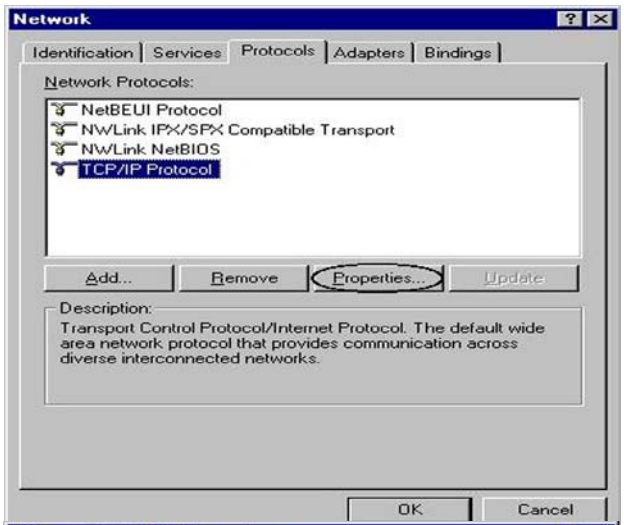
● Disable DNS

○ Enable DNS

Configuring a PC in Windows NT4.0

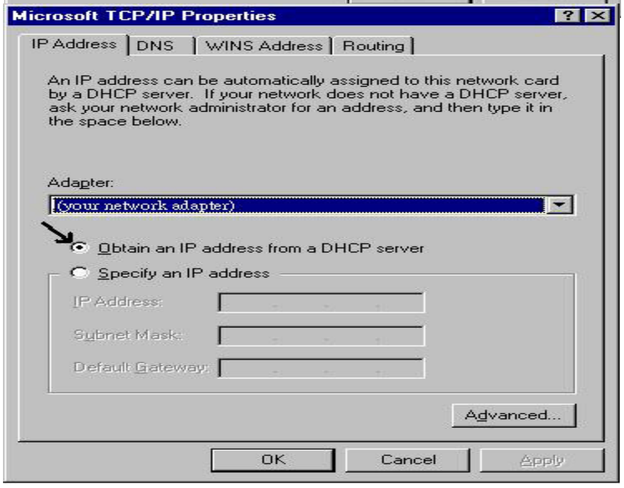
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.

2. Select TCP/IP Protocol and click Properties.



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

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



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

● Obtain an IP address from a DHCP server

Factory Default Settings

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

Web Interface (Username and Password)

Three user levels are provided by this router, namely **Administrator**, **Remote** and **Local** respectively. See Access Control .

Administrator

- Username: admin
- Password: admin

Local

- Username: user
- Password: user

Remote

- Username: support
- Password: support

⚠ Attention	If you have forgotten the username and/or password of the router, you can restore the device to its default setting by pressing the ***Reset Button*** more than ***5*** seconds.

Device LAN IPv4 settings

- IPv4 Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

Device LAN IPv6 settings

- IPv6 Address / prefix: Default is a link-local address and is different from each other as MAC address is different from one to one. For example: fe80:0000:0000:0000:0204:edff:fe01:0001 / 64, the prefix initiates by fe80::

DHCP server for IPv4

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

LAN and WAN Port Addresses

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

IPv4

LAN Port		WAN Port
IPv4 address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

IPv6

LAN Port		WAN Port
IPv6 address/prefix	Default is a link-local address and is different from each other as MAC address is different from one to one. For example :fe80::204:edff:fe01:1/64, the prefix initiates by fe80::	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP.
DHCP server function	Enabled	

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.

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

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

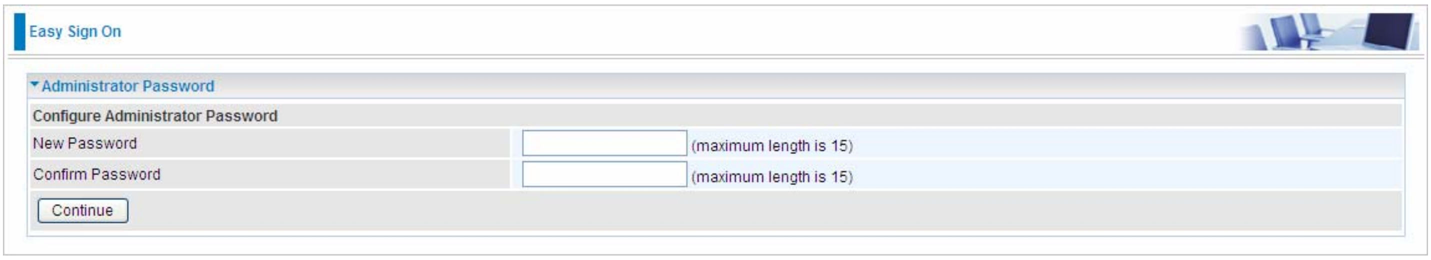
Easy Sign On (EZSO)

This special feature makes it easier for you to configure your router so that you can connect to the internet in a matter of seconds without having to logon to the router GUI for any detail configuration. This configuration method is usually auto initiated if user is to connect to the internet via Billion's router for the first time.

After setting up the router with all the appropriate cables plugged-in, open up your IE browser, the EZSO WEB GUI will automatically pop up and request that you enter some basic information that you have obtained from your ISP. By following the instructions given carefully and through the information you provide, the router will be configured in no time and you will find yourself surfing the internet sooner than you realize.

EZSO window pops up:

Step1: Set the administration password.



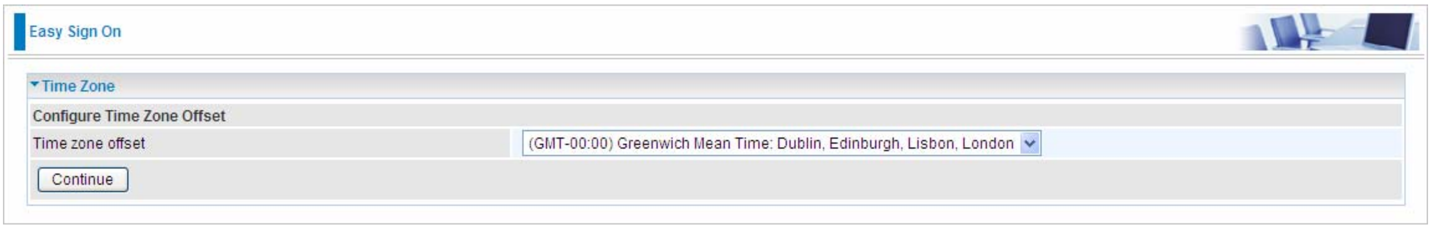
Easy Sign On

▾Administrator Password

Configure Administrator Password

New Password	(maximum length is 15)
Confirm Password	(maximum length is 15)

Step 2: Set the Time Zone.



Easy Sign On

▾Time Zone

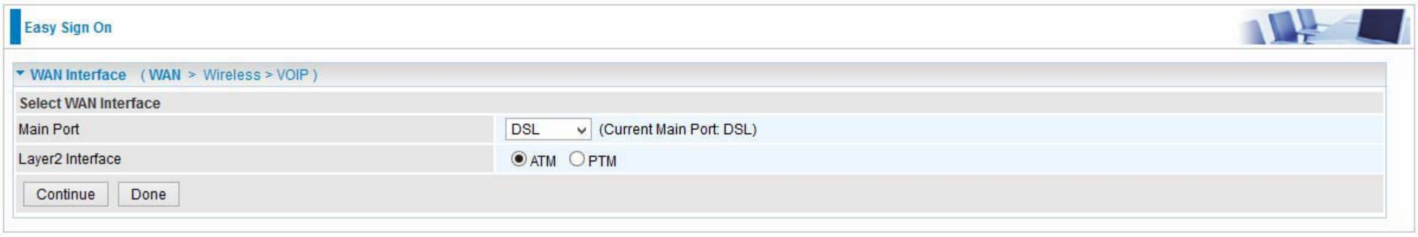
Configure Time Zone Offset

Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Step 3: Configure the WAN interface.

DSL mode

Before configuring with DSL mode, please confirm you have correctly connected the DSL line, and it is now synchronized.



Easy Sign On

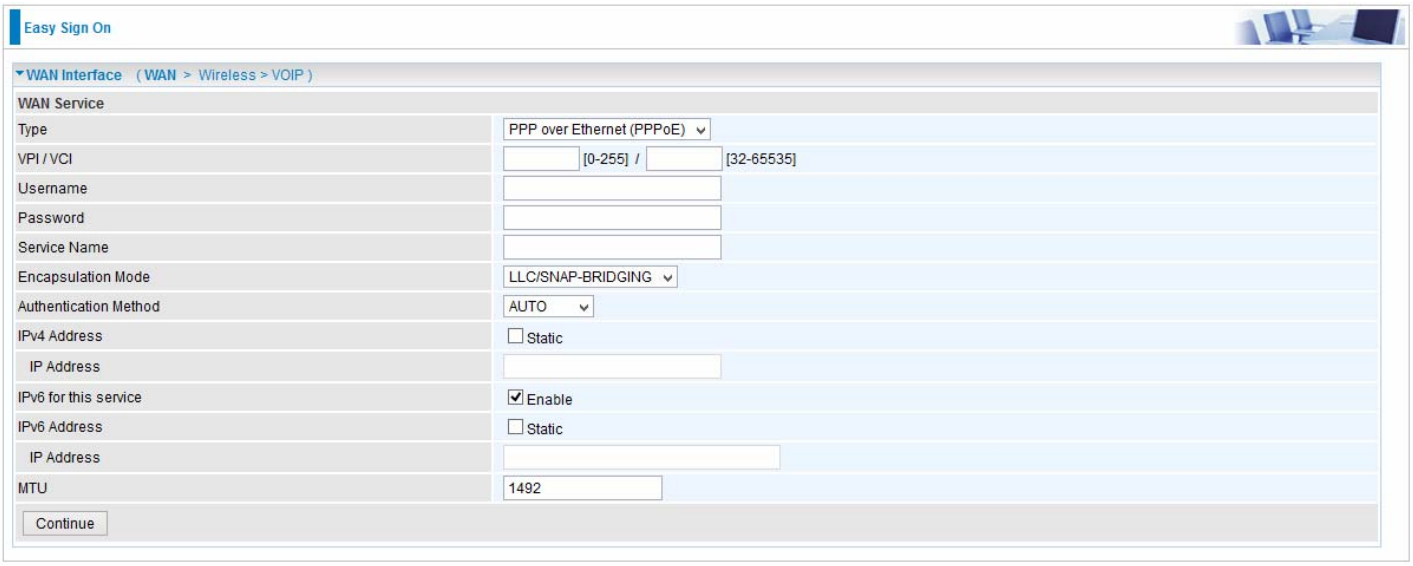
▾ WAN Interface (WAN > Wireless > VOIP)

Select WAN Interface

Main Port	DSL (Current Main Port: DSL)
Layer2 Interface	● ATM ○ PTM

1. Select DSL, press **Continue** to go on to next step, press “Done” to quit the setting.

2. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.



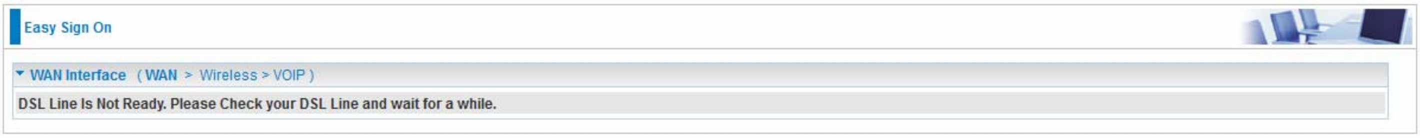
Easy Sign On

▾WAN Interface (WAN > Wireless > VOIP)

WAN Service	
Type	PPP over Ethernet (PPPoE) ⌄
VPI / VCI	[0-255] / [32-65535]
Username	
Password	
Service Name	
Encapsulation Mode	LLC/SNAP-BRIDGING ⌄
Authentication Method	AUTO ⌄
IPv4 Address	□ Static
IP Address	
IPv6 for this service	☑ Enable
IPv6 Address	□ Static
IP Address	
MTU	1492

Continue

If the DLS line doesn't synchronize, the page will pop up warning of the DSL connection failure.

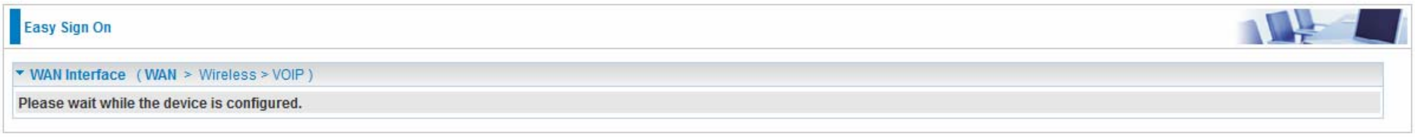


Easy Sign On

▾ WAN Interface (WAN > Wireless > VOIP)

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

3. Wait while the device is configured (DSL synchronized).

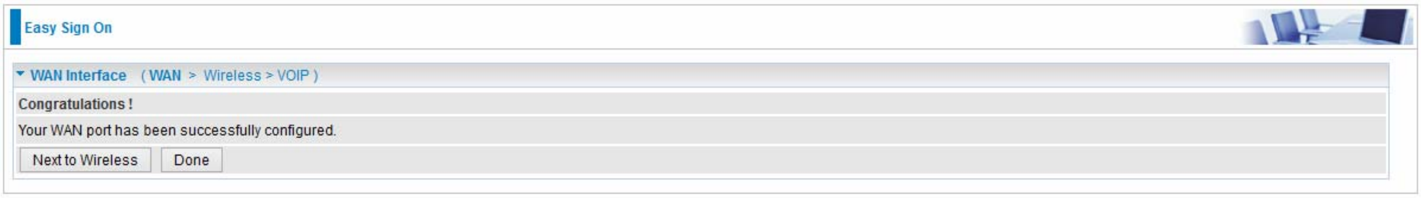


Easy Sign On

▾ WAN Interface (WAN > Wireless > VOIP)

Please wait while the device is configured.

4. WAN port configuration is success and next to wireless, if you want skip wireless setting, click **Done**.



Easy Sign On

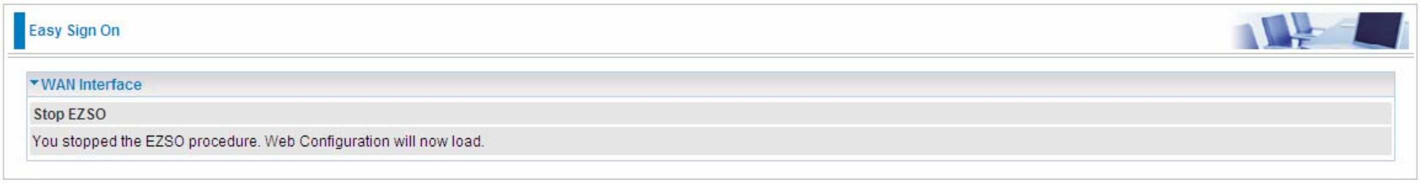
▾ WAN Interface (WAN > Wireless > VOIP)

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless | Done

Click **Done**, web configuration will be loaded, you will enter the web configuration page.



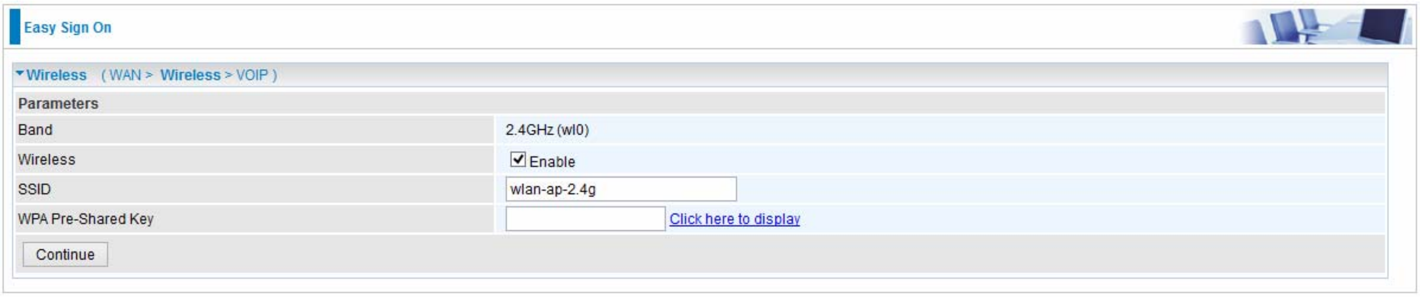
Easy Sign On

▾WAN Interface

Stop EZSO

You stopped the EZSO procedure. Web Configuration will now load.

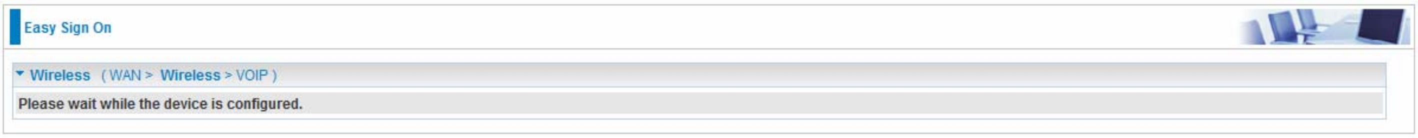
5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 7800VDP(O)X supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key. (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).



Easy Sign On

▾Wireless (WAN > Wireless > VOIP)

Parameters	
Band	2.4GHz (wl0)
Wireless	☑ Enable
SSID	wlan-ap-2.4g
WPA Pre-Shared Key	Click here to display

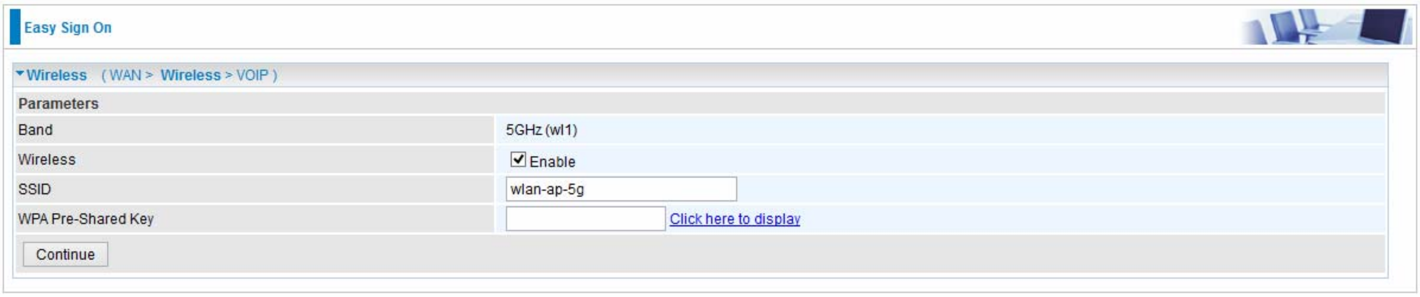


Easy Sign On

▾ Wireless (WAN > Wireless > VOIP)

Please wait while the device is configured.

6. Continue to set 5GHz wireless.

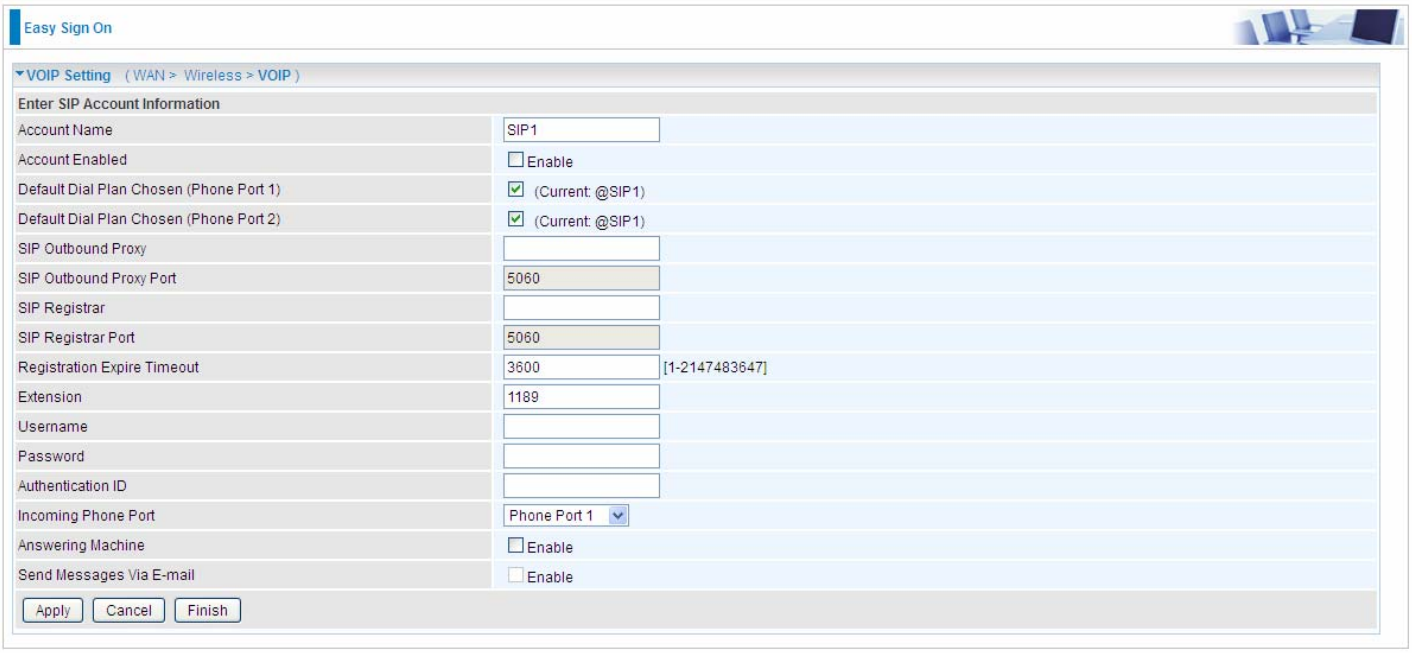


Easy Sign On

▾Wireless (WAN > Wireless > VOIP)

Parameters	
Band	5GHz (wl1)
Wireless	☑ Enable
SSID	wlan-ap-5g
WPA Pre-Shared Key	Click here to display

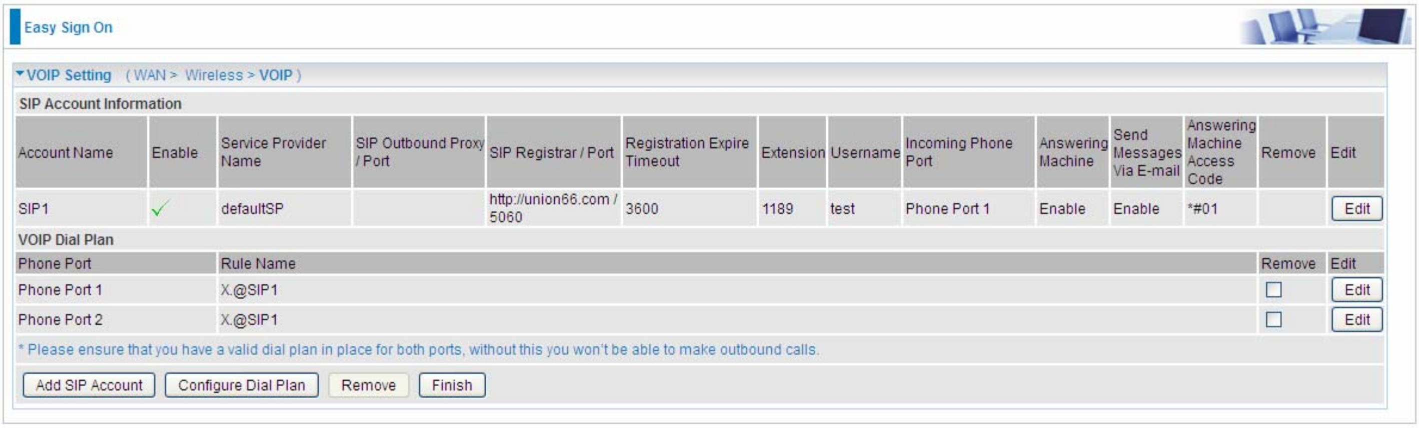
7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, write down the registration information and fill it in the following blanks. For detail, please refer to VoIP.



Easy Sign On

▾VOIP Setting (WAN > Wireless > VOIP)

Enter SIP Account Information	
Account Name	SIP1
Account Enabled	☐ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @SIP1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @SIP1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	1189
Username	
Password	
Authentication ID	
Incoming Phone Port	Phone Port 1
Answering Machine	☐ Enable
Send Messages Via E-mail	☐ Enable



Easy Sign On

▾VOIP Setting (WAN > Wireless > VOIP)

SIP Account Information

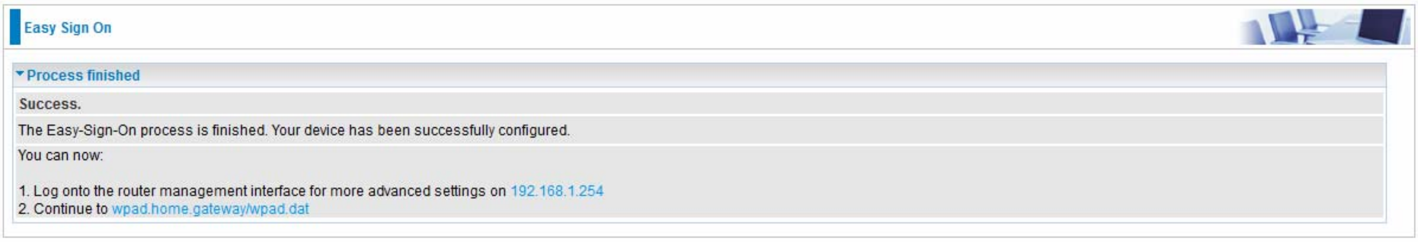
Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✓	defaultSP		http://union66.com / 5060	3600	1189	test	Phone Port 1	Enable	Enable	*#01		Edit

VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

8. In the above page, click finish to complete the EZSO settings.



Easy Sign On

▾Process finished

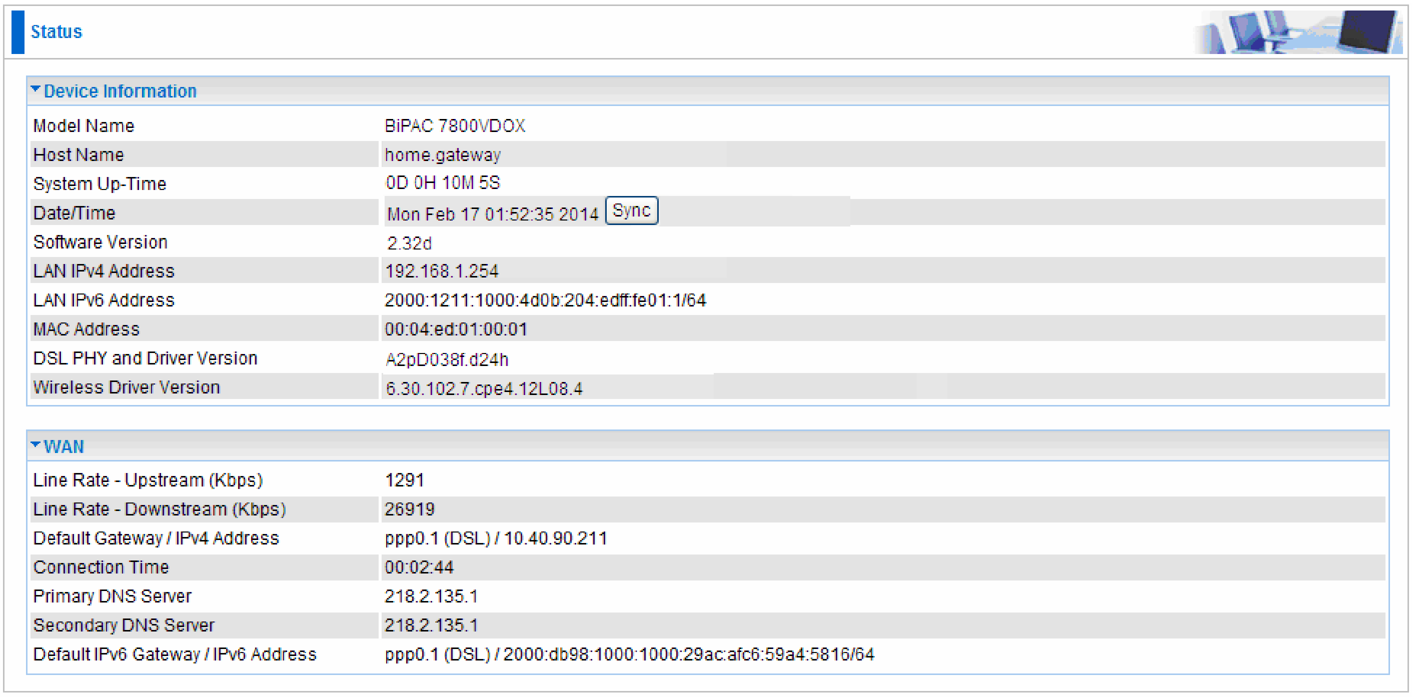
Success.

The Easy-Sign-On process is finished. Your device has been successfully configured.

You can now:

1. Log onto the router management interface for more advanced settings on 192.168.1.254
2. Continue to wpad.home.gateway/wpad.dat

Click link ***192.168.1.254***, it will lead you to the following page.



Status

▾Device Information

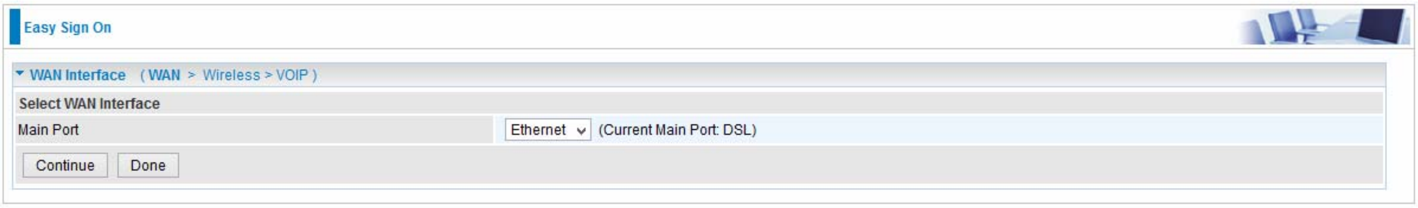
Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 10M 5S
Date/Time	Mon Feb 17 01:52:35 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

▾WAN

Line Rate - Upstream (Kbps)	1291
Line Rate - Downstream (Kbps)	26919
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

Ethernet mode

1. Select **Ethernet,** press **Continue** to go on to next step.

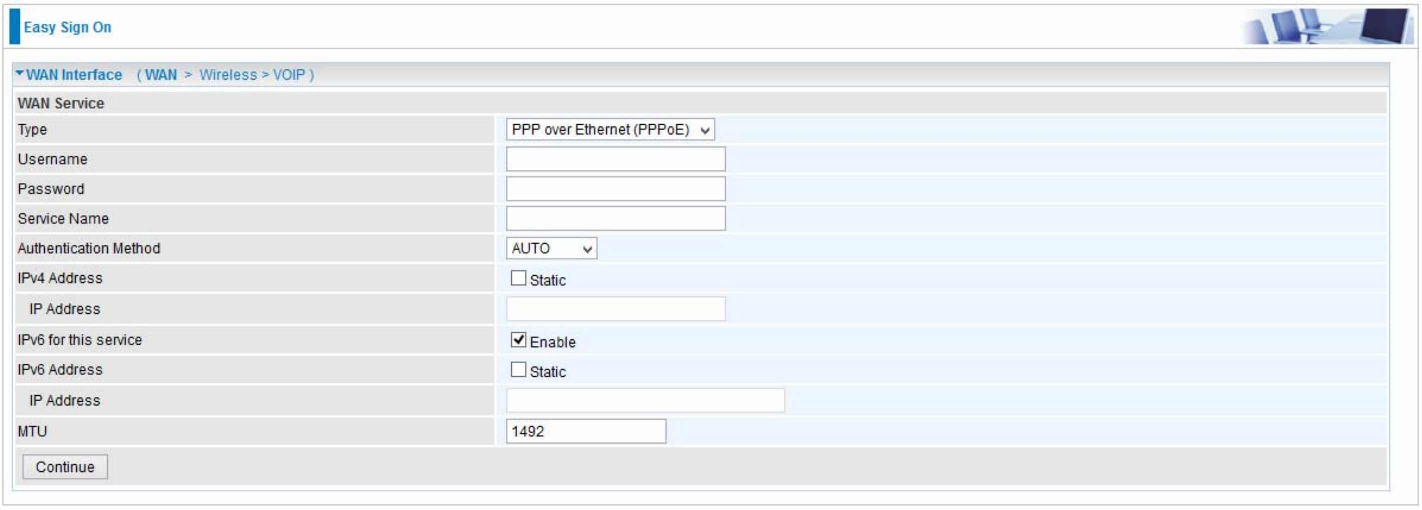


Easy Sign On

▾ WAN Interface (WAN > Wireless > VOIP)

Select WAN Interface	
Main Port	Ethernet ⌄ (Current Main Port: DSL)

2. Enter the username, password from your ISP, for IP and DNS settings, also refer to your ISP. Here IPv6 service is enabled by default.

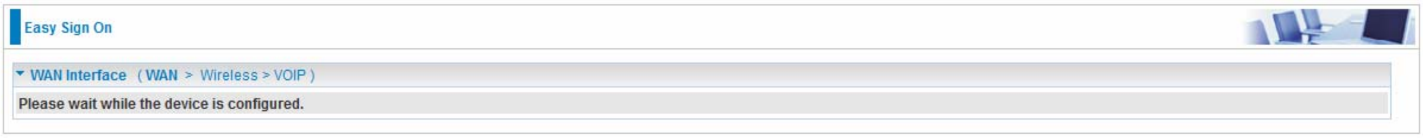


Easy Sign On

▾ WAN Interface (WAN > Wireless > VOIP)

WAN Service	
Type	PPP over Ethernet (PPPoE) ⌄
Username	
Password	
Service Name	
Authentication Method	AUTO ⌄
IPv4 Address	□ Static
IP Address	
IPv6 for this service	☑ Enable
IPv6 Address	□ Static
IP Address	
MTU	1492

3. Wait while the device is configured.

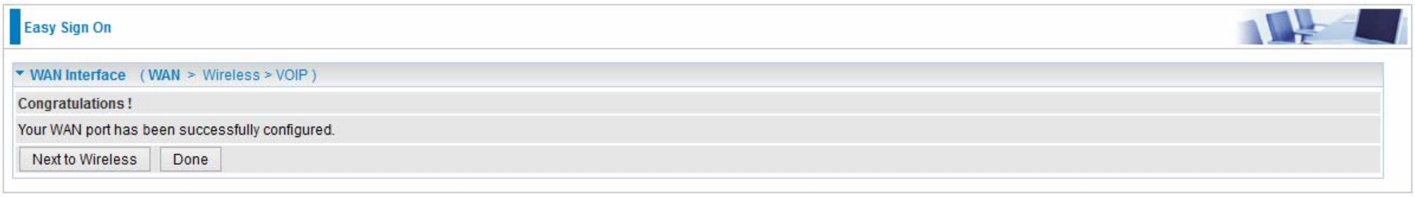


Easy Sign On

▾ WAN Interface (WAN > Wireless > VOIP)

Please wait while the device is configured.

4. WAN port configuration is success.



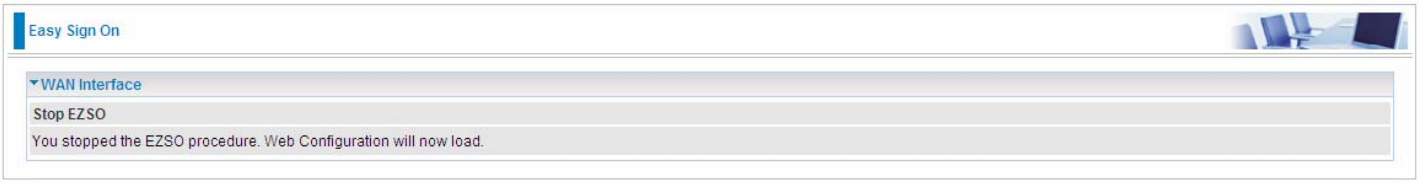
Easy Sign On

▾ WAN Interface (WAN > Wireless > VOIP)

Congratulations !

Your WAN port has been successfully configured.

Click **Done**, web configuration will be loaded, you will enter the web configuration page.



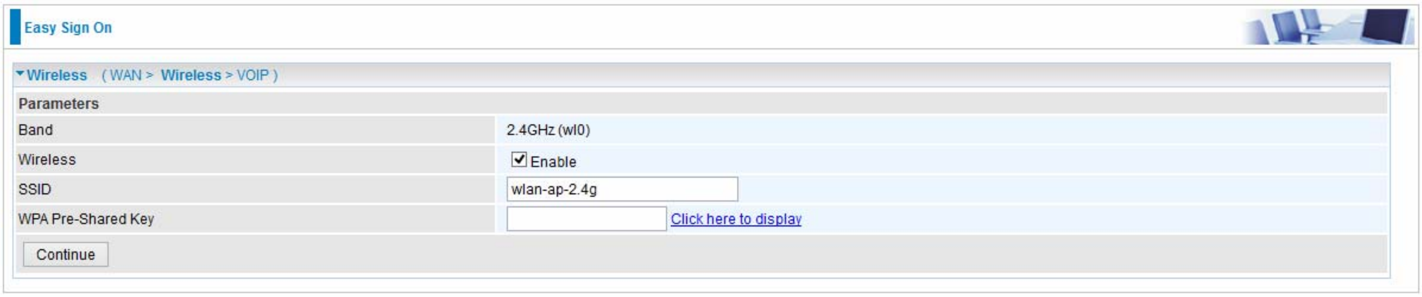
Easy Sign On

▾ WAN Interface

Stop EZSO

You stopped the EZSO procedure. Web Configuration will now load.

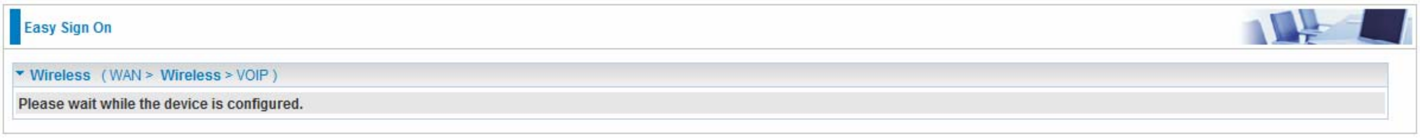
5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 7800VDP(O)X supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).



Easy Sign On

Wireless (WAN > Wireless > VOIP)

Parameters	
Band	2.4GHz (wl0)
Wireless	☑ Enable
SSID	wlan-ap-2.4g
WPA Pre-Shared Key	Click here to display

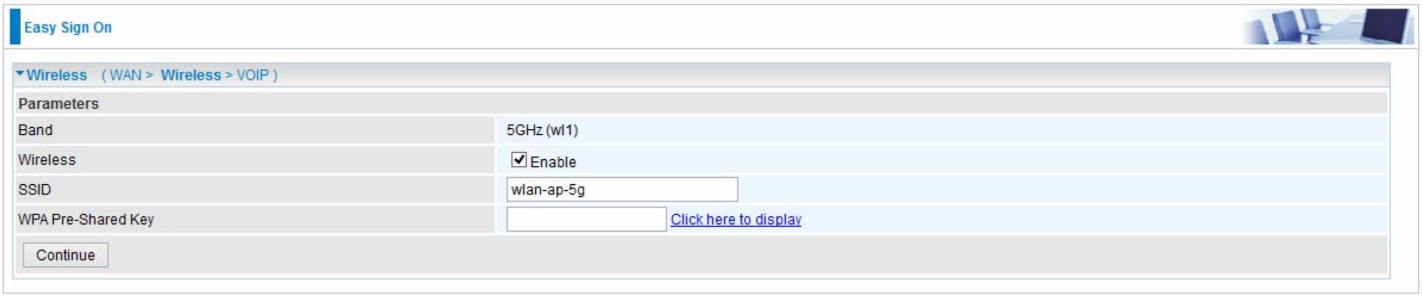


Easy Sign On

Wireless (WAN > Wireless > VOIP)

Please wait while the device is configured.

6. Continue to set 5GHz wireless.

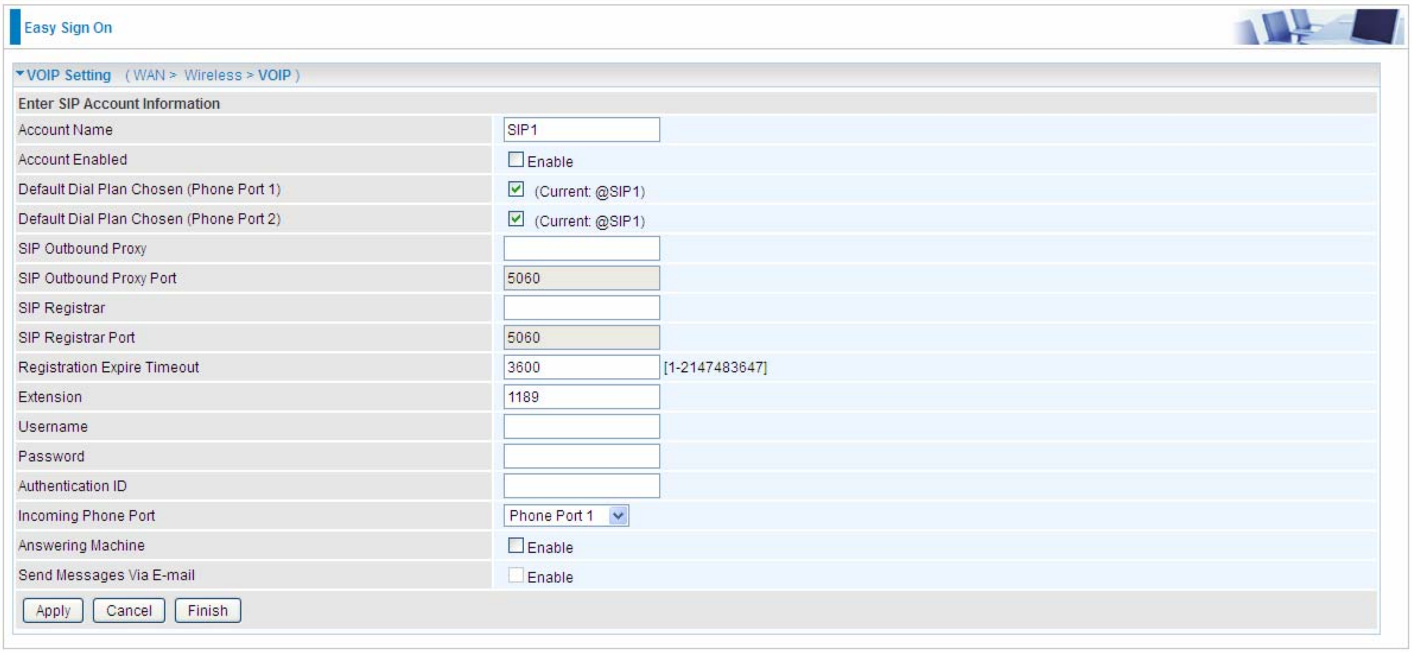


Easy Sign On

Wireless (WAN > Wireless > VOIP)

Parameters	
Band	5GHz (wl1)
Wireless	☑ Enable
SSID	wlan-ap-5g
WPA Pre-Shared Key	Click here to display

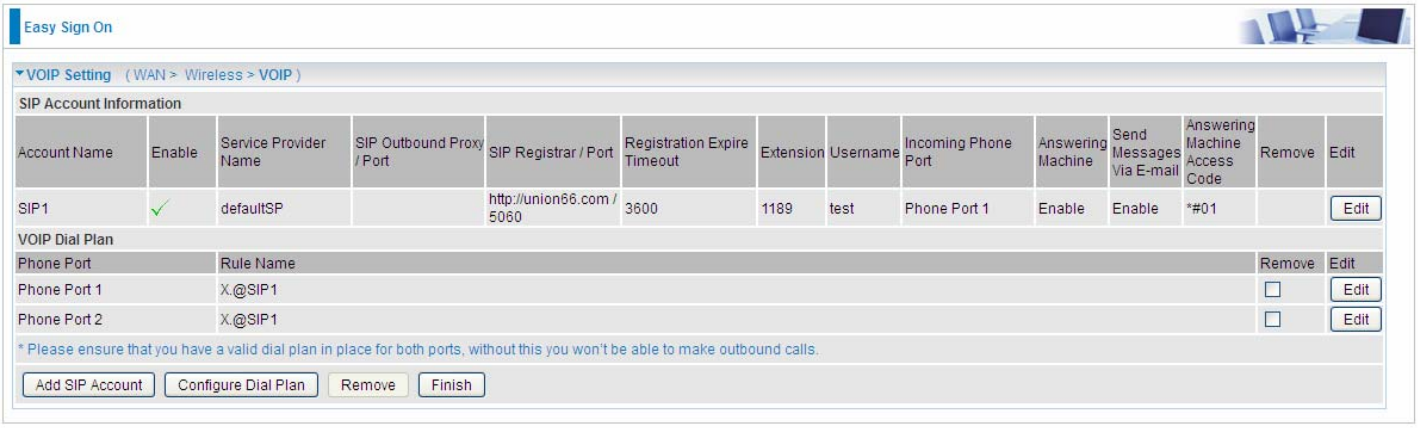
7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, write down the registration information and fill it in the following blanks. For detail, please refer to VoIP.



Easy Sign On

VOIP Setting (WAN > Wireless > VOIP)

Enter SIP Account Information	
Account Name	SIP1
Account Enabled	□ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @SIP1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @SIP1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	1189
Username	
Password	
Authentication ID	
Incoming Phone Port	Phone Port 1
Answering Machine	□ Enable
Send Messages Via E-mail	□ Enable



Easy Sign On

VOIP Setting (WAN > Wireless > VOIP)

SIP Account Information

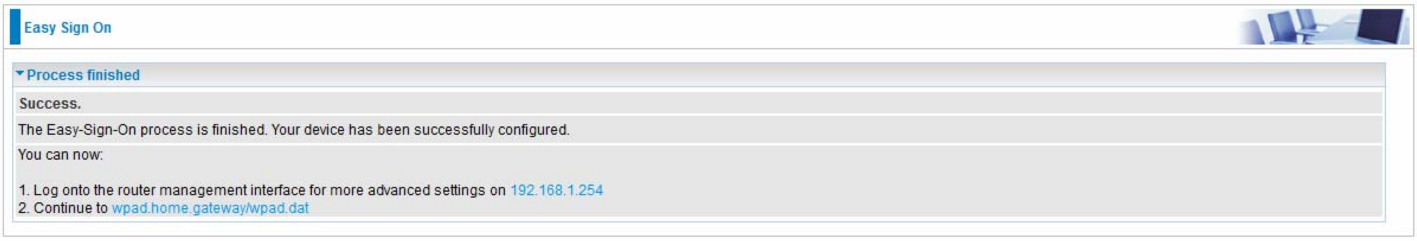
Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✓	defaultSP		http://union66.com / 5060	3600	1189	test	Phone Port 1	Enable	Enable	*#01		Edit

VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

8. In the above page, click finish to complete the EZSO settings.



Easy Sign On

Process finished

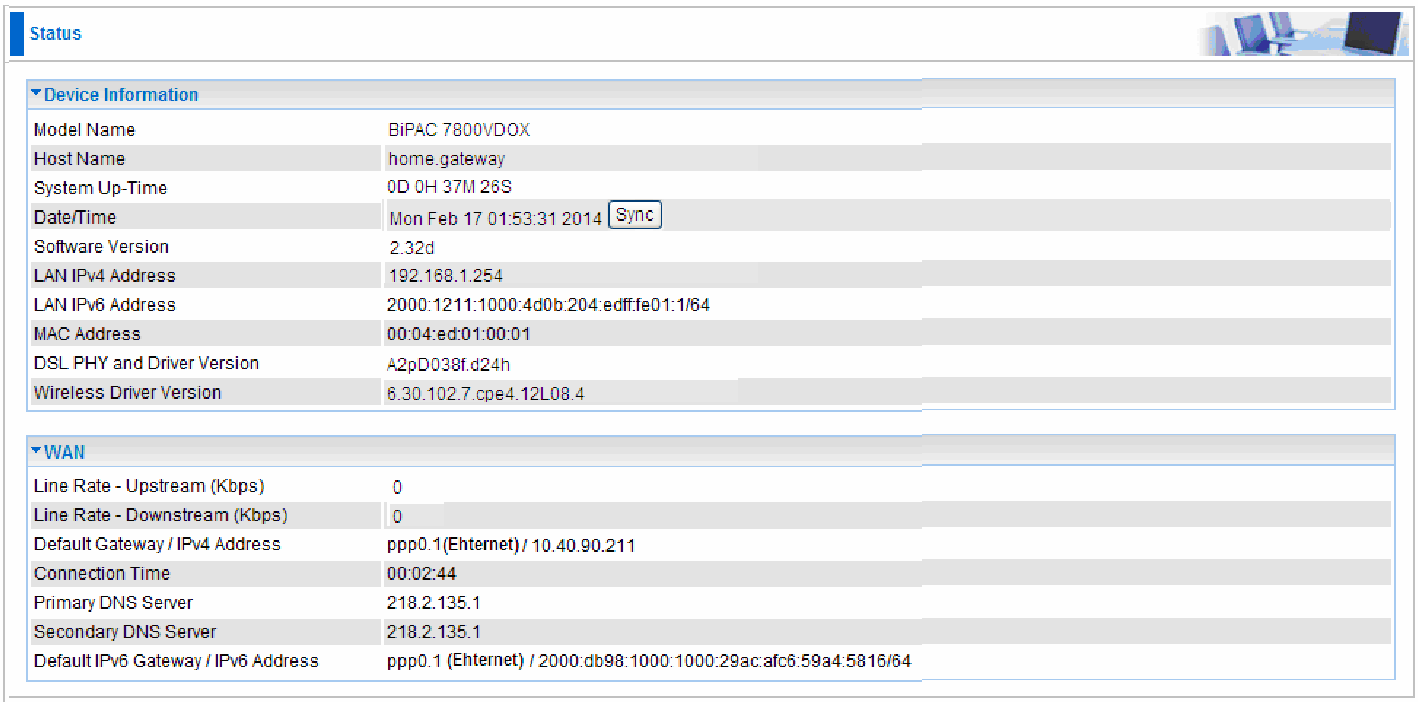
Success.

The Easy-Sign-On process is finished. Your device has been successfully configured.

You can now:

1. Log onto the router management interface for more advanced settings on 192.168.1.254
2. Continue to wpad.home.gateway/wpad.dat

Click ***192.168.1.254***, it will lead you to the following page.



Status

Device Information

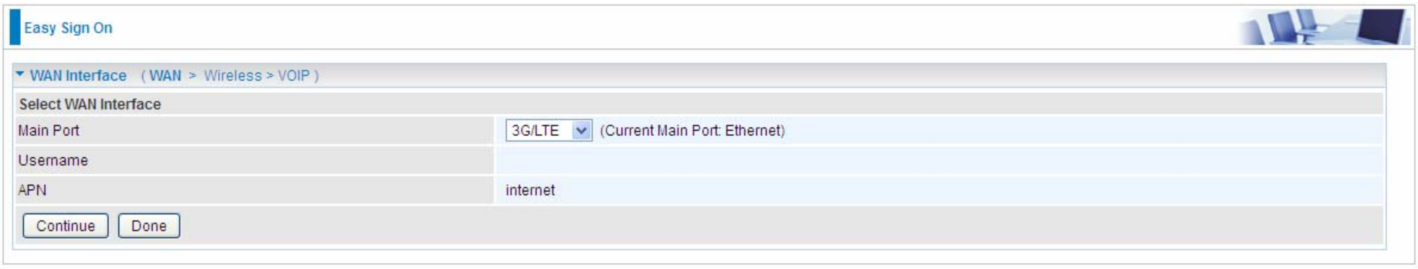
Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 37M 26S
Date/Time	Mon Feb 17 01:53:31 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp0.1(Ehternet) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (Ehternet) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

3G/LTE

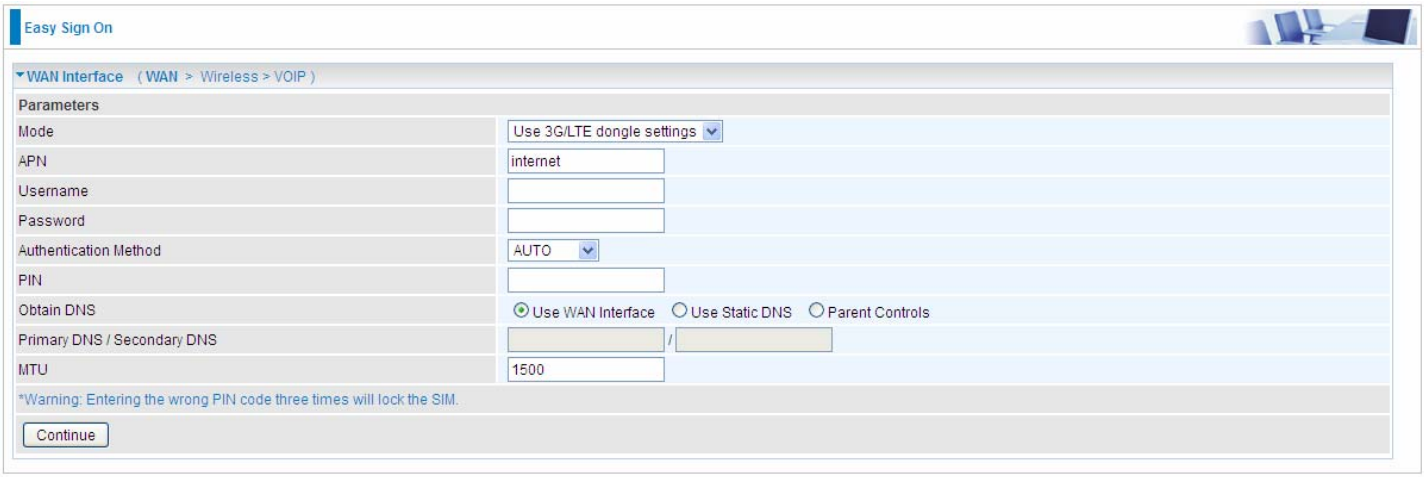
1. Select **3G/LTE,** press **Continue** to go on to next step.



Select WAN Interface

Main Port	3G/LTE (Current Main Port: Ethernet)
Username	
APN	internet

2. Enter the APN, username, password from your ISP, for settings about Authentication method, PIN, etc, also refer to your ISP.

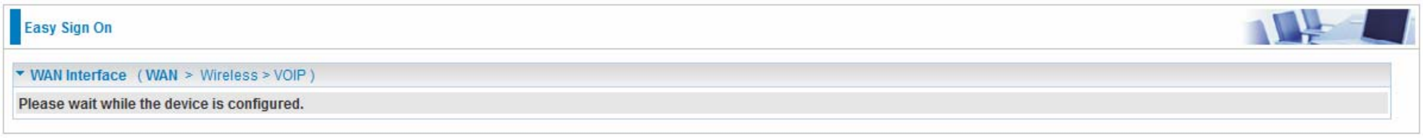


Parameters

Mode	Use 3G/LTE dongle settings
APN	internet
Username	
Password	
Authentication Method	AUTO
PIN	
Obtain DNS	● Use WAN Interface ○ Use Static DNS ○ Parent Controls
Primary DNS / Secondary DNS	/
MTU	1500

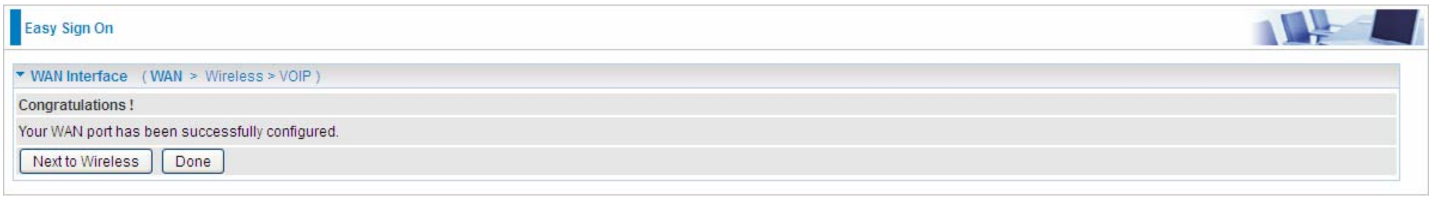
*Warning: Entering the wrong PIN code three times will lock the SIM.

3. Wait while the device is configured.



Please wait while the device is configured.

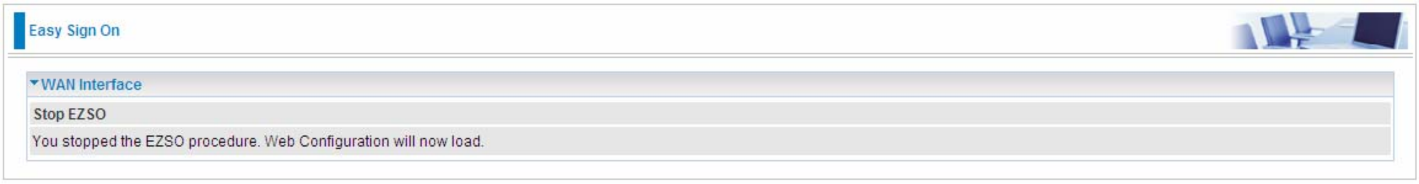
4. WAN port configuration is success.



Congratulations !

Your WAN port has been successfully configured.

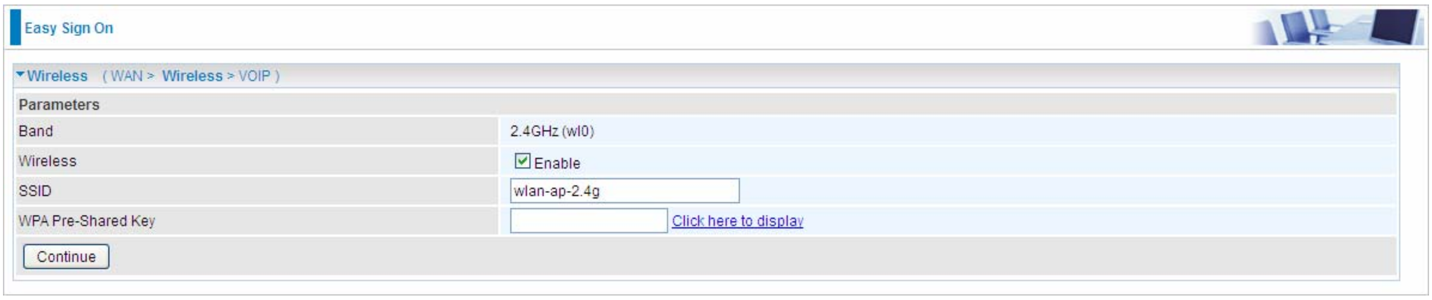
Click **Done**, web configuration will be loaded, you will enter the web configuration page.



Stop EZSO

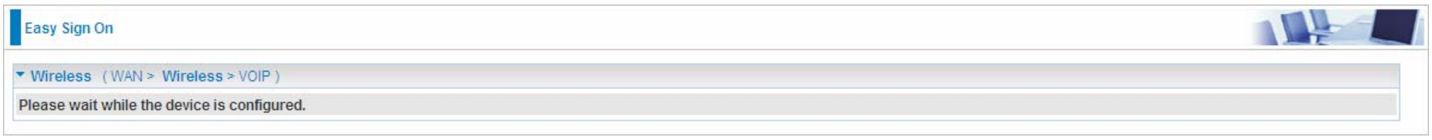
You stopped the EZSO procedure. Web Configuration will now load.

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 7800VDP(O)X supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).



▾Wireless (WAN > Wireless > VOIP)

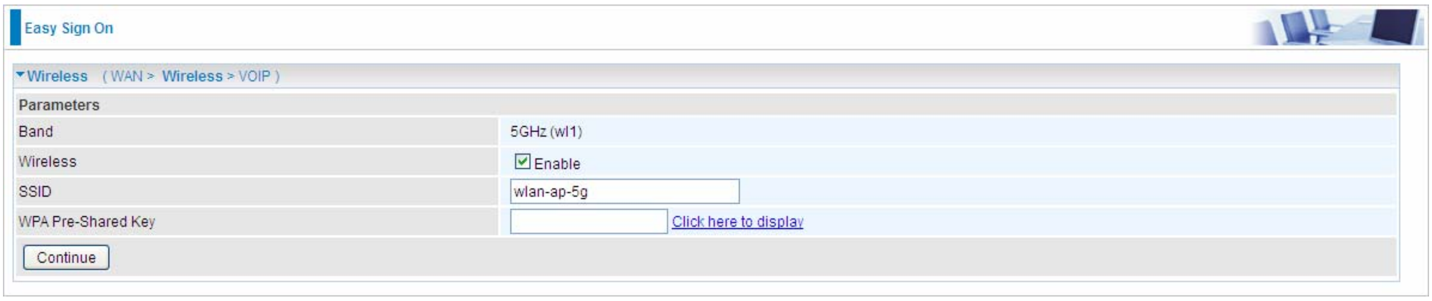
Parameters	
Band	2.4GHz (wl0)
Wireless	☑ Enable
SSID	wlan-ap-2.4g
WPA Pre-Shared Key	Click here to display



▾ Wireless (WAN > Wireless > VOIP)

Please wait while the device is configured.

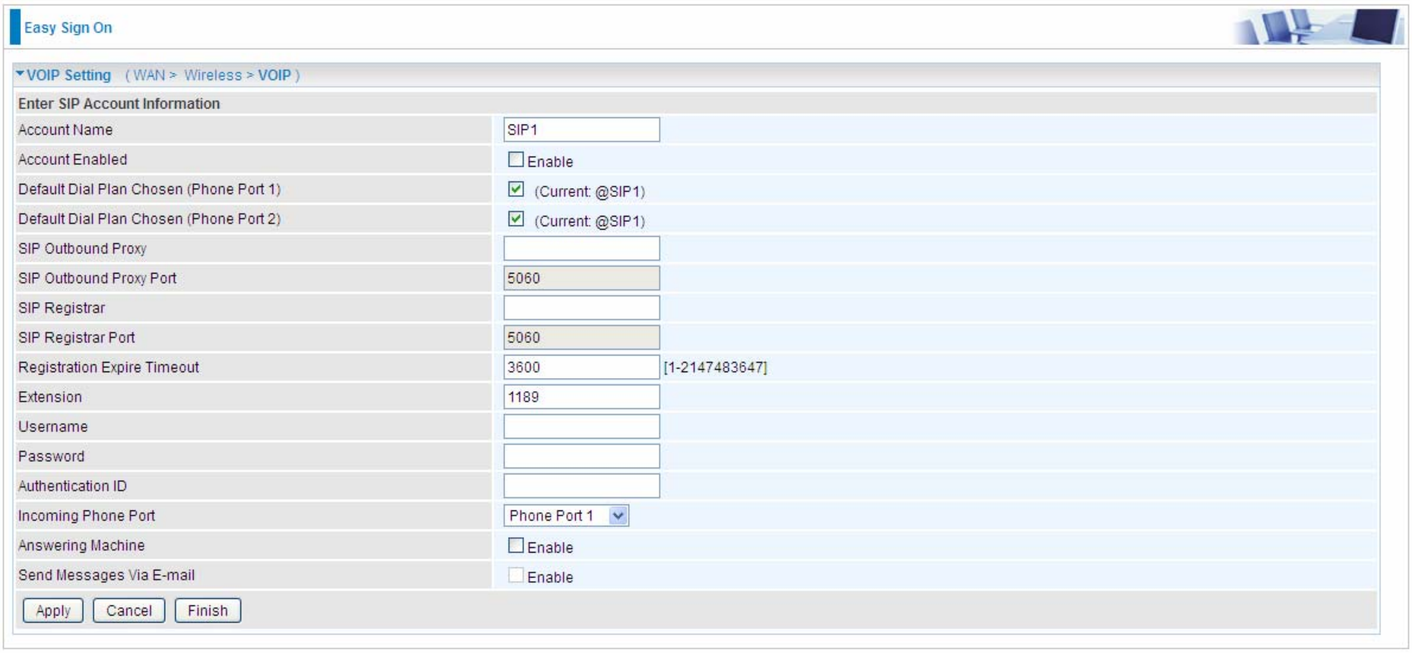
6. Continue to set 5GHz wireless.



▾Wireless (WAN > Wireless > VOIP)

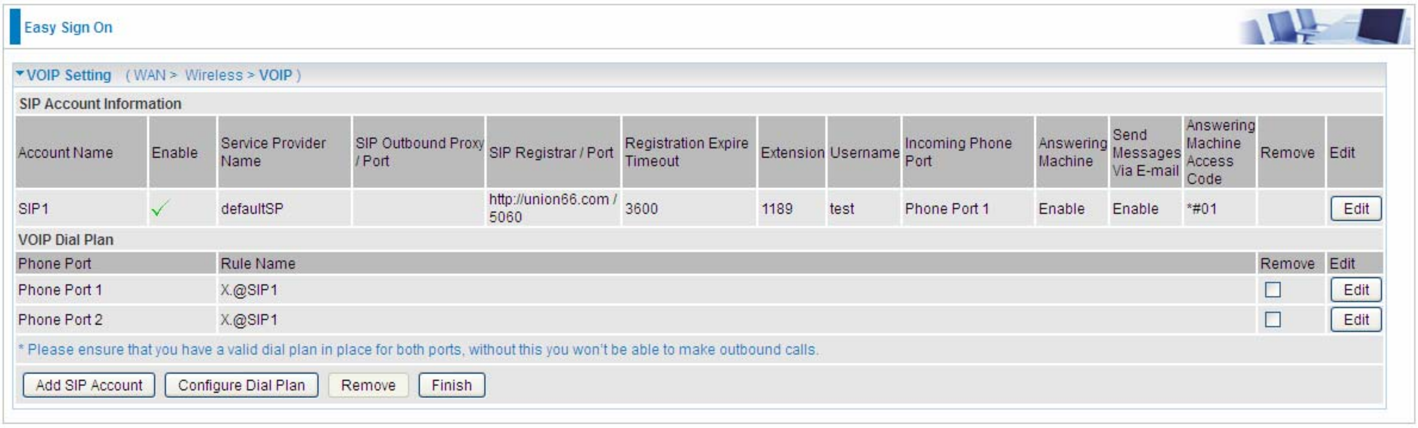
Parameters	
Band	5GHz (wl1)
Wireless	☑ Enable
SSID	wlan-ap-5g
WPA Pre-Shared Key	Click here to display

7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, write down the registration information and fill it in the following blanks. For detail, please refer to VoIP.



▾VOIP Setting (WAN > Wireless > VOIP)

Enter SIP Account Information	
Account Name	SIP1
Account Enabled	□ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @SIP1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @SIP1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	1189
Username	
Password	
Authentication ID	
Incoming Phone Port	Phone Port 1
Answering Machine	□ Enable
Send Messages Via E-mail	□ Enable


Easy Sign On

▾VOIP Setting (WAN > Wireless > VOIP)

SIP Account Information

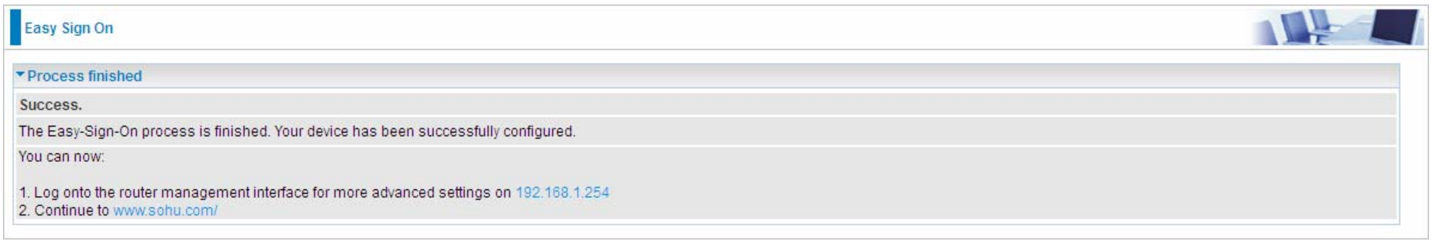
Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✓	defaultSP		http://union66.com / 5060	3600	1189	test	Phone Port 1	Enable	Enable	*#01		Edit

VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

8. In the above page, click finish to complete the EZSO settings.


Easy Sign On

▾Process finished

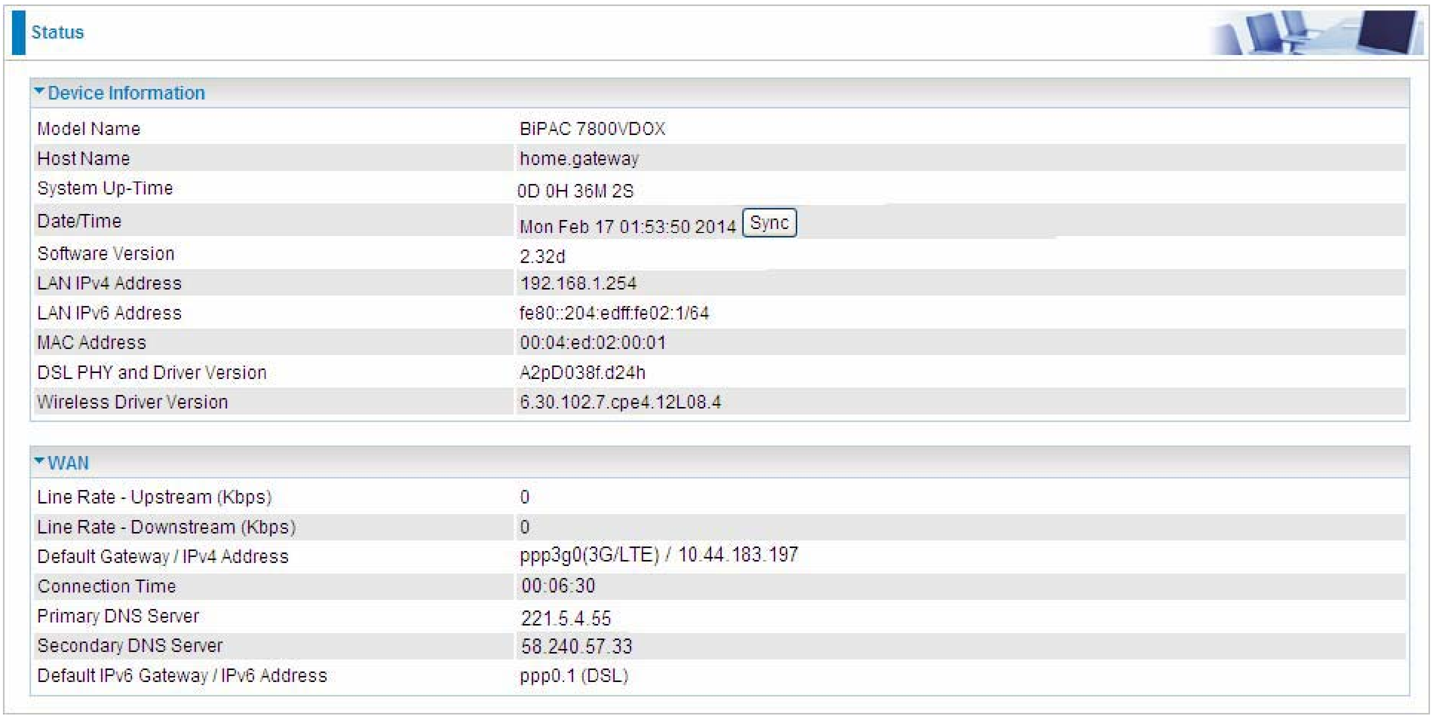
Success.

The Easy-Sign-On process is finished. Your device has been successfully configured.

You can now:

1. Log onto the router management interface for more advanced settings on 192.168.1.254
2. Continue to www.sohu.com/

Click ***192.168.1.254***, it will lead you to the following page.


Status

▾Device Information

Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 36M 2S
Date/Time	Mon Feb 17 01:53:50 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

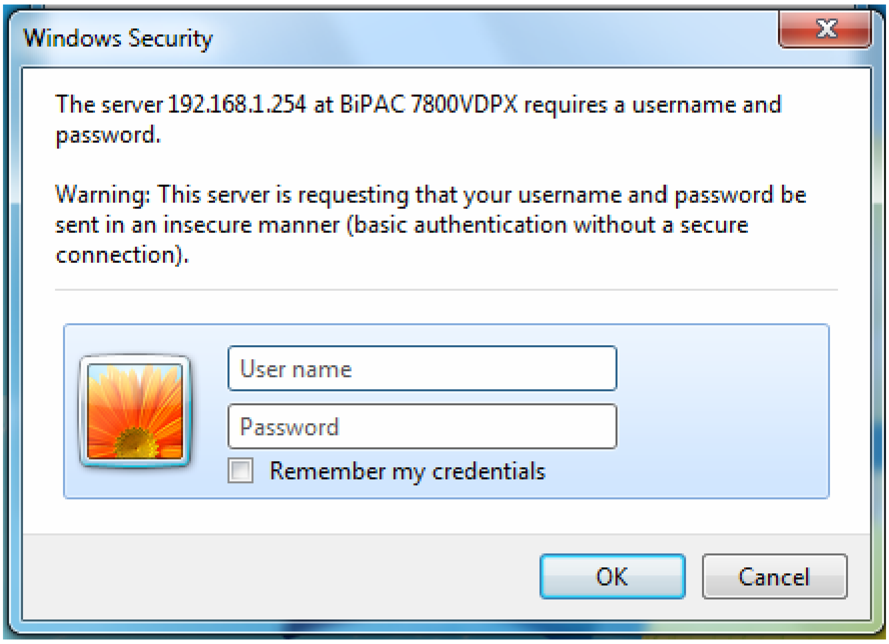
▾WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp3g0(3G/LTE) / 10.44.183.197
Connection Time	00:06:30
Primary DNS Server	221.5.4.55
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL)

Chapter 4: Configuration

Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.1.254, and click ➔ or press ‘Enter’ key on the keyboard, a login prompt window will appear. The default root username and password are “admin” and “admin” respectively.



Windows Security

The server 192.168.1.254 at BiPAC 7800VDPX 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).

Congratulations! You are now successfully logged in to the Firewall Router!

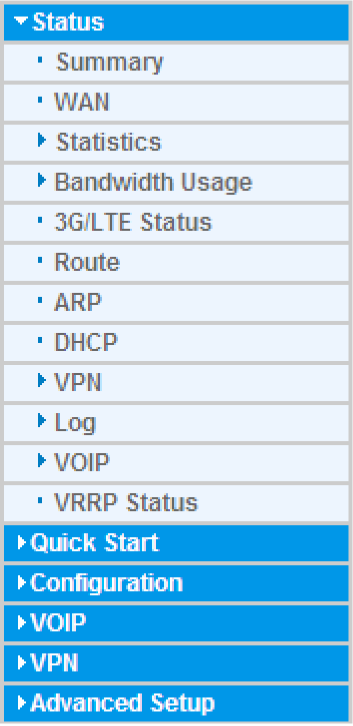
Once you have logged on to your BiPAC 7800VDP(O)X Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Status** (Summary, WAN, Statistics, Bandwidth Usage, 3G/LTE Status, Route, ARP, DHCP, VPN(7800VDOX only), Log, VOIP, VRRP Status)
- **Quick Start** (Quick Start, VOIP Quick Setup)
- **Configuration** (LAN, Wireless 2.4G(wl0), Wireless 5G(wl1), WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)
- **VoIP** (SIP Device, Service Provider, SIP Account, Call Forward, Call Through, Call Block, VoIP Dial Plan, PSTN Dial Plan, Phone Book)
- **VPN** (IPSec, VPN Account, Exceptional Rule Group, PPTP, L2TP, GRE)
- **Advanced Setup** (Routing, DNS, Static ARP, UPnP, Certificate, Multicast, Management, Diagnostics)

Note: VPN is only available for 7800VDOX.

Status

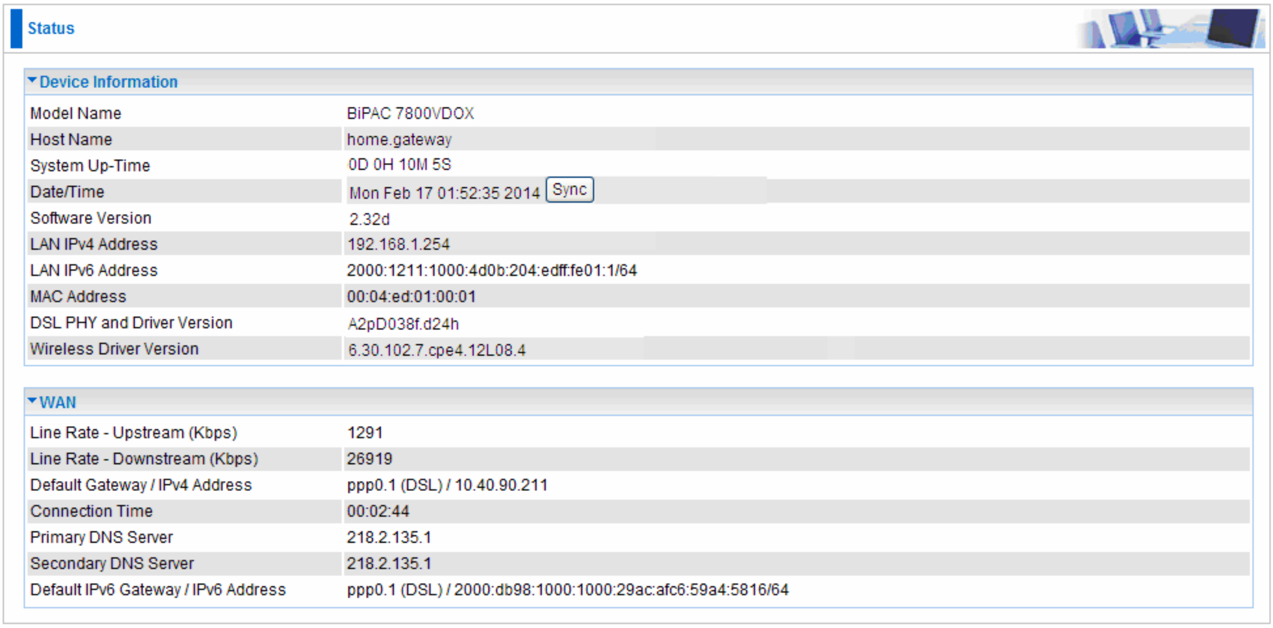
This Section gives users an easy access to the information about the working router and access to view the current status of the router. Here **Summary**, **WAN**, **Statistics**, **Bandwidth Usage**, **3G/LTE Status**, **Route**, **ARP**, **DHCP**, **VPN (7800VDOX only)**, **Log**, **VoIP** and **VRRP Status** subsections are included.



(7800VDOX)

Summary

The basic information about the device is provided here (the following is a configured screenshots to let users understand clearly).



Status

Device Information

Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 10M 5S
Date/Time	Mon Feb 17 01:52:35 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

Line Rate - Upstream (Kbps)	1291
Line Rate - Downstream (Kbps)	26919
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

Device Information

Model Name: Displays the model name.

Host Name: Displays the name of the router.

System Up-Time: Displays the elapsed time since the device is on.

Date/Time: Displays the current exact date and time. Sync button is to synchronize the Date/Time with your PC time without regard to connecting to internet or not.

Software Version: Firmware version.

LAN IPv4 Address: Displays the LAN IPv4 address.

LAN IPv6 Address: Displays the LAN IPv6 address. Default is a Link-Local address, but when connects to ISP, it will display the Global Address, like above figure.

MAC Address: Displays the MAC address.

DSL PHY and Driver Version: Display DSL PHY and Driver version.

Wireless Driver Version: Displays wireless driver version.

WAN

Line Rate – Upstream (Kbps): Display Upstream line Rate in Kbps.

Line Rate – Downstream (Kbps): Display Downstream line Rate in Kbps.

Default Gateway/IP4 Address: Display Default Gateway and the IPv4 address.

Connection Time: Display the elapsed time since ADSL connection is up.

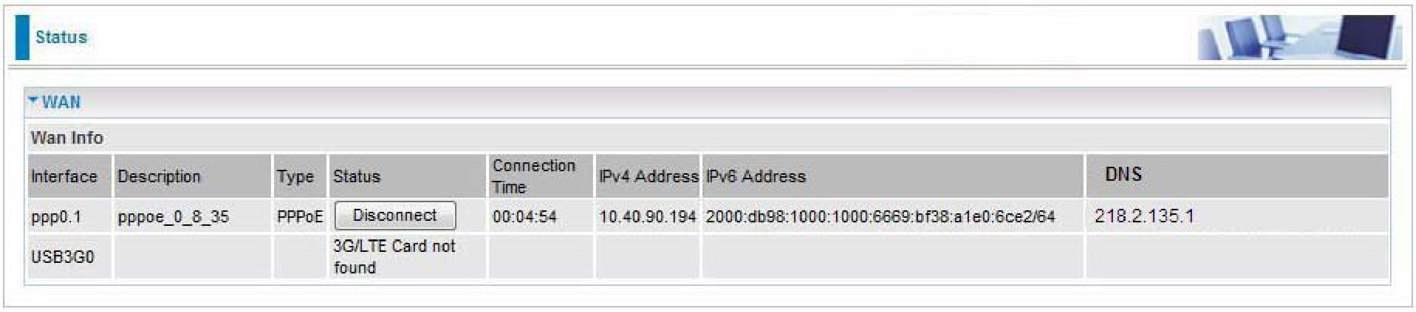
Primary DNS Server: Display IPV4 address of Primary DNS Server.

Secondary DNS Server: Display IPV4 address of Secondary DNS Server.

Default IPv6 Gateway/IPv6 Address: Display the IPv6 Gateway and the obtained IPv6 address.

WAN

This table displays the information of the WAN connections, users can turn here for WAN connection information.



Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64	218.2.135.1
USB3G0			3G/LTE Card not found				

Interface: The WAN connection interface.

Description: The description of this connection.

Type: The protocol used by this connection.

Status: To disconnect or connect the link.

Connection Time: The WAN connection time since WAN is up.

IPv4 Address: The WAN IPv4 Address the device obtained.

IPv6 Address: The WAN IPv6 Address the device obtained.

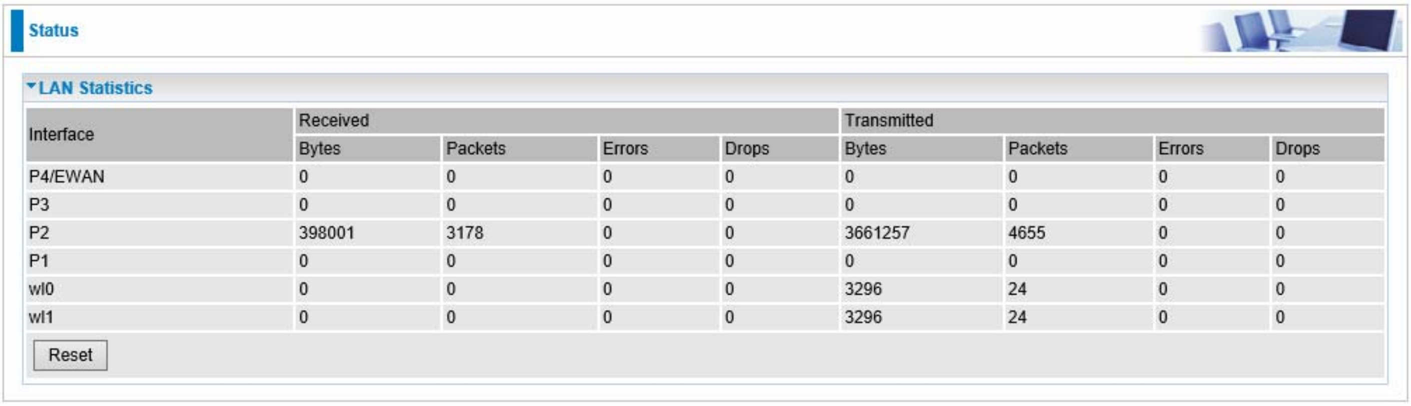
DNS: The DNS address the device obtained.

Statistics

LAN

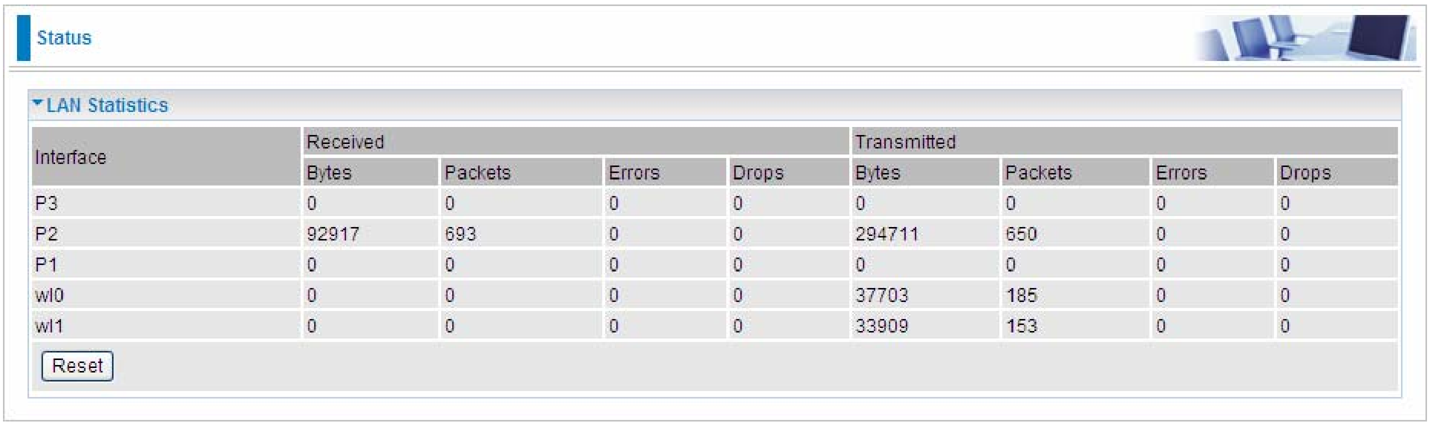
The table shows the statistics of LAN.

Note: P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.



Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P4/EWAN	0	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0	0
P2	398001	3178	0	0	3661257	4655	0	0
P1	0	0	0	0	0	0	0	0
wl0	0	0	0	0	3296	24	0	0
wl1	0	0	0	0	3296	24	0	0

(DSL)



Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P3	0	0	0	0	0	0	0	0
P2	92917	693	0	0	294711	650	0	0
P1	0	0	0	0	0	0	0	0
wl0	0	0	0	0	37703	185	0	0
wl1	0	0	0	0	33909	153	0	0

(EWAN)

Interface: List each LAN interface. P1-P4 indicates the four LAN interfaces.

Bytes: Display the Received and Transmitted traffic statistics in Bytes.

Packets: Display the Received and Transmitted traffic statistics in Packets.

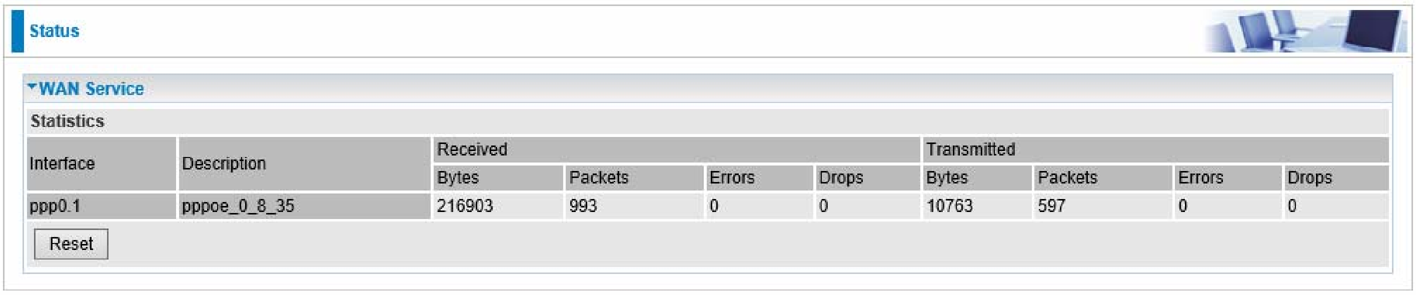
Errors: Display the statistics of errors arising in Receiving or Transmitting data.

Drops: Display the statistics of drops arising in Receiving or Transmitting data.

Reset: Press this button to refresh the statistics.

WAN Service

The table shows the statistics of WAN.



Status

▾WAN Service

Statistics

Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
ppp0.1	pppoe_0_8_35	216903	993	0	0	10763	597	0	0

Interface: Display the connection interface.

Description: the description for the connection.

Bytes: Display the WAN Received and Transmitted traffic statistics in Bytes.

Packets: Display the WAN Received and Transmitted traffic statistics in Packests.

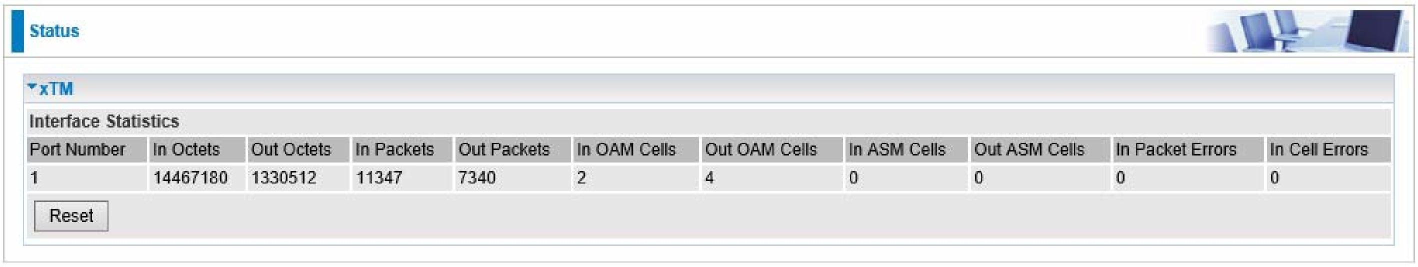
Errors: Display the statistics of errors arising in Receiving or Transmitting data.

Drops: Display the statistics of drops arising in Receiving or Transmitting data.

Reset: Press this button to refresh the statistics.

xTM

The Statistics-xTM screen displays all the xTM statistics



Status

▾xTM

Interface Statistics

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	14467180	1330512	11347	7340	2	4	0	0	0	0

Port Number: Shows number of the port for xTM.

In Octets: Number of received octets over the interface.

Out Octets: Number of transmitted octets over the interface.

In Packets: Number of received packets over the interface.

Out Packets: Number of transmitted packets over the interface.

In OAM Cells: Number of OAM cells received.

Out OAM Cells: Number of OAM cells transmitted.

In ASM Cells: Number of ASM cells received.

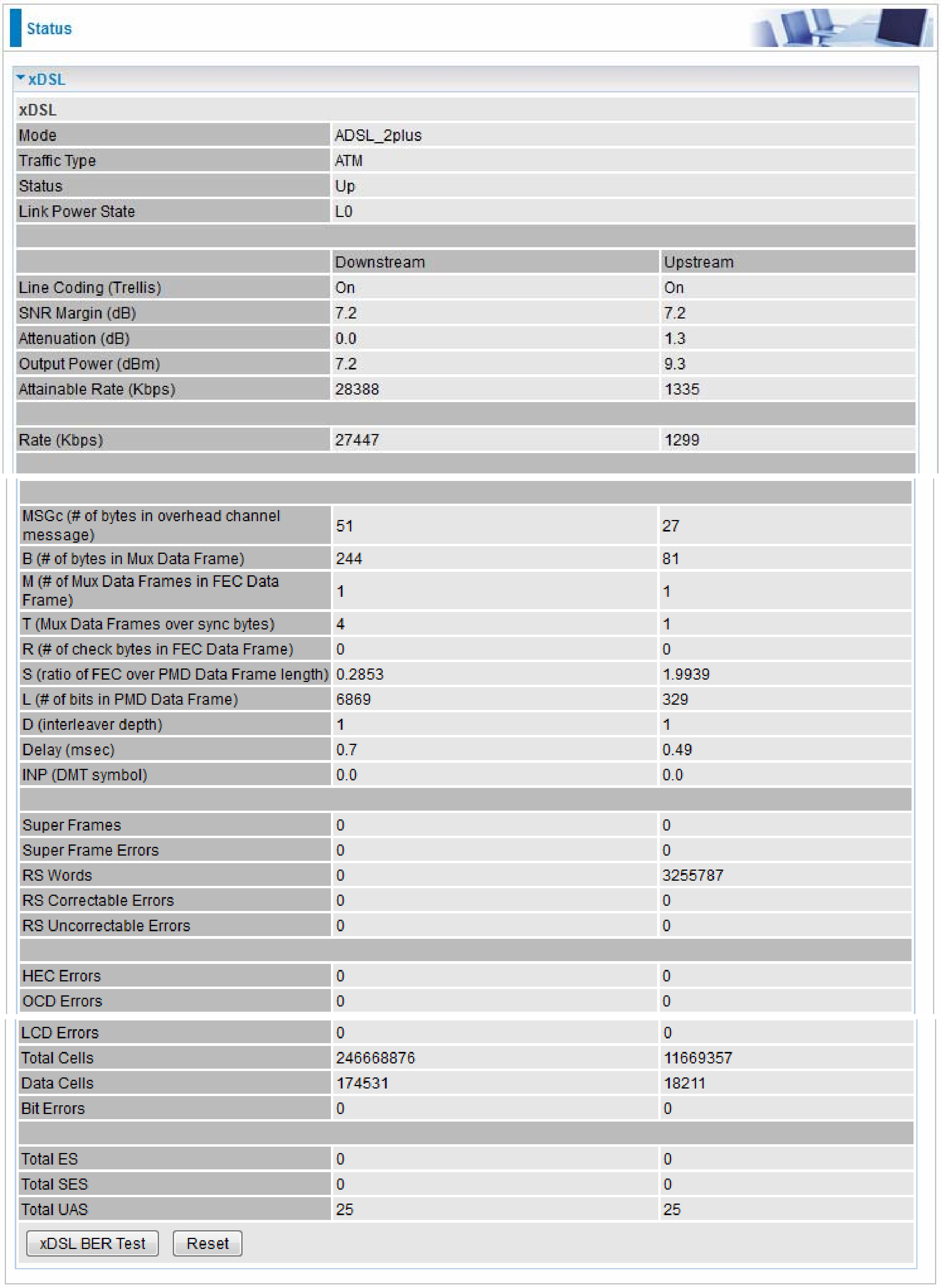
Out ASM Cells: Number of ASM cells transmitted.

In Packet Errors: Number of received packets with errors.

In Cell Errors: Number of received cells with errors.

Reset: Click to reset the statistics.

xDSL



xDSL		
Mode	ADSL_2plus	
Traffic Type	ATM	
Status	Up	
Link Power State	L0	
	Downstream	Upstream
Line Coding (Trellis)	On	On
SNR Margin (dB)	7.2	7.2
Attenuation (dB)	0.0	1.3
Output Power (dBm)	7.2	9.3
Attainable Rate (Kbps)	28388	1335
Rate (Kbps)	27447	1299
MSGc (# of bytes in overhead channel message)	51	27
B (# of bytes in Mux Data Frame)	244	81
M (# of Mux Data Frames in FEC Data Frame)	1	1
T (Mux Data Frames over sync bytes)	4	1
R (# of check bytes in FEC Data Frame)	0	0
S (ratio of FEC over PMD Data Frame length)	0.2853	1.9939
L (# of bits in PMD Data Frame)	6869	329
D (interleaver depth)	1	1
Delay (msec)	0.7	0.49
INP (DMT symbol)	0.0	0.0
Super Frames	0	0
Super Frame Errors	0	0
RS Words	0	3255787
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	0	0
OCD Errors	0	0
LCD Errors	0	0
Total Cells	246668876	11669357
Data Cells	174531	18211
Bit Errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	25	25

Mode: Modulation protocol, including G.dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+ and AnnexM.

Traffic Type: Transfer mode, here supports ATM and PTM.

Status: Show the status of DSL link.

Link Power State: Show link output power state.

Line Coding (Trellis): Trellis on/off.

SNR Margin (dB): Show the Signal to Noise Ratio(SNR) margin.

Attenuation (dB): This is estimate of average loop attenuation of signal.

Output Power (dBm): Show the output power.

Attainable Rate (Kbps): The sync rate you would obtain.

Rate (Kbps): Show the downstream and upstream rate in Kbps.

MSGc (#of bytes in overhead channel message): The number of bytes in overhead channel message.

B (# of bytes in Mux Data Frame): The number of bytes in Mux Data frame.

M (# of Mux Data Frames in FEC Data Frame): The number of Mux Data frames in FEC frame.

T (Mux Data Frames over sync bytes): The number of Mux Data frames over all the sync bytes.

R (# of check bytes in FEC Data Frame): The number of check bytes in FEC frame.

S (ratio of FEC over PMD Data Frame length): The ratio of FEC over PMD Data frame length

L (# of bits in PMD Data Frame): The number of bit in PMD Data frame

D (interleaver depth): Show the interleaver depth.

Delay (msec): Show the delay time in msec.

INP (DMT symbol): Show the DMT symbol.

Super Frames: The total number of super frames.

Super Frame Errors: the total number of super frame errors.

RS Words: Total number of Reed-Solomon code errors.

RS Correctable Errors: Total number of RS with correctable errors.

RS Uncorrectable Errors: Total number of RS words with uncorrectable errors.

HEC Errors: Total number of Header Error Checksum errors.

OCD Errors: Total number of out-of-cell Delineation errors.

LCD Errors: Total number of Loss of Cell Delineation.

Total Cells: Total number of cells.

Data Cells: Total number of data cells.

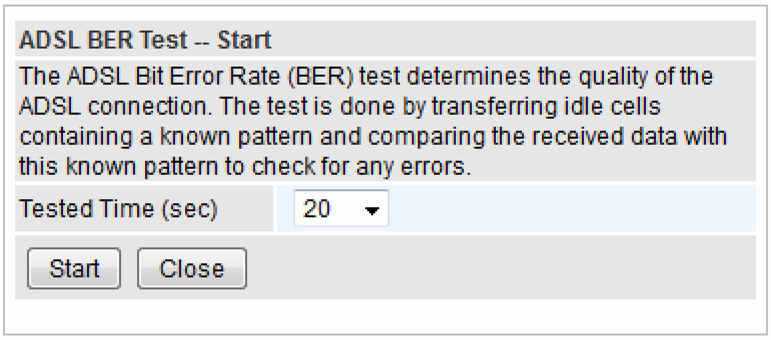
Bit Errors: Total number of bit errors.

Total ES: Total Number of Errored Seconds.

Total SES: Total Number of Severely Errored Seconds.

Total UAS: Total Number of Unavailable Seconds.

xDSL BER Test: Click this button to start a bit Error Rate Test. The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

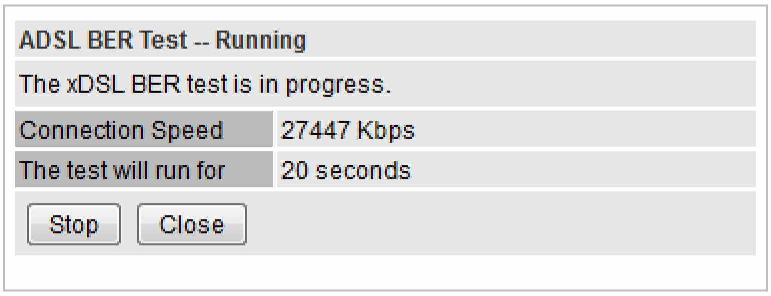


ADSL BER Test -- Start

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.

Tested Time (sec): 20

Select the Tested Time(sec), press **Start** to start test.

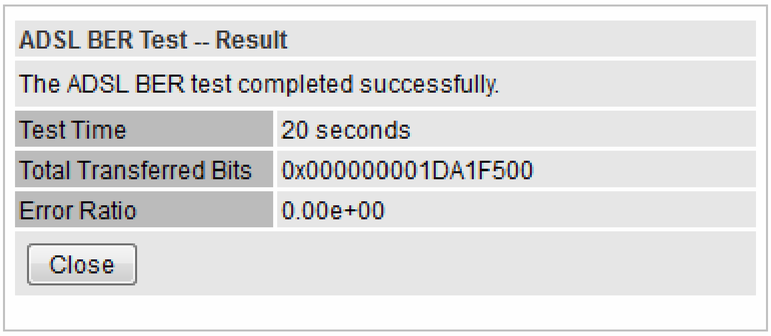


ADSL BER Test -- Running

The xDSL BER test is in progress.

Connection Speed	27447 Kbps
The test will run for	20 seconds

When it is OK, the following test result window will appear. You can view the quality of ADSL connection. Here the connection is OK.



ADSL BER Test -- Result

The ADSL BER test completed successfully.

Test Time	20 seconds
Total Transferred Bits	0x000000001DA1F500
Error Ratio	0.00e+00

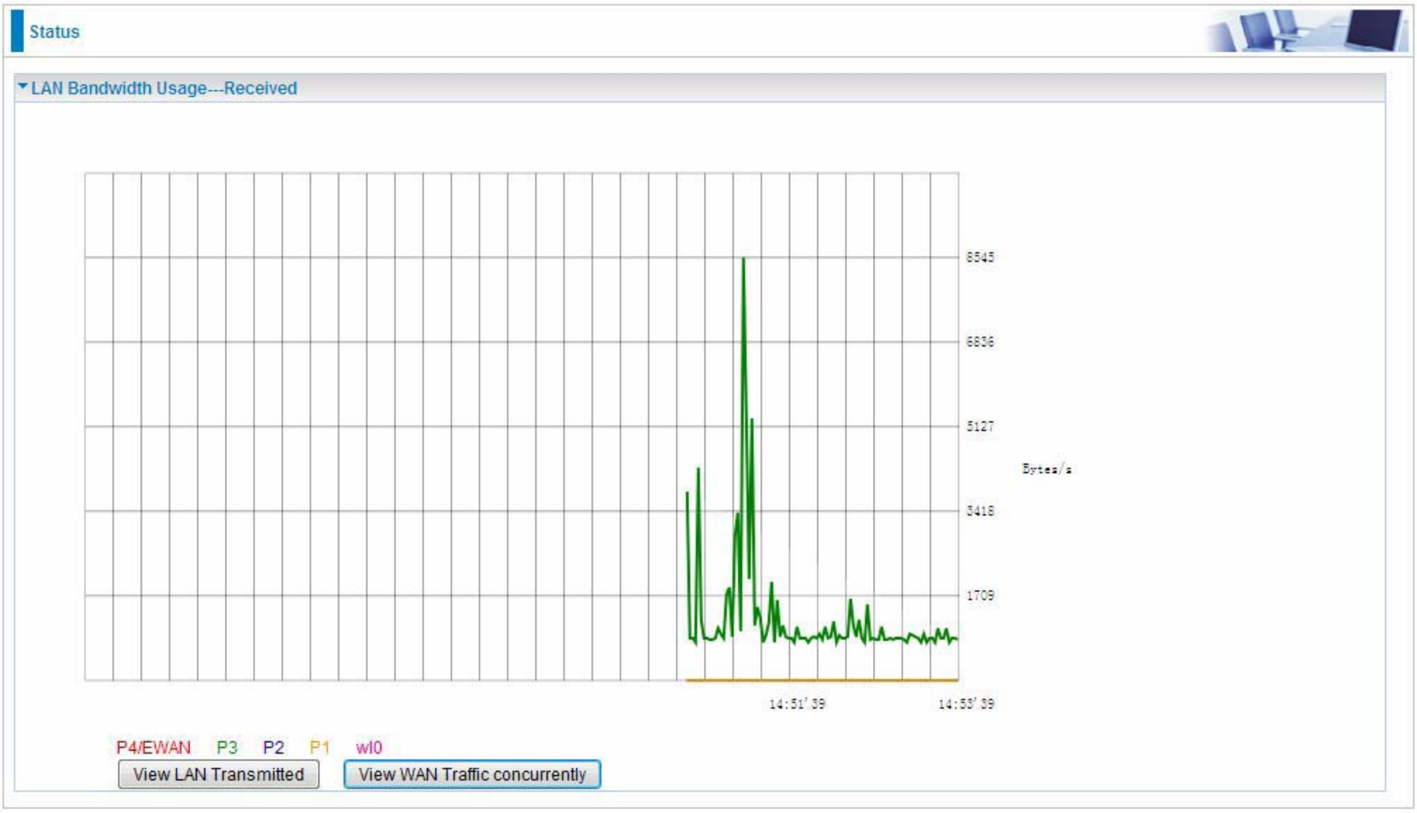
Reset: Click this button to reset the statistics.

Bandwidth Usage

Bandwidth Usage provides users direct view of bandwidth usage with simple diagram. Bandwidth usage shows the use of the bandwidth from two angles: Transmitted and Received, giving users a clear idea of the usage.

LAN

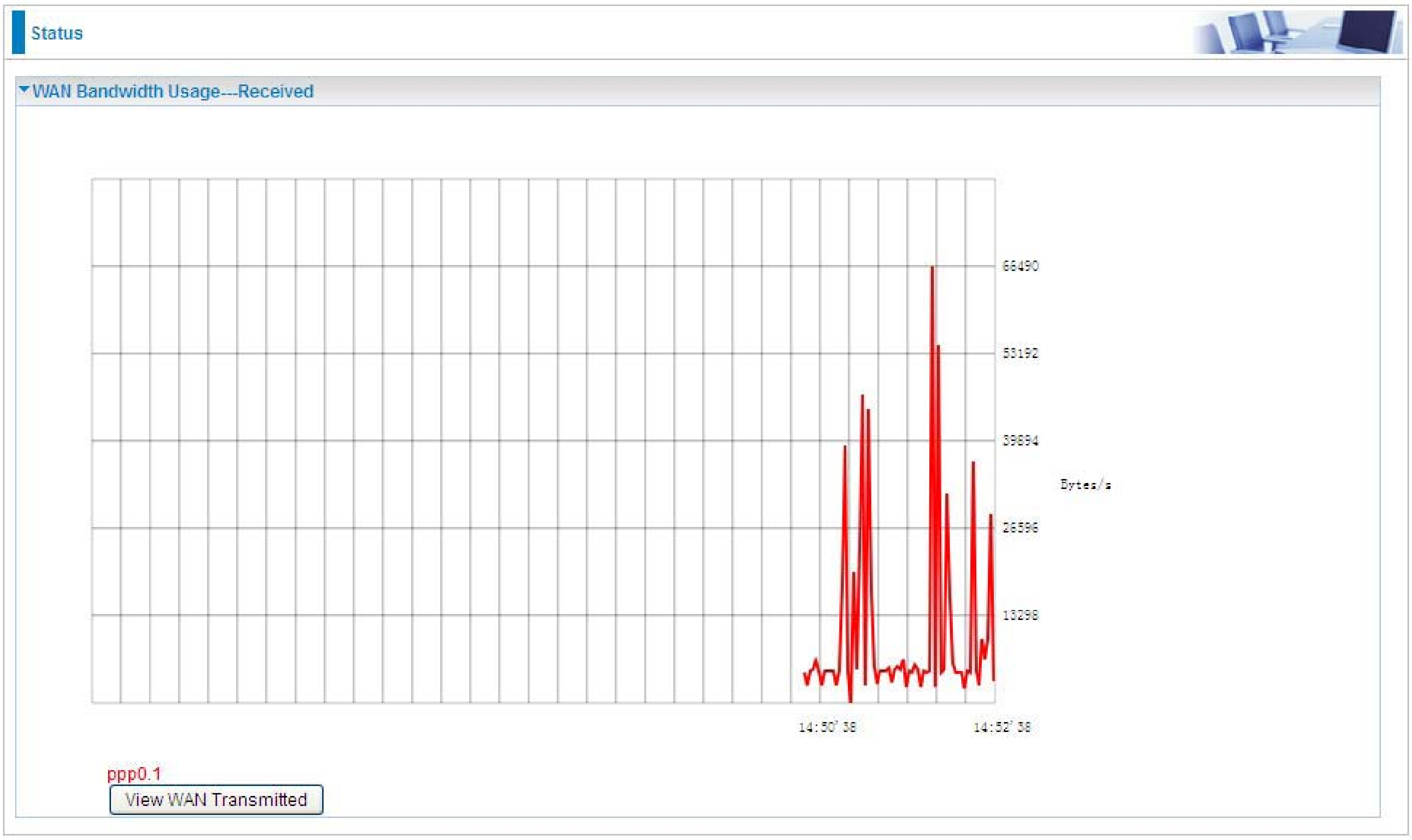
Note: P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.



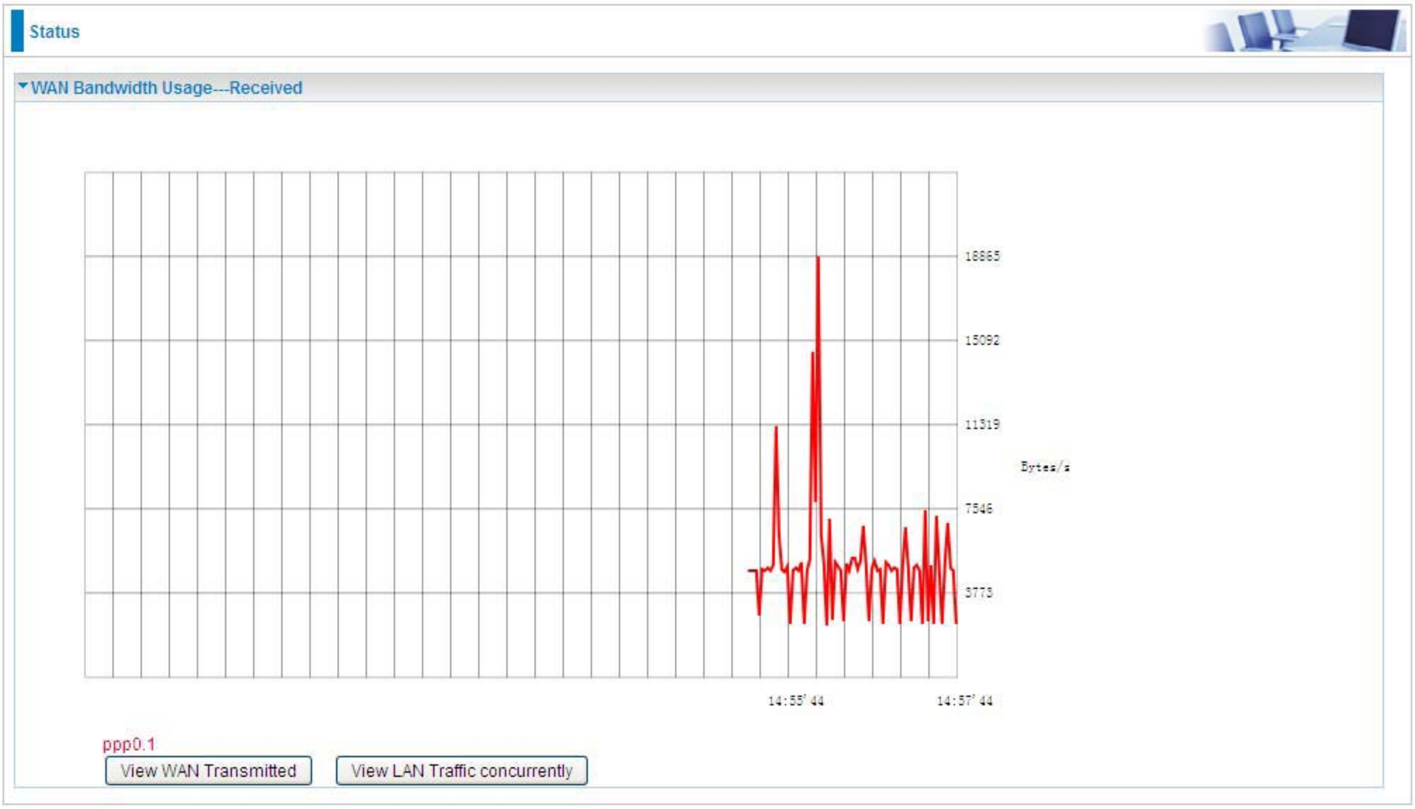
(DSL)

Press **View LAN Transmitted** button to change the diagram to the statistics from a Received Bytes of view. (**Note:** P3 means Ethernet port #3, and the traffic information of the port #3 is identified with green, the same color with P3 in the diagram; other ports all take the same mechanism.)

When you press **View WAN Traffic concurrently** button, the WAN Bandwidth Usage pops up so that users can view the WAN traffic concurrently.

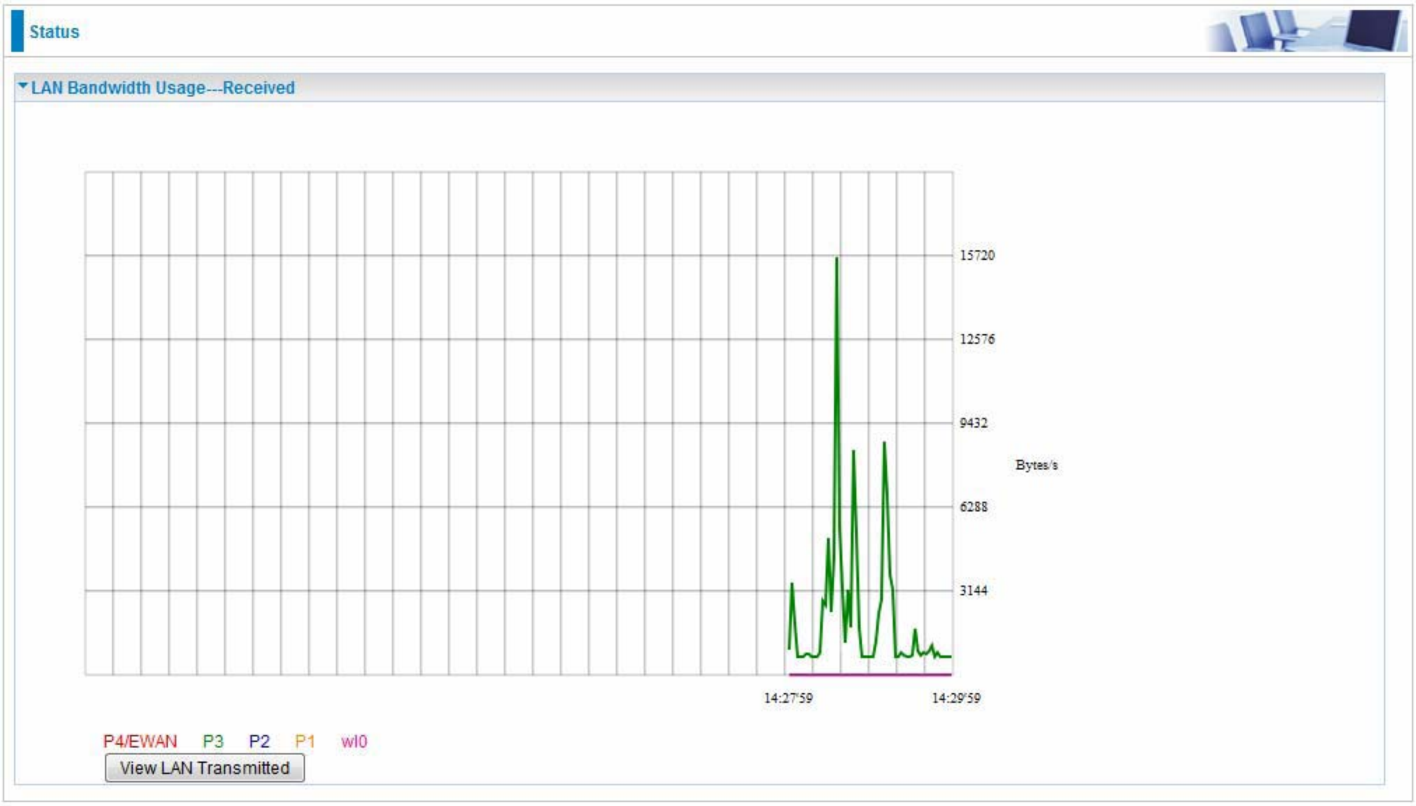


WAN Service

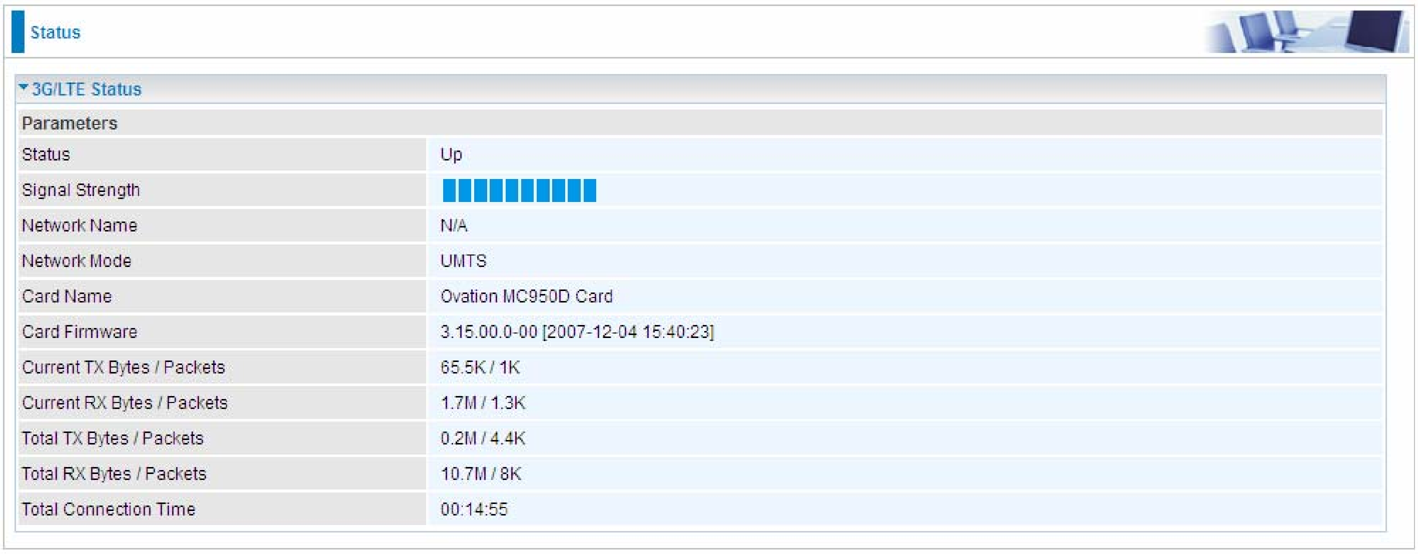


Press **View WAN Transmitted** button to change the diagram to the statistics from the Received Bytes' perspective.

Press **View LAN Traffic concurrently** button to directly switch to the LAN Bandwidth Usage page to view the LAN traffic concurrently.



3G/LTE Status



3G/LTE Status

Parameters	
Status	Up
Signal Strength	▮▮▮▮▮▮▮▮▮▮
Network Name	N/A
Network Mode	UMTS
Card Name	Ovation MC950D Card
Card Firmware	3.15.00.0-00 [2007-12-04 15:40:23]
Current TX Bytes / Packets	65.5K / 1K
Current RX Bytes / Packets	1.7M / 1.3K
Total TX Bytes / Packets	0.2M / 4.4K
Total RX Bytes / Packets	10.7M / 8K
Total Connection Time	00:14:55

Status: The current status of the 3G/LTE card.

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

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

Network Mode: The current operation mode for 3G/LTE card, it depends on service provider and card's limitation, GSM or UMTS.

Card Name: The name of the 3G/LTE card.

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

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

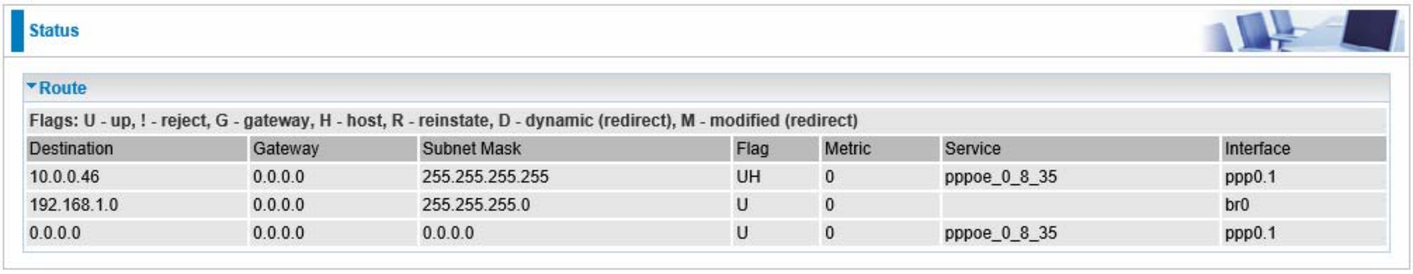
Current RX Bytes / Packets: The statistics of receive, count for this call.

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

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

Total Connection Time: The statistics of the connection time since system is ready.

Route



Status

▾Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect)

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.46	0.0.0.0	255.255.255.255	UH	0	pppoe_0_8_35	ppp0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_8_35	ppp0.1

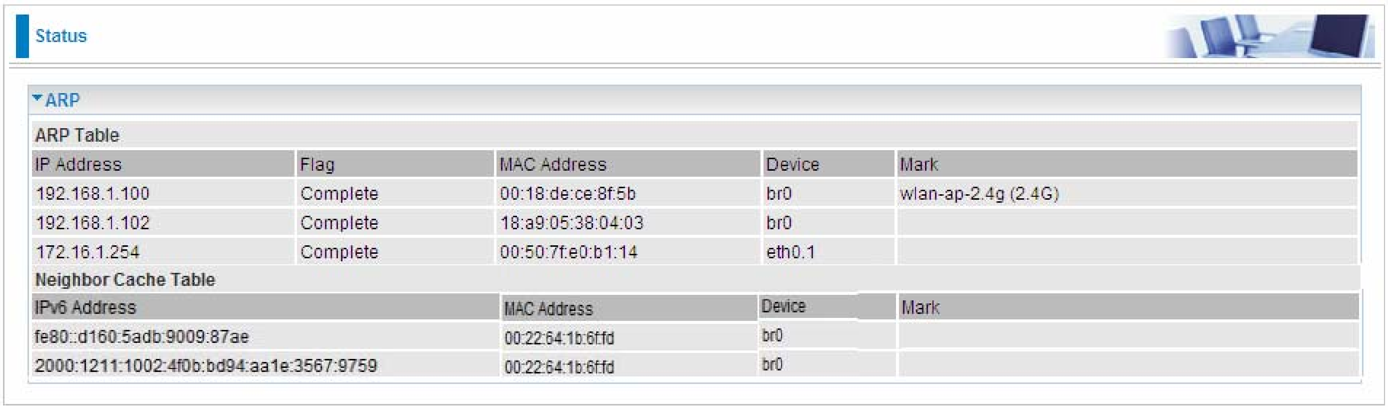
Destination: The IP address of destination network.
Gateway: The IP address of the gateway this route uses.
Subnet Mask: The destination subnet mask.
Flag: Show the status of the route.

- **U:** Show the route is activated or enabled.
- **H (host):** destination is host not the subnet.
- **G:** Show that the outside gateway is needed to forward packets in this route.
- **R:** Show that the route is reinstated from dynamic routing.
- **D:** Show that the route is dynamically installed by daemon or redirecting.
- **M:** Show the route is modified from routing daemon or redirect.

Metric: Display the number of hops counted as the Metric of the route.
Service: Display the service that this route uses.
Interface: Display the existing interface this route uses.

ARP

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's ***Security* – *MAC Filter*ing** function. Here IPv6 Neighbor Table, listed with IPv6 address-MAC mapping, is supported.



Status

▾ARP

ARP Table

IP Address	Flag	MAC Address	Device	Mark
192.168.1.100	Complete	00:18:de:ce:8f:5b	br0	wlan-ap-2.4g (2.4G)
192.168.1.102	Complete	18:a9:05:38:04:03	br0	
172.16.1.254	Complete	00:50:7f:e0:b1:14	eth0.1	

Neighbor Cache Table

IPv6 Address	MAC Address	Device	Mark
fe80::d160:5adb:9009:87ae	00:22:64:1b:6f:fd	br0	
2000:1211:1002:4f0b:bd94:aa1e:3567:9759	00:22:64:1b:6f:fd	br0	

ARP table

IP Address: Shows the IP Address of the device that the MAC address maps to.

Flag: Shows the current status of the ARP entries.

- Complete: the route resolving is processing well.
- M(Marked as permanent entry): the route is permanent.
- P (publish entry): publish this route item.

MAC Address: Shows the MAC address that is corresponded to the IP address of the device it is mapped to.

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays "br0".

Mark: Show clearly the SSID (WLAN) the device is in.

IPv6 Address

IPv6 address: Shows the IPv6 Address of the device that the MAC address maps to.

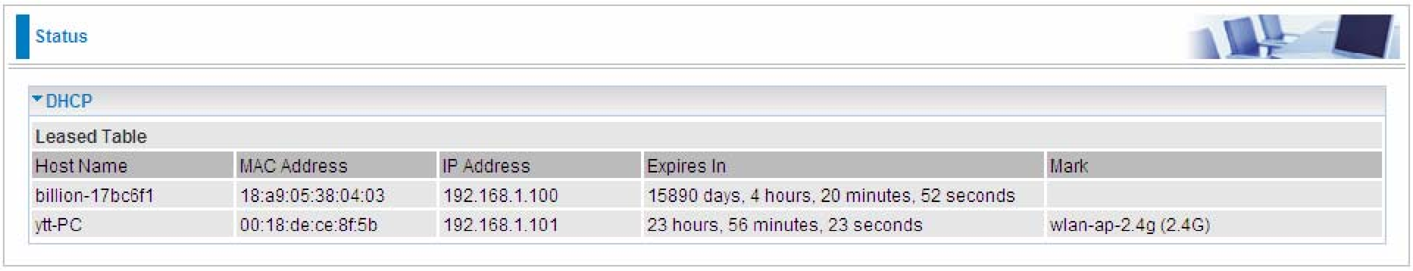
MAC Address: Shows the MAC address that is corresponded to the IPv6 address of the device it is mapped to.

Device: here refers to the physical interface, it is a concept to identify Clients from LAN or WAN. For example, the Clients in LAN, here displays "br0".

Mark: Show clearly the SSID (WLAN) the device is in.

DHCP

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



Leased Table

Host Name	MAC Address	IP Address	Expires In	Mark
billion-17bc6f1	18:a9:05:38:04:03	192.168.1.100	15890 days, 4 hours, 20 minutes, 52 seconds	
ytt-PC	00:18:de:ce:8f:5b	192.168.1.101	23 hours, 56 minutes, 23 seconds	wlan-ap-2.4g (2.4G)

Host Name: The Host Name of DHCP client.

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

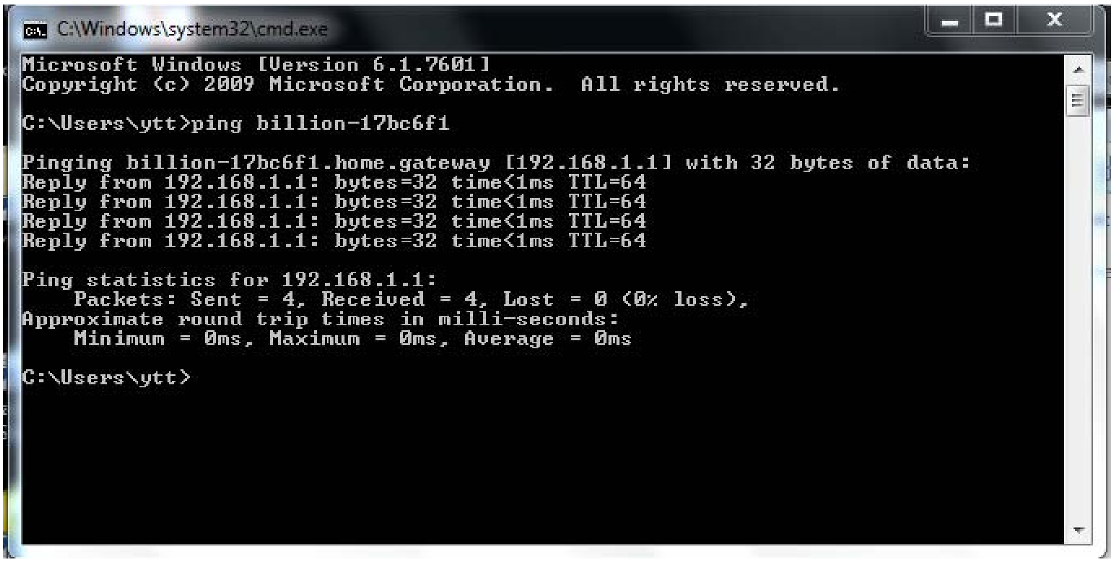
IP Address: The IP address which is assigned to the host with this MAC address.

Expires in: Show the remaining time after registration.

Mark: Show clearly the SSID (WLAN) the device is in.

Note: The devices are free to access each other through device name on condition that they all obtain their IPs from the DHCP. If the device IP is obtained from the DHCP, other devices can access the device through the device name.

For example, the PC ytt-PC can ping the billion-17bc6f1 using the host name instead of its IP.

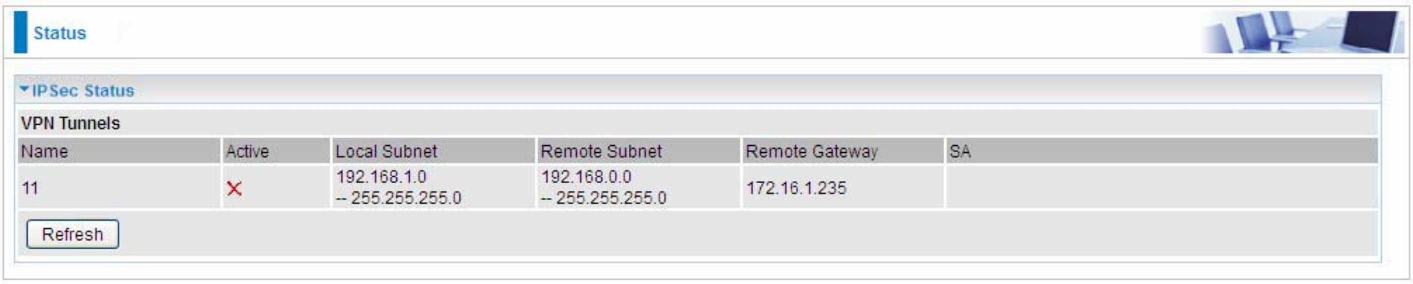


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\ytt>ping billion-17bc6f1

Pinging billion-17bc6f1.home.gateway [192.168.1.1] with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\ytt>
```

VPN (7800VDOX only)

VPN status viewing section provides users IPSec, PPTP, L2TP and GRE VPN status.

IPSec



▾IPSec Status

VPN Tunnels

Name	Active	Local Subnet	Remote Subnet	Remote Gateway	SA
11	✕	192.168.1.0 -- 255.255.255.0	192.168.0.0 -- 255.255.255.0	172.16.1.235	

Name: The IPSec connection name.

Active: Display the connection status.

Local Subnet: Display the local network.

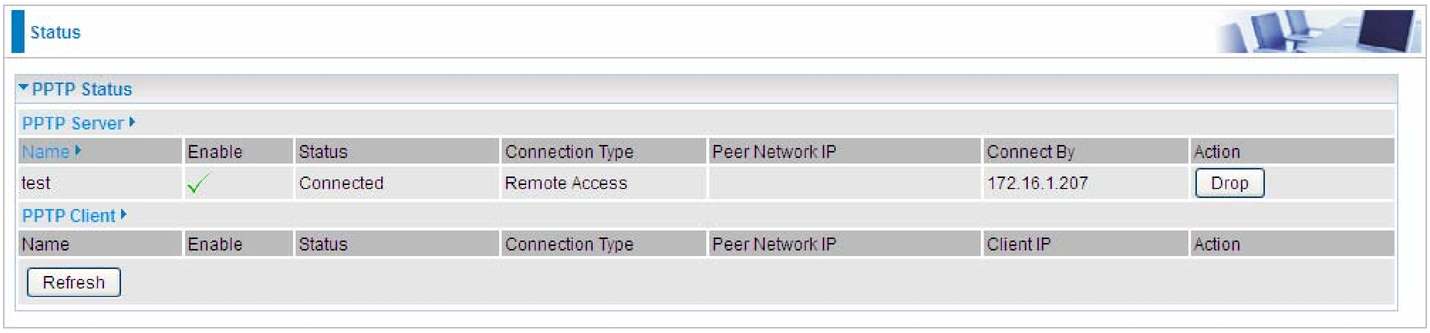
Remote Subnet: Display the remote network.

Remote Gateway: The remote gateway address.

SA: The Security Association for this IPSec entry.

Refresh: Click this button to refresh the tunnel status.

PPTP



PPTP Status

PPTP Server

Name	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test	✓	Connected	Remote Access		172.16.1.207	Drop

PPTP Client

Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action

PPTP Server

Name: The PPTP connection name.

Enable: Display the connection status with icons.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the remote network and subnet mask in LAN to LAN PPTP connection.

Connected By: Display the IP of remote connected client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

PPTP Client

Name: The PPTP connection name.

Enable: Display the connection status with icons.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

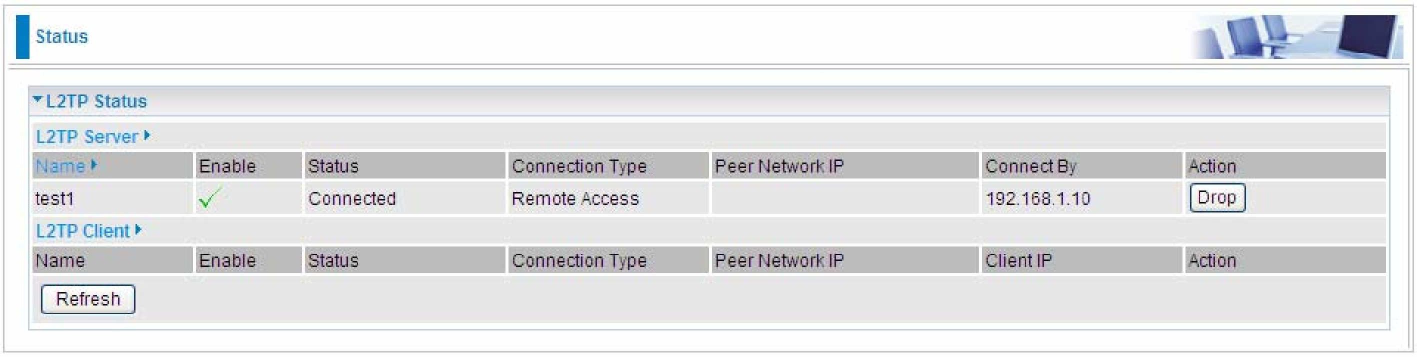
Peer Network IP: Display the remote network and subnet mask in LAN to LAN PPTP connection.

Client: Assigned IP by PPTP server.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

Refresh: Click this button to refresh the connection status.

L2TP



Status

▾L2TP Status

L2TP Server ▸

Name ▸	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test1	✓	Connected	Remote Access		192.168.1.10	Drop

L2TP Client ▸

Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action

Refresh

L2TP Server

Name: The L2TP connection name.

Enable: Display the connection status with icons.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the remote network and subnet mask in LAN to LAN L2TP connection.

Connected By: Display the IP of remote connected client.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

L2TP Client

Name: The L2TP connection name.

Enable: Display the connection status with icons.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

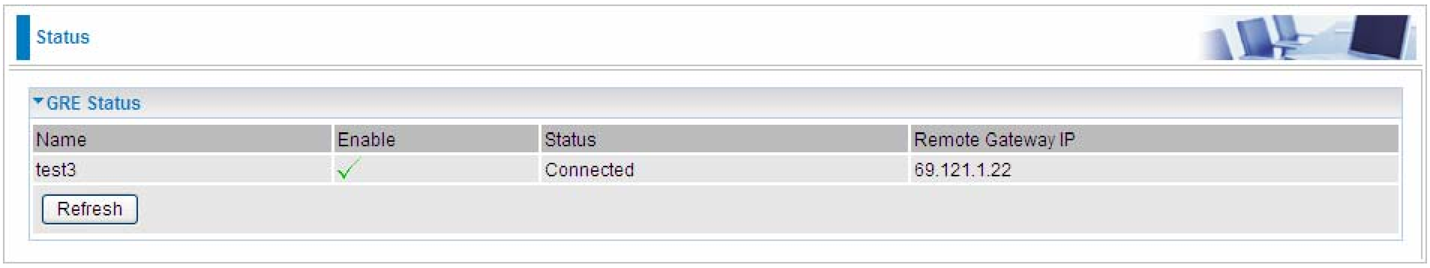
Peer Network IP: Display the remote network and subnet mask in LAN to LAN L2TP connection.

Client: Assigned IP by L2TP server.

Action: Act to the connection. Click Drop button to disconnect the tunnel connection.

Refresh: Click this button to refresh the connection status.

GRE



GRE Status

Name	Enable	Status	Remote Gateway IP
test3	✓	Connected	69.121.1.22

Name: The GRE connection name.

Enable: Display the connection status with icons.

Status: The connection status, connected or disable.

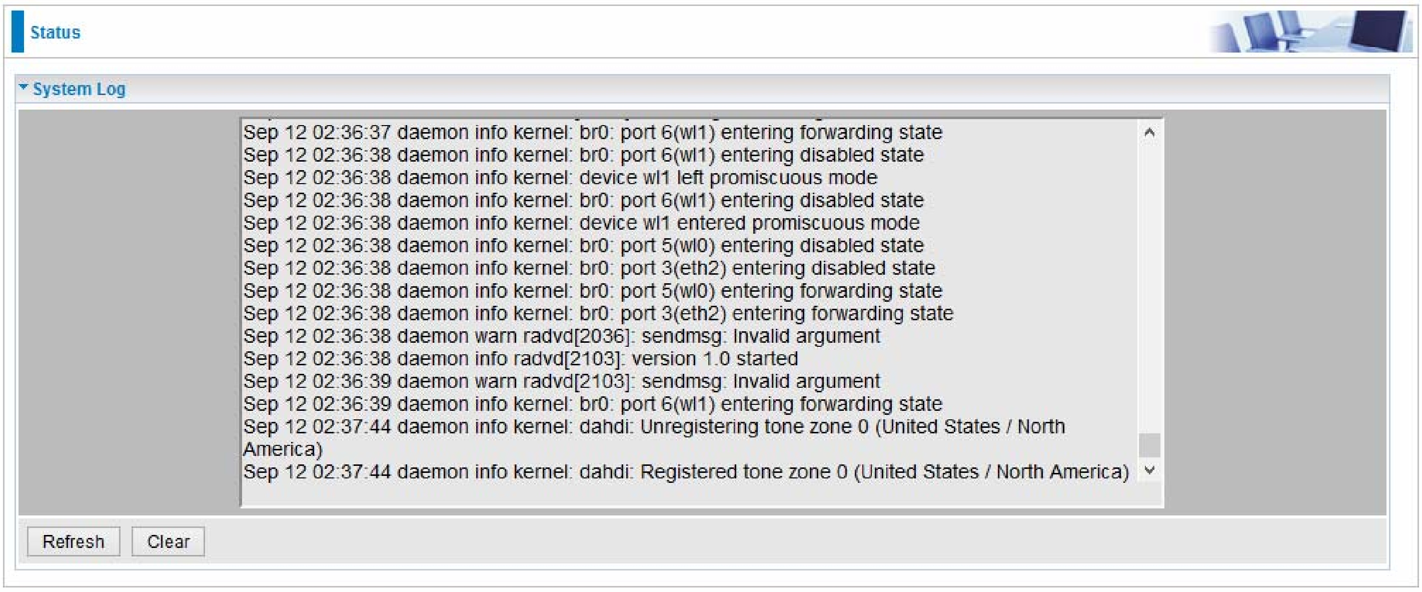
Remote Gateway: The IP of remote gateway.

Refresh: Click this button to refresh the connection status.

Log

System Log

Display system logs accumulated up to the present time. You can trace historical information with this function. And the log policy can be configured in Configure Log section.

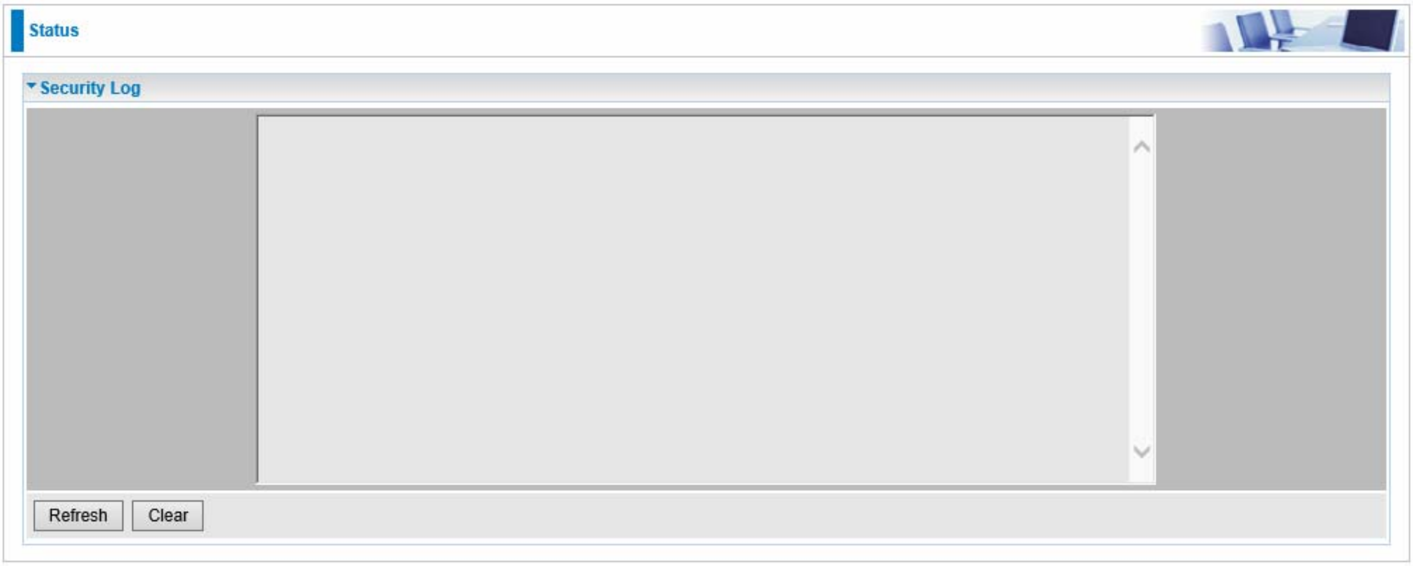


```
Sep 12 02:36:37 daemon info kernel: br0: port 6(wl1) entering forwarding state
Sep 12 02:36:38 daemon info kernel: br0: port 6(wl1) entering disabled state
Sep 12 02:36:38 daemon info kernel: device wl1 left promiscuous mode
Sep 12 02:36:38 daemon info kernel: br0: port 6(wl1) entering disabled state
Sep 12 02:36:38 daemon info kernel: device wl1 entered promiscuous mode
Sep 12 02:36:38 daemon info kernel: br0: port 5(wl0) entering disabled state
Sep 12 02:36:38 daemon info kernel: br0: port 3(eth2) entering disabled state
Sep 12 02:36:38 daemon info kernel: br0: port 5(wl0) entering forwarding state
Sep 12 02:36:38 daemon info kernel: br0: port 3(eth2) entering forwarding state
Sep 12 02:36:38 daemon warn radvd[2036]: sendmsg: Invalid argument
Sep 12 02:36:38 daemon info radvd[2103]: version 1.0 started
Sep 12 02:36:39 daemon warn radvd[2103]: sendmsg: Invalid argument
Sep 12 02:36:39 daemon info kernel: br0: port 6(wl1) entering forwarding state
Sep 12 02:37:44 daemon info kernel: dahdi: Unregistering tone zone 0 (United States / North
America)
Sep 12 02:37:44 daemon info kernel: dahdi: Registered tone zone 0 (United States / North America)
```

Refresh: Click to update the system log.
Clear: Click to clear the current log from the screen.

Security Log

Security log displays the message logged about security, like filter messages and some firewall message. You can turn to IP Filtering Outgoing, IP Filtering Incoming, URL Filter to determine if you want to log this information. Also you can turn to Configure Log section below to determine the level to log the message. You can use this to track potential threats to your system and network.



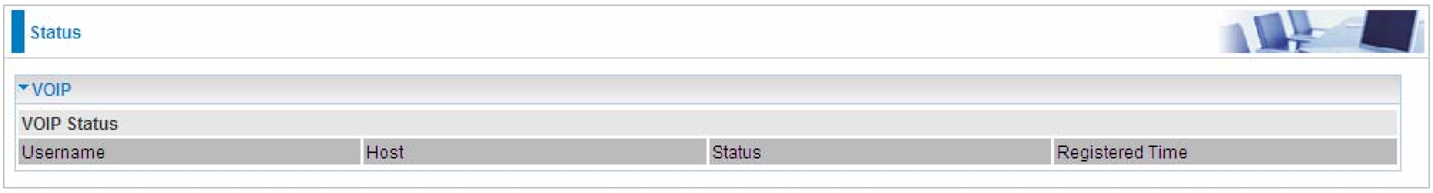
Refresh: Click to update the system log.

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

VoIP

Status

This VoIP status table displays the status of the VoIP phone usage, including **Username** - the username registered in SIP Account, **Host**- the SIP registrar address, **Status** – the process in use, **Registered Time** – the lasting period since the VoIP is up.



Status

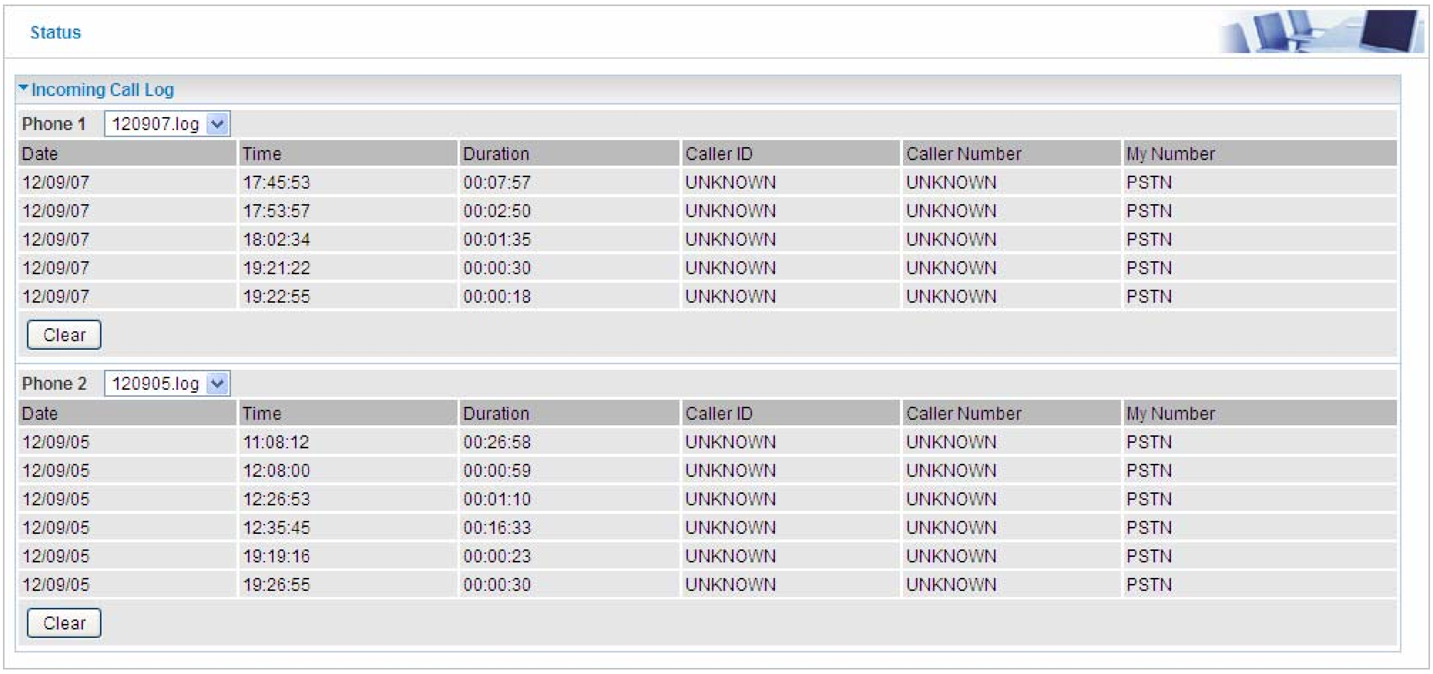
▾VOIP

VOIP Status

Username	Host	Status	Registered Time

Incoming Call Log

Incoming call log monitors incoming calls. It records all incoming call information ranging from ***Date***, ***Time***, ***Duration***, ***Caller ID***, ***Caller Number*** & ***My Number***.



Phone 1 120907.log

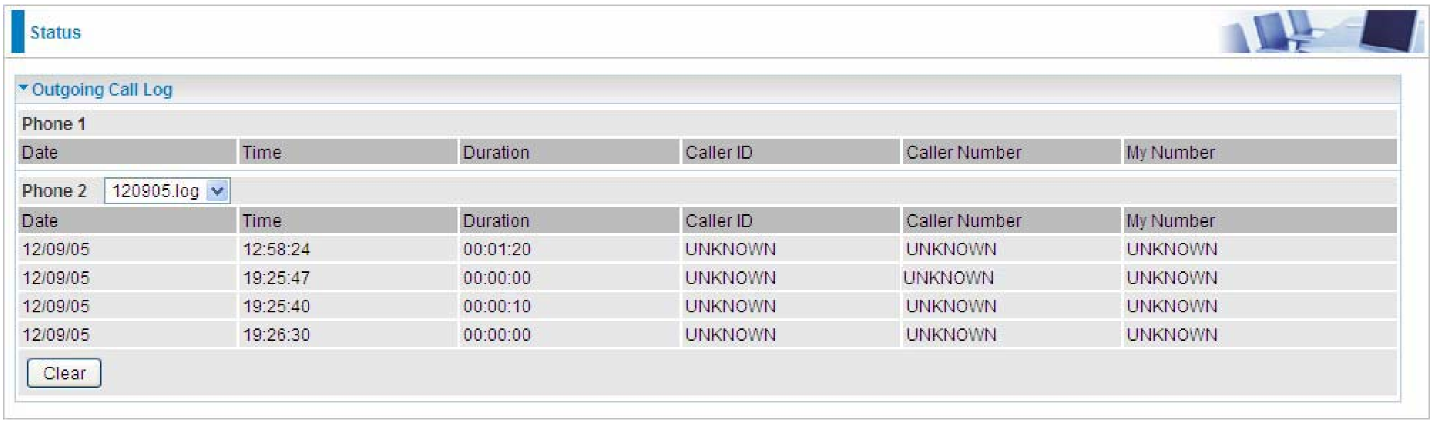
Date	Time	Duration	Caller ID	Caller Number	My Number
12/09/07	17:45:53	00:07:57	UNKNOWN	UNKNOWN	PSTN
12/09/07	17:53:57	00:02:50	UNKNOWN	UNKNOWN	PSTN
12/09/07	18:02:34	00:01:35	UNKNOWN	UNKNOWN	PSTN
12/09/07	19:21:22	00:00:30	UNKNOWN	UNKNOWN	PSTN
12/09/07	19:22:55	00:00:18	UNKNOWN	UNKNOWN	PSTN

Phone 2 120905.log

Date	Time	Duration	Caller ID	Caller Number	My Number
12/09/05	11:08:12	00:26:58	UNKNOWN	UNKNOWN	PSTN
12/09/05	12:08:00	00:00:59	UNKNOWN	UNKNOWN	PSTN
12/09/05	12:26:53	00:01:10	UNKNOWN	UNKNOWN	PSTN
12/09/05	12:35:45	00:16:33	UNKNOWN	UNKNOWN	PSTN
12/09/05	19:19:16	00:00:23	UNKNOWN	UNKNOWN	PSTN
12/09/05	19:26:55	00:00:30	UNKNOWN	UNKNOWN	PSTN

Outgoing Call Log

Outgoing call log monitors outgoing calls. It records all outgoing call information ranging from ***Date***, ***Time***, ***Duration***, ***Caller ID***, ***Caller Number*** & ***My Number***.



Phone 1

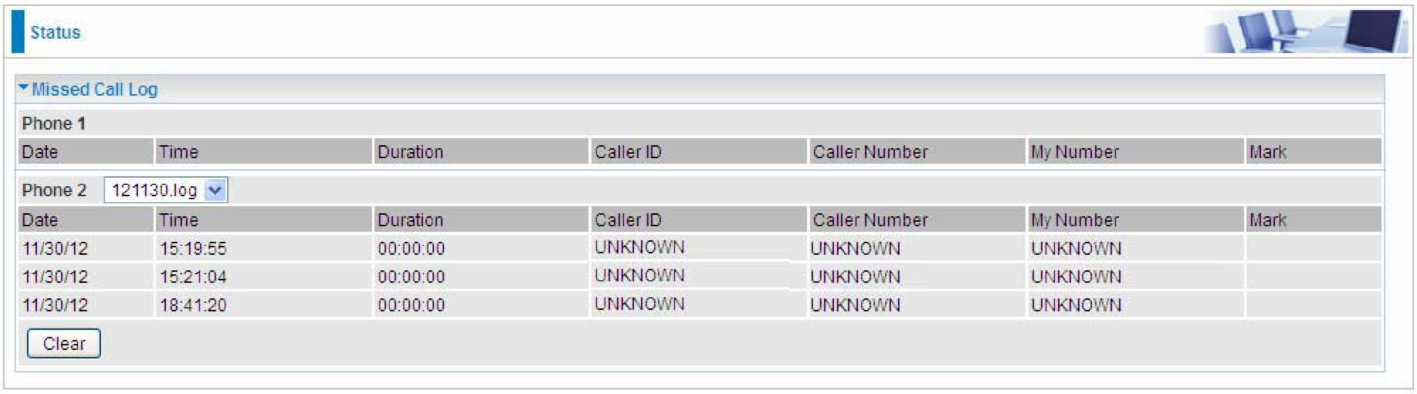
Date	Time	Duration	Caller ID	Caller Number	My Number

Phone 2 120905.log

Date	Time	Duration	Caller ID	Caller Number	My Number
12/09/05	12:58:24	00:01:20	UNKNOWN	UNKNOWN	UNKNOWN
12/09/05	19:25:47	00:00:00	UNKNOWN	UNKNOWN	UNKNOWN
12/09/05	19:25:40	00:00:10	UNKNOWN	UNKNOWN	UNKNOWN
12/09/05	19:26:30	00:00:00	UNKNOWN	UNKNOWN	UNKNOWN

Missed Call Log

Missed call log monitors missed calls. It records all missed call information ranging from ***Date***, ***Time***, ***Duration***, ***CallerID***, ***Caller Number***, ***My Number*** *and* ***Mark*** - the reason why the call is not answered, with possible value reading DND, CF, CB or empty.



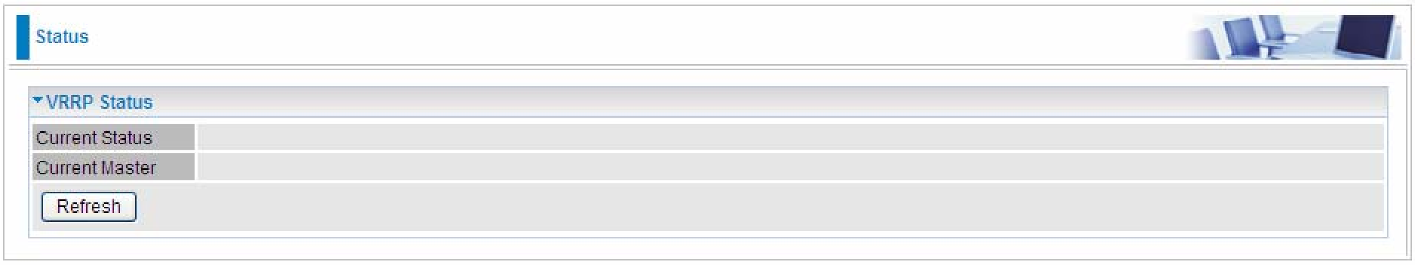
Phone 1

Date	Time	Duration	Caller ID	Caller Number	My Number	Mark

Phone 2 121130.log

Date	Time	Duration	Caller ID	Caller Number	My Number	Mark
11/30/12	15:19:55	00:00:00	UNKNOWN	UNKNOWN	UNKNOWN	
11/30/12	15:21:04	00:00:00	UNKNOWN	UNKNOWN	UNKNOWN	
11/30/12	18:41:20	00:00:00	UNKNOWN	UNKNOWN	UNKNOWN	

VRRP Status



Current Status: Show VRRP current status, Master or Backup.

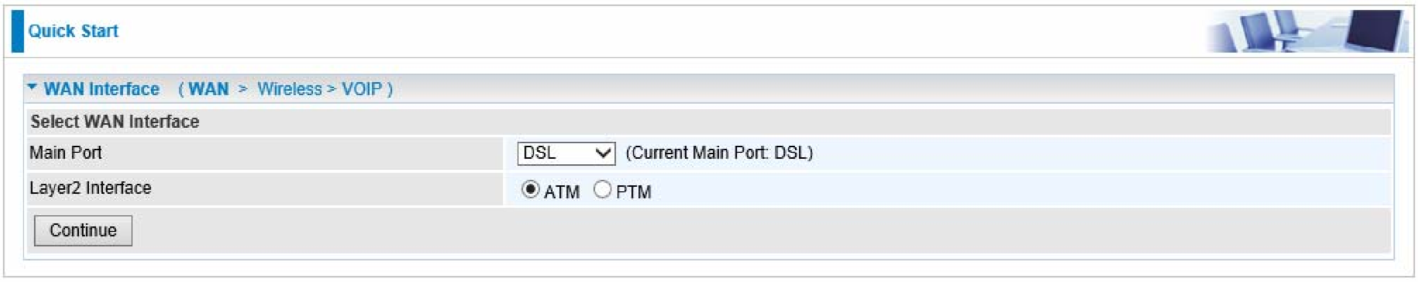
Current Master: Show the IP address of current master.

Quick Start

Quick Start

This part allows you to quickly configure and connect your router to internet.

DSL mode



Quick Start

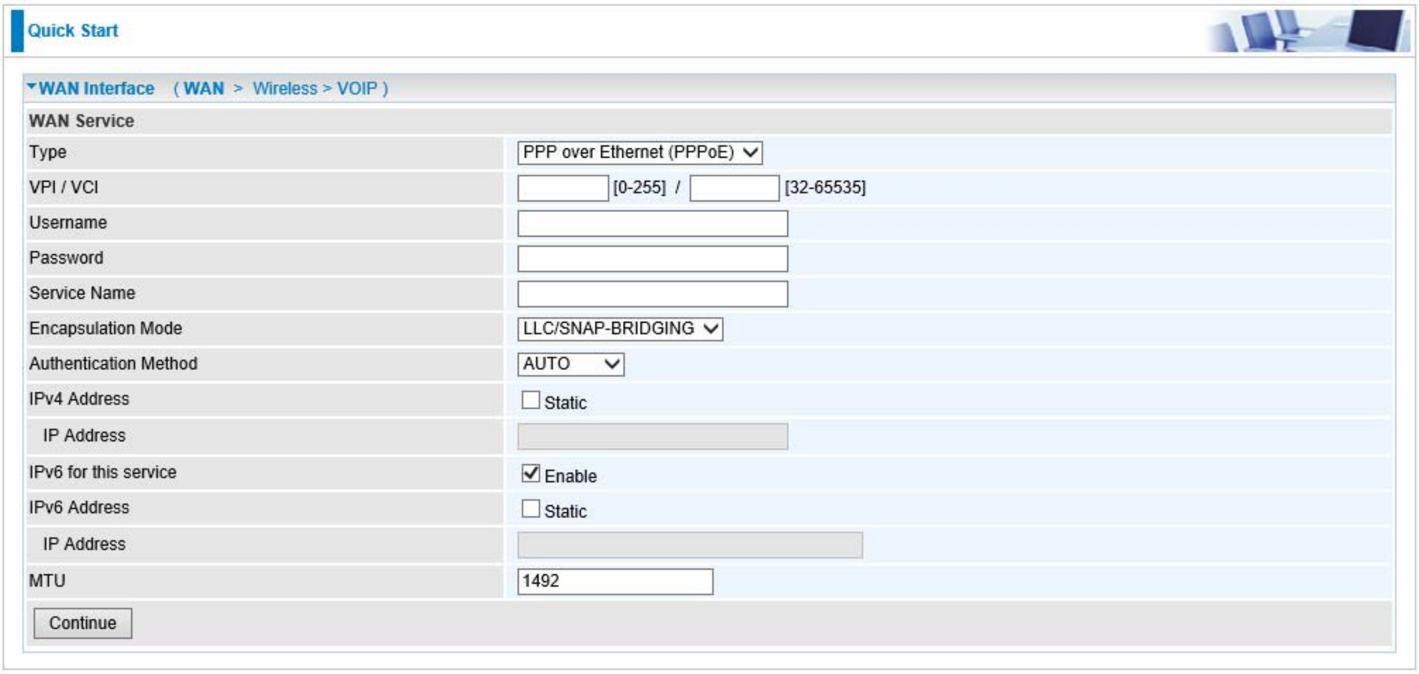
▾ WAN Interface (WAN > Wireless > VOIP)

Select WAN Interface	
Main Port	DSL (Current Main Port: DSL)
Layer2 Interface	● ATM ○ PTM

Continue

1. Select DSL, press **Continue** to go on to next step.

2. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.



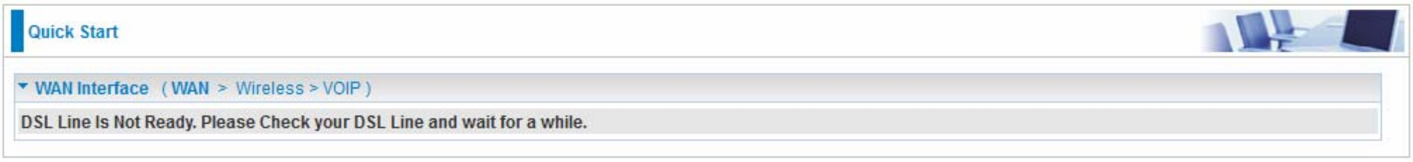
Quick Start

▾WAN Interface (WAN > Wireless > VOIP)

WAN Service	
Type	PPP over Ethernet (PPPoE)
VPI / VCI	[0-255] / [32-65535]
Username	
Password	
Service Name	
Encapsulation Mode	LLC/SNAP-BRIDGING
Authentication Method	AUTO
IPv4 Address	□ Static
IP Address	
IPv6 for this service	☑ Enable
IPv6 Address	□ Static
IP Address	
MTU	1492

Continue

If the DLS line is not synchronized, the page will pop up warning of the DSL connection failure.

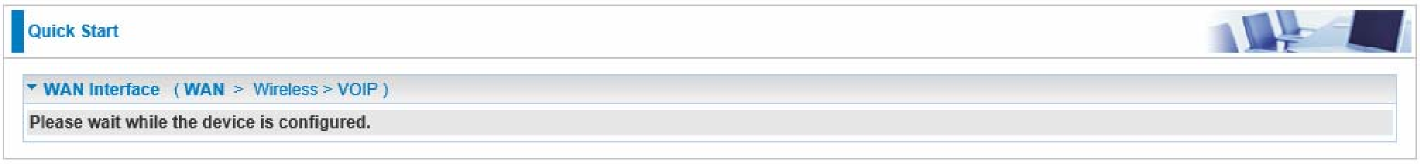


Quick Start

▾ WAN Interface (WAN > Wireless > VOIP)

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

3. Wait while the device is configured.

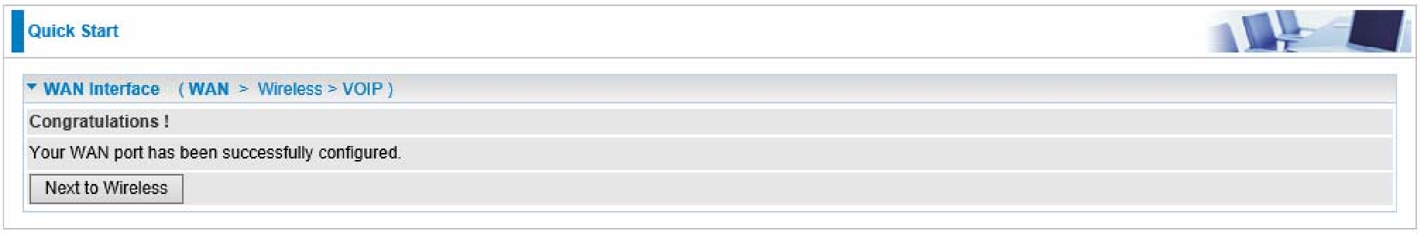


Quick Start

▼ WAN Interface (WAN > Wireless > VOIP)

Please wait while the device is configured.

4. WAN port configuration is successful.



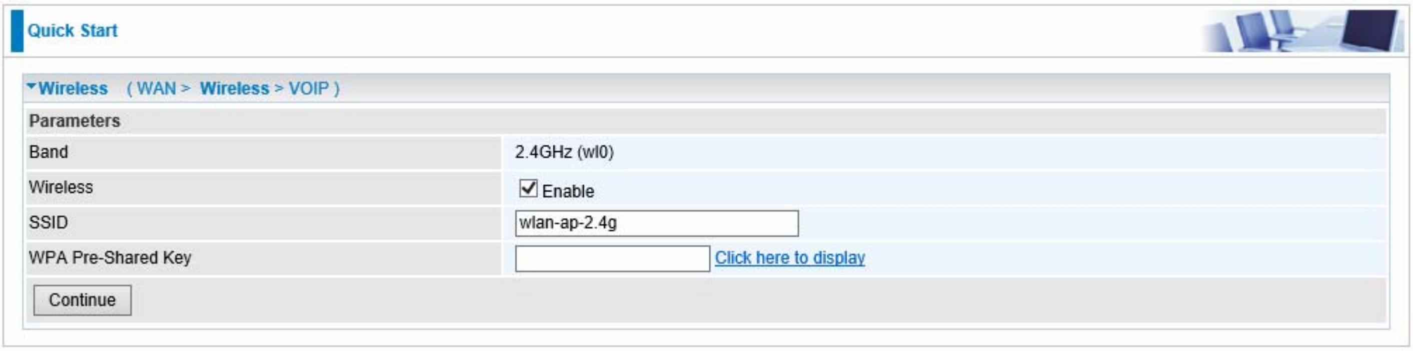
Quick Start

▼ WAN Interface (WAN > Wireless > VOIP)

Congratulations !

Your WAN port has been successfully configured.

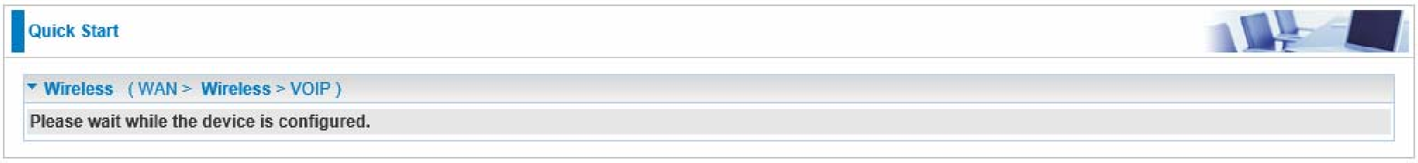
5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 7800VDP(O)X supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).



Quick Start

▼Wireless (WAN > Wireless > VOIP)

Parameters	
Band	2.4GHz (wl0)
Wireless	☑ Enable
SSID	wlan-ap-2.4g
WPA Pre-Shared Key	Click here to display

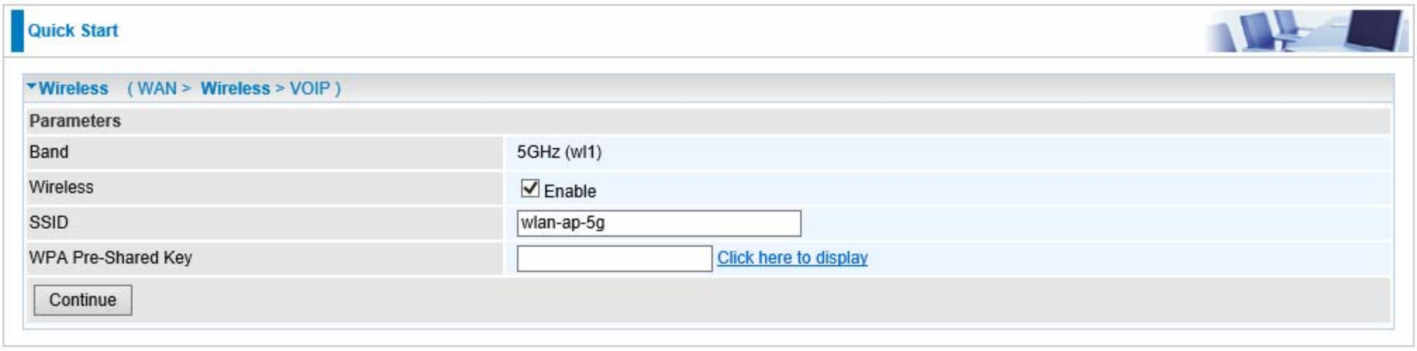


Quick Start

▼ Wireless (WAN > Wireless > VOIP)

Please wait while the device is configured.

6. Continue to set 5GHz wireless.

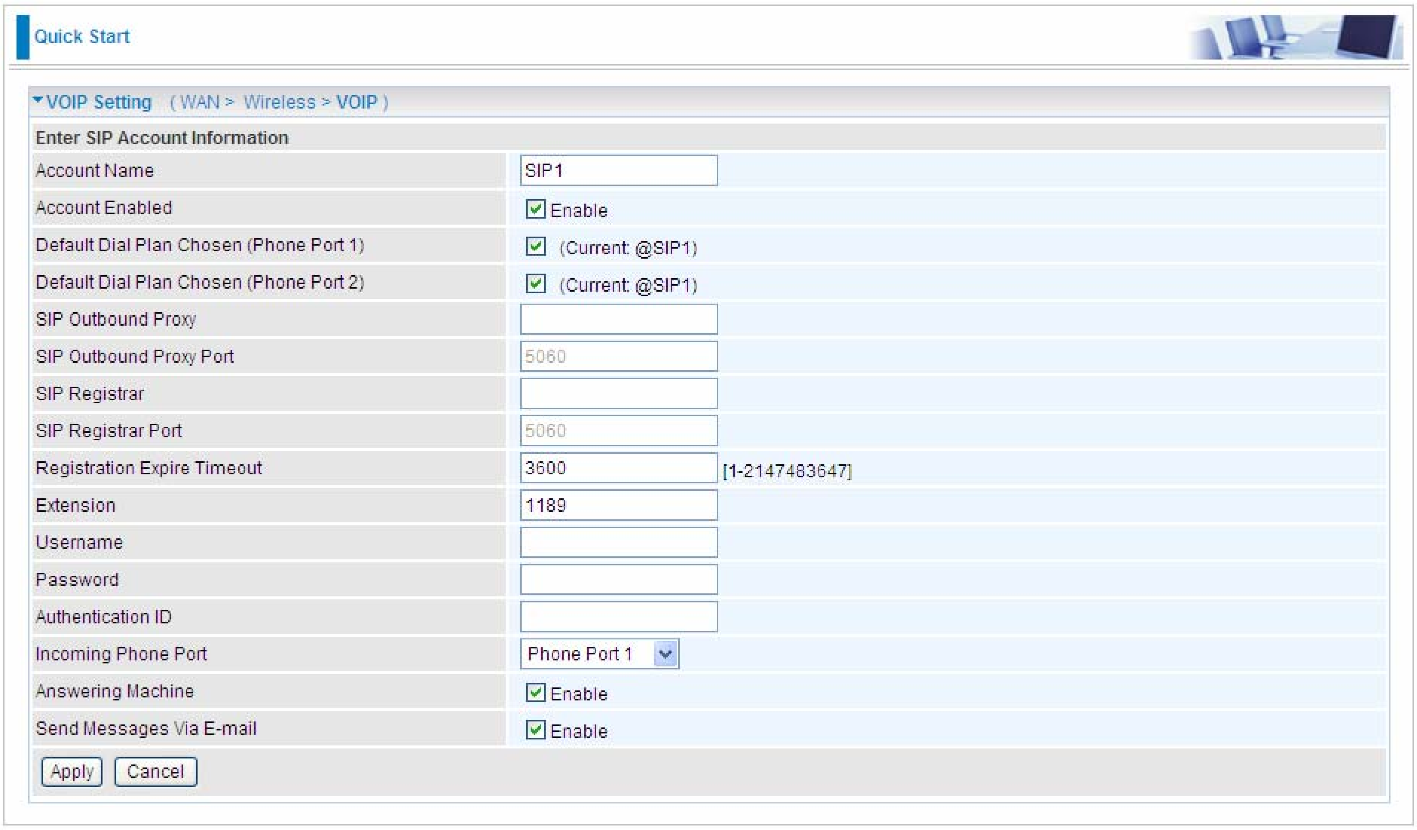


Quick Start

▼Wireless (WAN > Wireless > VOIP)

Parameters	
Band	5GHz (wl1)
Wireless	☑ Enable
SSID	wlan-ap-5g
WPA Pre-Shared Key	Click here to display

7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, please write down the registration information and fill it in the following blanks.



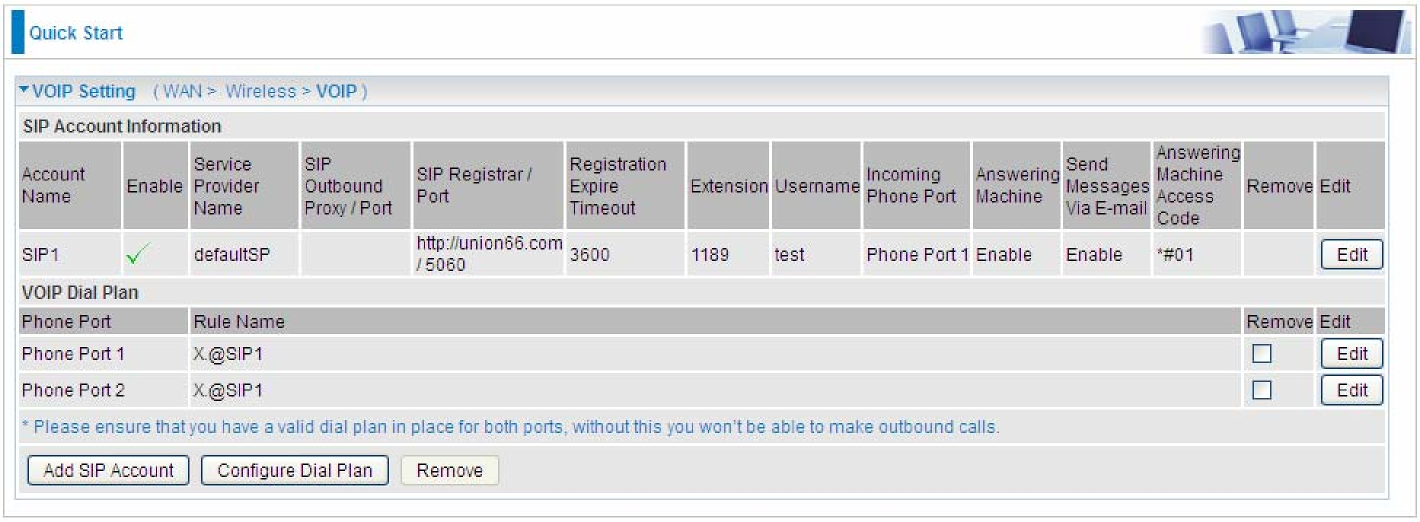
Quick Start

▾VOIP Setting (WAN > Wireless > VOIP)

Enter SIP Account Information

Account Name	SIP1
Account Enabled	☑ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @SIP1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @SIP1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	1189
Username	
Password	
Authentication ID	
Incoming Phone Port	Phone Port 1
Answering Machine	☑ Enable
Send Messages Via E-mail	☑ Enable

Apply Cancel



Quick Start

▾VOIP Setting (WAN > Wireless > VOIP)

SIP Account Information

Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✓	defaultSP		http://union66.com / 5060	3600	1189	test	Phone Port 1	Enable	Enable	*#01		Edit

VOIP Dial Plan

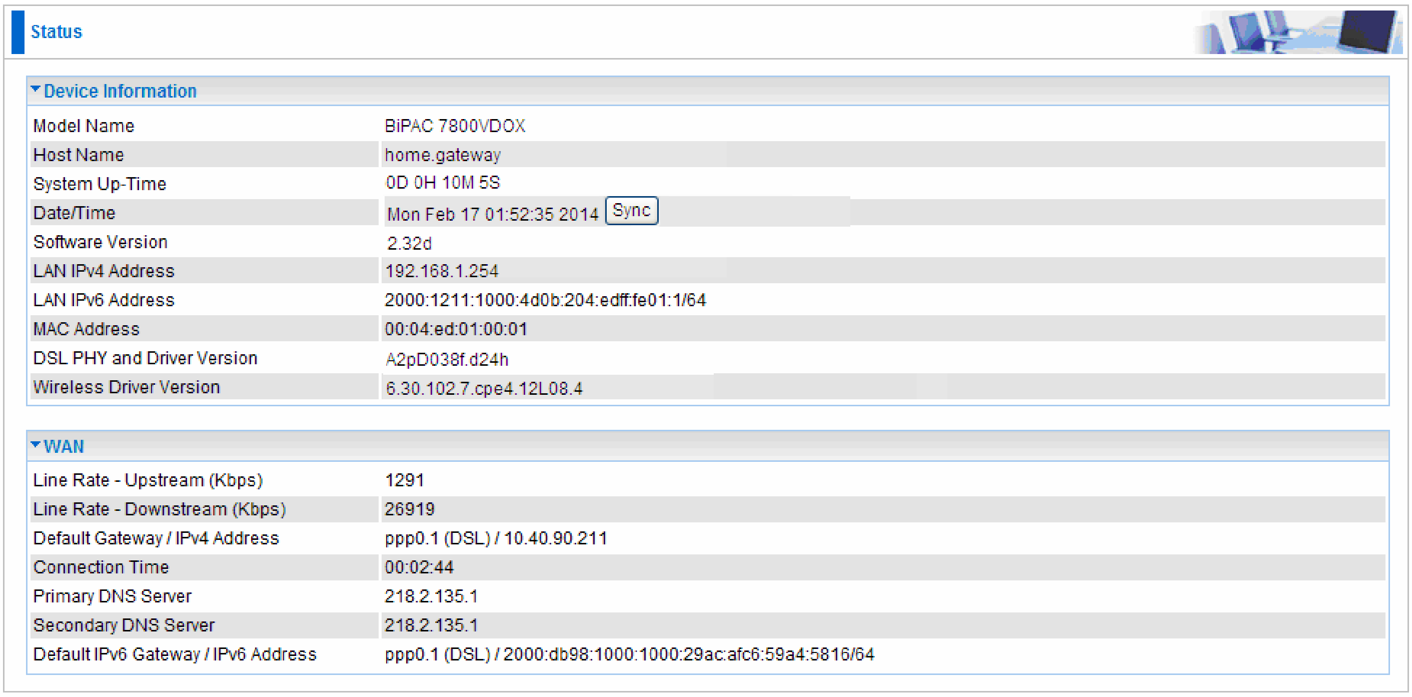
Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

Add SIP Account Configure Dial Plan Remove

In this page, user can continue to add SIP account and configure dial plan, for more, please refer to SIP Account and VoIP Plan.

If Quick Start is finished, user can turn to Status > Summary to see the basic information.



Status

▾Device Information

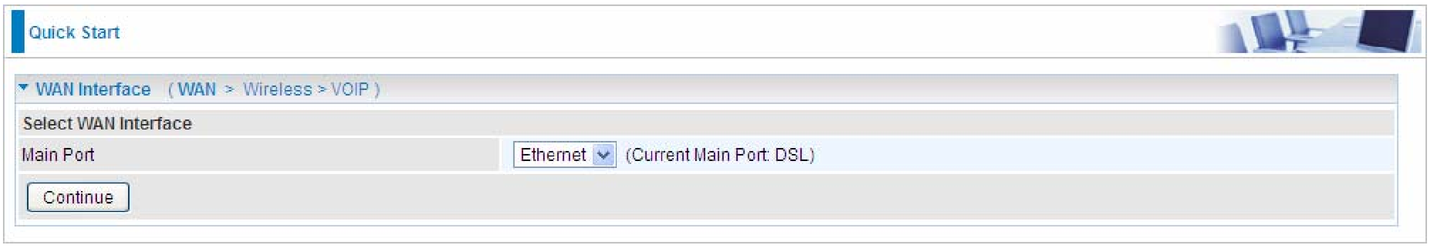
Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 10M 5S
Date/Time	Mon Feb 17 01:52:35 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

▾WAN

Line Rate - Upstream (Kbps)	1291
Line Rate - Downstream (Kbps)	26919
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

Ethernet mode

1. Select **Ethernet,** press **Continue** to go on to next step.

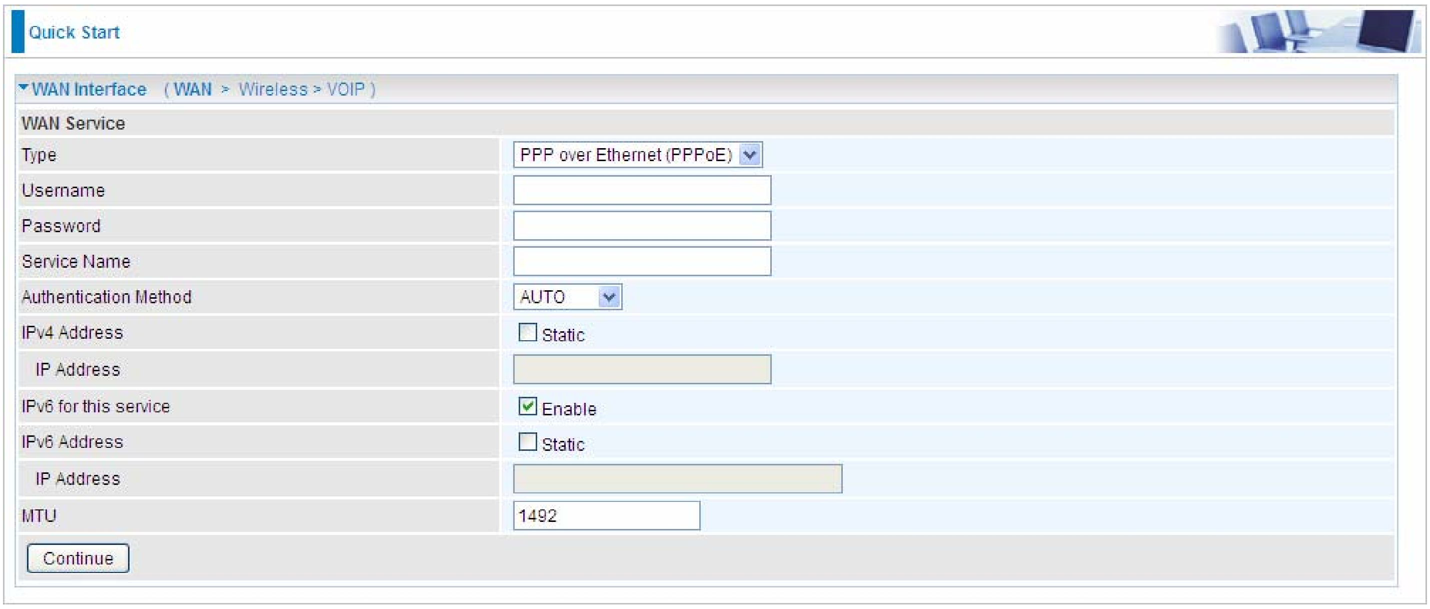


Quick Start

▾ WAN Interface (WAN > Wireless > VOIP)

Select WAN Interface	
Main Port	Ethernet ▾ (Current Main Port: DSL)

2. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.

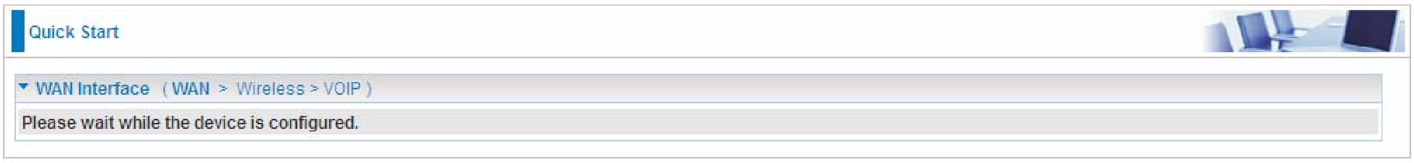


Quick Start

▾ WAN Interface (WAN > Wireless > VOIP)

WAN Service	
Type	PPP over Ethernet (PPPoE) ▾
Username	
Password	
Service Name	
Authentication Method	AUTO ▾
IPv4 Address	□ Static
IP Address	
IPv6 for this service	☑ Enable
IPv6 Address	□ Static
IP Address	
MTU	1492

3. Wait while the device is configured.

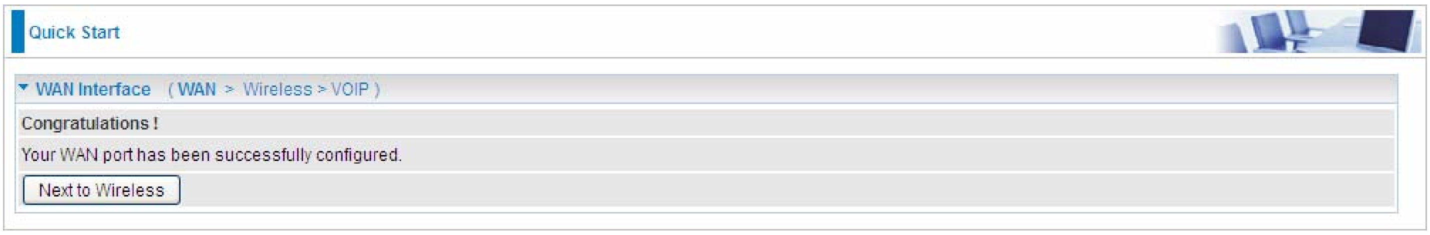


Quick Start

▾ WAN Interface (WAN > Wireless > VOIP)

Please wait while the device is configured.

4. WAN port configuration is successful.



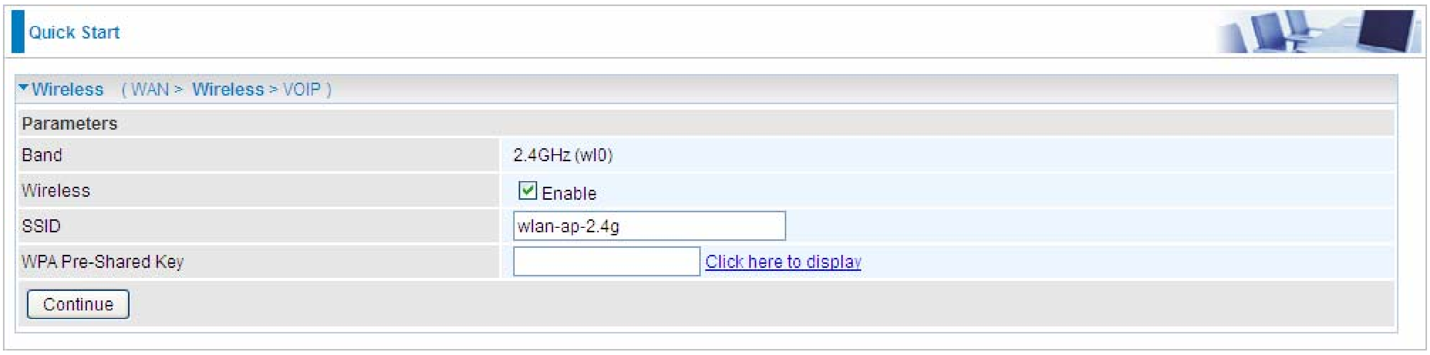
Quick Start

▾ WAN Interface (WAN > Wireless > VOIP)

Congratulations !

Your WAN port has been successfully configured.

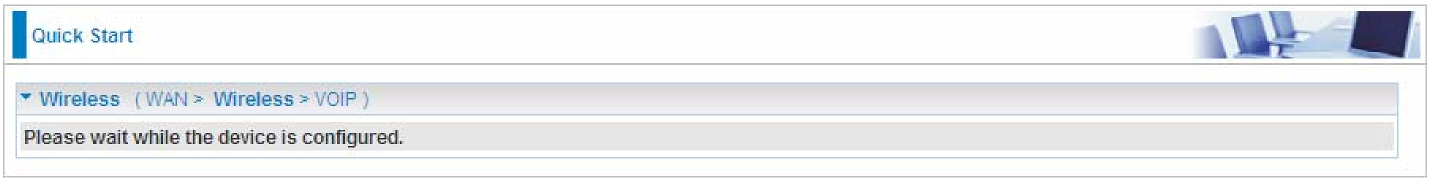
5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The device supports dual-band wireless connections, in Quick Start part, users can only enable or disable the wireless on the band and the exact SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES). For detail setting, please go to the Wireless part in this Manual.



Quick Start

▾Wireless (WAN > Wireless > VOIP)

Parameters	
Band	2.4GHz (wl0)
Wireless	☑ Enable
SSID	wlan-ap-2.4g
WPA Pre-Shared Key	Click here to display

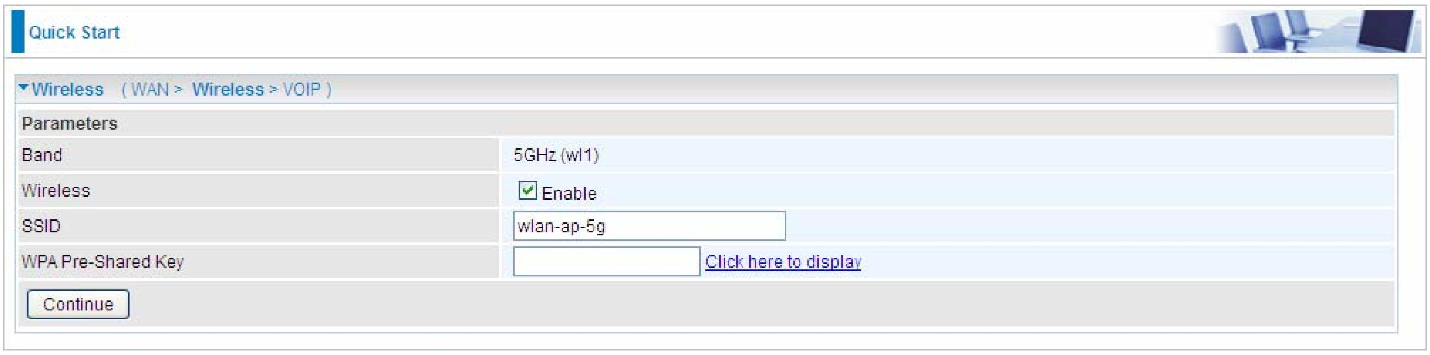


Quick Start

▾ Wireless (WAN > Wireless > VOIP)

Please wait while the device is configured.

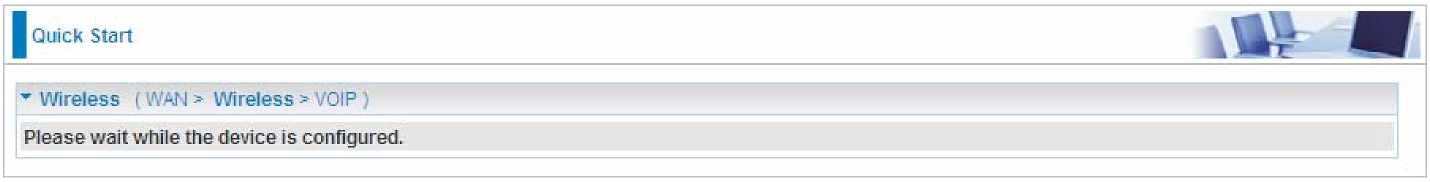
6. Continue to set 5GHz wireless.



Quick Start

▾Wireless (WAN > Wireless > VOIP)

Parameters	
Band	5GHz (wl1)
Wireless	☑ Enable
SSID	wlan-ap-5g
WPA Pre-Shared Key	Click here to display

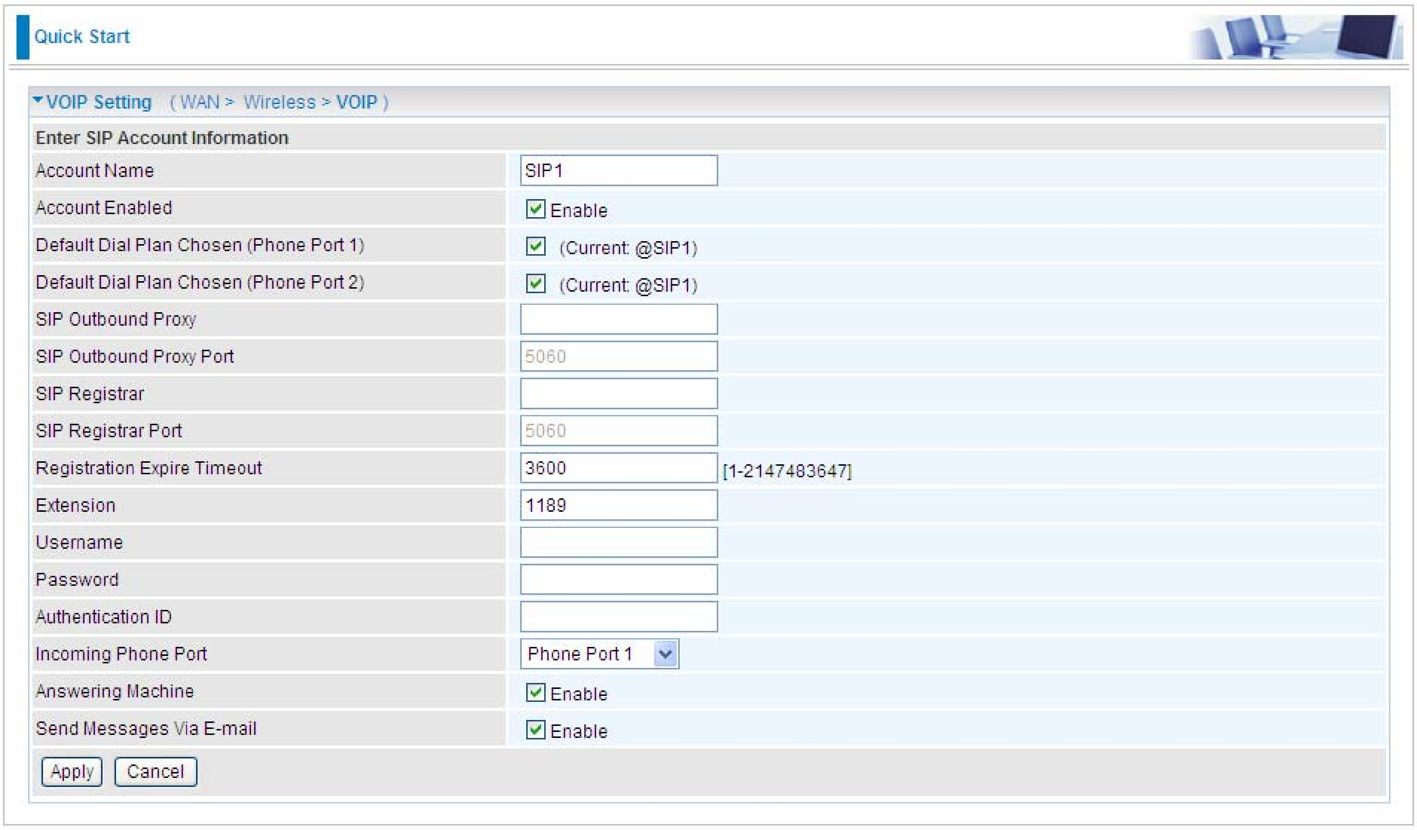


Quick Start

▾ Wireless (WAN > Wireless > VOIP)

Please wait while the device is configured.

7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, write down the registration information and fill it in the following blanks.



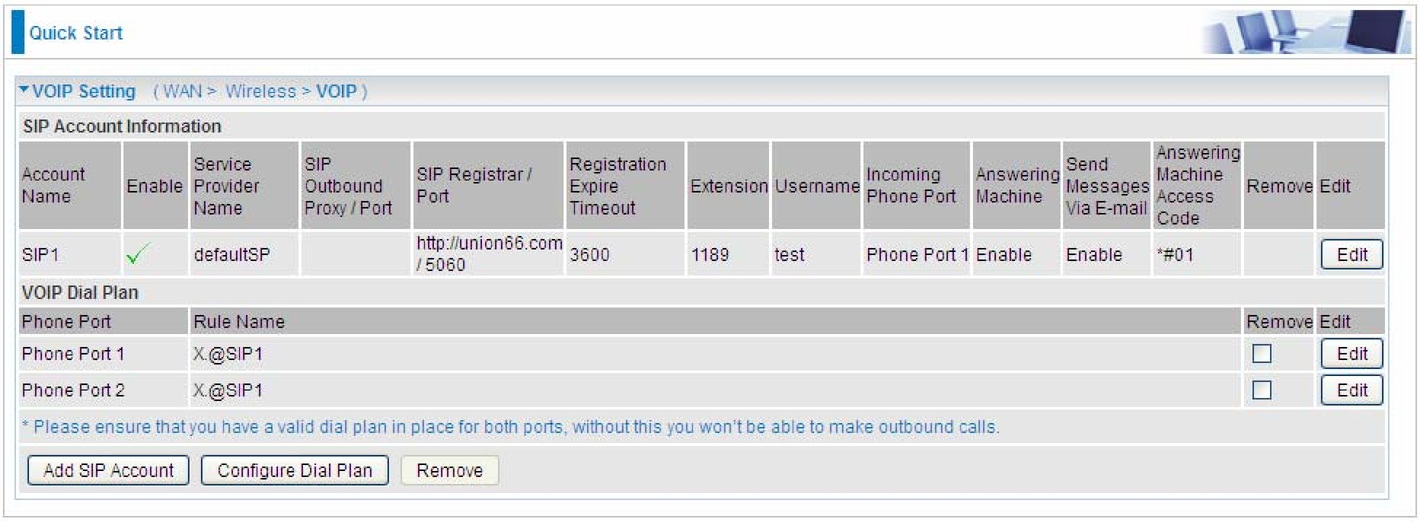
Quick Start

▾VOIP Setting (WAN > Wireless > VOIP)

Enter SIP Account Information

Account Name	SIP1
Account Enabled	☑ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @SIP1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @SIP1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	1189
Username	
Password	
Authentication ID	
Incoming Phone Port	Phone Port 1
Answering Machine	☑ Enable
Send Messages Via E-mail	☑ Enable

Apply Cancel



Quick Start

▾VOIP Setting (WAN > Wireless > VOIP)

SIP Account Information

Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✓	defaultSP		http://union66.com / 5060	3600	1189	test	Phone Port 1	Enable	Enable	*#01		Edit

VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

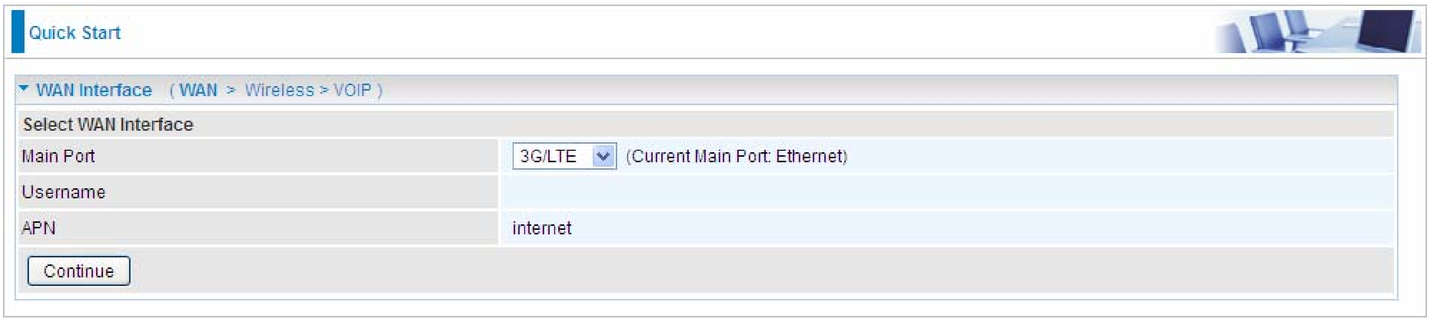
* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

Add SIP Account Configure Dial Plan Remove

In this page, user can continue to add SIP account and configure dial plan, for more, please refer to SIP Account and VoIP Plan.

3G/LTE

1. Select **3G/LTE,** press **Continue** to go on to next step.



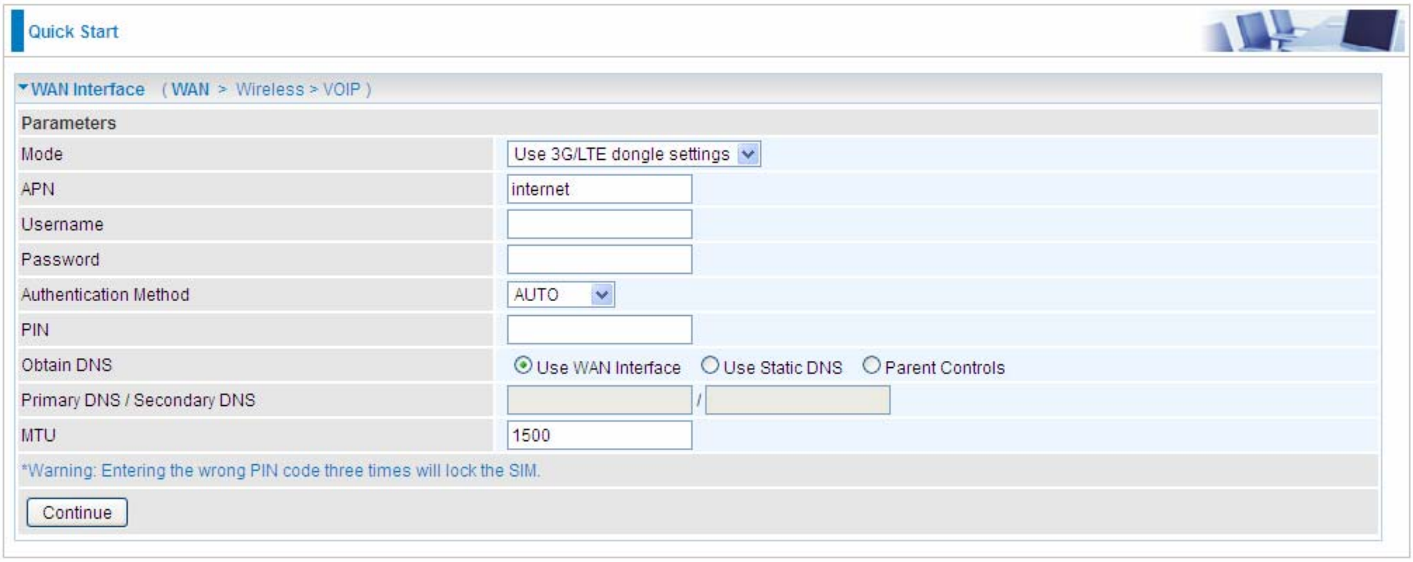
Quick Start

WAN Interface (WAN > Wireless > VOIP)

Select WAN Interface

Main Port	3G/LTE (Current Main Port: Ethernet)
Username	
APN	internet

2. Select the 3G mode, and enter the APN, username, password from your ISP; and check with your ISP with the authentication method setting.



Quick Start

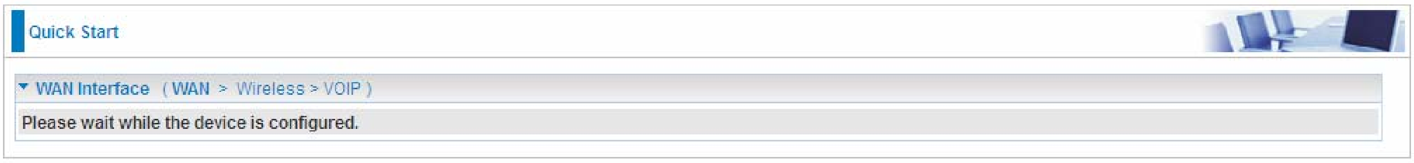
WAN Interface (WAN > Wireless > VOIP)

Parameters

Mode	Use 3G/LTE dongle settings
APN	internet
Username	
Password	
Authentication Method	AUTO
PIN	
Obtain DNS	● Use WAN Interface ○ Use Static DNS ○ Parent Controls
Primary DNS / Secondary DNS	/
MTU	1500

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

3. Wait while the device is configured.

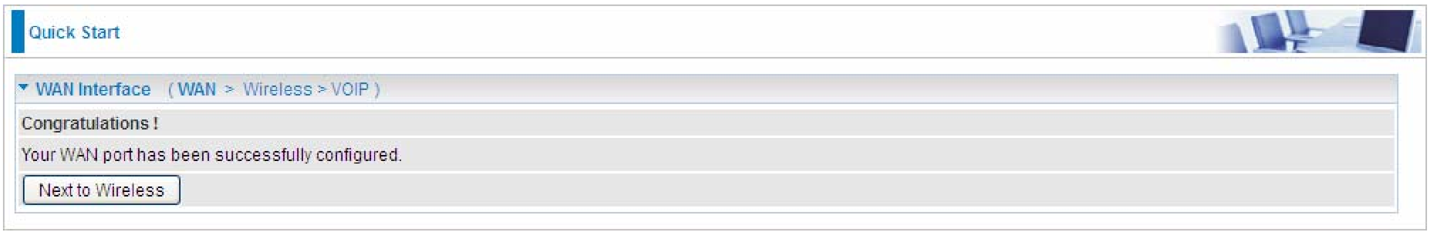


Quick Start

WAN Interface (WAN > Wireless > VOIP)

Please wait while the device is configured.

4. WAN port configuration is successful.



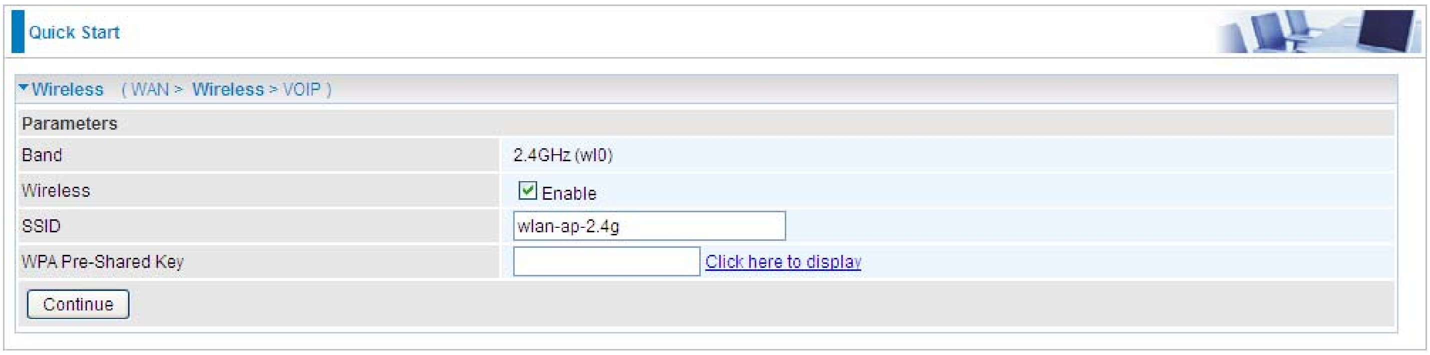
Quick Start

WAN Interface (WAN > Wireless > VOIP)

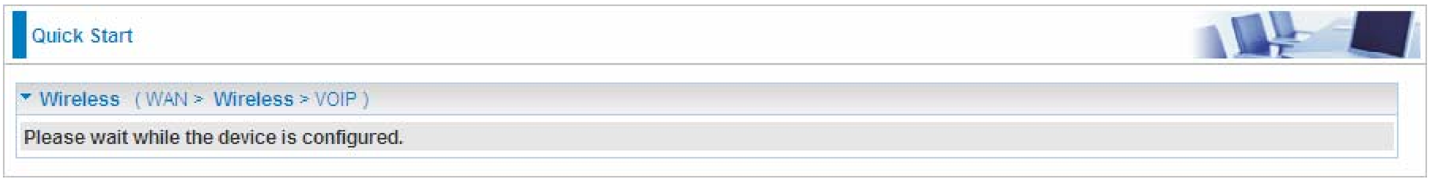
Congratulations !

Your WAN port has been successfully configured.

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The device supports dual-band wireless connections, in Quick Start part, users can only enable or disable the wireless on the band and the exact SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES). For detail setting, please go to the Wireless part in this Manual.

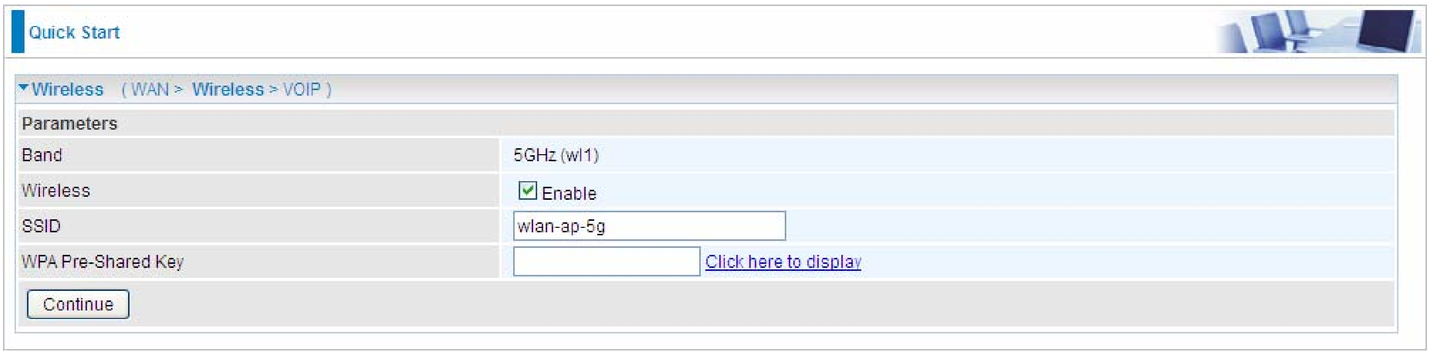


Parameters	
Band	2.4GHz (wl0)
Wireless	☑ Enable
SSID	wlan-ap-2.4g
WPA Pre-Shared Key	Click here to display

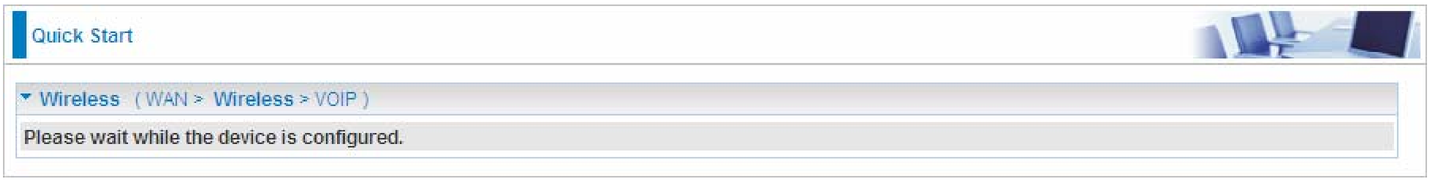


Please wait while the device is configured.

6. Continue to set 5GHz wireless.

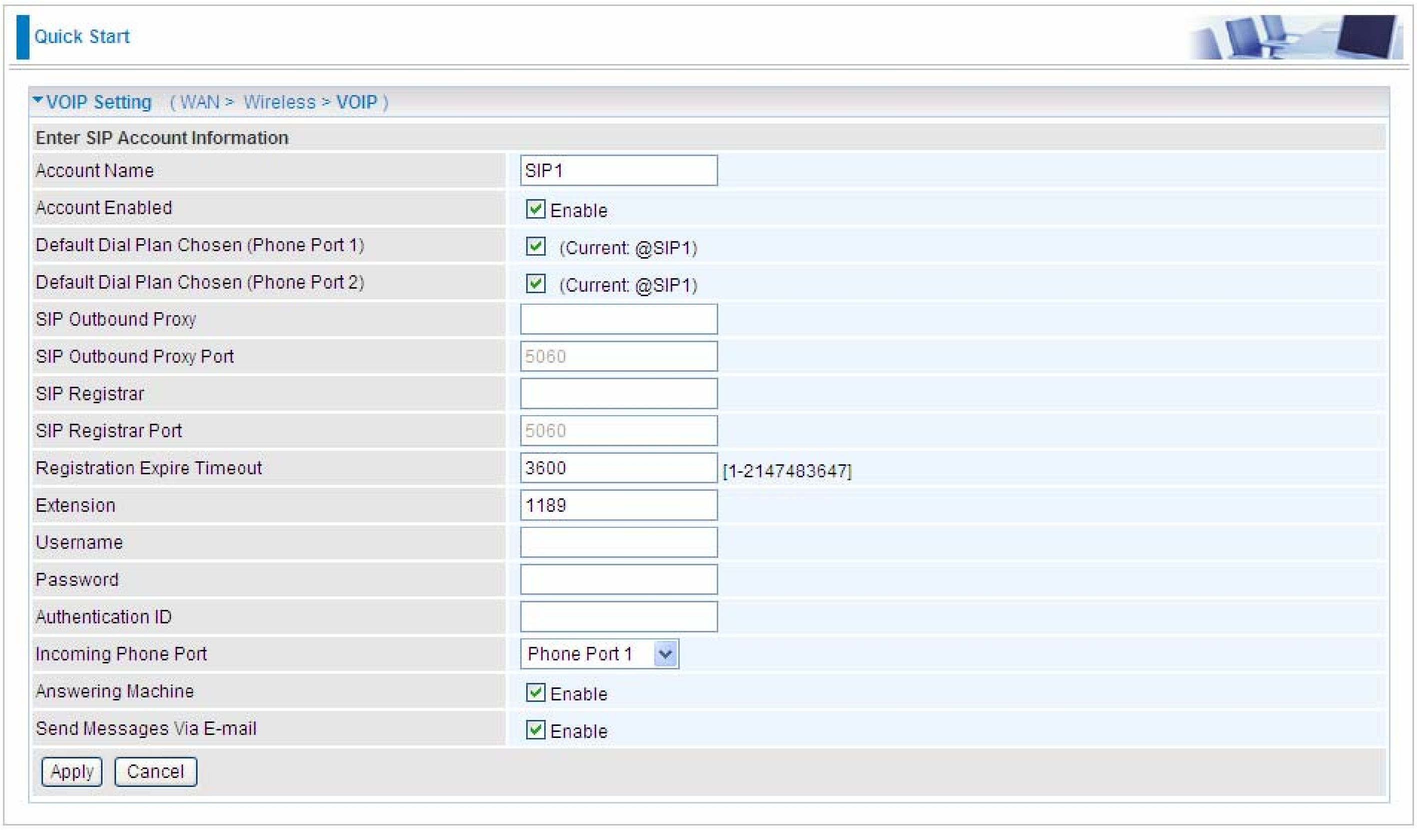


Parameters	
Band	5GHz (wl1)
Wireless	☑ Enable
SSID	wlan-ap-5g
WPA Pre-Shared Key	Click here to display



Please wait while the device is configured.

7. Set the VoIP parameters. First user should turn to a VoIP service provider to register a SIP account, write down the registration information and fill it in the following blanks.

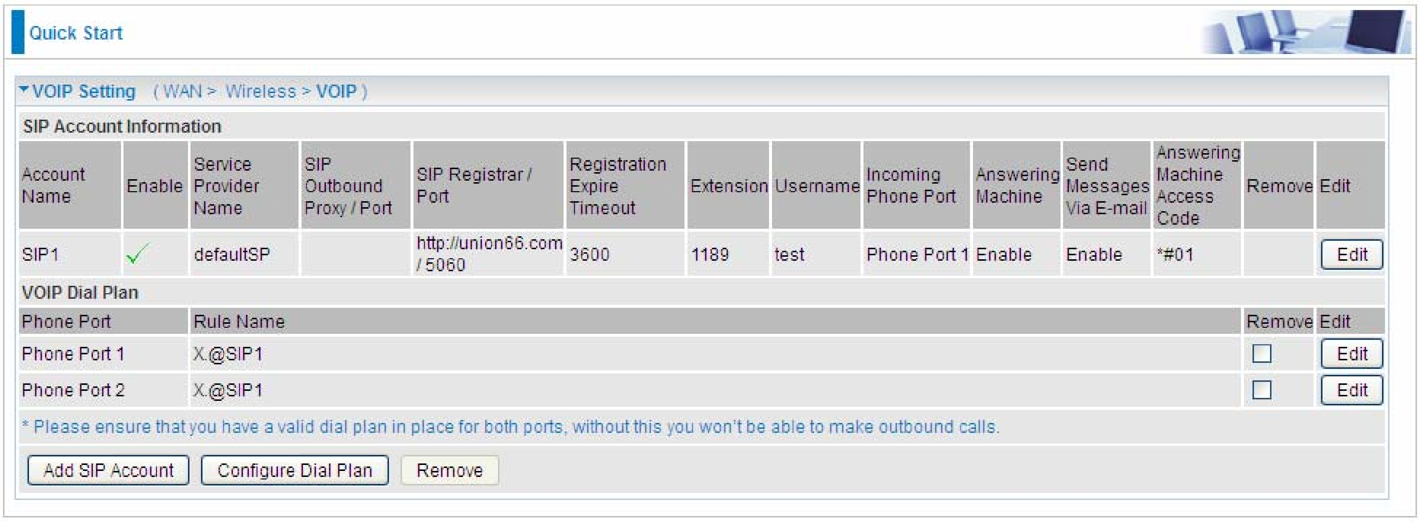


Quick Start

▾VOIP Setting (WAN > Wireless > VOIP)

Enter SIP Account Information

Account Name	SIP1
Account Enabled	☑ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @SIP1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @SIP1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	1189
Username	
Password	
Authentication ID	
Incoming Phone Port	Phone Port 1
Answering Machine	☑ Enable
Send Messages Via E-mail	☑ Enable



Quick Start

▾VOIP Setting (WAN > Wireless > VOIP)

SIP Account Information

Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✓	defaultSP		http://union66.com / 5060	3600	1189	test	Phone Port 1	Enable	Enable	*#01		Edit

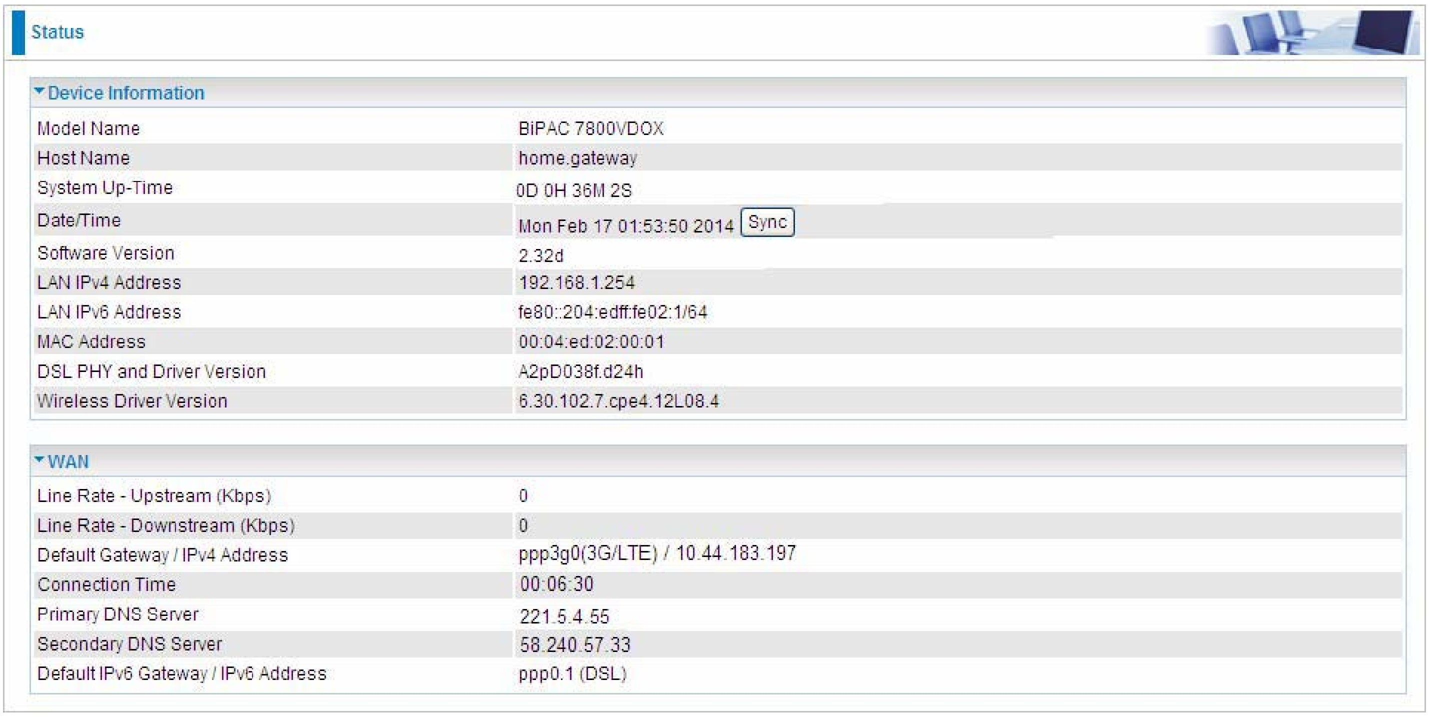
VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

In this page, user can continue to add SIP account and configure dial plan, for more, please refer to SIP Account and VoIP Plan.

If Quick Start is finished, user can turn to Status > Summary to see the basic information.



Status

Device Information

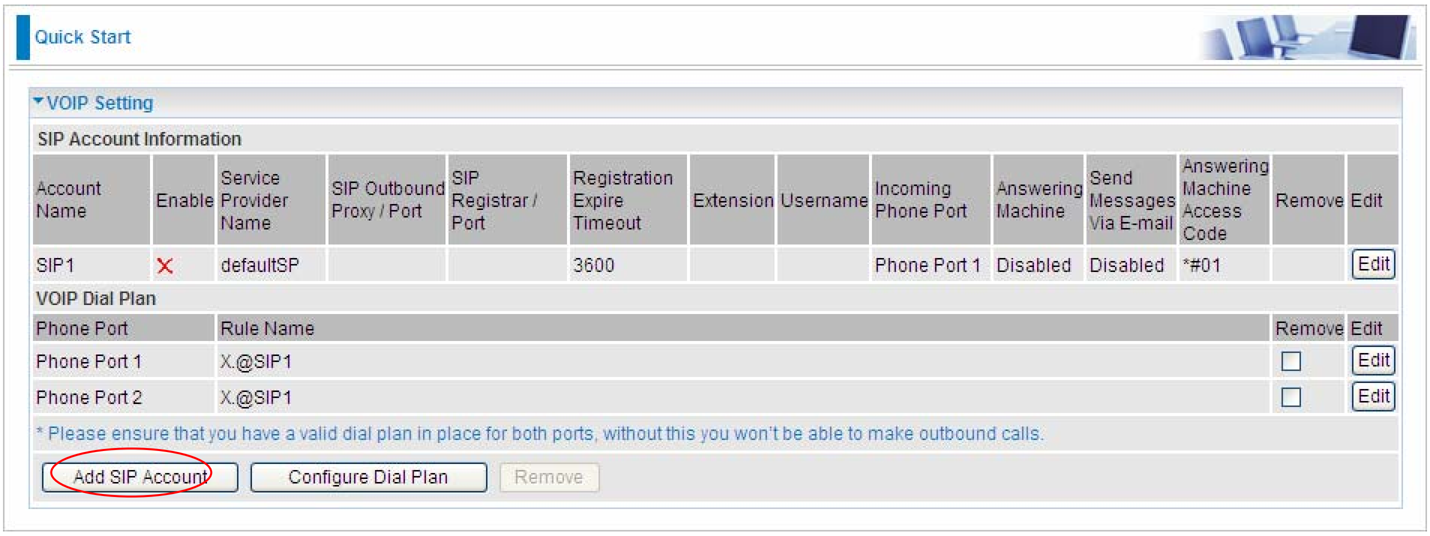
Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 36M 2S
Date/Time	Mon Feb 17 01:53:50 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp3g0(3G/LTE) / 10.44.183.197
Connection Time	00:06:30
Primary DNS Server	221.5.4.55
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL)

VoIP Quick Setup

"VoIP Quick Setup" links to quick VoIP setting pages. In this part, users can conduct the necessary settings (SIP account, VoIP Dial Plan, etc) of VoIP for use. For detail settings, please refer to VoIP.



Quick Start

▾VOIP Setting

SIP Account Information

Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
SIP1	✗	defaultSP			3600			Phone Port 1	Disabled	Disabled	*#01		Edit

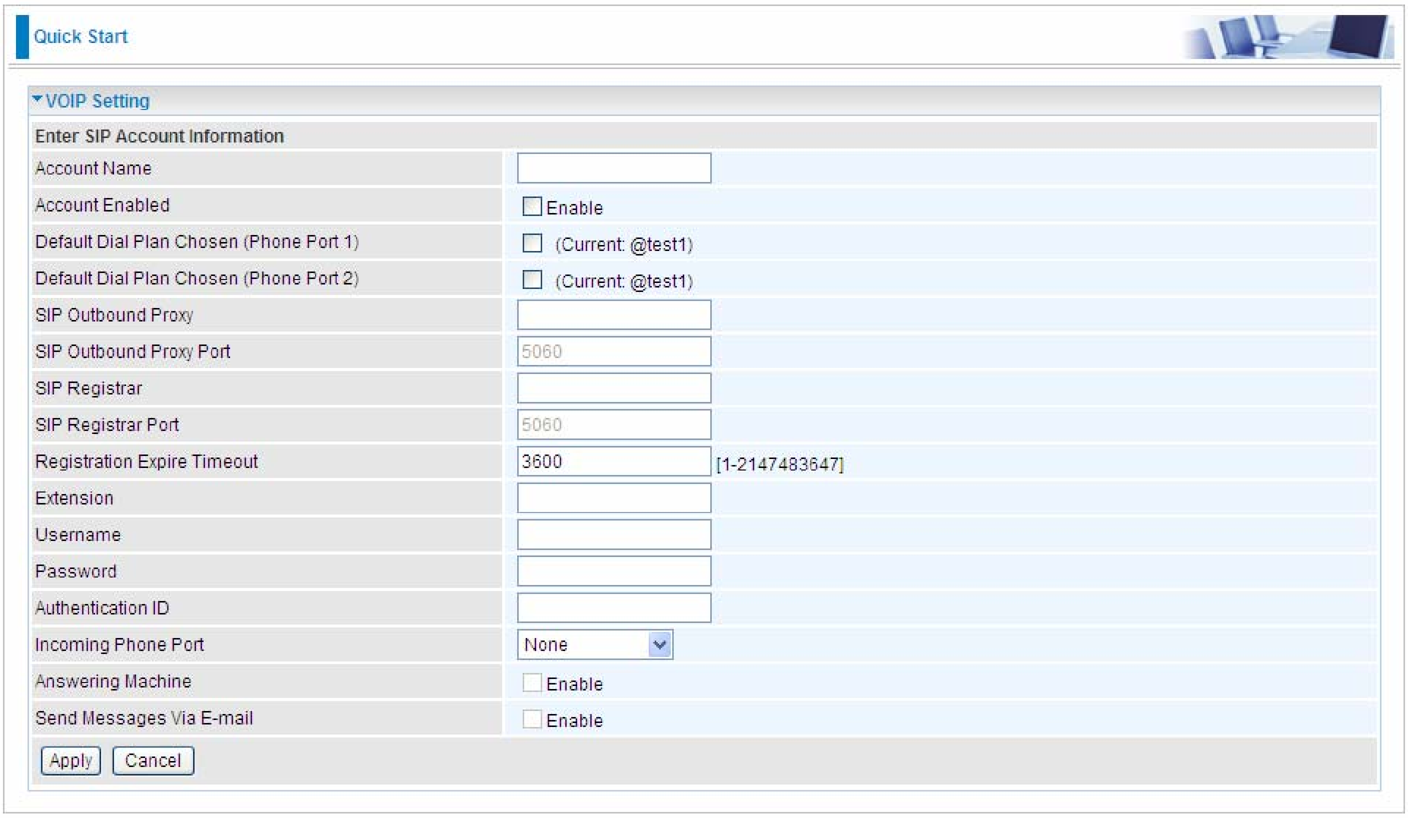
VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@SIP1	□	Edit
Phone Port 2	X.@SIP1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

Picture1

Click **Add SIP Account** to add new sip accounts (set the registration information).



Quick Start

▾VOIP Setting

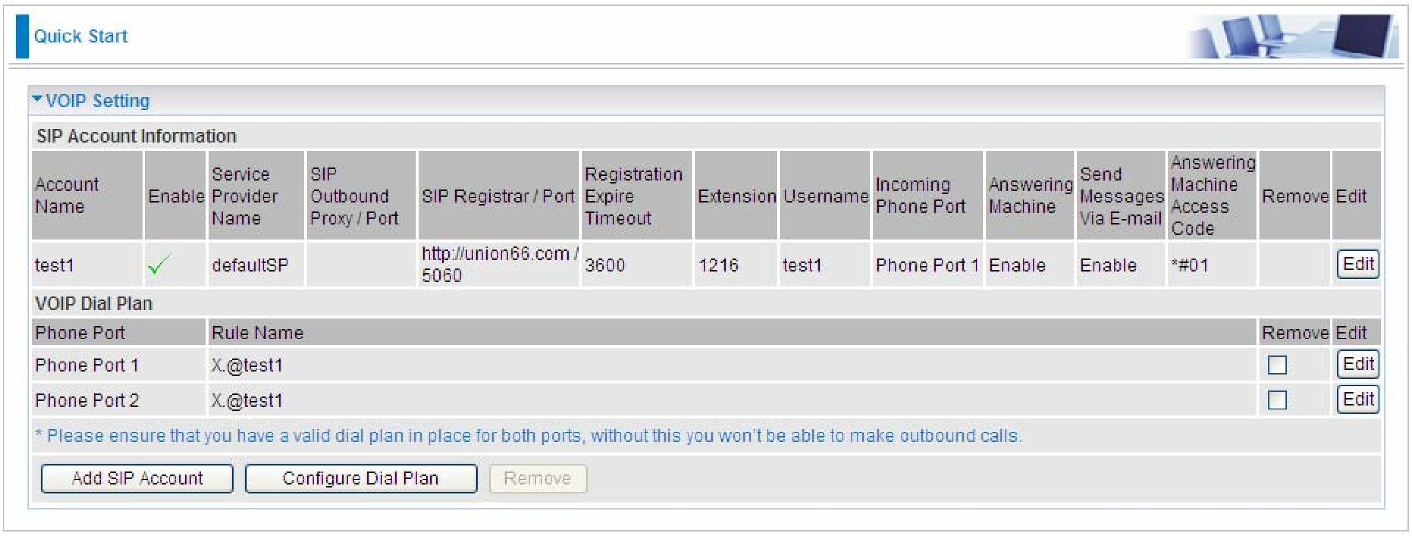
Enter SIP Account Information

Account Name	
Account Enabled	□ Enable
Default Dial Plan Chosen (Phone Port 1)	□ (Current: @test1)
Default Dial Plan Chosen (Phone Port 2)	□ (Current: @test1)
SIP Outbound Proxy	
SIP Outbound Proxy Port	5060
SIP Registrar	
SIP Registrar Port	5060
Registration Expire Timeout	3600 [1-2147483647]
Extension	
Username	
Password	
Authentication ID	
Incoming Phone Port	None
Answering Machine	□ Enable
Send Messages Via E-mail	□ Enable

Picture2

Click **Apply** to save the settings.

For example:



▾VOIP Setting

SIP Account Information

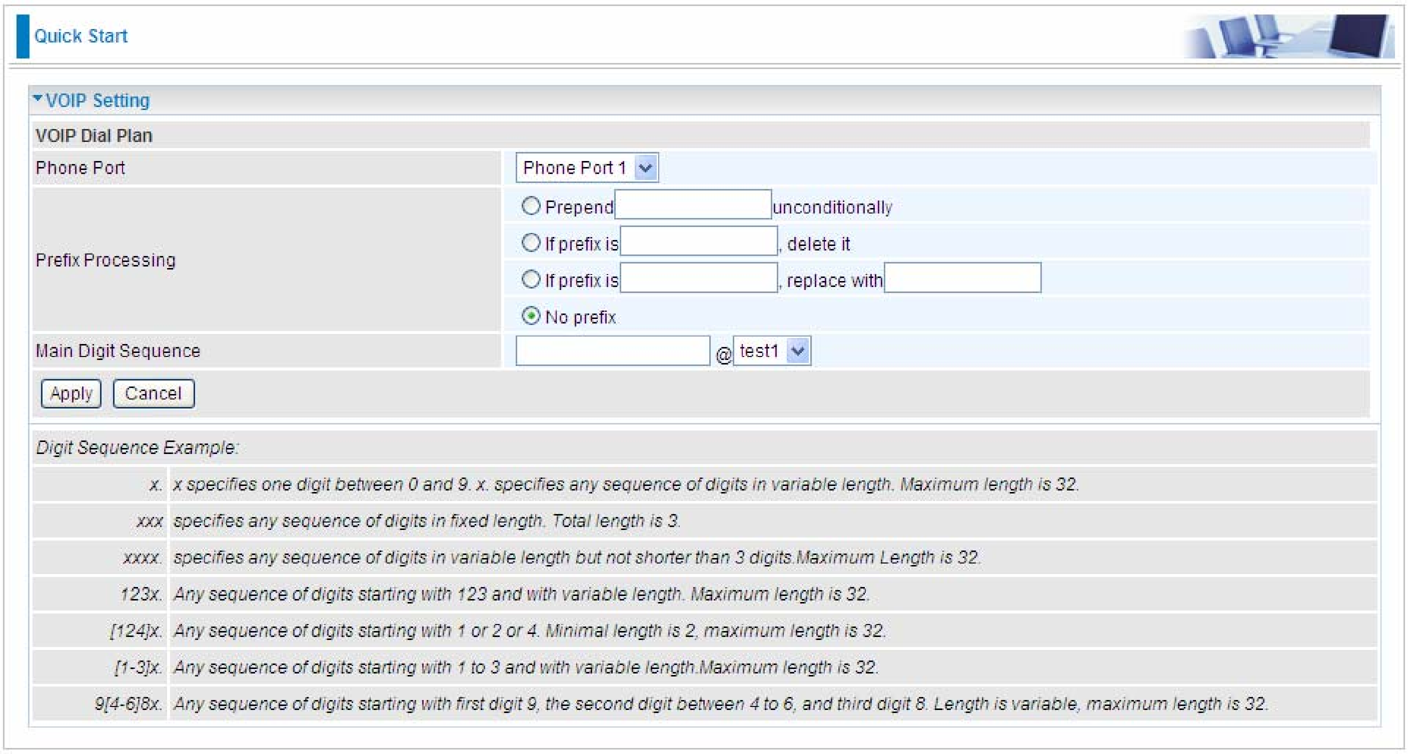
Account Name	Enable	Service Provider Name	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Extension	Username	Incoming Phone Port	Answering Machine	Send Messages Via E-mail	Answering Machine Access Code	Remove	Edit
test1	✓	defaultSP		http://union66.com / 5060	3600	1216	test1	Phone Port 1	Enable	Enable	*#01		Edit

VOIP Dial Plan

Phone Port	Rule Name	Remove	Edit
Phone Port 1	X.@test1	□	Edit
Phone Port 2	X.@test1	□	Edit

* Please ensure that you have a valid dial plan in place for both ports, without this you won't be able to make outbound calls.

In picture1, click **Configure Dial Plan** to extend to configure the dial plan. Please go to VOIP Plan to get more.



▾VOIP Setting

VOIP Dial Plan

Phone Port	Phone Port 1
Prefix Processing	○ Prepend ___ unconditionally ○ If prefix is ___, delete it ○ If prefix is ___, replace with ___ ● No prefix
Main Digit Sequence	___ @ test1

Digit Sequence Example:

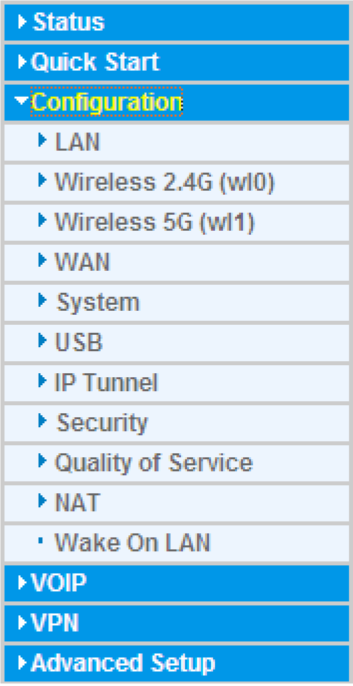
x.	*x specifies one digit between 0 and 9. x. specifies any sequence of digits in variable length. Maximum length is 32.*
xxx	*specifies any sequence of digits in fixed length. Total length is 3.*
xxxx.	*specifies any sequence of digits in variable length but not shorter than 3 digits.Maximum Length is 32.*
123x.	*Any sequence of digits starting with 123 and with variable length. Maximum length is 32.*
[124]x.	*Any sequence of digits starting with 1 or 2 or 4. Minimal length is 2, maximum length is 32.*
[1-3]x.	*Any sequence of digits starting with 1 to 3 and with variable length.Maximum length is 32.*
9[4-6]8x.	*Any sequence of digits starting with first digit 9, the second digit between 4 to 6, and third digit 8. Length is variable, maximum length is 32.*

Picture3

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, **Wireless 2.4G (wl0)**, **Wireless 5G (wl1)**, **WAN**, **System**, **USB**, **IP Tunnel**, **Security**, **Quality of Service**, **NAT** and **Wake On LAN**.



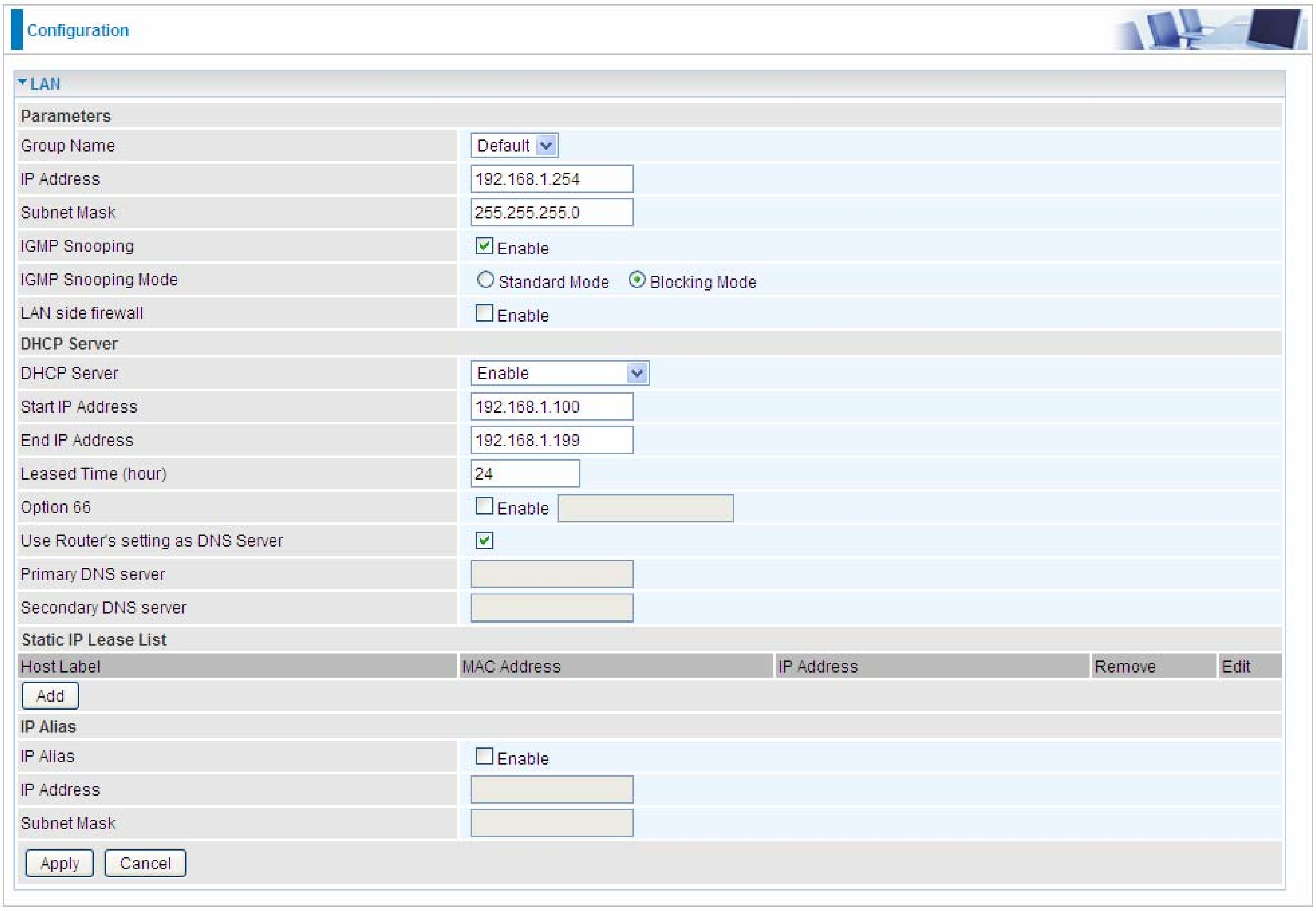
(7800VDOX)

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 network where many computers are connected. This type of network is area defined and is usually limited to a confined region within a building.

Ethernet



Configuration

▾LAN

Parameters				
Group Name	Default			
IP Address	192.168.1.254			
Subnet Mask	255.255.255.0			
IGMP Snooping	☑ Enable			
IGMP Snooping Mode	○ Standard Mode ● Blocking Mode			
LAN side firewall	□ Enable			
DHCP Server				
DHCP Server	Enable			
Start IP Address	192.168.1.100			
End IP Address	192.168.1.199			
Leased Time (hour)	24			
Option 66	□ Enable			
Use Router's setting as DNS Server	☑			
Primary DNS server				
Secondary DNS server				
Static IP Lease List				
Host Label	MAC Address	IP Address	Remove	Edit
Add				
IP Alias				
IP Alias	□ Enable			
IP Address				
Subnet Mask				
Apply Cancel				

Parameters

Group Name: This refers to the group you set in **Interface Grouping** section; you can set the parameters for the specific group. Select the group via the drop-down box. For more information please refer to Interface Grouping of this manual.

IP address: the IP address of the router. Default is 192.168.1.254.

Subnet Mask: the default Subnet mask on the router.

IGMP Snooping: Enable or disable the IGMP Snooping function. Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that have members of that group."

When enabled, you will see two modes:

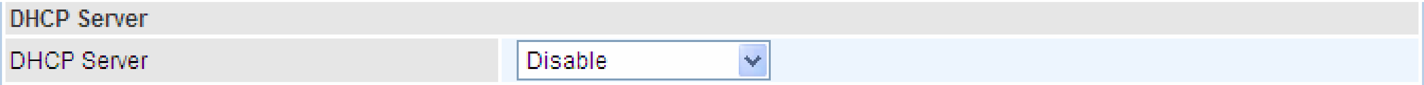
- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

LAN side firewall: Enable to drop all traffic from the specified LAN group interface. After activating it, all incoming packets by default will be dropped, and the user on the specified LAN group interface can't access CPE anymore. But, you can still access the internet service. If user wants to manage the CPE, please turn to IP Filtering Incoming to add the allowing rules. **Note** that all incoming packets by default will be dropped if the LAN side firewall is enabled and user cannot manage this CPE from the specified LAN group.

DHCP Server

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

ⓘ Disable

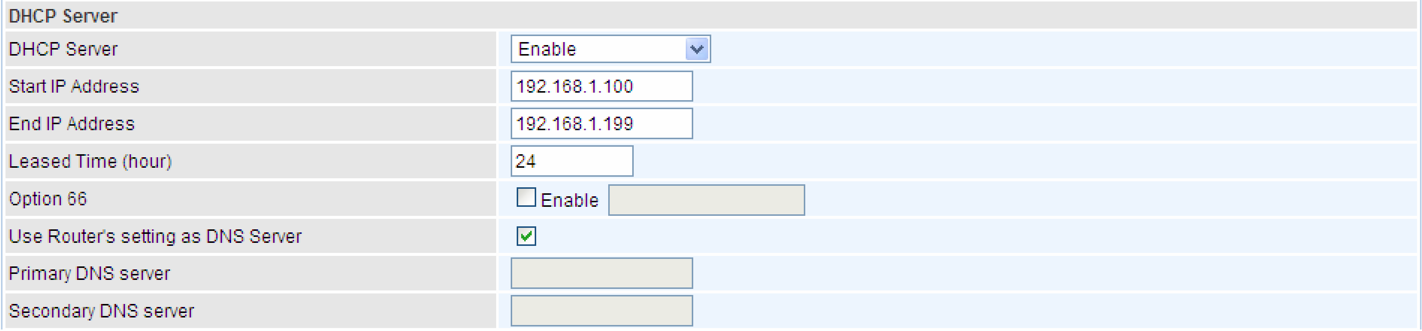


DHCP Server	
DHCP Server	Disable ▾

Disable the DHCP Server function.

ⓘ Enable

Enable the DHCP function, enter the information wanted. Here as default.



DHCP Server	
DHCP Server	Enable ▾
Start IP Address	192.168.1.100
End IP Address	192.168.1.199
Leased Time (hour)	24
Option 66	□ Enable
Use Router's setting as DNS Server	☑
Primary DNS server	
Secondary DNS server	

Start IP Address: The start IP address of the range the DHCP Server used to assign to the Clients.

End IP Address: The end IP address f the range the DHCP Server used to assign to the Clients.

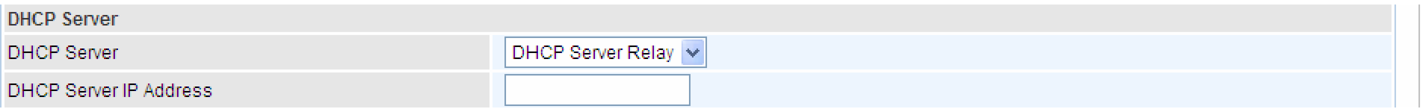
Leased Time (hour): The leased time for each DHCP Client.

Option 66: Click Enable to activate DHCP option 66 for some special devices, like IPTV Set Box. The devices can get firmware or some special service from the TFTP server. User needs to set the IP or hostname of the TFTP server.

User Router's setting as DNS server: Select whether to enable use router's setting as DNS server to allow different LAN group with different DNS server settings.
If enabled, the PCs on the LAN side obtain the router's setting as DNS server. If disabled, please specify exactly the primary/secondary DNS server.

Primary/Secondary DNS server: Specify your primary/secondary DNS server for your LAN devices.

ⓘ DHCP Server Relay

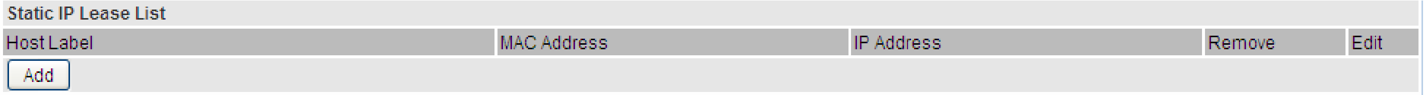


DHCP Server	
DHCP Server	DHCP Server Relay ▾
DHCP Server IP Address	

DHCP Server IP Address: Please enter the DHCP Server IP address.

Static IP List

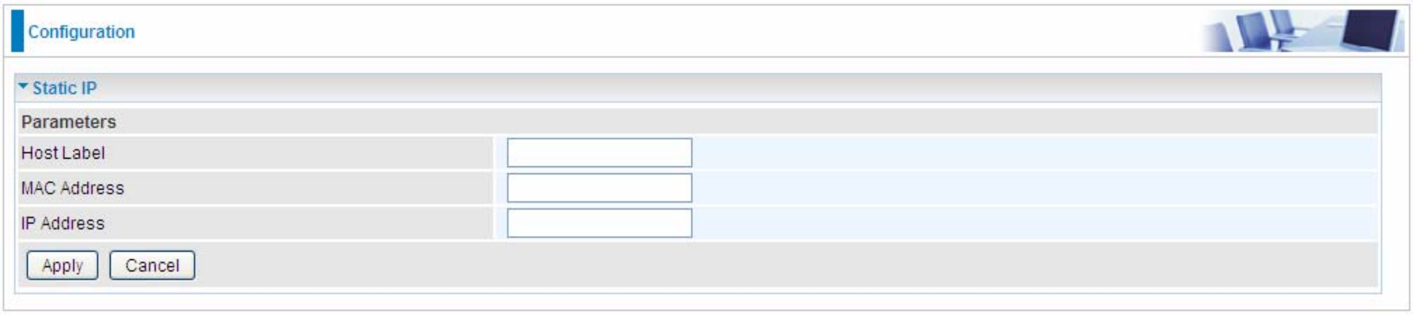
The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assigns IP Addresses to Clients.



Static IP Lease List

Host Label	MAC Address	IP Address	Remove	Edit

Press **Add** to the Static IP List.



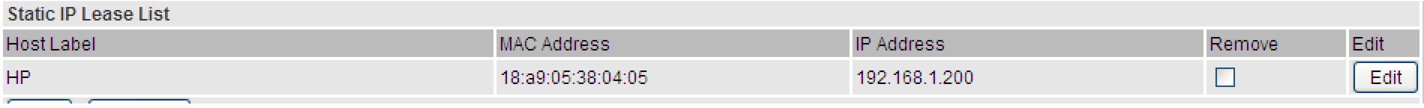
Configuration

▾ Static IP

Parameters

Host Label	
MAC Address	
IP Address	

Enter the MAC Address, IP Address, and then click Apply to confirm your settings. But the IP assigned should be outside the range of 192.168.1.100-192.168.1.199.

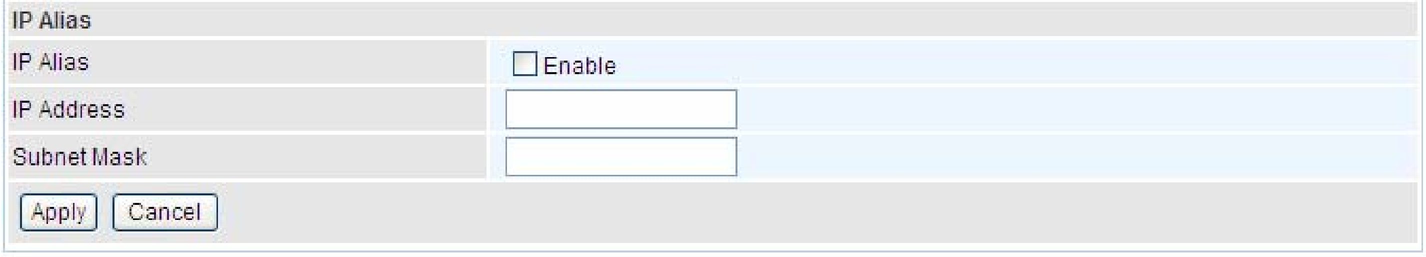


Static IP Lease List

Host Label	MAC Address	IP Address	Remove	Edit
HP	18:a9:05:38:04:05	192.168.1.200	□	Edit

IP Alias

This function allows the creation of multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node.



IP Alias

IP Alias	□ Enable
IP Address	
Subnet Mask	

IP Alias: Check whether to enable this function.

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

Subnet Mask: Specify a subnet mask on this virtual interface.

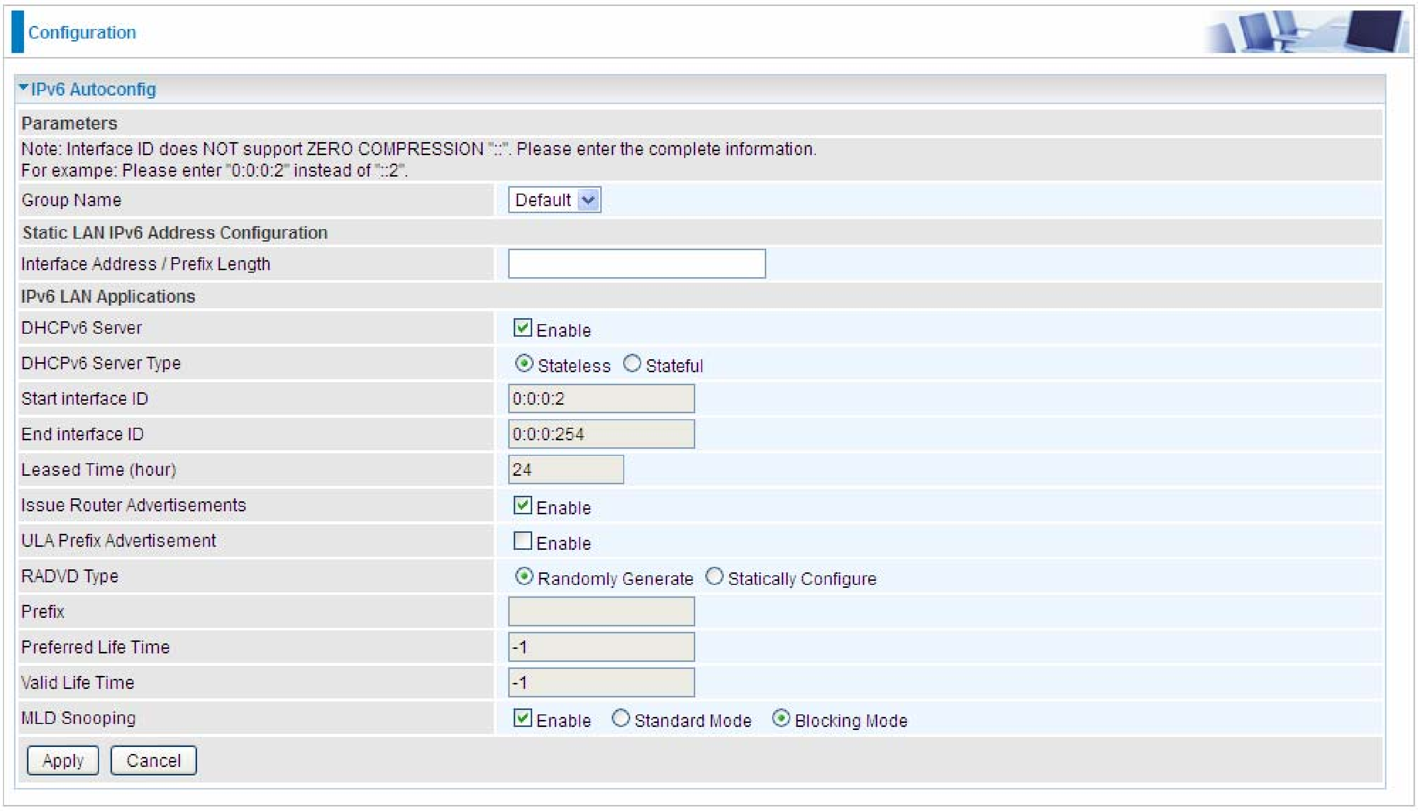
Click **Apply** to apply your settings.

IPv6 Autoconfig

The IPv6 address composes of two parts, the prefix and the interface ID.

There are two ways to dynamically configure IPv6 address on hosts. One is “stateful” configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful auto-configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

The second way is “stateless” configuration. Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn’t configure anything on the client.



Parameters

Note: Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.
For exampe: Please enter "0:0:0:2" instead of "::2".

Group Name	Default
Static LAN IPv6 Address Configuration	
Interface Address / Prefix Length	
IPv6 LAN Applications	
DHCPv6 Server	☑ Enable
DHCPv6 Server Type	● Stateless ○ Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	☑ Enable
ULA Prefix Advertisement	□ Enable
RADVD Type	● Randomly Generate ○ Statically Configure
Prefix	
Preferred Life Time	-1
Valid Life Time	-1
MLD Snooping	☑ Enable ○ Standard Mode ● Blocking Mode

Group Name: Here group refers to the group you set in **Interface Grouping** section, you can set the parameters for the specific group. Select the group by the drop-down box. For more information please refer to **Interface Grouping** of this manual.

Static LAN IPv6 Address Configuration

Interface Address / Prefix Length: Enter the static LAN IPv6 address.

IPv6 LAN application

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is available. **Stateless:** If selected, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers, but they can obtain such information like DNS from DHCPv6 Server. **Stateful:** if selected, the PCs in LAN will be configured like in IPv4 mode, thus obtain addresses and DNS information from DHCPv6 server.

Start interface ID: Enter the start interface ID. The IPv6 address composed of two parts, thus, the prefix and the interface ID. Interface is like the Host ID compared to IPv4.

End interface ID: Enter the end interface ID.

Note: Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information.
For example: Please enter "0:0:0:2" instead of "::2".

Leased Time (hour): The leased time, similar to leased time in DHCPv4, is a time limit assigned to clients, when expires, the assigned ID will be recycled and reassigned.

Issue Router Advertisement: Check whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically.

ULA Prefix Advertisement: Enable this parameter to include the ipv6 ULA address in the RA messages. ULA, unique local address, is an IPv6 address in the block fc00::/7. It is approximately the IPv6 counterpart of the IPv4 private address. They are not routable in the global IPv6 Internet.

RADVD Type: The way that ULA prefix is generated.

- Randomly Generated
- Statically Configured: select to set manually in the following parameters.

Prefix: Set the prefix manually.

Preferred Life Time: The ULA prefix life time. When the time is over, the ULA prefix is invalid any more, -1 means no limit.

Valid Life Time: It is a time threshold, when the time is over, clients should obtain new IPv6 address from the router through RA; -1 means to be limitless.

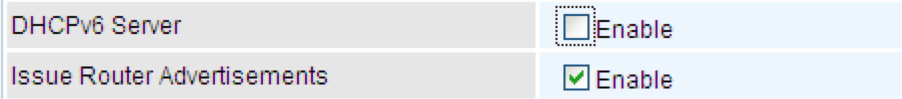
MLD snooping: Similar to IGMP snooping, listens in on the MLD conversation between hosts and routers by processing MLD packets sent in a multicast network, and it analyzes all MLD packets between hosts and the connected multicast routers in the network. Without MLD snooping, multicast traffic is treated in the same manner as broadcast traffic - that is, it is forwarded to all ports. With MLD snooping, multicast traffic of a group is only forwarded to ports that have members of that group.

- **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- **Blocking Mode:** In blocking mode, the multicast data will be blocked when there is no client subscribes to a multicast group, it won’t flood to the bridge ports.

Stateless and Stateful IPv6 address Configuration

Stateless: Two methods can be carried.

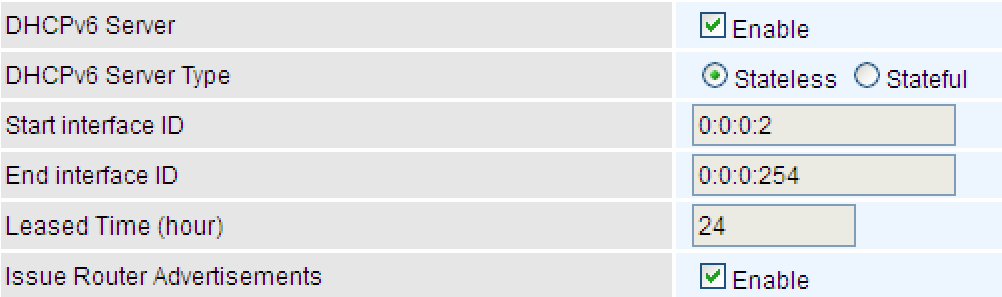
ⓘ With DHCPv6 disabled, but Issue Router Advertisement Enabled



DHCPv6 Server	□ Enable
Issue Router Advertisements	☑ Enable

With this method, the PCs in LAN are configured through RA mode, thus, the PCs in LAN are configured through RA mode, to obtain the prefix message and generate an address using a combination of locally available information (MAC address) and information (prefix) advertised by routers.

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled

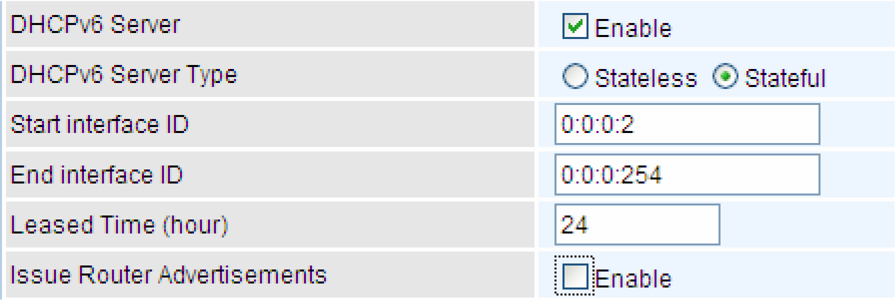


DHCPv6 Server	☑ Enable
DHCPv6 Server Type	● Stateless ○ Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	☑ Enable

With this method, the PCs' addresses in LAN are configured like above method, but they can obtain such information like DNS from DHCPv6 Server.

Stateful: two methods can be adopted.

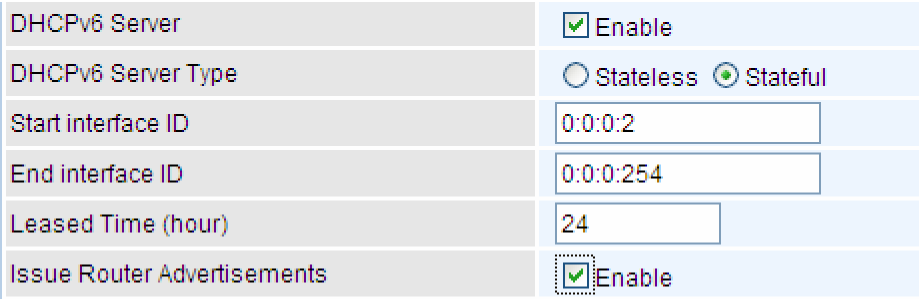
ⓘ With only DHCPv6 enabled



DHCPv6 Server	☑ Enable
DHCPv6 Server Type	○ Stateless ● Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	□ Enable

With this method, the PCs' addresses are configured the same as in IPv4, that is addresses are assigned by DHCPv6 server.

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled



DHCPv6 Server	☑ Enable
DHCPv6 Server Type	○ Stateless ● Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	☑ Enable

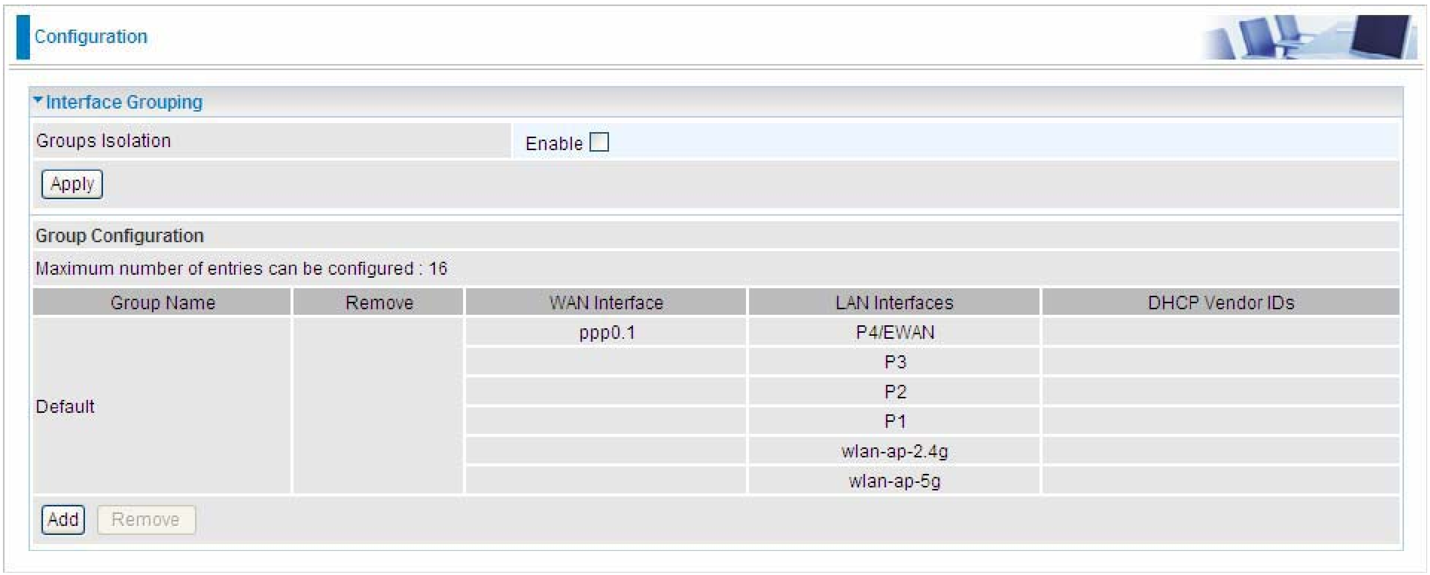
With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

(Please **Note:** P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.)



Groups Isolation Enable □

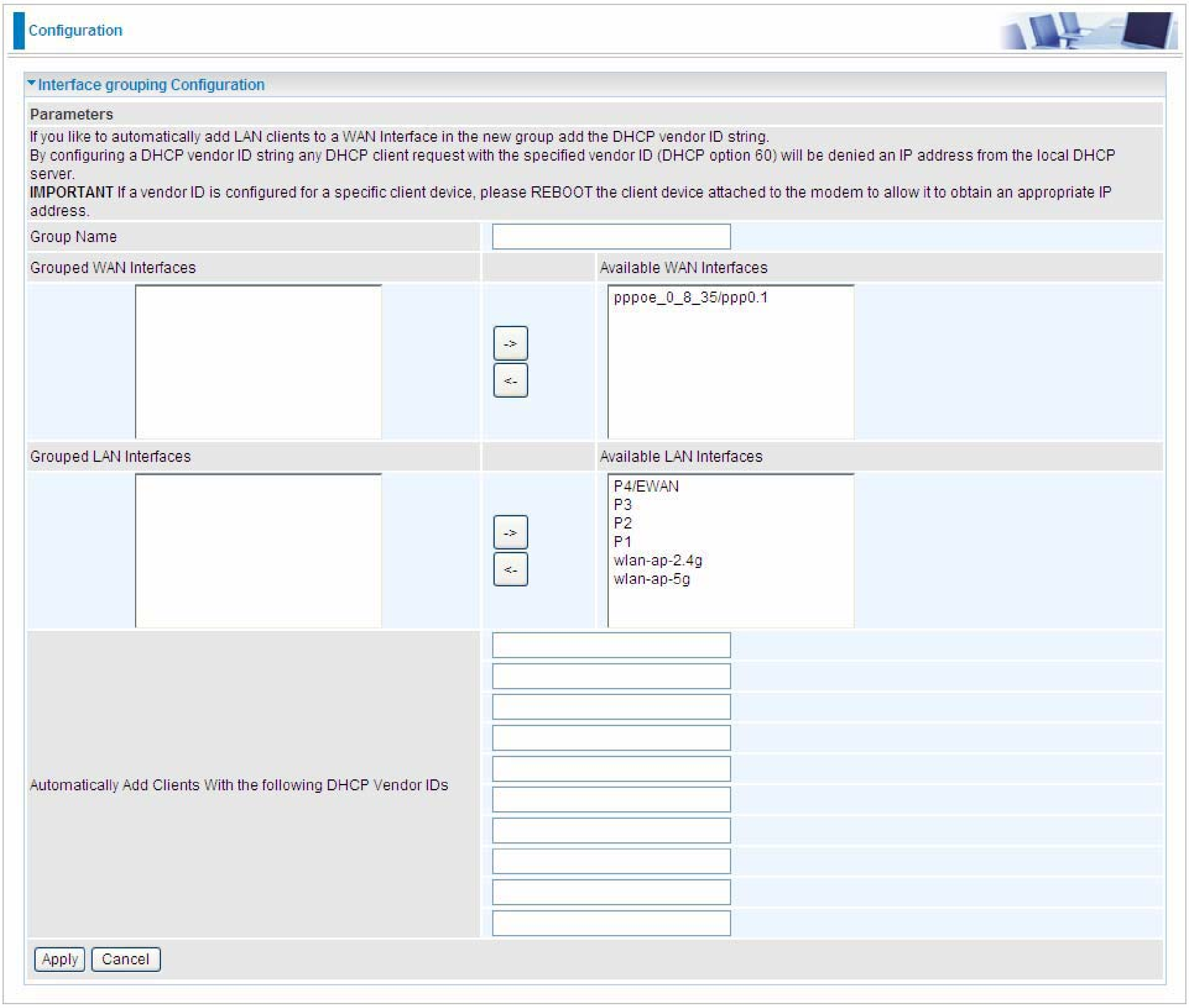
Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	P4/EWAN	
			P3	
			P2	
			P1	
			wlan-ap-2.4g	
			wlan-ap-5g	

Group Isolation: If enabled, devices in one group are not able to access those in the other group.

Click **Add** to add groups.



Configuration

Interface grouping Configuration

Parameters

If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.
By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name

Grouped WAN Interfaces		Available WAN Interfaces
	-> <-	pppoe_0_8_35/ppp0.1

Grouped LAN Interfaces		Available LAN Interfaces
	-> <-	P4/EWAN P3 P2 P1 wlan-ap-2.4g wlan-ap-5g

Automatically Add Clients With the following DHCP Vendor IDs

Group Name: Type a group name.

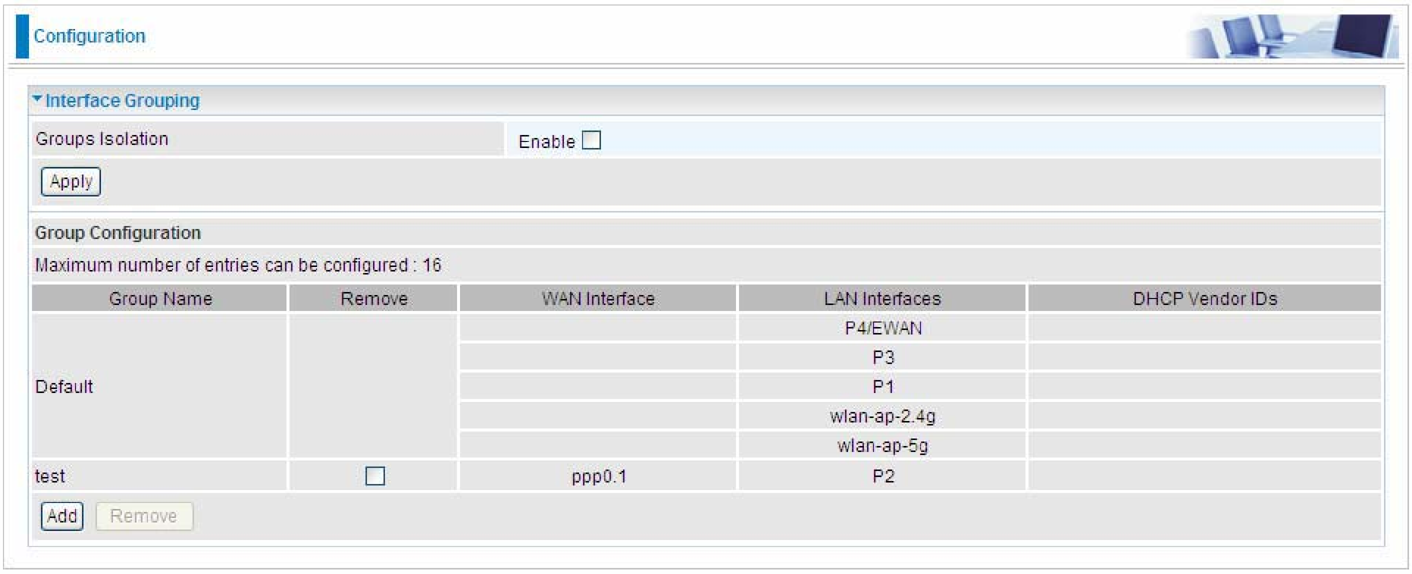
Grouped WAN Interfaces: Select from the box the WAN interface you want to applied in the group.

Grouped LAN Interfaces: Select the LAN interfaces you want to group as a single group from ***Available LAN Interfaces***.

Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

Click **Apply** to confirm your settings and your added group will be listed in the Interface Grouping table below.

In group "test", P2 and PPP0.1 are grouped in one group, they have their only network , see LAN.



Configuration

▾Interface Grouping

Groups Isolation   Enable □

Apply

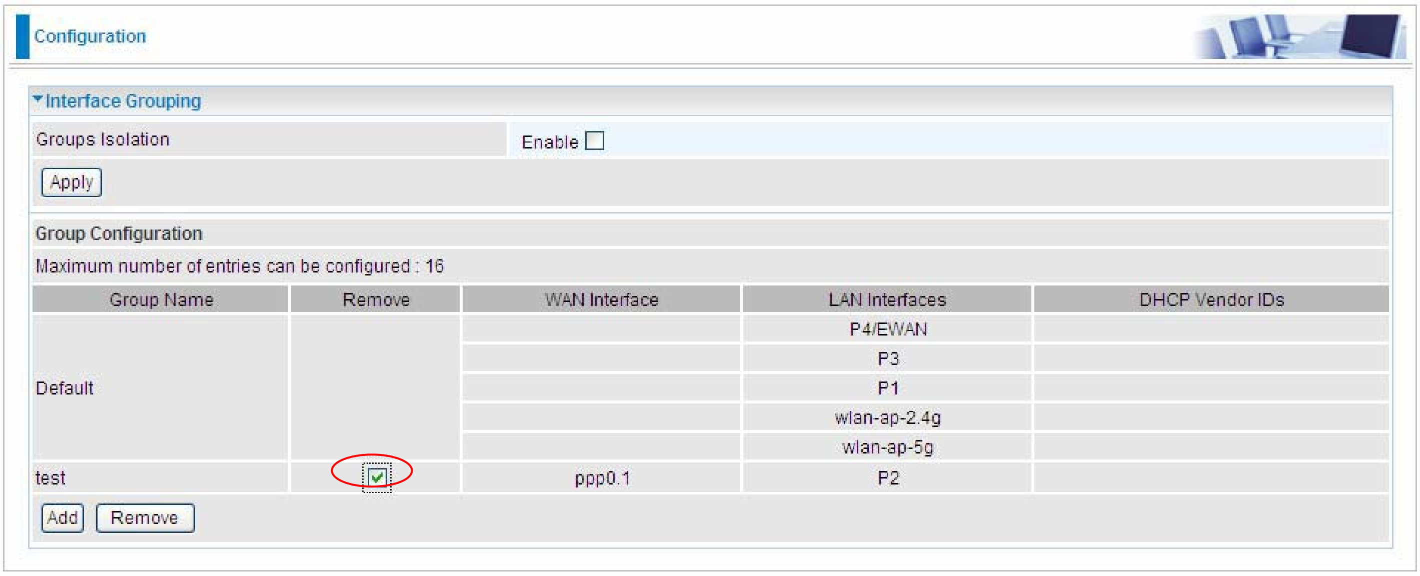
Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P4/EWAN	
			P3	
			P1	
			wlan-ap-2.4g	
			wlan-ap-5g	
test	□	ppp0.1	P2	

Add   Remove

If you want to remove the group, check the box as the following and press **Remove**.



Configuration

▾Interface Grouping

Groups Isolation   Enable □

Apply

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default			P4/EWAN	
			P3	
			P1	
			wlan-ap-2.4g	
			wlan-ap-5g	
test	☑	ppp0.1	P2	

Add   Remove

Note: If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string.

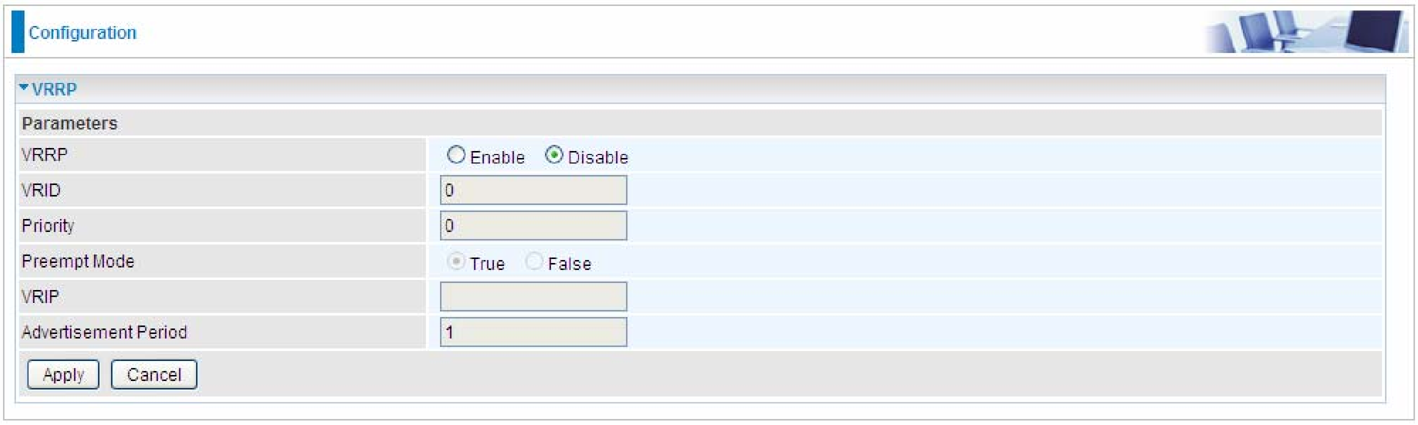
By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Each LAN interface can only be added into one group and one WAN interface can only be used in one group.

VRRP

VRRP is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers in a LAN. The VRRP router controlling the IP address associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses in a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.



VRRP	○ Enable ● Disable
VRID	0
Priority	0
Preempt Mode	● True ○ False
VRIP	
Advertisement Period	1

VRRP: Check Enable radio button to activate this function. The default setting is “Disable”.

VRID: A master or backup router running the VRRP protocol may participate in one VRID instance.

Priority: Specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. The priority value for the VRRP router that owns the IP address associated with the virtual router MUST be 255. VRRP routers backing up a virtual router MUST use priority values between 1 and 254. The default priority value for VRRP routers backing up a virtual router is 100. The priority value zero (0) has special meaning indicating that the current Master has stopped participating in VRRP. This is used to trigger Backup routers to quickly transition to Master without having to wait for the current Master to timeout.

Preempt Mode: When preempt mode is enabled, a backup router always takes over the responsibility of the master router. When disabled, the lower priority backup is left in the master state.

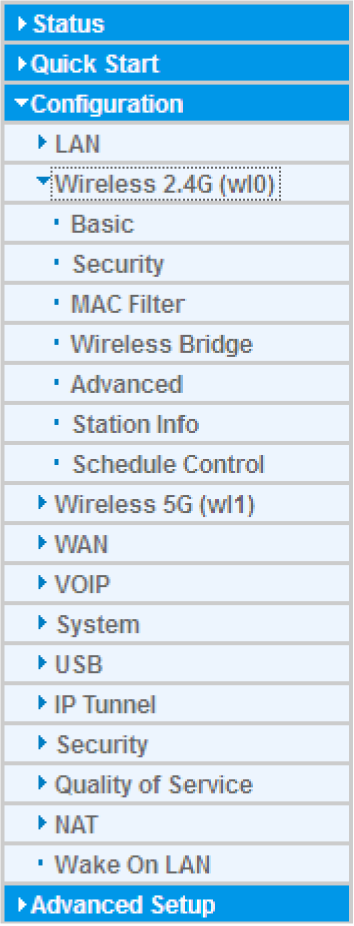
VRIP: One IP address that is associated with the virtual router.

Advertisement period: Indicates the time interval in seconds between advertisements. The default value is 1 second.

Wireless 2.4G(wl0)

This section provides you ways to configure wireless access. The BiPAC 7800VDP(O)X utilizes two radio bands-2.4GHz and 5GHz simultaneously, to run wireless connection for users. Wl0, operating on 2.4GHz, has sub-items as **Basic**, **Security**, **MAC Filter**, **Wireless Bridge**, **Advanced**, **Station Info** and **Schedule Control** here. Wl1, running on 5GHz, are to set with the same ways as in Wl0.

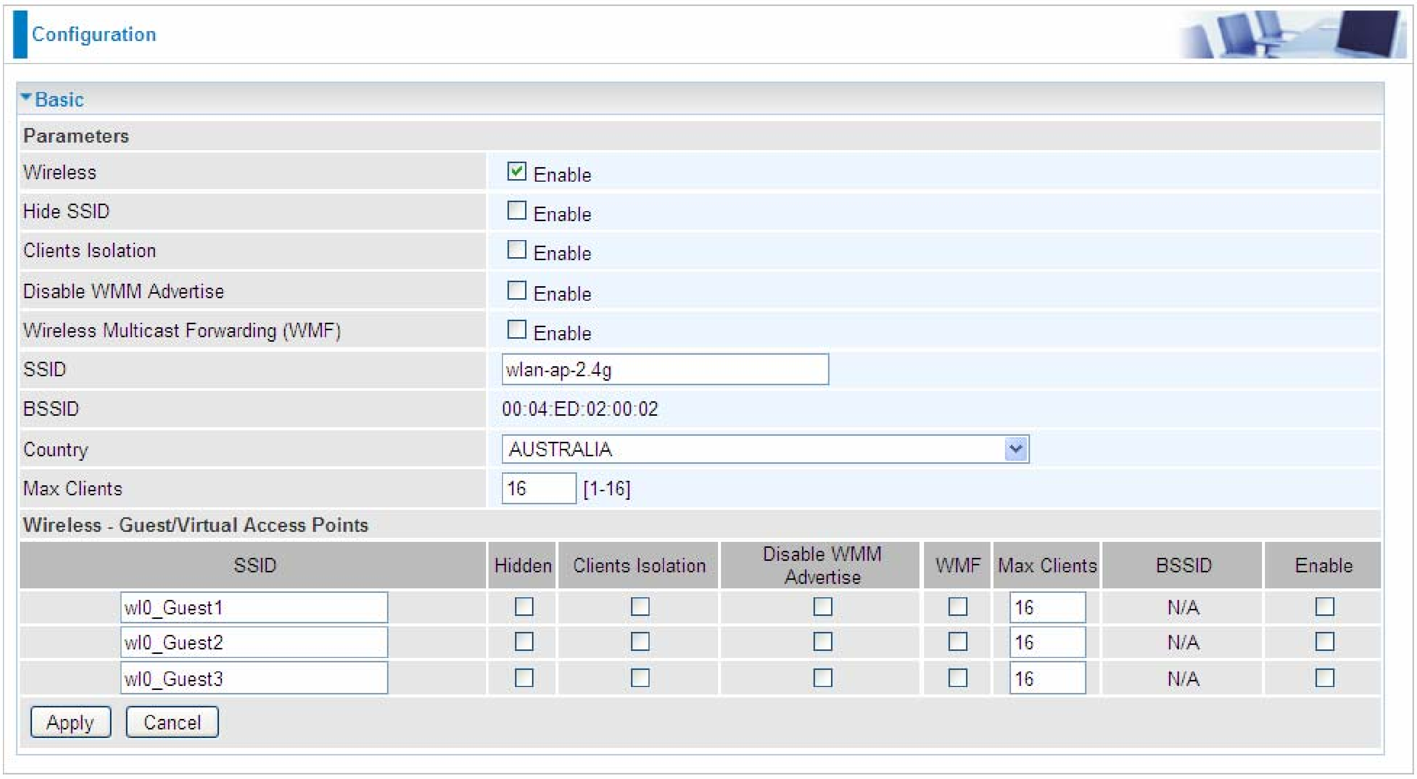
Note: The dual-band wireless is simultaneous with different clients, not the same one. Users can freely choose the optimum radio band wireless connection base on your environment.



(7800VDOX)

Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs.



Configuration

▾Basic

Parameters	
Wireless	☑ Enable
Hide SSID	□ Enable
Clients Isolation	□ Enable
Disable WMM Advertise	□ Enable
Wireless Multicast Forwarding (WMF)	□ Enable
SSID	wlan-ap-2.4g
BSSID	00:04:ED:02:00:02
Country	AUSTRALIA
Max Clients	16 [1-16]

Wireless - Guest/Virtual Access Points

SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
wl0_Guest1	□	□	□	□	16	N/A	□
wl0_Guest2	□	□	□	□	16	N/A	□
wl0_Guest3	□	□	□	□	16	N/A	□

Apply Cancel

Wireless: Default setting is set to Enable. If you do not have any wireless devices, check the checkbox again to unselect.

Hide SSID: It is function in which transmits its SSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Check the checkbox to determine whether you want to hide SSID.

Clients Isolation: If you enabled this function, then each of your wireless clients will not be able to communicate with each other.

Disable WMM Advertise: Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video).

Check to disable or enable this function.

Wireless multicast Forwarding (WMF): check to enable or disable wireless multicast forwarding.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap-2.4g to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

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

BSSID: Basic Set Service Identifier, it is a local managed IEEE MAC address, and is 48 bits value.

Country: Different countries have different wireless band resources, so you can select the appropriate Country according to your location.

Max Clients: enter the number of max clients the wireless network can supports,1-16.

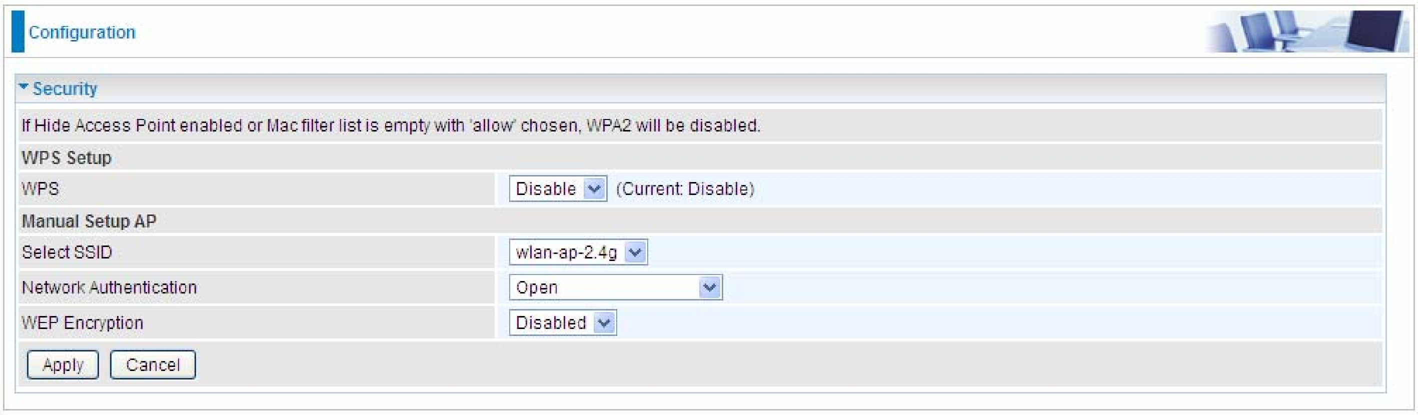
Guest/virtual Access Points: A "Virtual Access Point" is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple "Virtual APs", each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Here you can enable some Virtual APs according to the request. And the other parameters of virtual APs are the same to the above.

Click **Apply** to apply your settings.

Security

Wireless security prevents unauthorized access or damage to computers using wireless network.



▾ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup	
WPS	Disable (Current: Disable)
Manual Setup AP	
Select SSID	wlan-ap-2.4g
Network Authentication	Open
WEP Encryption	Disabled

Note：

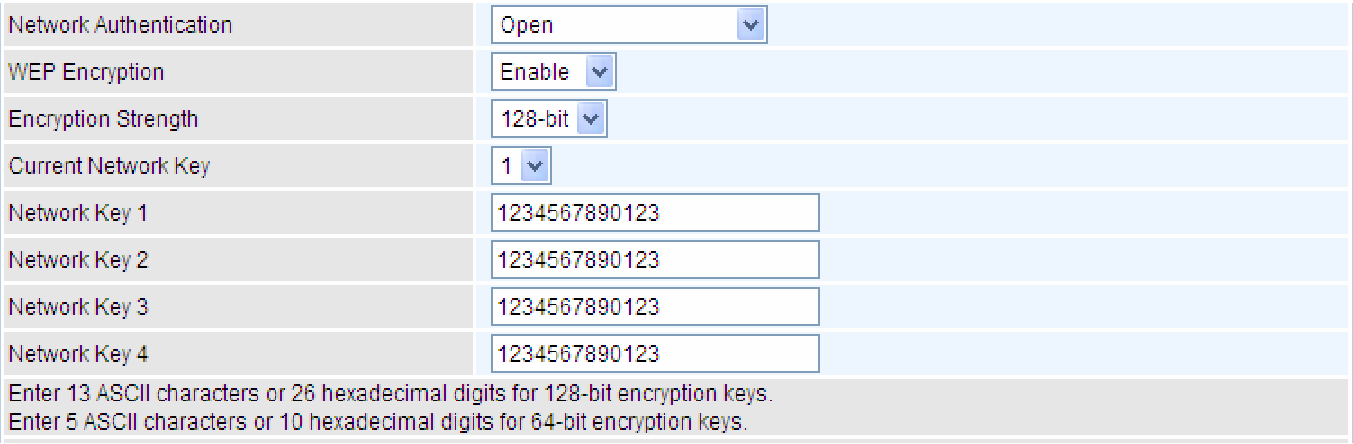
The WPS feature will also be unavailable when the security setting is not WPA2 or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

Manual Setup AP

Select SSID: select the SSID you want these settings apply to.

Network Authentication

① **Open**



Network Authentication	Open
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	1
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

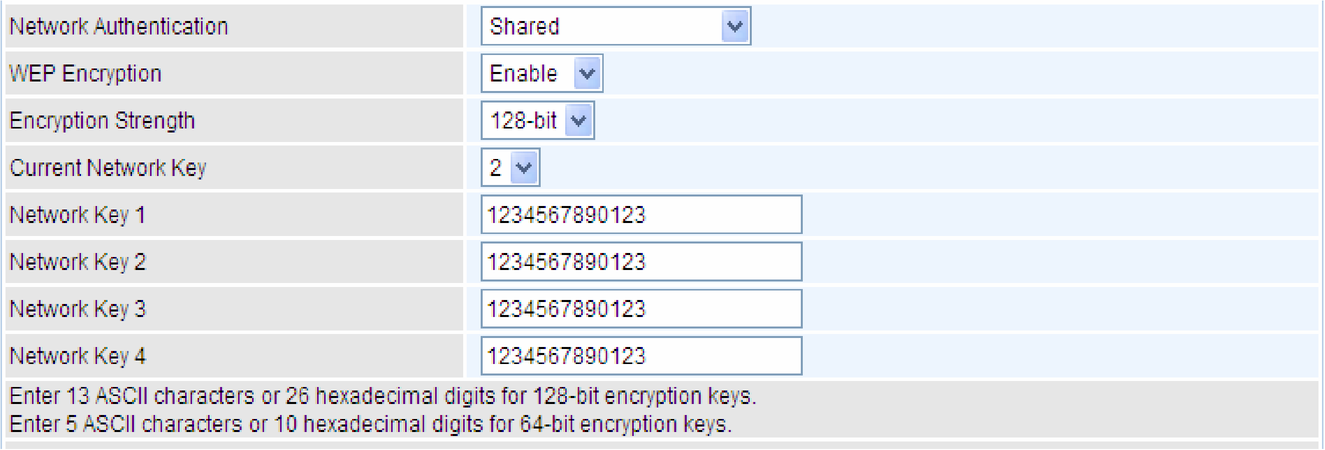
Encryption Strength: Select the strength, 128-bit or 64-bit.

Current Network Key: Select the one to be the current network key. Please refer to key 1- 4 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Shared

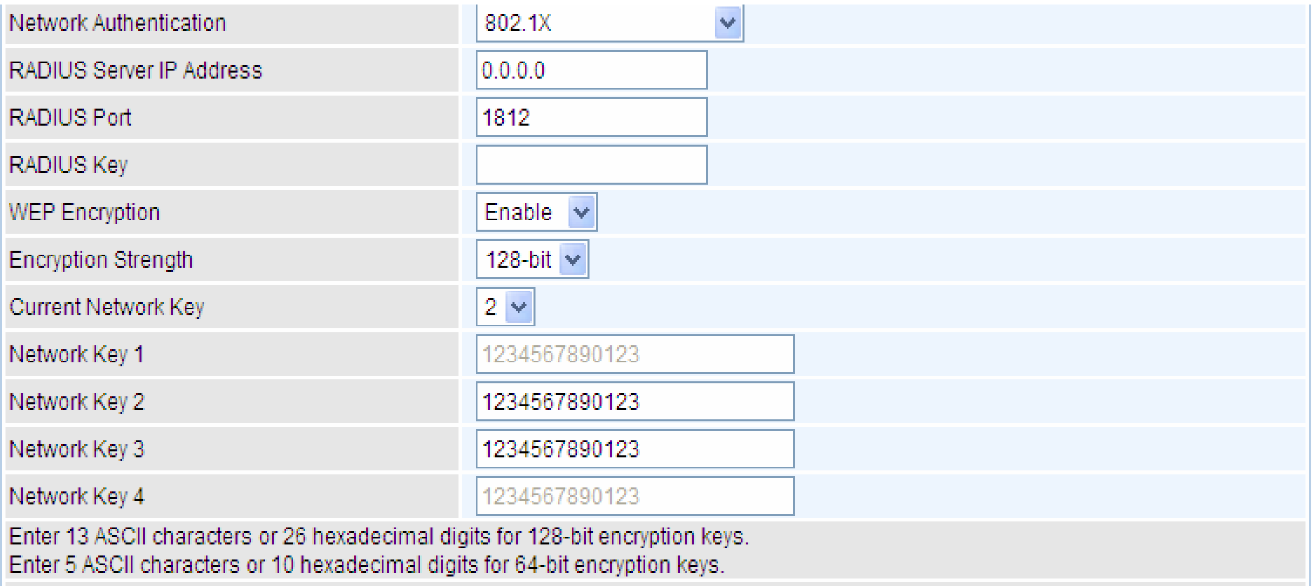
This is similar to network authentication ‘Open’. But here the WEP Encryption must be enabled.



Network Authentication	Shared
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

802.1x



Network Authentication	802.1X
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys.
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

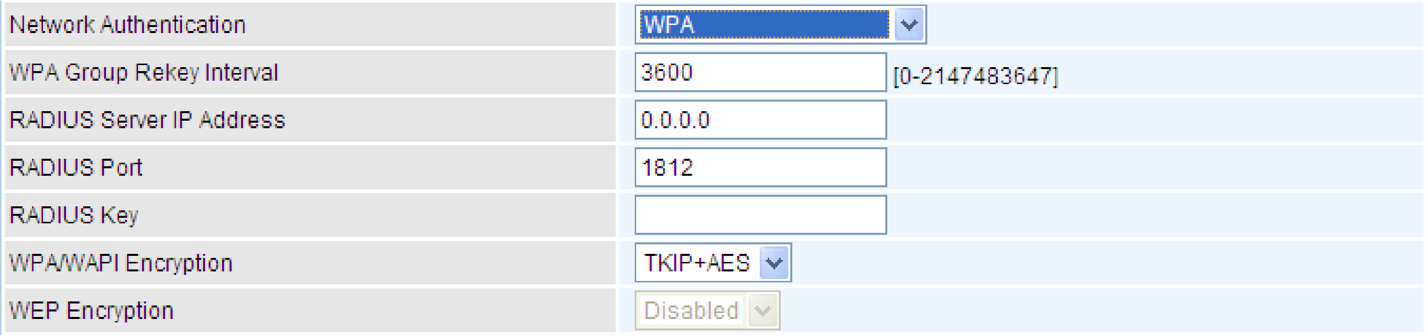
RADIUS Key: Enter the password of RADIUS authentication server.

WEP Encryption: Select to enable or disable WEP Encryption. Here select Enable.

Current Network Key: Select the one to be the current network key. Please refer to key 2- 3 below.

Network Key (1- 4): Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

WPA



Network Authentication	WPA
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	TKIP+AES
WEP Encryption	Disabled

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

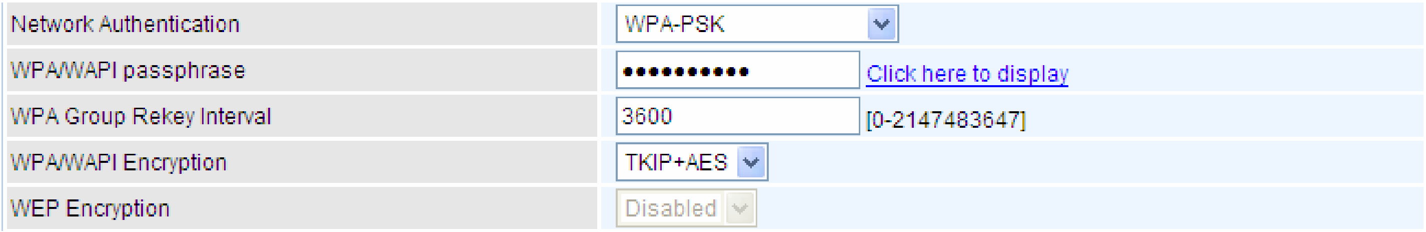
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPA-PSK / WPA2-PSK



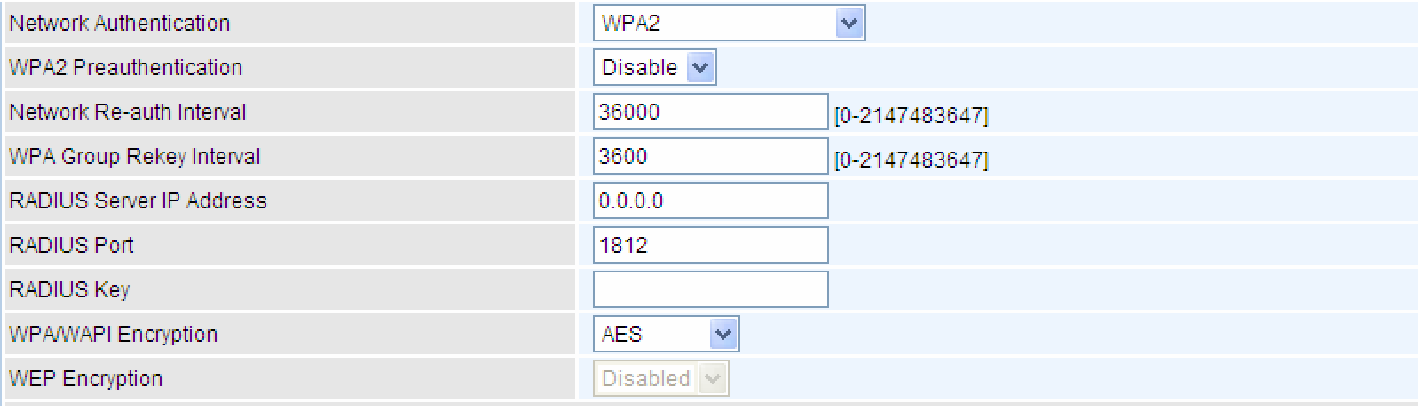
Network Authentication	WPA-PSK
WPA/WAPI passphrase	•••••••••• Click here to display
WPA Group Rekey Interval	3600 [0-2147483647]
WPA/WAPI Encryption	TKIP+AES
WEP Encryption	Disabled

WPA/WAPI passphrase: Enter the WPA.WAPI passphrase; you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPA2



Network Authentication	WPA2
WPA2 Preauthentication	Disable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentication to the new AP, and when handoff happens, this mode will help reduce the association time.

Network Re-auth Interval: the interval for network Re-authentication. This is in seconds.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

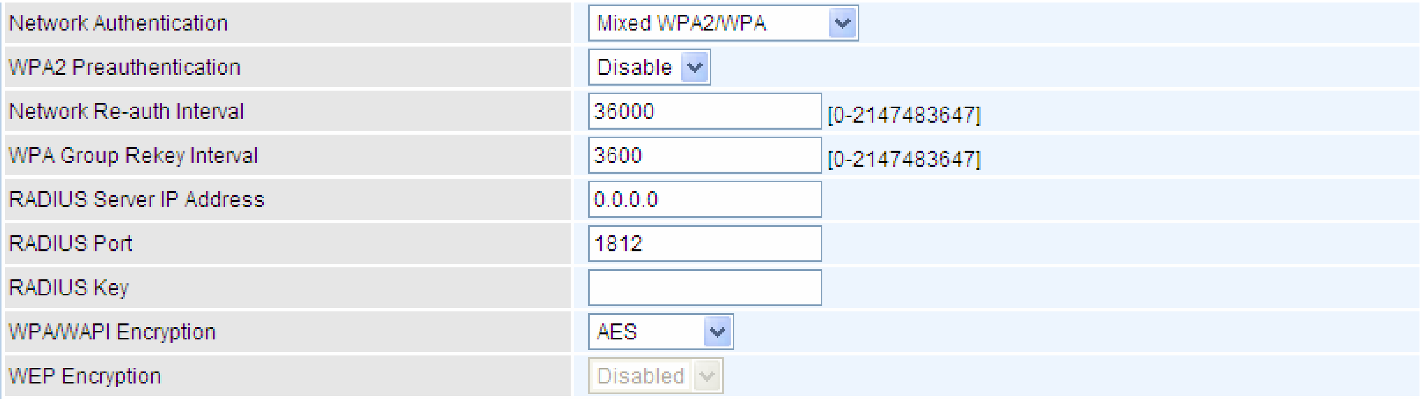
RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server. This is in seconds.

RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

Mixed WPA2/WPA



Network Authentication	Mixed WPA2/WPA
WPA2 Preauthentication	Disable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	3600 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA2 Preauthentication: When a wireless client wants to handoff to another AP, with preauthentication, it can perform 802.1X authentications to the new AP, and when handoff happens, this mode will help reduce the association time used.

Network Re-auth Interval: the interval for network Re-authentication. The unit is second.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

RADIUS Server IP Address: RADIUS(Remote Authentication Dial In User Service), Enter the IP address of RADIUS authentication server.

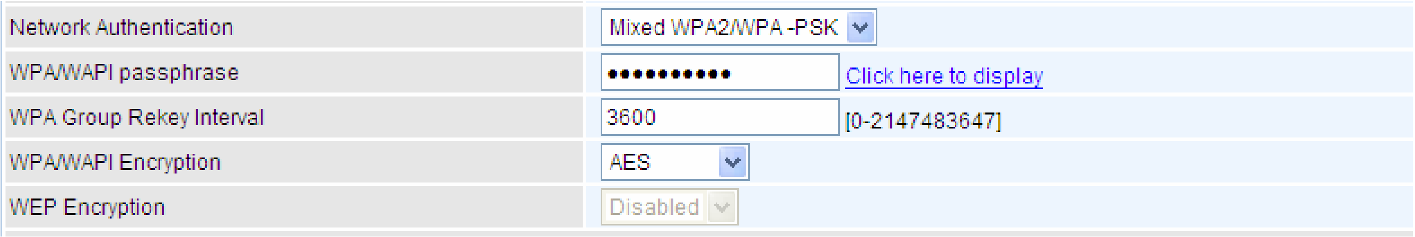
RADIUS Server Port: Enter the port number of RADIUS authentication server here.

RADIUS Key: Enter the password of RADIUS authentication server.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and

TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

ⓘ Mixed WPA2/WPA-PSk



Network Authentication	Mixed WPA2/WPA -PSK
WPA/WAPI passphrase	●●●●●●●●●●● Click here to display
WPA Group Rekey Interval	3600 [0-2147483647]
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

WPA/WAPI passphrase: enter the WPA.WAPI passphrase, you can **click here to display** to view it.

WPA Group ReKey Internal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). The unit is second.

WPA/WAPI Encryption: There are two Algorithms, AES (Advanced Encryption Standard) and TKIP(Temporal Key Integrity Protocol) which help to protect the wireless communication.

WPS Setup

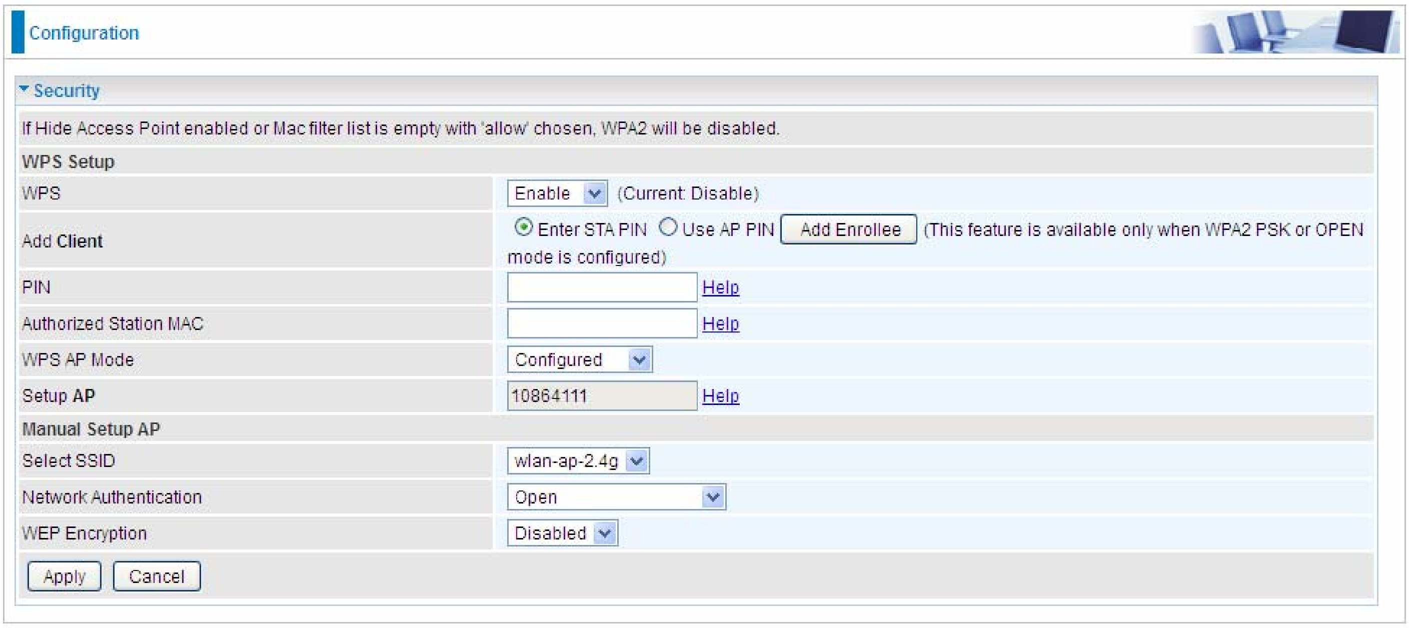
WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure AP settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known **PIN method** is supported to configure WPS.

WPS: Select enable to enable WPS function. Please note that WPS can only be available when WPA2-PSK or OPEN mode is configured.

Note:

1) WPS feature is only available when in WPA2 or OPEN mode in security settings.

2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select "Configured" in the WPS AP Mode below, and default WPS AP Mode is "Configured". When AP is configured as Enrollee, the WPS AP Mode below should be changed to "Unconfigured". Follow the following steps.



Configuration

▾ Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

WPS	Enable ▾ (Current: Disable)
Add Client	● Enter STA PIN ○ Use AP PIN [Add Enrollee] (This feature is available only when WPA2 PSK or OPEN mode is configured)
PIN	Help
Authorized Station MAC	Help
WPS AP Mode	Configured ▾
Setup AP	10864111 Help

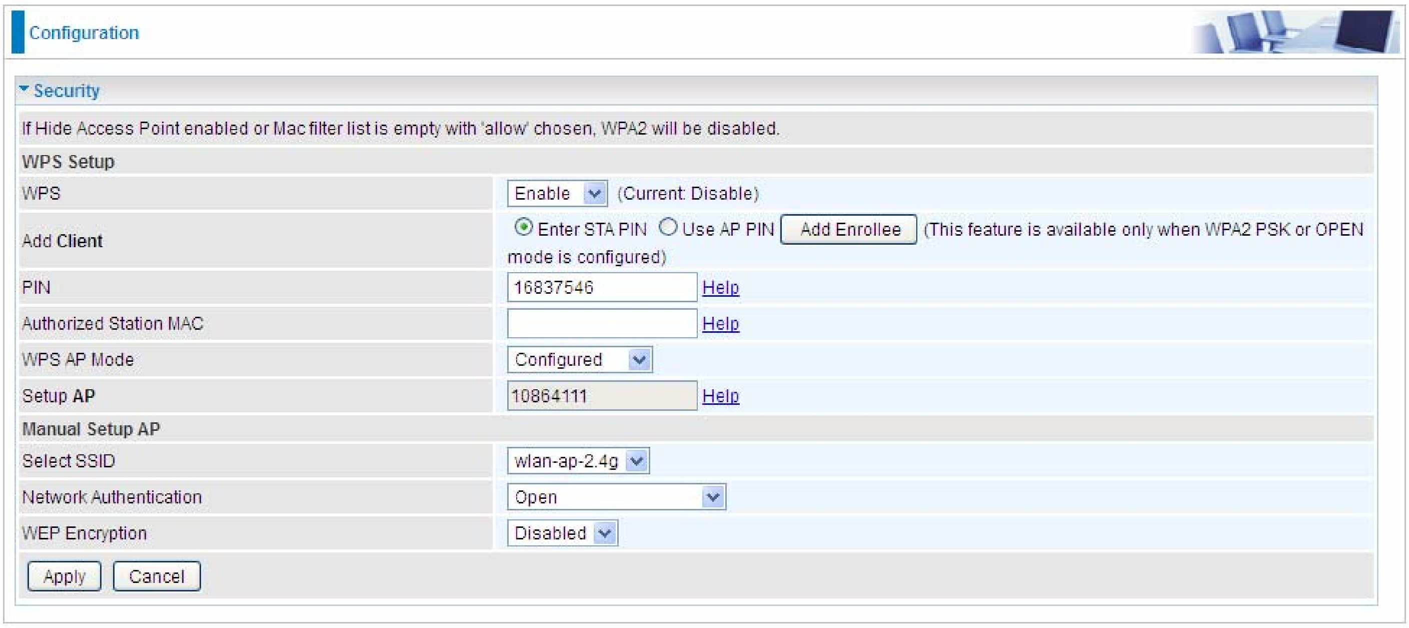
Manual Setup AP

Select SSID	wlan-ap-2.4g ▾
Network Authentication	Open ▾
WEP Encryption	Disabled ▾

Configure AP as Registrar

Add Enrollee with PIN method

1. Select radio button “***Enter STA PIN***”.
2. Input PIN from Enrollee Station (16837546 in this example), Or else users can **alternatively** enter the authorized station MAC ***Help:*** it is to help users to understand the concept and correct operation.
3. Click Add Enrolee .



Configuration

Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

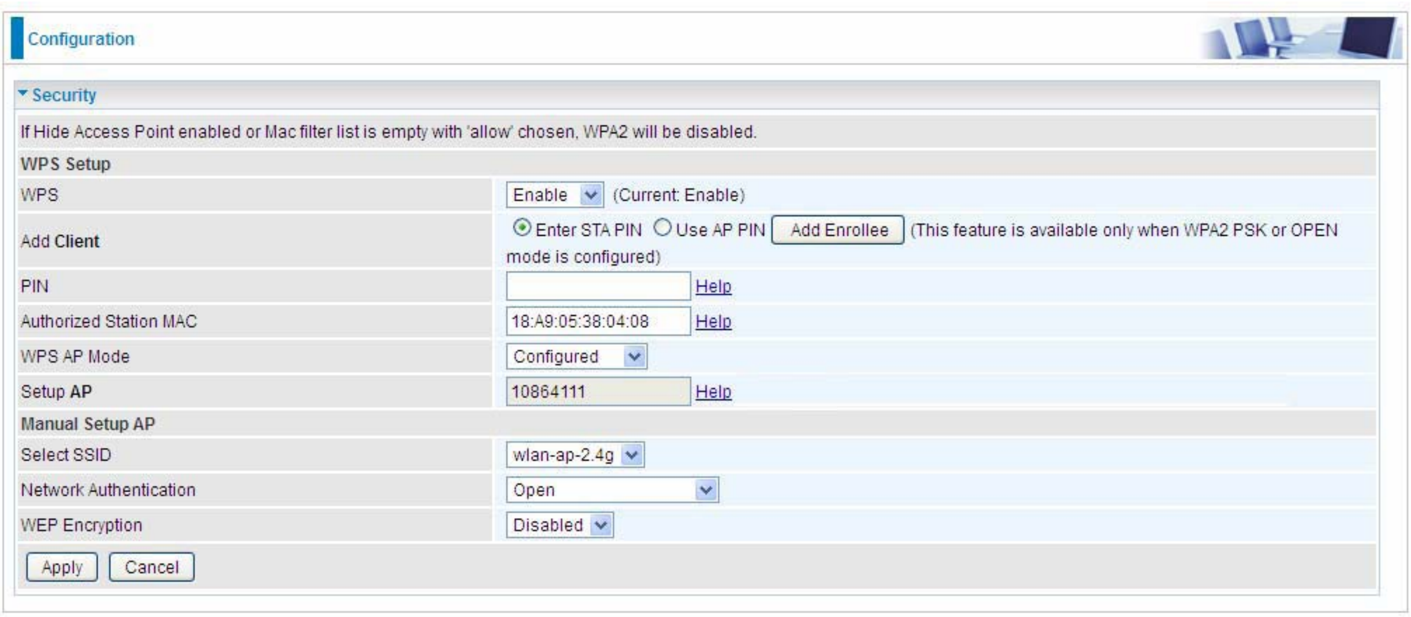
WPS	Enable (Current: Disable)
Add Client	● Enter STA PIN ○ Use AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)
PIN	16837546 Help
Authorized Station MAC	Help
WPS AP Mode	Configured
Setup AP	10864111 Help

Manual Setup AP

Select SSID	wlan-ap-2.4g
Network Authentication	Open
WEP Encryption	Disabled

Apply Cancel

(Station PIN)



Configuration

Security

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

WPS Setup

WPS	Enable (Current: Enable)
Add Client	● Enter STA PIN ○ Use AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)
PIN	Help
Authorized Station MAC	18:A9:05:38:04:08 Help
WPS AP Mode	Configured
Setup AP	10864111 Help

Manual Setup AP

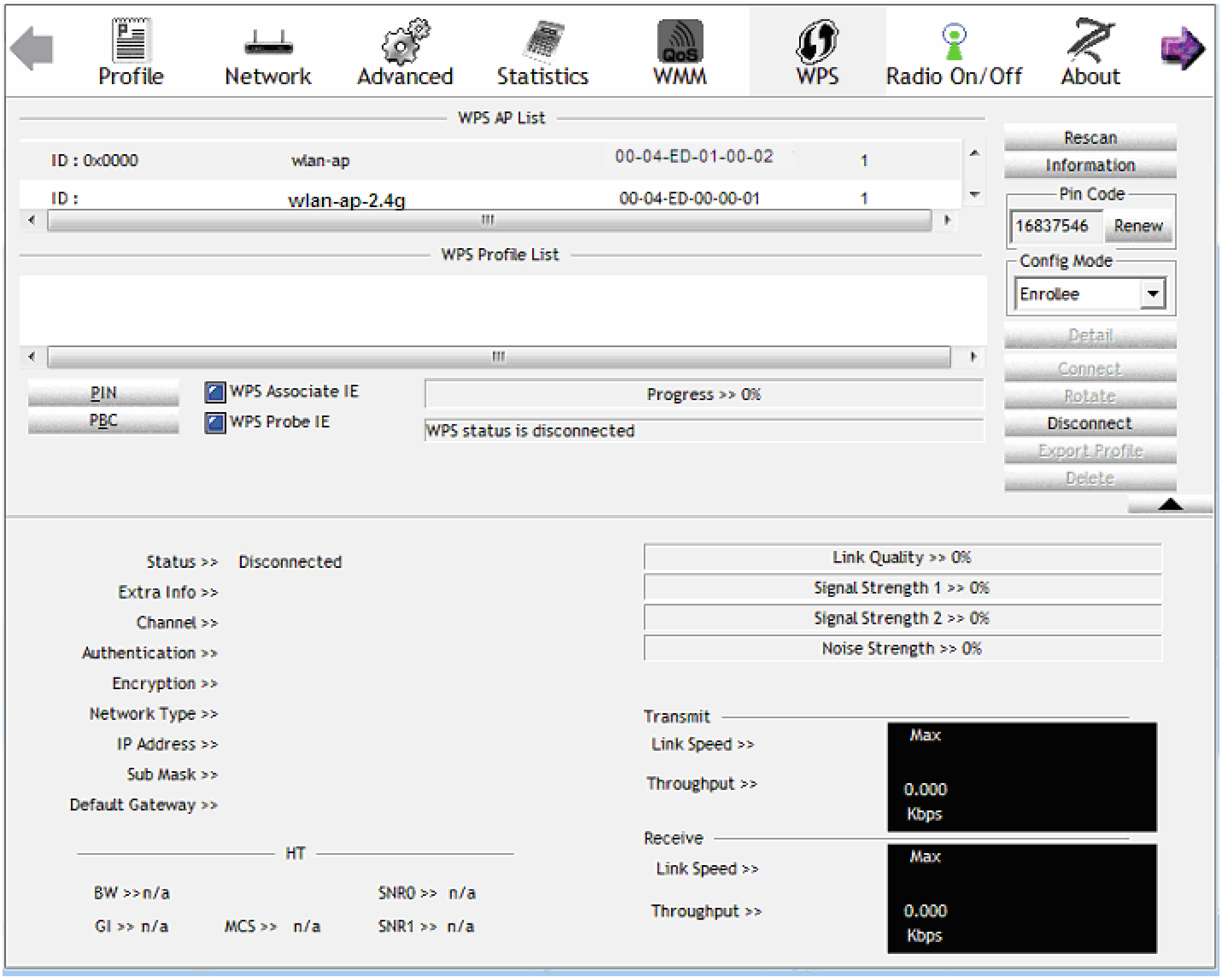
Select SSID	wlan-ap-2.4g
Network Authentication	Open
WEP Encryption	Disabled

Apply Cancel

(Station MAC)

Note: Users can **alternatively** input PIN from Enrollee Station or enter the authorized station MAC.

4. Operate Station to start WPS Adding Enrollee. Launch the wireless client's WPS utility (eg.Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. Wlan-ap-2.4g) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



WPS AP List

ID : 0x0000	wlan-ap	00-04-ED-01-00-02	1
ID :	wlan-ap-2.4g	00-04-ED-00-00-01	1

WPS Profile List

Pin Code: 16837546

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

WPS status is disconnected

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit

Link Speed >>

Throughput >>

Max

0.000 Kbps

Receive

Link Speed >>

Throughput >>

Max

0.000 Kbps

HT

BW >>n/a

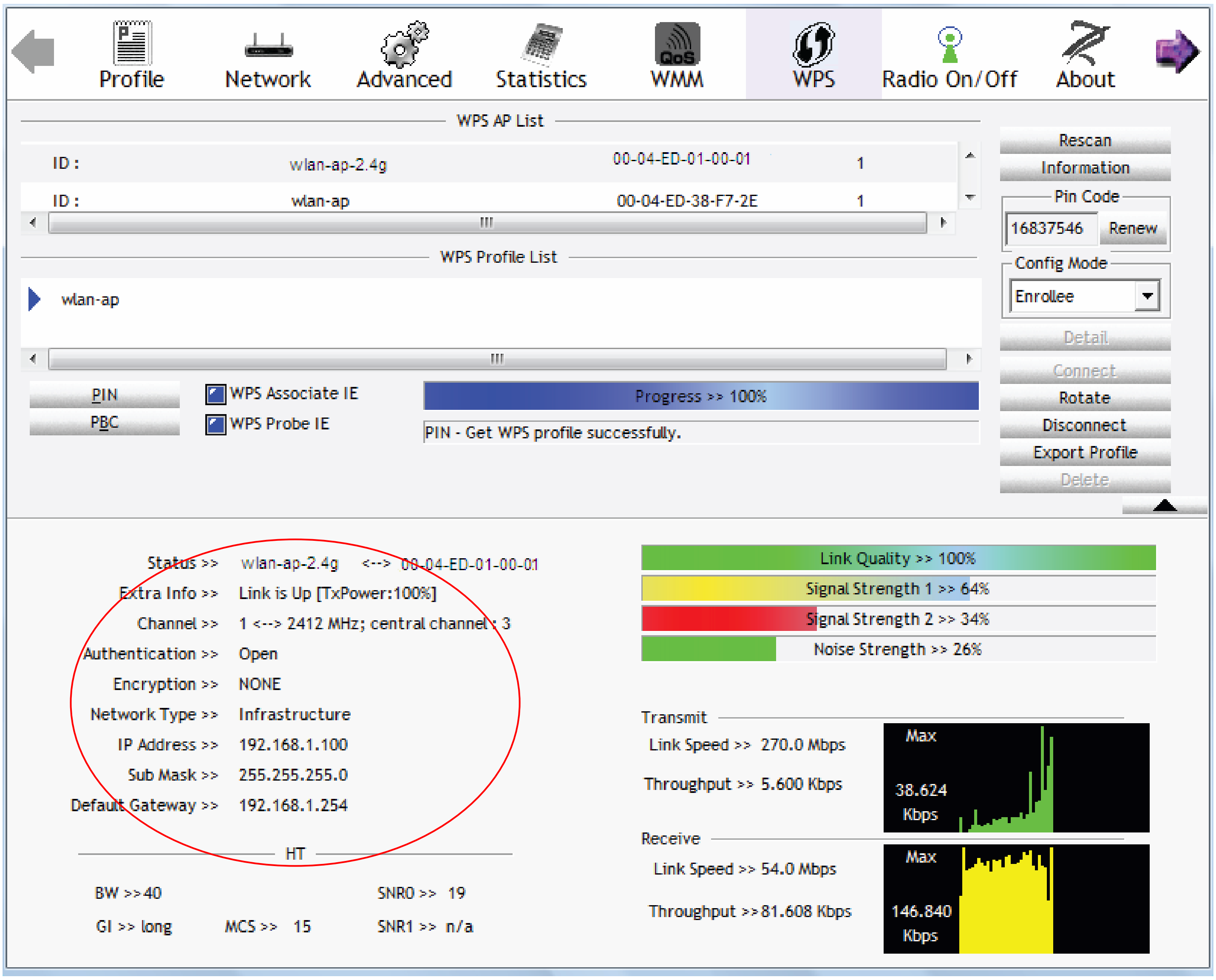
GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

4. The client's SSID and security settings will now be configured to match the SSID and security settings of the registrar.



WPS AP List

ID : wlan-ap-2.4g 00-04-ED-01-00-01 1

ID : wlan-ap 00-04-ED-38-F7-2E 1

Pin Code: 16837546

Config Mode: Enrollee

WPS Profile List

wlan-ap

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Status >> wlan-ap-2.4g <--> 00-04-ED-01-00-01

Extra Info >> Link is Up [TxPower:100%]

Channel >> 1 <--> 2412 MHz; central channel : 3

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 192.168.1.100

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.1.254

BW >> 40

GI >> long MCS >> 15

SNR0 >> 19

SNR1 >> n/a

Link Quality >> 100%

Signal Strength 1 >> 64%

Signal Strength 2 >> 34%

Noise Strength >> 26%

Transmit

Link Speed >> 270.0 Mbps

Throughput >> 5.600 Kbps

Max 38.624 Kbps

Receive

Link Speed >> 54.0 Mbps

Throughput >> 81.608 Kbps

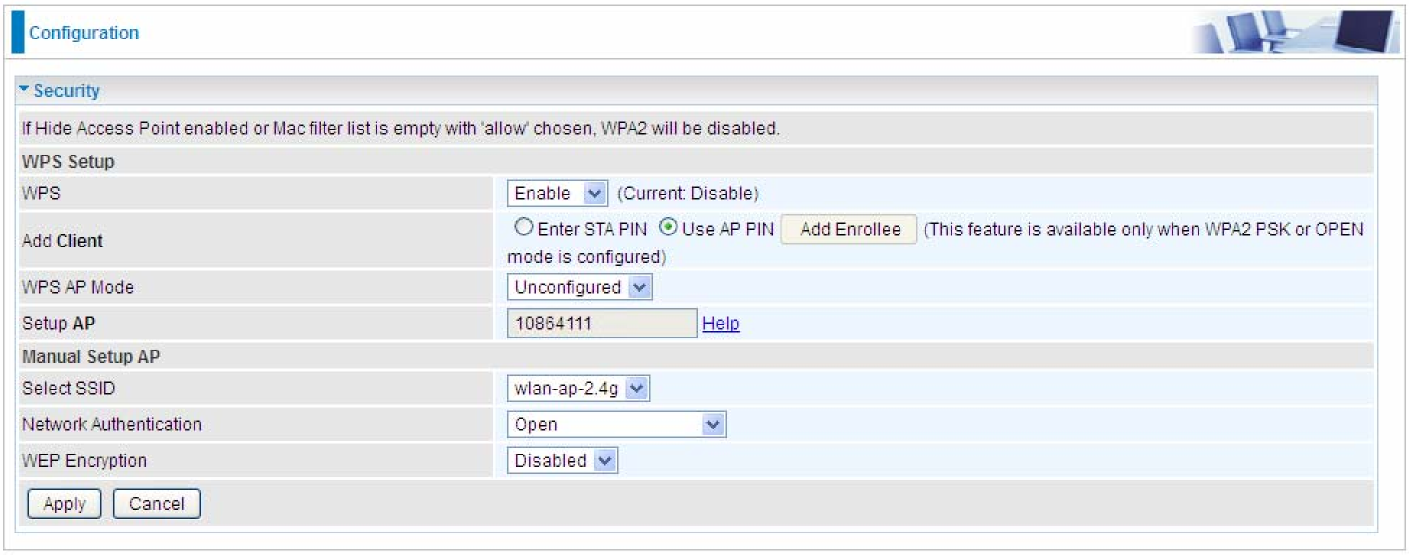
Max 146.840 Kbps

You can check the message in the red ellipse with the security parameters you set, here we all use the default.

Configure AP as Enrollee

Add Registrar with PIN Method

1. Set AP to "***Unconfigured Mode***"



If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.

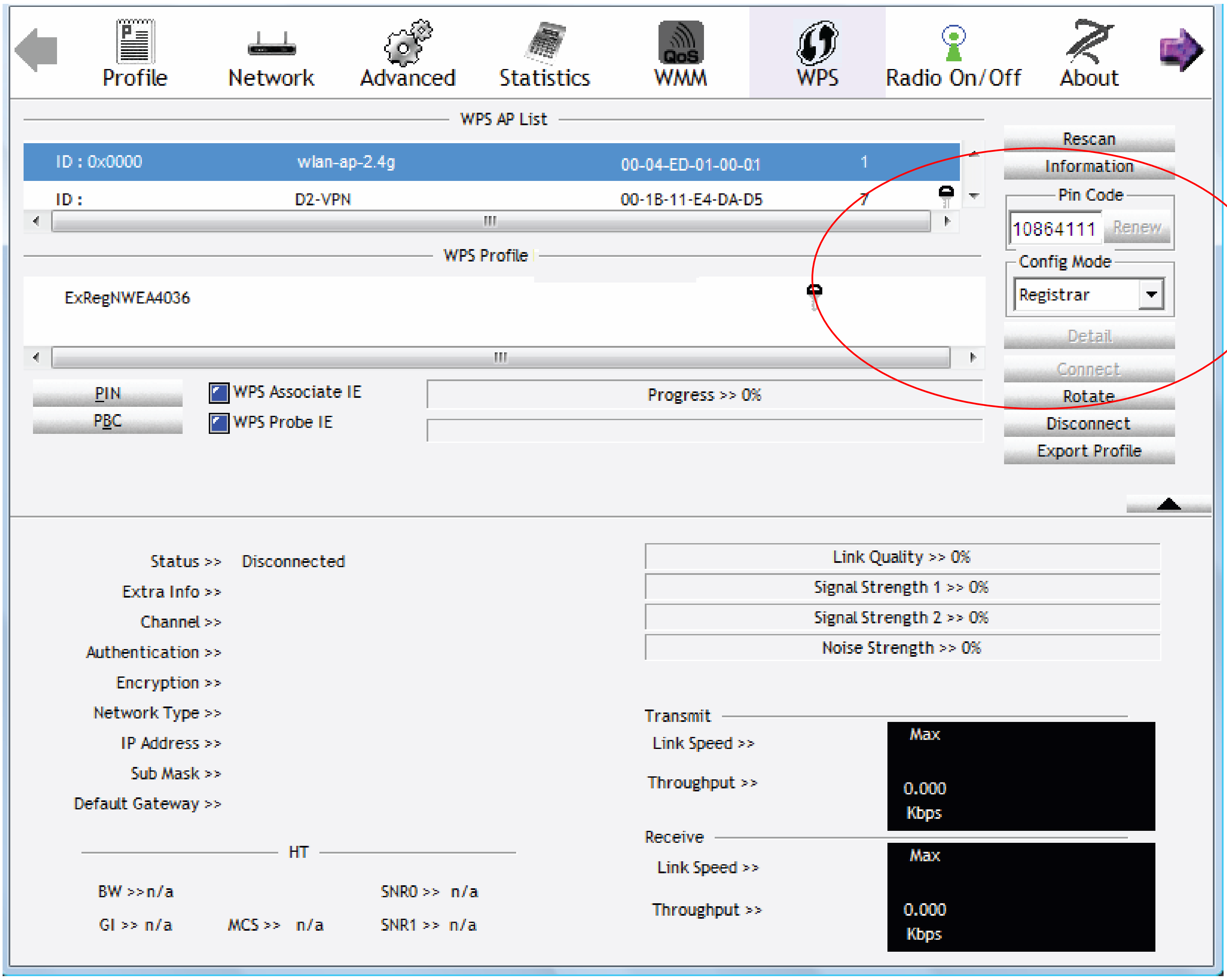
WPS Setup

WPS	Enable (Current: Disable)
Add Client	○ Enter STA PIN ● Use AP PIN Add Enrollee (This feature is available only when WPA2 PSK or OPEN mode is configured)
WPS AP Mode	Unconfigured
Setup AP	10864111 Help

Manual Setup AP

Select SSID	wlan-ap-2.4g
Network Authentication	Open
WEP Encryption	Disabled

2. Launch the wireless client’s WPS utility (eg. Ralink Utility). Set the Config Mode as **Registrar**. Enter the **PIN** number (13076542 (device) for example) in the PIN Code column then choose the correct AP (eg. wlan-ap-2.4g) from the WPS AP List section before pressing the PIN button to run the scan.



WPS AP List

ID : 0x0000	wlan-ap-2.4g	00-04-ED-01-00-01	1
ID :	D2-VPN	00-1B-11-E4-DA-D5	7

Pin Code: 10864111

Config Mode: Registrar

WPS Profile

ExRegNWEA4036

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

Status >> Disconnected

Extra Info >>

Channel >>

Authentication >>

Encryption >>

Network Type >>

IP Address >>

Sub Mask >>

Default Gateway >>

HT

BW >>n/a

GI >> n/a

MCS >> n/a

SNR0 >> n/a

SNR1 >> n/a

Link Quality >> 0%

Signal Strength 1 >> 0%

Signal Strength 2 >> 0%

Noise Strength >> 0%

Transmit

Link Speed >>

Throughput >>

Max

0.000 Kbps

Receive

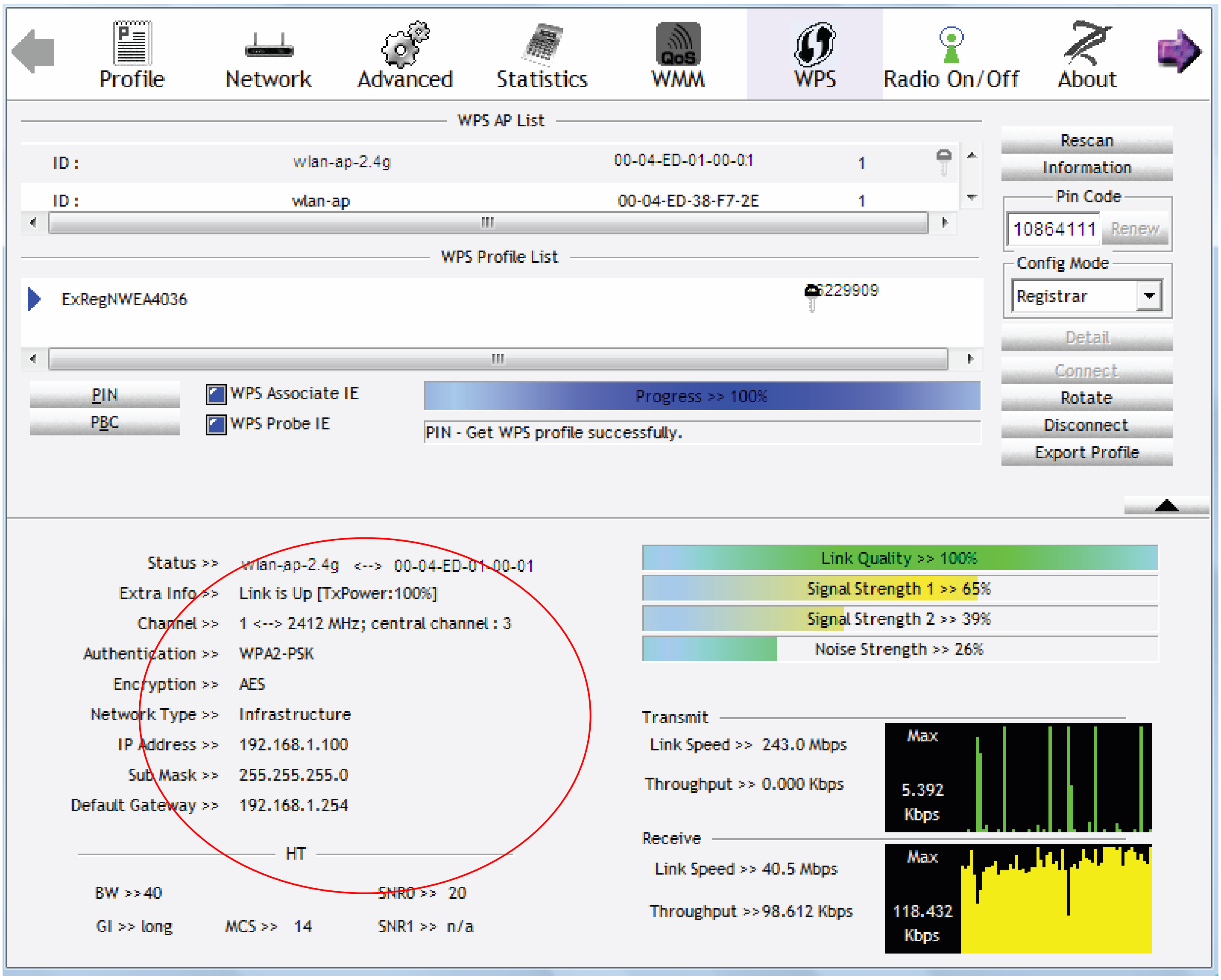
Link Speed >>

Throughput >>

Max

0.000 Kbps

3. The router's (AP's) SSID and security setting will now be configured to match the SSID and security setting of the registrar.



WPS AP List

ID :	wlan-ap-2.4g	00-04-ED-01-00-01	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1

Pin Code: 10864111

Config Mode: Registrar

WPS Profile List

ExRegNWEA4036 8229909

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

Status >> wlan-ap-2.4g <--> 00-04-ED-01-00-01
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 3
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.1.100
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.254

HT

BW >> 40 SNR0 >> 20
GI >> long MCS >> 14 SNR1 >> n/a

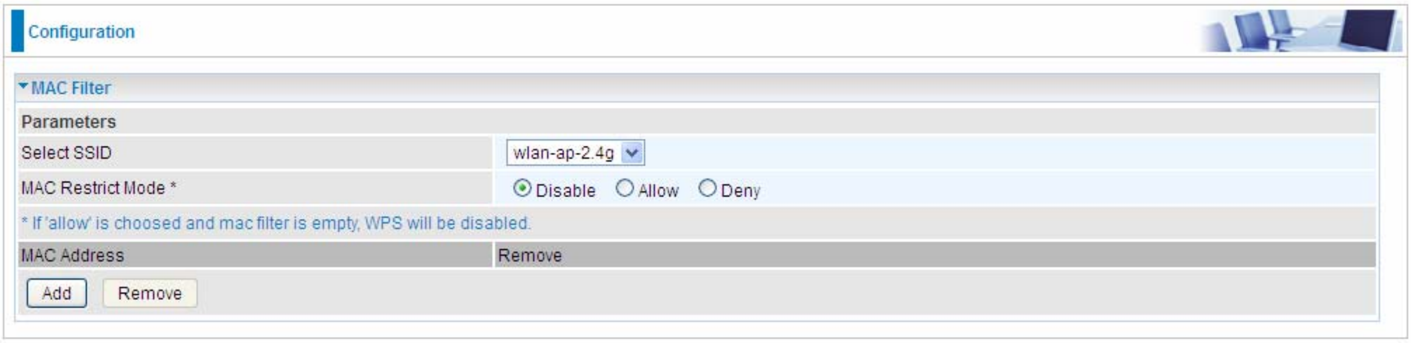
Link Quality >> 100%
Signal Strength 1 >> 65%
Signal Strength 2 >> 39%
Noise Strength >> 26%

Transmit
Link Speed >> 243.0 Mbps
Throughput >> 0.000 Kbps
Max 5.392 Kbps

Receive
Link Speed >> 40.5 Mbps
Throughput >> 98.612 Kbps
Max 118.432 Kbps

4. Do Web Page refresh after ER complete AP Configuration to check the new parameters setting.

MAC Filter



Configuration

MAC Filter

Parameters

Select SSID	wlan-ap-2.4g
MAC Restrict Mode *	● Disable ○ Allow ○ Deny

* If 'allow' is choosed and mac filter is empty, WPS will be disabled.

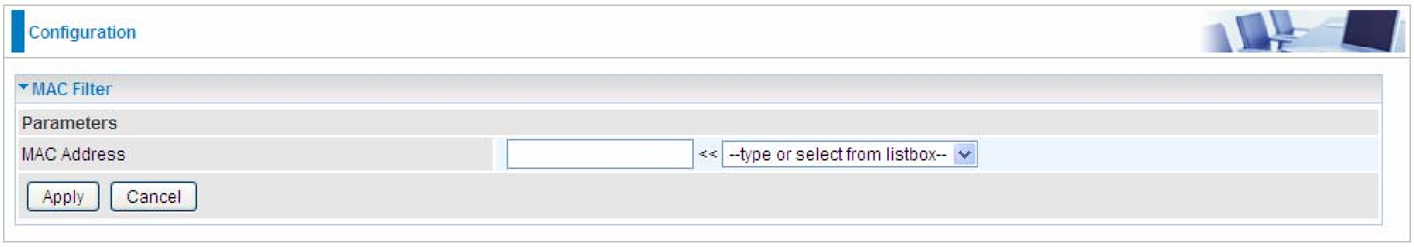
MAC Address	Remove

Select SSID: Select the SSID you want this filter applies to.

MAC Restrict Mode:

- **Disable:** disable the MAC Filter function.
- **Allow**: allow the hosts with the following listed MACs to access the wireless network.
- **Deny**: deny the hosts with the following listed MACs to access the wireless network.

Click **Add** to add the MACs.



Configuration

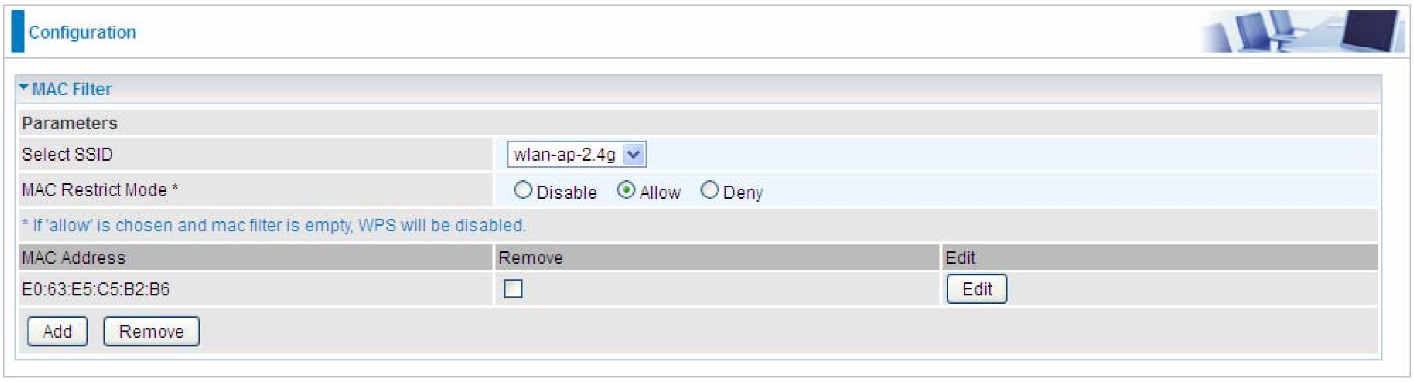
MAC Filter

Parameters

MAC Address	<< --type or select from listbox--

MAC Address: Enter the MAC address(es) or select the MAC address(es). The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Click **Apply** to apply your settings and the item will be listed below.



Configuration

MAC Filter

Parameters

Select SSID	wlan-ap-2.4g
MAC Restrict Mode *	○ Disable ● Allow ○ Deny

* If 'allow' is chosen and mac filter is empty, WPS will be disabled.

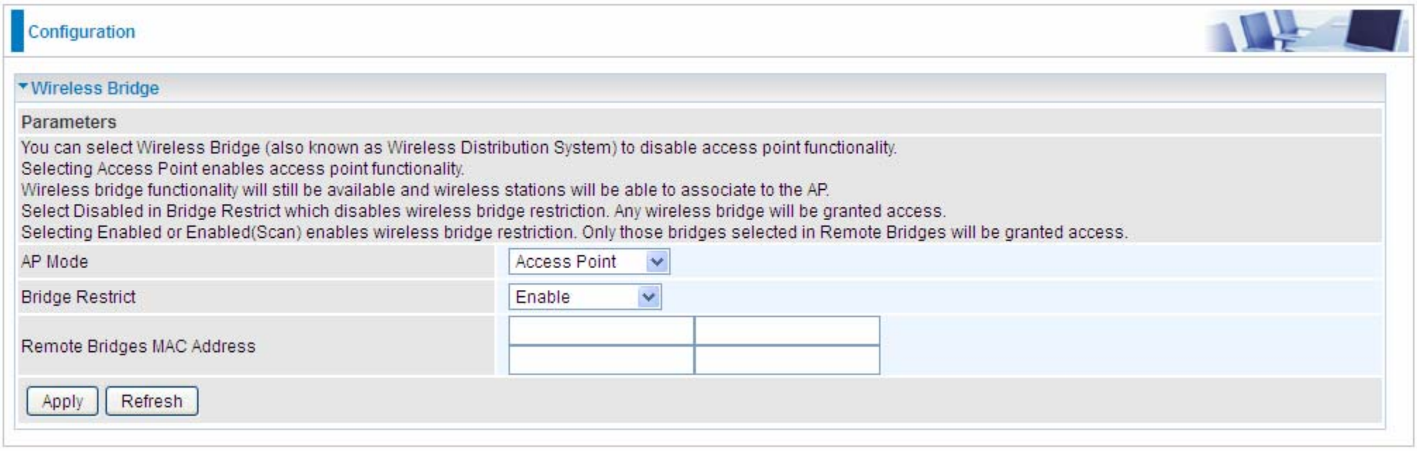
MAC Address	Remove	Edit
E0:63:E5:C5:B2:B6	□	Edit

.

Wireless Bridge

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.

Here you can select what role the AP server has, AP or wireless bridge (WDS).



Parameters

You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality.
Selecting Access Point enables access point functionality.
Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access.
Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

AP Mode	Access Point
Bridge Restrict	Enable
Remote Bridges MAC Address	

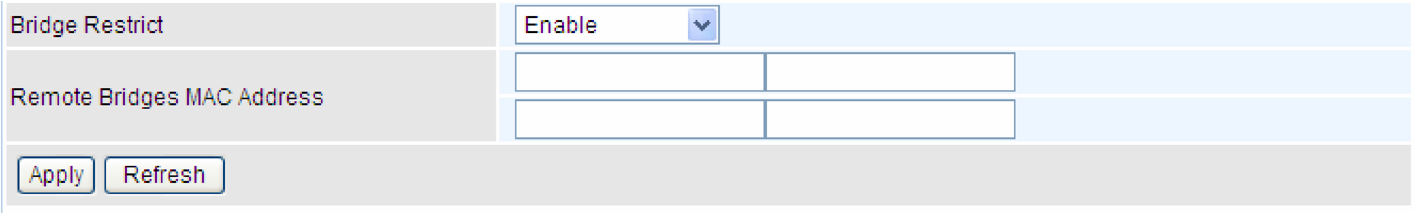
AP Mode: determines whether the gateway will act as an Access point or as a Bridge.

- **Access Point**: the gateway communicates with both clients and bridges.
- **Wireless Bridge**: the gateway communicates with other WDS devices only. In this mode, the gateway doesn't communicate with client devices.

If your wireless network includes repeaters that use WDS, the gateway in wireless bridge mode will also communicate with your repeaters. The gateway in wireless bridge mode will not communicate with a repeater that uses a proprietary (non-WDS) mode.

Bridge Restrict: When **AP Mode** is set to **Wireless Bridge**, this determines whether the gateway will communicate with all other bridges or only specific ones:

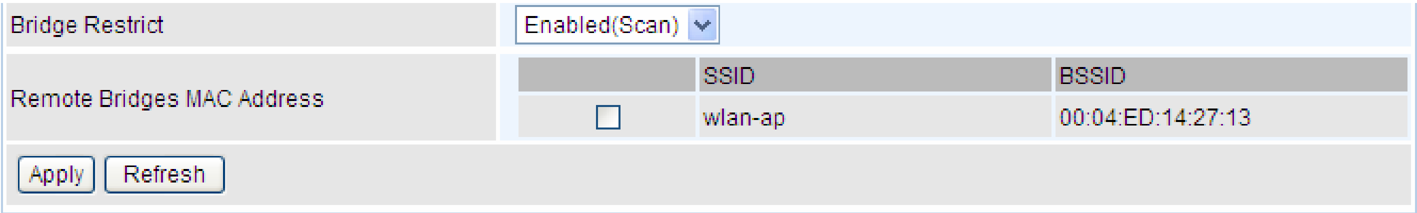
- **Enable:** to enable wireless bridge restriction. Only those specified in the Remote MAC Address the gateway can communicate with.



Bridge Restrict	Enable
Remote Bridges MAC Address	

Remote Bridge MAC Address: enter the remote bridge MAC addresses. Here up to 4 bridge MAC addresses are supported.

- **Enabled (Scan):** to enable wireless bridge restriction. Only those scanned by the gateway can communicate.



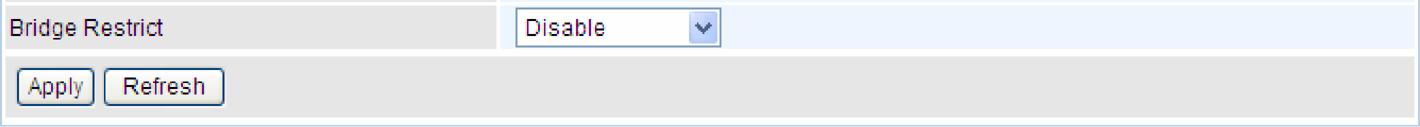
Bridge Restrict: Enabled(Scan)

Remote Bridges MAC Address

	SSID	BSSID
□	wlan-ap	00:04:ED:14:27:13

Remote Bridge MAC Address: select the remote bridge MAC addresses.

- ⓘ **Disable:** Does not restrict the gateway communicating with bridges that have their MAC address listed, but it is still open to communicate with all bridges that are in the same network.

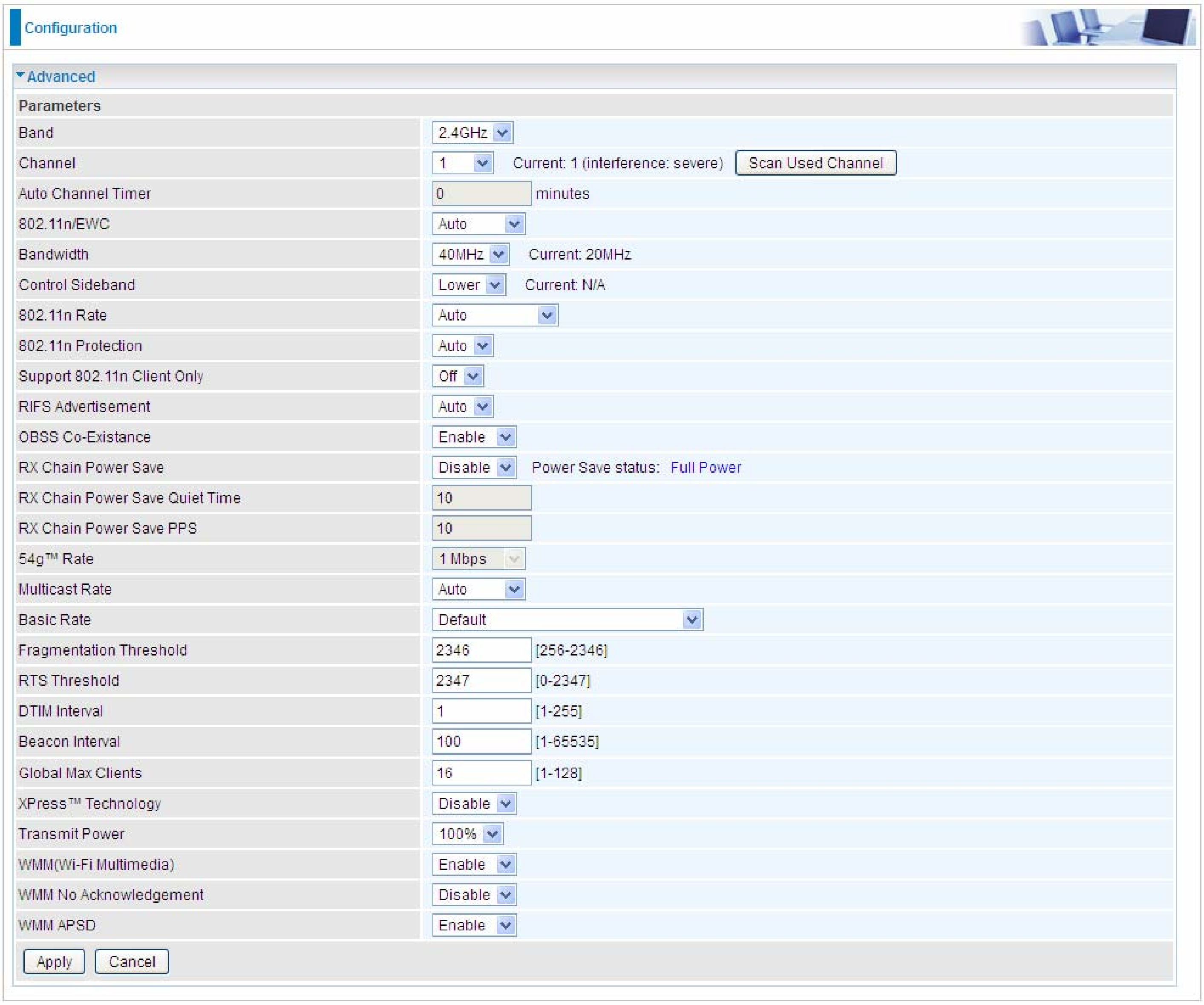


Bridge Restrict: Disable

Click **Apply** to apply your settings.

Advanced

Here users can set some advanced parameters about wireless.



Configuration

Advanced

Parameters	
Band	2.4GHz
Channel	1 Current: 1 (interference: severe) Scan Used Channel
Auto Channel Timer	0 minutes
802.11n/EWC	Auto
Bandwidth	40MHz Current: 20MHz
Control Sideband	Lower Current: N/A
802.11n Rate	Auto
802.11n Protection	Auto
Support 802.11n Client Only	Off
RIFS Advertisement	Auto
OBSS Co-Existance	Enable
RX Chain Power Save	Disable Power Save status: Full Power
RX Chain Power Save Quiet Time	10
RX Chain Power Save PPS	10
54g™ Rate	1 Mbps
Multicast Rate	Auto
Basic Rate	Default
Fragmentation Threshold	2346 [256-2346]
RTS Threshold	2347 [0-2347]
DTIM Interval	1 [1-255]
Beacon Interval	100 [1-65535]
Global Max Clients	16 [1-128]
XPress™ Technology	Disable
Transmit Power	100%
WMM(Wi-Fi Multimedia)	Enable
WMM No Acknowledgement	Disable
WMM APSD	Enable

Band: select frequency band. Here 2.4GHz.

Channel: Allows channel selection of a specific channel (1-7) or Auto mode.

Scan Used Channel: Press the button to scan and list all channels being used.

Auto Channel Timer (min): The auto channel times length it takes to scan in minutes. Only available for auto channel mode.

802.11n/EWC: select to auto enable or disable 802.11n.

Bandwidth: Select bandwidth. The higher the bandwidth the better the performance will be.

Control Sideband: only available for 40MHz. It allows you to select upper sideband or lower sideband. Sideband refers to the frequency band either above (**upper sideband**) or below (**lower sideband**) the carrier frequency, within which fall the spectral components produced by modulation of a carrier wave.

802.11n Rate: This allows you to select the fixed transmission rate or auto.

802.11n Protection: turn off for maximize throughput. Auto for greater security.

Support 802.11n Client Only: turn on the option to only provide wireless access to the clients operating at 802.11n speeds.

RIFS Advertisement: Reduced Inter-frame Spacing (RIFS) is a 802.11n feature that also improves performance by reducing the amount of dead time required between OFDM transmissions. Select Off to disable this function or auto to enable this function.

OBSS Co-Existence: coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

RX Chain Power Save: Enabling this feature turns off one of the Receive chains, going from 2x2 to 2x1 to save power.

RX Chain Power Save Quiet Time: The number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature activates itself.

RX Chain Power Save PPS: The maximum number of packets per seconds that can be processed by the WLAN interface for a duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

Multicast Rate: Setting for multicast packets transmission rate.

Basic Rate: Setting for basic transmission rate. It is not a specific kind of rate, it is a series of rates supported. When set to Default, the router can transmit with all kinds of standardized rates.

Fragmentation Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

DTIM Interval: Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 1- 65535. The beacon transmissions identify the presence of an access point.

Global Max Clients: Here you have the option of setting the limit of the number of clients who can connect to your wireless network.

XPress™ Technology: It has been designed to improve the wireless network efficiency. Default is disabled.

Regulatory Mode: Select to deny any regulatory mode, which is only for **5GHz** band wireless. There are two regulatory modes:

802.11h: The standard solves interference problems with e.g. satellites and radar using the same 5 GHz band as 802.11a or 802.11n dual-band access points.

802.11d: This standard automatically adjusts its allowed frequencies, power levels and bandwidth accordingly to the country it's located in.
This means that manufacturers don't need to make country specific products.

Transmit Power: select the transmitting power of your wireless signal.

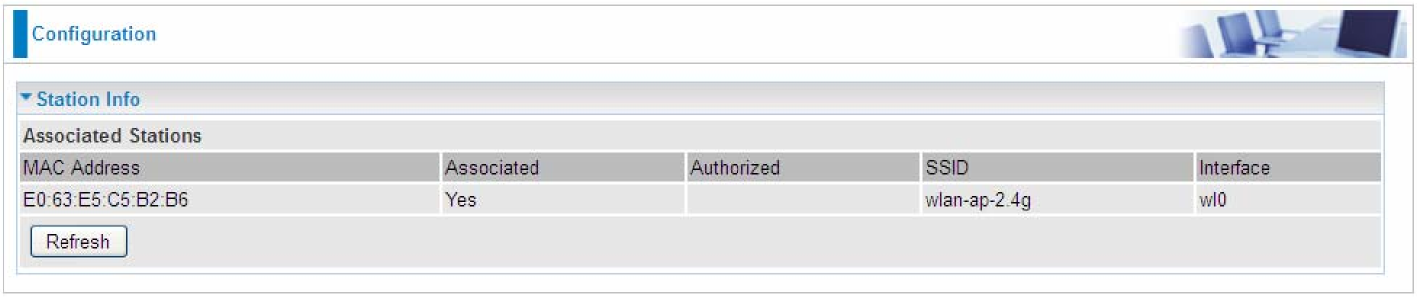
WMM (Wi-Fi Multimedia): you can choose to enable or disable this function which allows for priority of certain data over wireless network.

WMM No Acknowledgement: Refers to the acknowledge policy at the MAC level. Enabling WMM No Acknowledgement can result in more efficient throughput but higher error rates in noisy Radio Frequency (RF) environment.

WMM APSD: Automatic Power Save Delivery. Enable this to save power.

Station Info

Here you can view information about the wireless clients.



Associated Stations

MAC Address	Associated	Authorized	SSID	Interface
E0:63:E5:C5:B2:B6	Yes		wlan-ap-2.4g	wl0

MAC Address: The MAC address of the wireless clients.

Associated: List all the stations that are associated with the Access Point. If a station is idle for too long, it is removed from this list

Authorized: List those devices with authorized access**.**

SSID: Show the current SSID of the client.

Interface: To show which interface the wireless client is connected to.

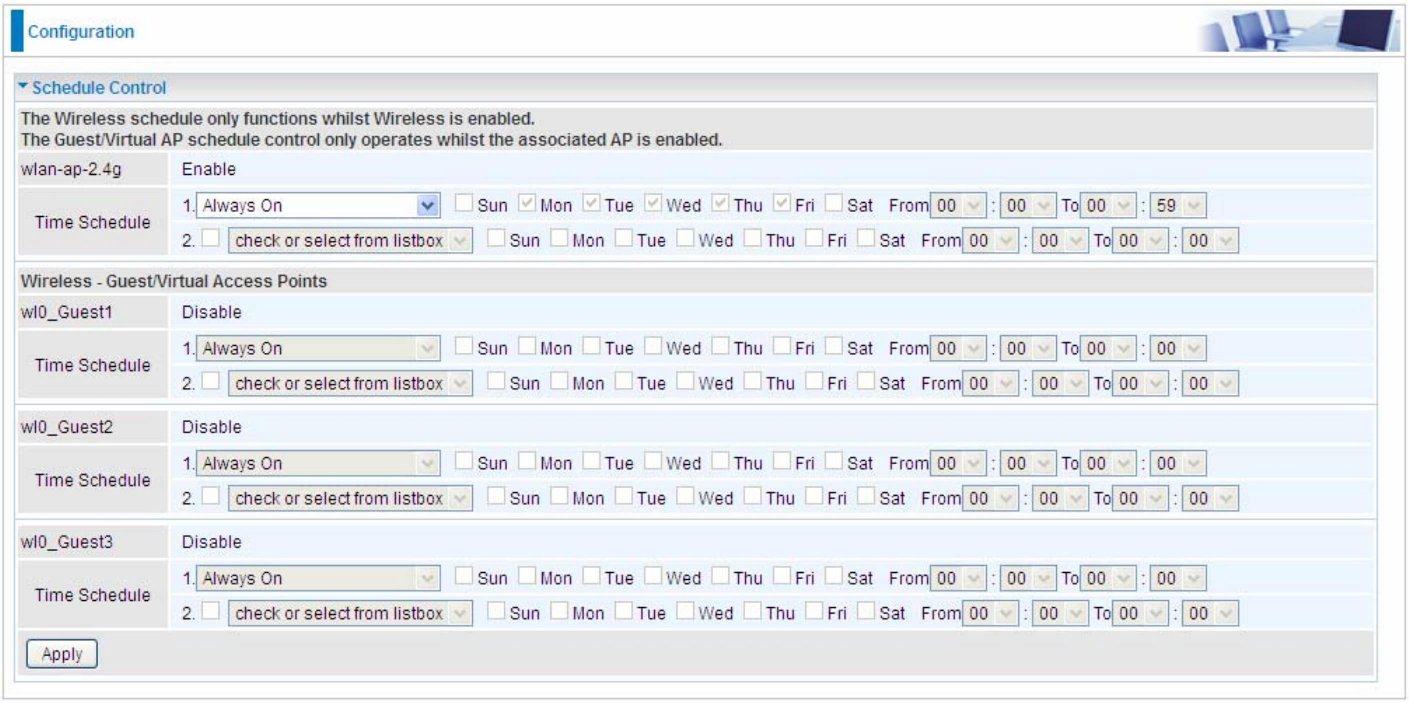
Refresh: To get the latest information.

Schedule Control

Schedule control is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access.

The Wireless schedule only functions whilst Wireless is enabled.
The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

For detail setting the timeslot, user can turn to Time Schedule .



▾ Schedule Control

The Wireless schedule only functions whilst Wireless is enabled.
The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.

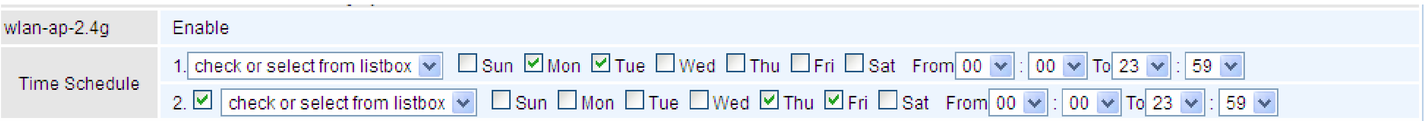
wlan-ap-2.4g	Enable	
Time Schedule	1.	Always On ▾ □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat From 00 : 00 To 00 : 59
	2. □	check or select from listbox ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00

Wireless - Guest/Virtual Access Points

wl0_Guest1	Disable	
Time Schedule	1.	Always On ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00
	2. □	check or select from listbox ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00
wl0_Guest2	Disable	
Time Schedule	1.	Always On ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00
	2. □	check or select from listbox ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00
wl0_Guest3	Disable	
Time Schedule	1.	Always On ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00
	2. □	check or select from listbox ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00

Time Schedule: Set when the SSID works. If user wants the SSID works all the time, please select "Always On"; if not, please set or select the exact time your want the SSID works. Here user can set two separate intervals.

For example: user wants the SSID "*wlan-ap-2.4g*" to work on weekdays except for Wednesday, under this circumstance, user can set as shown below. (7800VDP(O)X offers a optimal way to set two separate timeslots when user needs to activate the SSID during separate intervals.)



wlan-ap-2.4g	Enable	
Time Schedule	1.	check or select from listbox ▾ □ Sun ☑ Mon ☑ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 23 : 59
	2. ☑	check or select from listbox ▾ □ Sun □ Mon □ Tue □ Wed ☑ Thu ☑ Fri □ Sat From 00 : 00 To 23 : 59

Wireless 5G(wl1)

The BiPAC 7800VDP(O)X uses to radio band-2.4GHz and 5GHz simultaneously, to run wireless connection for users. Wl1, operating on 5GHz, has sub-items as **Basic**, **Security**, **MAC Filter**, **Wireless Bridge**, **Advanced**, **Station Info** and **Schedule Control** here.

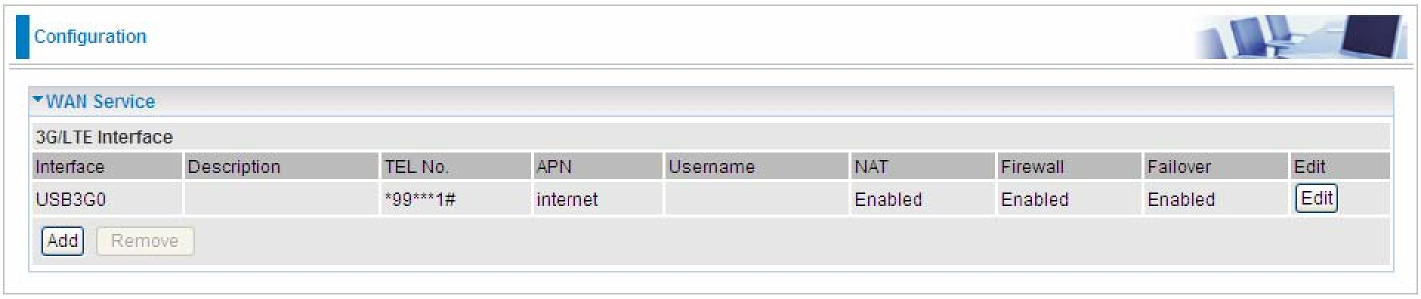
See Wireless 2.4G(wl0).

WAN-Wide Area Network

A WAN (Wide Area Network) is a computer network that covers a broad geographical area (eg. Internet) used to connect LAN and other types of network systems.

WAN Service

Two WAN interfaces are provided for WAN connection: DSL and Ethernet.



Configuration

WAN Service

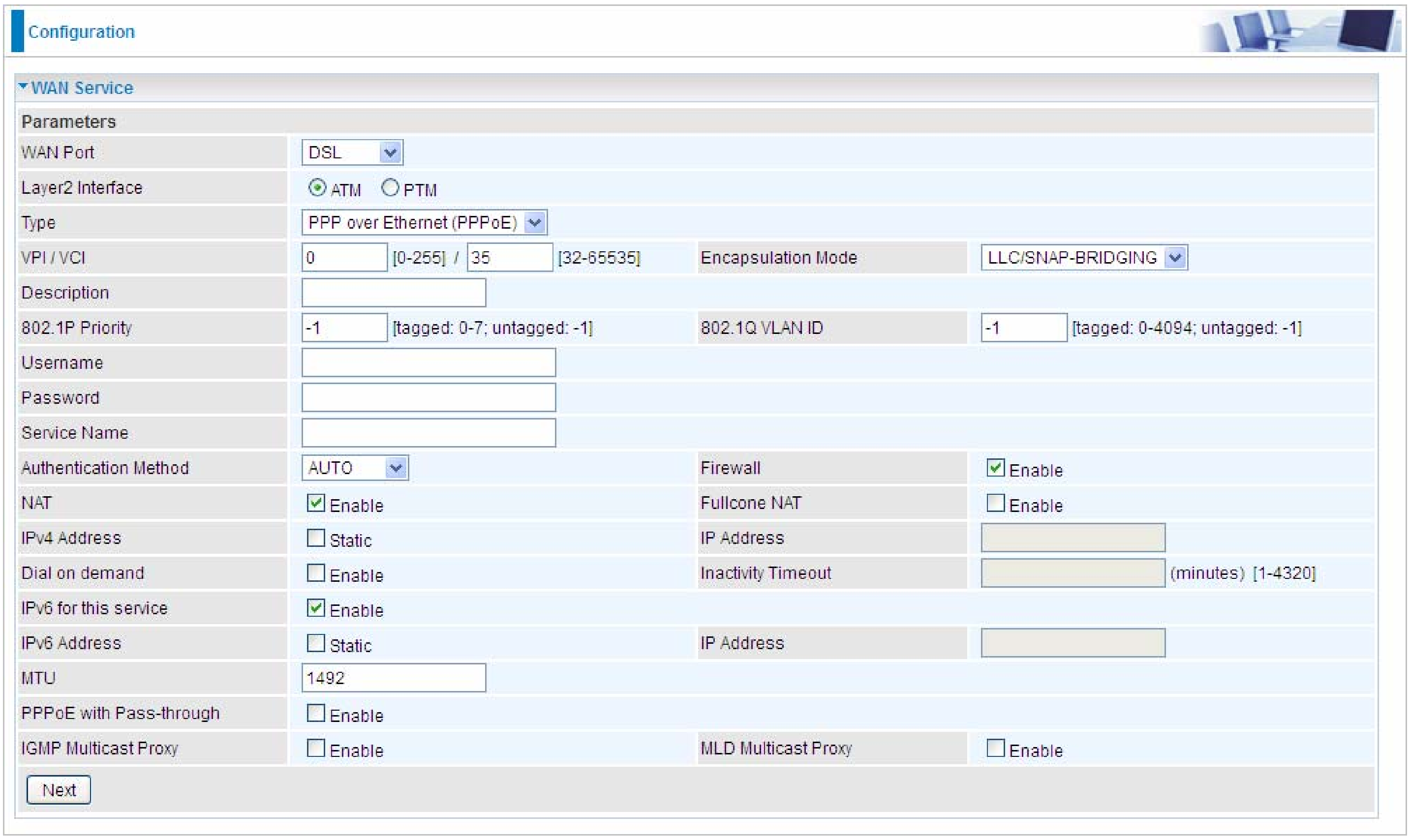
3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Click **Add** to add new WAN connections.

DSL

In DSL mode, there are two transfer modes for you to configure for WAN connection, namely ATM and PTM, configuration of PTM mode is similar as ATM mode, here take ATM mode WAN configuration for example.



Configuration

WAN Service

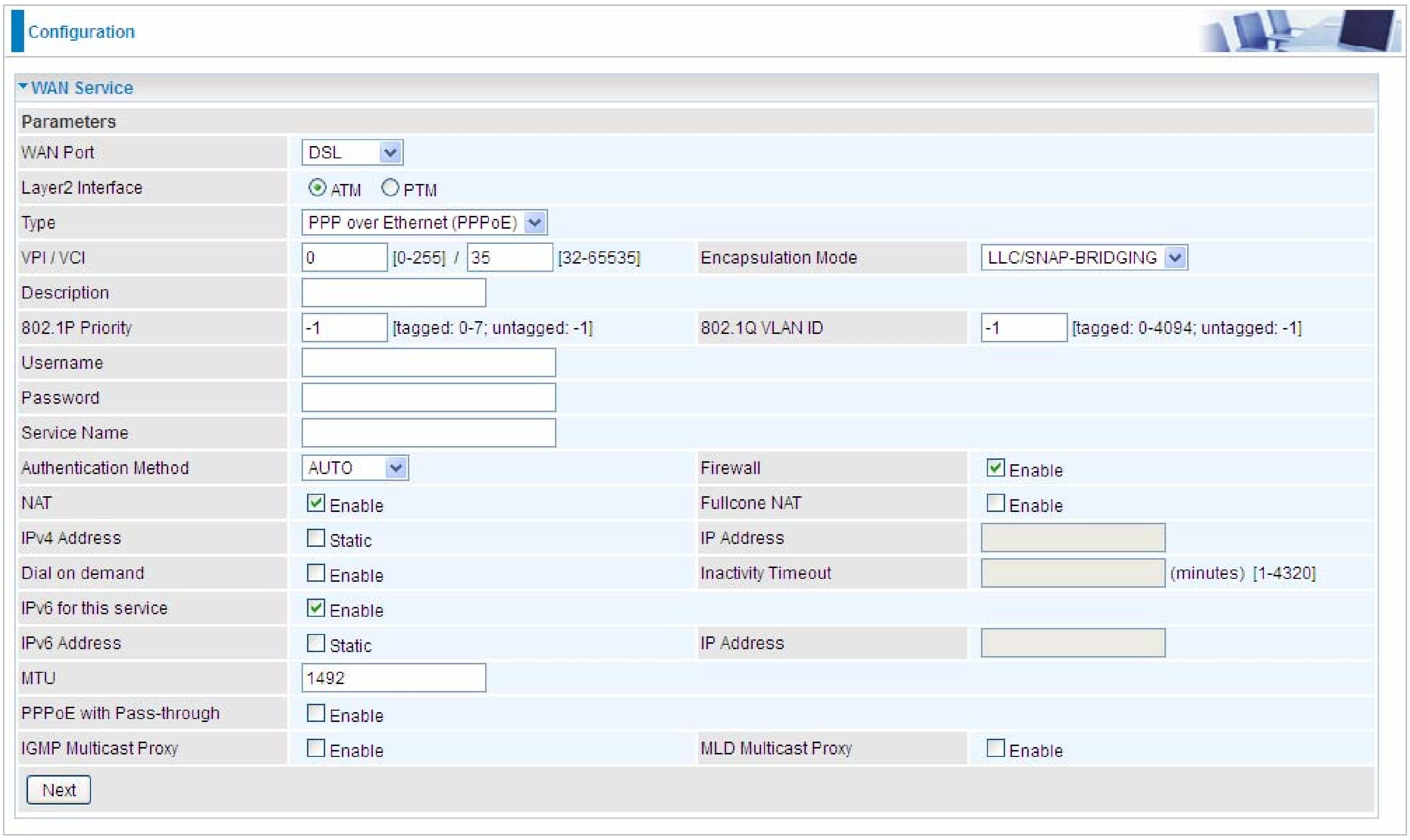
Parameters

WAN Port	DSL		
Layer2 Interface	● ATM ○ PTM		
Type	PPP over Ethernet (PPPoE)		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO	Firewall	☑ Enable
NAT	☑ Enable	Fullcone NAT	□ Enable
IPv4 Address	□ Static	IP Address	
Dial on demand	□ Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	☑ Enable		
IPv6 Address	□ Static	IP Address	
MTU	1492		
PPPoE with Pass-through	□ Enable		
IGMP Multicast Proxy	□ Enable	MLD Multicast Proxy	□ Enable

Layer2 Interface: 2 transfer mode, ATM or PTM.

PPPoE

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



Configuration

WAN Service

Parameters

WAN Port	DSL		
Layer2 Interface	● ATM ○ PTM		
Type	PPP over Ethernet (PPPoE)		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO	Firewall	☑ Enable
NAT	☑ Enable	Fullcone NAT	□ Enable
IPv4 Address	□ Static	IP Address	
Dial on demand	□ Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	☑ Enable		
IPv6 Address	□ Static	IP Address	
MTU	1492		
PPPoE with Pass-through	□ Enable		
IGMP Multicast Proxy	□ Enable	MLD Multicast Proxy	□ Enable

Next

VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purpose, user can define it yourselfe.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

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 to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. Of Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

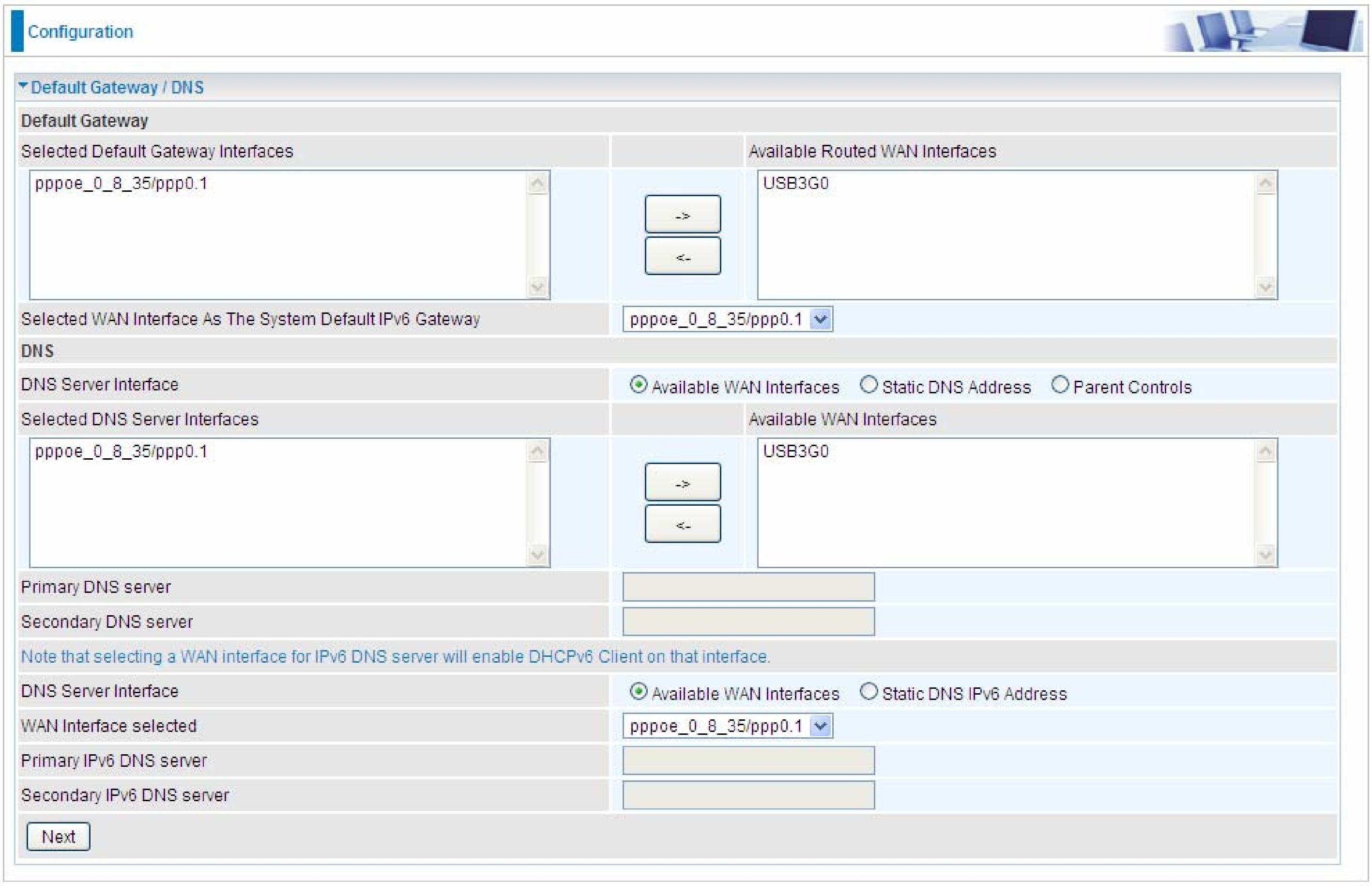
MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Configuration

Default Gateway / DNS

Default Gateway		
Selected Default Gateway Interfaces		Available Routed WAN Interfaces
pppoe_0_8_35/ppp0.1	-> <-	USB3G0
Selected WAN Interface As The System Default IPv6 Gateway	pppoe_0_8_35/ppp0.1	
DNS		
DNS Server Interface	● Available WAN Interfaces ○ Static DNS Address ○ Parent Controls	
Selected DNS Server Interfaces		Available WAN Interfaces
pppoe_0_8_35/ppp0.1	-> <-	USB3G0
Primary DNS server		
Secondary DNS server		
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.		
DNS Server Interface	● Available WAN Interfaces ○ Static DNS IPv6 Address	
WAN Interface selected	pppoe_0_8_35/ppp0.1	
Primary IPv6 DNS server		
Secondary IPv6 DNS server		

Next

Default Gateway

Select default gateway for you connection (IPv4 and IPv6).

DNS

➢ IPv4

Three ways to set an IPv4 DNS server

- **Available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

➢ IPv6

Obtain IPv6 DNS info from a WAN interface

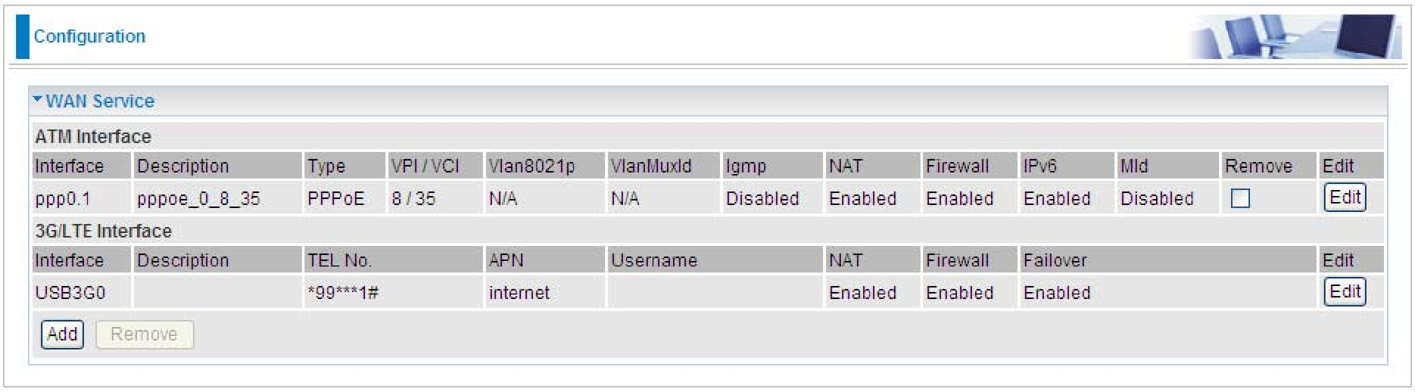
WAN Interface selected: Select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

Static DNS IPv6 Address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

If you don't need a service, select the item you want to remove, check the checkbox, then press **Remove**.

Press **Edit** button to re-edit this service settings.



Configuration

WAN Service

ATM Interface

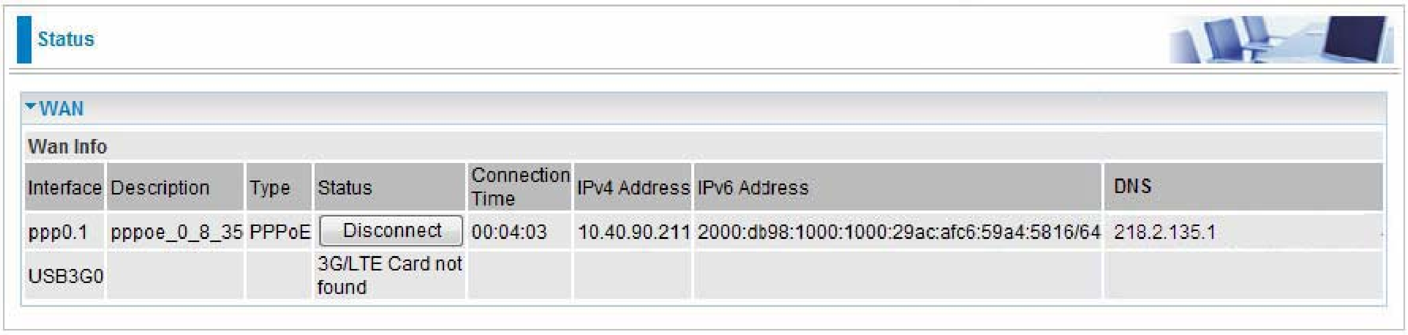
Interface	Description	Type	VPI / VCI	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8 / 35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	□	Edit

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

When configuration is successfully completely, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).

(IPv4 or IPv6)

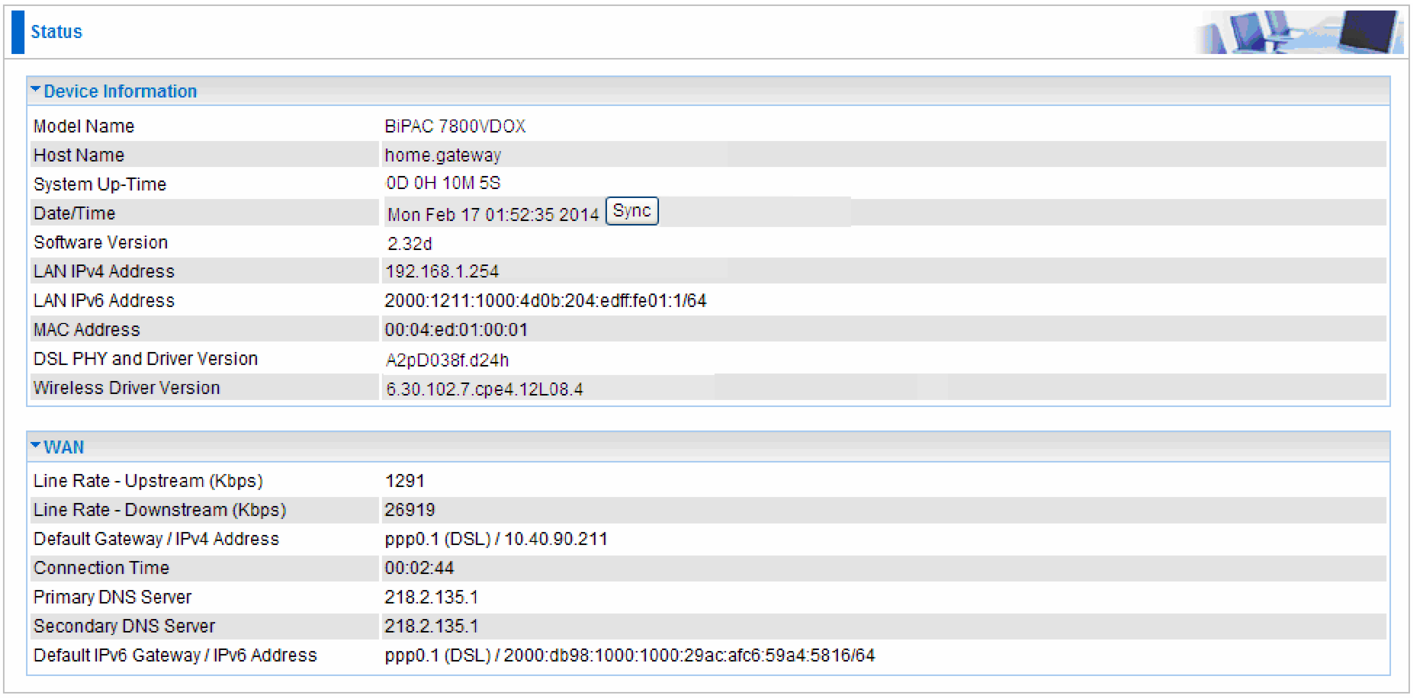


Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	00:04:03	10.40.90.211	2000:db98:1000:1000:29ac:afc6:59a4:5816/64	218.2.135.1
USB3G0			3G/LTE Card not found				



Status

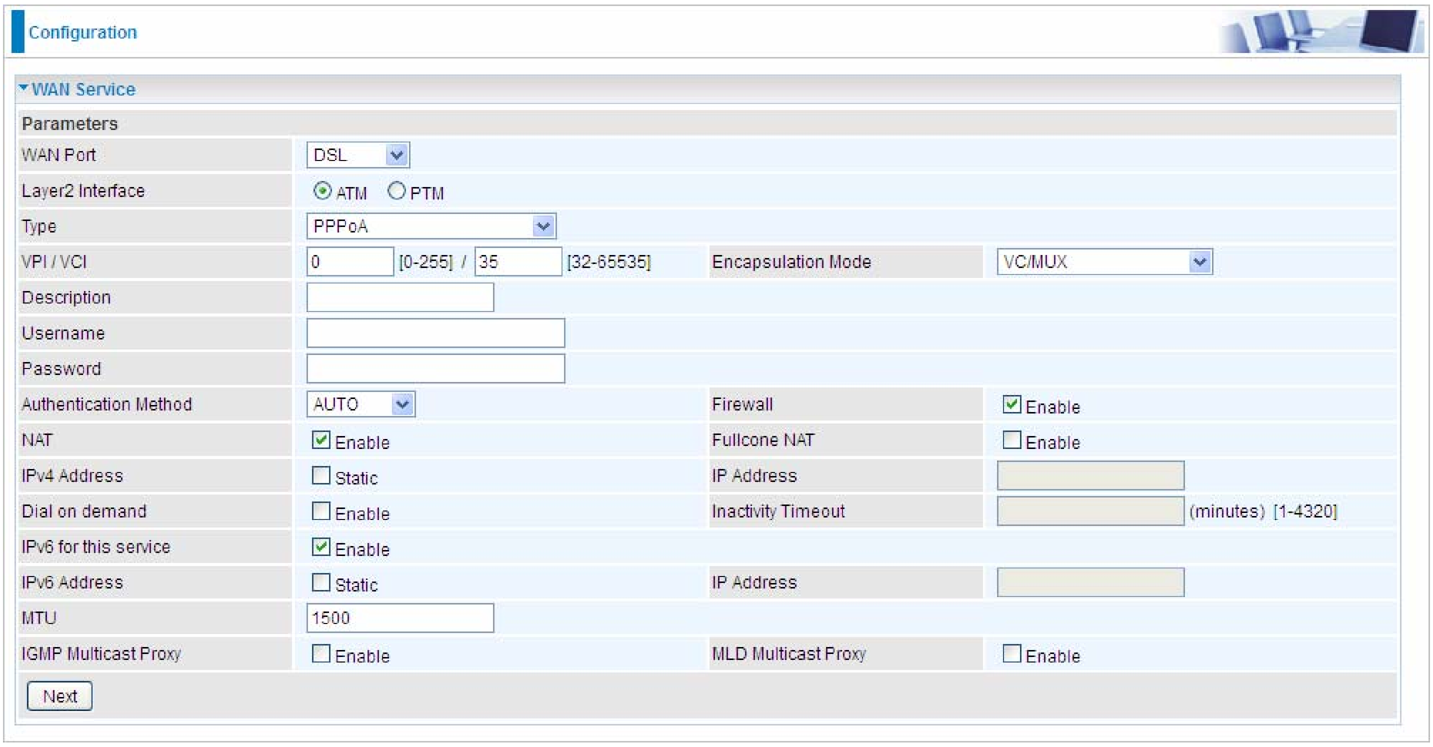
Device Information

Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 10M 5S
Date/Time	Mon Feb 17 01:52:35 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

Line Rate - Upstream (Kbps)	1291
Line Rate - Downstream (Kbps)	26919
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

PPPoA



Configuration

WAN Service

Parameters			
WAN Port	DSL		
Layer2 Interface	● ATM ○ PTM		
Type	PPPoA		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	VC/MUX
Description			
Username			
Password			
Authentication Method	AUTO	Firewall	☑ Enable
NAT	☑ Enable	Fullcone NAT	□ Enable
IPv4 Address	□ Static	IP Address	
Dial on demand	□ Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	☑ Enable		
IPv6 Address	□ Static	IP Address	
MTU	1500		
IGMP Multicast Proxy	□ Enable	MLD Multicast Proxy	□ Enable

VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

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 to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Note: In this connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT or disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted cone NAT. With Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

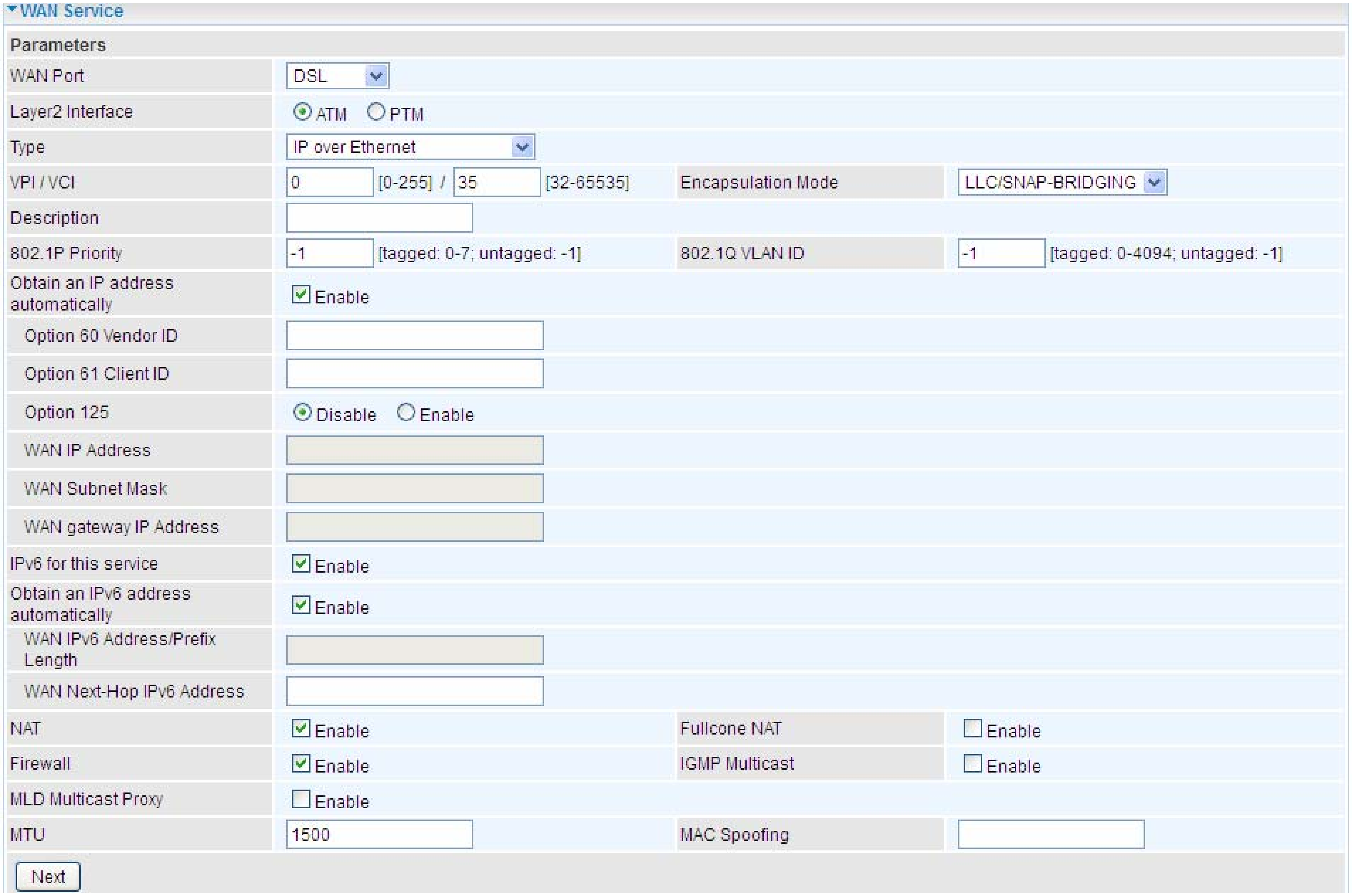
MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.

IP over Ethernet



▾WAN Service

Parameters			
WAN Port	DSL		
Layer2 Interface	● ATM ○ PTM		
Type	IP over Ethernet		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Obtain an IP address automatically	☑ Enable		
Option 60 Vendor ID			
Option 61 Client ID			
Option 125	● Disable ○ Enable		
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	☑ Enable		
Obtain an IPv6 address automatically	☑ Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	☑ Enable	Fullcone NAT	□ Enable
Firewall	☑ Enable	IGMP Multicast	□ Enable
MLD Multicast Proxy	□ Enable		
MTU	1500	MAC Spoofing	

VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

Option 61 Client ID: Enter the associated information provided by your ISP.

Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the prestored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is ***Disable***.

WAN IP Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

IPv6 for this service: Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

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 to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast: IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery**

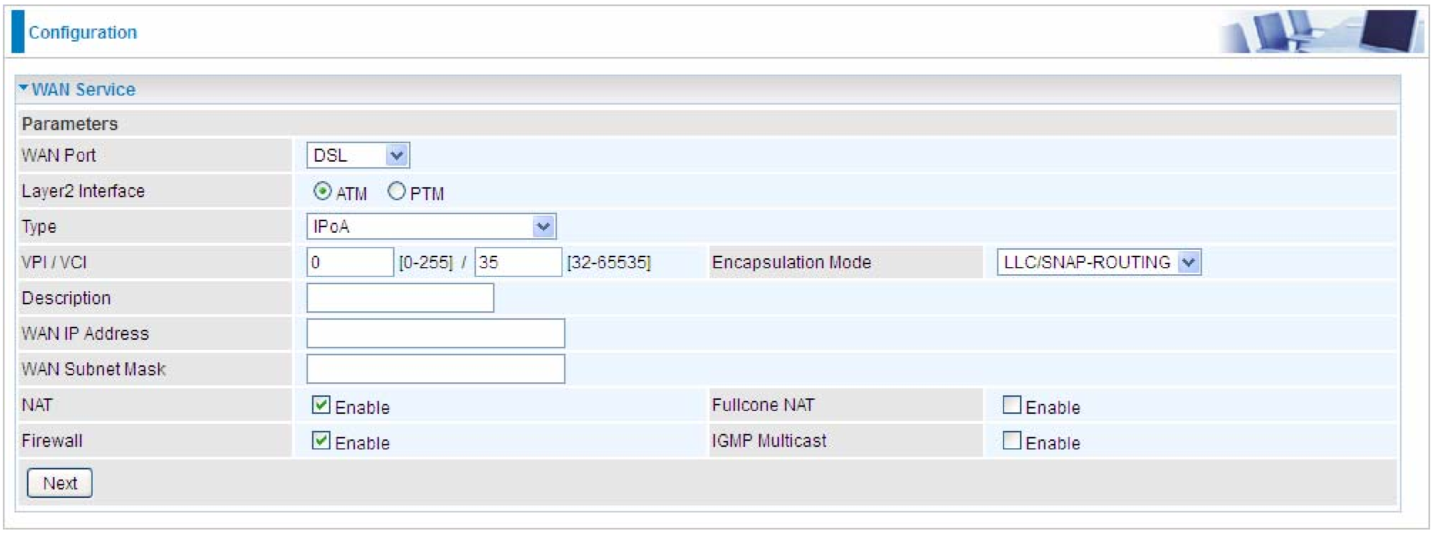
Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

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

MAC Spoofing: This option is required by some service providers specifying some specific MAC allowed for connecting in network. You must fill in the MAC address specified by your service provider when this information is required.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.

IPoA



Configuration

WAN Service

Parameters

WAN Port	DSL		
Layer2 Interface	● ATM ○ PTM		
Type	IPoA		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-ROUTING
Description			
WAN IP Address			
WAN Subnet Mask			
NAT	☑ Enable	Fullcone NAT	□ Enable
Firewall	☑ Enable	IGMP Multicast	□ Enable

VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

Description: User-defined description for the connection, commonly for friendly use.

WAN IP: Enter the WAN IP from the ISP.

WAN Subnet Mask: Enter the WAN Subnet Mask from the ISP.

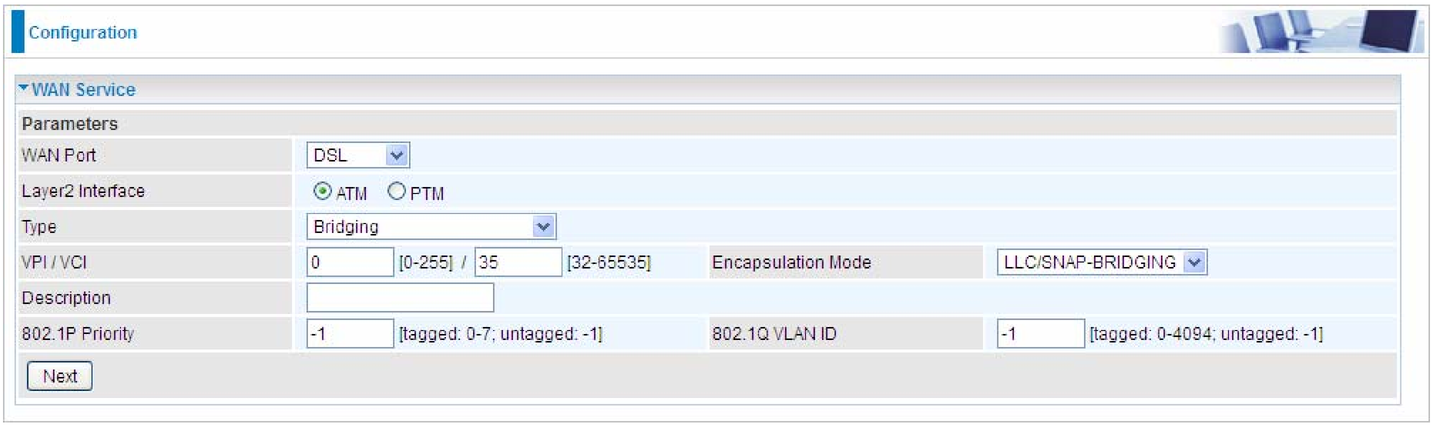
NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account by sharing the single IP address. If users on your LAN have their own public IP addresses to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

IGMP Multicast: IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

Bridging



Configuration

▾WAN Service

Parameters

WAN Port	DSL		
Layer2 Interface	● ATM ○ PTM		
Type	Bridging		
VPI / VCI	0 [0-255] / 35 [32-65535]	Encapsulation Mode	LLC/SNAP-BRIDGING
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]

VCP/VPI: Enter the VCI/VPI combination from you ISP.

Encapsulation Mode: Select the encapsulation mode, LLC/SNAP-BRIDGING, or VC/MUX.

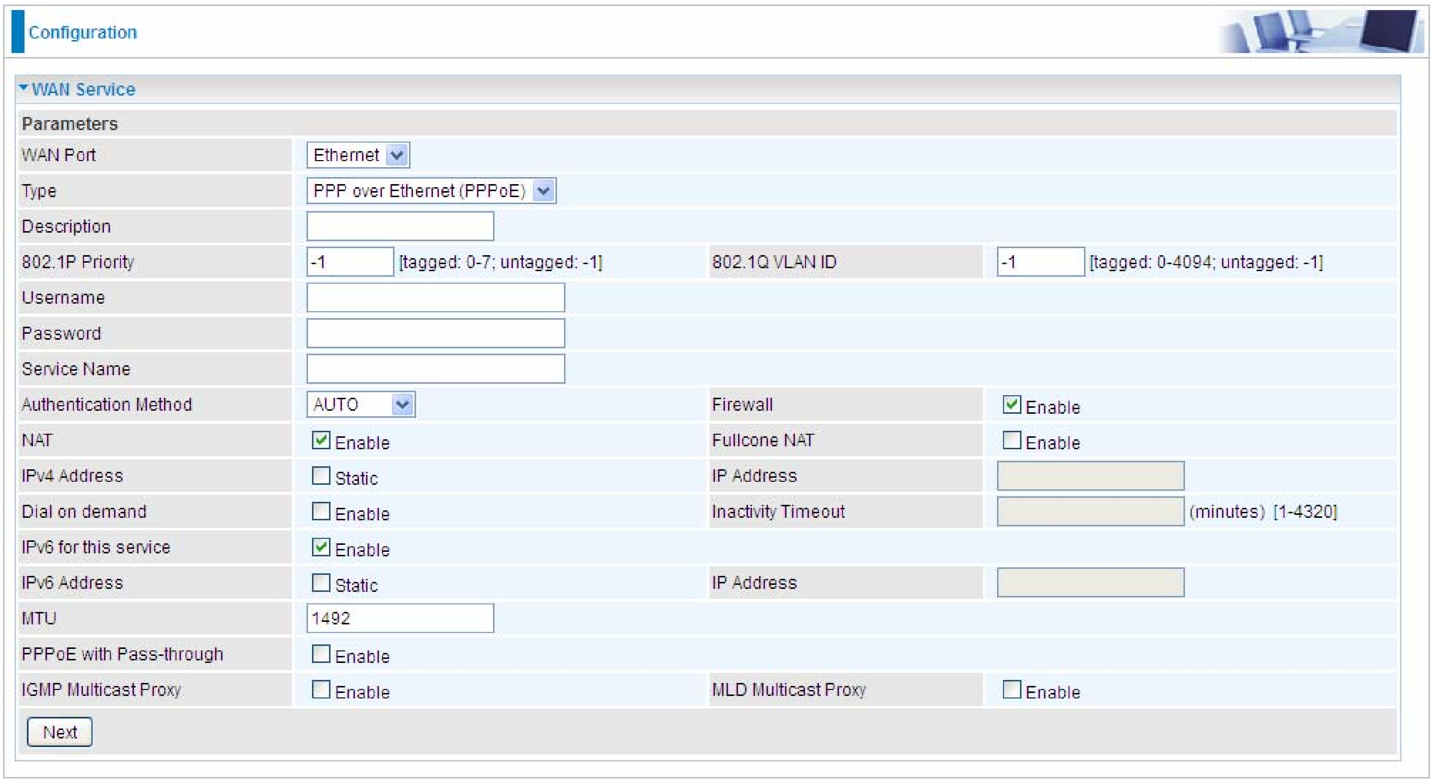
Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

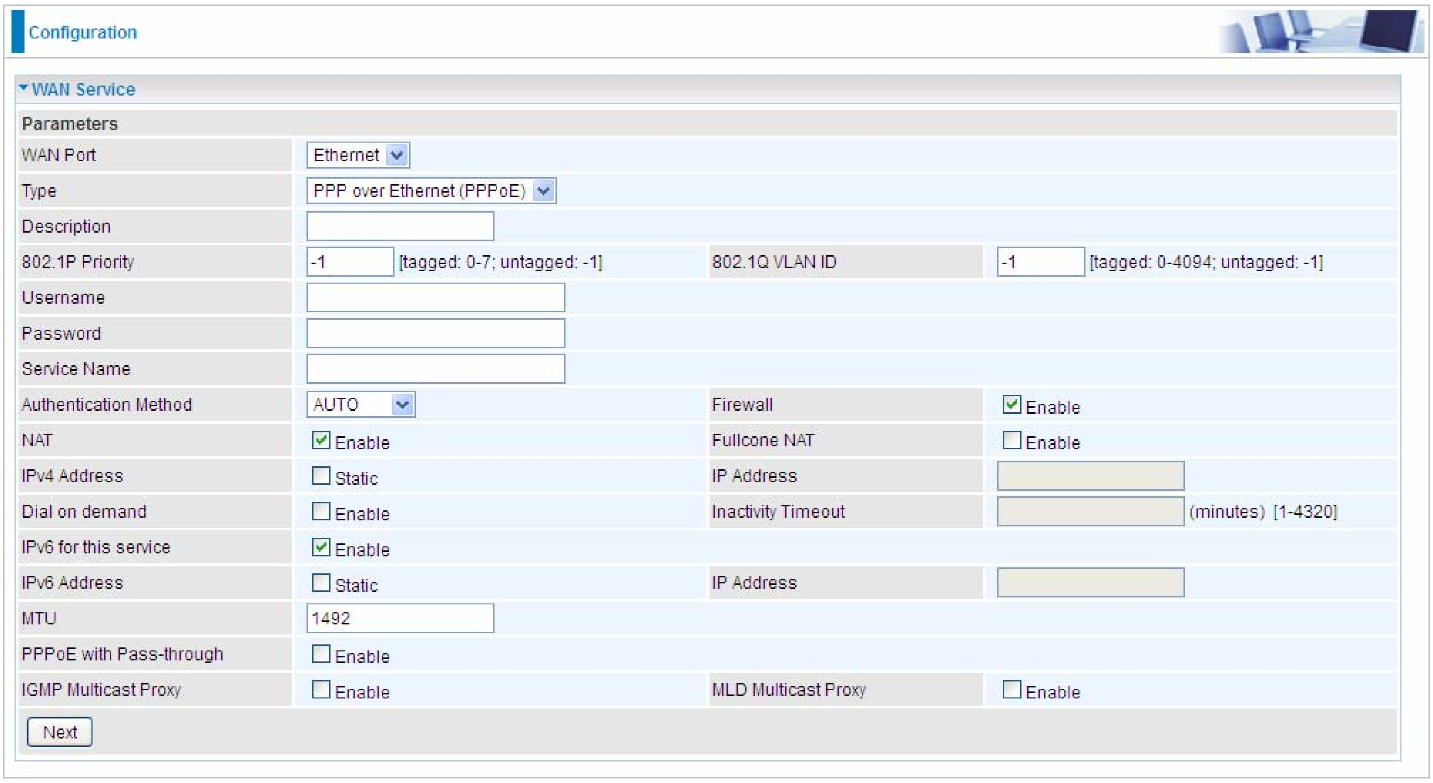
ⓘ Ethernet

Ethernet WAN connection is well known as directly broadband WAN connection.



Parameters			
WAN Port	Ethernet ▾		
Type	PPP over Ethernet (PPPoE) ▾		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO ▾	Firewall	☑ Enable
NAT	☑ Enable	Fullcone NAT	□ Enable
IPv4 Address	□ Static	IP Address	
Dial on demand	□ Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	☑ Enable		
IPv6 Address	□ Static	IP Address	
MTU	1492		
PPPoE with Pass-through	□ Enable		
IGMP Multicast Proxy	□ Enable	MLD Multicast Proxy	□ Enable

PPPoE


Configuration
WAN Service

Parameters			
WAN Port	Ethernet ▾		
Type	PPP over Ethernet (PPPoE) ▾		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Username			
Password			
Service Name			
Authentication Method	AUTO ▾	Firewall	☑ Enable
NAT	☑ Enable	Fullcone NAT	□ Enable
IPv4 Address	□ Static	IP Address	
Dial on demand	□ Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	☑ Enable		
IPv6 Address	□ Static	IP Address	
MTU	1492		
PPPoE with Pass-through	□ Enable		
IGMP Multicast Proxy	□ Enable	MLD Multicast Proxy	□ Enable

Next

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Username: Enter the account obtained from the ISP.

Password: Enter the password obtained from the ISP.

Service Name: The item is for identification purpose, user can define it yourselfe.

Authentication Method: Default is ***Auto***. Or else your ISP will advise you the appropriate mode.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

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 to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host by sending a packet to the mapped external address.

Note: In PPPoE connection, NAT is enabled by default, you can determine whether to enable Fullcone NAT. and while you disable Fullcone NAT and only use NAT, the default NAT type is Port Restricted or Port-Restricted cone NAT, the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P

IPv4 Address: Select whether to set static IPv4 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address get from the ISP.

Dial on demand: It is a parameter to let users to dial for connection to internet themselves. It is useful when saving internet fees.

Inactivity Timeout: The set Inactivity timeout period, unit: minutes. It is combined use with Dial on Demand, users should specify the concrete time interval for dial on demand.

IPv6 for this service: Enable to use IPv6 service.

IPv6 Address: Select whether to set static IPv6 address or obtain automatically.

IP Address: If ***Static*** is enabled in the above field, enter the static IPv4 address.

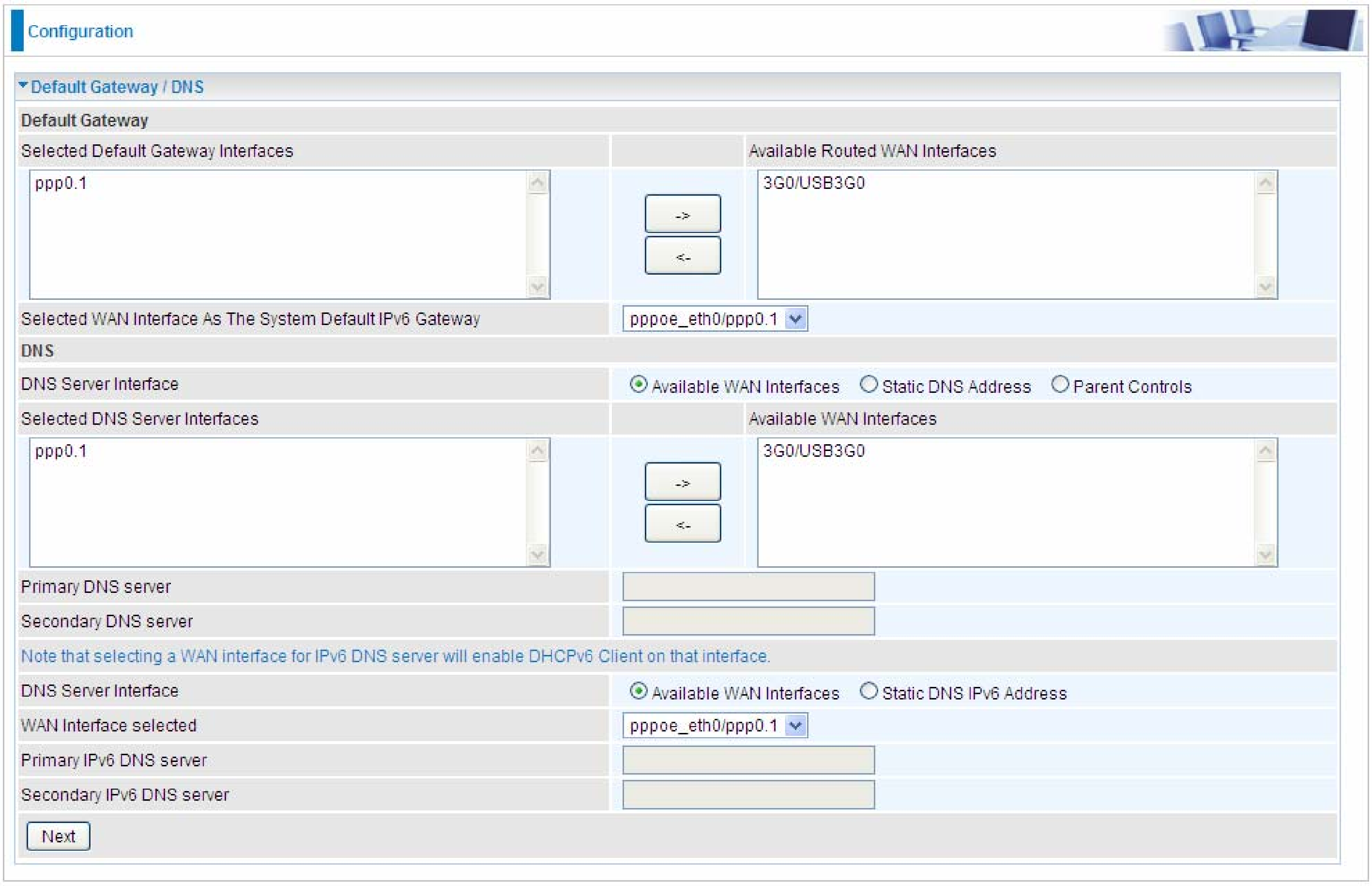
MTU: Maximum Transmission Unit, the size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

PPPoE with Pass-through: Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

IGMP Multicast Proxy: Check whether to enable this feature. IGMP (**Internet Group Management Protocol**) Proxy intercepts the IGMP request from Clients and set up the multicast-forwarding table, it takes over some of the router's job, simplifying the router's job and multicast communication.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

Click **Next** to continue to set the default gateway and DNS for IPv4 and IPv6.



Configuration

▾Default Gateway / DNS

Default Gateway		
Selected Default Gateway Interfaces		Available Routed WAN Interfaces
ppp0.1	-> <-	3G0/USB3G0
Selected WAN Interface As The System Default IPv6 Gateway	pppoe_eth0/ppp0.1	
DNS		
DNS Server Interface	● Available WAN Interfaces ○ Static DNS Address ○ Parent Controls	
Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1	-> <-	3G0/USB3G0
Primary DNS server		
Secondary DNS server		
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.		
DNS Server Interface	● Available WAN Interfaces ○ Static DNS IPv6 Address	
WAN Interface selected	pppoe_eth0/ppp0.1	
Primary IPv6 DNS server		
Secondary IPv6 DNS server		
Next		

Default Gateway

Select default gateway for you connection (IPv4 and IPv6).

DNS

- **IPv4**

Three ways to set an IPv4 DNS server

- **Available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

- **IPv6**

Obtain IPv6 DNS info from a WAN interface

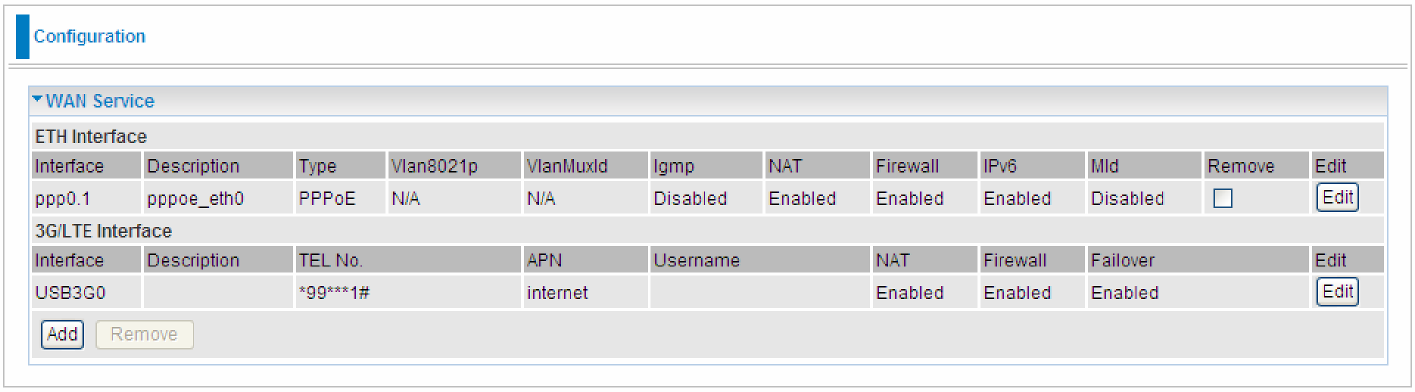
WAN Interface selected: Select one configured IPv6 WAN connection from the menu to be as an IPv6 DNS.

Static DNS IPv6 Address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

If you don’t need the service, select the item you want to remove, check the checkbox, then press **Remove**, it will be OK.

Press **Edit** button to re-edit this service settings.



Configuration

WAN Service

ETH Interface

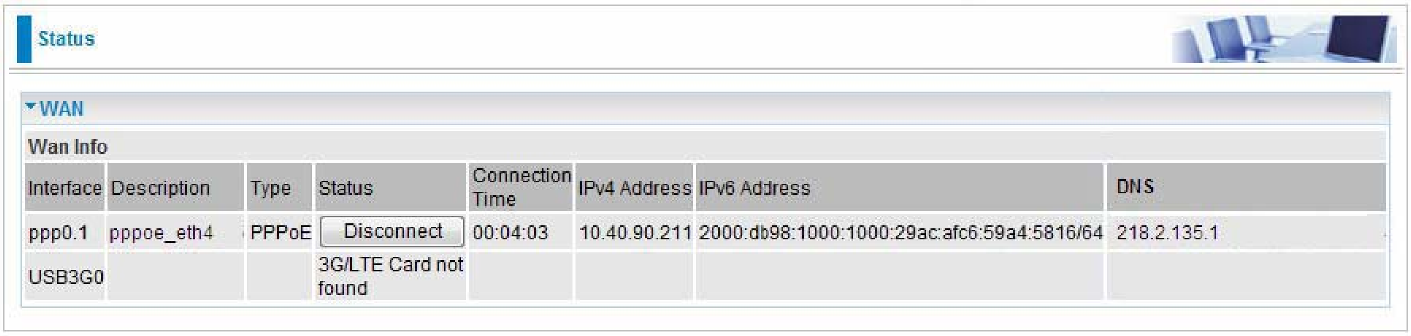
Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_eth0	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	□	Edit

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Here the corresponding WAN Service has been configured, if it is OK, you can access the internet. You can go to **Status>WAN** or **Summary** to view the WAN connection information (if your ISP provides IPv6 service, then you will obtain an IPv6 address).

(IPv4 or IPv6)



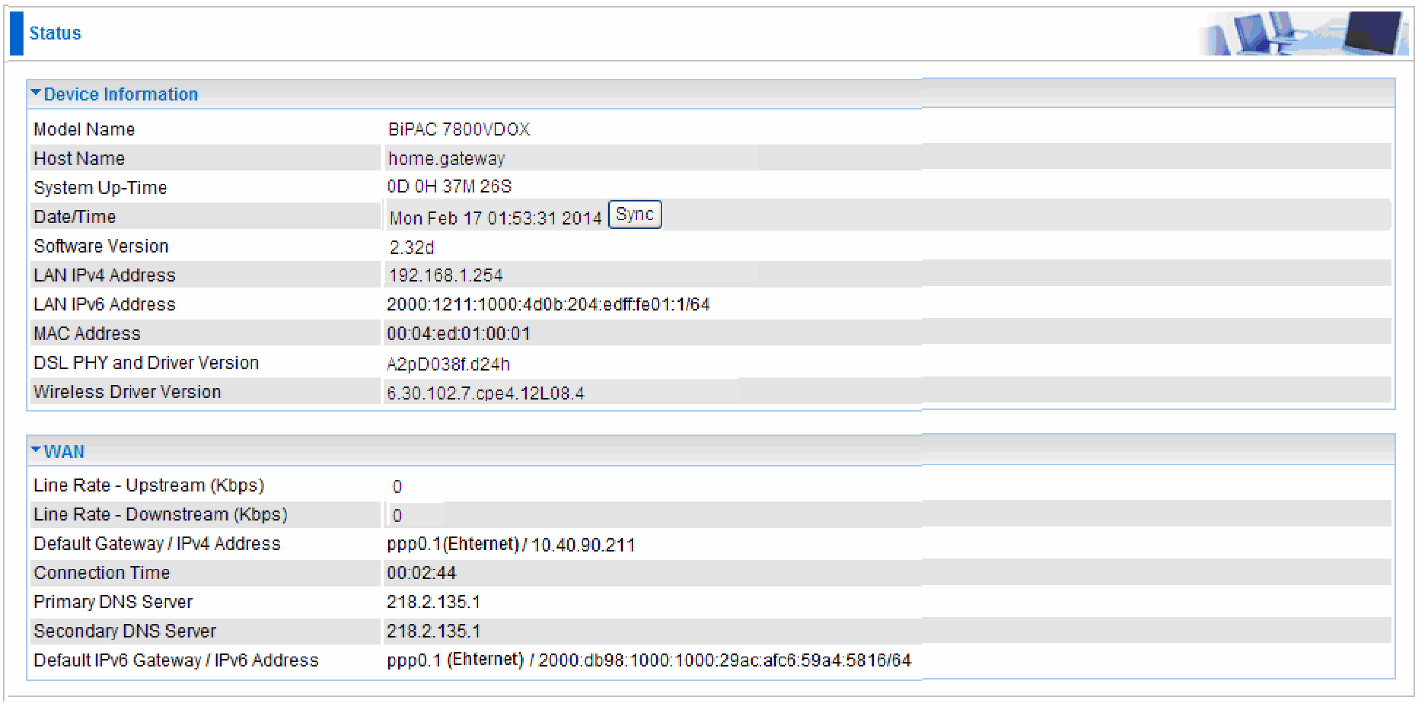
Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_eth4	PPPoE	Disconnect	00:04:03	10.40.90.211	2000:db98:1000:1000:29ac:afc6:59a4:5816/64	218.2.135.1
USB3G0			3G/LTE Card not found				

The device summary information



Status

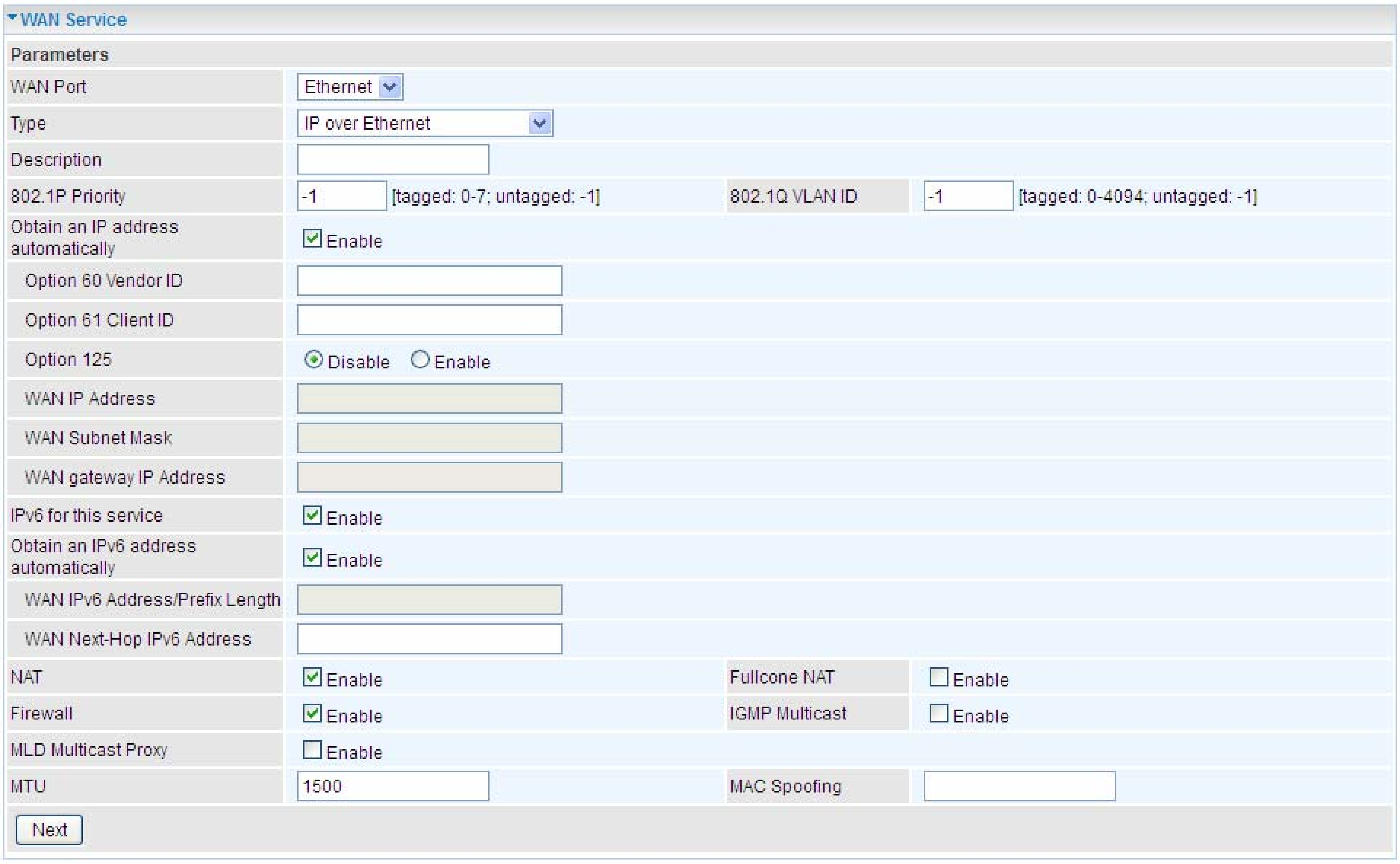
Device Information

Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 37M 26S
Date/Time	Mon Feb 17 01:53:31 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp0.1(Ehternet) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (Ehternet) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

IP over Ethernet



▾WAN Service

Parameters			
WAN Port	Ethernet		
Type	IP over Ethernet		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]
Obtain an IP address automatically	☑ Enable		
Option 60 Vendor ID			
Option 61 Client ID			
Option 125	● Disable ○ Enable		
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	☑ Enable		
Obtain an IPv6 address automatically	☑ Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	☑ Enable	Fullcone NAT	□ Enable
Firewall	☑ Enable	IGMP Multicast	□ Enable
MLD Multicast Proxy	□ Enable		
MTU	1500	MAC Spoofing	

Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

Here two modes are supported for users to deal with the IP and DNS. You can select obtain automatically or manually input the information according to your ISP.

Obtain an IP address automatically: Check whether to enable this function.

Option 60 Vendor ID: Enter the associated information by your ISP. This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors may choose to define specific vendor class identifiers to convey particular configuration or other identification information about a client.

Option 61 Client ID: Enter the associated information provided by your ISP.

Option 125: Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate option 125 message into DHCP offer packet before forward it to clients. After the clients receive the packet, it check the option 125 field in the packet with the pre-stored message, if it is matched, then the client accepts this offer, otherwise it will be abandoned. Check Enable or Disable this function. Default setting is ***Disable***.

WAN IP Address: Enter your IPv4 address to the device provided by your ISP.

WAN Subnet Mask: Enter your submask to the device provided by your ISP.

WAN gateway IP Address: Enter your gateway IP address to the device provided by your ISP.

IPv6 for this service: Enable to use IPv6 service.

Obtain an IPv6 address automatically: check whether to enable or disable this feature.

WAN IPv6 Address/Prefix Length: Enter the WAN IPv6 Address/Prefix Length from your ISP.

WAN Next-Hop IPv6 Address: Enter the WAN Next-Hop IPv6 Address from your ISP.

Note: If you don't know well about the DHCP Option, you can leave it empty or leave it as default.

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 to access the Internet, NAT function can be disabled. When enabled, a Fullcone NAT parameter will appear, you can determine whether to enable Fullcone NAT. While only NAT enabled, the default NAT type Port-Restricted cone NAT will be used.

Fullcone NAT: Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

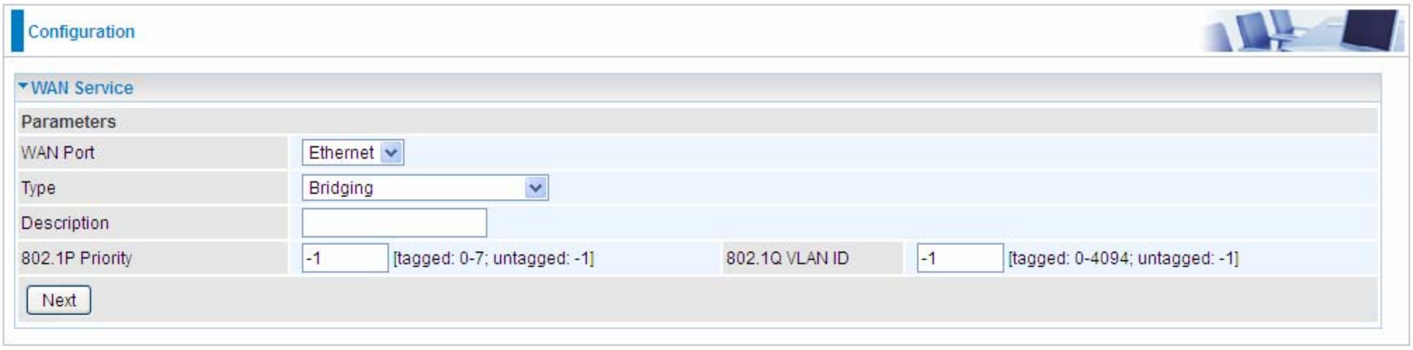
IGMP Multicast: IGMP (**Internet Group Membership** Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast routers. Check this item to enable IGMP multicast on that WAN interface for multicast forwarding.

MLD Multicast Proxy: check whether to enable this function. MLD (**Multicast Listener Discovery** Protocol) Proxy intercepts the MLD request from Clients a set up the multicast-forwarding table. it takes over some of the router's job, simplifying the router's job and multicast communication. Support MLDv1 and MLDv2.

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

MAC Spoofing: This option is required by some service providers specifying some specific MAC allowed to join in network. You must fill in the MAC address specified by your service provider when this information is required.

Bridging



Configuration

WAN Service

Parameters			
WAN Port	Ethernet		
Type	Bridging		
Description			
802.1P Priority	-1 [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	-1 [tagged: 0-4094; untagged: -1]

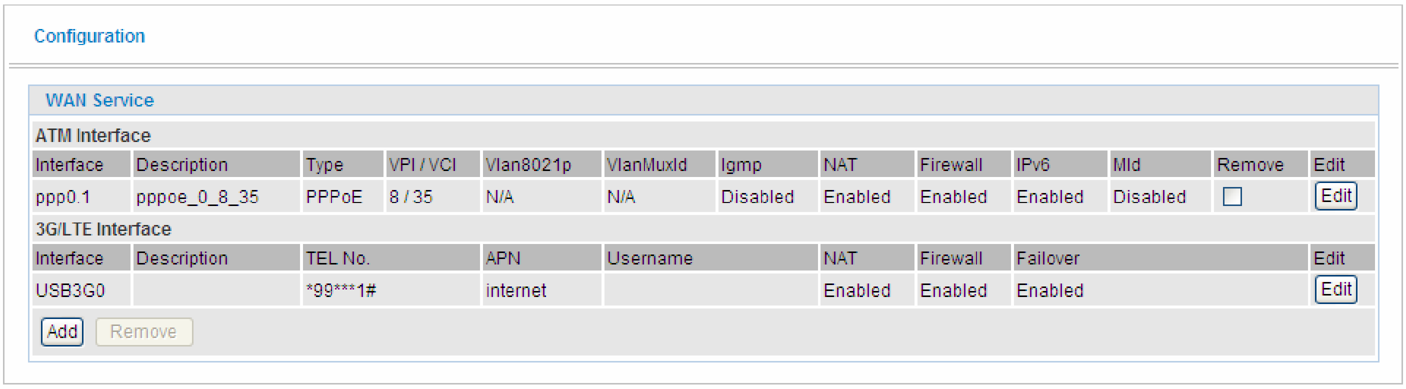
Description: User-defined description for the connection, commonly for friendly use.

802.1P Priority: The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

802.1Q VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

ⓘ 3G/LTE

Select 3G/LTE to configure the route to enjoy the mobility. By default the 3G/LTE interface is on, user can edit the parameters to meet your own requirements.



Configuration

WAN Service

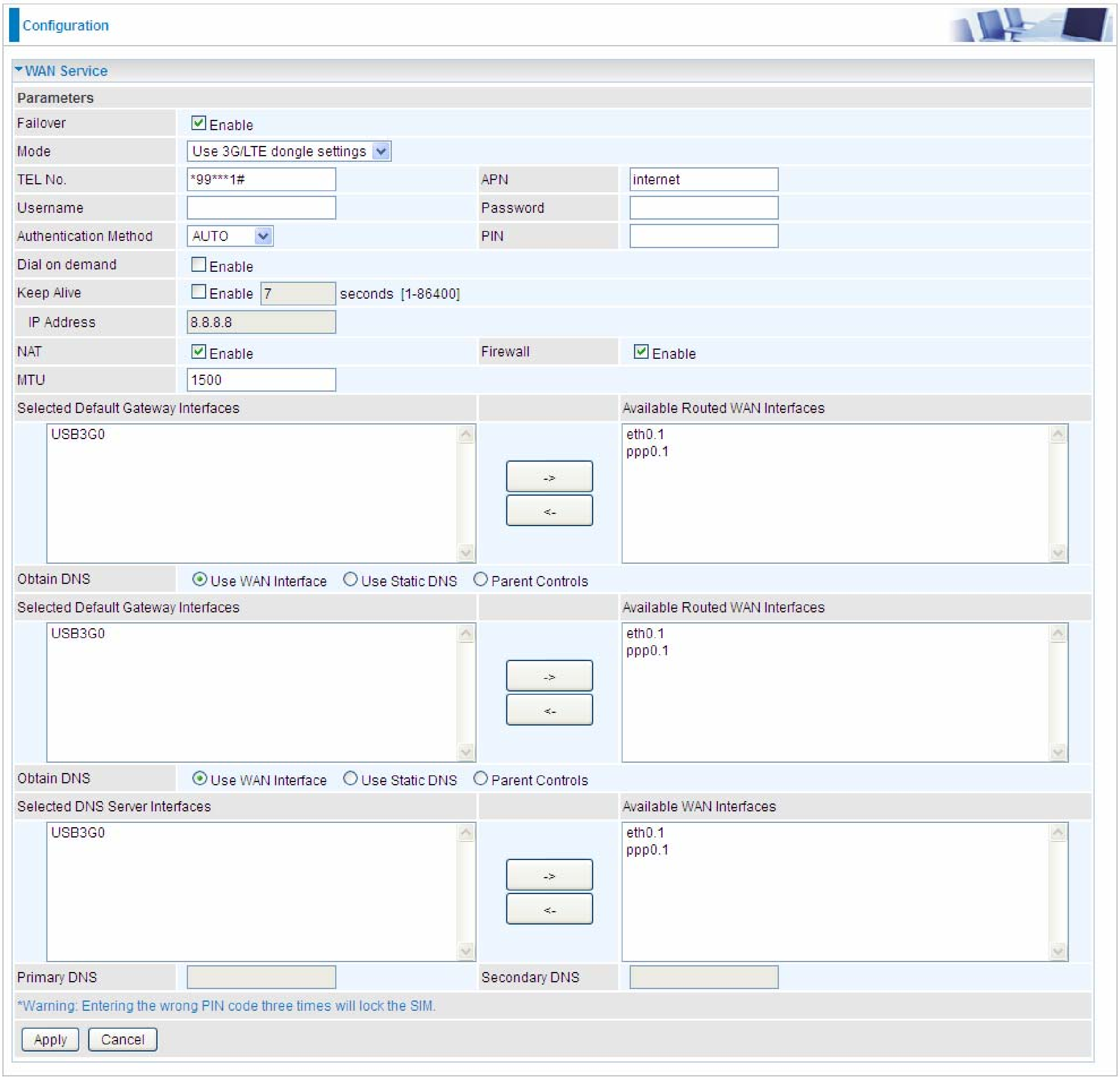
ATM Interface

Interface	Description	Type	VPI / VCI	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8 / 35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	□	Edit

3G/LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Failover	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	Edit

Click **Edit** button to enter the 3G/LTE configuration page.



Configuration

WAN Service

Parameters

Failover	☑ Enable		
Mode	Use 3G/LTE dongle settings		
TEL No.	*99***1#	APN	internet
Username		Password	
Authentication Method	AUTO	PIN	
Dial on demand	□ Enable		
Keep Alive	□ Enable 7 seconds [1-86400]		
IP Address	8.8.8.8		
NAT	☑ Enable	Firewall	☑ Enable
MTU	1500		

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
USB3G0	-> <-	eth0.1 ppp0.1

Obtain DNS ● Use WAN Interface ○ Use Static DNS ○ Parent Controls

Selected Default Gateway Interfaces		Available Routed WAN Interfaces
USB3G0	-> <-	eth0.1 ppp0.1

Obtain DNS ● Use WAN Interface ○ Use Static DNS ○ Parent Controls

Selected DNS Server Interfaces		Available WAN Interfaces
USB3G0	-> <-	eth0.1 ppp0.1

Primary DNS		Secondary DNS	

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

Failover: If enabled, the 3G/LTE will work in failover mode and be brought up only when there is no active default route. In this mode, 3G/LTE work as a backup for the WAN connectivity. While if disabled, 3G/LTE serves as a normal interface, and can only be brought up when it has been configured to achieve a mobile connectivity.

Mode: There are 6 options of phone service standards: GSM 2G only, UTMS 3G only, GSM 2G preferred, UMTS 3G preferred, Automatic, and Use 3G/LTE 3g dongle settings. If you are uncertain what services are available to you, and then please select Automatic.

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

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

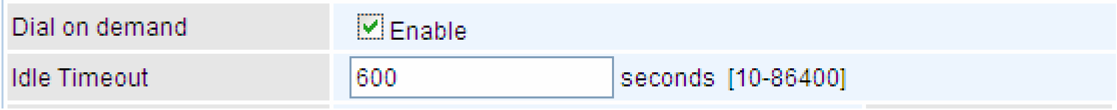
Username/Password: Enter the username and password provided by your service provider. The username and password are case sensitive.

Authentication Protocol: Default is Auto. Please consult your service provider on whether to use PAP, CHAP or MSCHAP.

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

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

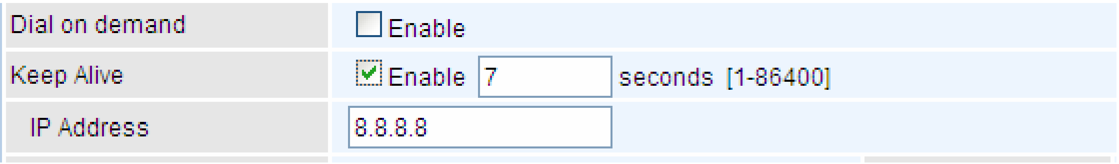
  Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time. Default is 600 seconds.



Dial on demand	☑ Enable	
Idle Timeout	600	seconds [10-86400]

- ⓘ **Keep Alive:** Check Enable to allow the router to send message out every 7 seconds (can be changed base on need) to prevent the connection being dropped by ISP.

  IP Address: The IP address is used to "ping", and router will ping the IP to find whether the connection is still on.



Dial on demand	□ Enable	
Keep Alive	☑ Enable 7	seconds [1-86400]
IP Address	8.8.8.8	

NAT: Check to enable the NAT function.

Firewall: Enable to drop all traffic from WAN side. If enabled, all incoming packets by default would be dropped, and please turn to IP Filtering Incoming to add allowing rules.

MTU: MTU (Maximum Transmission Unit) is the size of the largest datagram that IP will attempt to send through the interface.

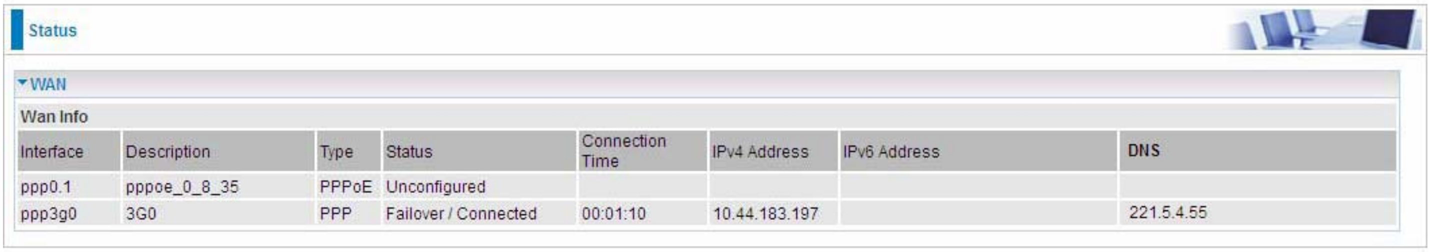
Select default gateway interfaces: Select from the interfaces the default gateway, here commonly we select ppp3g0.

Selected DNS Server Interfaces: Three ways to set a DNS server.

- **Available WAN interfaces:** Select a desirable WAN interface as the DNS server.
- **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

Click **Apply** to confirm the settings.

Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information (Here user can see the 3G/LTE failover).

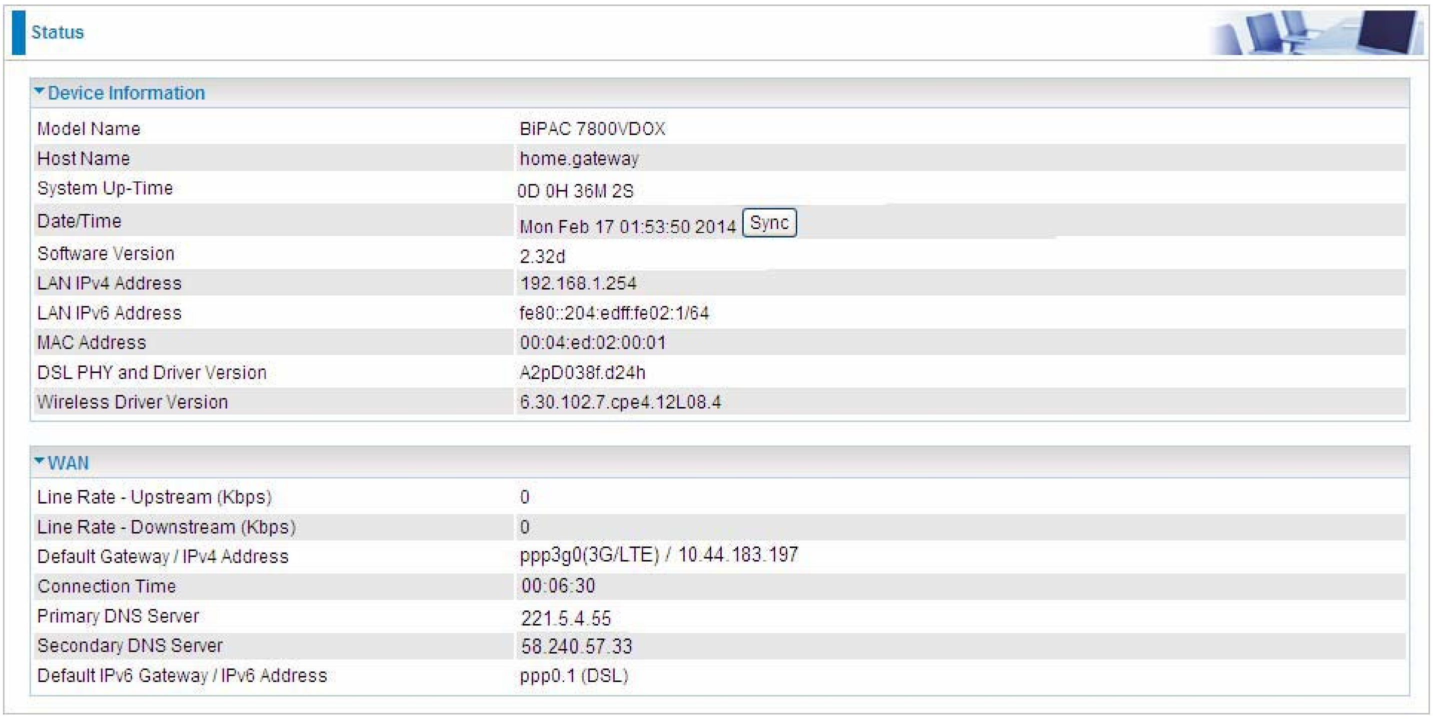


Status

WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Unconfigured				
ppp3g0	3G0	PPP	Failover / Connected	00:01:10	10.44.183.197		221.5.4.55



Status

Device Information

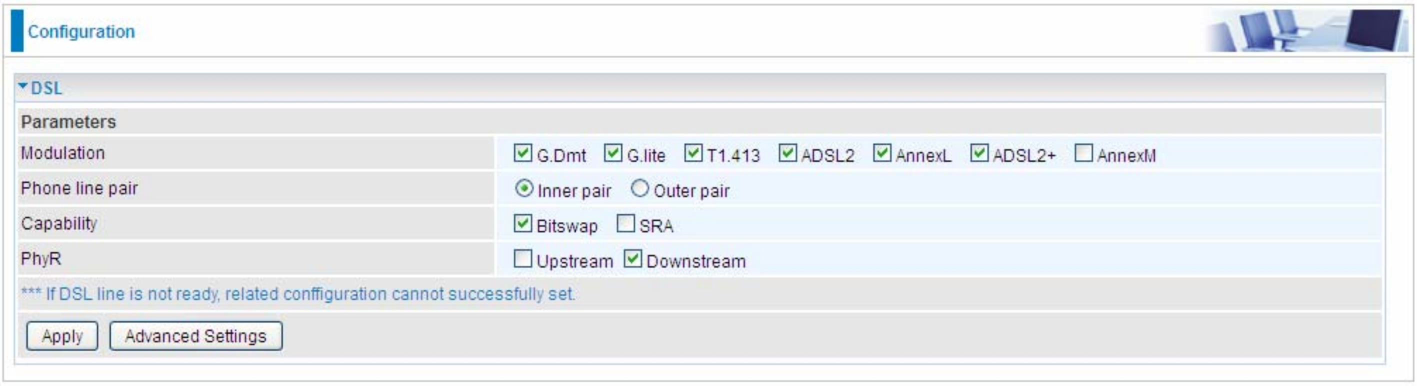
Model Name	BiPAC 7800VDOX
Host Name	home.gateway
System Up-Time	0D 0H 36M 2S
Date/Time	Mon Feb 17 01:53:50 2014 Sync
Software Version	2.32d
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe02:1/64
MAC Address	00:04:ed:02:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	ppp3g0(3G/LTE) / 10.44.183.197
Connection Time	00:06:30
Primary DNS Server	221.5.4.55
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL)

DSL

This screen allows you to set DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.



Parameters	
Modulation	☑ G.Dmt ☑ G.lite ☑ T1.413 ☑ ADSL2 ☑ AnnexL ☑ ADSL2+ ☐ AnnexM
Phone line pair	● Inner pair ○ Outer pair
Capability	☑ Bitswap ☐ SRA
PhyR	☐ Upstream ☑ Downstream

*** If DSL line is not ready, related configuration cannot successfully set.

Modulation: There are 7 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, ”ADSL2+”, “AnnexM” that user can select for this connection.

Phone line pair: This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

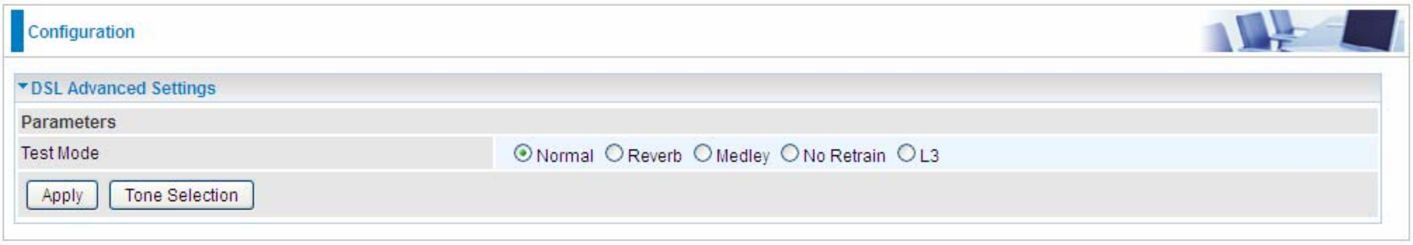
Capability: There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- Bitswap Enable: Allows bitswaping function.
- SRA Enable: Allows seamless rate adaptation.

PhyR: A new technology to control impulse and noise to improve the BER and DSL data quality.

Click **Apply** to confirm the settings.

Click Advanced Settings to future configure DSL.



Parameters	
Test Mode	● Normal ○ Reverb ○ Medley ○ No Retrain ○ L3

Select the Test Mode, or leave it as default.

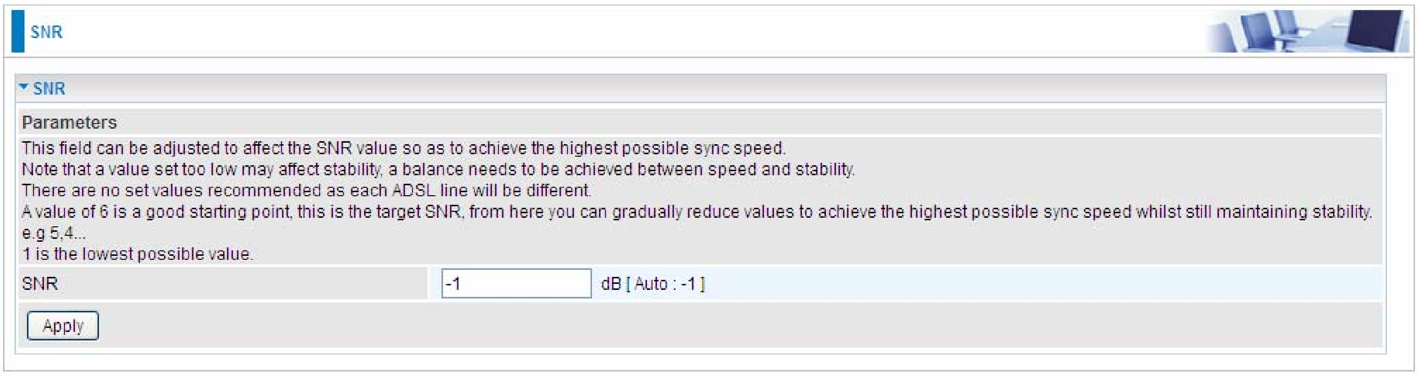
Tone Selection: This should be left as default or be configured by an advanced user.

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream。

SNR

Signal-to-noise ratio (often abbreviated **SNR** or **S/N**) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.



This field can be adjusted to affect the SNR value so as to achieve the highest possible sync speed.
Note that a value set too low may affect stability, a balance needs to be achieved between speed and stability.
There are no set values recommended as each ADSL line will be different.
A value of 6 is a good starting point, this is the target SNR, from here you can gradually reduce values to achieve the highest possible sync speed whilst still maintaining stability.
e.g 5,4...
1 is the lowest possible value.

SNR: -1 dB [Auto : -1]

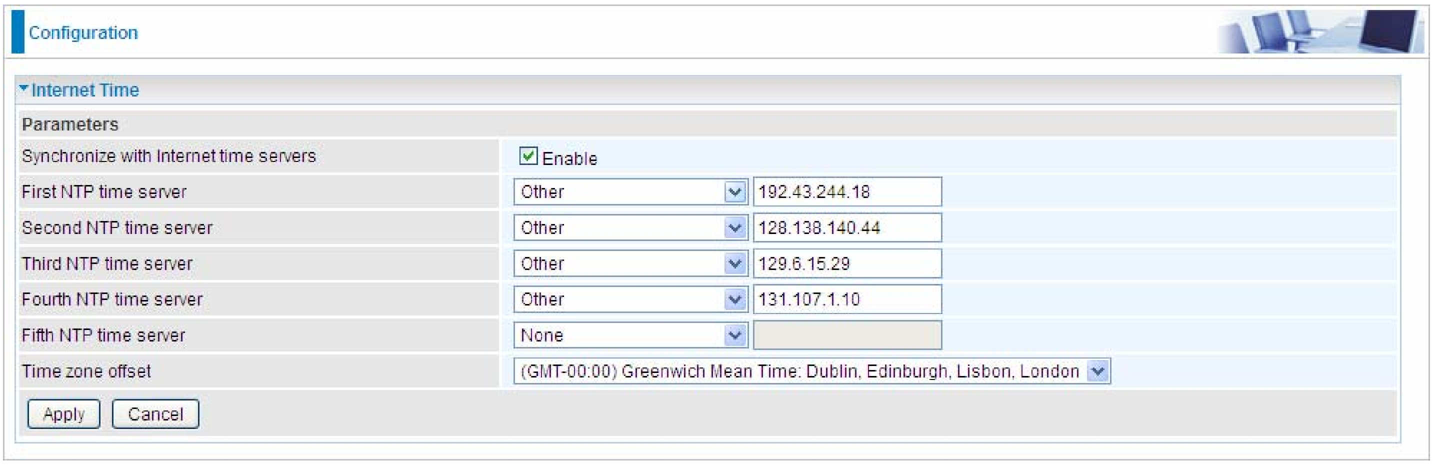
SNR: Change the value to adjust the DSL link rate, more suitable for an advanced user.

System

Internet Time

The router does not have a real time clock on board; instead, it uses the Network Time Protocol (NTP) to get the most current time from an NTP server.

NTP is a protocol for synchronization of computers. It can enable computers synchronize to the NTP server or clock source with a high accuracy.



Configuration

Internet Time

Parameters		
Synchronize with Internet time servers	☑ Enable	
First NTP time server	Other	192.43.244.18
Second NTP time server	Other	128.138.140.44
Third NTP time server	Other	129.6.15.29
Fourth NTP time server	Other	131.107.1.10
Fifth NTP time server	None	
Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	

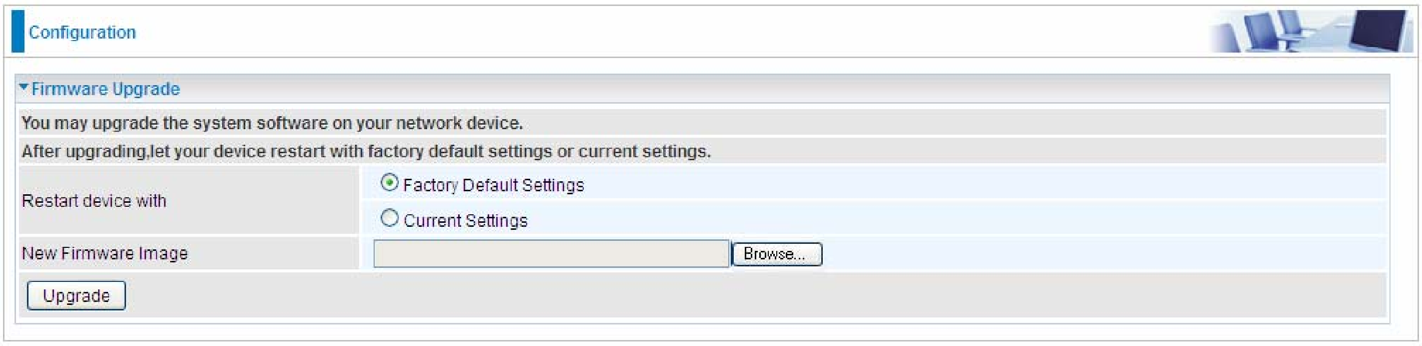
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP 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 NTP server for you to use.

Click **Apply** to apply your settings.

Firmware Upgrade

Software upgrading lets you experience new and integral functions of your router.



Configuration

▾Firmware Upgrade

You may upgrade the system software on your network device.

After upgrading,let your device restart with factory default settings or current settings.

Restart device with	● Factory Default Settings ○ Current Settings
New Firmware Image	[ ] Browse...

Upgrade

Restart device with:

- **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.
- **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.

Your router’s “firmware” is the software that allows it to operate and provides all its functionality.

Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

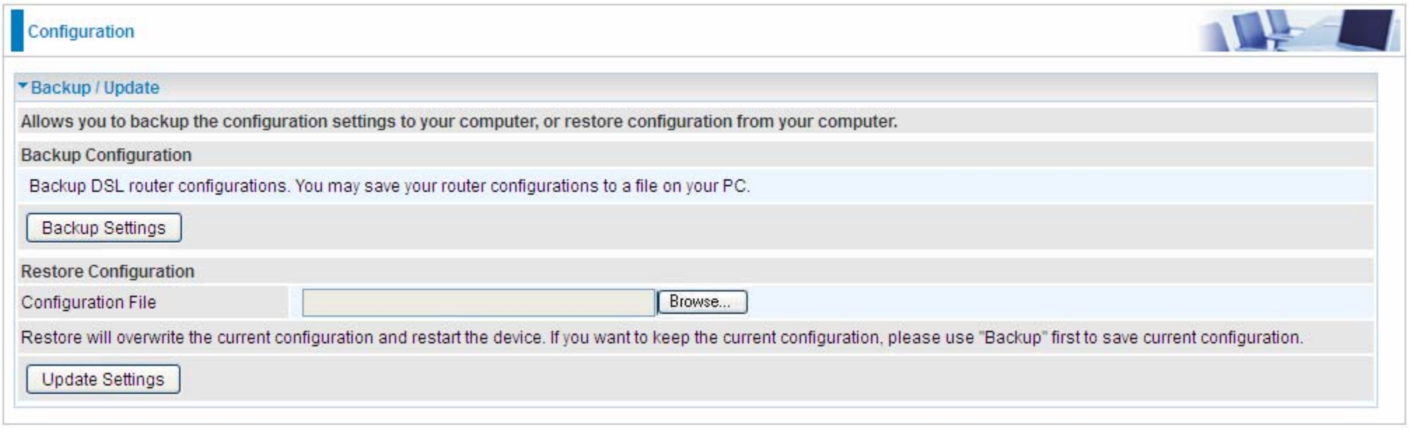
Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click **Upgrade** to update the firmware in your router.

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 / Update

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



Configuration

▾Backup / Update

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

Backup Configuration

Backup DSL router configurations. You may save your router configurations to a file on your PC.

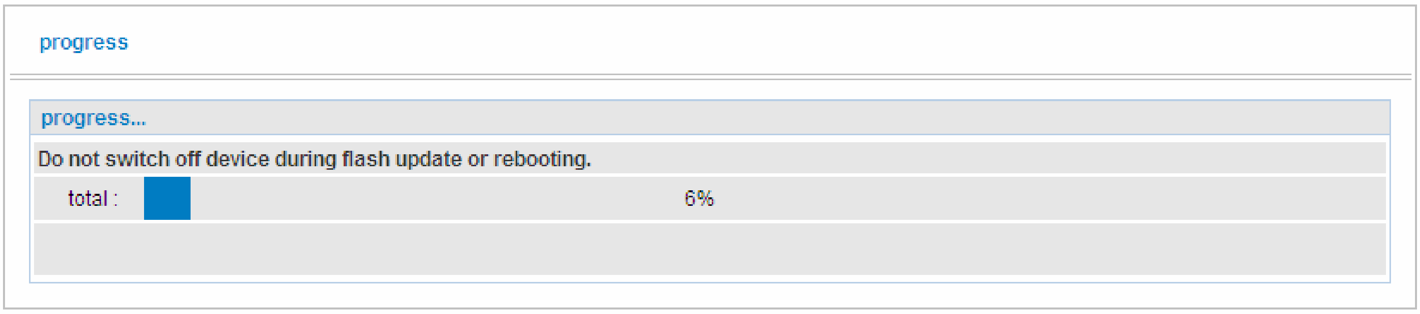
Restore Configuration

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.

Click **Backup Settings**, a window appears, click save , then browse the location where you want to save the backup file.

Click **Browse** and browse to the location where your backup file is saved, the click **Open.** Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.



progress

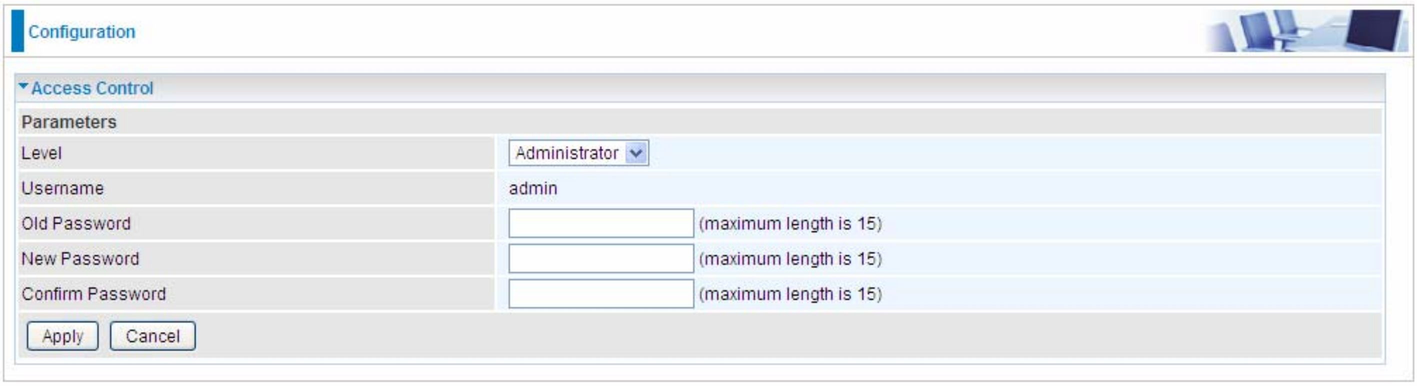
progress...

Do not switch off device during flash update or rebooting.

total : 6%

Access Control

Access Control is used to prevent unauthorized access to the router configuration page. Here you can change the login user password. Three user levels are provided here. Each user level there's a default provided user. You must access the router with the appropriate username and password. Here the corresponding passwords are allowed to change.



Parameters	
Level	Administrator
Username	admin
Old Password	(maximum length is 15)
New Password	(maximum length is 15)
Confirm Password	(maximum length is 15)

Level: select which level you want to change password to. There are three default levels.

- **Administrator:** the root user, corresponding default username and password are admin and admin respectively.
- **Remote:** username for the remote user to login, corresponding default username and password are support and support respectively.
- **Local:** username for the general user, when logon to the web page, only lit items would be listed for common user, corresponding default username password are user and user respectively.

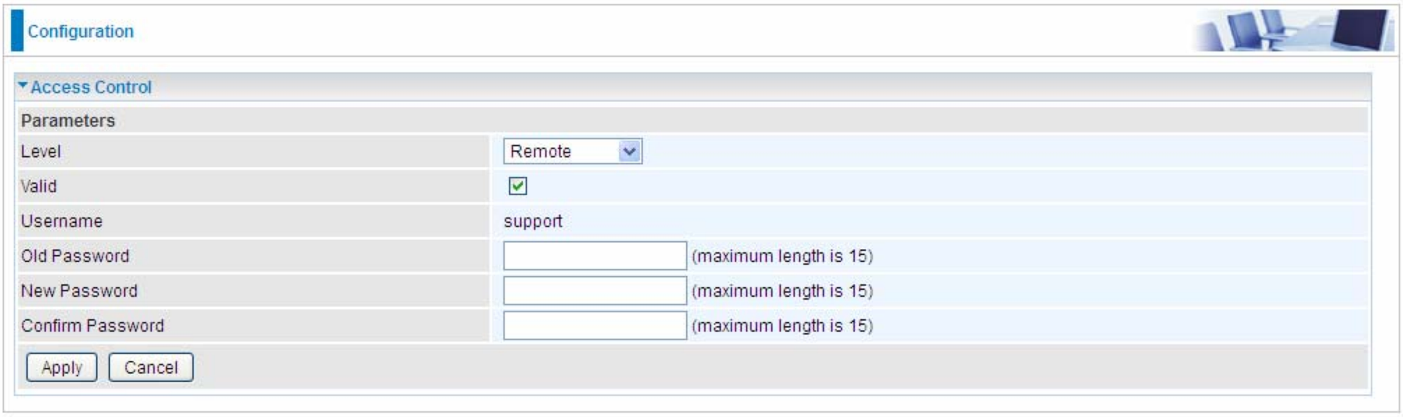
Username: the default username for each user level.

Old Password: Enter the old password.

New Password: Enter the new password.

Confirm Password: Enter again the new password to confirm.

Note: By default the accounts of **Remote** and **Local** are disabled, please click **Valid** check-box to activate the accounts.

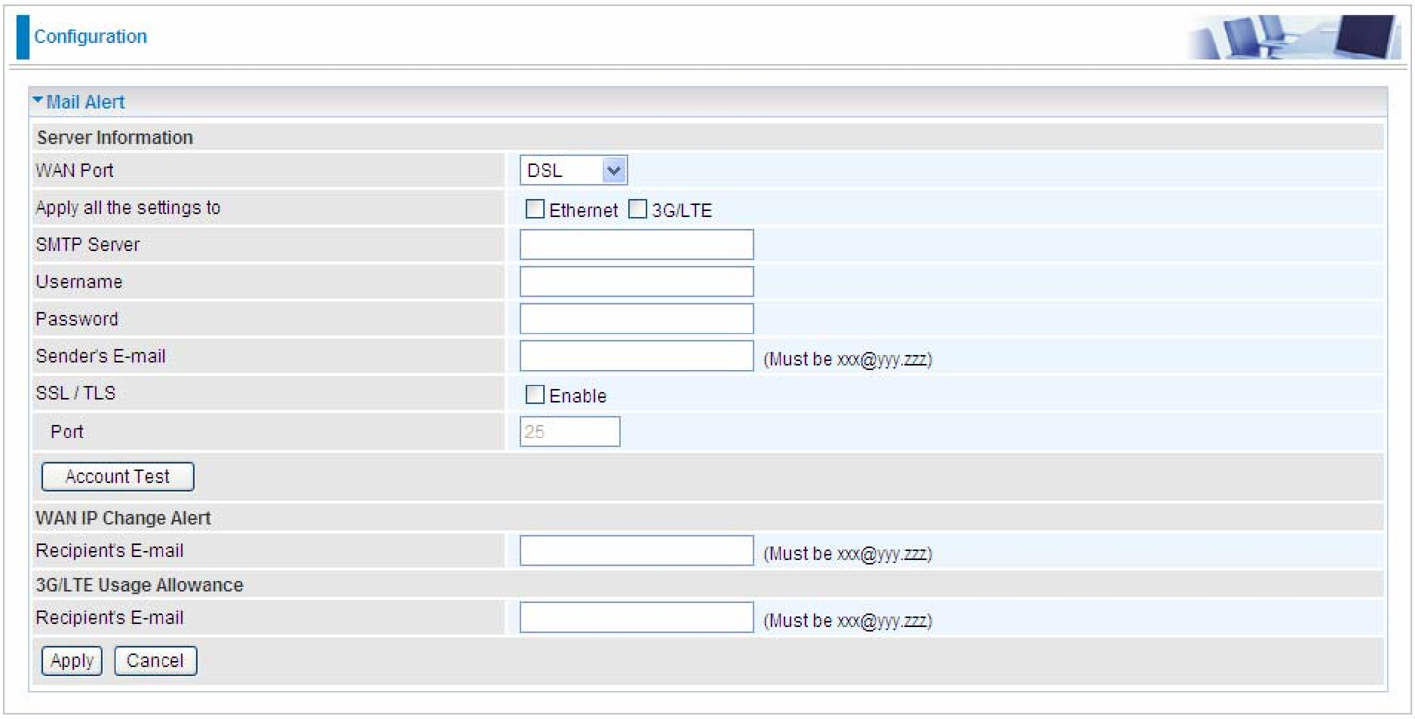


Parameters	
Level	Remote
Valid	☑
Username	support
Old Password	(maximum length is 15)
New Password	(maximum length is 15)
Confirm Password	(maximum length is 15)

Click **Apply** to apply your new settings.

Mail Alert

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



Configuration

▾Mail Alert

Server Information	
WAN Port	DSL
Apply all the settings to	□ Ethernet □ 3G/LTE
SMTP Server	
Username	
Password	
Sender's E-mail	(Must be xxx@yyy.zzz)
SSL / TLS	□ Enable
Port	25
Account Test	
WAN IP Change Alert	
Recipient's E-mail	(Must be xxx@yyy.zzz)
3G/LTE Usage Allowance	
Recipient's E-mail	(Must be xxx@yyy.zzz)

WAN Port: Mail Alert feature can be applicable to every WAN mode: Ethernet，DSL and 3G/LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

Apply all settings to: check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

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

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

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL: check to whether to enable SSL encryption feature.

Port: the port, default is 25.

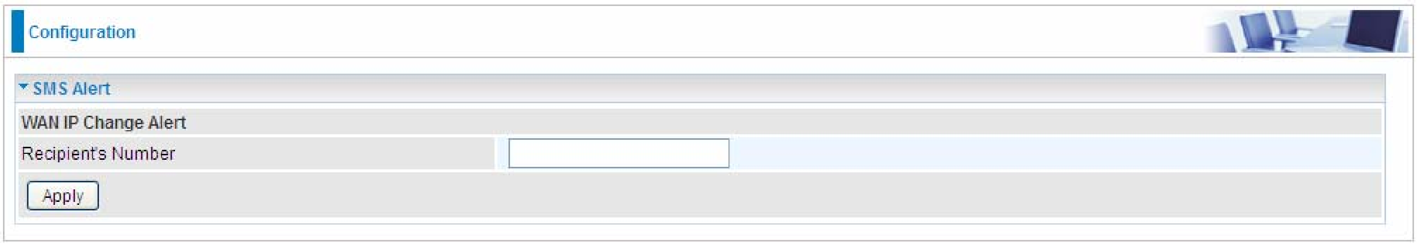
Account Test: Press this button to test the connectivity and feasibility to your sender's e-mail.

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

Recipient's Email (3G/LTE Usage Allowance): Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

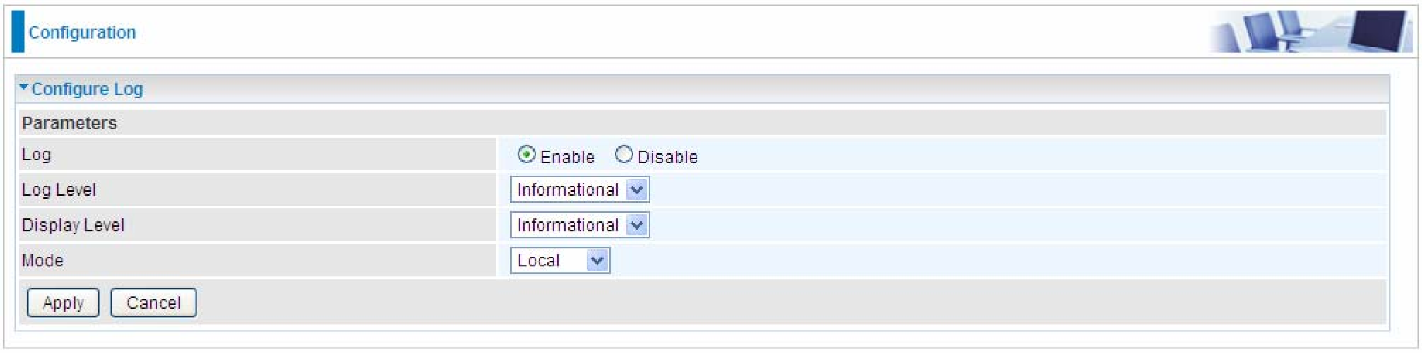
SMS Alert

SMS, Short Message Service, is to inform clients the information clients subscribe. The BiPAC 7800VDP(O)X offers SMS alert sending clients alert messages when a WAN IP change is detected.



Recipient’s Number (WAN IP Change Alert): Enter the Recipient’s number that will receive the alert message once a WAN IP change has been detected.

Configure Log



Configuration

Configure Log

Parameters	
Log	● Enable ○ Disable
Log Level	Informational
Display Level	Informational
Mode	Local

Log: Enable or disable this function.

Log level: Select your log level. The log level allows you to configure which types of events are logged. There are eight log levels from high to low are displayed below:

- **Emergency** = system is unusable
- **Alert** = action must be taken immediately
- **Critical** = critical conditions
- **Error** = error conditions
- **Warning** = warning conditions
- **Notice** = normal but significant conditions
- **Informational** = information events
- **Debugging** = debug-level messages

The gateway records all log events at the chosen level and above. For instance, if you set the log level to Critical, all critical, alert, and emergency events are logged, but none of the others are recorded

Display Level: Display the log according to the level you set when you view system log. Once you set the display level, the logs of the same or higher priority will be displayed.

Mode: Select the mode the system log adopted. Three modes: local, Remote and Both.

- **Local**: Select this mode to store the logs in the router's local memory.
- **Remote**: Select this mode to send the log information to a remote log server. Then you must assign the remote log server and port, 514 is often used.
- **Both**: Logs stored adopting above two ways.

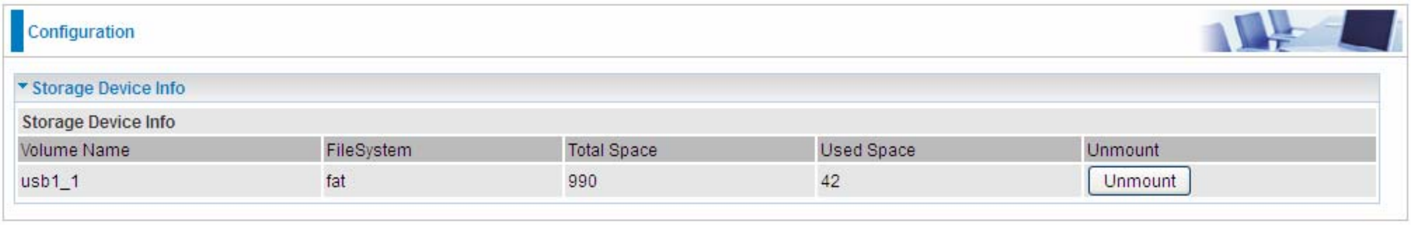
Click **Apply** to save your settings.

USB

Storage here refers to network sharing in the network environment, USB devices act as the storage carrier for DLNA, common file sharing.

Storage Device Info

This part provides users direct access to the storage information like the total volume, the used and the remaining capacity of the device.



Storage Device Info

Volume Name	FileSystem	Total Space	Used Space	Unmount
usb1_1	fat	990	42	Unmount

Volume Name: Display the storage volume name

FileSystem: Display the storage device’s file system format, well-known is FAT.

Total Space: Display the total space of the storage, with unit MB.

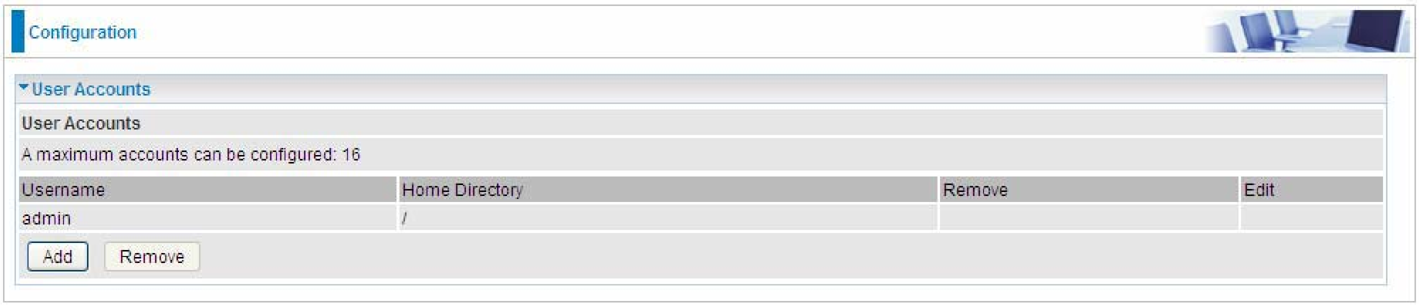
Used Space: Display the remaining space of each partition, unit MB.

Unmount: Click **Unmount** button if you want to uninstall the USB device. Please **Note** that first click **Unmount** before you uninstall your USB storage.

User Account

Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data.

Default user admin.

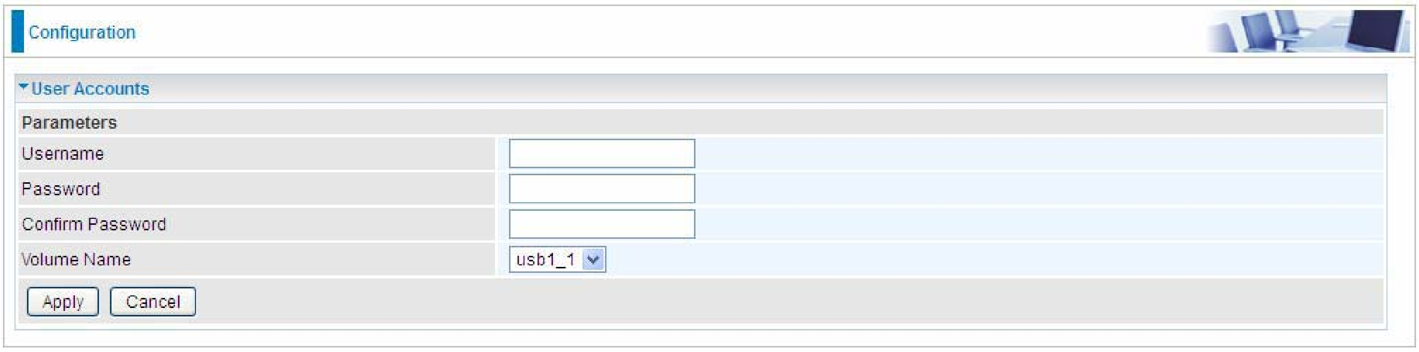


User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		

Click **Add** button, enter the user account-adding page:



Username	
Password	
Confirm Password	
Volume Name	usb1_1

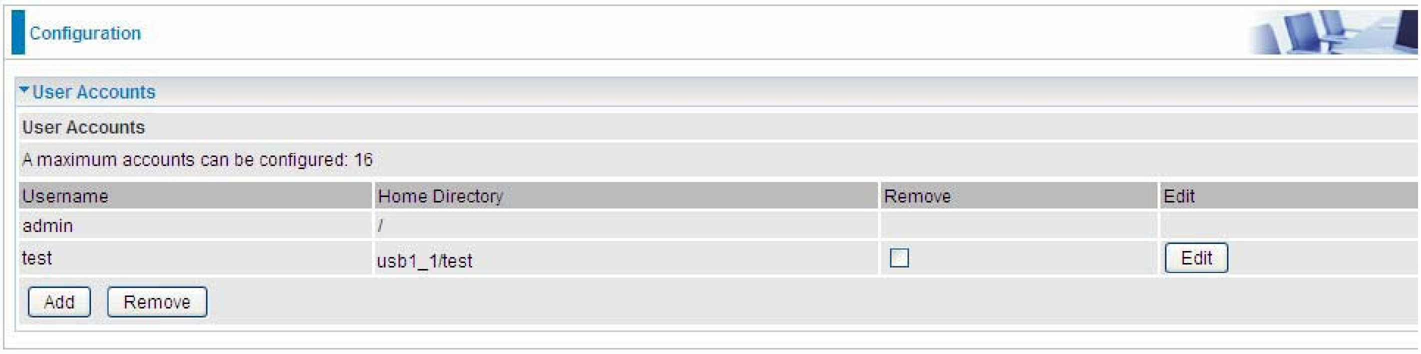
Username: user-defined name, but simpler and more convenient to remember would be favorable.

Password: Set the password.

Confirm Password: Reset the password for confirmation.

Volume Name: Select Volume name, as to create access to the volume of the specified partition of the storage.

For example, a user ***test*** is setup behind the usb1_1.



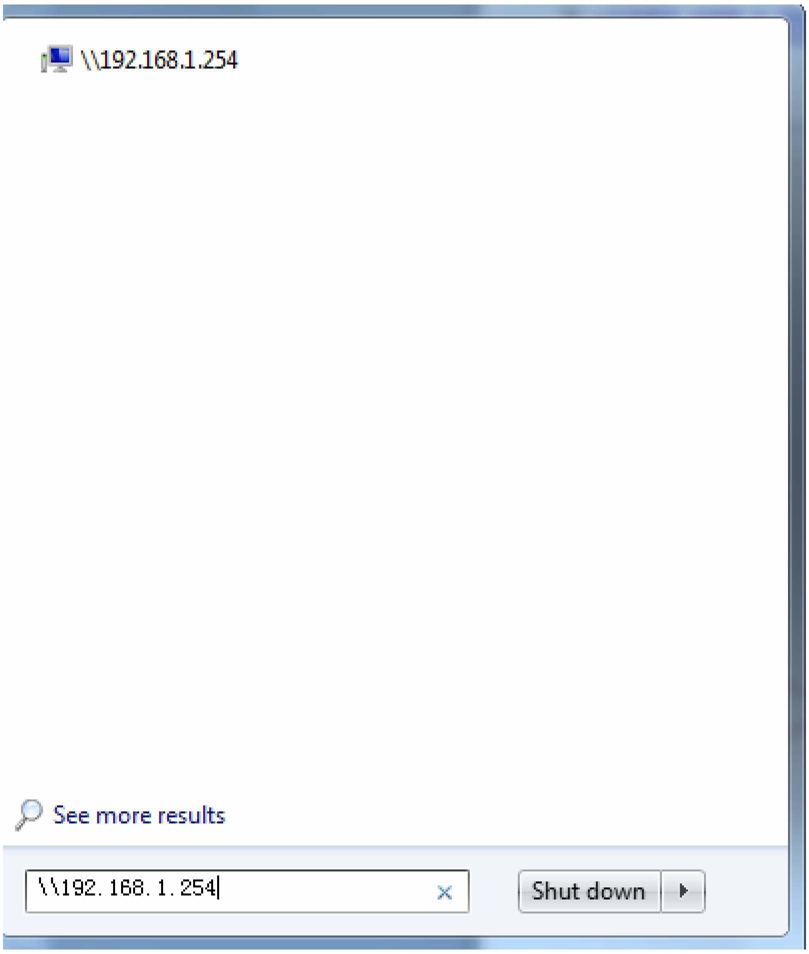
User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		
test	usb1_1/test	□	Edit

Accessing mechanism of Storage:

In your computer, Click **Start** > **Run**, enter \\192.168.1.254

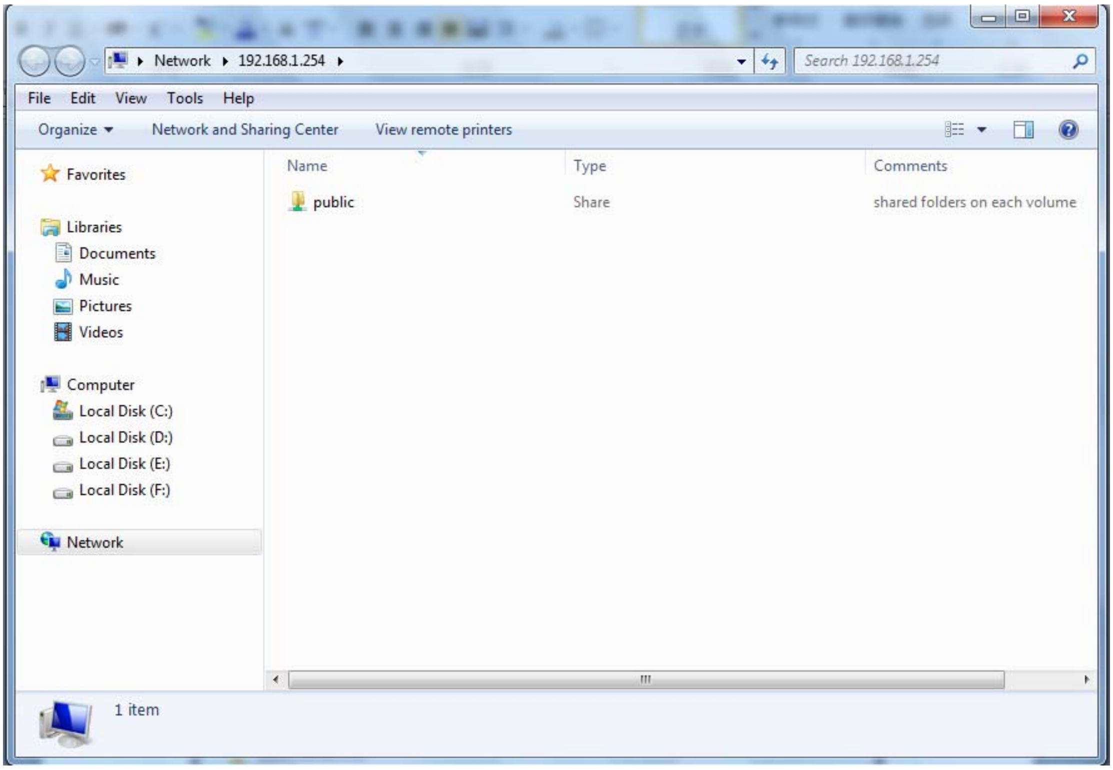


When accessing the network storage, you can see a folder named “***public***”, users should have the account to enter, and the account can be set at the User Accounts section.

When first logged on to the network folder, you will see the “***public***” folder.

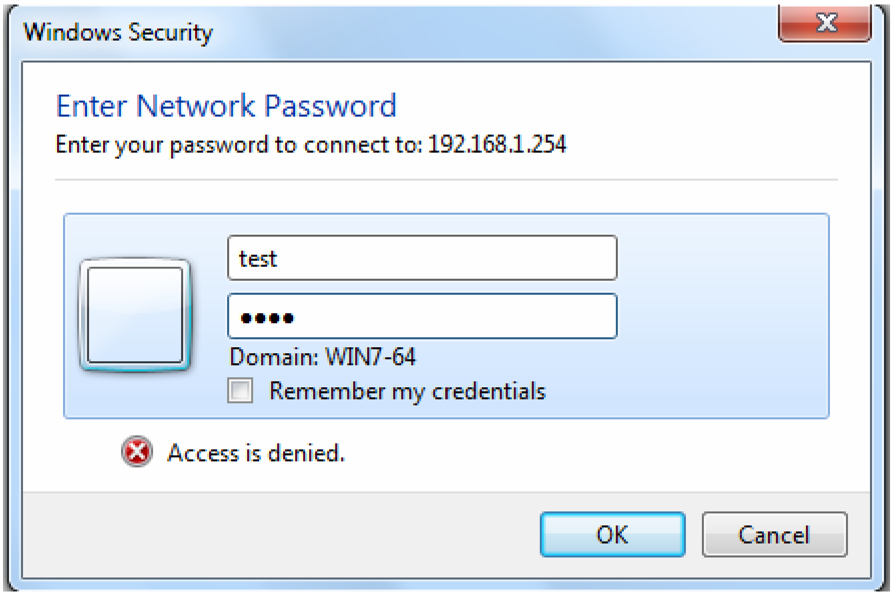
Public: The public sharing space for each user in the USB Storage.

When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



Name	Type	Comments
public	Share	shared folders on each volume

Access the folder ***public***.



Windows Security

Enter Network Password

Enter your password to connect to: 192.168.1.254

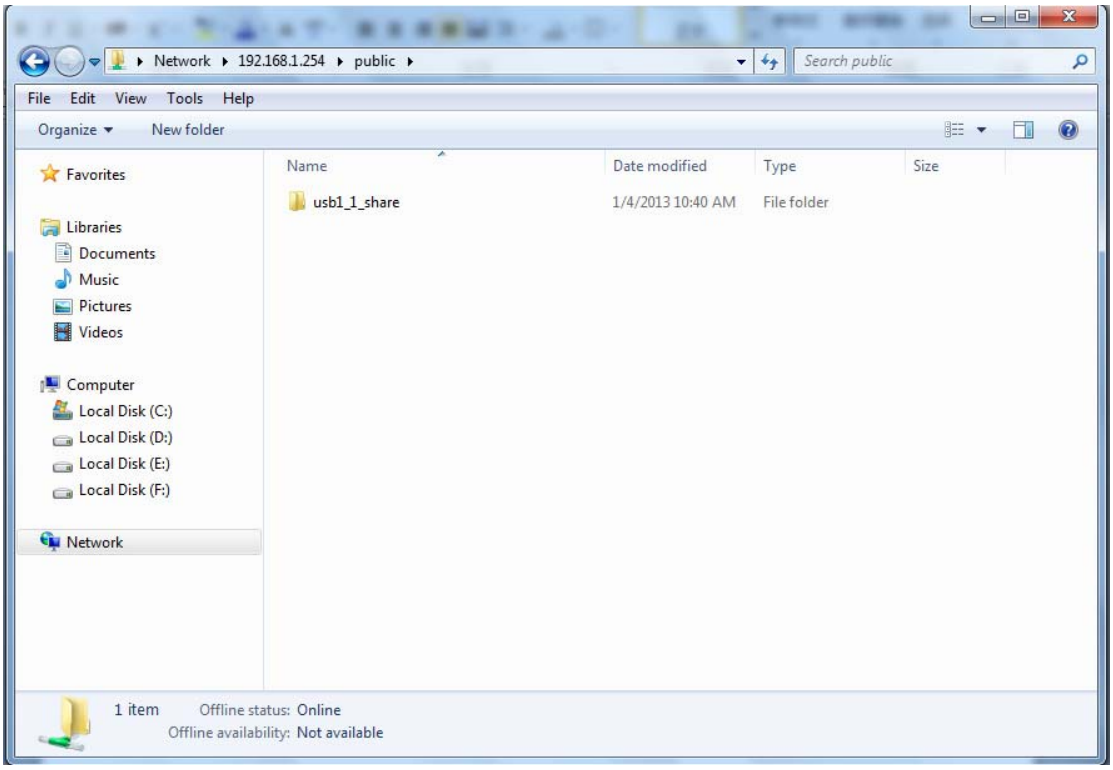
test

●●●●

Domain: WIN7-64

□ Remember my credentials

Access is denied.

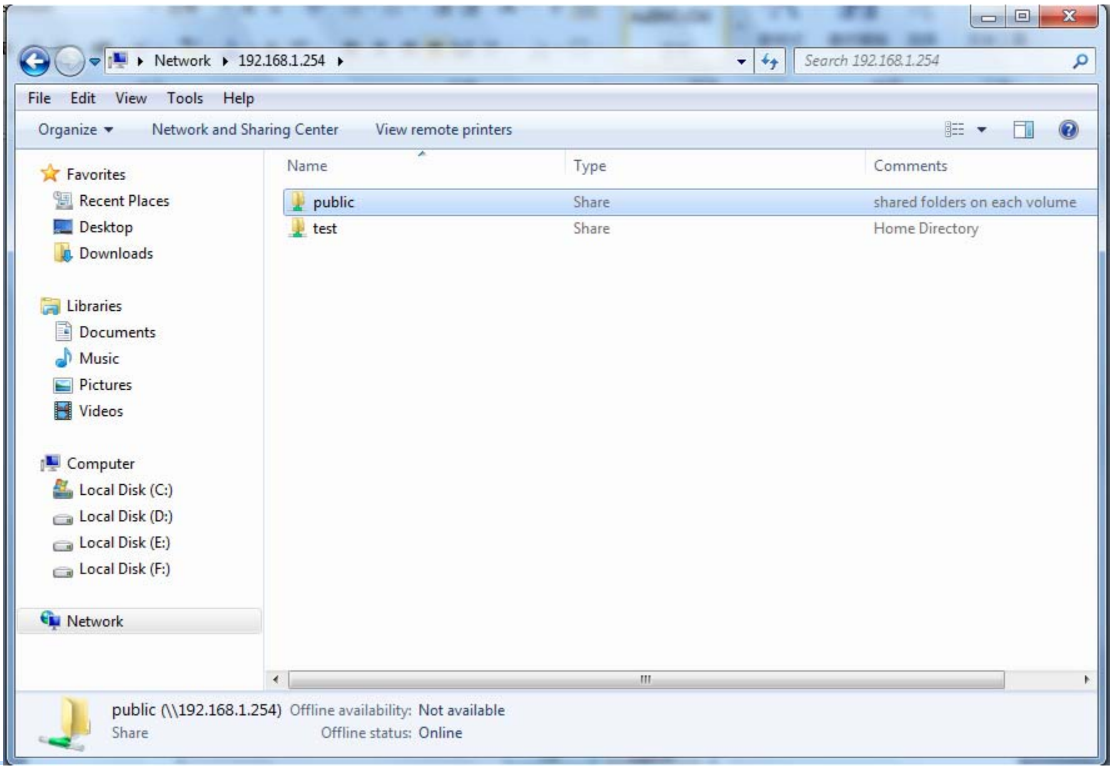


Name	Date modified	Type	Size
usb1_1_share	1/4/2013 10:40 AM	File folder	

1 item Offline status: Online

Offline availability: Not available

When successfully accessed, the private folder of each user is established, and user can see from the following picture. The ***test*** fold in the picture is the private space for each user.



Name	Type	Comments
public	Share	shared folders on each volume
test	Share	Home Directory

public (\\192.168.1.254) Offline availability: Not available
Share Offline status: Online

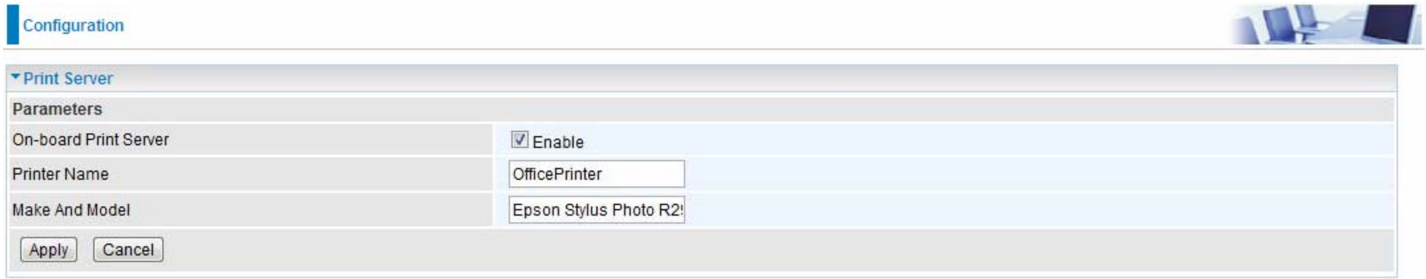
Print Server

The Print Server feature allows you to share a printer on your network by connecting a USB cable from your printer to the USB port on the 7800VDPX. This allows you to print from any location on your network.

Note: Only USB printers are supported

Setup of the printer is a 3 step process

1. Connect the printer to the 7800VDPX's USB port
2. Enable the print server on the 7800VDPX
3. Install the printer drivers on the PC you want to print from



Configuration

Print Server

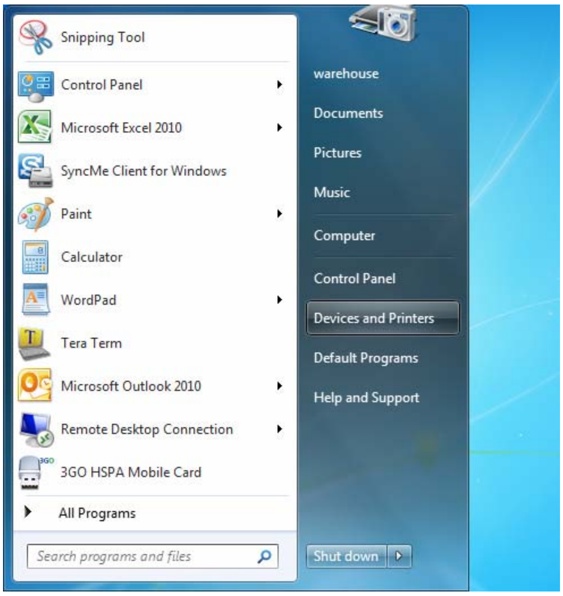
Parameters	
On-board Print Server	☑ Enable
Printer Name	OfficePrinter
Make And Model	Epson Stylus Photo R2!

On-board Print Server: Check Enable to activate the print server
Printer Name: Enter the Printer name, for example, *OfficePrinter*
Make and Model: Enter in the Make and Model information for the printer, for example, *Epson Stylus Photo R290*

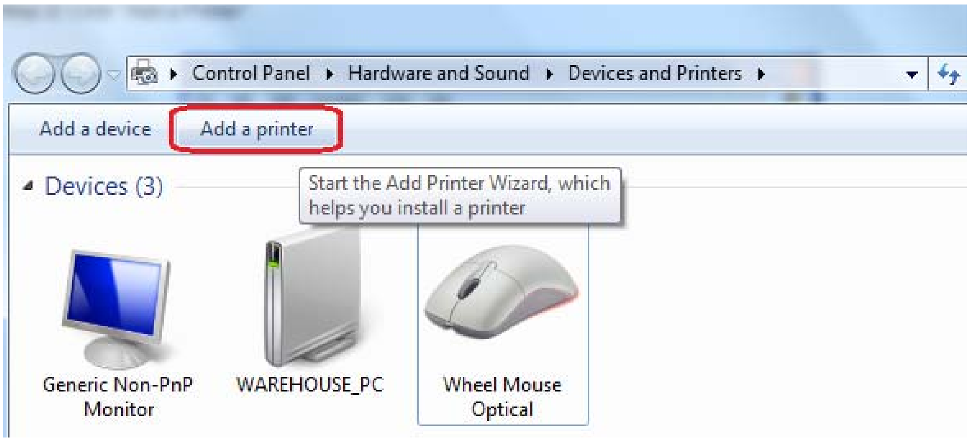
Note:
The ***Printer name*** can be any text string up to **40** characters. It cannot contain spaces.
The ***Make and Mode***l can be any text string up to **128** characters.

Set up of Printer client (Windows 7)

Step 1: Click **Start** and select "Devices and Printers"

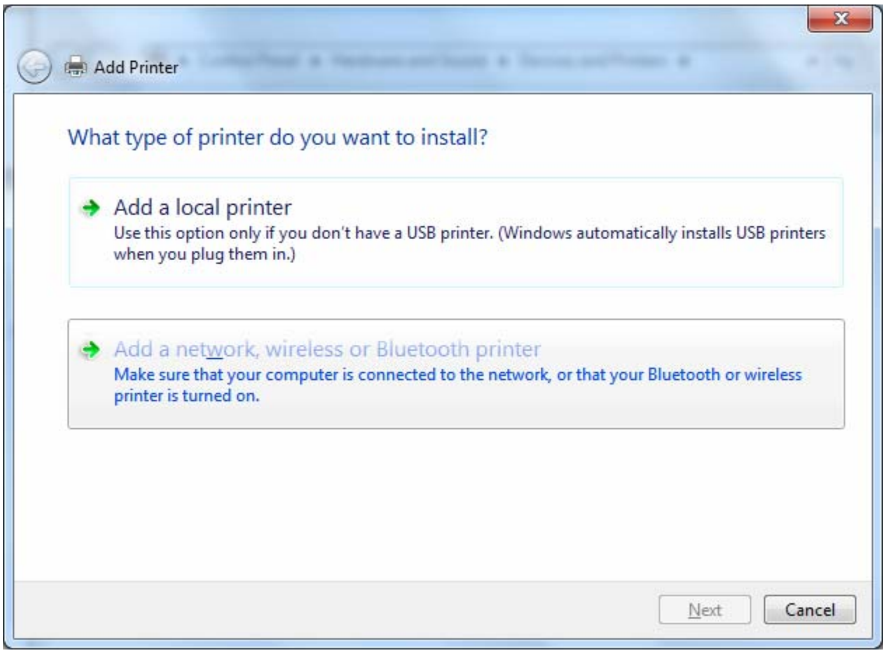


Step 2: Click ''Add a Printer''.



Start the Add Printer Wizard, which helps you install a printer

Step 3: Click “Add a network, wireless or Bluetooth printer



What type of printer do you want to install?

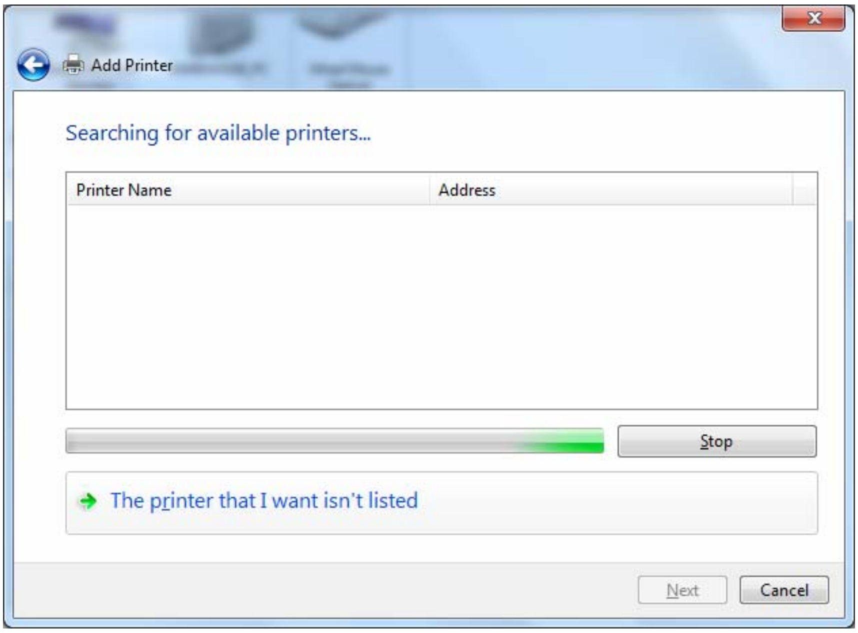
Add a local printer

Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer

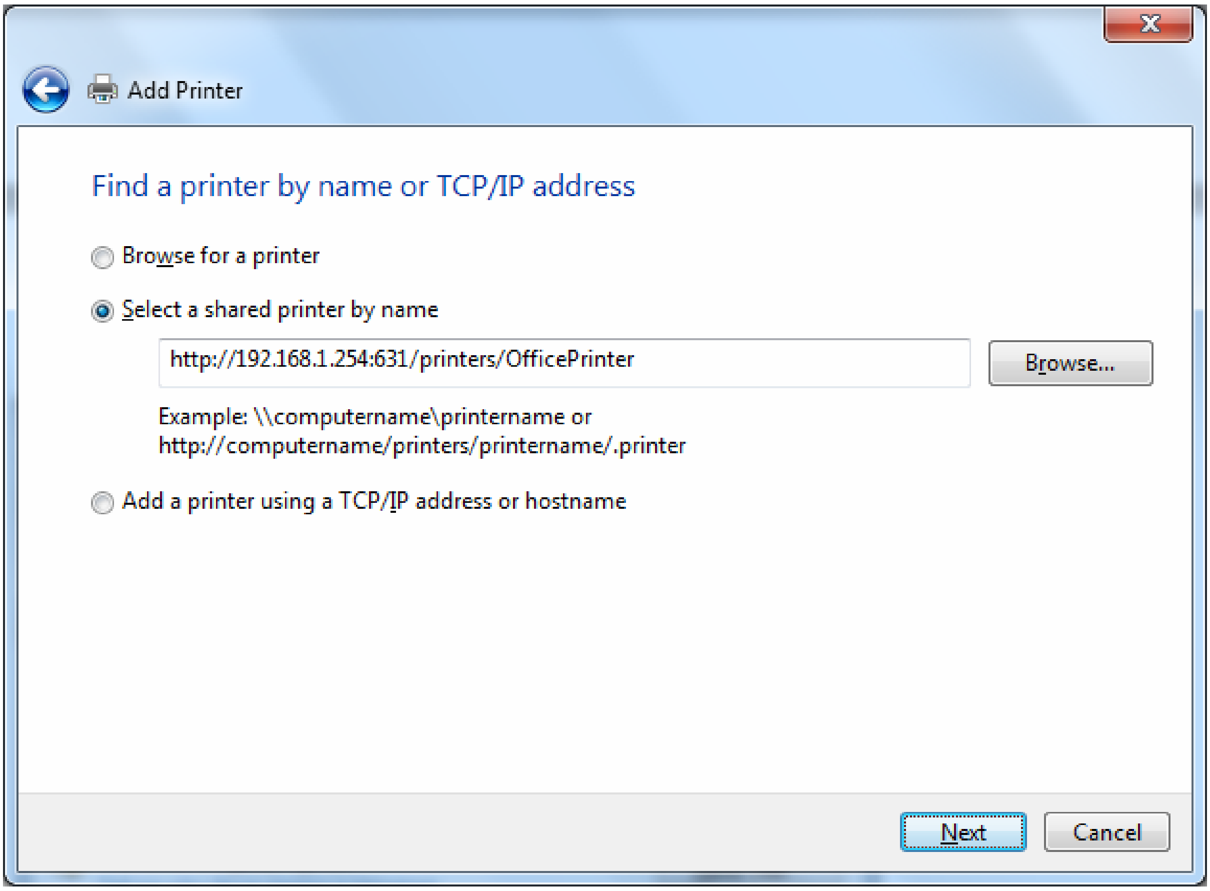
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

Step 4: Click "The printer that I want isn't listed"


Add Printer

Searching for available printers...

Step 5: Select "Select a shared printer by name"
Enter http://7800VDPX- LAN-IP:631/printers/printer-name or. Make sure printer's name is the same as what you set in the 7800VDPX earlier
For Example: *http://192.168.1.254:631/printers/OfficePrinter*
OfficePrinter is the Printer Name we setup earlier


Add Printer

Find a printer by name or TCP/IP address

○ Browse for a printer

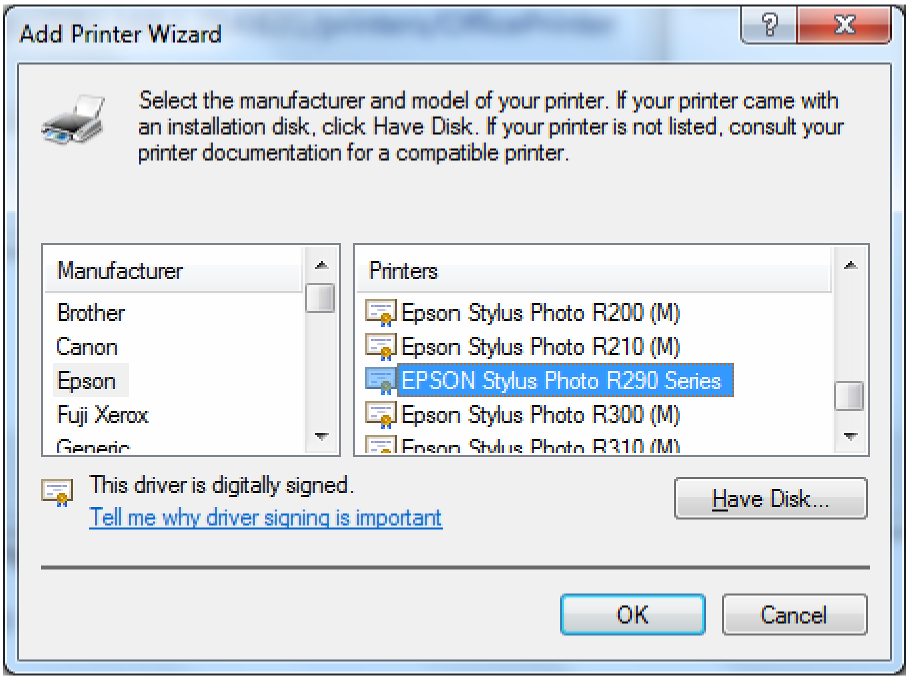
● Select a shared printer by name

http://192.168.1.254:631/printers/OfficePrinter

Example: \\computername\printername or
http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname

Step 6: Click "Next" to add the printer driver. If your printer is not listed and your printer came with an installation disk, click "Have Disk" find it and install the driver.

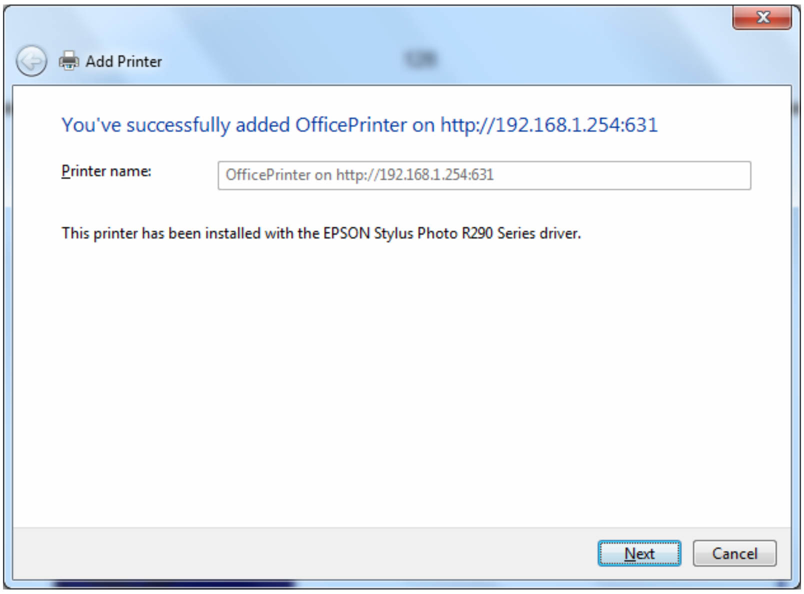


Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

Manufacturer	Printers
Brother	Epson Stylus Photo R200 (M)
Canon	Epson Stylus Photo R210 (M)
Epson	EPSON Stylus Photo R290 Series
Fuji Xerox	Epson Stylus Photo R300 (M)
Generic	Epson Stylus Photo R310 (M)

This driver is digitally signed.
Tell me why driver signing is important

Step 7: Click "Next"

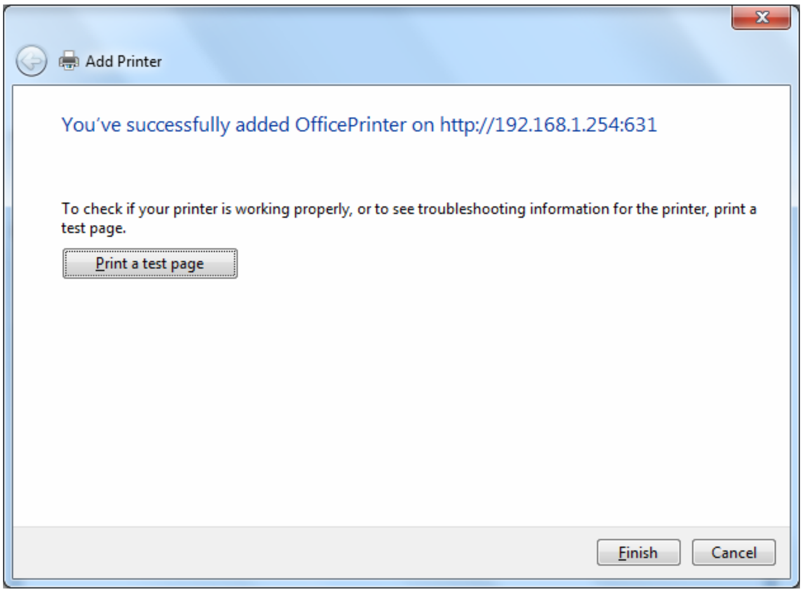


You've successfully added OfficePrinter on http://192.168.1.254:631

Printer name: OfficePrinter on http://192.168.1.254:631

This printer has been installed with the EPSON Stylus Photo R290 Series driver.

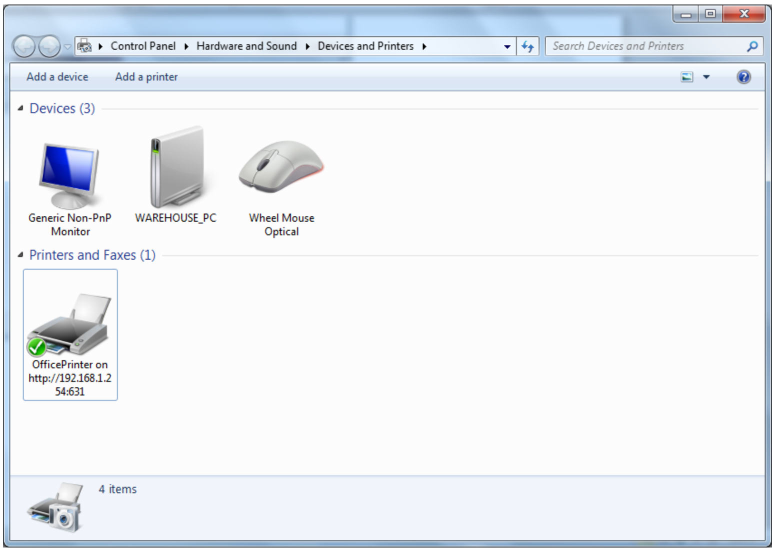
Step 8: Click "Next" and you are done



You've successfully added OfficePrinter on http://192.168.1.254:631

To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.

You will now be able to see your printer on the Devices and Printers Page



Control Panel ▸ Hardware and Sound ▸ Devices and Printers ▸
Search Devices and Printers
Add a device
Add a printer
Devices (3)
Generic Non-PnP Monitor
WAREHOUSE_PC
Wheel Mouse Optical
Printers and Faxes (1)
OfficePrinter on http://192.168.1.254:631
4 items

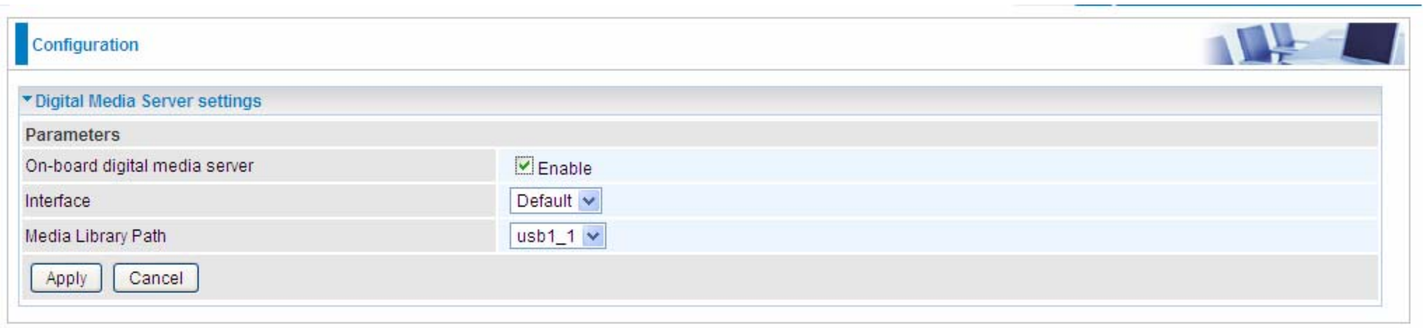
DLNA

The Digital Living Network Alliance (DLNA) is a non-profit collaborative trade organization established by Sony in June 2003, which is responsible for defining interoperability guidelines to enable sharing of digital media between consumer devices such as computers, printers, cameras, cell phones and other multiple devices.

DLNA uses Universal Plug and Play (UPnP) for media management, discovery and control. UPnP defines the types of devices ('server', 'renderer', 'controller') that DLNA supports and the mechanism for accessing media over a network.

Overall, DLNA allows more convenience, more choices and enjoyment of your digital content through DLNA certified devices. Any DLNA certified devices or software can access the DLNA server.

With USB storage, 7800VDP(O)X can serve as a DLNA server.



Configuration

▾Digital Media Server settings

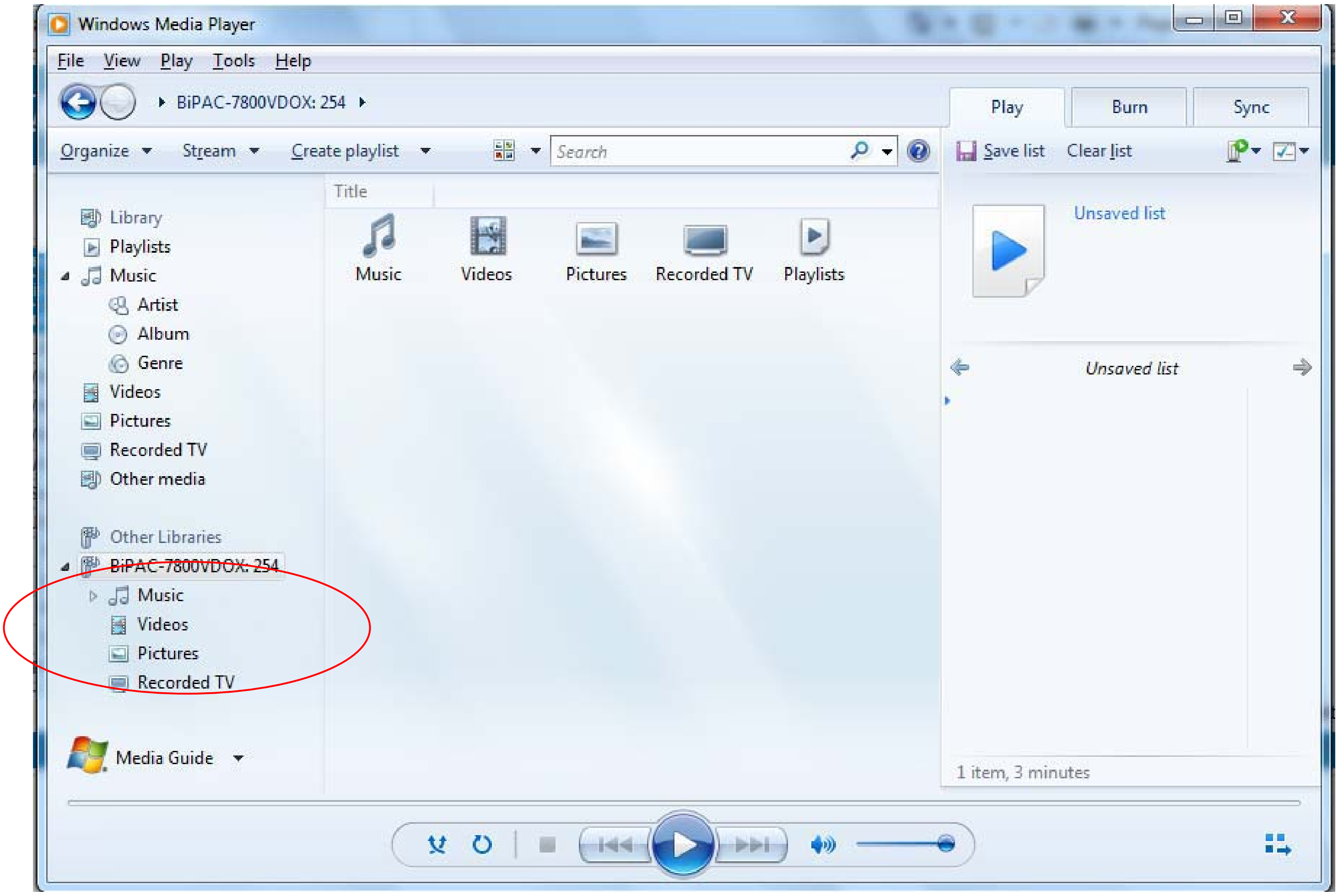
Parameters	
On-board digital media server	☑ Enable
Interface	Default
Media Library Path	usb1_1

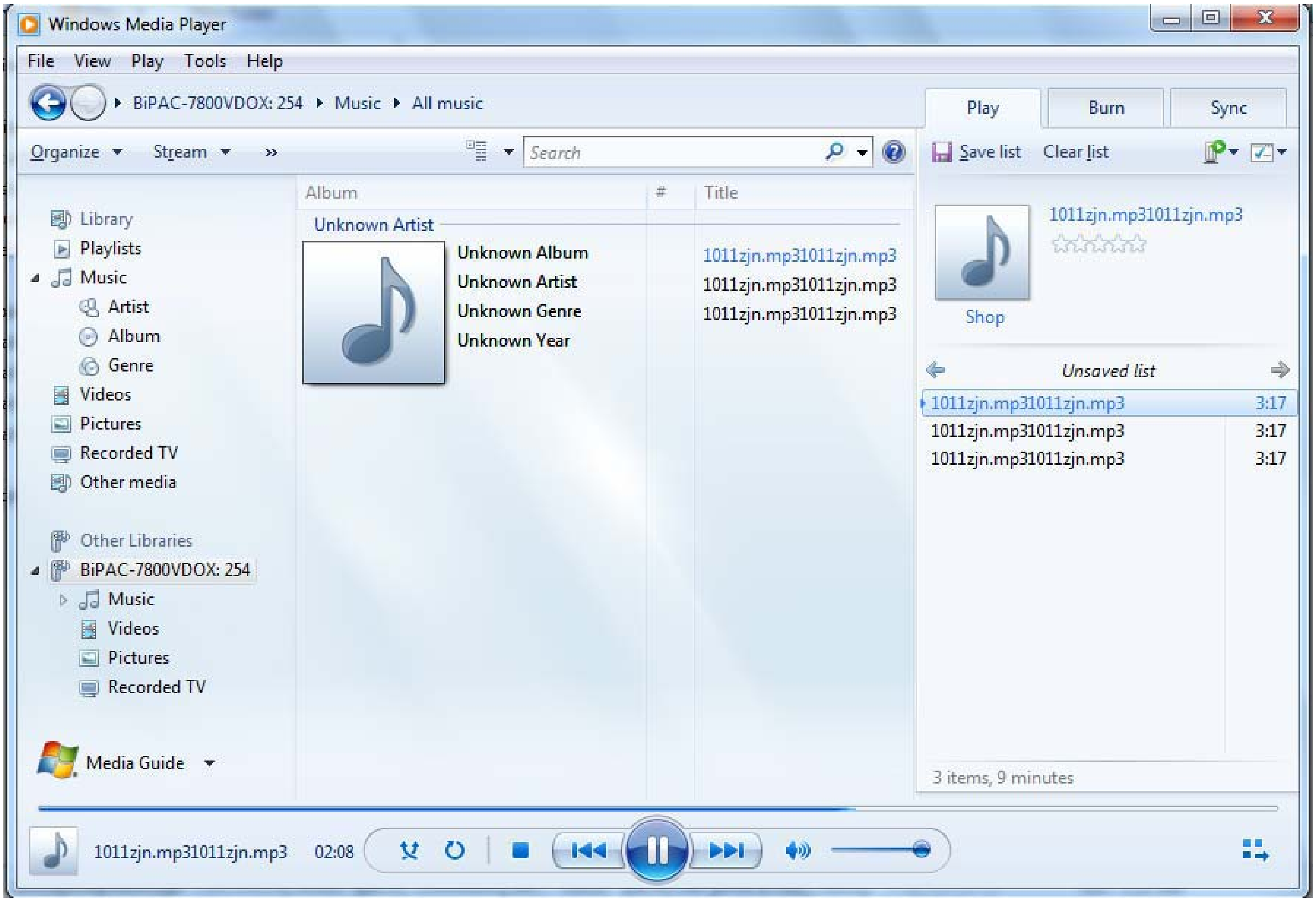
On-board digital media server: Enable to share the device as a DLNA server.

Interface: The VLAN group, it is the bound interface for DLNA server accessing.

Media Library Path: Default is usb1_1, total USB space (pictures, videos, music, etc, all can be accessed with this path).

Take Windows media player in Windows 7 accessing the DLNA server for example for usage of DLNA .





(7800VDOX)

IP Tunnel

An IP Tunnel is an Internet Protocol (IP) network communication channels between two networks of different protocols. It is used to transport another network protocol by encapsulation of its packets.

IP Tunnels are often used to connect two disjoint IP networks that do not have a native routing path to each other, via an underlying routable protocol across an intermediate transport network, like VPN.

Another prominent use of IP Tunnel is to connect islands of IPv6 installations across the IPv4 internet.

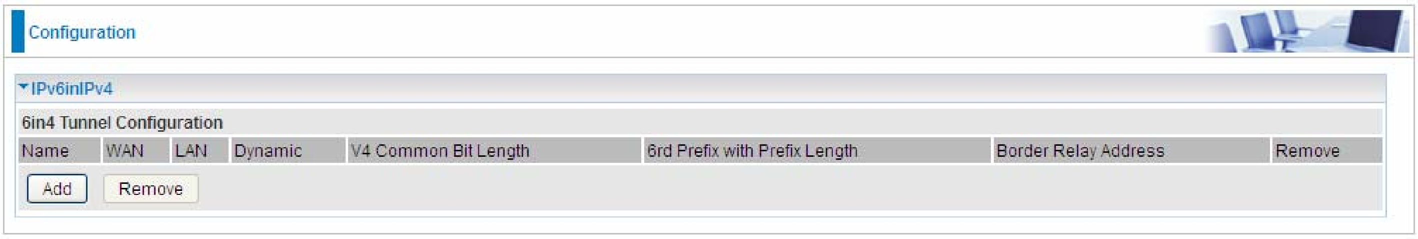
IPv6inIPv4

6in4 is an Internet transition mechanism for migrating from IPv4 to IPv6. 6in4 uses tunneling to encapsulate IPv6 traffic over explicitly configured IPv4 links. The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP Protocol number set to 41. This protocol number is specifically designated for IPv6 capsulation.

6RD:

6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of internet service providers (ISPs).

It is derived from 6to4, a preexisting mechanism to transporting IPv6 packets over IPv4 infrastructure network, with the significant change that it operates entirely within the enduser's ISP network, thus avoiding the major architectural problems inherent in the original design of 6to4.



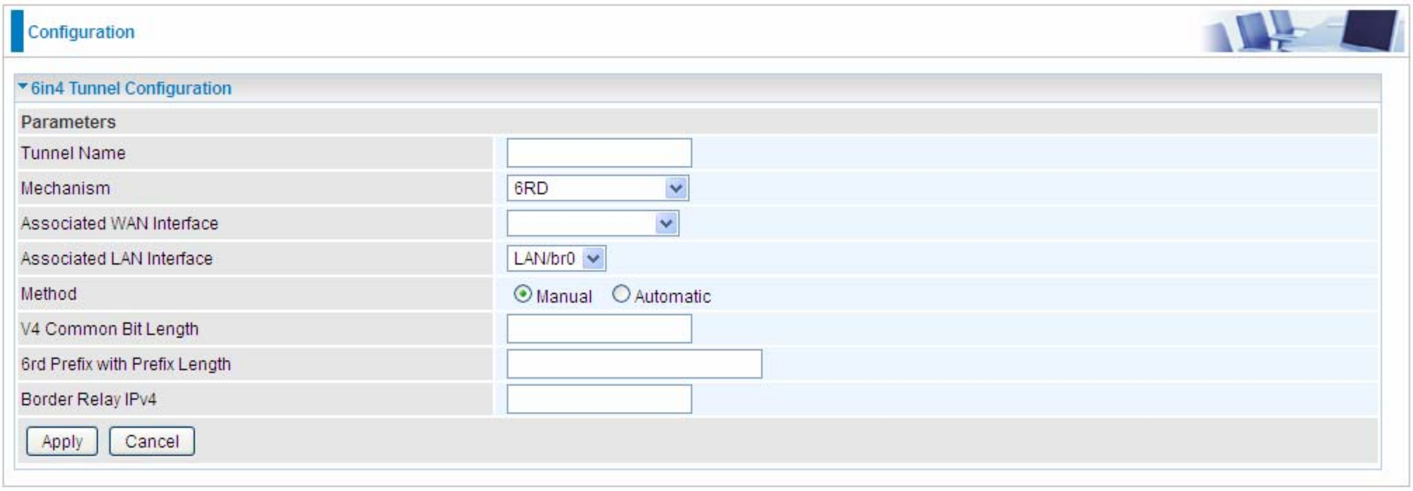
Configuration

▾IPv6inIPv4

6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	V4 Common Bit Length	6rd Prefix with Prefix Length	Border Relay Address	Remove

Click **Add** button to manually add the 6in4 rules.



Configuration

▾6in4 Tunnel Configuration

Parameters	
Tunnel Name	
Mechanism	6RD
Associated WAN Interface	
Associated LAN Interface	LAN/br0
Method	● Manual ○ Automatic
V4 Common Bit Length	
6rd Prefix with Prefix Length	
Border Relay IPv4	

Tunnel Name: User-defined name.

Mechanism: Here only 6RD.

Associated WAN Interface: The applied WAN interface with the set tunnel, thus when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Set the linked LAN interface with the tunnel.

Method: 6rd operation mechanism: manually configured or automatically configured. If manually, please fill out the following 6rd parameters.

V4 Common Bit Length: Specify the length of IPv4 address carried in IPv6 prefix, for example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

6rd Prefix with Prefix Length: Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP(The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

Border Relay IPv4 Address: The IPv4 address of the border relay. The relay is used to unwrap capsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

IPv4inIPv6

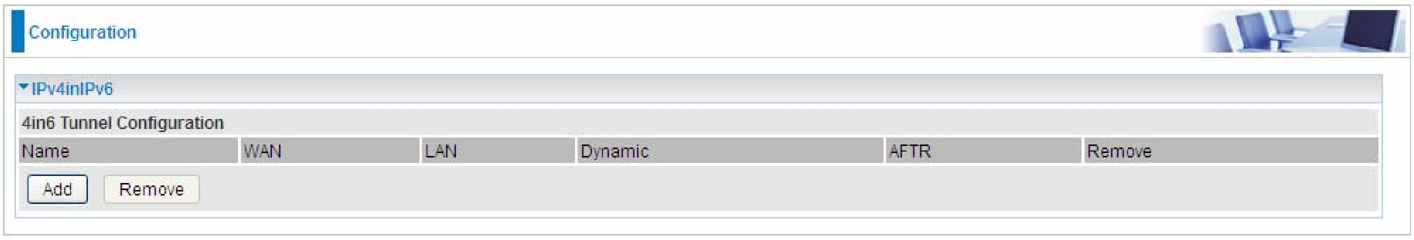
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. 4in6 tunnels are usually manually configured but they can be automated using protocols such as TSP to allow easy connection to a tunnel broker.

DS – Lite

DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.



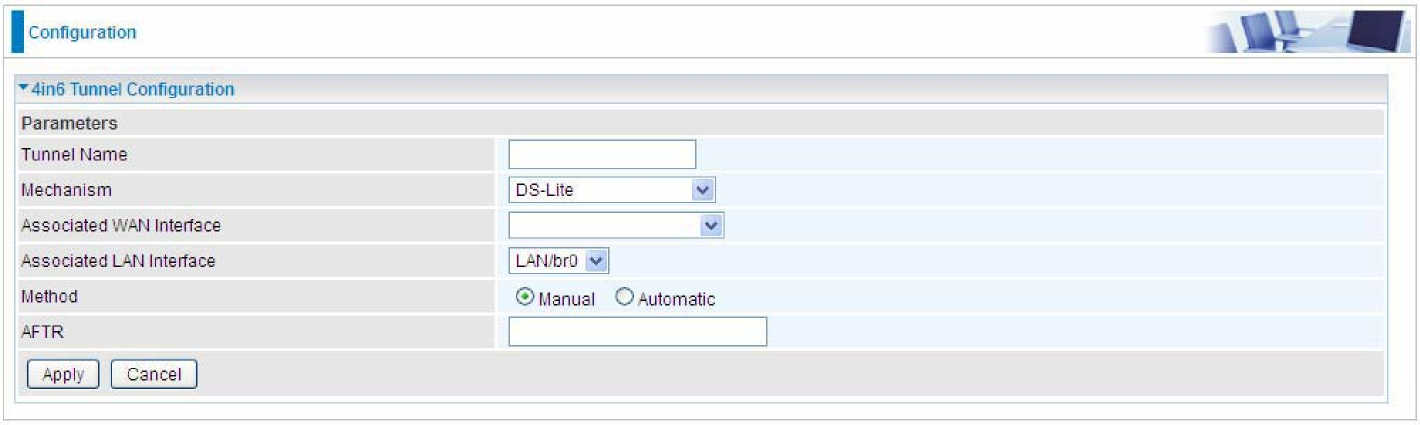
Configuration

▾IPv4inIPv6

4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove

Click **Add** button to manually add the 4in6 rules.



Configuration

▾4in6 Tunnel Configuration

Parameters	
Tunnel Name	
Mechanism	DS-Lite
Associated WAN Interface	
Associated LAN Interface	LAN/br0
Method	● Manual ○ Automatic
AFTR	

Tunnel Name: User-defined tunnel name.

Mechanism: It is the 4in6 tunnel operation technology. Please select DS-Lite.

Associated WAN Interface: The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

Associated LAN Interface: Specify the linked LAN interface with the tunnel.

Method: Manually to specify the AFTP (Address Family Transition Router) address or Automatic.

AFTR: Specify the address of AFTP (Address Family Transition Router) from your ISP.

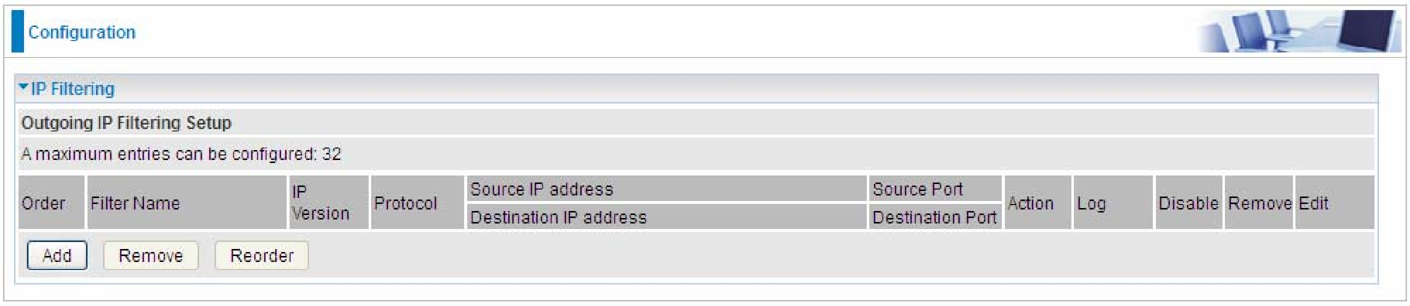
Security

IP Filtering Outgoing

IP filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is **“or”** operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

Outbound IP Filtering by default is set to **forward** all outgoing traffic from LAN to go through the router, but user can set rules to **block** the specific outgoing traffic.

Note: The maximum number of entries: 32.



Configuration

▾IP Filtering

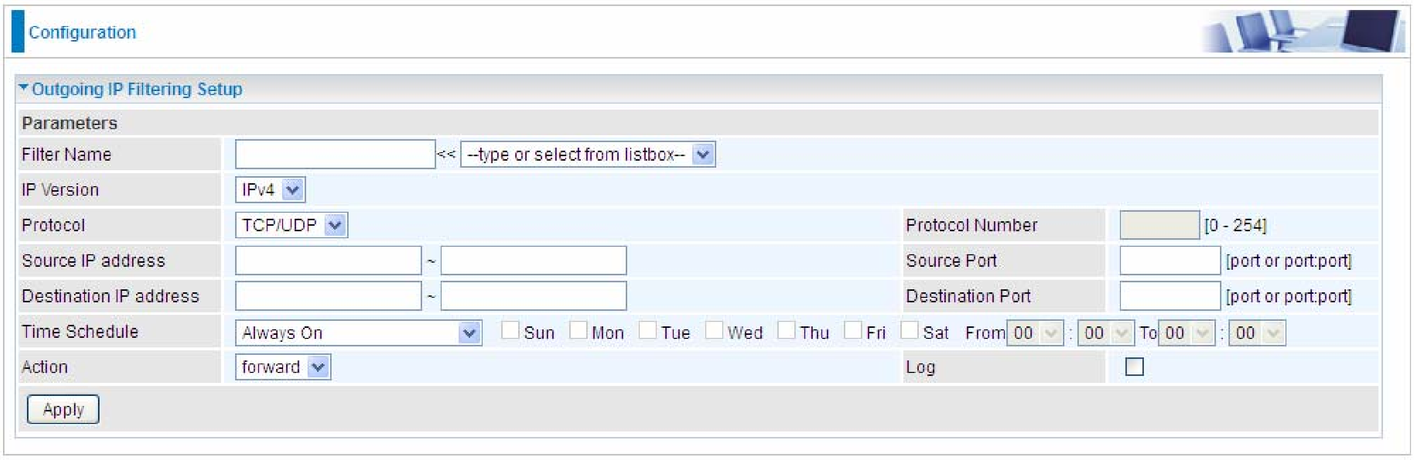
Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Action	Log	Disable	Remove	Edit

Add | Remove | Reorder

Click **Add** button to enter the exact rule setting page.



Configuration

▾Outgoing IP Filtering Setup

Parameters

Filter Name	<< --type or select from listbox--		
IP Version	IPv4		
Protocol	TCP/UDP	Protocol Number	[0 - 254]
Source IP address	~	Source Port	[port or port:port]
Destination IP address	~	Destination Port	[port or port:port]
Time Schedule	Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00		
Action	forward	Log	□

Apply

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP,RAW, Any) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

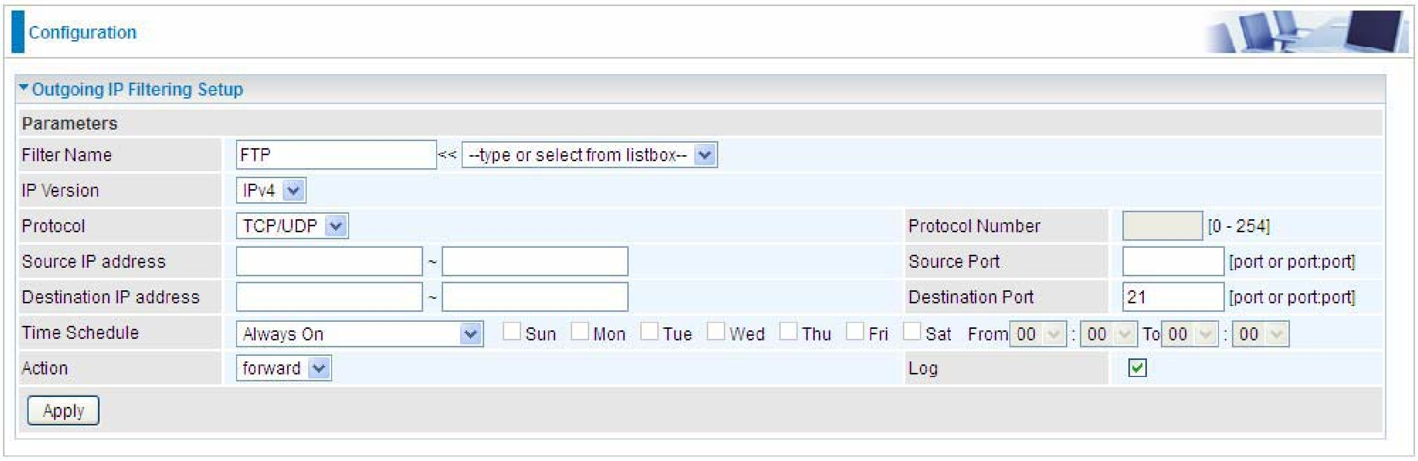
Destination Port [port or port: port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon” ✓ ” in list table indicating the rule is inactive. See Time Schedule.

Action: Select to **drop** or **forward** the packets fit the outgoing filtering rule.

Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

Example: For example, if there is an outgoing rule set as follows, then the 21 application between source IP and destination IP will be blocked. Or exactly in the rule below, all traffic trying to access FTP will be blocked.



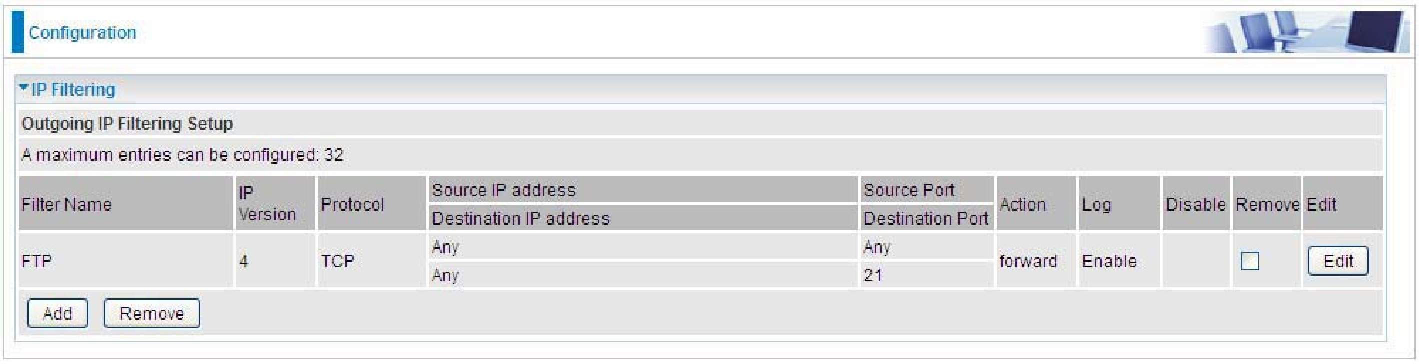
Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name	FTP << --type or select from listbox--		
IP Version	IPv4		
Protocol	TCP/UDP	Protocol Number	[0 - 254]
Source IP address	~	Source Port	[port or port:port]
Destination IP address	~	Destination Port	21 [port or port:port]
Time Schedule	Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00		
Action	forward	Log	☑

Apply



Configuration

IP Filtering

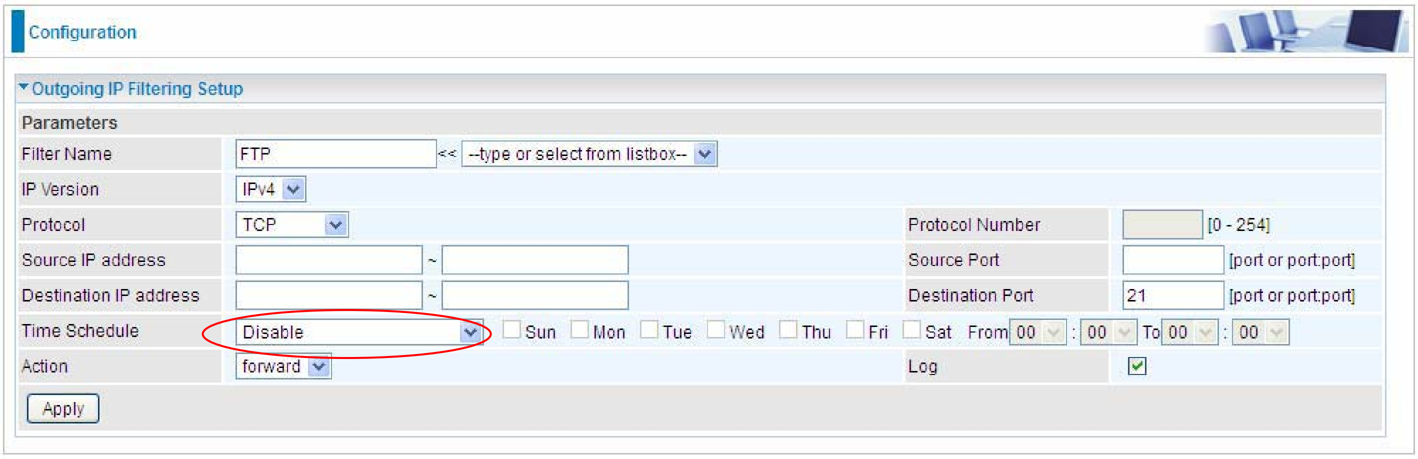
Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Filter Name	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Action	Log	Disable	Remove	Edit
FTP	4	TCP	Any Any	Any 21	forward	Enable		□	Edit

Add Remove

(The rule is active; disable field shows the status of the rule, active or inactive)

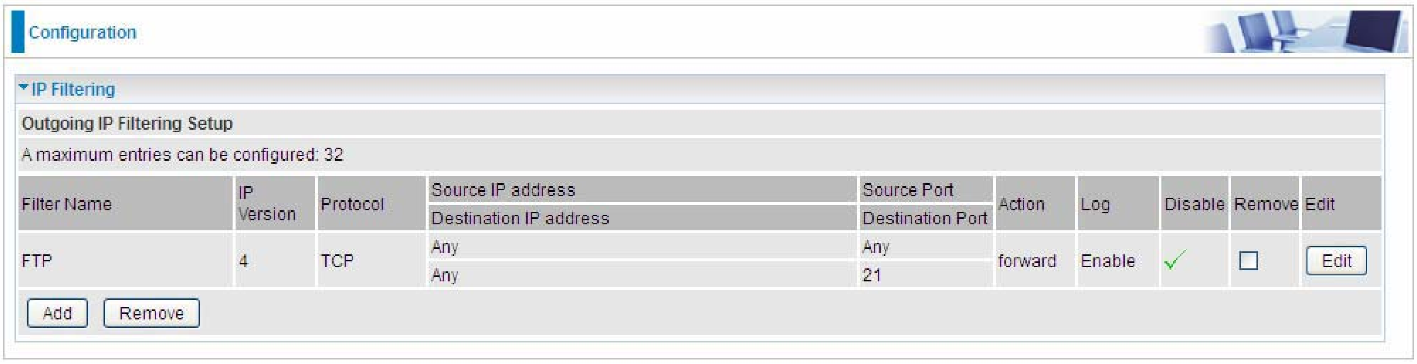


Configuration

▾ Outgoing IP Filtering Setup

Parameters

Filter Name	FTP << --type or select from listbox--		
IP Version	IPv4		
Protocol	TCP	Protocol Number	[0 - 254]
Source IP address	~	Source Port	[port or port:port]
Destination IP address	~	Destination Port	21 [port or port:port]
Time Schedule	Disable □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00		
Action	forward	Log	☑



Configuration

▾ IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

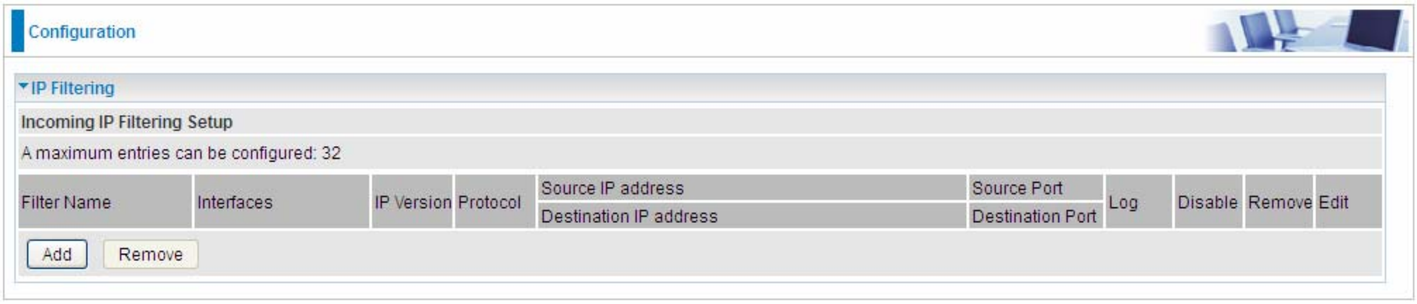
Filter Name	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Action	Log	Disable	Remove	Edit
FTP	4	TCP	Any Any	Any 21	forward	Enable	✓	□	Edit

(Rule inactive)

IP Filtering Incoming

Incoming IP Filtering is set by default to **block** all incoming traffic, but user can set rules to **forward** the specific incoming traffic.

Note:
1. The maximum number of entries: 32.
2. When LAN side firewall or firewall in WAN interface(s) is enabled, user can move here to add allowing rules to pass through the firewall.



Configuration

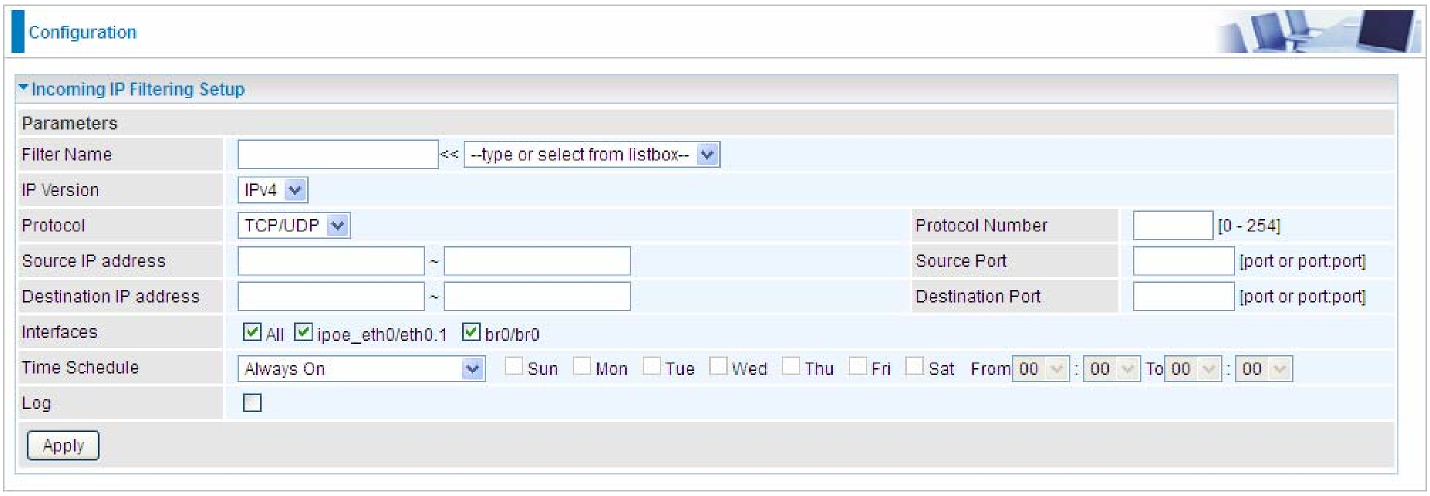
▾IP Filtering

Incoming IP Filtering Setup

A maximum entries can be configured: 32

Filter Name	Interfaces	IP Version	Protocol	Source IP address Destination IP address	Source Port Destination Port	Log	Disable	Remove	Edit

Click **Add** button to enter the exact rule setting page.



Configuration

▾Incoming IP Filtering Setup

Parameters

Filter Name	<< --type or select from listbox--		
IP Version	IPv4		
Protocol	TCP/UDP	Protocol Number	[0 - 254]
Source IP address	~	Source Port	[port or port:port]
Destination IP address	~	Destination Port	[port or port:port]
Interfaces	☑ All ☑ ipoe_eth0/eth0.1 ☑ br0/br0		
Time Schedule	Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00		
Log	□		

Filter Name: A user-defined rule name. User can select simply from the list box for the application for quick setup.

IP Version: Select the IP Version, IPv4 or IPv6.

Protocol: Set the traffic type (TCP/UDP, TCP, UDP, ICMP, RAW, Any) that the rule applies to.

Source IP address: This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range.. If you leave empty, it means any IP address.

Source Port [port or port:port]: The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

Destination IP address: Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

Destination Port [port or port : port]: Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535

Interfaces: Check if the filter rule applies to all interfaces. User can base on need select interfaces to make the rule take effect with those interfaces.

Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00-19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon” ✓ ” in the list table indicating the rule is inactive. See Time Schedule.

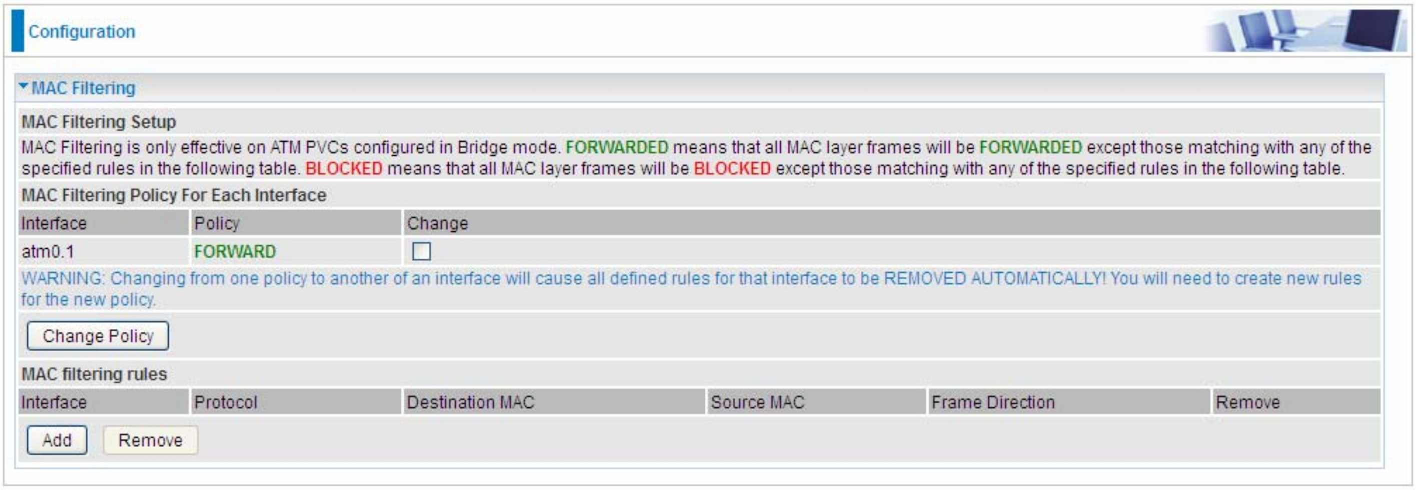
Log: check the check-box to record the security log. To check the log, users can turn to Security Log.

MAC Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

FORWARDED means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the following table.

BLOCKED means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the following table.



Configuration

▾MAC Filtering

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface

Interface	Policy	Change
atm0.1	FORWARD	□

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

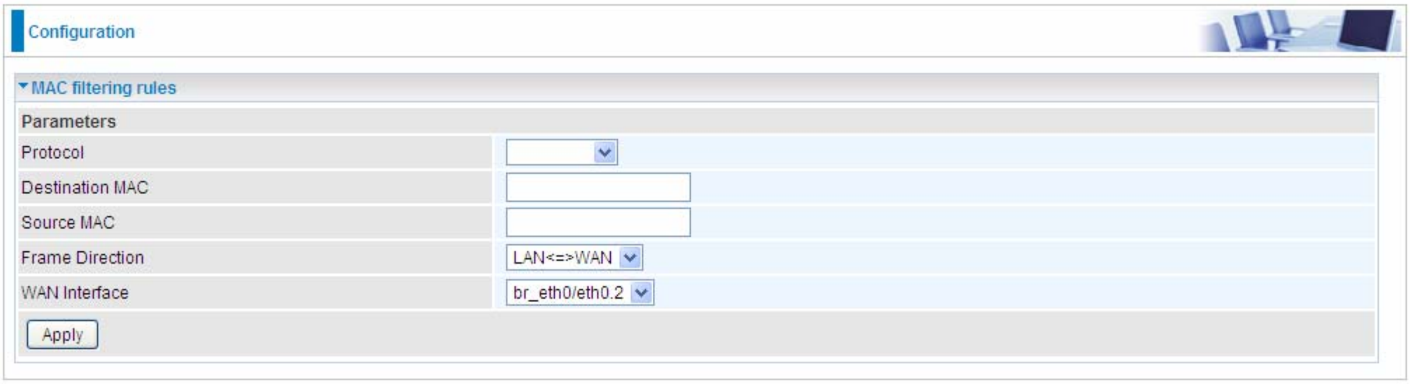
MAC filtering rules

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

By default, all MAC frames of the interface in Bridge Mode will be **forwarded**, you can check **Change** checkbox and then press **Change Policy** to change the settings to the interface.

For example, from above, the interface atm0.1 is of bridge mode, and all the MAC layer frames will be **forward**, but you can set some rules to let some item matched the rules to be **blocked**.

Click **Add** button to add the rules.



Configuration

▾MAC filtering rules

Parameters

Protocol	
Destination MAC	
Source MAC	
Frame Direction	LAN<=>WAN
WAN Interface	br_eth0/eth0.2

Protocol type: Select from the drop-down menu the protocol that applies to this rule.

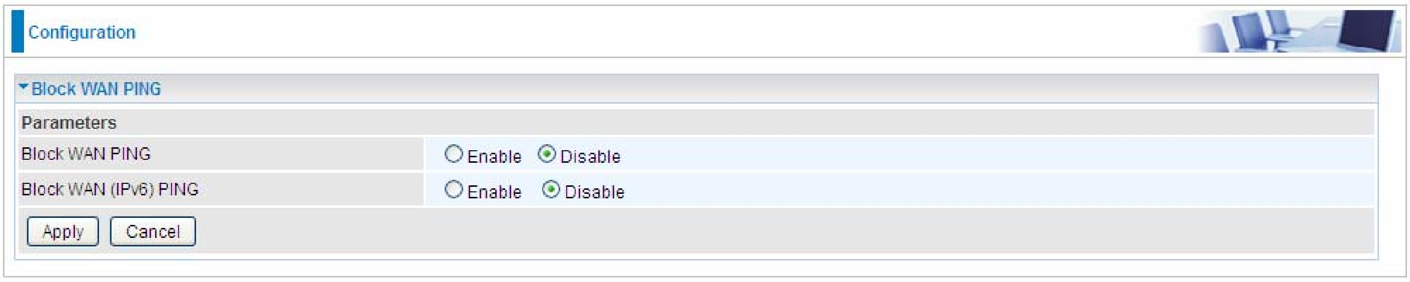
Destination /Source MAC Address: Enter the destination/source address.

Frame Direction: Select the frame direction this rule applies, both LAN and WAN: LAN <=>WAN, only LAN to WAN: LAN=>WAN, only WAN to LAN: WAN=>LAN.

WAN Interfaces: Select the interfaces configured in Bridge mode.

Blocking WAN PING

This feature is enabled to let your router not respond to any ping command when someone others “Ping” your WAN IP.



Block WAN PING

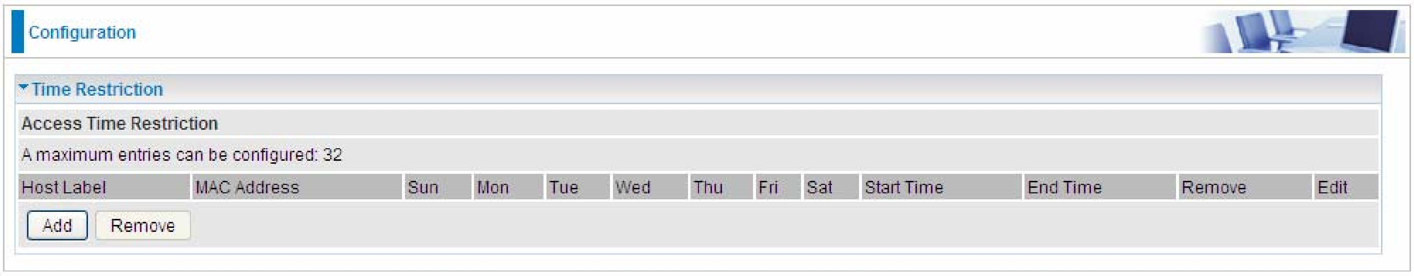
Parameters	
Block WAN PING	○ Enable ● Disable
Block WAN (IPv6) PING	○ Enable ● Disable

Time Restriction

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN during the specified time.

This page adds time of day restriction to a special LAN device connected to the router. To **Restrict** LAN device(s), please click Add button to add the device(s), from accessing internet under some set time. To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

Note: The maximum entries configured: 32.



Configuration

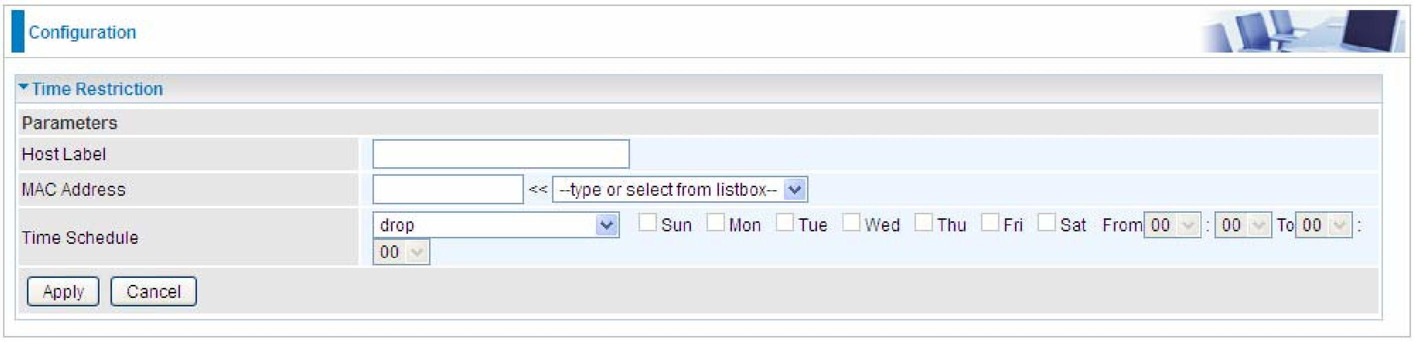
Time Restriction

Access Time Restriction

A maximum entries can be configured: 32

Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit

Click **Add** to add the rules.



Configuration

Time Restriction

Parameters

Host Label	
MAC Address	<< --type or select from listbox--
Time Schedule	drop □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00

Host Label: User-defined name.

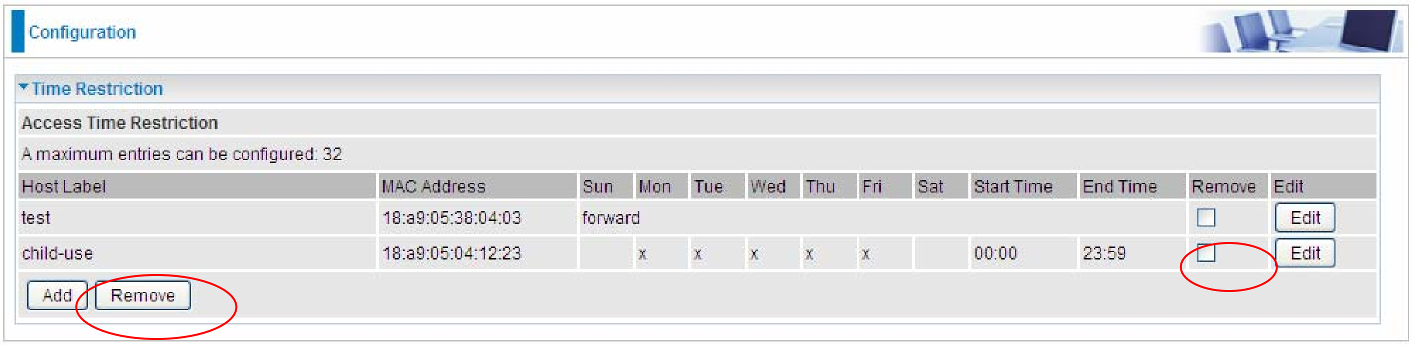
MAC Address: Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. For convenience, user can select from the list box.

Time Schedule: To determine when the rule works.

- **Drop:** To drop the MAC entries always; in other words, the MACs are blocked access to router and internet always.
- **Forward:** To forward the MAC entries always; in other words, the MACs are granted access to the router and internet always.
- **Check or select from listbox:** To set the time duration during which the MACs are blocked from access the router and internet. "**select from listbox**" means that you can select the already set timeslot in "**Time Schedule**" section during which the MACs are blocked from access the router and internet.

Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.

An example:


Configuration

▾Time Restriction

Access Time Restriction

A maximum entries can be configured: 32

Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit
test	18:a9:05:38:04:03	forward									□	Edit
child-use	18:a9:05:04:12:23		x	x	x	x	x		00:00	23:59	□	Edit

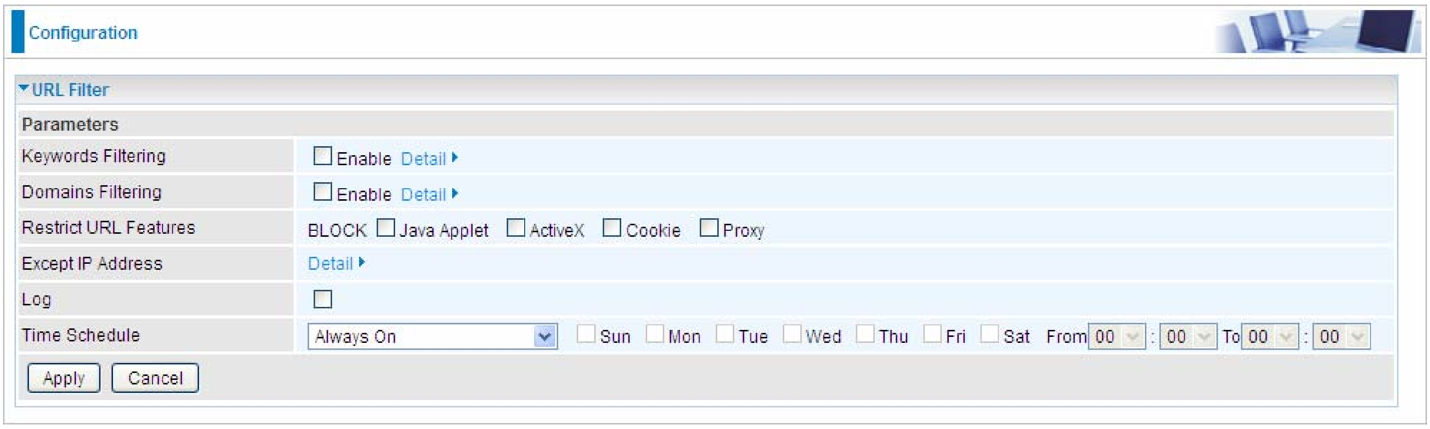
Here you can see that the user “child-use” with a MAC of 18:a9:05:04:12:23 is blocked to access the router from 00:00 to 23:59 Monday through Friday.
The “test” can access the internet always.

If you needn’t this rule, you can check the box, press Remove, it will be OK.

URL Filter

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

Note:
1) URL Filter rules apply to both IPv4 and IPv6 sources.
2) But in **Exception IP Address** part, user can click Detail ▸ to set the exception IP address(es) for IPv4 and IPv6 respectively.



Configuration

▾URL Filter

Parameters	
Keywords Filtering	□ Enable Detail ▸
Domains Filtering	□ Enable Detail ▸
Restrict URL Features	BLOCK □ Java Applet □ ActiveX □ Cookie □ Proxy
Except IP Address	Detail ▸
Log	□
Time Schedule	Always On ▾ □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 ▾ : 00 ▾ To 00 ▾ : 00 ▾

Apply Cancel

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.

Domains Filtering: This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

Restrict URL Features: Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

Exception IP Address: You can input a list of IP addresses as the exception list for URL filtering. These IPs will not be covered by the URL rules.

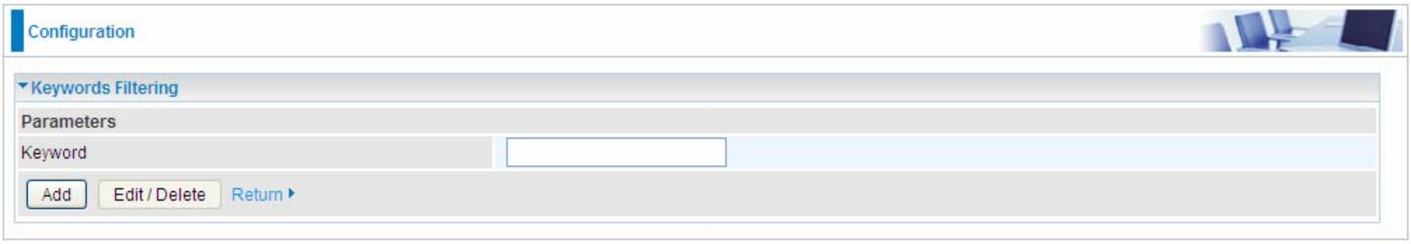
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled. See Time Schedule.

Log: Select Enable for this option if you will like to capture the logs for this URL filter policy. To check the log, users can turn to Security Log.

Keywords Filtering

Note: Maximum number of entries: 32.

Click Detail ▸ to add the keywords.



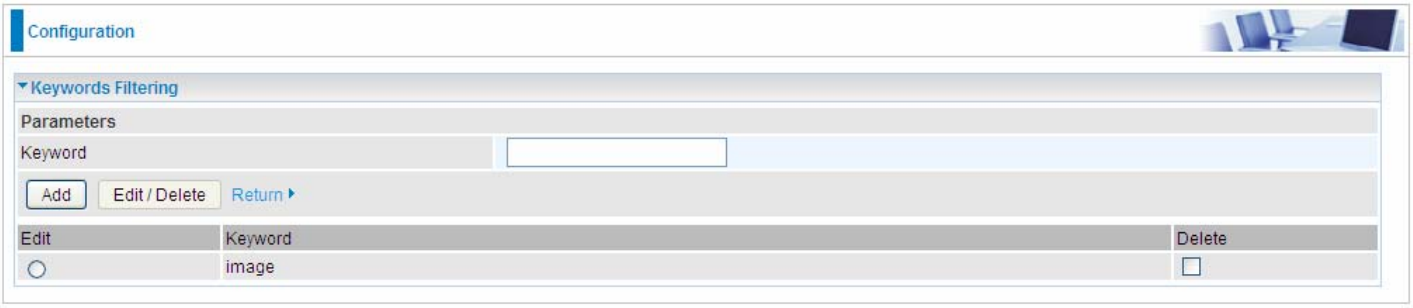
Configuration

▾ Keywords Filtering

Parameters

Keyword

Enter the Keyword, for example image, and then click **Add.**



Configuration

▾ Keywords Filtering

Parameters

Keyword

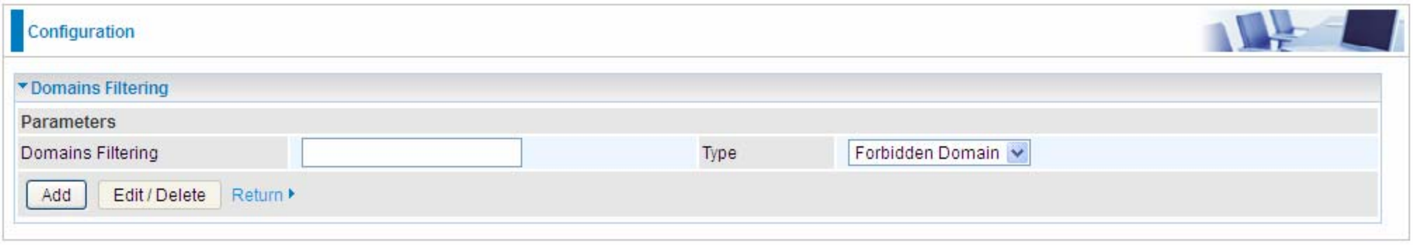
Edit	Keyword	Delete
○	image	□

You can add other keywords like this. The keywords you add will be listed as above. If you want to reedit the keyword, press the Edit radio button left beside the item, and the word will listed in the Keyword field, edit, and then press **Edit/Delete** to confirm. If you want to delete certain keyword, check Delete checkbox right beside the item, and press **Edit/Delete**. Click **Return** to be back to the previous page.

Domain Filtering

Note: Maximum number of entries: 32.

Click Detail ▸ to add Domains.



Configuration

▾ Domains Filtering

Parameters

Domains Filtering

Type: Forbidden Domain

Domain Filtering: enter the domain you want this filter to apply.

Type: select the action this filter deals with the Domain.

- **Forbidden Domain:** The domain is forbidden access.
- **Trusted Domain:** The domain is trusted and allowed access.

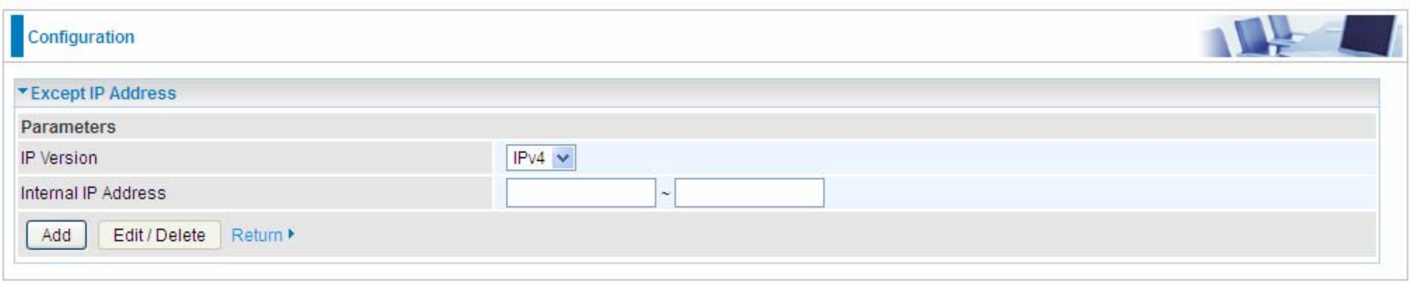
Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Add**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously. For specific process, please refer to ***Keywords***

Filtering.

Exception IP Address

In the section, users can set the exception IP respectively for IPv4 and IPv6.

Click Detail ▸ to add the IP Addresses.



Configuration

Except IP Address

Parameters	
IP Version	IPv4
Internal IP Address	~

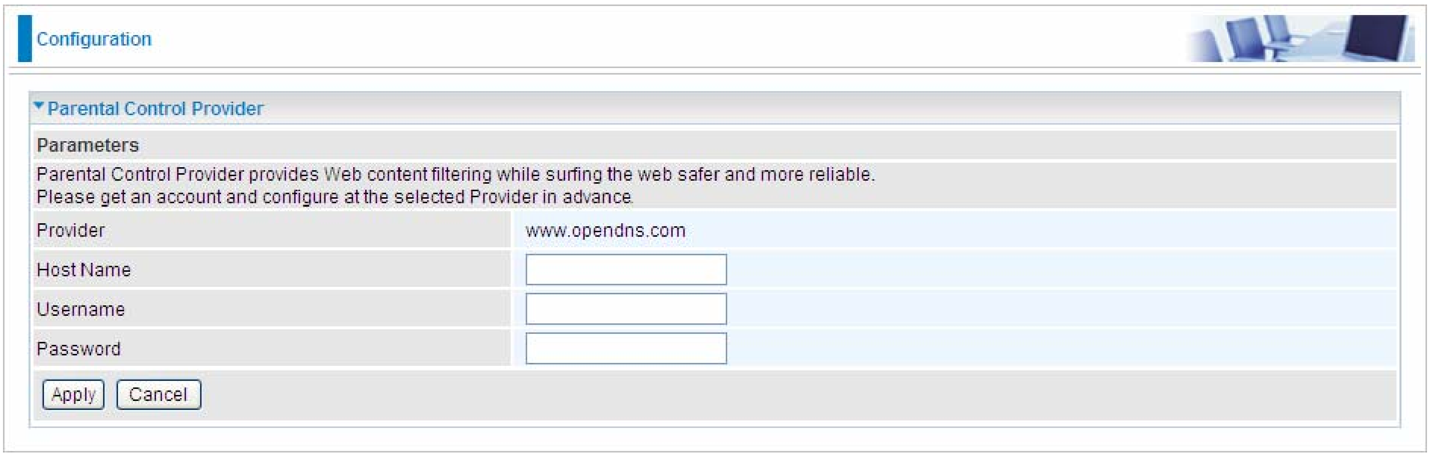
Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the ***Exception List***, and excluded from the URL filtering rules in effect. For specific process, please refer to ***Keywords Filtering*.**

For example, users can set IPv4 client 192.168.1.103 in your network as a exception address that is not limited to the rules set in URL filter (or IPv4 clients (a range)). And also an IPv6 client (2000:1211:1002:6ba4:d160:5adb:9009:87ae) or IPv6 clients(a range) can be the exceptions from the URL rules.

At the URL Filter page, press **Apply** to confirm your settings.

Parental Control Provider

Parental Control Provider provides Web content filtering offering safer and more reliable web surfing for users. Please get an account and configure at the selected Provider “www.opendns.com” in advance. To use parental control (DNS), user needs to configure to use parental control (DNS provided by parental control provider) to access internet at WAN configuration or DNS page(See DNS).



Parental Control Provider provides Web content filtering while surfing the web safer and more reliable.
Please get an account and configure at the selected Provider in advance.

Provider	www.opendns.com
Host Name	
Username	
Password	

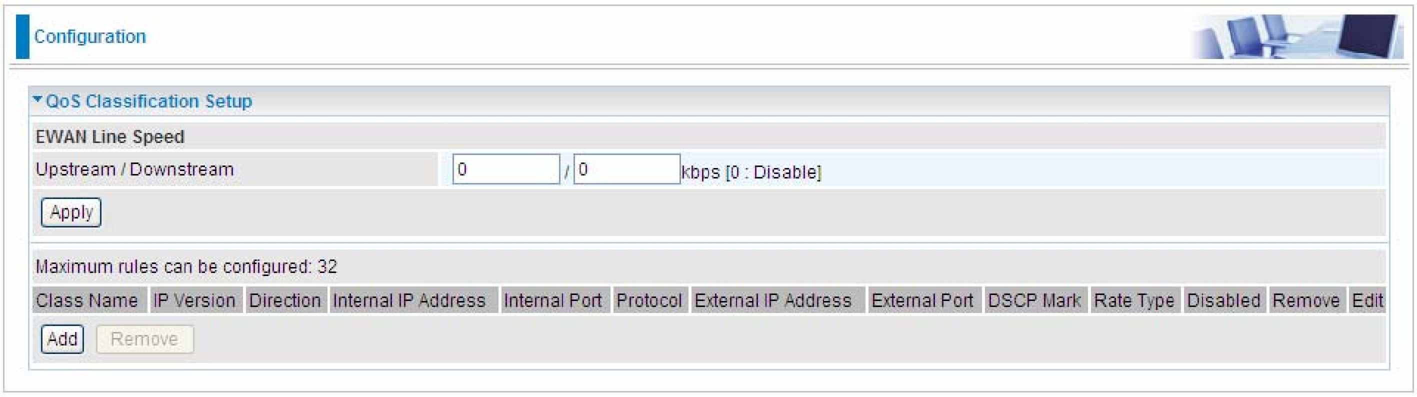
Host Name, Username and Password: Enter your registered domain name and your username and password at the provider website www.opendns.com.

QoS - Quality of Service

Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). This feature allows you to control the quality and speed of throughput for each application when the system is running with full upstream load.

Note: ADSL line speed is based on the ADSL sync rate. But there is no QoS on 3G/LTE as the 3G/LTE line speed is various and can not be known exactly.



Configuration

QoS Classification Setup

EWAN Line Speed

Upstream / Downstream	0 / 0 kbps [0 : Disable]

Apply

Maximum rules can be configured: 32

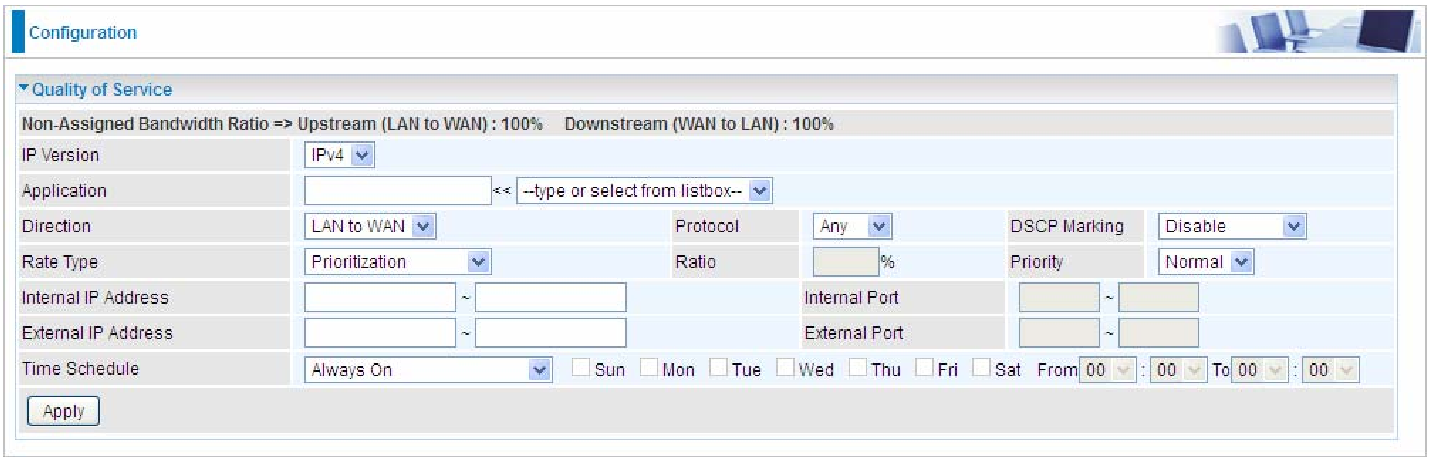
Class Name	IP Version	Direction	Internal IP Address	Internal Port	Protocol	External IP Address	External Port	DSCP Mark	Rate Type	Disabled	Remove	Edit

Add Remove

EWAN Line Speed

Upstream / Downstream: Specify the upstream and downstream rate of the EWAN interface. Click **Apply** to save the EWAN rate settings.

Click **Add** to enter QoS rules.



Configuration

Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

IP Version	IPv4				
Application	<< --type or select from listbox--				
Direction	LAN to WAN	Protocol	Any	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	%	Priority	Normal
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	~		
Time Schedule	Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00				

Apply

IP Version: Select either IPv4 or IPv6 base on need.

Application: Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

Direction: Shows the direction mode of the QoS application.

- **LAN to WAN:** You want to control the traffic from local network to the outside (Upstream). You can assign the priority for the application or you can limit the rate of the application.
  Eg: you have a FTP server inside the local network, and you want to have a limited control by the QoS policy and so you need to add a policy with LAN to WAN direction setting.
- **WAN to LAN:** Control traffic from WAN to LAN (Downstream).

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

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.

IP Precedence and DSCP Mapping Table

Mapping Table	
Default (000000)	Best Effort
EF(101110)	Expedited Forwarding
AF11 (001010)	Assured Forwarding Class1(L)
AF12 (001100)	Assured Forwarding Class1(M)
AF13 (001110)	Assured Forwarding Class1(H)
AF21 (010010)	Assured Forwarding Class1(L)
AF22 (010100)	Assured Forwarding Class1(M)
AF23 (010110)	Assured Forwarding Class1(H)
AF31 (011010)	Assured Forwarding Class1(L)
AF32 (011100)	Assured Forwarding Class1(M)
AF33 (011110)	Assured Forwarding Class1(H)
AF41 (100010)	Assured Forwarding Class1(L)
AF42 (100100)	Assured Forwarding Class1(M)
AF43 (100110)	Assured Forwarding Class1(H)
CS1(001000)	Class Selector(IP precedence)1
CS2(010000)	Class Selector(IP precedence) 2
CS3(011000)	Class Selector(IP precedence)3
CS4(100000)	Class Selector(IP precedence) 4
CS5(101000)	Class Selector(IP precedence) 5
CS6(110000)	Class Selector(IP precedence) 6
CS7(111000)	Class Selector(IP precedence) 7

DSCP offers three levels of service, Class Selector (CS), Assured Forwarding (AF) and Expedited Forwarding (EF). AF1, AF2, AF3 and AF4 are four levels of assured forwarding services. Each AF has three different packet loss priorities from high, medium, to low. Also, CS1-CS7 indicates the IP precedence.

Rate Type: You can choose ***Limited*** , ***Prioritization*** *or* ***Set DSCP Marking***.

- ⓘ **Limited (Maximum):** Specify a limited data rate for this policy. It also is the maximum rate for this policy. When you choose ***Limited***, type the ***Ratio*** proportion. As above FTP server example, you may want to “throttle” the outgoing FTP speed to 20% of 256K and limit to it, you may use this type.
- ⓘ **Prioritization:** Specify the rate type control for the rule to be used. If you choose ***Prioritization*** for the rule, you parameter ***Priority*** would be available, you can set the priority for this rule.
- ⓘ **Set DSCP Marking:** When select ***Set DSCP Marking***, the packets matching the rule will be forwarded according to the pre-set DSCP marking.

Ratio: The rate percent of each application/policy compared to total traffic on the interface with limited rate type. For example, we want to only allow 20% of the total data for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is 20%*256*0.9 = 46kbps. (For 0.9 is an estimated factor for the effective data transfer rate for an ADSL LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8)

Priority: Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to Normal. You may adjust this setting to fit your policy / application.

Internal IP Address: The IP address values for Local LAN devices you want to give control.

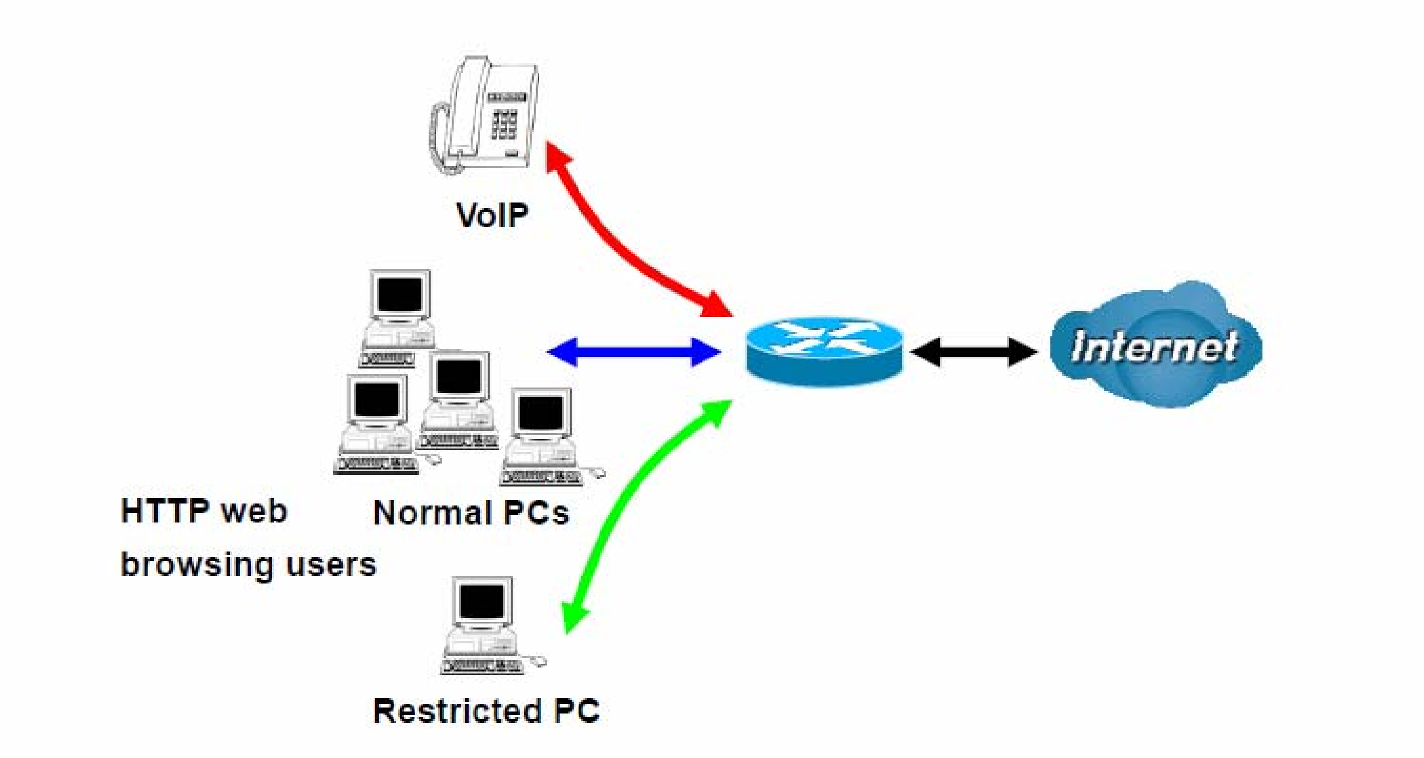
Internal Port: The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

External Port: The Port number on the remote / WAN side.

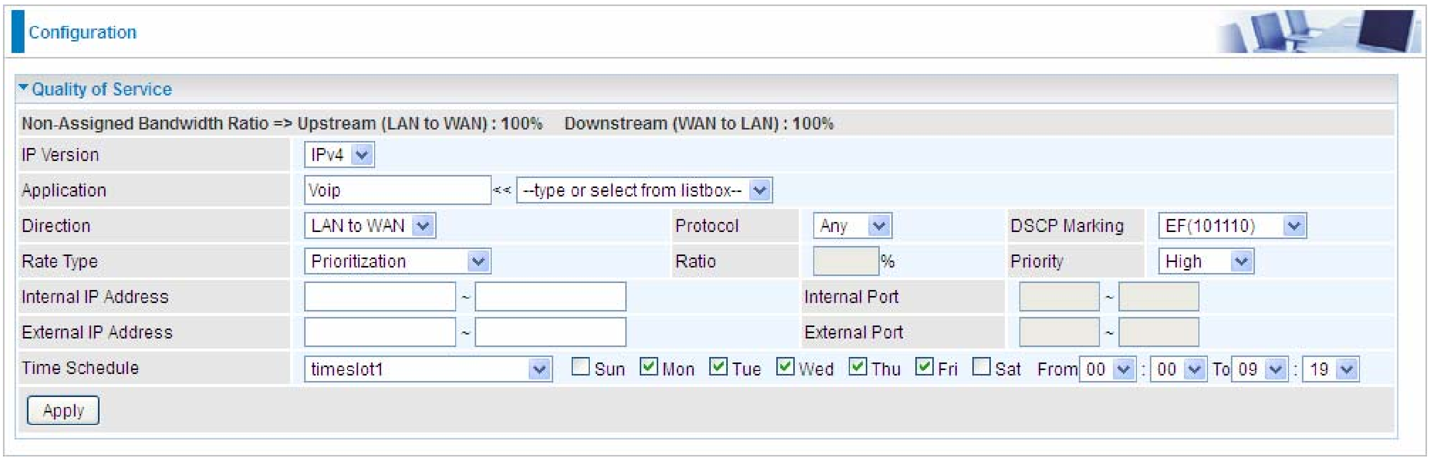
Time Schedule: Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00- 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon” ✓ ” indicating the rule is inactive. See Time Schedule.

Examples: Common usage



1. Give outgoing VoIP traffic more priority.

The default queue priority is normal, so if you have VoIP users in your local network, you can set a higher priority to the outgoing VoIP traffic.



Configuration

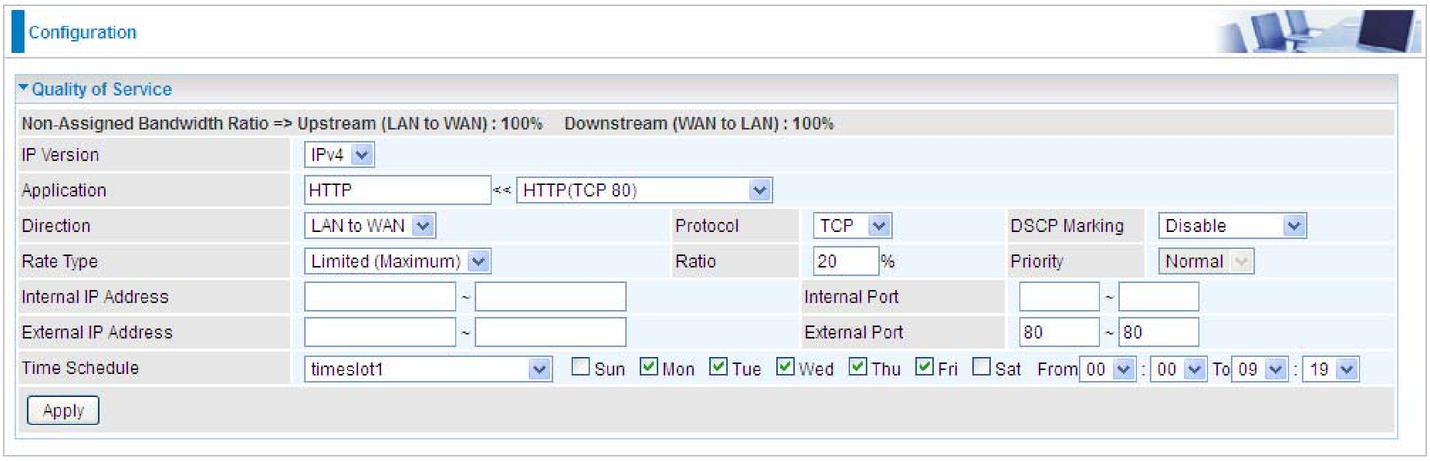
▾ Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100%   Downstream (WAN to LAN) : 100%

IP Version	IPv4				
Application	Voip << --type or select from listbox--				
Direction	LAN to WAN	Protocol	Any	DSCP Marking	EF(101110)
Rate Type	Prioritization	Ratio	%	Priority	High
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	~		
Time Schedule	timeslot1 ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat From 00 : 00 To 09 : 19				

Apply

2. Give regular web http access a limited rate



Configuration

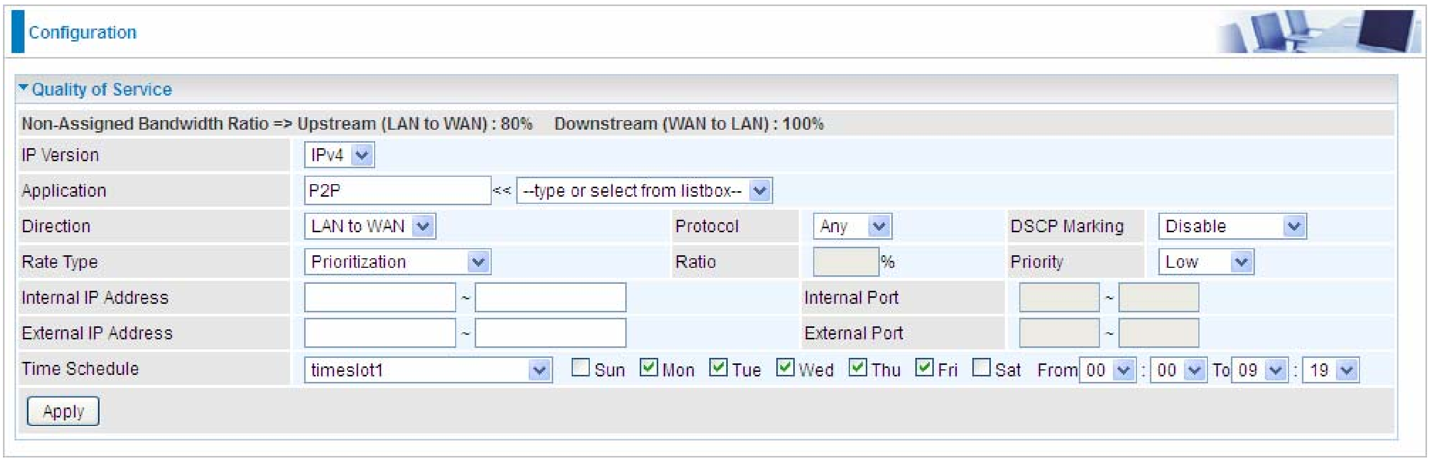
▾ Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100%   Downstream (WAN to LAN) : 100%

IP Version	IPv4				
Application	HTTP << HTTP(TCP 80)				
Direction	LAN to WAN	Protocol	TCP	DSCP Marking	Disable
Rate Type	Limited (Maximum)	Ratio	20 %	Priority	Normal
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	80 ~ 80		
Time Schedule	timeslot1 ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat From 00 : 00 To 09 : 19				

Apply

3. If you are actively engaged in P2P and are afraid of slowing down internet access for other users within your network, you can then use QoS to set a rule that has low priority. In this way, P2P application will not congest the data transmission with other applications.



Configuration

▾ Quality of Service

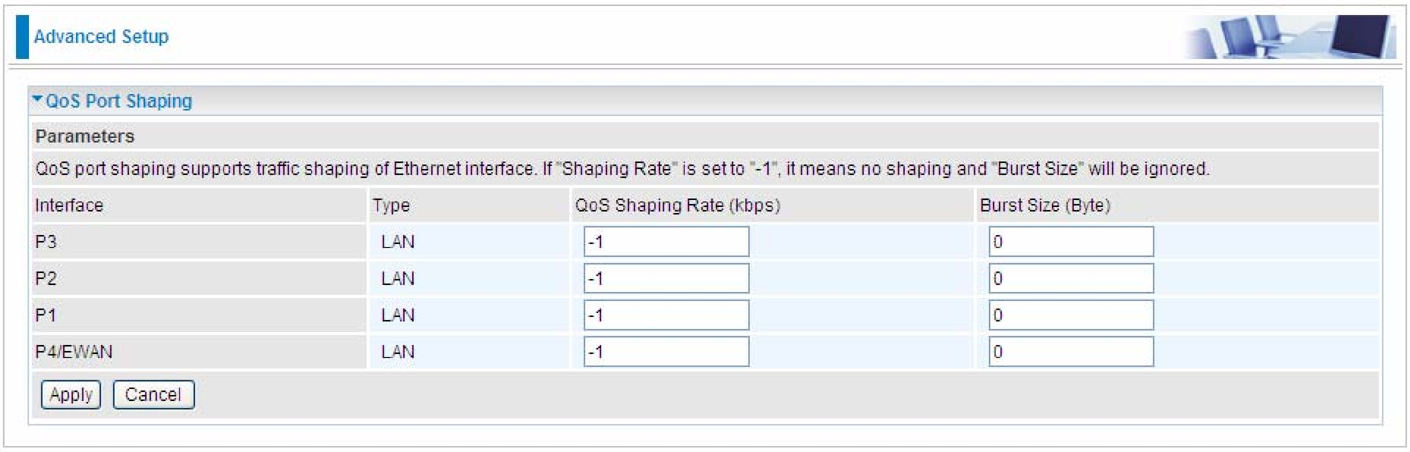
Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 80%   Downstream (WAN to LAN) : 100%

IP Version	IPv4				
Application	P2P << --type or select from listbox--				
Direction	LAN to WAN	Protocol	Any	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	%	Priority	Low
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	~		
Time Schedule	timeslot1	□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat	From 00 : 00 To 09 : 19		

Other applications, like FTP, Mail access, users can use QoS to control based on need.

QoS Port Shaping

QoS port shaping supports traffic shaping of Ethernet interfaces. It forcefully maximizes the throughput of the Ethernet interface. When “Shaping Rate” is set to “-1”, no shaping will be in place and the “Burst Size” is to be ignored.



Parameters

QoS port shaping supports traffic shaping of Ethernet interface. If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	QoS Shaping Rate (kbps)	Burst Size (Byte)
P3	LAN	-1	0
P2	LAN	-1	0
P1	LAN	-1	0
P4/EWAN	LAN	-1	0

Interface: P1-P4. P4 used as EWAN also covered.

Type: All LAN when P4 is LAN port; P4 used as EWAN, type WAN and all others LAN.

QoS Shaping Rate (Kbps): Set the forcefully maximum rate.

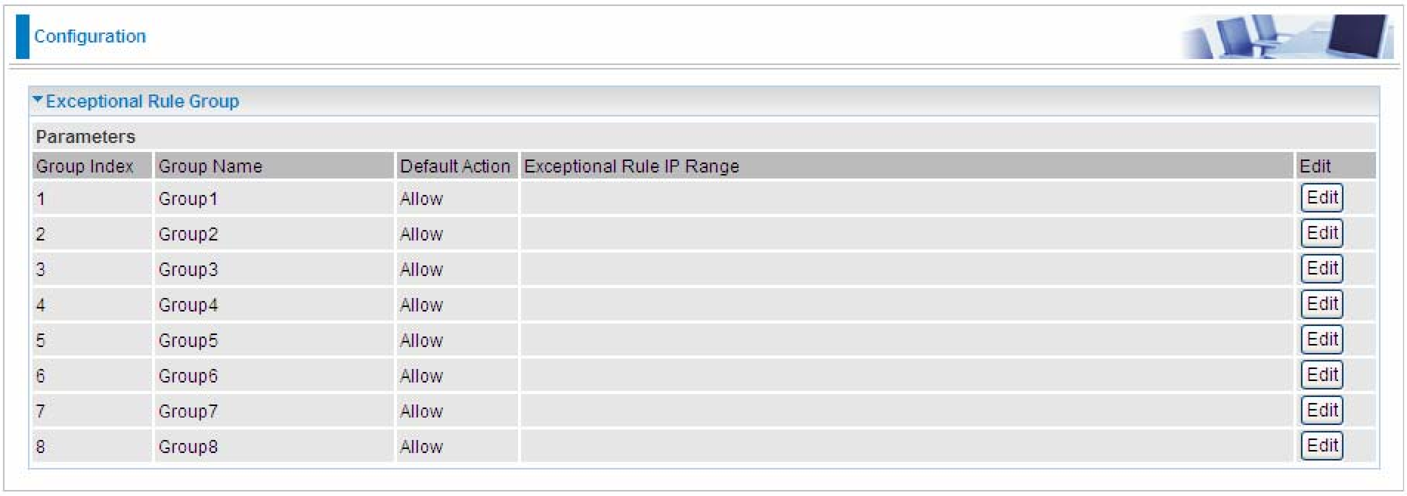
Burst Size(Bytes): Set the forcefully Burst Size.

NAT

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

Exceptional Rule Group

Exceptional Rule is dedicated to giving or blocking Virtual Server/ DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



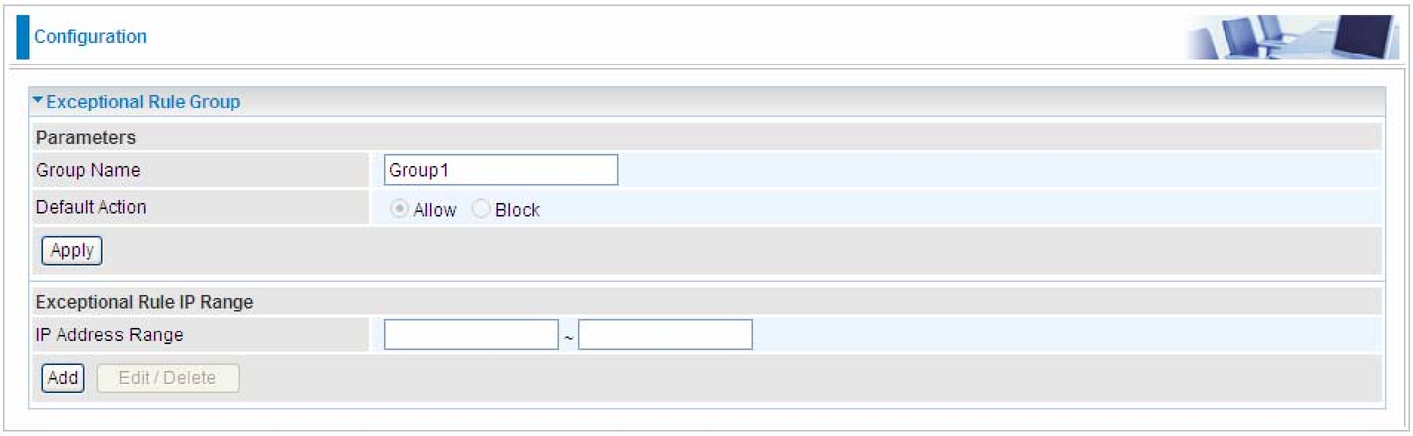
Configuration

▾Exceptional Rule Group

Parameters

Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

Press **Edit** to set the exceptional IP (IP Range).



Configuration

▾Exceptional Rule Group

Parameters

Group Name	Group1
Default Action	● Allow ○ Block

Exceptional Rule IP Range

IP Address Range	~

Default Action: Please first set the range to make **"Default Action"** setting available**.** Set "Allow" to ban the listed IP or IPs to access the Virtual Server and DMZ Host

Check "Block" to grant access to the listed IP or IPs to Virtual Server and DMZ Host.

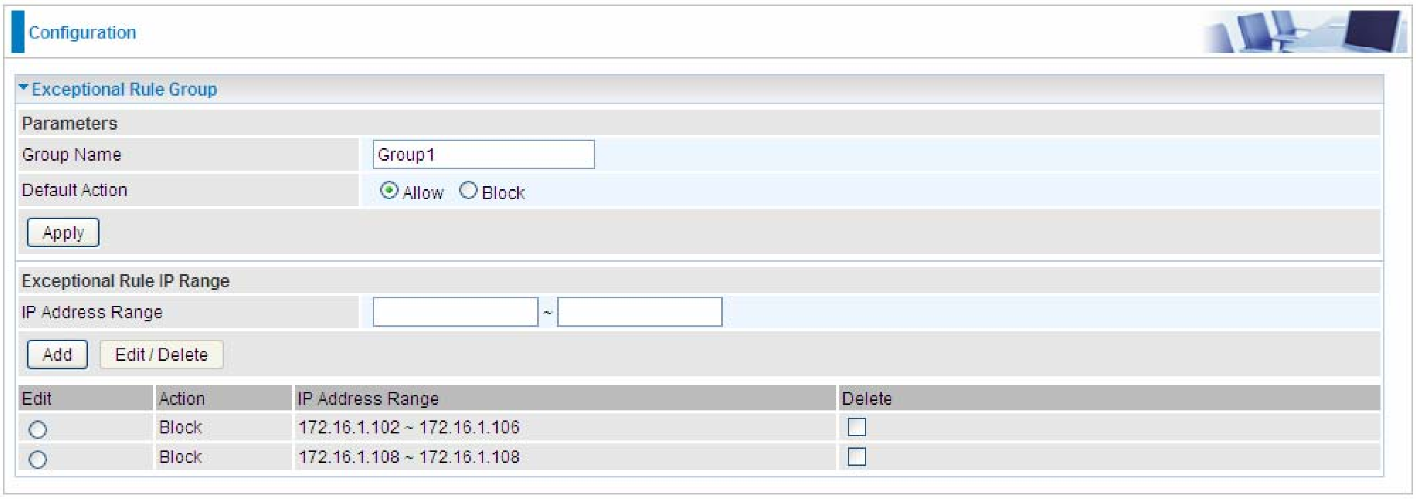
Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

IP Address Range: Specify the IP address range; IPv4 address range can be supported.

Click **Add** to add the IP Range.

For instance, if user wants to block IP range of 172.16.1.102-172.16.1.106 from accessing your set virtual server and DMZ host, you can add this IP range and valid it.



Configuration

▾ Exceptional Rule Group

Parameters	
Group Name	Group1
Default Action	● Allow ○ Block

Exceptional Rule IP Range	
IP Address Range	~

Edit	Action	IP Address Range	Delete
○	Block	172.16.1.102 ~ 172.16.1.106	□
○	Block	172.16.1.108 ~ 172.16.1.108	□

Virtual Servers

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

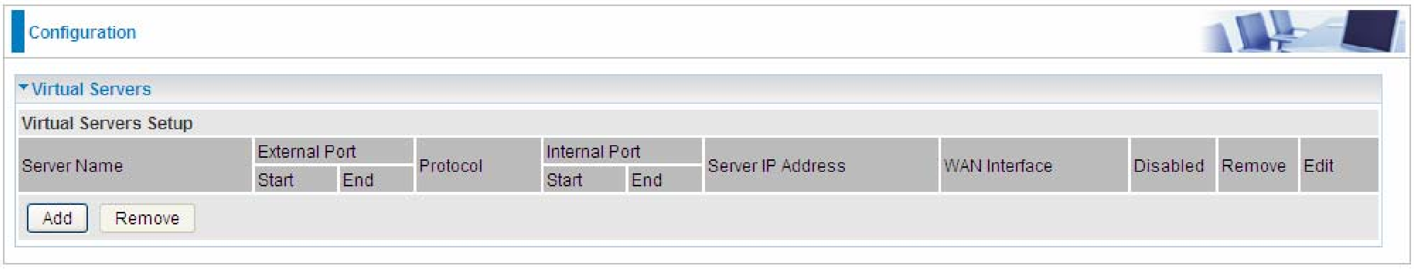
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing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

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

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

This part is only available when NAT is enabled.

Note: The maximum number of entries: 64.

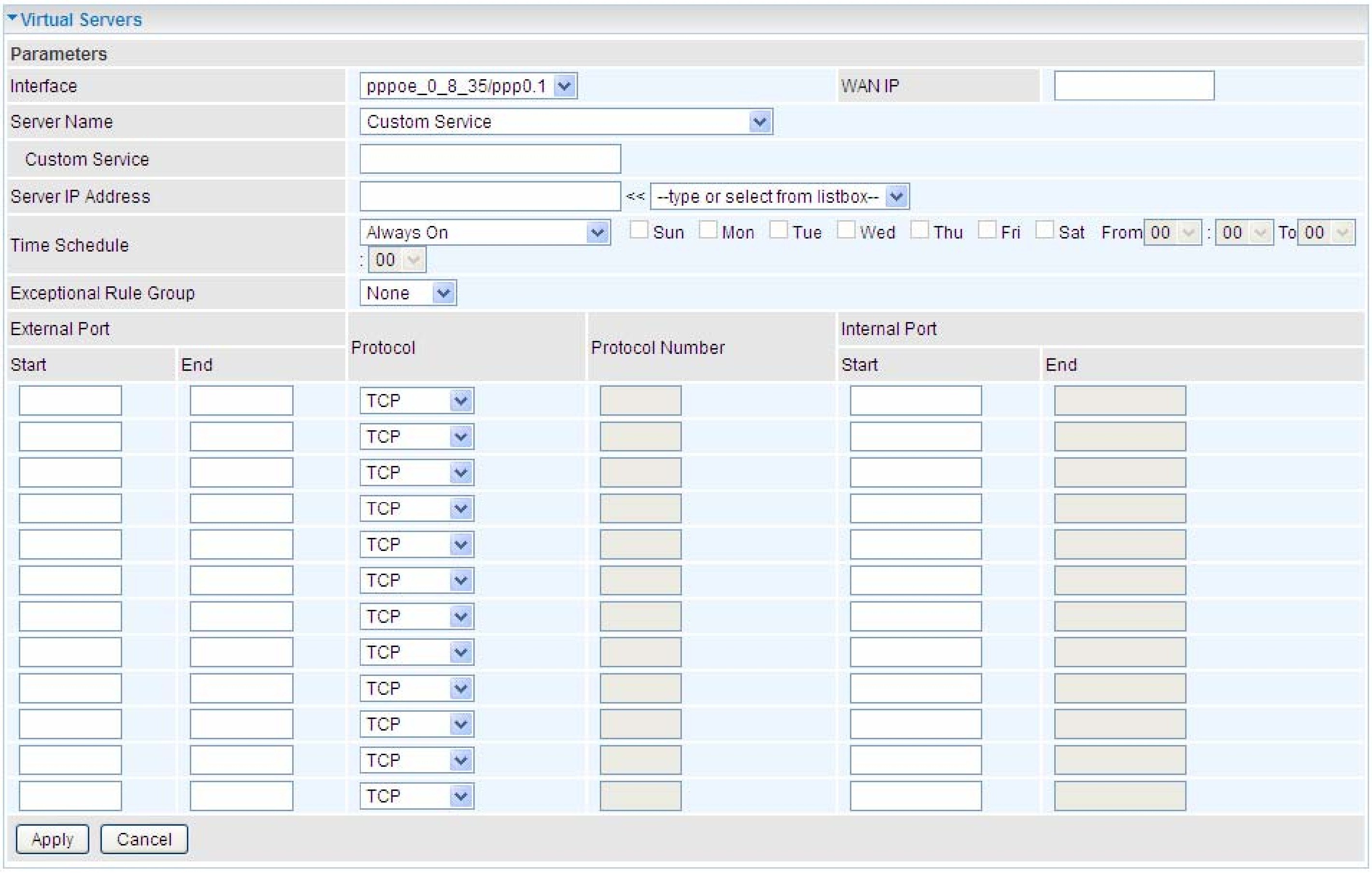


Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					

It is virtual server listing table as you see, Click **Add** to move on.

The following configuration page will appear to let you configure.



Virtual Servers

Parameters			
Interface	pppoe_0_8_35/ppp0.1	WAN IP	
Server Name	Custom Service		
Custom Service			
Server IP Address	<< --type or select from listbox--		
Time Schedule	Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00		
Exceptional Rule Group	None		

External Port		Protocol	Protocol Number	Internal Port	
Start	End			Start	End
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Interface: Select from the drop-down menu the interface you want the virtual server(s) to apply.

WAN IP: To specify the exact WAN IP address. It can be flexible while there are multiple WAN IPs on one interface. If the WAN IP field is empty, 78VDP(O)X uses the current wan IP of this interface.

Server Name: Select the server name from the drop-down menu.

Custom Service: It is a kind of service to let users customize the service they want. Enter the user-defined service name here. It is a parameter only available when users select **Custom Service** in the above parameter.

Server IP Address: Enter your server IP Address here. User can select from the list box for quick setup.

External Port

- **Start:** Enter a port number as the external starting number for the range you want to give access to internal network.
- **End:** Enter a port number as the external ending number for the range you want to give access to internal network.

Internal Port

- **Start:** Enter a port number as the internal staring number.
- **End:** Here it will generate automatically according to the End port number of External port and can't be modified.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

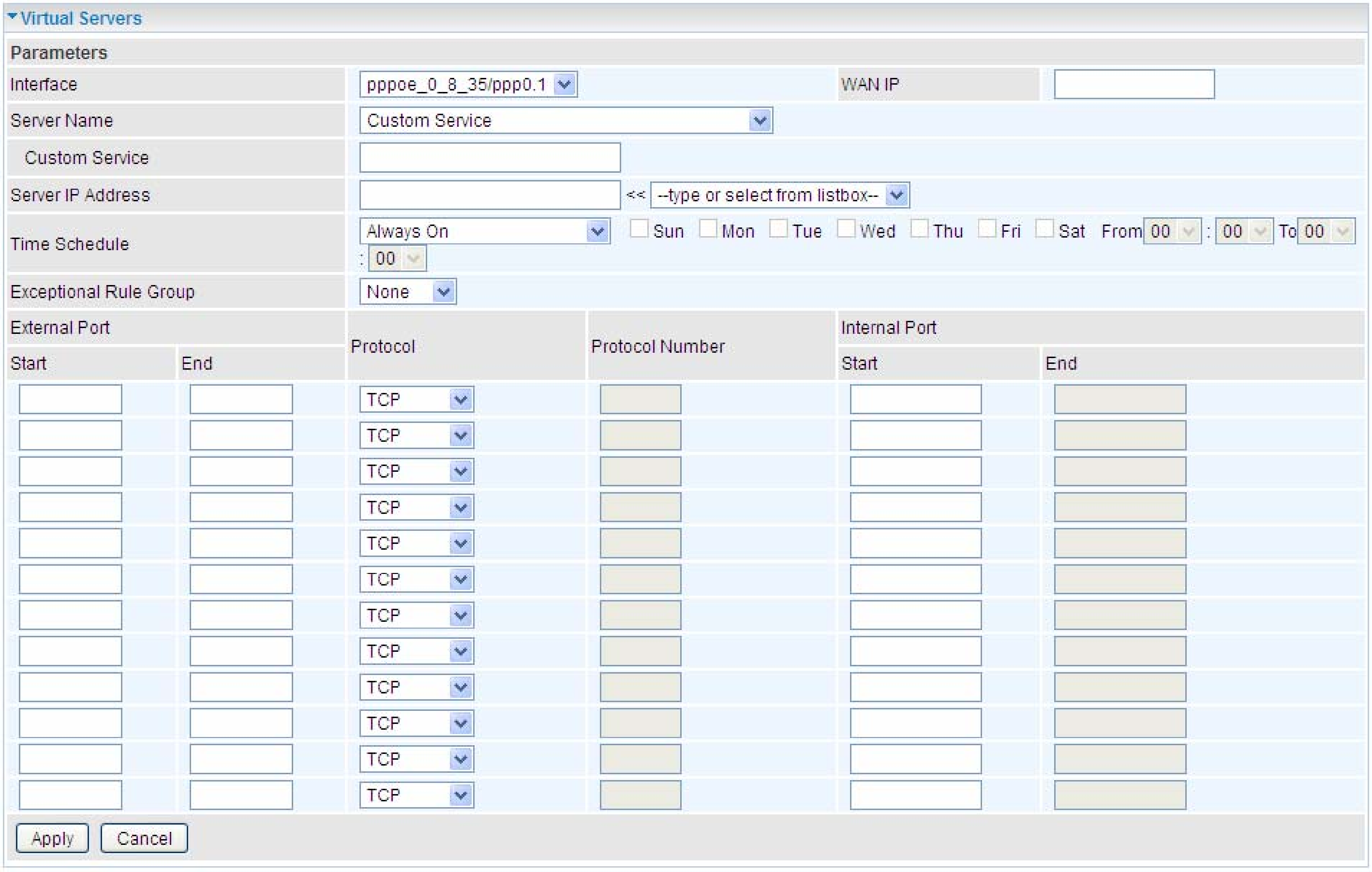
Time Schedule: Select or set exactly when the Virtual Server works. When set to "Always On", the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to "Disable", the rule is disabled and there will be an icon ✓ in the list table indicating the rule is disabled. See Time Schedule.

Exceptional Rule Group: Select the exceptional group listed. It is to grant or block Virtual Server access to a group of IPs. For example, as we set previously group 1 blocking access to

172.16.1.102-172.16.1.106. If here you want to block Virtual Server access to this IP range, you can select Group1.

Set up

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.



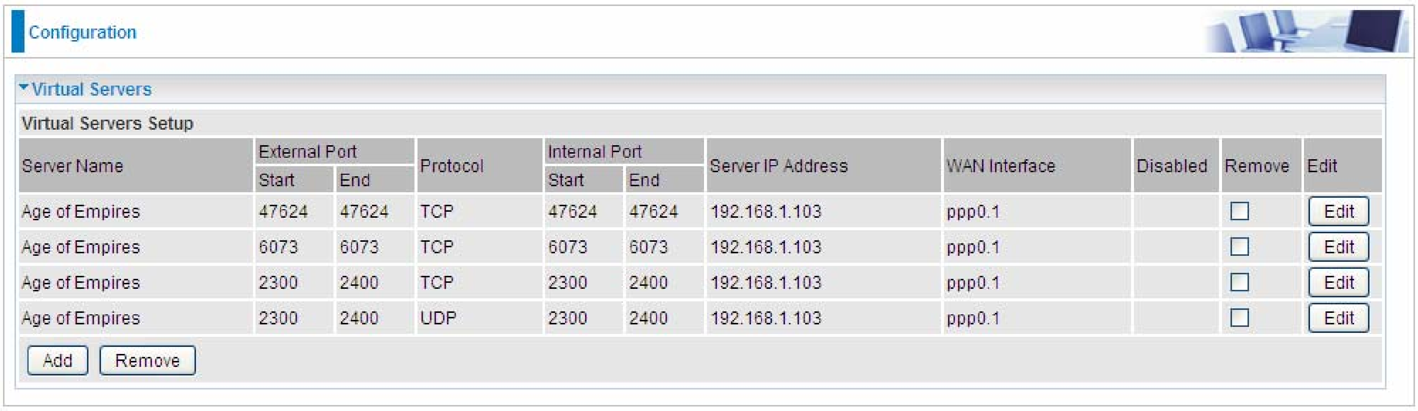
Virtual Servers

Parameters

Interface	pppoe_0_8_35/ppp0.1	WAN IP	
Server Name	Custom Service		
Custom Service			
Server IP Address	<< --type or select from listbox--		
Time Schedule	Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00		
Exceptional Rule Group	None		

External Port		Protocol	Protocol Number	Internal Port	
Start	End			Start	End
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

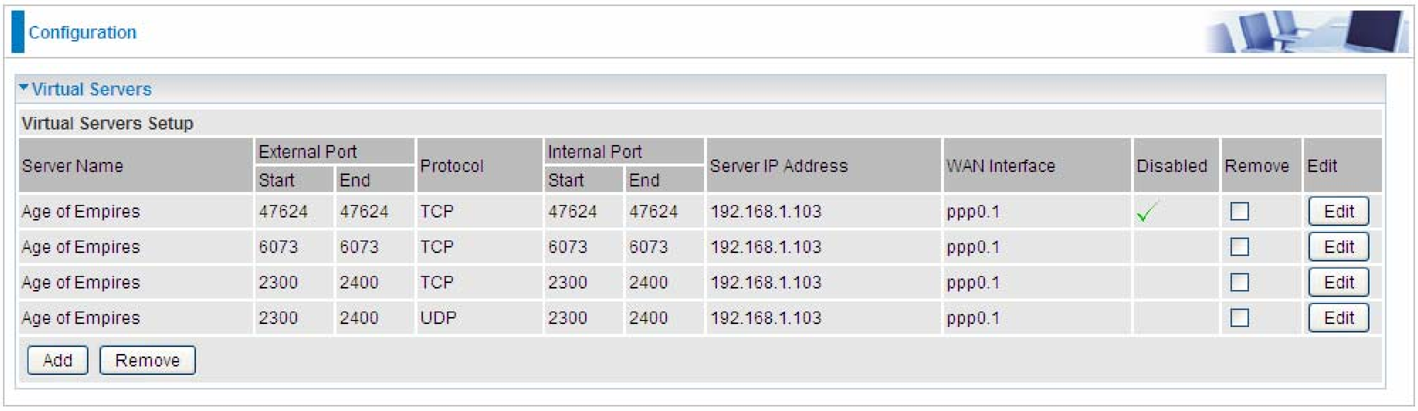
2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.



Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1		□	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		□	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		□	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		□	Edit



Configuration

Virtual Servers

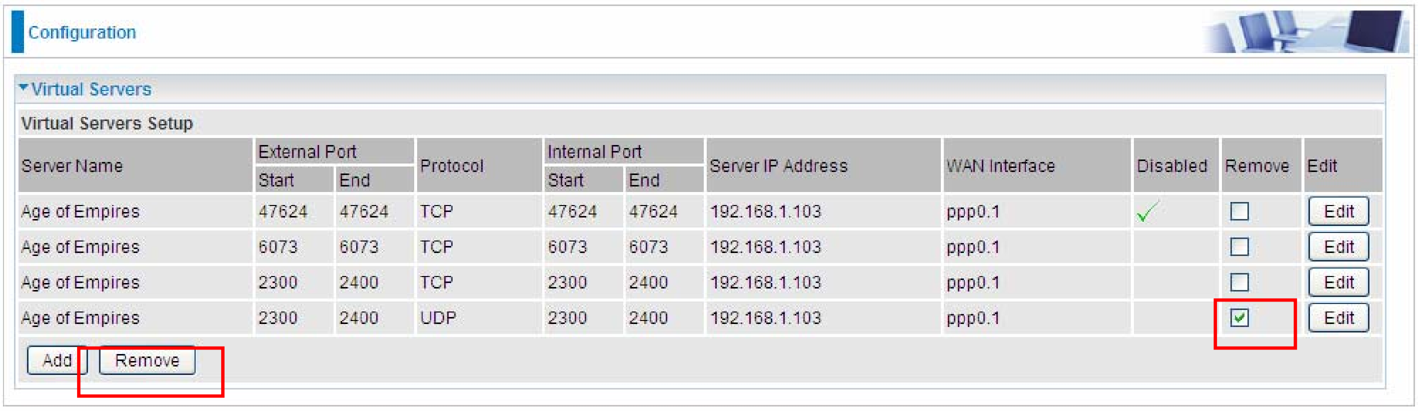
Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	✓	□	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		□	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		□	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		□	Edit

(✓ Means the rule is inactive)

Remove

If you don’t need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press **Remove**, it will be OK.



Configuration

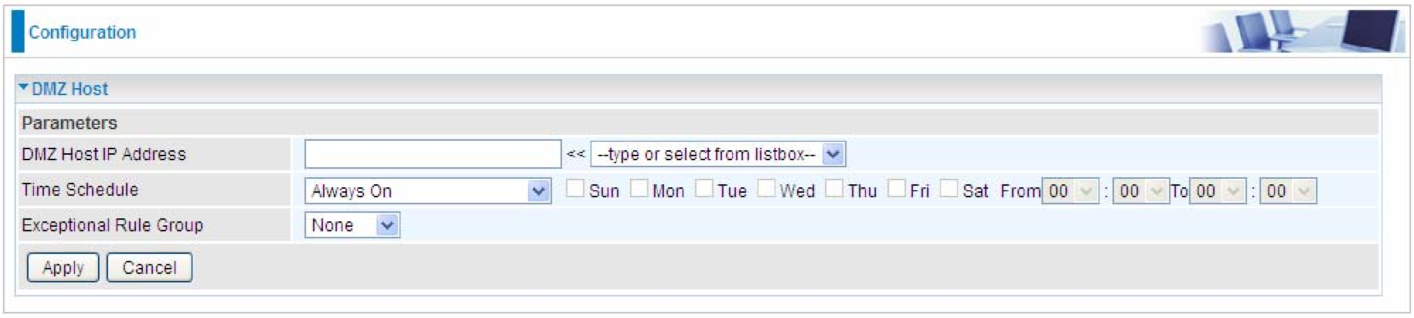
Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	✓	□	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		□	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		□	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		☑	Edit

DMZ Host

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



Configuration

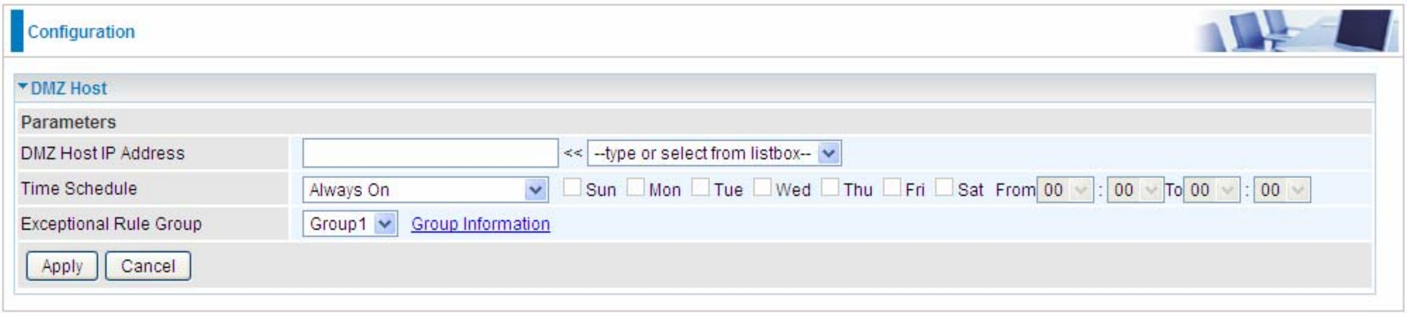
DMZ Host

Parameters

DMZ Host IP Address: [ ] << --type or select from listbox--

Time Schedule: Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00

Exceptional Rule Group: None



Configuration

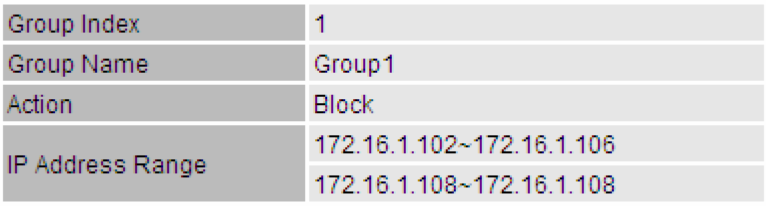
DMZ Host

Parameters

DMZ Host IP Address: [ ] << --type or select from listbox--

Time Schedule: Always On □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00

Exceptional Rule Group: Group1 Group Information



Group Index	1
Group Name	Group1
Action	Block
IP Address Range	172.16.1.102~172.16.1.106
	172.16.1.108~172.16.1.108

(Group Information)

DMZ Host IP Address: Enter the IP Address of a host you want it to be a DMZ host. Select from the list box to quick set the DMZ.

Time Schedule: Select or set exactly when the DMZ works. When set to "Always On", the DMZ will work all time; and also you can set the precise time when DMZ works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to "Disable", the DMZ Host is disabled. See Time Schedule.

Exceptional Rule Group: Select the exceptional group listed. It is to grant or block DMZ access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block DMZ Access to this IP range, you can select Group1.

NOTE:

Using port mapping does have security implications, since outside users are 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 simply using DMZ or creating a Virtual Server entry for "All" protocols, as doing so results in all connection attempts to your public IP address accessing the specified PC.

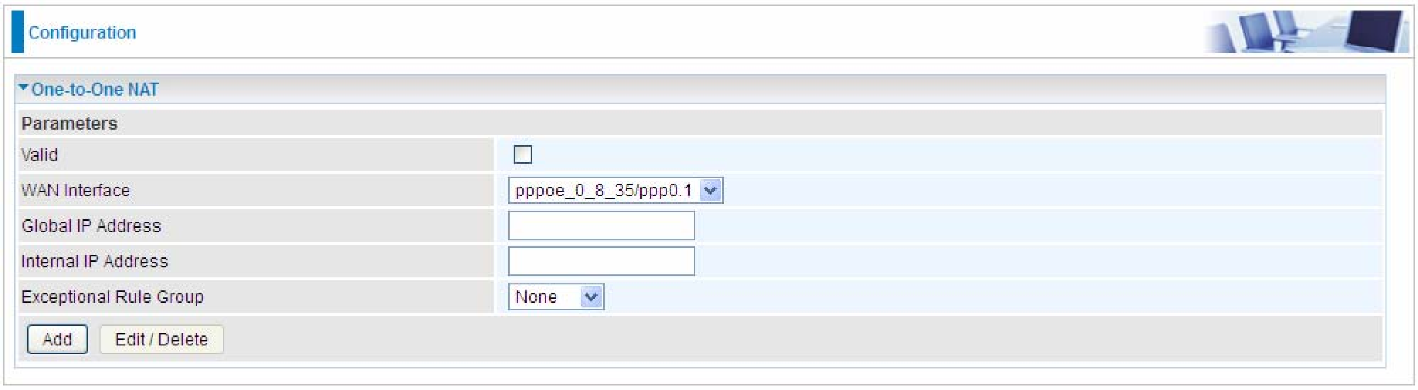
Attention

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

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

One-to-One NAT

One-to-One NAT maps a specific private/local address to a global/public IP address. If user has multiple global/public IP addresses from your ISP, you are free to use one-to-one NAT to assign some specific public IP for an internal IP like a public web server mapped with a global/public IP for outside access.



Parameters	
Valid	☐
WAN Interface	pppoe_0_8_35/ppp0.1
Global IP Address	
Internal IP Address	
Exceptional Rule Group	None

Valid: Check whether to valid the one-to-one NAT mapping rule.

WAN Interface: Select one based WAN interface to configure the one-to-one NAT.

Global IP address: The Global IP mapped to an internal device. It can be left empty, and under this circumstance, it can be reached through the WAN IP of interface set in the field above.

Internal Address: The IP address of an internal device in the LAN.

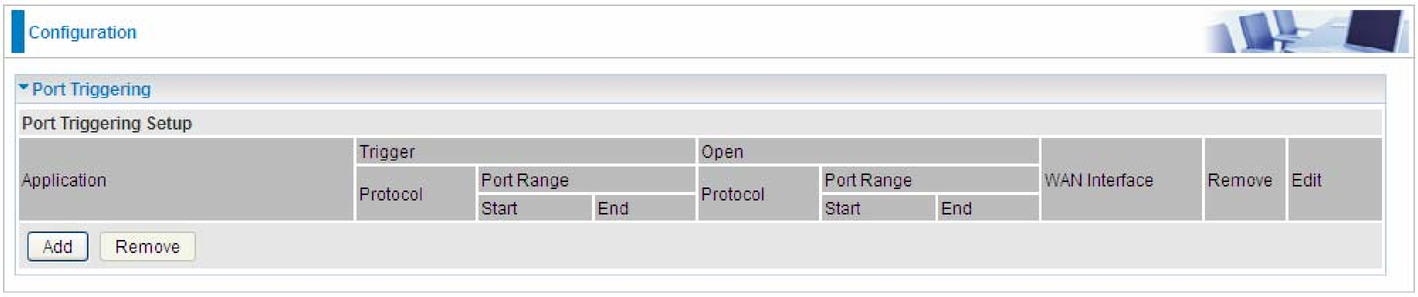
Exceptional Rule Group: Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to 123.1.1.2.

For example, you have an ADSL connection of pppoe_0_8_35/ppp0.1 interface with three fixed global IP, and you then can assign the other two global IPs to two internal devices respectively.

If you have a WEB server (IP address: 192.168.1.3) and a FTP server (IP address: 192.168.1.4) in local network, owning a public IP address range of 123.1.1.2 to 123.1.1.4 assigned by ISP. 123.1.1.2 is used as WAN IP address of the router, 123.1.1.3 is used for WEB server and 123.1.1.4 is used for FTP server. With One-to-One NAT, the servers with private IP addresses can be accessed at the corresponding valid public IP addresses.

Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.



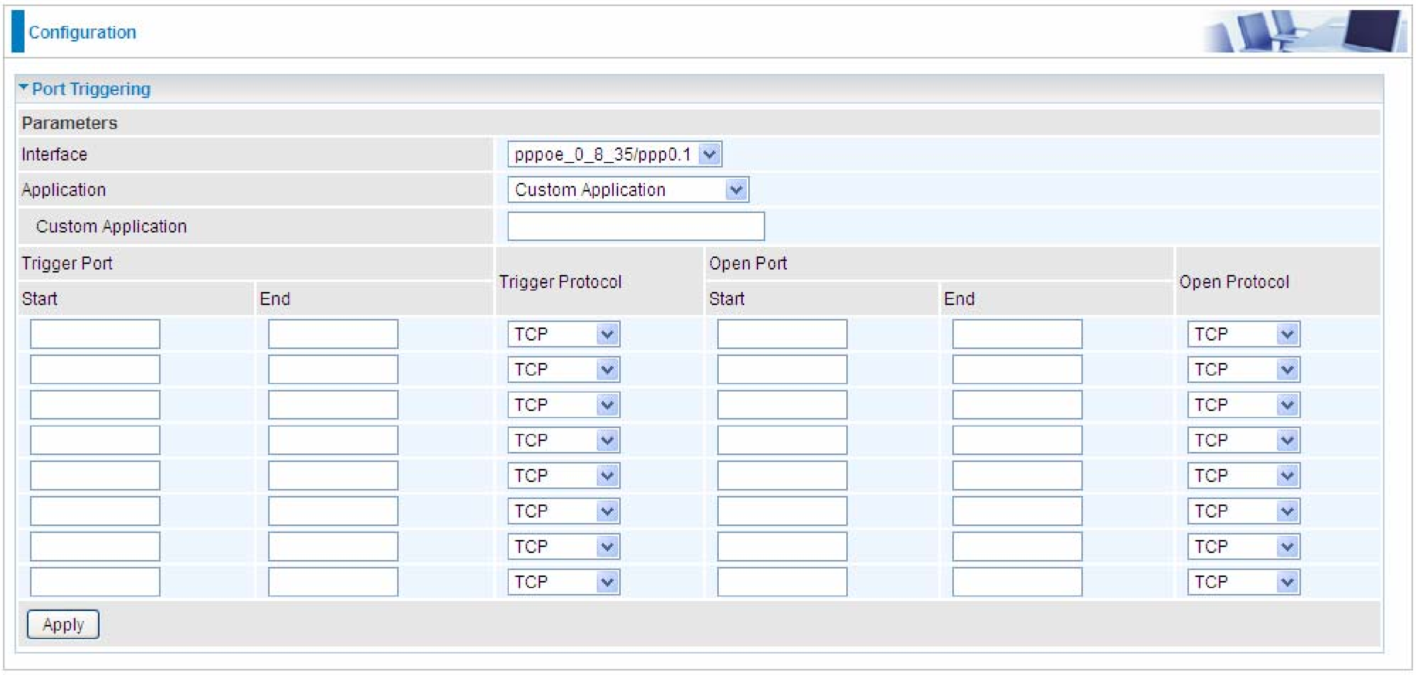
Configuration

Port Triggering

Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove	Edit
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			

Click **Add** to add a port triggering rule.



Configuration

Port Triggering

Parameters

Interface	pppoe_0_8_35/ppp0.1
Application	Custom Application
Custom Application	

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Interface: Select from the drop-down menu the interface you want the port triggering rules apply to.

Application: Preinstalled applications or Custom Application user can customize the utility yourself.

Custom Application: It is a kind of service to let users themselves customizes the service they want. Enter the user-defined service name here.

Trigger Port

- ⓘ **Start:** Enter a port number as the triggering port starting number.
- ⓘ **End:** Enter a port number as the triggering port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the trigger port.

Open port

- **Start:** Enter a port number as the open port staring number.
- **End:** Enter a port number as the open port ending number.

Any port in the range delimited by the 'Start' and 'End' would be the preset forwarding port or open port.

Protocol: select the protocol this service used: TCP/UDP, TCP, UDP.

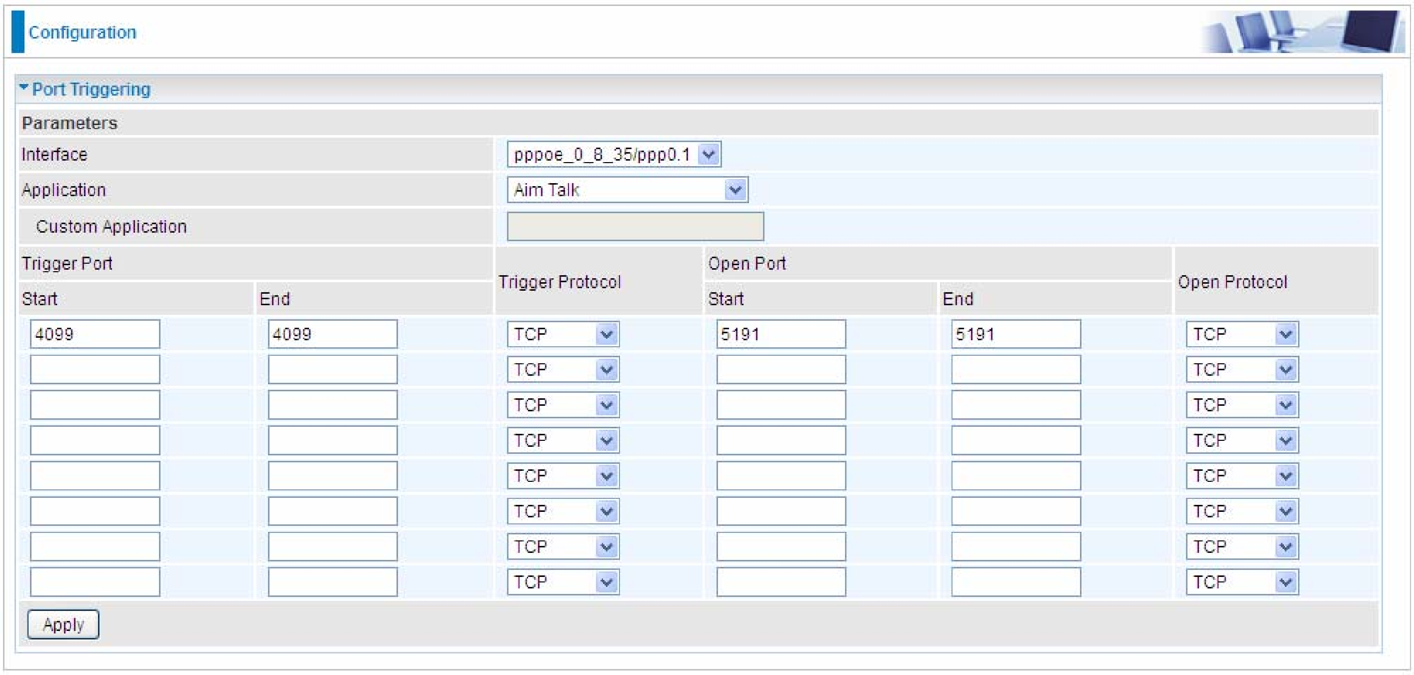
Set up

An example of how port triggering works, when a client behind a NAT router connecting to Aim Talk, it is a TCP connection with the default port 4099.

When connecting to Aim Talk, the client typically makes an outgoing connection on port 4099 to the Aim Talk server, but when the computer is behind the NAT, the NAT silently drops this connection because it does not know which computer behind the NAT to send the request to connect.

So, in this case, port triggering in the router is working, when an outbound connection is attempted on port 4099 (or any port in the range set), it should allow inbound connections to that particular computer.

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.



Configuration

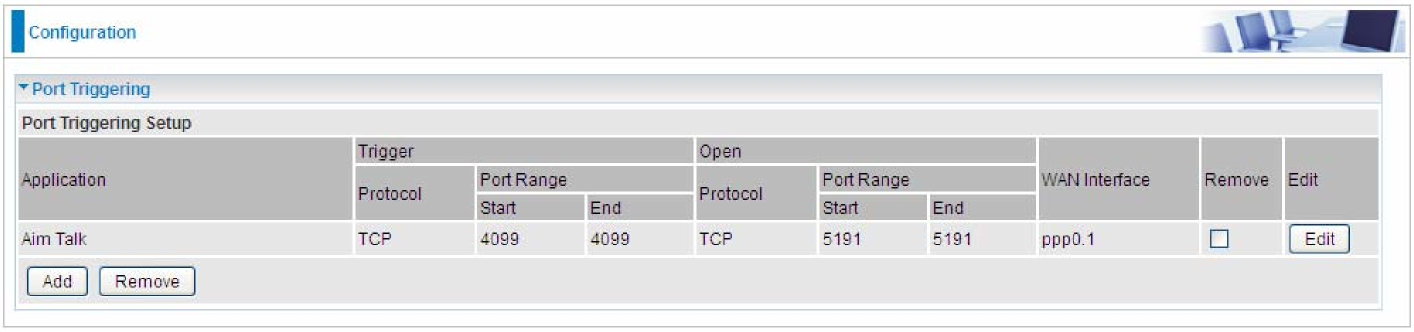
Port Triggering

Parameters

Interface	pppoe_0_8_35/ppp0.1
Application	Aim Talk
Custom Application	

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
4099	4099	TCP	5191	5191	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.



Configuration

Port Triggering

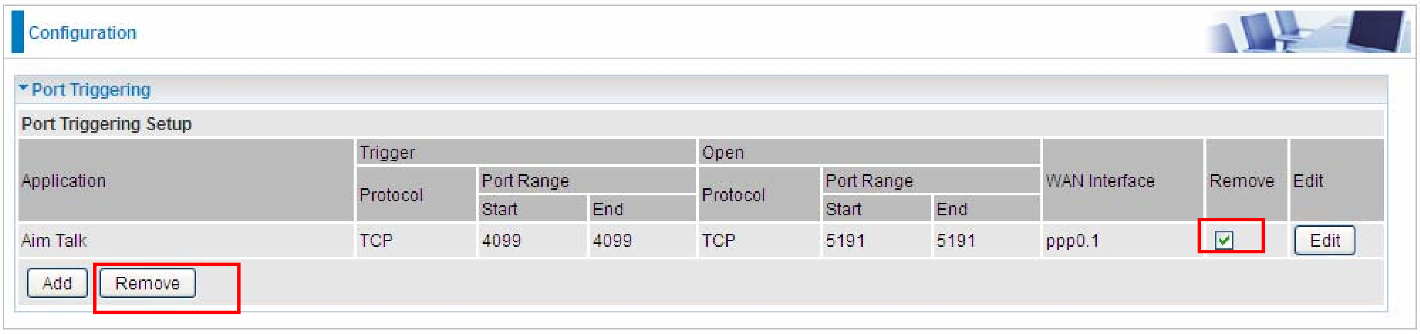
Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove	Edit
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	□	Edit

Edit/Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, and then press **Remove**.

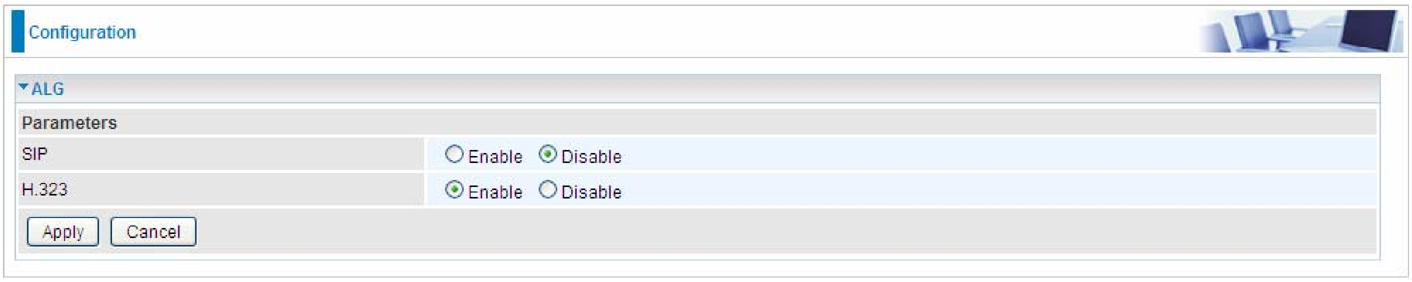
Click **Edit** to re-edit your port-triggering rule.



Application	Trigger			Open			WAN Interface	Remove	Edit
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	☑	Edit

ALG

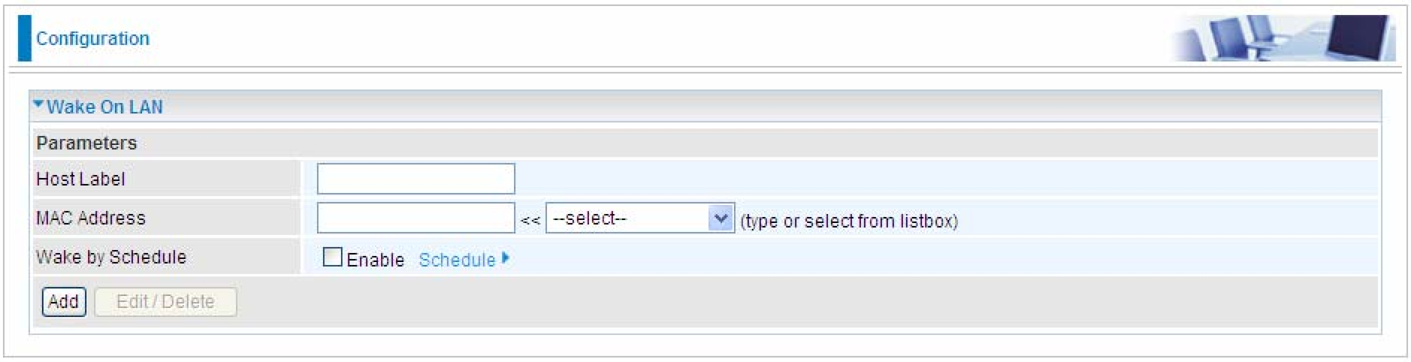
The ALG Controls enable or disable protocols over application layer.



Parameters	
SIP	○ Enable ● Disable
H.323	● Enable ○ Disable

Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.



Configuration

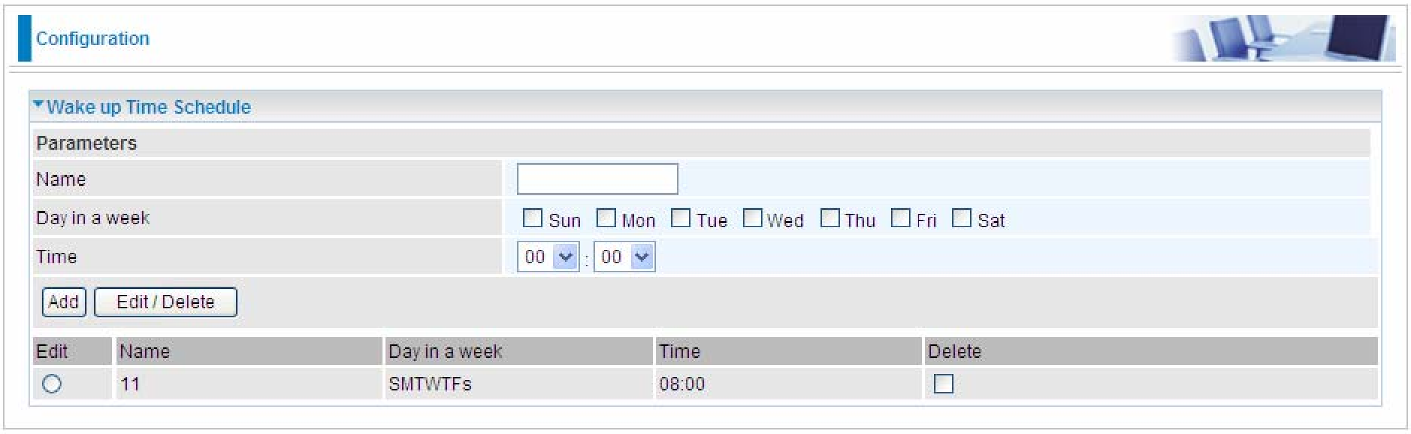
▾Wake On LAN

Parameters	
Host Label	
MAC Address	<< --select-- (type or select from listbox)
Wake by Schedule	□ Enable Schedule ▸

Host Label: Enter identification for the host.

Select: Select MAC address of the computer that you want to wake up or turn on remotely.

Wake by Schedule: Enable to wake up your set device at some specific time. For instance, user can set to get some device woken up at 8:00 every weekday. Click Schedule to enter time schedule configuring page to set the exact timeline.



Configuration

▾Wake up Time Schedule

Parameters	
Name	
Day in a week	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Time	00 : 00

Edit	Name	Day in a week	Time	Delete
○	11	SMTWTFs	08:00	□

Add: After selecting, click Add then you can submit the Wake-up action.

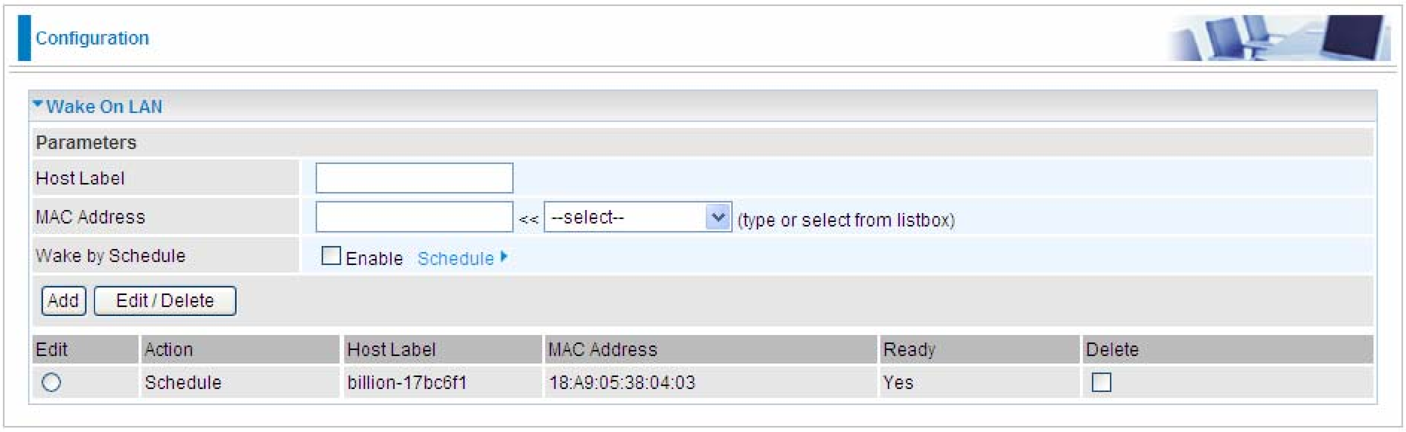
Edit/Delete: Click to edit or delete the selected MAC address.

Ready:

“Yes” indicating the remote computer is ready for your waking up.

“No” indicating the machine is not ready for your waking up.

Delete: Delete the selected MAC address.



Configuration

▾Wake On LAN

Parameters	
Host Label	
MAC Address	<< --select-- (type or select from listbox)
Wake by Schedule	□ Enable Schedule ▸

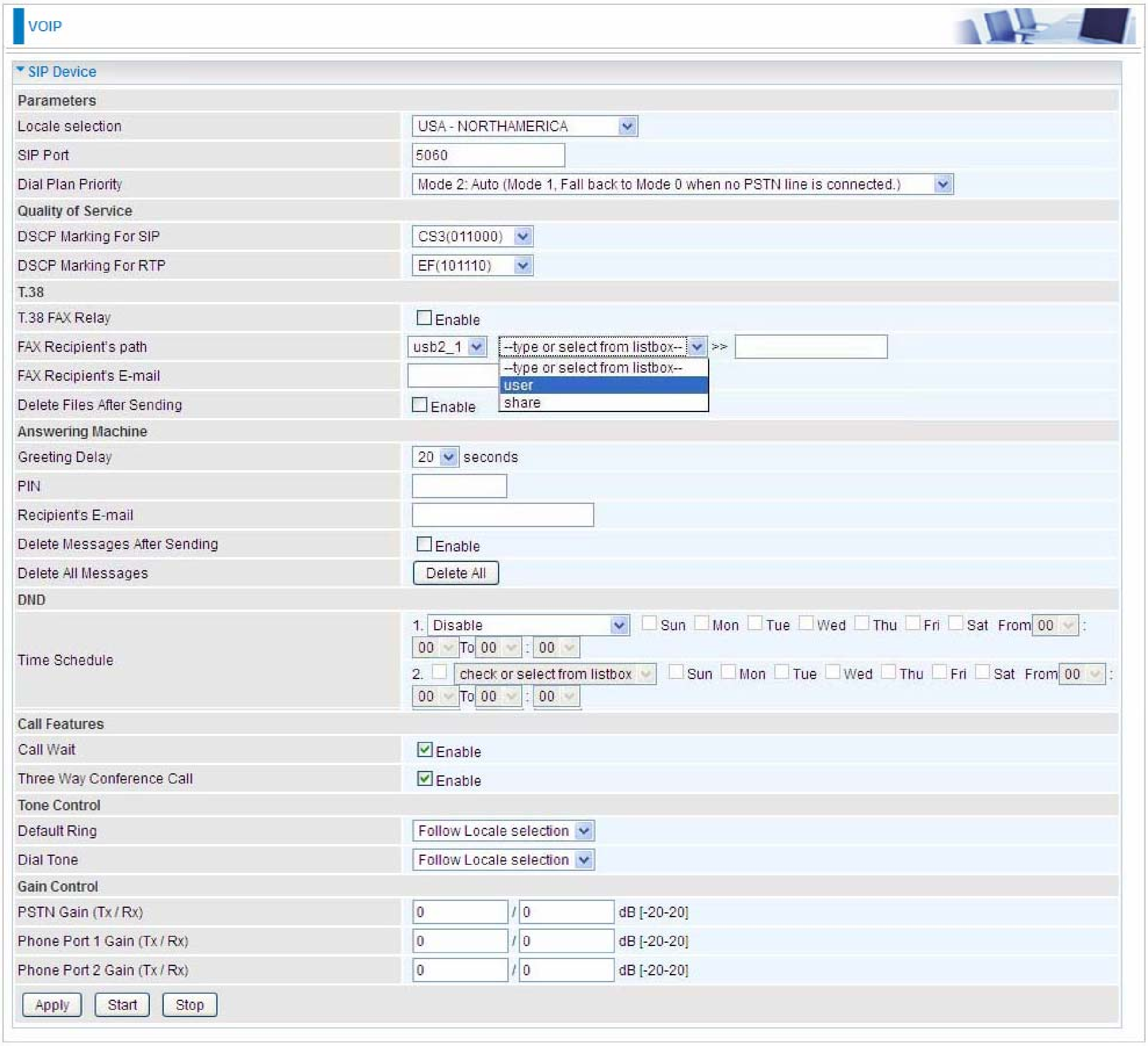
Edit	Action	Host Label	MAC Address	Ready	Delete
○	Schedule	billion-17bc6f1	18:A9:05:38:04:03	Yes	□

VoIP

VoIP, or Voice over Internet Protocol, enables telephone calls through existing internet connections instead of going through the traditional PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long-distance call, but also top quality voice calls over the internet.

Five sub-items to be covered to configure the VoIP feature, namely **SIP Device**, **Service Provider**, **SIP Account**, **Call Forward**, **Call Trough**, **Call Block**, **VoIP Dial Plan**, **PSTN Dial Plan, Phone Book**

SIP Device



▾ SIP Device

Parameters	
Locale selection	USA - NORTHAMERICA
SIP Port	5060
Dial Plan Priority	Mode 2: Auto (Mode 1, Fall back to Mode 0 when no PSTN line is connected.)
Quality of Service	
DSCP Marking For SIP	CS3(011000)
DSCP Marking For RTP	EF(101110)
T.38	
T.38 FAX Relay	□ Enable
FAX Recipient's path	usb2_1 --type or select from listbox-- >> --type or select from listbox-- user share
FAX Recipient's E-mail	
Delete Files After Sending	□ Enable
Answering Machine	
Greeting Delay	20 seconds
PIN	
Recipient's E-mail	
Delete Messages After Sending	□ Enable
Delete All Messages	Delete All
DND	
Time Schedule	1. Disable □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00 2. □ check or select from listbox □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 00 : 00 To 00 : 00
Call Features	
Call Wait	☑ Enable
Three Way Conference Call	☑ Enable
Tone Control	
Default Ring	Follow Locale selection
Dial Tone	Follow Locale selection
Gain Control	
PSTN Gain (Tx / Rx)	0 / 0 dB [-20-20]
Phone Port 1 Gain (Tx / Rx)	0 / 0 dB [-20-20]
Phone Port 2 Gain (Tx / Rx)	0 / 0 dB [-20-20]

Locale: This selection is a drop-down box, which allows users to select the country for which the VoIP device is operating. When a country is selected, the country parameters are automatically loaded. Different countries can have their special ring mechanism.

SIP Port: Set the SIP port, default 5060.

Dial Plan Priority: Three modes for users to set the dial mechanism, default is set to Auto, thus PSTN only with exception.

- **Mode 0:** VoIP only and ignore all PSTN dial plans, send all calls to VoIP, including Emergency calls.
- **Mode 1:** Default, which means that under this mode, the dial mechanism always match PSTN plan first, then move to VoIP plan.
- **Auto:** Auto, this means the dial system will fall back to Mode 0 (VoIP) when no PSTN is connected.

Quality of Service

User can mark DSCP for outgoing SIP and RTP. VoIP flow to control VoIP QoS.

DSCP Marking For SIP: Set the DSCP marking for SIP VoIP packets for QoS proceeding.

DSCP Marking For RTP: Set the DSCP marking for RTP VoIP packets for QoS proceeding.

T.38

T.38 relay is a way to permit faxes to be transported across IP networks between existing fax terminals. The T.38 fax gateway converts and encapsulates the fax sent from the terminal fax machines into a T.38 date stream. Then the gateway send the converted date packets to a T.38 enabled end point such as a fax or fax server or another T.38 gateway that converts it back to the analog signal to realize the communication between two fax terminals.

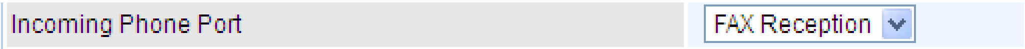
T.38 Relay: Click Enable to allow transmission of fax over IP network between two fax machines. If T.38 relay is disabled, the analog fax signal is transmitted as the normal audio data. If T.38 relay is enabled, the fax signal is converted to T.38 signal.

FAX Recipient's path: Set the path directly for storing the fax file to the storage.

Note: For common fax usage, user should have a fax connected to the router, creating a fax environment between two fax terminals, and the fax file(s) would be received through fax connected to the router as what we usually perform.

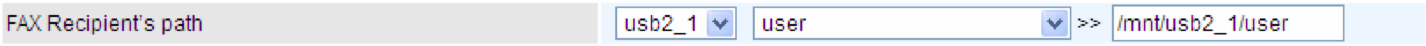
But if user does not get a fax or he wants to store the fax to the file directly, he then can enable Fax Reception feature. Select or enter manually the reception path for the file. (Here user can turn to USB for help.)

1) Set the field "Incoming Phone Port" to "FAX Reception" at the "VoIP Account" page.



Incoming Phone Port | FAX Reception

2) Set the path user wants fax file saved at "FAX Recipient's path" at the "SIP Device" page.



FAX Recipient's path | usb2_1 | user >> /mnt/usb2_1/user

3) The incoming VoIP call for the specified VoIP account will be treated as Fax and saved to path.

FAX Recipient's E-mail: Enter the recipient's email address. Once the fax file is delivered, the fax file will be mailed to the account specified by the "Recipient's Email",

Delete Files After Sending: The files will be deleted from system once the mail is sent out.

Answering Machine

The answering machine is a device for answering telephones and recording callers' messages and being enabled for both VoIP and PSTN.

The operation for the answering machine:

***#00:** Record user own greeting message;

1) Start the recording after the beep sound

2) Press # while finished.

3) Hang up after the beep is heard. (system needs time on file translation and save to storage).

***#99:** Delete the user's greeting message

***#98:** Play the greeting message

***#xx:** Access the specified answering machine where xx (automatically designated by the system) can be found at the "SIP Account" page.

***#96:** Enable the answering machine

***#97:** Disable the answering machine

1) After the beep sound, dial the specified code xx where xx can be found at the "SIP Account" page.

2) Hang up after the beep is heard. (system needs time on file translation and save to storage).

***#90:** Access the PSTN A/M.
Note: 7800VDP(O)X uses the 1st available phone port to record the PSTN message. So, the answer machine stops recording if user picks up the specified phone.

Greeting Delay: The parameter is used as a threshhold for the answer machine to automatically answer and record the messgae. There are seven items marking 0, 5, 10, 15, 20, 25, 30 respectively. For example, if set to 0s, when there is an incoming call, the answering machine will respond immediately and record the message. And if it is set to 20s, then the call will keep ringing until time out of 20s (without user picking up the phone) before it can respond and record the meassge.

PIN: The set password (no exceeding 8 digits) for listening to message. The customer should press the PIN number so as to listen to the message. Leave it empty, and user can listen to the message without entering password first.

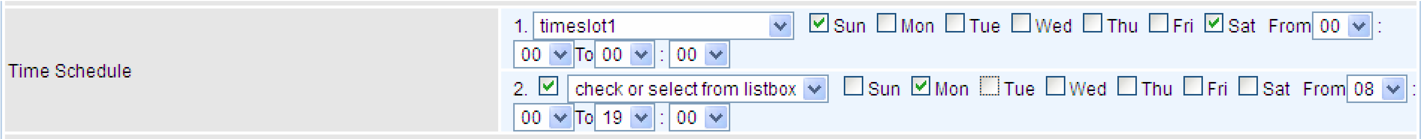
Recipient's Email: Enter the recipient's email address. Once the voice message is left (answering machine operation), the voice message will be mailed to the account specified by the "Recipient's Email",

Deleting Messages After Sending: The message will be deleted from system once the mail is sent out.

Delete All Messages: Press the "Delete All" button to delete all messages stored in the system all at once.

DND

User can set the time period here, during which both incoming VoIP and PSTN calls will be rejected.



Time Schedule

1. timeslot1 ☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat From 00 : 00 To 00 : 00

2. ☑ check or select from listbox □ Sun ☑ Mon □ Tue □ Wed □ Thu □ Fri □ Sat From 08 : 00 To 19 : 00

Time Schedule: When set to "Always On", all the incoming calls will be rejected constantly; and also you can set the precise time when the incoming calls are supposed to rejected. Or you can select the already set timeslot in "**Time Schedule**". And when set to "Disable", there will be no time restrictions on incoming calls. See Time Schedule.

Call Features

Call Wait: Enable to activate Call Wait feature. When you are busy on a call, and another call comes in, while the Call Wait feature is enabled, you can hear a hint sound indicating there is another call in for you to decide whether to answer by slightly pressing the key "Flash" to keep the original call.

Three Way Conference Call: Enable to activate three way conference call.

Tone Control

Default Ring: Support “Follow Locale selection” (Different countries have their special tone mechanism) and another 4 embedded ring tones.

Dial Tone: Support “Follow Locale selection” and another 5 embedded dial tones.

Gain Control

Gain control is to reduce the bad performance of quality issue caused by noise or echo, etc. Rx means the performance of receiving and the Tx implies the performance of transimitting. A plus quantity is to raise the performance while a negative quantity is to cut the performance (Rx: +1 to increase the performance of receiving by 1 point and if set -1, the performance will be cut by 1 point, the range is -20- 20.).

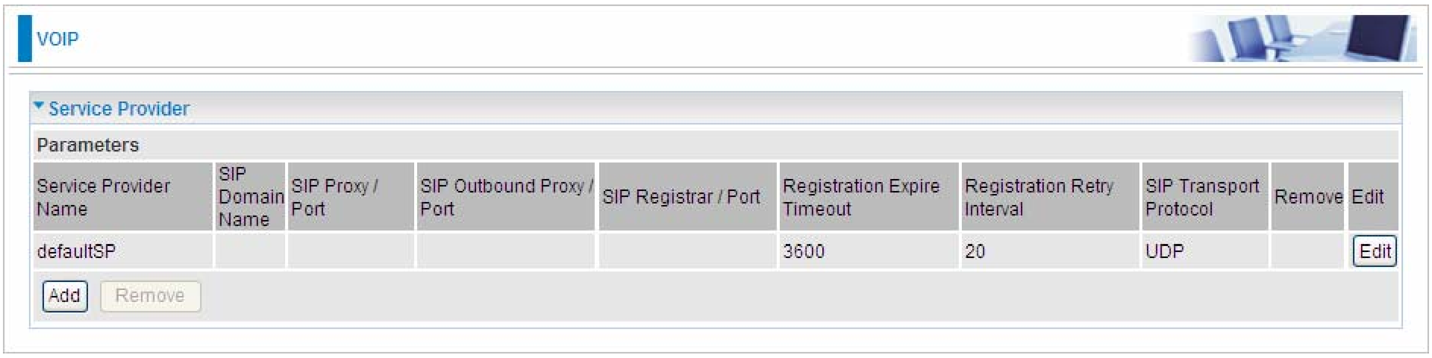
PSTN Gain: Set the PSTN gain, Tune the gain between -20-20 of the Rx and Tx respectively to obtain a appropriate PSTN call environment.

Phone Port 1 Gain: Set the gain. Tune the gain between -20-20 of the Rx and Tx respectively to ensure a clear phone call.

Phone Port 2 Gain: Set the gain. Tune the gain between -20-20 of the Rx and Tx respectively to ensure a clear phone call.

Service Provider

Register to a SIP service provider is an essential step before making the VoIP call. Users can find out SIP service provider, and register a SIP account, jotting down the registration information and configuring in router.



VOIP

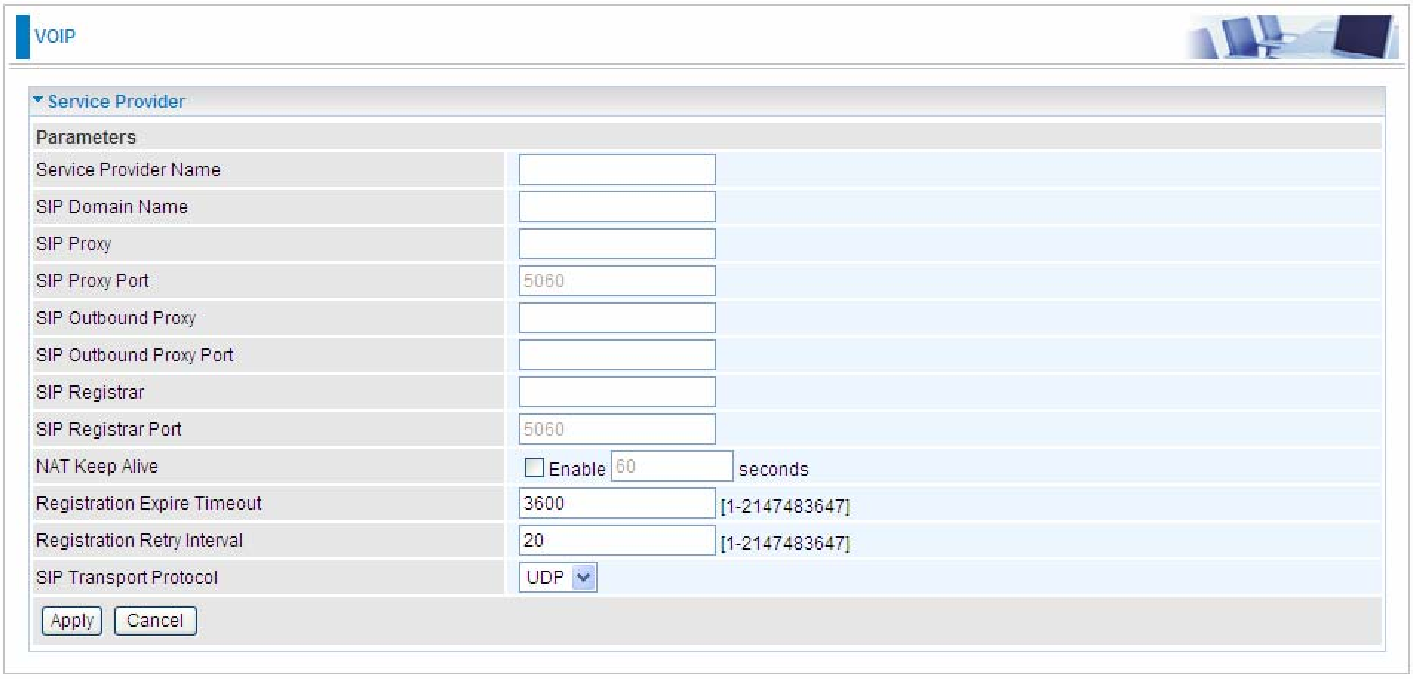
Service Provider

Parameters

Service Provider Name	SIP Domain Name	SIP Proxy / Port	SIP Outbound Proxy / Port	SIP Registrar / Port	Registration Expire Timeout	Registration Retry Interval	SIP Transport Protocol	Remove	Edit
defaultSP					3600	20	UDP		Edit

Add Remove

BiPAC 7800VDP(O)X offers a defaultSP item, you can change the settings or add a new Service Provider yourself.



VOIP

Service Provider

Parameters

Service Provider Name	
SIP Domain Name	
SIP Proxy	
SIP Proxy Port	5060
SIP Outbound Proxy	
SIP Outbound Proxy Port	
SIP Registrar	
SIP Registrar Port	5060
NAT Keep Alive	□ Enable 60 seconds
Registration Expire Timeout	3600 [1-2147483647]
Registration Retry Interval	20 [1-2147483647]
SIP Transport Protocol	UDP

Apply Cancel

Service Provider Name: Name of provider of the VoIP service

SIP Domain Name: Enter the SIP registrar domain name.

SIP Proxy: Also seen as SIP server, it manages the setup of calls between SIP devices including the controlling of call routing and some necessary functions such as registration, authentication, and network access control. Type the SIP Proxy address you obtain after you register from the service provider.

SIP Proxy Port: The port number set on your SIP proxy serve that the SIP proxy server uses to make network connections, default is 5060.

SIP Outbound Proxy: SIP outbound proxy is in similar use as SIP proxy, but when the SIP devices are behind a firewall or a router or NAT, the SIP outbound proxy is the useful way to let SIP traffic to pass from the internal network to the internet. Enter the SIP outbound proxy server address here.

SIP Outbound Proxy port: Enter the port, normally 5060.

SIP Registrar: Type the VoIP SIP registrar IP address.

SIP Registrar Port: Type the port; it will listen to register requests from VoIP devices.

NAT Keep Alive: Disabled by default. User can enable it if 7800VDP(O)X is placed behind a NAT router to ping SIP server every 60seconds (can be changed base on need) to verify the SIP server is working.

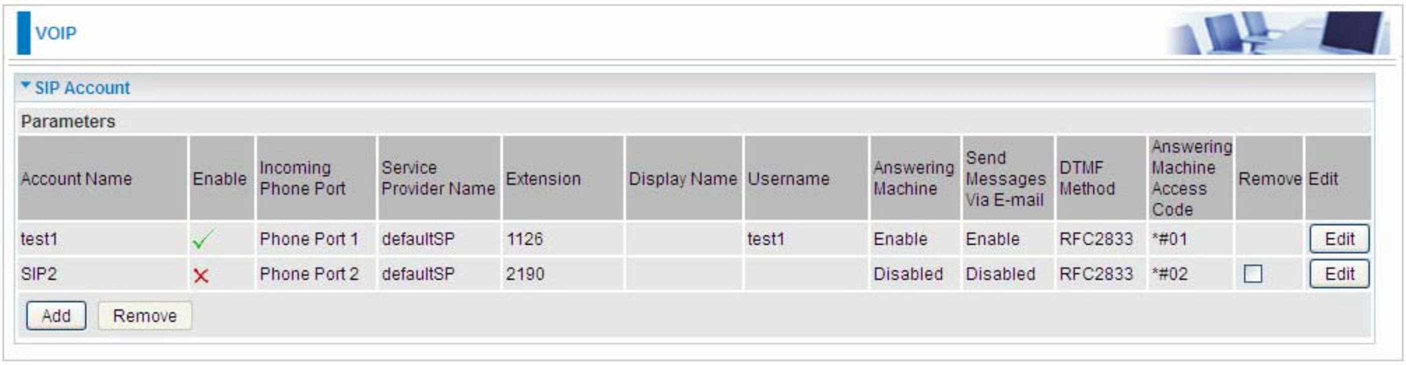
Registration Expire Timeout: This sets time interval before timeout.

Registration Retry Interval: The interval set to retry sending registration message.

SIP Transport Protocol: The protocol adopted to transport SIP, UDP commonly used.

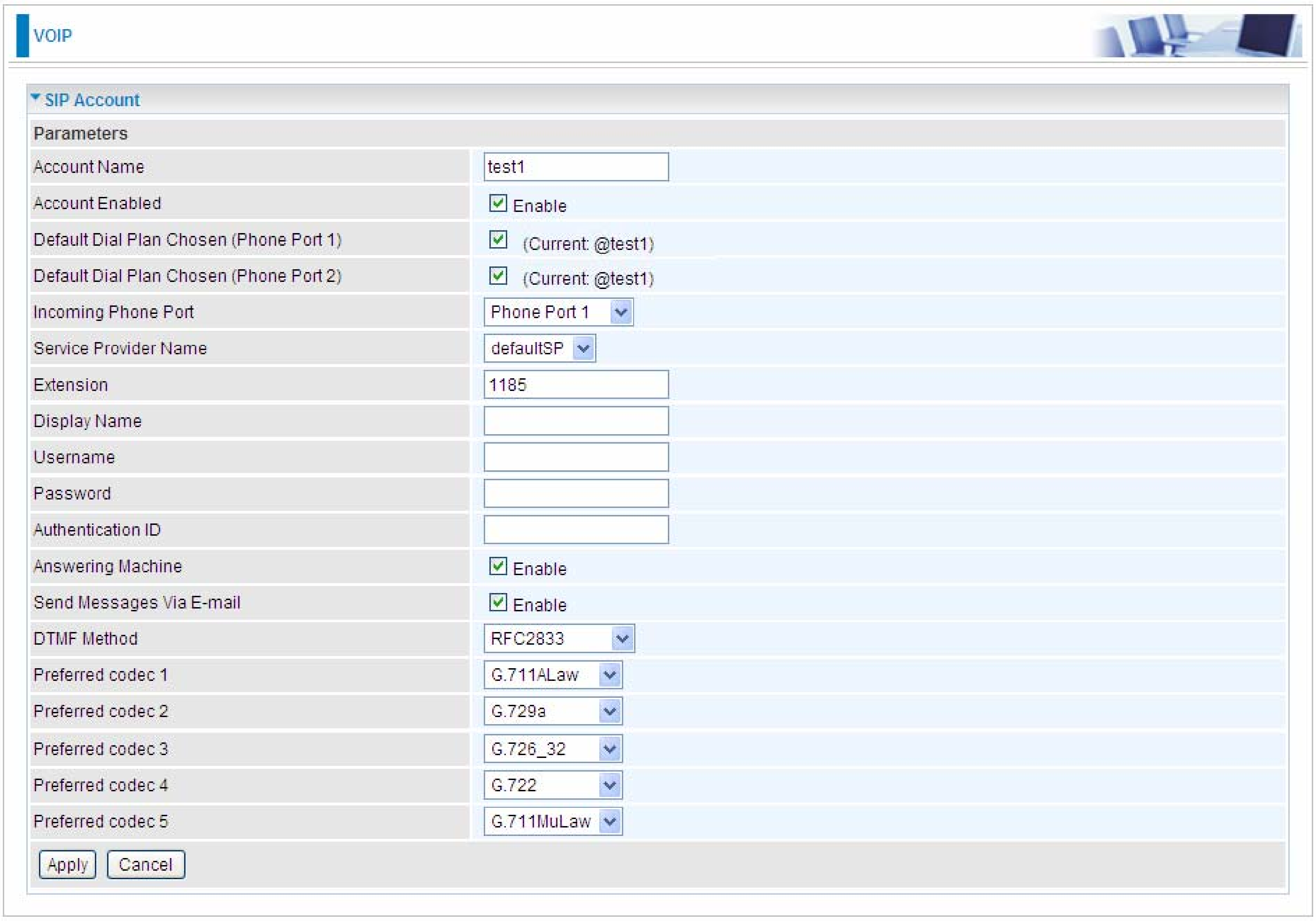
SIP Account

SIP account is an independent section for SIP account settings, including Extension number, etc.



Account Name	Enable	Incoming Phone Port	Service Provider Name	Extension	Display Name	Username	Answering Machine	Send Messages Via E-mail	DTMF Method	Answering Machine Access Code	Remove	Edit
test1	✓	Phone Port 1	defaultSP	1126		test1	Enable	Enable	RFC2833	*#01		Edit
SIP2	✗	Phone Port 2	defaultSP	2190			Disabled	Disabled	RFC2833	*#02	□	Edit

Click **Add** or **Edit** to add new account or modify the existing sip account.



Parameters	
Account Name	test1
Account Enabled	☑ Enable
Default Dial Plan Chosen (Phone Port 1)	☑ (Current: @test1)
Default Dial Plan Chosen (Phone Port 2)	☑ (Current: @test1)
Incoming Phone Port	Phone Port 1
Service Provider Name	defaultSP
Extension	1185
Display Name	
Username	
Password	
Authentication ID	
Answering Machine	☑ Enable
Send Messages Via E-mail	☑ Enable
DTMF Method	RFC2833
Preferred codec 1	G.711ALaw
Preferred codec 2	G.729a
Preferred codec 3	G.726_32
Preferred codec 4	G.722
Preferred codec 5	G.711MuLaw

Account Name: User-defined account name.

Account Enabled: Enable to activate the sip account.

Default Dial Plan Chosen (Port 1): Enable to allow user to set the account as the default VoIP rules for port 1.

Default Dial Plan Chosen (Port 2): Enable to allow user to set the account as the default VoIP rules for port 2.

Incoming Phone Port: Select which phone port you are setting.

Extension: The Phone number.

Display Name: Enter a display name to identify the phone, like indicating the phone usage.

User Name: The user name user registers in the sip server.

Password: The password user registers in the sip server.

Authentication ID: It is an authentication code required for some ISP, and can be left empty if not required.

Answering Machine: Enable to activate the answering machine feature so that user can record and listen to the messages of this phone.

Send Message Via E-mail: Enable to send message left by callers via e-mail to the user.

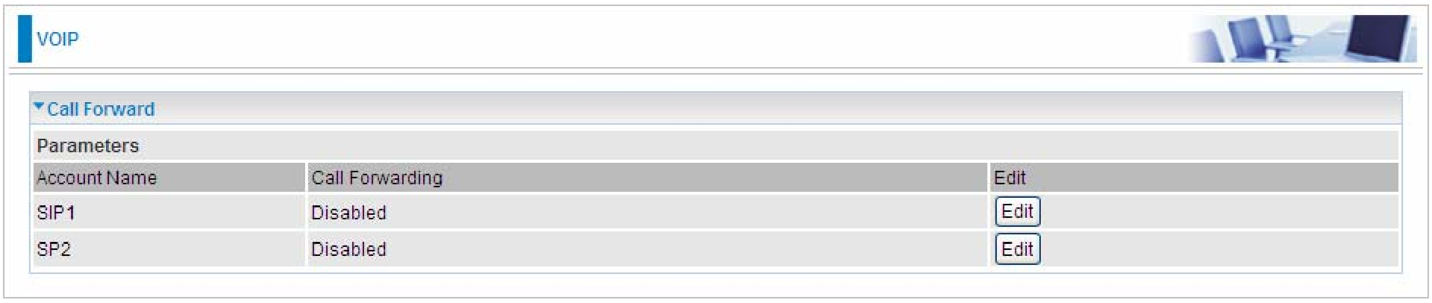
DTMF Method: DTMF stands for "Dual-Tone Multi-Frequency", and is a telecommunication signaling over analog telephone lines widely used between telephone handsets and other communication devices and the switching center. “DTMG method” provides ways to transmit DTMF for VoIP, such as RFC 2833, SIP Info, SIP Info (short), Inband and Auto, and RFC2833 is the widely used one.

Preferred codec#1,2,3,4,5: Codec is known as Coder-Decoder used for data signal conversion. Set the priority of voice compression; Priority 1 owns the top priority.

- **G.711A-LAW:** It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample into 8-bit value.
- **G.**729a: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- **G.726_32:** It is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 32kbit/s.
- **G.722:** G.722 is an ITU standard codec that provides 7 kHz wideband audio at data rates from 48, 56 and 64 kbit/s. G.722 sample audio data at a rate of 16 kHz (using 14 bits), double that of traditional telephony interfaces, which results in superior audio quality and clarity.
- **G.711Mu-Law:** It is a basic non-compressed encoder and decoder technique. µ-LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample.

Call Forward

Call features is designed to allow all calls or specific calls redirected to some specified call number when under some special situation or contingency occurs.



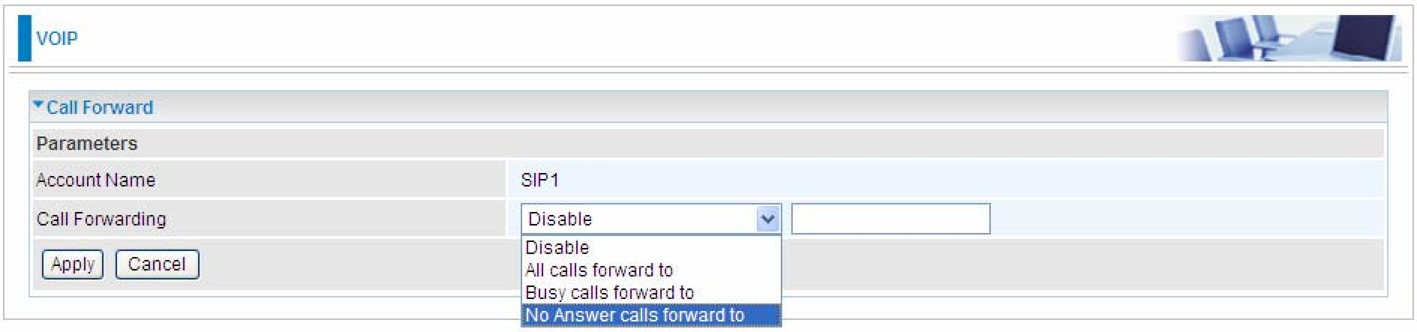
VOIP

▾Call Forward

Parameters

Account Name	Call Forwarding	Edit
SIP1	Disabled	Edit
SP2	Disabled	Edit

Click **Edit** to change the Call Features.



VOIP

▾Call Forward

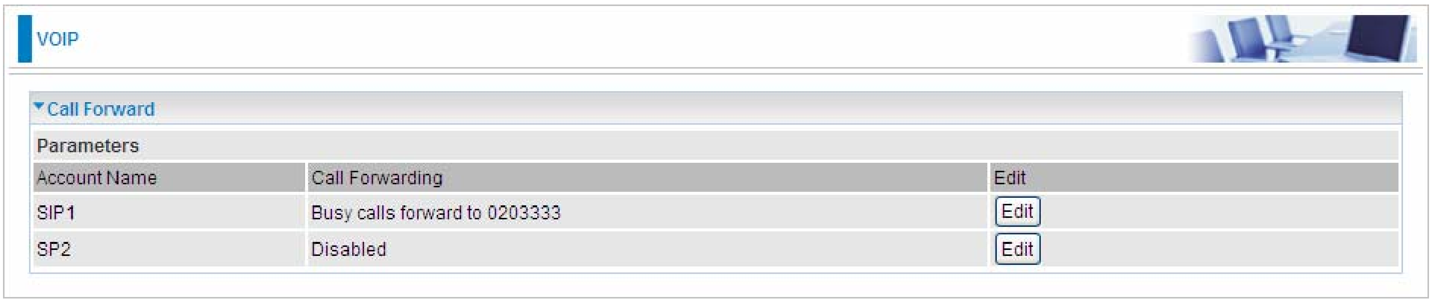
Parameters

Account Name	SIP1
Call Forwarding	Disable

Call Forwarding:

- **All calls forward to:** Set the call number to receive all the incoming calls unconditionally.
- **Busy calls forward to:** Set the call number to receive only busy calls.
- **No Answer calls forward to:** Set the call number to receive calls that are not answered.

Click **Apply** to save your settings.



VOIP

▾Call Forward

Parameters

Account Name	Call Forwarding	Edit
SIP1	Busy calls forward to 0203333	Edit
SP2	Disabled	Edit

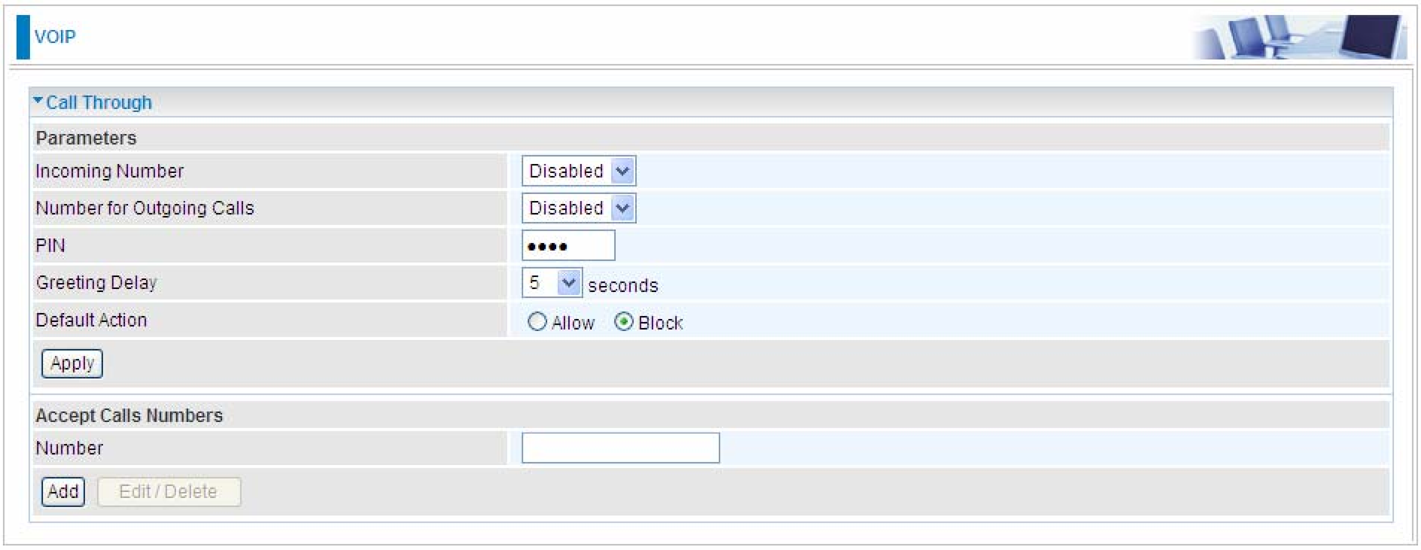
(Busy calls forwarded to 0203333)

Call Through

With the “Call Through” function, you can configure your 7800VDP(O)X so that certain calls are forwarded to any destination number using a cheaper telephone connection, for example via landline or mobile network, this can save costs.

Example: You are on the road and would like to use your mobile telephone to call somebody abroad. You can either call that person directly, or you can call your 7800VDP(O)X at home and let the 7800VDP(O)X forward to the extension abroad via the Internet or less-expensive landline connection at a much less expensive rate.

Note: Two call logs can be generated when call through feature is activated in Missed Call Log, and Outgoing Call Log.



VOIP

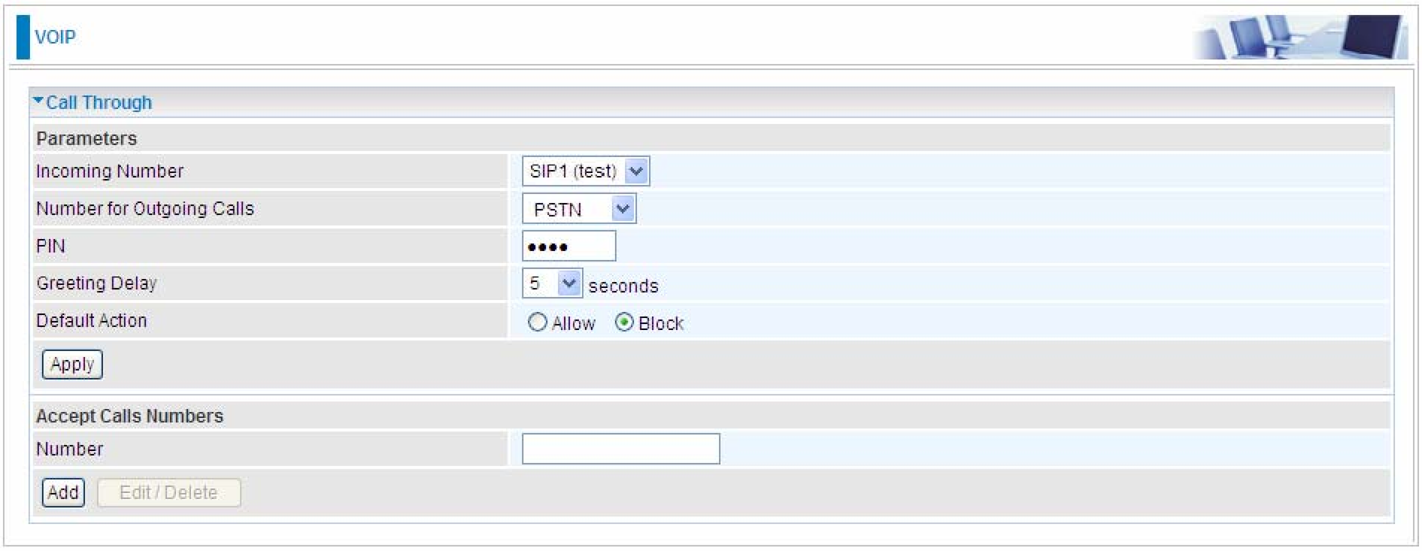
Call Through

Parameters	
Incoming Number	Disabled
Number for Outgoing Calls	Disabled
PIN	••••
Greeting Delay	5 seconds
Default Action	○ Allow ● Block

Apply

Accept Calls Numbers	
Number	

Add Edit / Delete



VOIP

Call Through

Parameters	
Incoming Number	SIP1 (test)
Number for Outgoing Calls	PSTN
PIN	••••
Greeting Delay	5 seconds
Default Action	○ Allow ● Block

Apply

Accept Calls Numbers	
Number	

Add Edit / Delete

Parameters

Incoming Number: Select a number (SIP account or PSTN) for which you wish to enable the Call Through feature.

Number for Outgoing Calls: Select a number (SIP account or PSTN) to be used to forward the call to the destination.

PIN: A four-digit password for forwarding calls. Default is 1234. It has to be input before user input the destination call number.

Greeting Delay: Greeting delay specifies how long the call through feature will be activated after caller calls the incoming number.

Default Action: To define call through feature access authority to certain numbers.

- **Allow:** The list of numbers in “Accept Call Numbers” are authorized to use call through feature.
- **Block:** The list of numbers in “Accept Call Numbers” are blocked from call through feature use.

If only certain callers should be allowed to use the call through function, user can enter these telephone numbers with the corresponding area code on “Accept Calls Numbers”.

Apply: Press **Apply** button to save the call through settings.

Accept Call Numbers:

Number: Add numbers to the “Accept Call Numbers” list. If the default action is “Allow”, these numbers are to activate call through feature. User can set a list of up to 8 call numbers.

Note: 1. Call through and call forward can’t be used at the same time.

2. "Accept Call Number" is only checked with the SIP call.

3. These 2 conditions must be met before Call Through take effect –

1). The incoming call must be from the specified "Incoming Number" side.

2). The calling party must be same as the "Accept Call Number" if default action is “allow”. Or if default action is “block”, the caller cannot be in the “Accept Call Number”. Empty "Accept Call Number" means any calling party.

How to use call through feature:

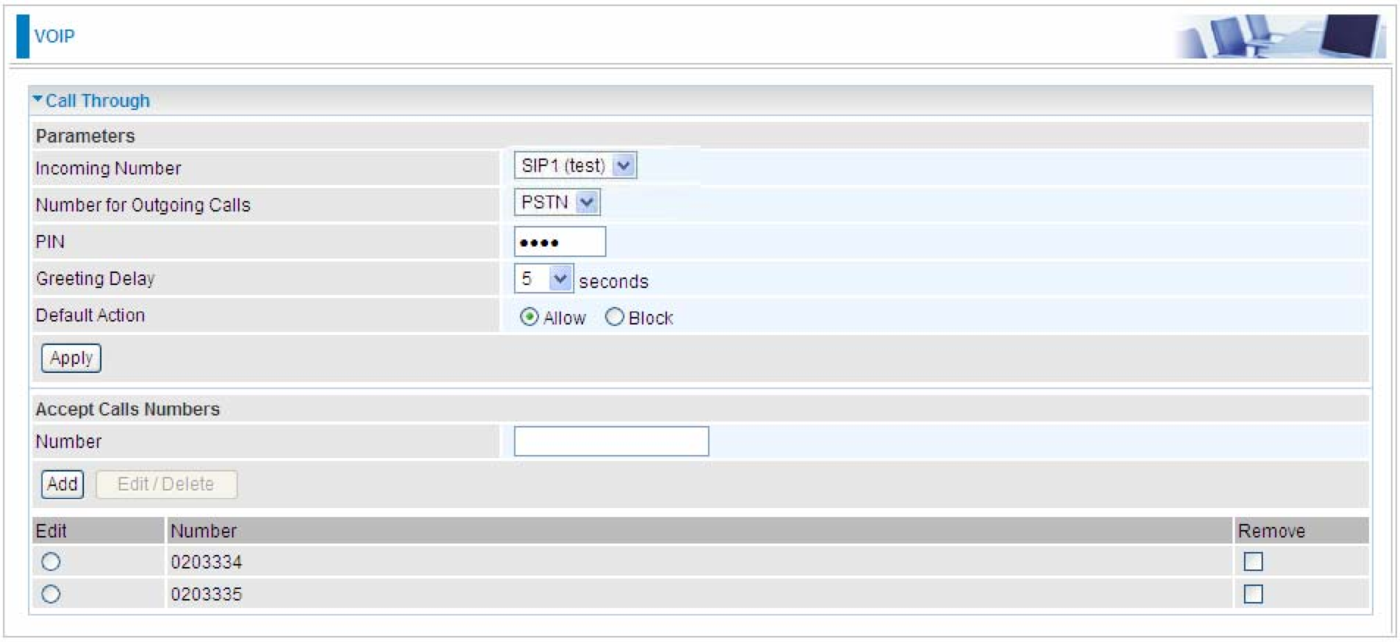
We have a valid triggering list including number “0203334” and “0203335”(Default action is allow, Greeting delay set to 5 seconds). Only “0203334” and “0203335” can use the call through feature.

1.”Incoming Number” is SIP1. The caller (0203334) makes a call to SIP1 to enable call through feature. The caller can hear a “beep” hint tone after 5 seconds indicating Call Through feature is triggered. Caller types PIN code with a “#” to end this PIN input operation (PIN + #).

2. Another “beep” hint tone is coming to imply caller can input the favorable destination call number, also with a “#” to complete your current operation.

3. When you hear the ring-back tone, the call is dialed out to the desired destination via the number specified in “Number for outgoing calls” field, please be waiting.

Note: When the “Incoming Number” is PSTN, hint tone is not available. Please just follow the correct operation but forget the hind tone.



VOIP

Call Through

Parameters

Incoming Number	SIP1 (test)
Number for Outgoing Calls	PSTN
PIN	••••
Greeting Delay	5 seconds
Default Action	● Allow ○ Block

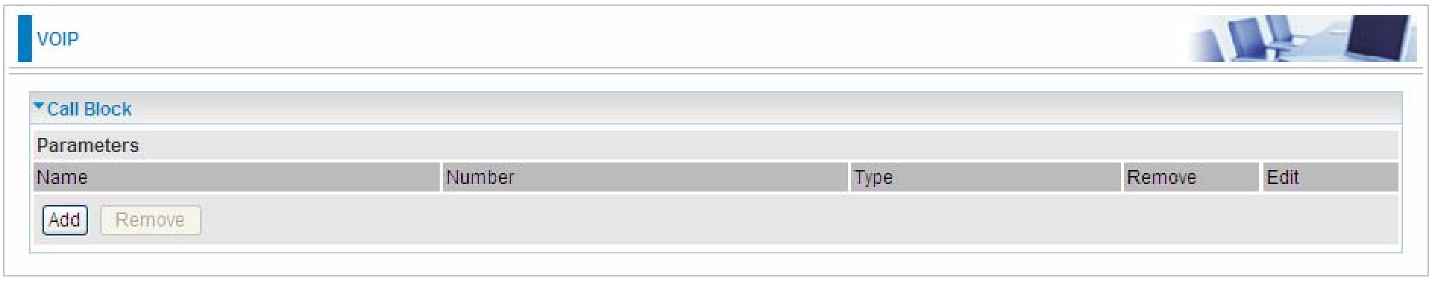
Accept Calls Numbers

Number	

Edit	Number	Remove
○	0203334	□
○	0203335	□

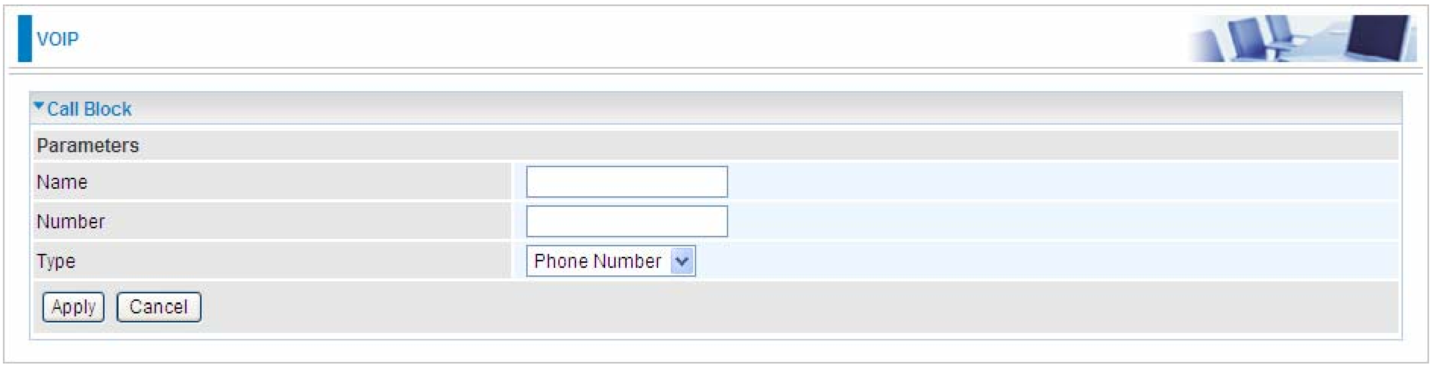
Call Block

Call block is for user to pre-set the unfavorable call numbers that user does not want to come in, resembling the call blacklist.



Name	Number	Type	Remove	Edit

Click **Add** to add the unfavorable call numbers to the list.



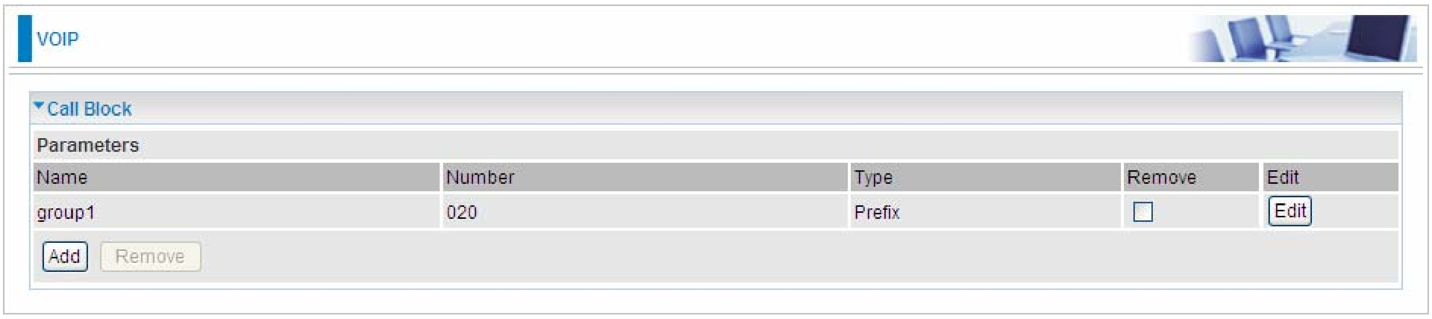
Name	
Number	
Type	Phone Number

Name: The identification for the call number(s).

Number: Type the number, depending on the selected "Type" below. If "Phone Number" is selected, please input the complete phone number; while if "Prefix" is selected, please input the prefix number featuring a group of unfavorable call numbers.

Type: Phone Number and Prefix.

Click **Apply** to save the call blacklist.

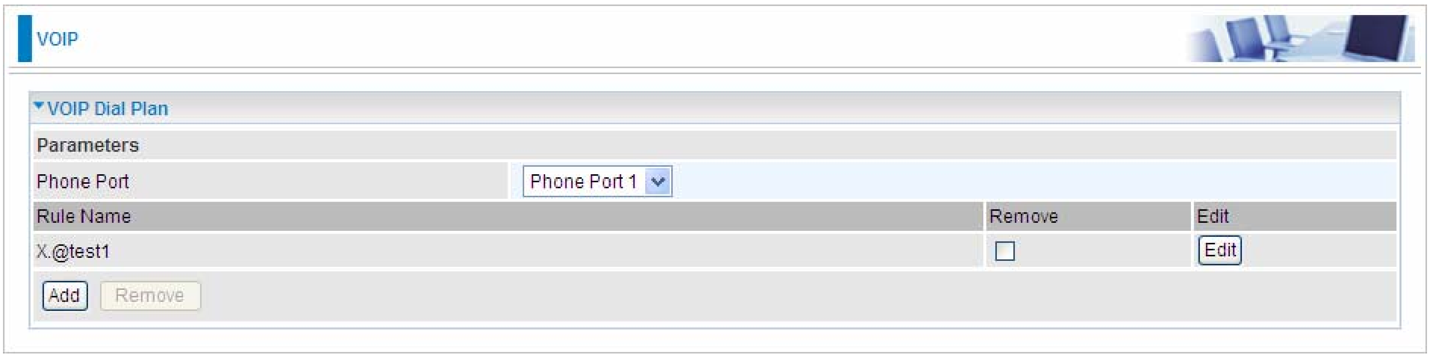


Name	Number	Type	Remove	Edit
group1	020	Prefix	□	Edit

(Group1 calls all banned)

VOIP Dial Plan

This section helps you to make a number dial via VoIP. You no longer need to memorize a long dial string or number for making a VoIP call. Go to Configuration > VOIP > VOIP Dial Plan.



VOIP Dial Plan

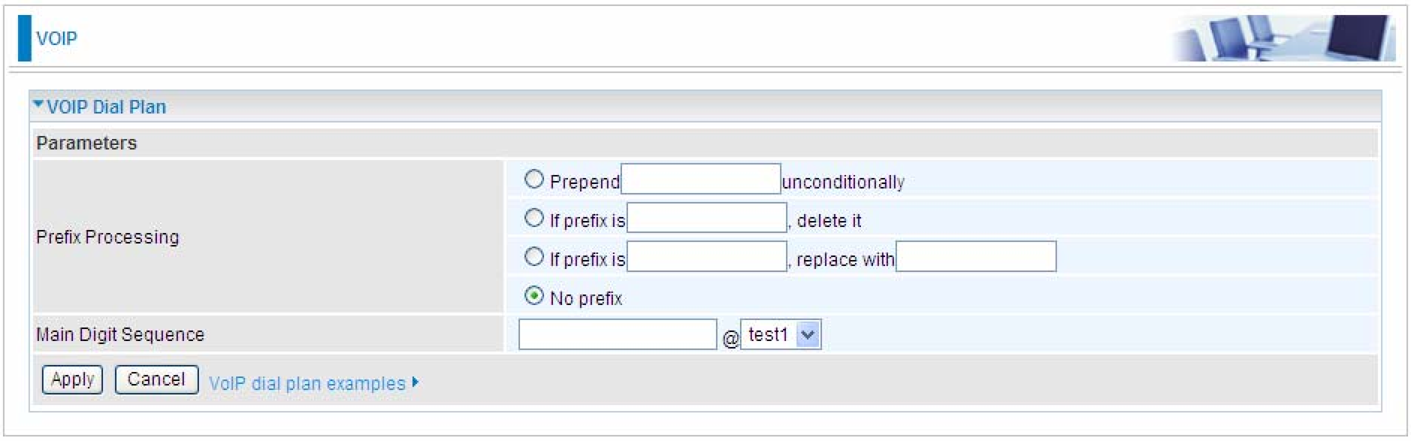
Parameters

Phone Port: Phone Port 1

Rule Name	Remove	Edit
X.@test1	□	Edit

Phone Port: Set the phone the VoIP dial rule relates to. When phone port is set to Phone Port 1, the rules will apply to phone1.

Click **Add** to create new rules.



VOIP Dial Plan

Parameters

Prefix Processing:
○ Prepend ____ unconditionally
○ If prefix is ____, delete it
○ If prefix is ____, replace with ____
● No prefix

Main Digit Sequence: ____ @ test1

Prefix Processing:

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

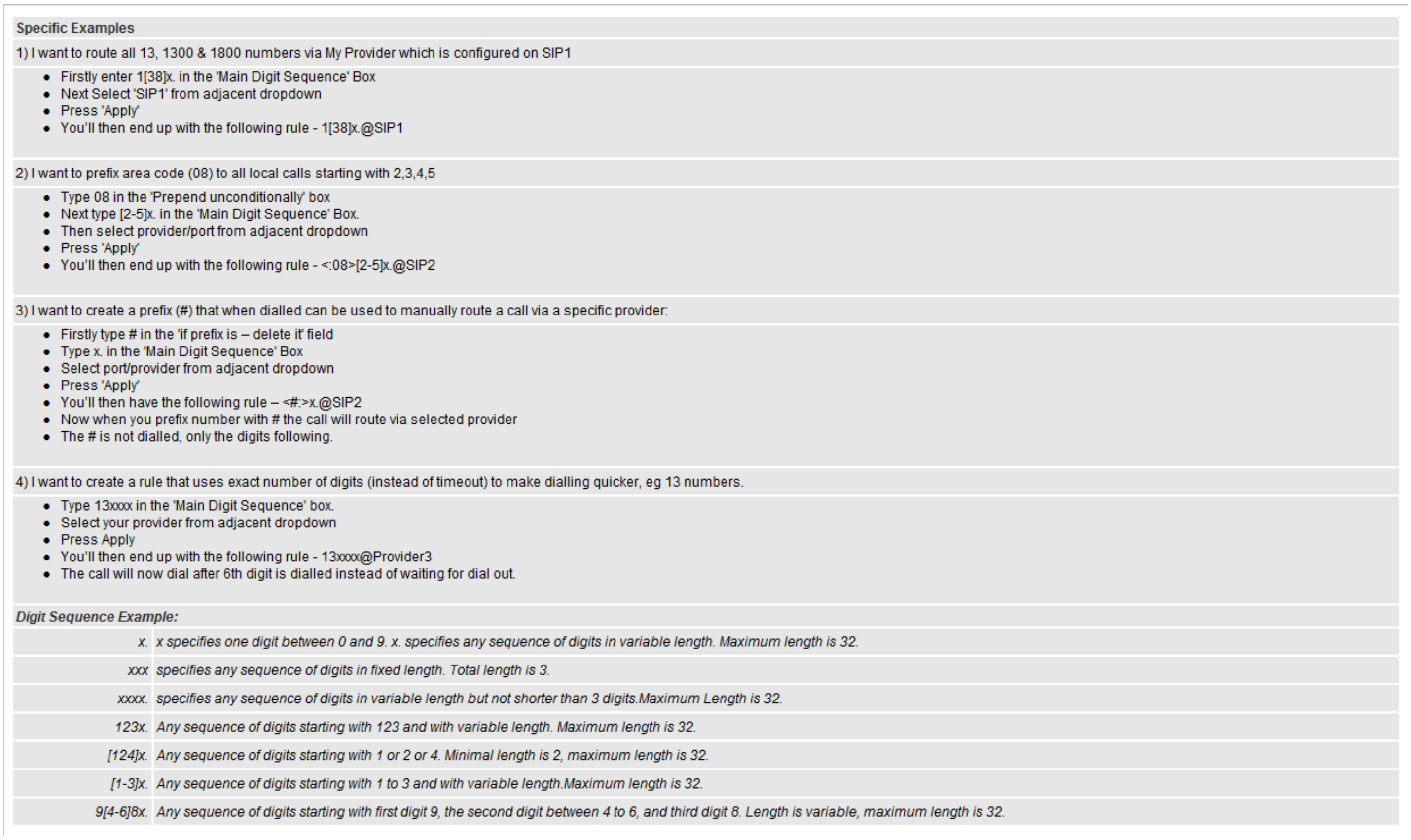
Note: For special service with *, #, you may need to check with your VoIP or Local Telephone Service Provider for information.

- **If Prefix is xxx, delete it:** Prefix xxx is removed from the dialed numbers before making a call.
- **If Prefix is xxx, replace with yyy:** Prefix xxx is replaced with yyy when making a call.
- **No prefix:** No prefix is appended to the front of the dialed numbers. It is set as in default settings.

Main Digit Sequence: The call(s) can be called out via SIP. VoIP dial plan examples ▸ leads users to regular usage for this parameter.

<@ SIPgateway>: This is used for the Intelligent Call Routing feature where you need to set up your **SIP account** on the VoIP User-defined Profiles link on the VoIP Wizard page.

Digit sequence Example	**Description**
x.	x specifies one digit between 0 and 9. x. specifies any sequence of digits in variable length. Maximum length is 32.
xxx	Specifies any sequence of digits in fixed length. Total length is 3.
xxxx.	Specifies any sequence of digits in variable length but not shorter than 4 digits. Maximum Length is 32.
123x.	Any sequence of digits starting with 123 and with variable length. Maximum length is 32.
[124]x.	Any sequence of digits starting with 1 or 2 or 4. Minimal length is 2, maximum length is 32.
[1-3]x.	Any sequence of digits starting with 1 to 3 and with variable length. Maximum length is 32.
9[4-6]8x.	Any sequence of digits starting with first digit 9, the second digit between 4 to 6, and third digit 8. Length is variable, maximum length is 32.



Specific Examples

1) I want to route all 13, 1300 & 1800 numbers via My Provider which is configured on SIP1

- Firstly enter 1[38]x. in the 'Main Digit Sequence' Box
- Next Select 'SIP1' from adjacent dropdown
- Press 'Apply'
- You'll then end up with the following rule - 1[38]x.@SIP1

2) I want to prefix area code (08) to all local calls starting with 2,3,4,5

- Type 08 in the 'Prepend unconditionally' box
- Next type [2-5]x. in the 'Main Digit Sequence' Box.
- Then select provider/port from adjacent dropdown
- Press 'Apply'
- You'll then end up with the following rule - <:08>[2-5]x.@SIP2

3) I want to create a prefix (#) that when dialled can be used to manually route a call via a specific provider:

- Firstly type # in the 'if prefix is – delete it' field
- Type x. in the 'Main Digit Sequence' Box
- Select port/provider from adjacent dropdown
- Press 'Apply'
- You'll then have the following rule – <#:>x.@SIP2
- Now when you prefix number with # the call will route via selected provider
- The # is not dialled, only the digits following.

4) I want to create a rule that uses exact number of digits (instead of timeout) to make dialling quicker, eg 13 numbers.

- Type 13xxxx in the 'Main Digit Sequence' box.
- Select your provider from adjacent dropdown
- Press Apply
- You'll then end up with the following rule - 13xxxx@Provider3
- The call will now dial after 6th digit is dialled instead of waiting for dial out.

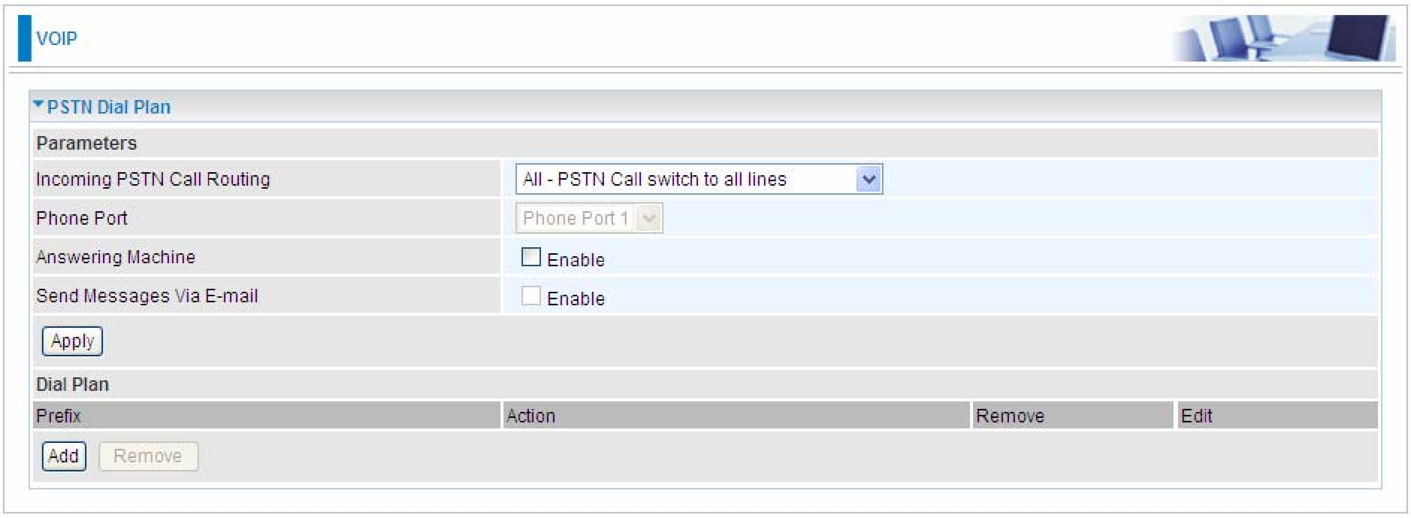
Digit Sequence Example:

x.	*x specifies one digit between 0 and 9. x. specifies any sequence of digits in variable length. Maximum length is 32.*
xxx	*specifies any sequence of digits in fixed length. Total length is 3.*
xxxx.	*specifies any sequence of digits in variable length but not shorter than 3 digits.Maximum Length is 32.*
123x.	*Any sequence of digits starting with 123 and with variable length. Maximum length is 32.*
[124]x.	*Any sequence of digits starting with 1 or 2 or 4. Minimal length is 2, maximum length is 32.*
[1-3]x.	*Any sequence of digits starting with 1 to 3 and with variable length.Maximum length is 32.*
9[4-6]8x.	*Any sequence of digits starting with first digit 9, the second digit between 4 to 6, and third digit 8. Length is variable, maximum length is 32.*

PSTN Dial Plan

PSTN Dial Plan assists in routing calls via PSTN. You can define a range of dial plans to make regular calls from VoIP switch to PSTN line. Prefix numbers are essential in distinguishing between VoIP and Regular phone calls. If actual numbers dialed matches prefix number defined in this dial plan, the dialed number will be routed via PSTN. Otherwise, the number will be routed via VoIP network.

Note: A maximum of 12 rules for the PSTN dial plan.



VOIP

PSTN Dial Plan

Parameters

Incoming PSTN Call Routing	All - PSTN Call switch to all lines
Phone Port	Phone Port 1
Answering Machine	□ Enable
Send Messages Via E-mail	□ Enable

Apply

Dial Plan

Prefix	Action	Remove	Edit

Add Remove

Parameters

Incoming PSTN Call Routing: Measures to deal with incoming PSTN calls.

- **Auto:** Change the incoming call to another idle line, for example, if Phone 1 is busy, then the incoming call would be switched to Phone port 2.
- **Line:** If a PSTN call rings on phone 1, and when Phone 1 is busy, there will be a warning of the incoming call.
- **All:** Both Phone1 and Phone2 ring when a PSTN call is received.

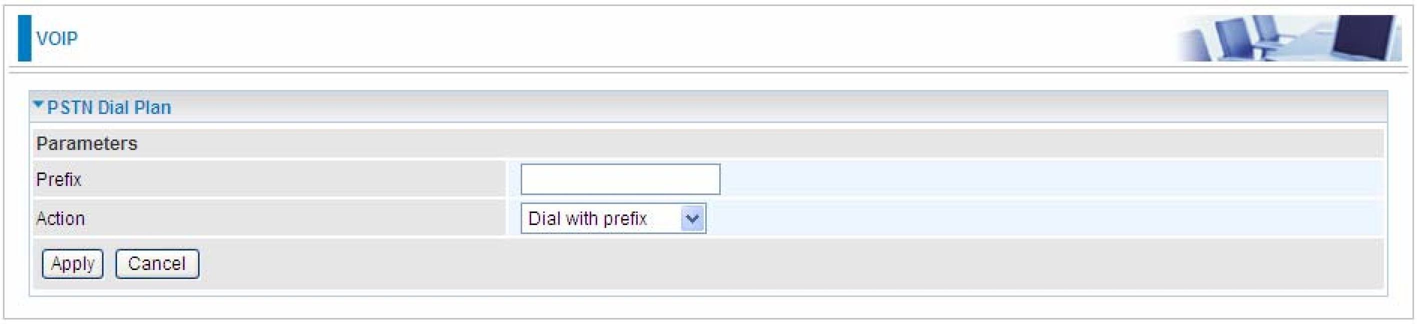
Phone Port: Decide which phone the incoming PSTN call routing applies to.

Answering Machine: Enable to activate the answering machine feature for PSTN so that user can record and listen to the messages of this phone.

Send Message Via E-mail: Enable to send message left by callers via e-mail to the user.

Dial Plan

Click **Add** to add new rules.



VOIP

PSTN Dial Plan

Parameters

Prefix	
Action	Dial with prefix

Apply Cancel

Prefix: Specify number(S) marking as the tag for switching to a PSTN call.

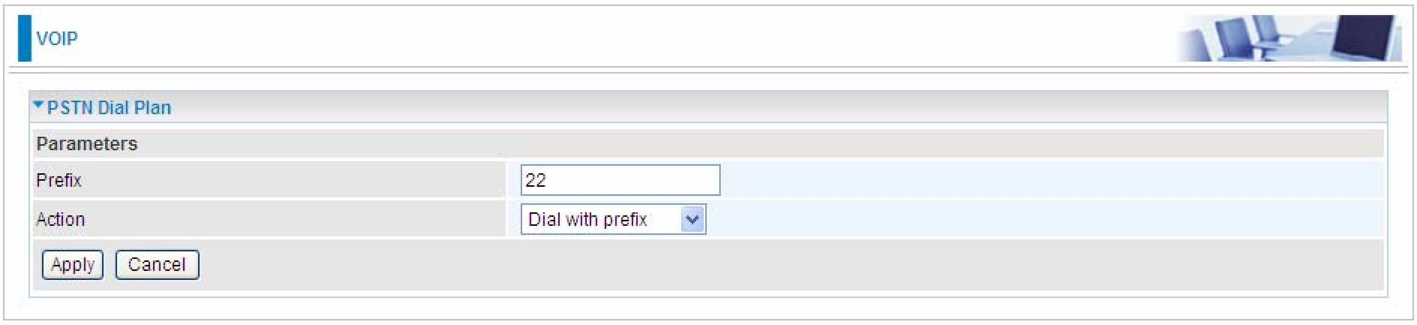
Action: The dialing mechanism.

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

Note: The x. wildcard character is supported here by PSTN dial plan. x specifies one digit between 0 and 9. x. specifies any sequence of variable length, the maximum length is 32.

Examples of PSTN dial plan:

1. Dial with Prefix

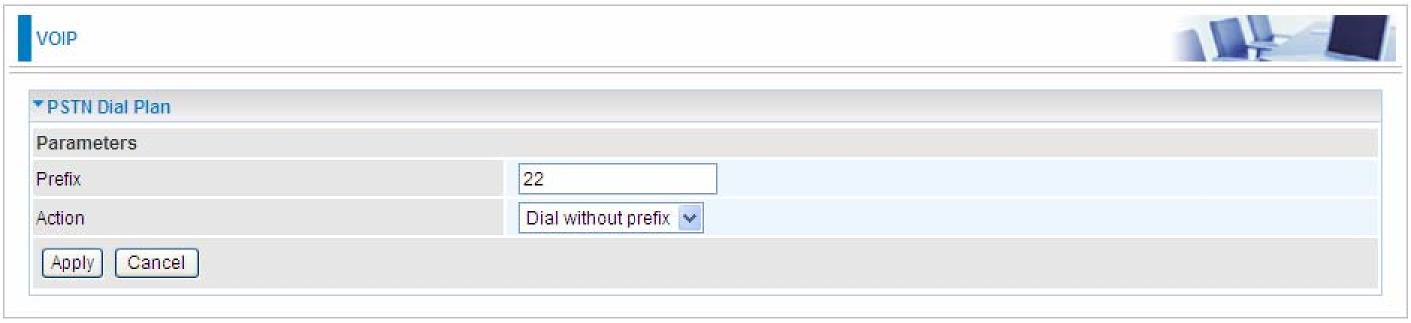


Parameters

Prefix	22
Action	Dial with prefix

If you dial 2250505, number 2250505 will be dialed out via FXO to make a regular phone call.

2. Dial without Prefix

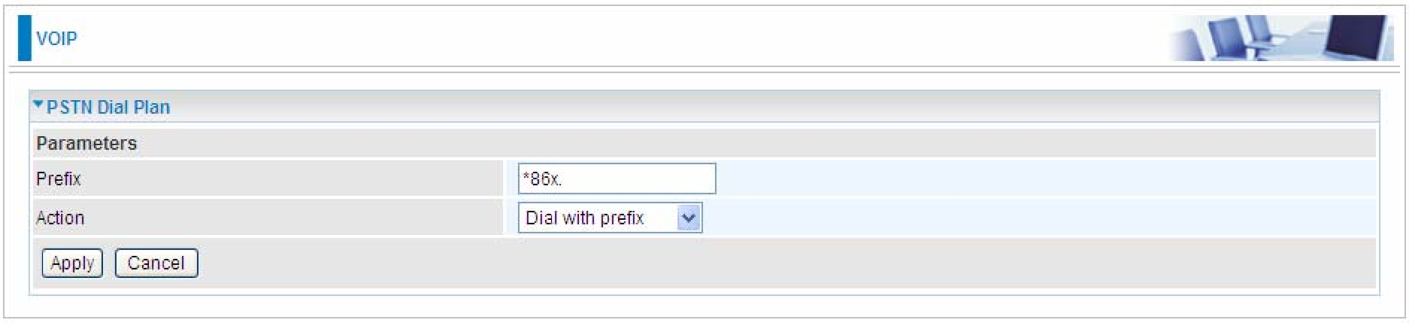


Parameters

Prefix	22
Action	Dial without prefix

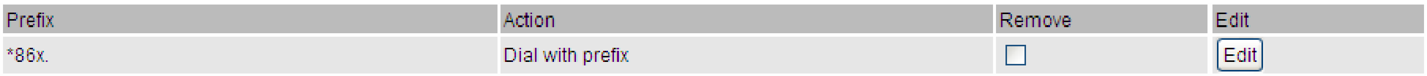
In this example, if user wants to dial out 50505(the destination extension number), please first dial 22 and it will get the PSTN dial tone from CO site and then dial 50505 to make a regular phone call.

3. With x wildcard character.



Parameters

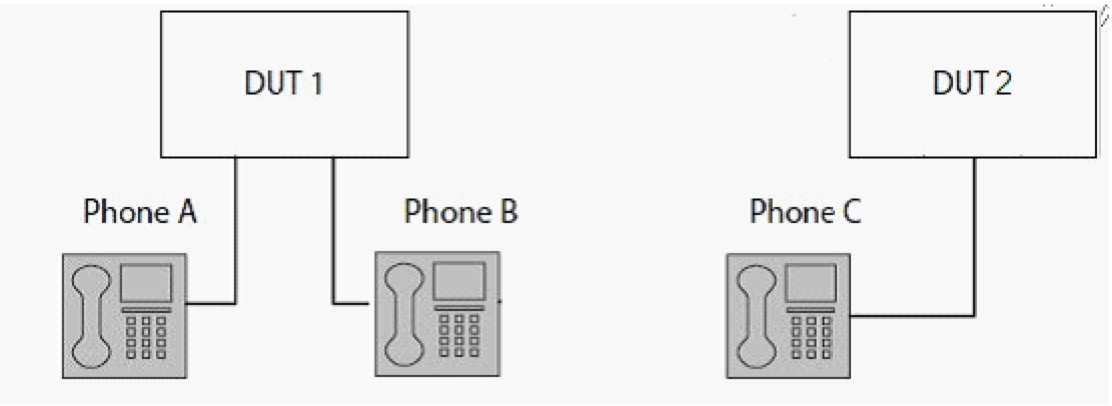
Prefix	*86x.
Action	Dial with prefix



Prefix	Action	Remove	Edit
*86x.	Dial with prefix	□	Edit

If User wants numbers with prefix *860, *8601, *862, etc all to be dialed out via FXO together with these prefix, and then he could turn to the reference above.

How to establish conference call: 3 –way call scenario



Case 1: Phone A invites Phone C to join a conference call

Step – 1: Phone A presses flash (hold original call), and A hears the dial tone

Step – 2: Phone A calls Phone C. C and A are on a new call.

Step – 3: Phone A presses flash (hold new call) and return to original call

Step – 4: Phone A tells Phone B that he wants to set up a conference with Phone C.

Step – 5: Phone A presses flash again to merge all 3 calls

Case 2: Phone C dials in and wants to join Phone A and Phone B's conference

Step – 1: Phone A and Phone B on a call, then Phone C dials Phone A and A hears a waiting tone

Step – 2: Phone A presses flash and picks up the call waiting call

Step – 3: Phone A presses flash to hold the call with Phone C and return to original call with Phone B

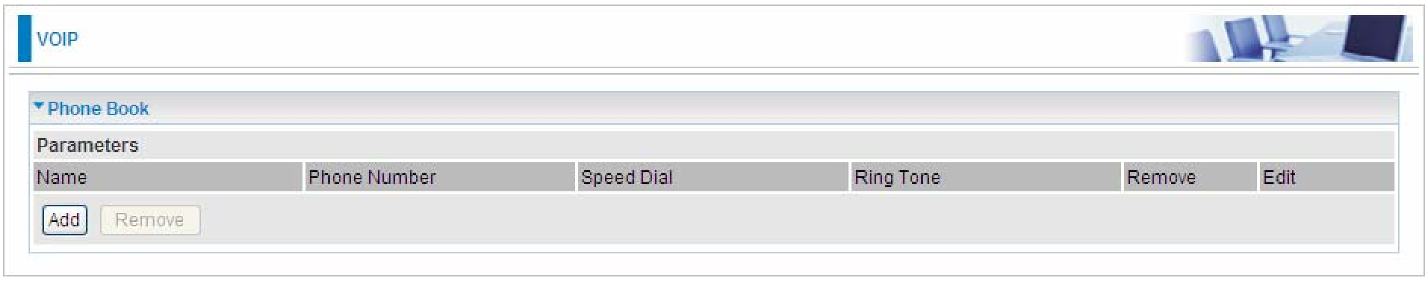
Step – 4: Phone A tells Phone B that he wants to set up a conference with Phone C.

Step – 5: Phone A presses flash again to merge all 3 calls.

Phone Book

Phone Book / Speed Dial comes at hand to store frequently used telephone number(s) that you can press **1xx instead of the exact dialing-out number on the phone keyboard to make a quick dialing. For example, if the destination number 5522772 is mapped to a speed-dial number of **105, and then user can easily press **105 on the phone keyboard, you will be delivered to the destination of 5532772, call established.

Note: xx, please remember only two digits (0-9) allowed to identify the phone number.

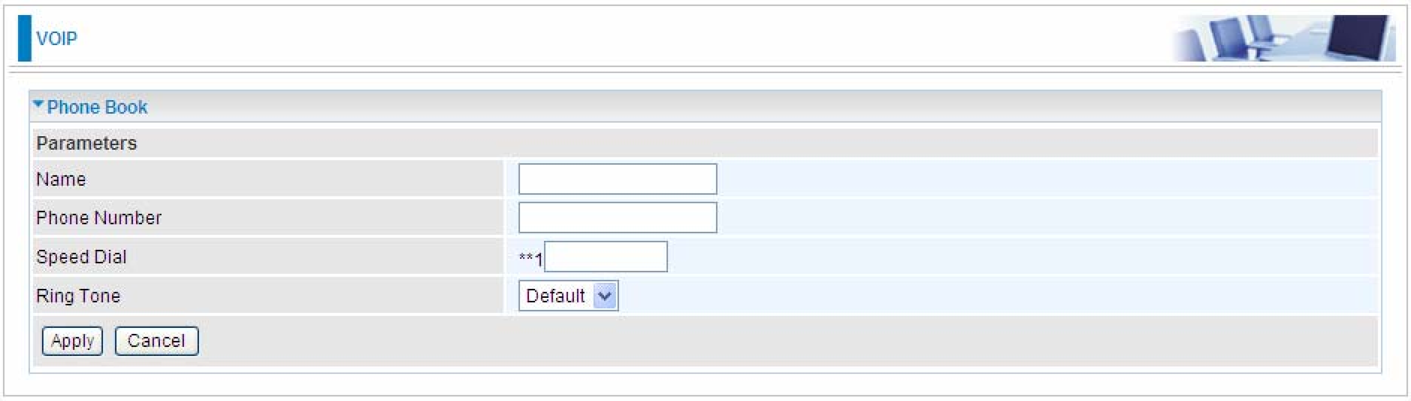


VOIP

Phone Book

Parameters

Name	Phone Number	Speed Dial	Ring Tone	Remove	Edit



VOIP

Phone Book

Parameters

Name	
Phone Number	
Speed Dial	**1
Ring Tone	Default

Name: User-defined identification.

Phone Number: The full destination phone number user wants to be simplified to a speed-dial number.

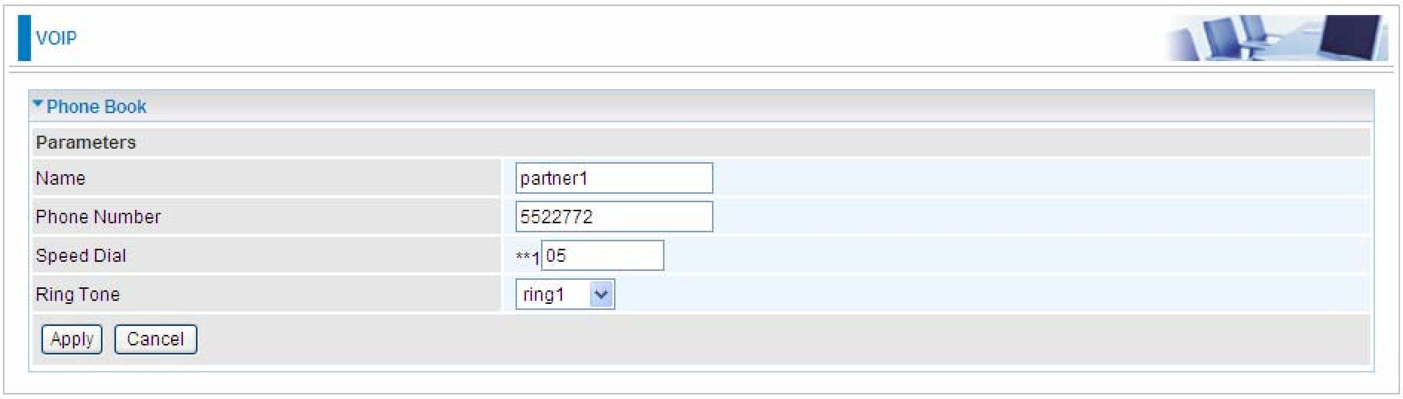
Speed Dial: Set the speed-dial number for the destination number.

Ring Tone: Support up to 5 different ring tones for the default ring tone. User also can set the different ring tone by the calling party. If the calling party is not defined, the ring tone is the default one.

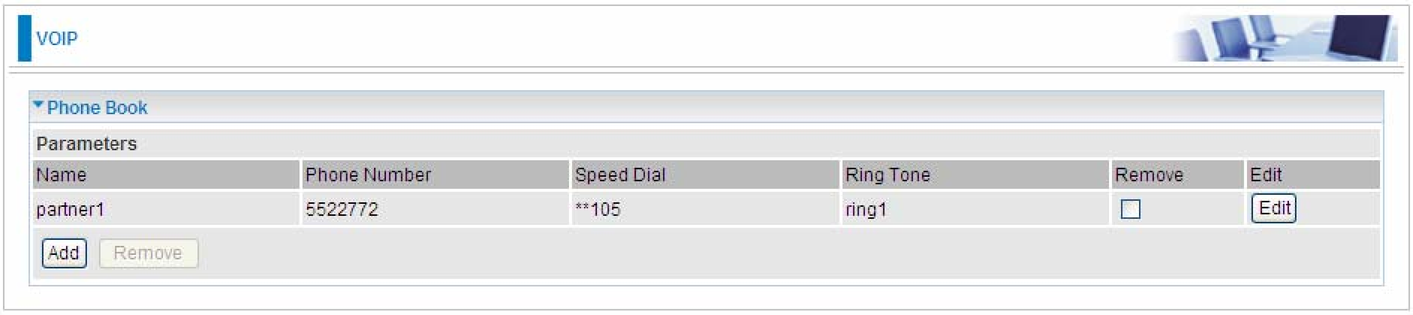
Simple example:

A user wants to simplify a frequently used phone number to an easy and friendly number for a quick dialing, and then speed dial is a good choice for him.

For example, the frequently used phone number is 5522772, and mapped to **105, then he can only dial out **105 to make the call.



Parameters	
Name	partner1
Phone Number	5522772
Speed Dial	**1 05
Ring Tone	ring1



Name	Phone Number	Speed Dial	Ring Tone	Remove	Edit
partner1	5522772	**105	ring1	□	Edit

VPN

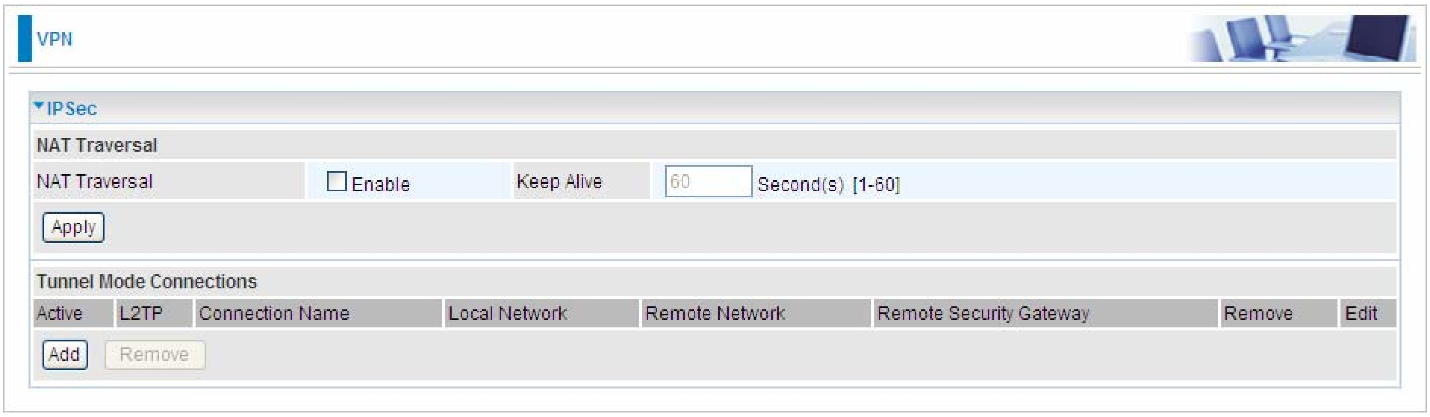
A **virtual private network** (**VPN**) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

IPSec

Internet Protocol Security (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

Note: A maximum of 16 sessions for IPSec.



VPN

▾IPSec

NAT Traversal

NAT Traversal	□ Enable	Keep Alive	60 Second(s) [1-60]

Tunnel Mode Connections

Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit

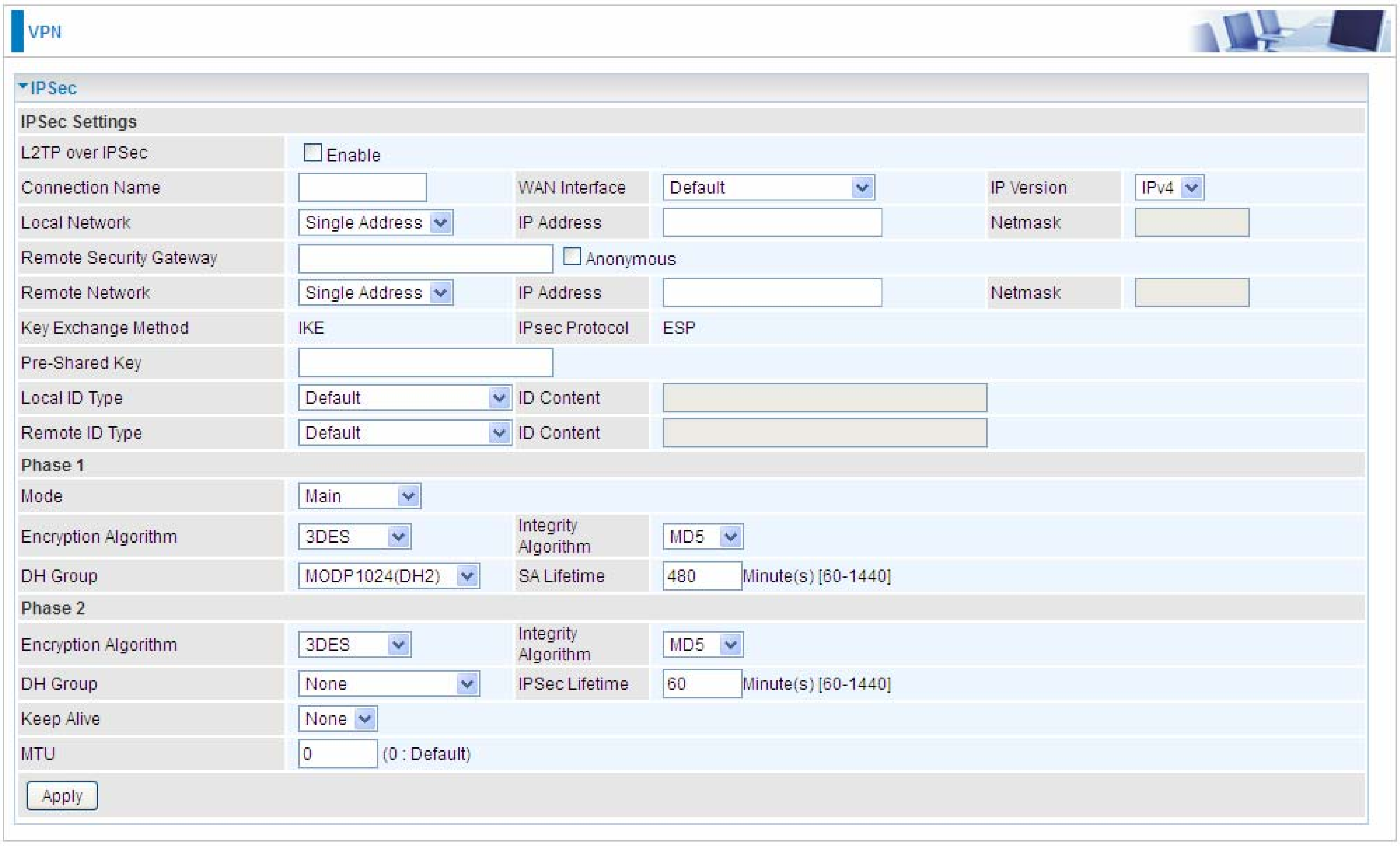
NAT Traversal

NAT Traversal: This directive enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

Keep Alive: Type the interval time(sec) for sending packets to keep the NAT Traversal alive.

Click **Apply** to save and apply your settings.

Click **Add** to create IPSec connections.



VPN

IPSec

IPSec Settings					
L2TP over IPSec	□ Enable				
Connection Name		WAN Interface	Default	IP Version	IPv4
Local Network	Single Address	IP Address		Netmask	
Remote Security Gateway		□ Anonymous			
Remote Network	Single Address	IP Address		Netmask	
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key					
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	None				
MTU	0 (0 : Default)				

IPSec Settings

L2TP over IPSec: Select Enable if user wants to use L2TP over IPSec. See L2TPover IPSec

Connection Name: A given name for the connection, but it should contain no spaces (e.g. “connection-to-office”).

WAN Interface: Select the set used interface for the IPSec connection, when you select adsl pppoe_0_0_35/ppp0.1 interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

IP Version: Select the IP version base on your network framework.

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

- **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

IP Address: The local network address.

Netmask: The local network netmask.

Remote Secure Gateway: The IP address of the remote VPN device that is connected and establishes a VPN tunnel.

Anonymous: Enable any IP to connect in.

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

- **Single Address:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

Key Exchange Method: Displays key exchange method.

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

Local ID Type and **Remote ID Type:** When the mode of phase 1 is aggressive, Local and Remote peers can be identified by other IDs.

ID content: Enter ID content the name you want to identify when the Local and Remote Type are Domain Name; Enter ID content IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

Phase 1

Mode: Select IKE mode from the drop-down menu: ***Main*** or ***Aggressive***. This IKE provides secured key generation and key management.

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

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

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). 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.

DH 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). MODP stands for Modular Exponentiation Groups.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. Enter a value to issue an initial connection request for a new VPN tunnel. Default is 480 minutes (28800 seconds). A short SA time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

Phase 2

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

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

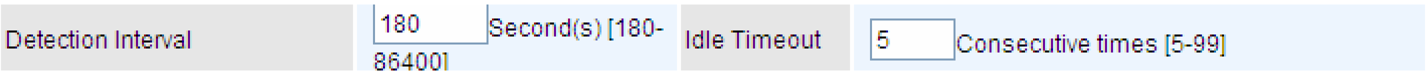
DH Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Ping for Keep Alive: Select the operation methods:

- **None:** The default setting is “None”. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.

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

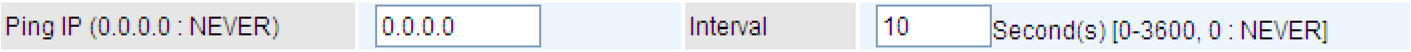


Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5	Consecutive times [5-99]

Detection Interval: The period cycle for dead peer detection. The interval can be 180~86400 seconds.

Idle Timeout: Auto-disconnect the IPSec connection after trying several consecutive times.

- **Ping:** This mode will detect whether the remote IPSec peer has lost or not by pinging specify IP address.



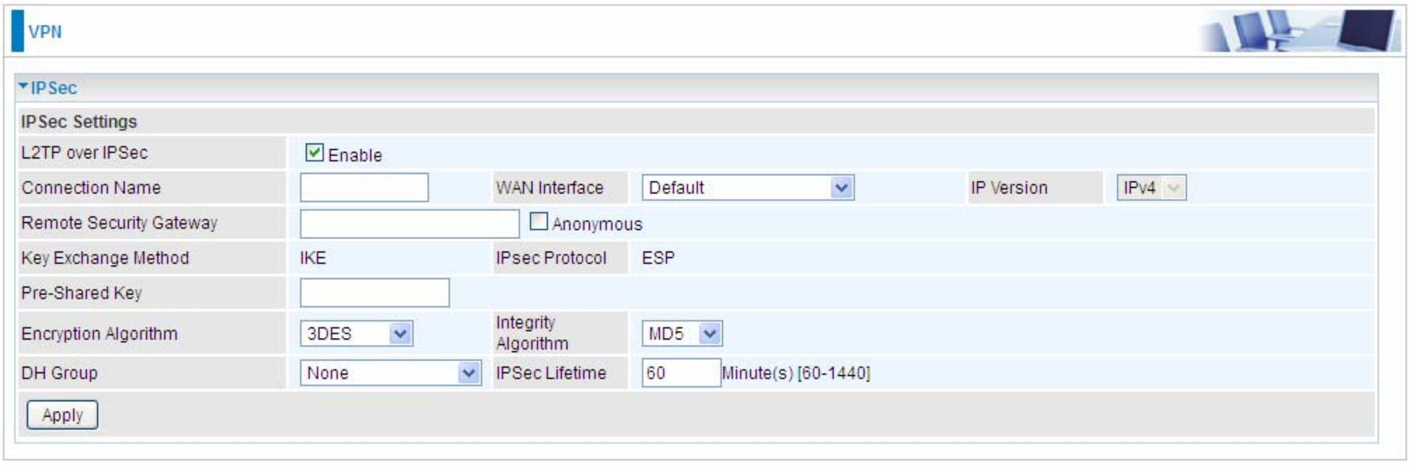
Ping IP (0.0.0.0 : NEVER)	0.0.0.0	Interval	10	Second(s) [0-3600, 0 : NEVER]

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

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

MTU: Maximum Transmission Unit, maximum value is 1500.

IPSec for L2TP



VPN

▾IPSec

IPSec Settings

L2TP over IPSec	☑ Enable				
Connection Name		WAN Interface	Default	IP Version	IPv4
Remote Security Gateway	□ Anonymous				
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key					
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		

Apply

Connection Name: A given name for the connection, but it should contain no spaces (e.g. “connection-to-office”).

WAN Interface: Select the set interface for the IPSec tunnel.

Remote Security Gateway: Input the IP of remote security gateway.

Key Exchange Method: Displays key exchange method.

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

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

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

Integrity Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmit. There are 2 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

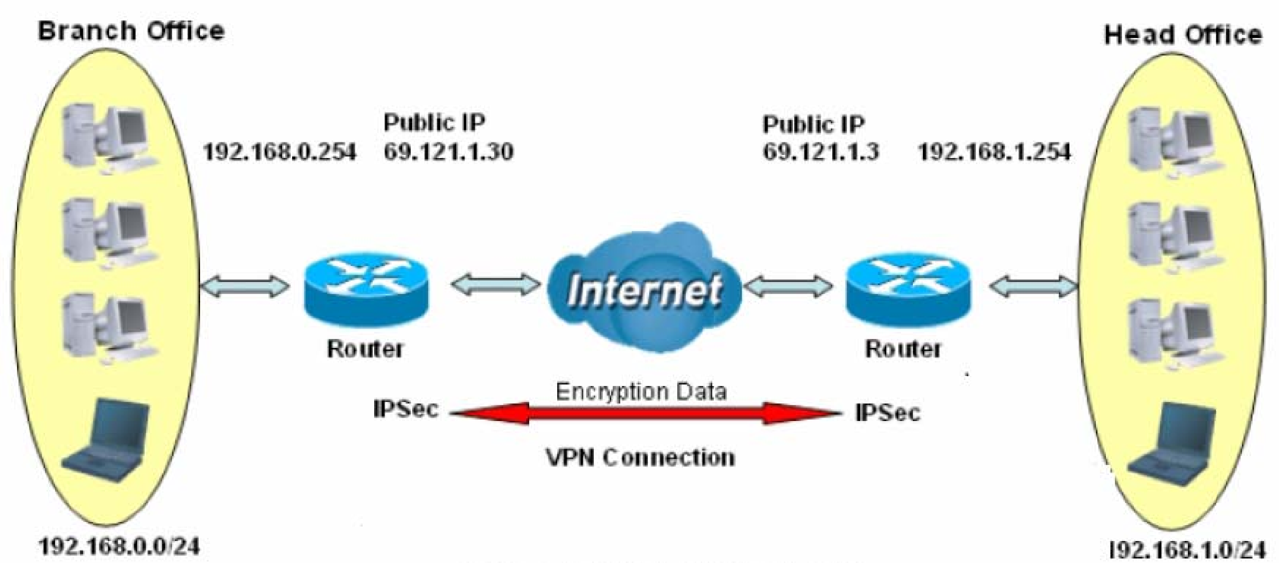
- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

DH 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). MODP stands for Modular Exponentiation Groups.

IPSec Lifetime: Specify the number of minutes that IPSec will stay active before new encryption and authentication key will be exchanged. Enter a value to negotiate and establish secure authentication. Default is 60 minutes (3600 seconds). A short time increases security by forcing the two parties to update the keys. However, every time when the VPN tunnel re- negotiates, access through the tunnel will be temporarily disconnected.

Examples:

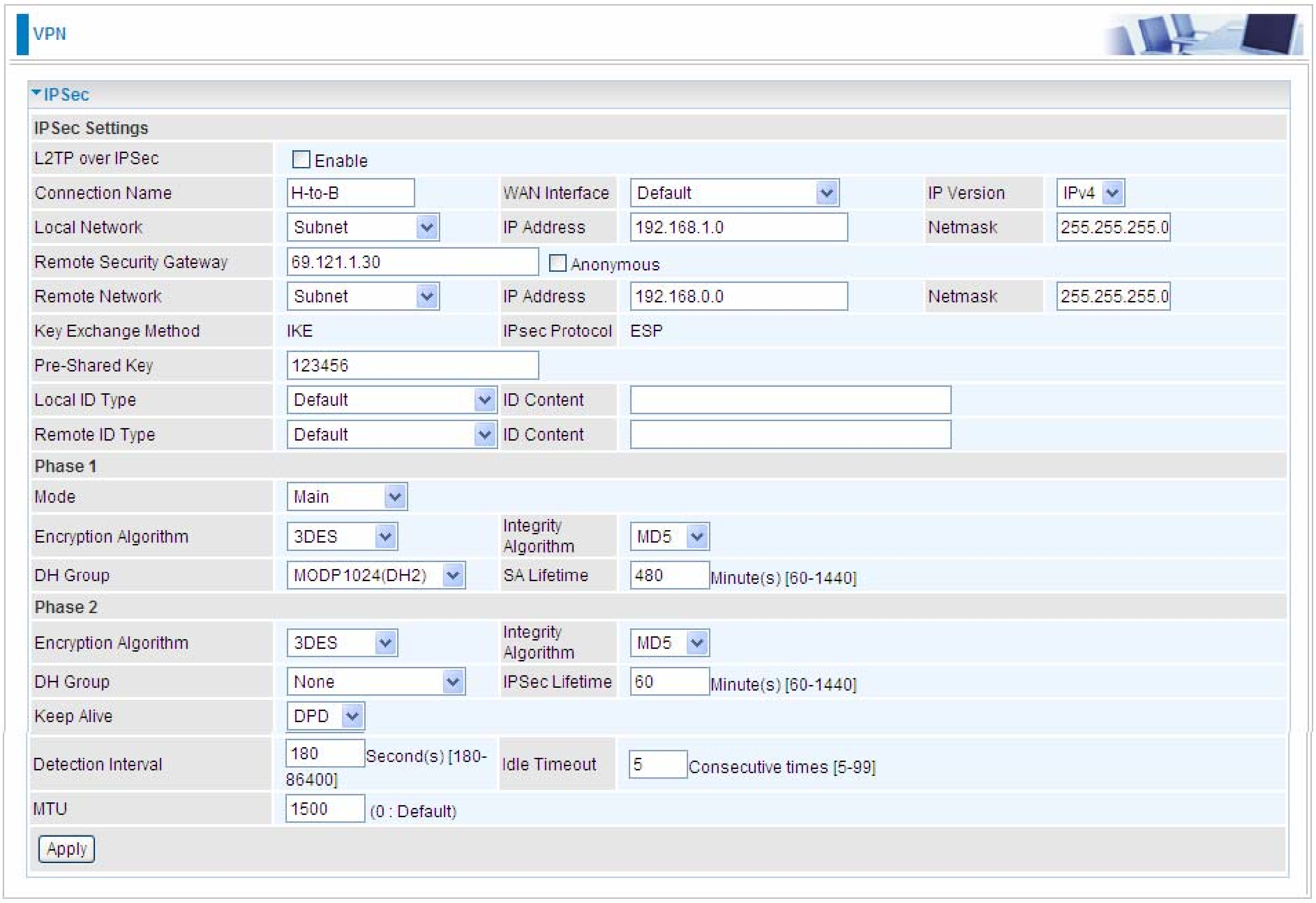
1. **LAN-to-LAN connection**
Two BiPAC 7800VDOXs want to setup a secure IPSec VPN tunnel
Note: The IPSec Settings shall be consistent between the two routers.



IPSec VPN-LAN to LAN

Head Office Side:
Setup details:

Item	Function		Description
1	Connection Name	H-to-B	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Secure Gateway Address(Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Subnet		Select Subnet
	IP Address	192.168.0.0	Branch office network
	Netmask	255.255.255.0	
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	

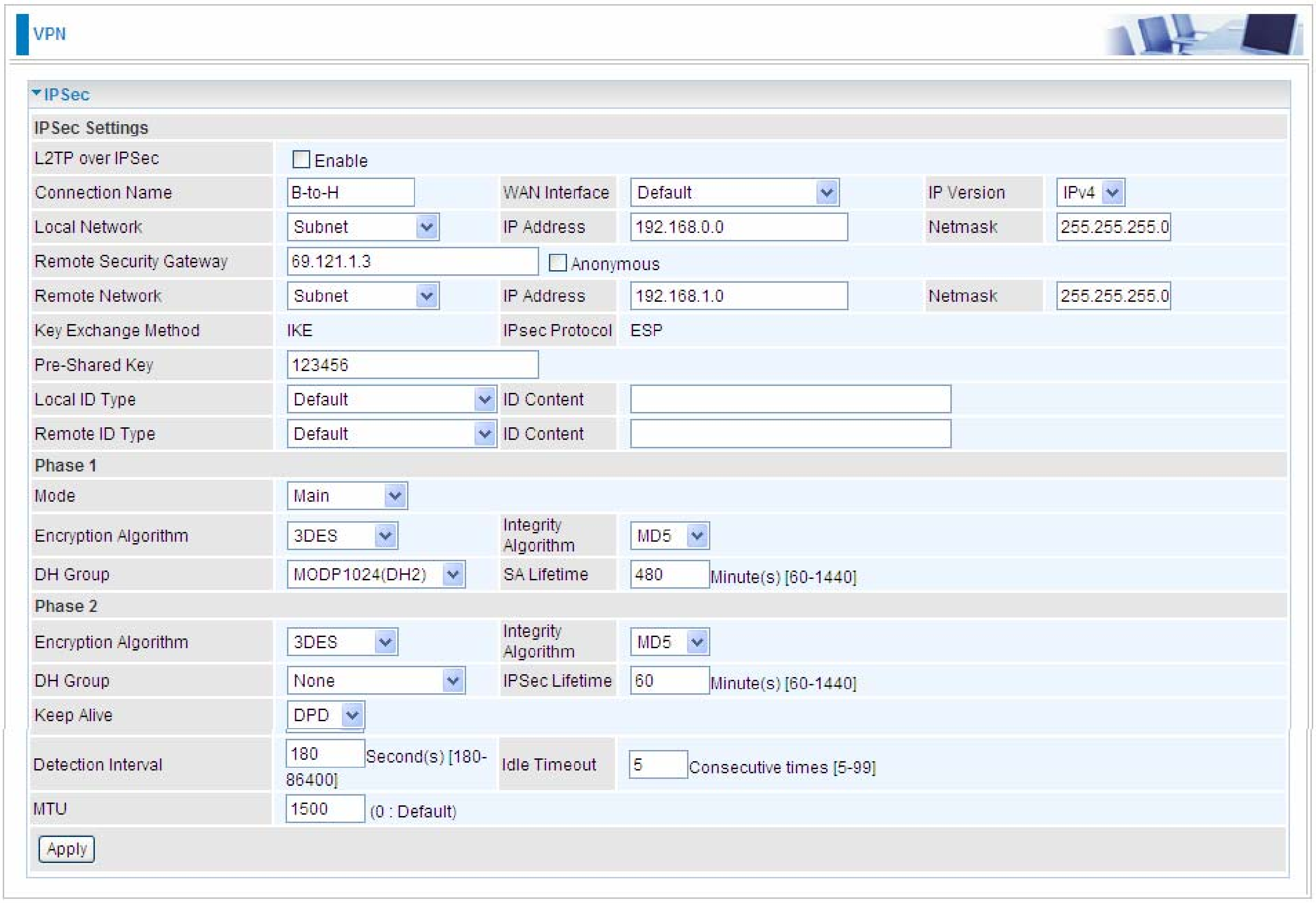


IPSec Settings

L2TP over IPSec	□ Enable				
Connection Name	H-to-B	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30 □ Anonymous				
Remote Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD				
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]		
MTU	1500 (0 : Default)				

Branch Office Side:
Setup details: the same operation as done in Head Office side

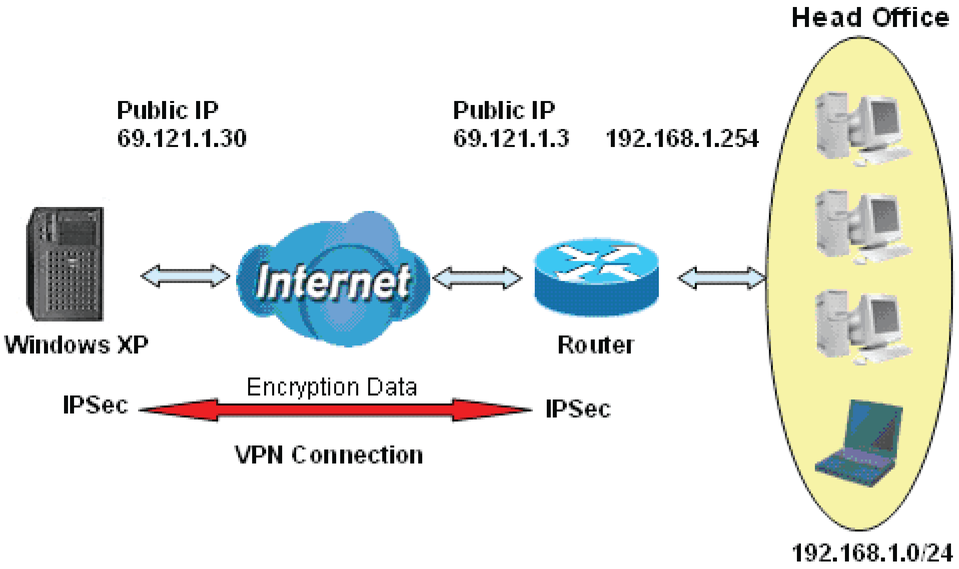
Item	Function		Description
1	Connection Name	B-to-H	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.0.0	Branch Office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway Address(Hostanme)	69.121.1.3	IP address of the Head office router (on WAN side)
4	Remote Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head office network
	Netmask	255.255.255.0	
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



IPSec Settings

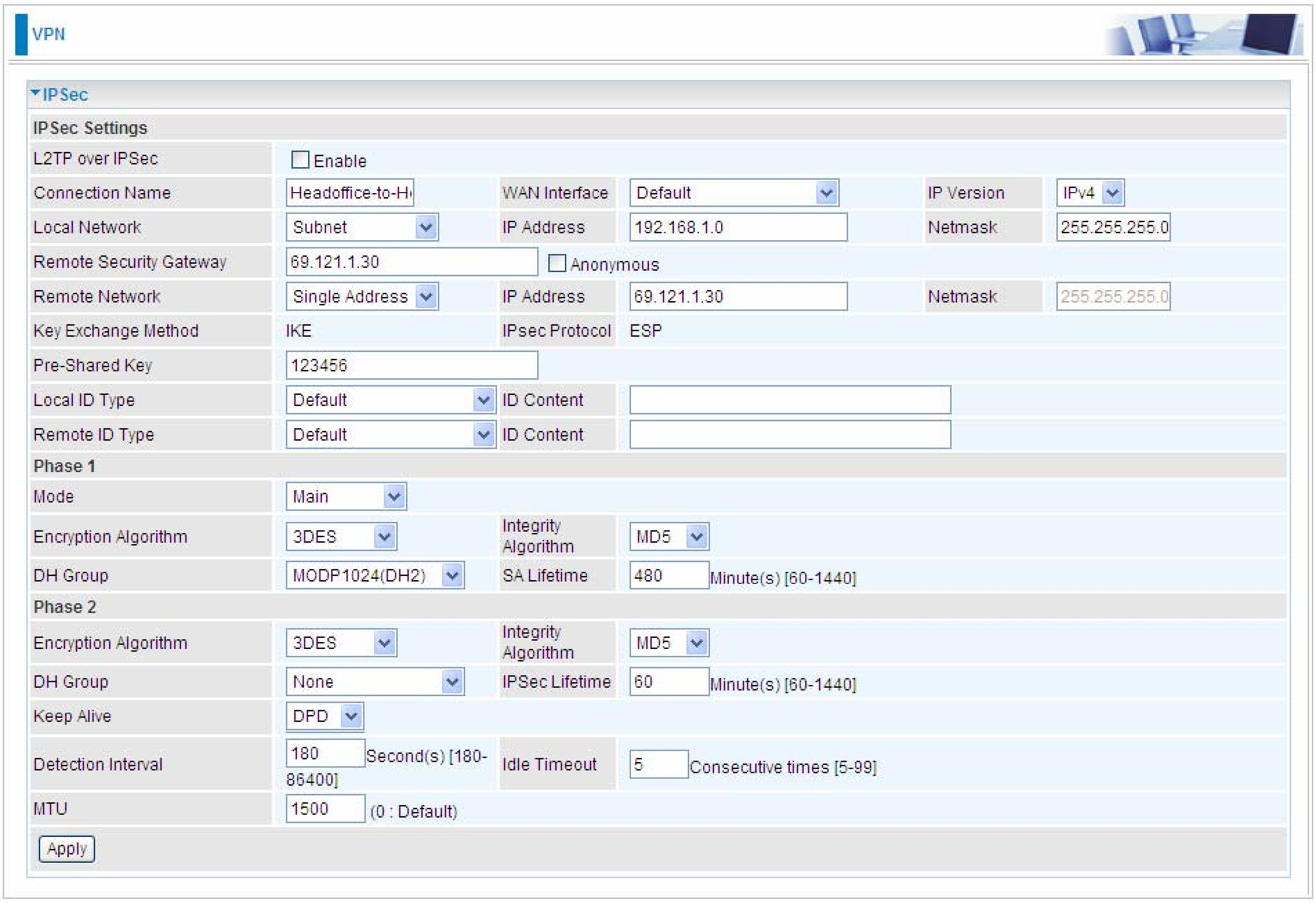
L2TP over IPSec	□ Enable				
Connection Name	B-to-H	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.0.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.3 □ Anonymous				
Remote Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			
Phase 1					
Mode	Main				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]		
Phase 2					
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]		
Keep Alive	DPD				
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]		
MTU	1500 (0 : Default)				

2. Host to LAN
Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



IPSec VPN-Host to LAN

Item	Function		Description
1	Connection Name	Headoffice-to-Host	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway (Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Single Address	69.121.1.30	Host
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	



VPN

IPSec

IPSec Settings

L2TP over IPSec	□ Enable				
Connection Name	Headoffice-to-H	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	192.168.1.0	Netmask	255.255.255.0
Remote Security Gateway	69.121.1.30 □ Anonymous				
Remote Network	Single Address	IP Address	69.121.1.30	Netmask	255.255.255.0
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Local ID Type	Default	ID Content			
Remote ID Type	Default	ID Content			

Phase 1

Mode	Main		
Encryption Algorithm	3DES	Integrity Algorithm	MD5
DH Group	MODP1024(DH2)	SA Lifetime	480 Minute(s) [60-1440]

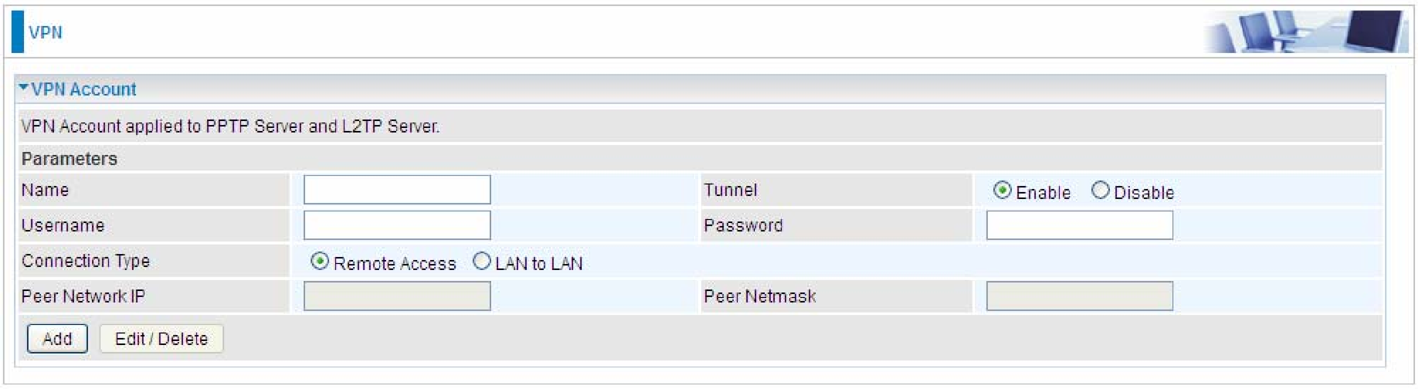
Phase 2

Encryption Algorithm	3DES	Integrity Algorithm	MD5
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]
Keep Alive	DPD		
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]
MTU	1500 (0 : Default)		

Apply

VPN Account

PPTP and L2TP server share the same account database set in VPN Account page.



VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

Name		Tunnel	● Enable ○ Disable
Username		Password	
Connection Type	● Remote Access ○ LAN to LAN		
Peer Network IP		Peer Netmask	

Name: A user-defined name for the connection.

Tunnel: Select **Enable** to activate the account. PPTP(L2TP) server is waiting for the client to connect to this account.

Username: Please input the username for this account.

Password: Please input the password for this account.

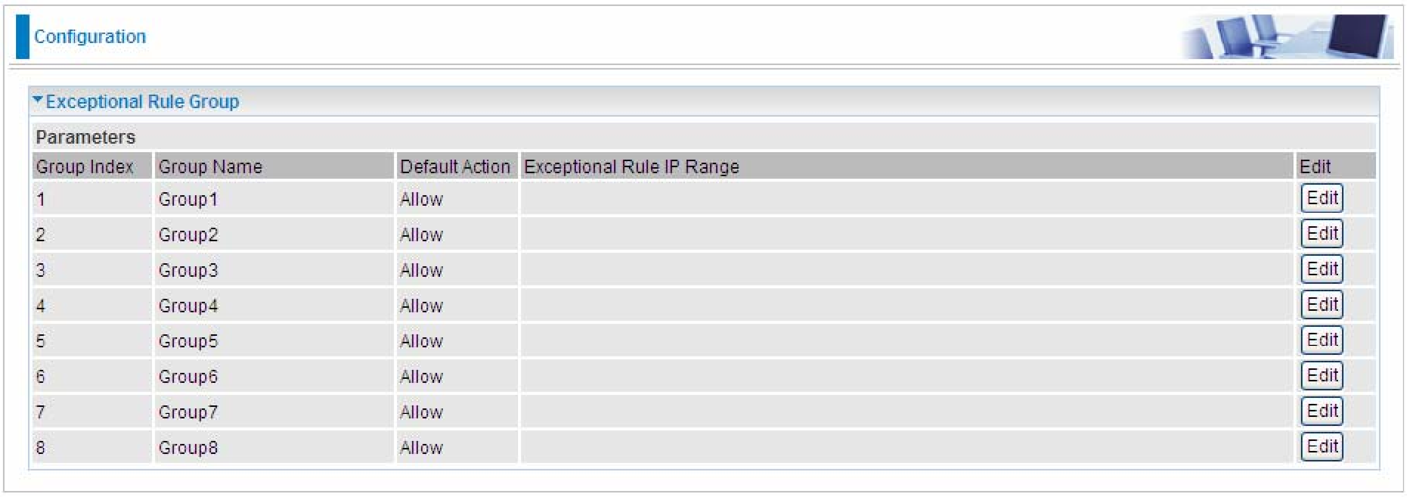
Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

Exceptional Rule Group

Exceptional Rule is dedicated to giving or blocking PPTP/L2TP server access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



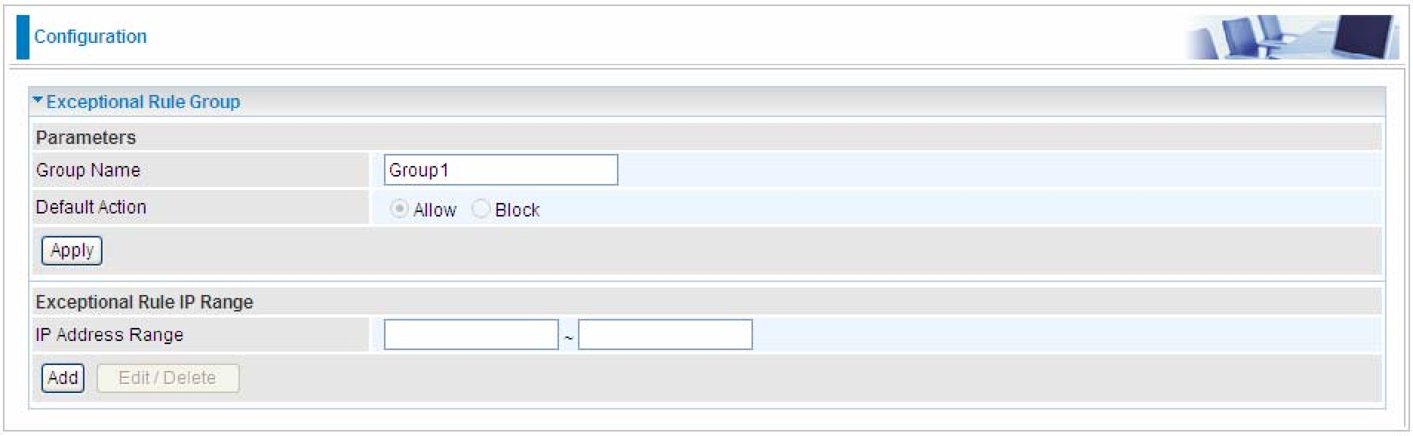
Configuration

Exceptional Rule Group

Parameters

Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

Press **Edit** to set the exceptional IP (IP Range).



Configuration

Exceptional Rule Group

Parameters

Group Name	Group1
Default Action	● Allow ○ Block

Exceptional Rule IP Range

IP Address Range	~

Default Action: Please first set the range to make **"Default Action"** setting available**.** Set "Allow" to ban the listed IP or IPs to access the PPTP and L2TP server.

Check "Block" to grant access to the listed IP or IPs to the PPTP and L2TP server.

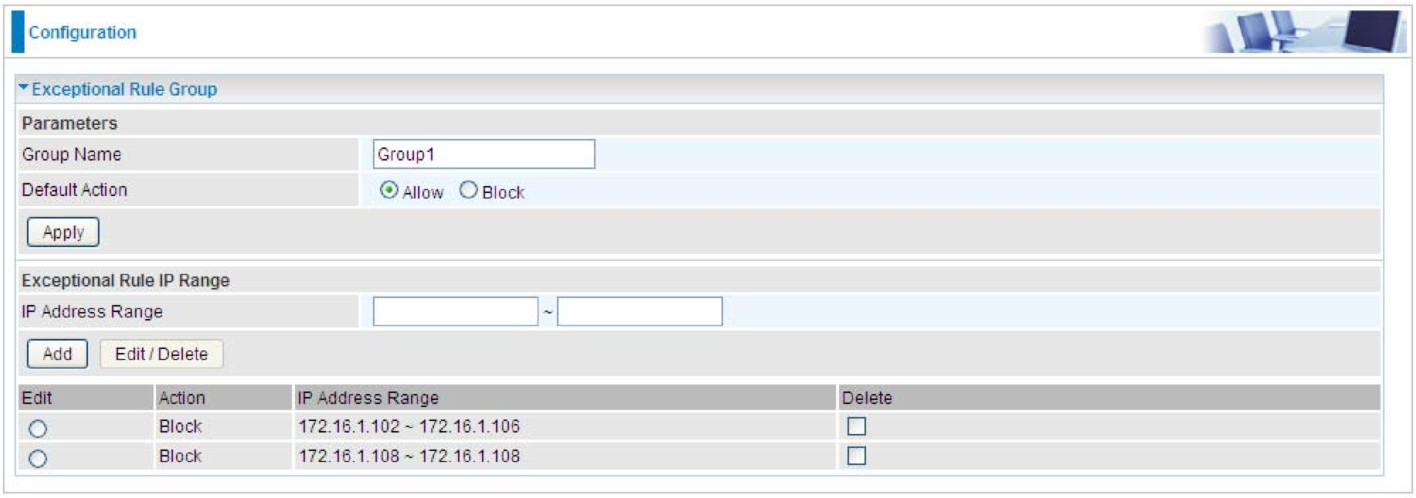
Apply: Press **Apply** button to apply the change.

Exceptional Rule Range

IP Address Range: Specify the IP address range; IPv4 address range can be supported.

Click **Add** to add the IP Range.

For instance, if user wants to block IP range of 172.16.1.102-172.16.1.106 from accessing your PPTP and L2TP server, you can add this IP range and valid it.



Configuration

▾Exceptional Rule Group

Parameters

Group Name	Group1
Default Action	● Allow ○ Block

Apply

Exceptional Rule IP Range

IP Address Range	~

Add Edit / Delete

Edit	Action	IP Address Range	Delete
○	Block	172.16.1.102 ~ 172.16.1.106	□
○	Block	172.16.1.108 ~ 172.16.1.108	□

PPTP

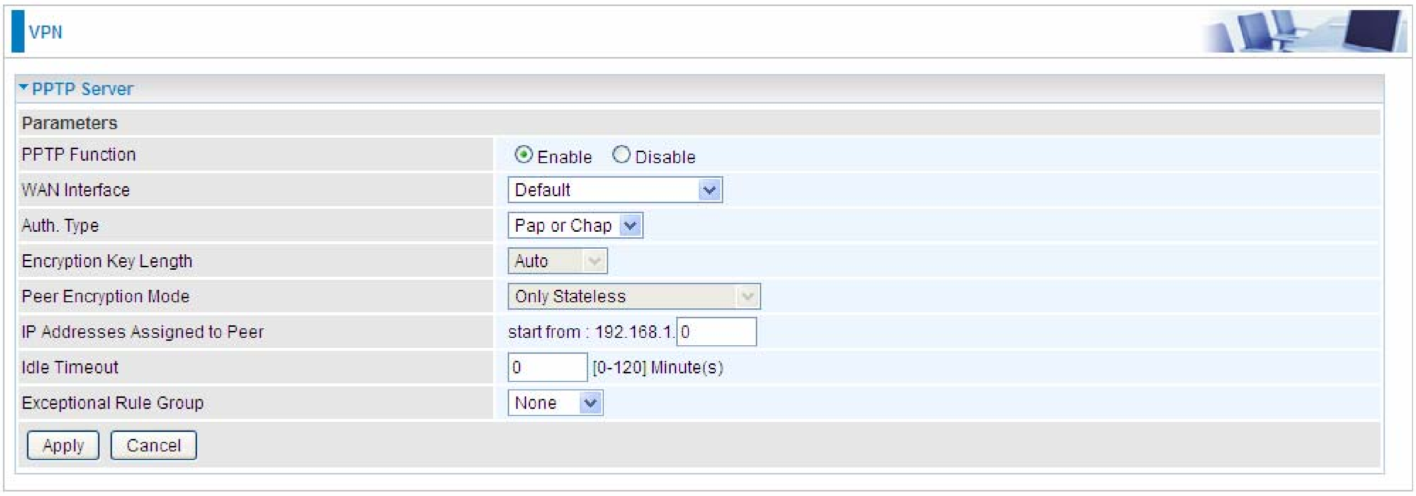
The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, Microsoft CHAP V1/V2 or EAP-TLS. The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2 or EAP-TLS.

Note: 4 sessions for Client and 4 sessions for Server respectively.

PPTP Server

In PPTP session, users can set the basaic parameters(authentication, encyption, peer address, etc) for PPTP Server, and accounts in the next page of PPTP Account. They both constitutes the PPTP Server setting.



VPN

▾ PPTP Server

Parameters	
PPTP Function	● Enable ○ Disable
WAN Interface	Default
Auth. Type	Pap or Chap
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1. 0
Idle Timeout	0 [0-120] Minute(s)
Exceptional Rule Group	None

PPTP Funtion: Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap and MS-CHAPv2. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

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.

Peer Encryption Mode: You may select “Only Stateless” or “Allow Stateless and Stateful” mode. The key will be changed every packet when you select Stateless mode.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254.

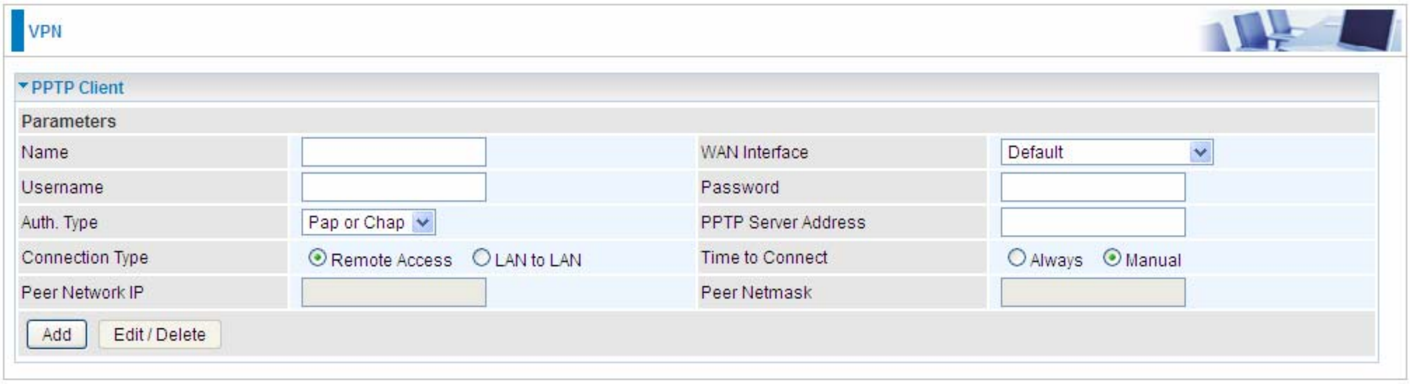
Idle Timeout: Specify the time for remote peer to be disconnected without any activities, from 0~120 minutes.

Exceptional Rule Group: Select to grant or block access to a group of IPs to the PPTP server. See Exceptional Rule Group. If there is not any restriction, select none.

Click **Apply** to submit your PPTP Server basic settings.

PPTP Client

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.



VPN

PPTP Client

Parameters			
Name		WAN Interface	Default
Username		Password	
Auth. Type	Pap or Chap	PPTP Server Address	
Connection Type	● Remote Access ○ LAN to LAN	Time to Connect	○ Always ● Manual
Peer Network IP		Peer Netmask	

Name: user-defined name for identification.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

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

PPTP Server Address: Enter the IP address of the PPTP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

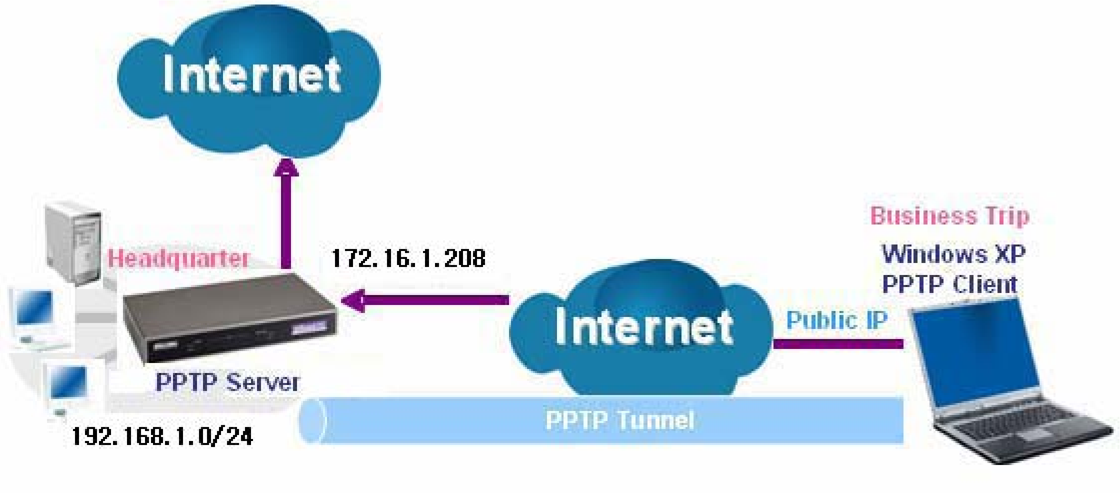
Time to Connect: Select Always to keep the connection always on, or Manual to connect manually any time.

Peer Network IP: Please input the subnet IP for Server peer.

Peer Netmask: Please input the Netmask for server peer.

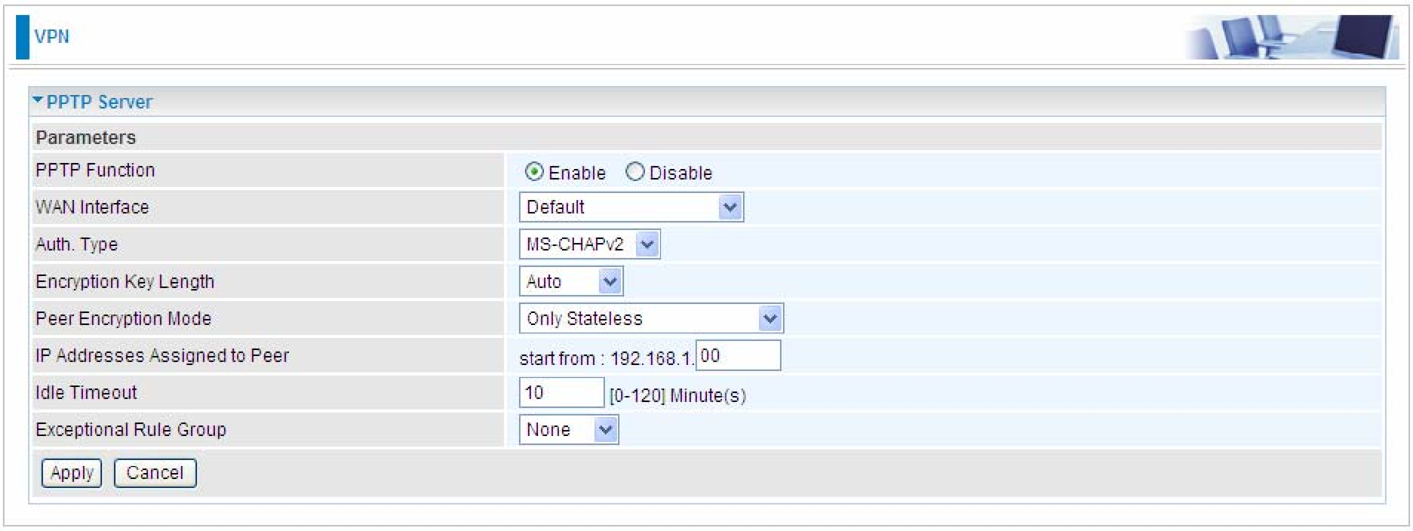
Click **Add** button to save your changes.

Example: PPTP Remote Access with Windows7
(Note: inside test with 172.16.1.208, just an example for illustration)



Server Side:

1. Configuration > **VPN** > **PPTP** and Enable the PPTP function, Click **Apply**.



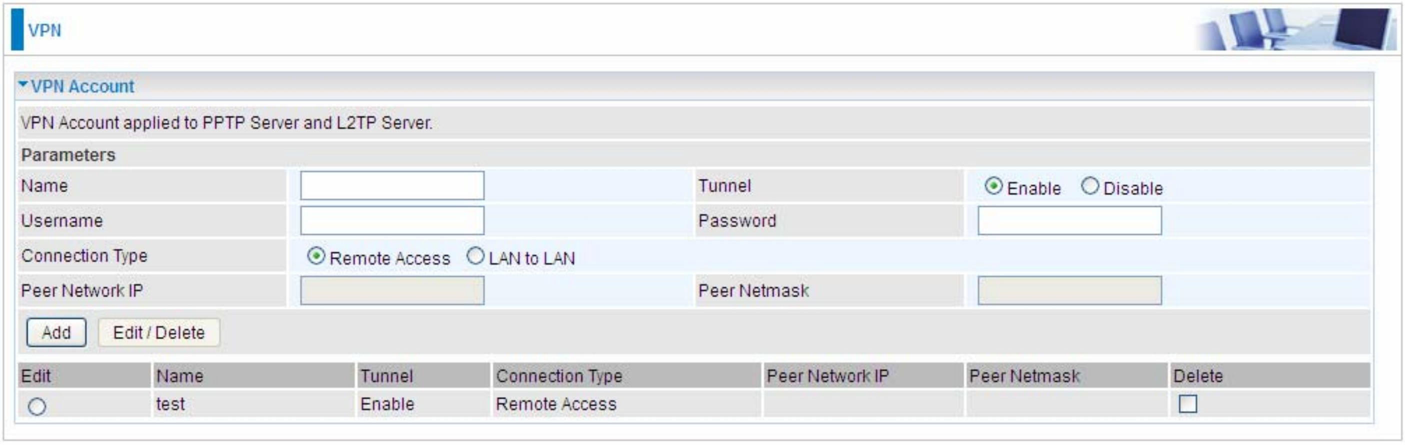
VPN

▾PPTP Server

Parameters	
PPTP Function	● Enable ○ Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1. 00
Idle Timeout	10 [0-120] Minute(s)
Exceptional Rule Group	None

Apply Cancel

2. Create a PPTP Account "test".



VPN

▾VPN Account

VPN Account applied to PPTP Server and L2TP Server.

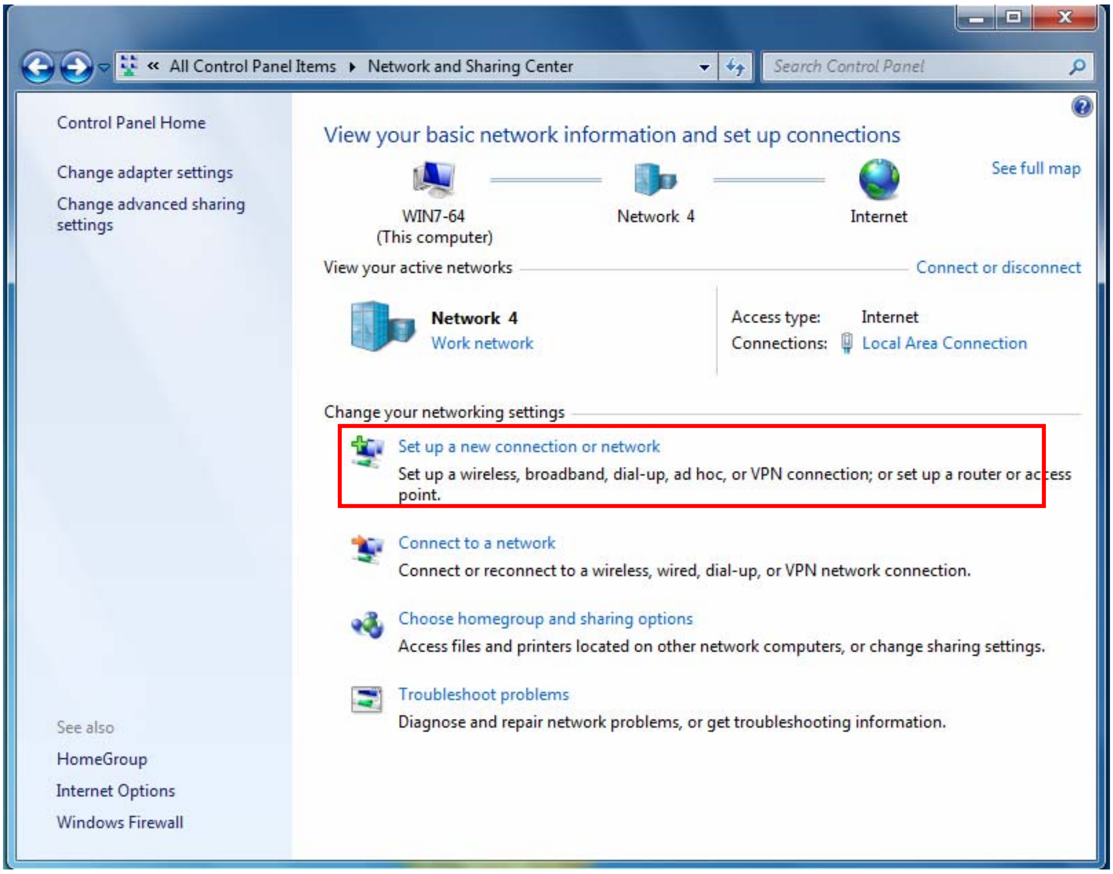
Parameters			
Name		Tunnel	● Enable ○ Disable
Username		Password	
Connection Type	● Remote Access ○ LAN to LAN		
Peer Network IP		Peer Netmask	

Add Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
○	test	Enable	Remote Access			□

Client Side:

1. In Windows7 click **Start** > **Control Panel**> **Network and Sharing Center,** Click **Set up a new connection network**.



View your basic network information and set up connections

View your active networks — Connect or disconnect

Network 4
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

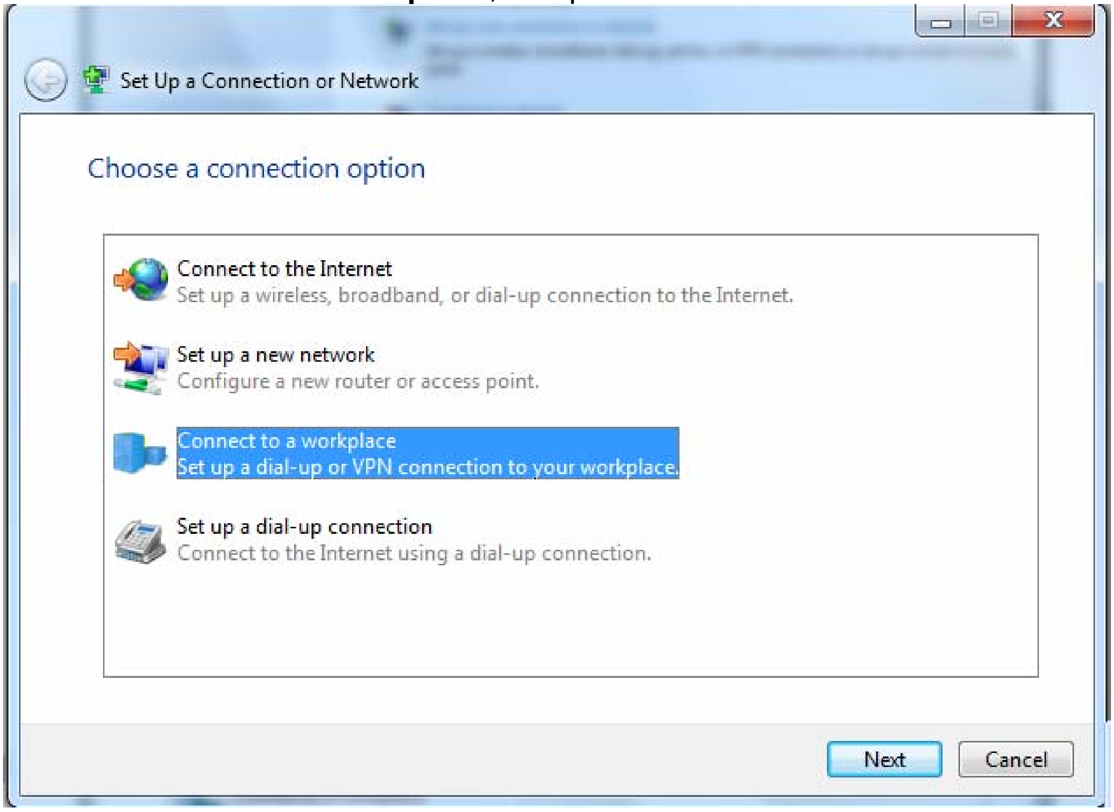
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2. Click **Connect to a workplace**, and press **Next**.



Set Up a Connection or Network

Choose a connection option

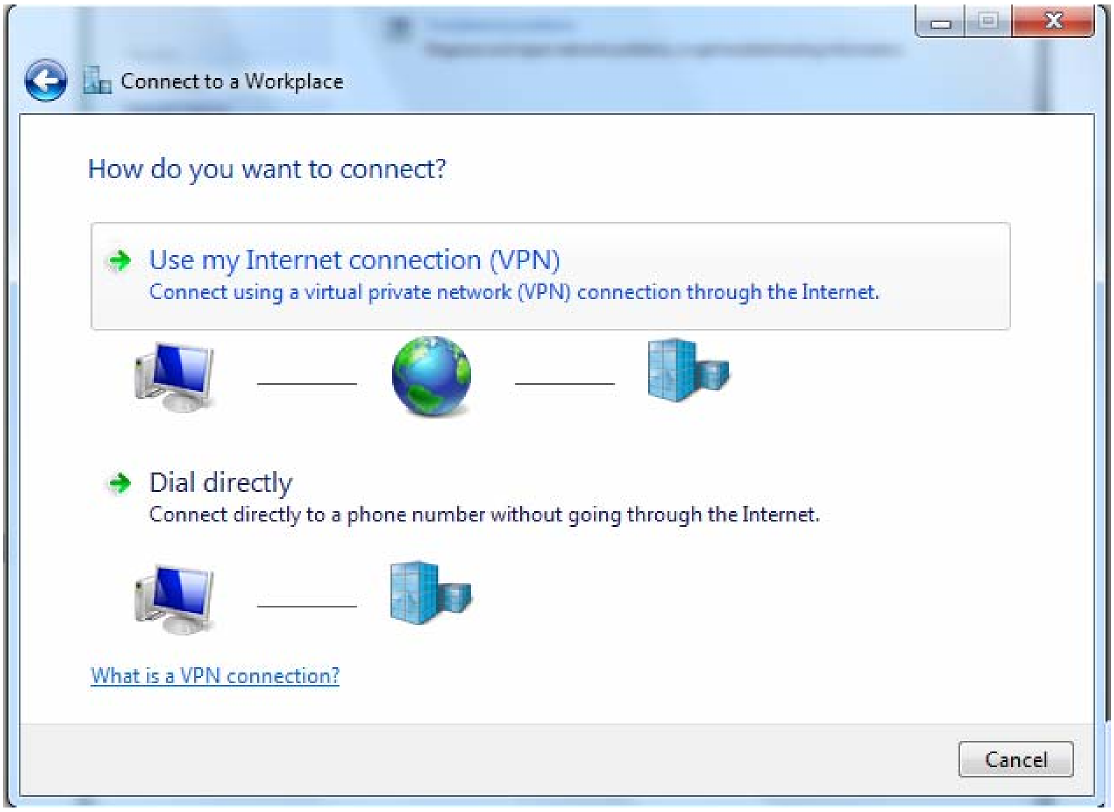
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

3. Select **Use my Internet connection (VPN)** and press **Next**.



Connect to a Workplace

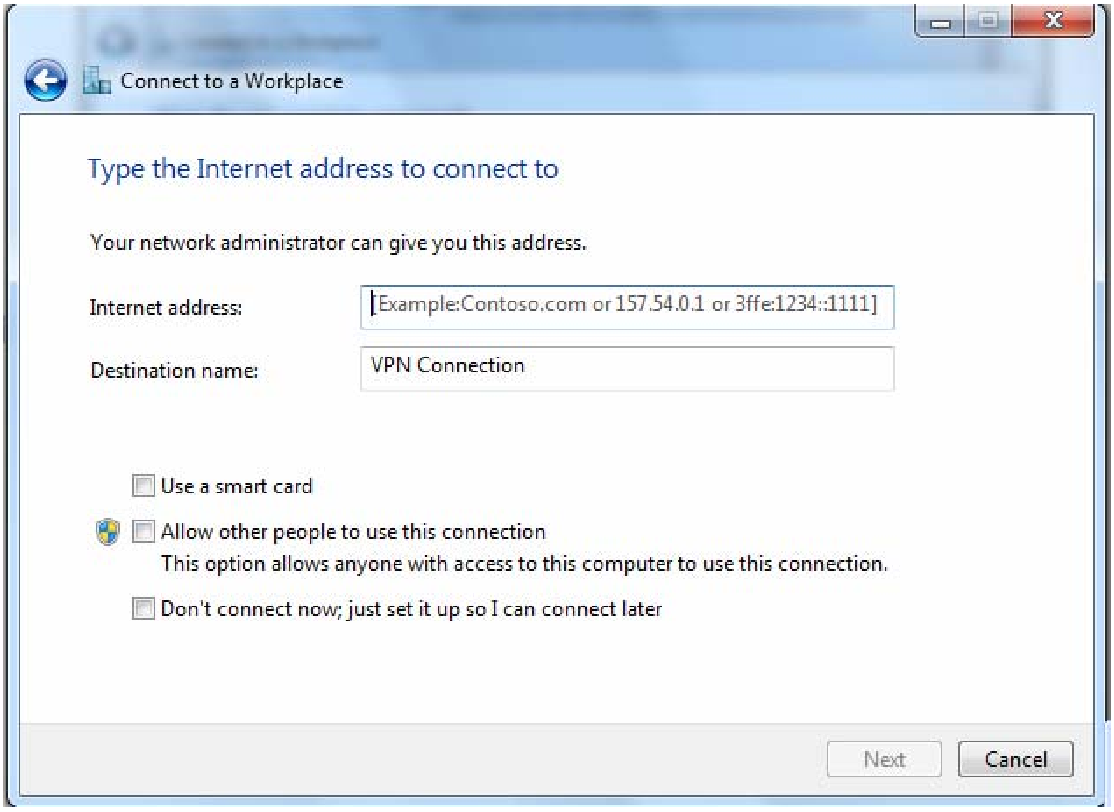
How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

4. Input **Internet address** and **Destination name** for this connection and press **Next**.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

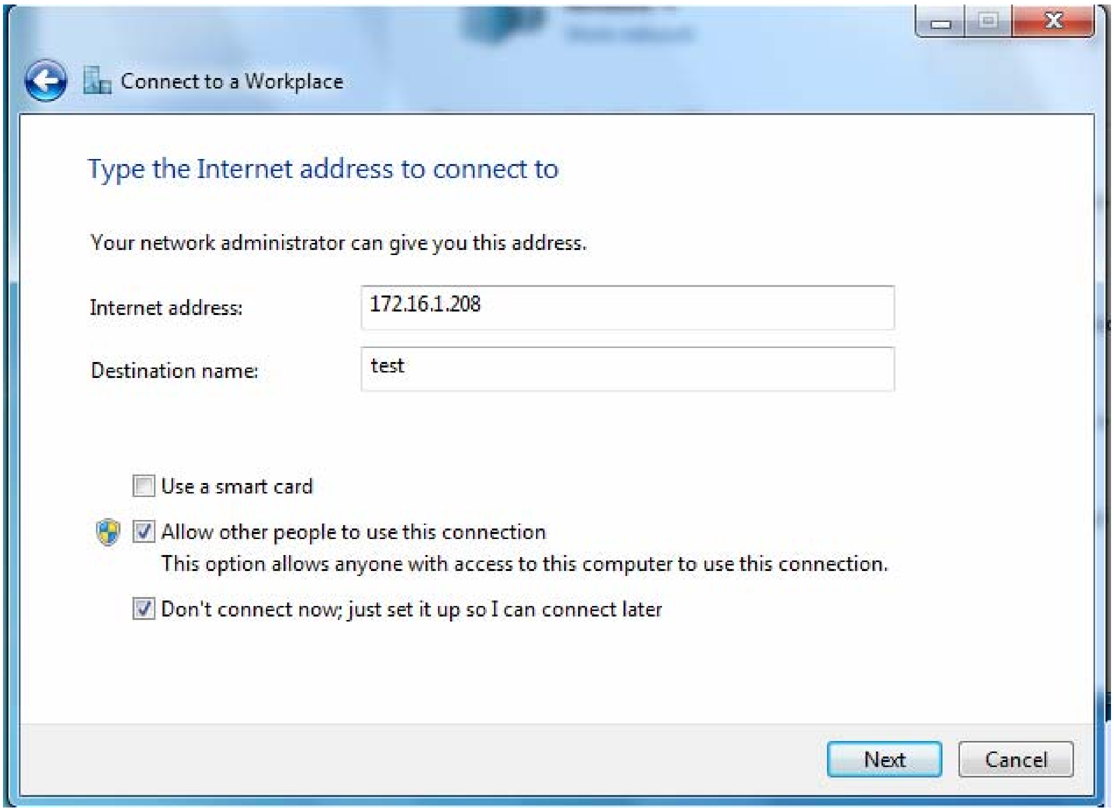
Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.208

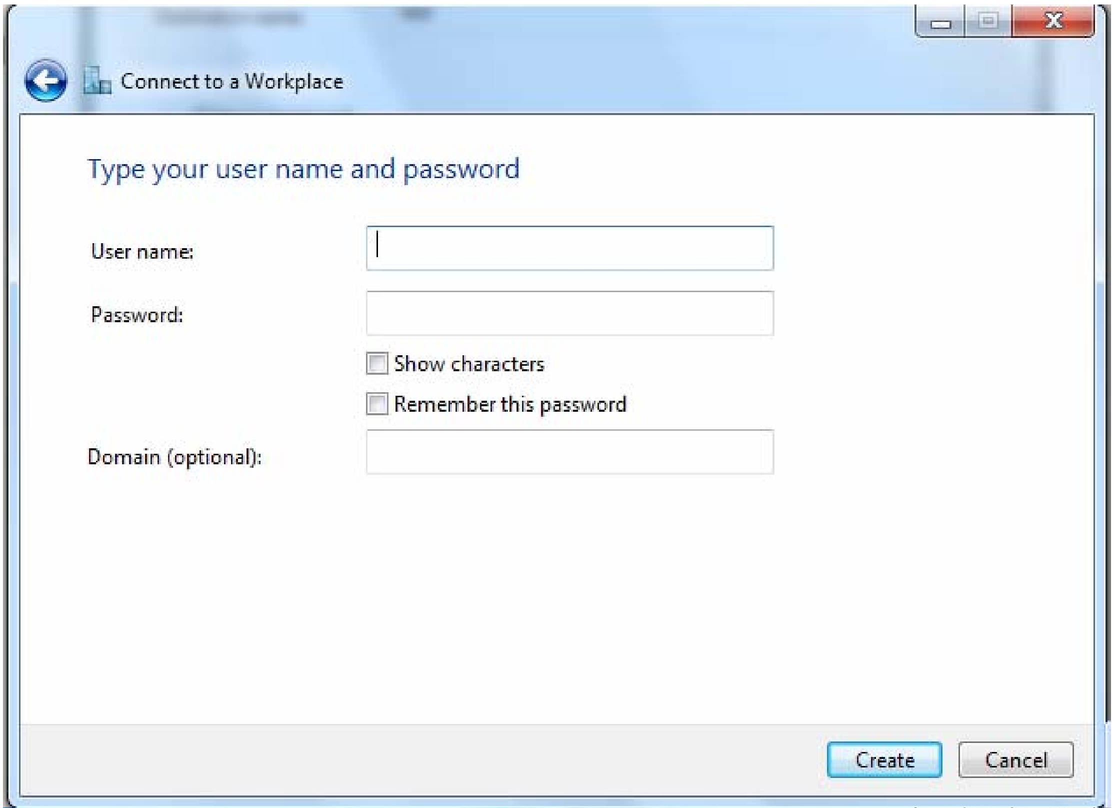
Destination name: test

□ Use a smart card

☑ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

5. Input the account (**user name** and **password**) and press **Create**.



Connect to a Workplace

Type your user name and password

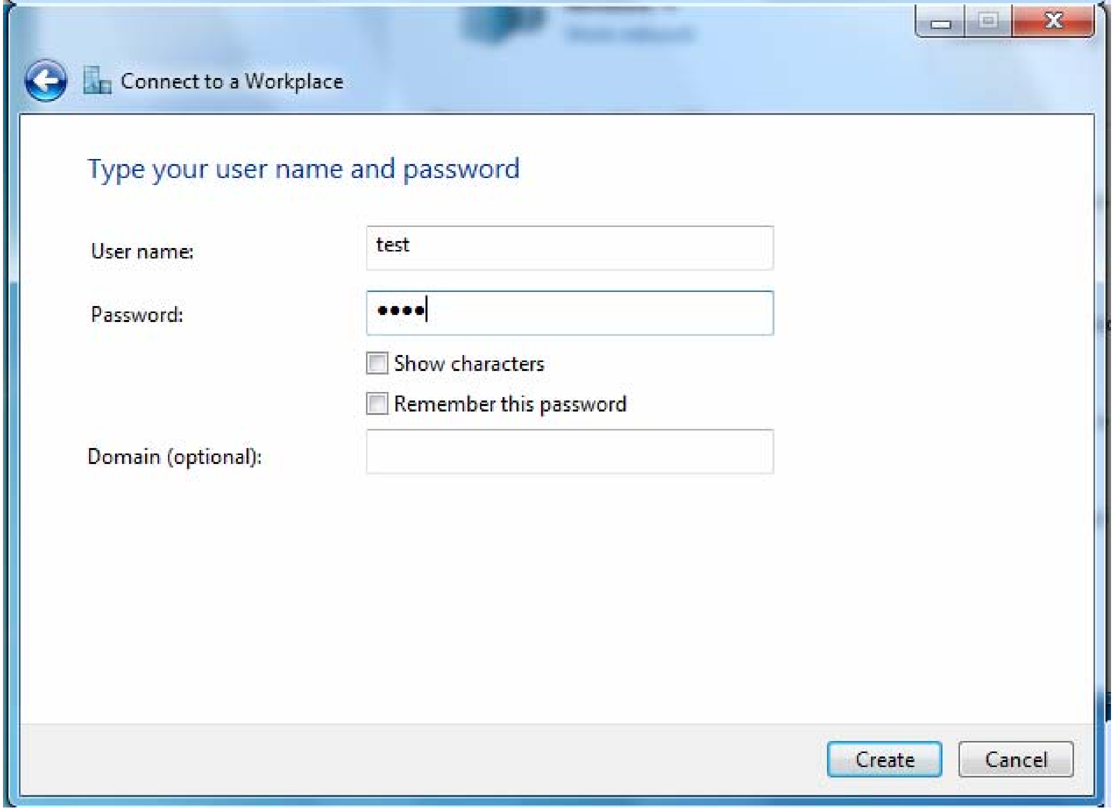
User name:

Password:

□ Show characters

□ Remember this password

Domain (optional):



Connect to a Workplace

Type your user name and password

User name: test

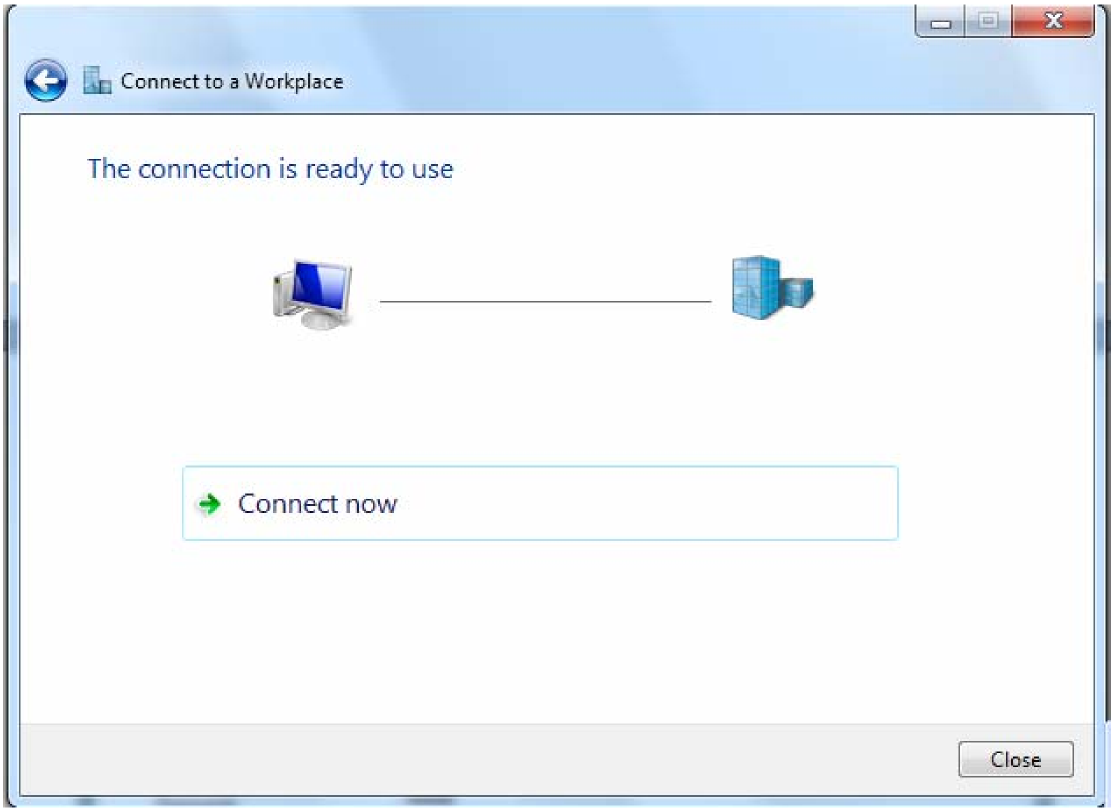
Password: ••••

□ Show characters

□ Remember this password

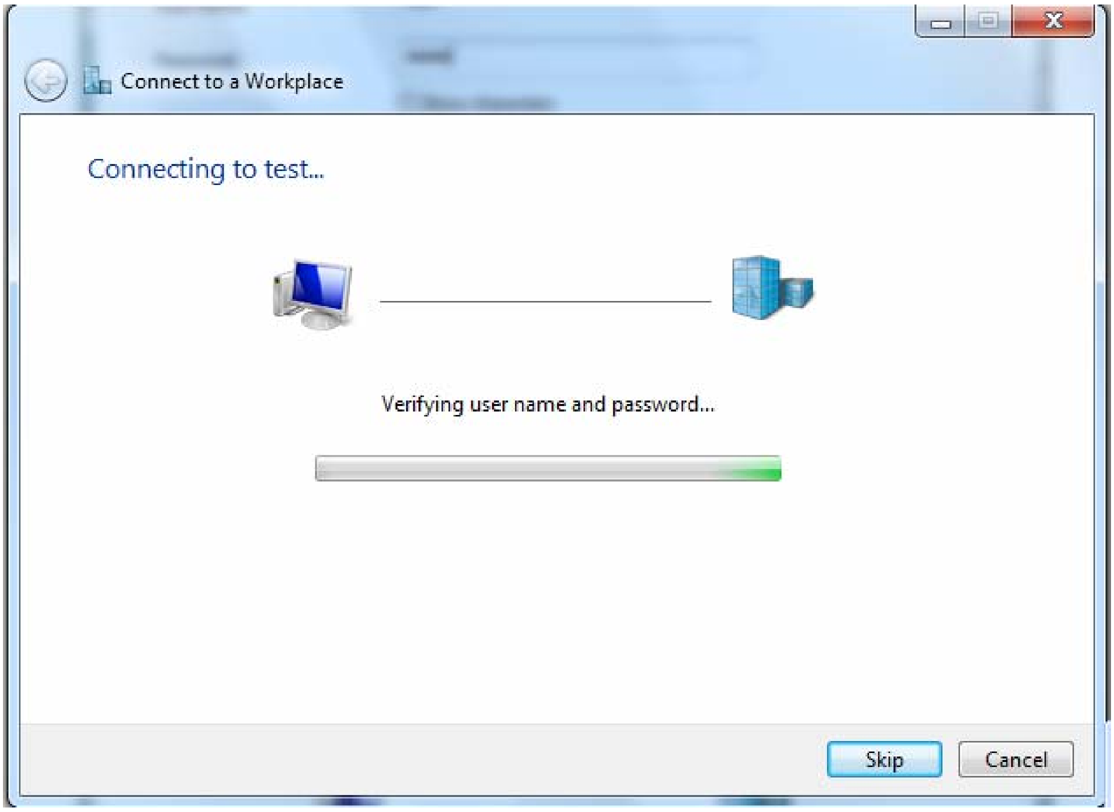
Domain (optional):

6. Connect to the server.



Connect to a Workplace

The connection is ready to use

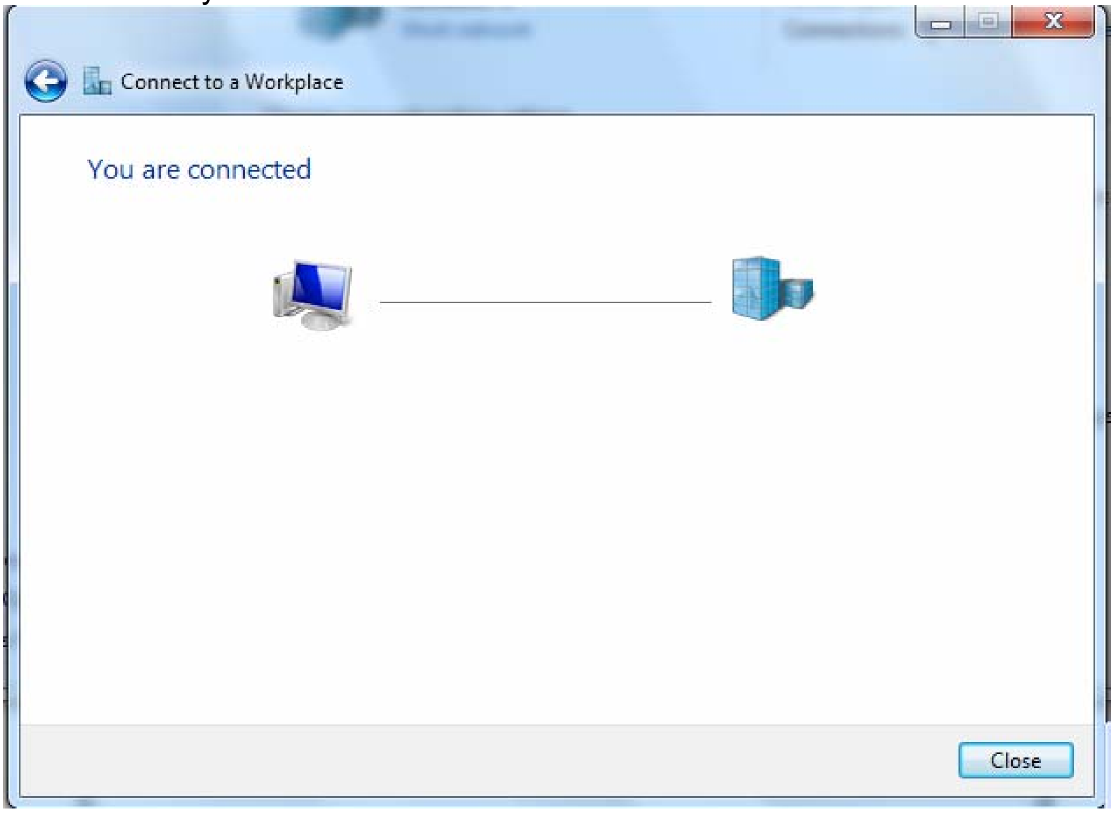


Connect to a Workplace

Connecting to test...

Verifying user name and password...

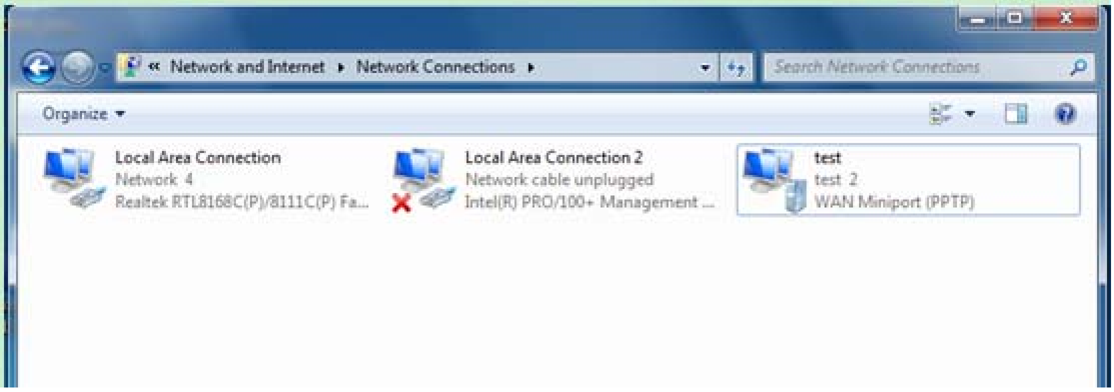
7. Successfully connected.



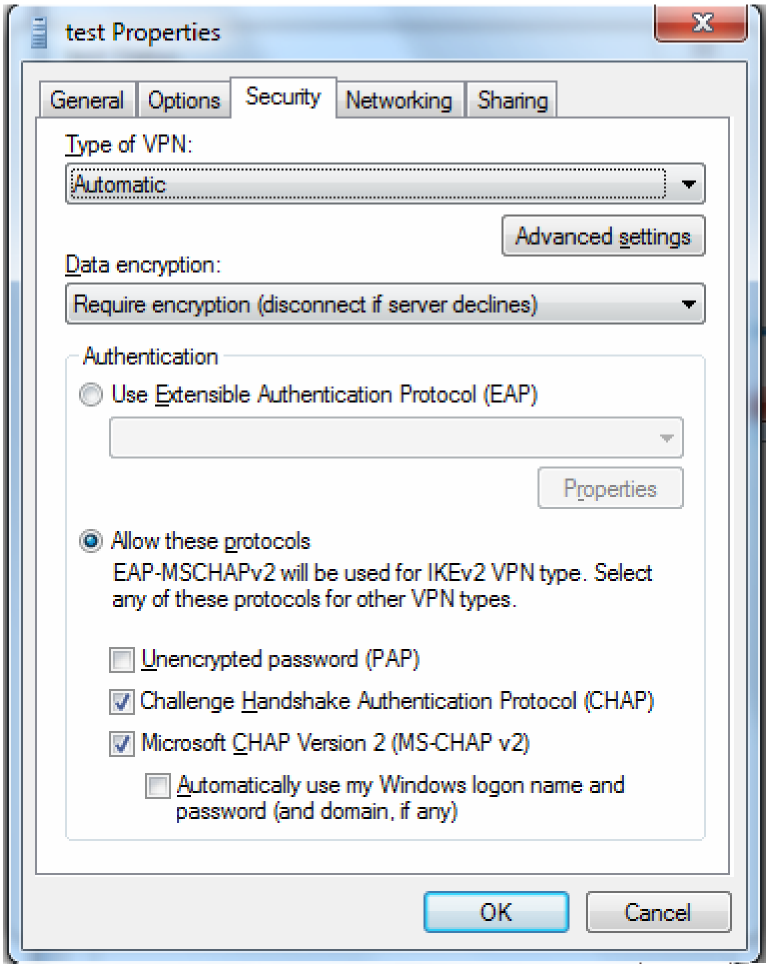
Connect to a Workplace

You are connected

PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click “test” icon, and select “Properties” to change the security parameters (if the connection fails, users can go here to change the settings)



« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Local Area Connection
Network 4
Realtek RTL8168C(P)/8111C(P) Fa...
Local Area Connection 2
Network cable unplugged
Intel(R) PRO/100+ Management ...
test
test 2
WAN Miniport (PPTP)



Type of VPN: Automatic

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

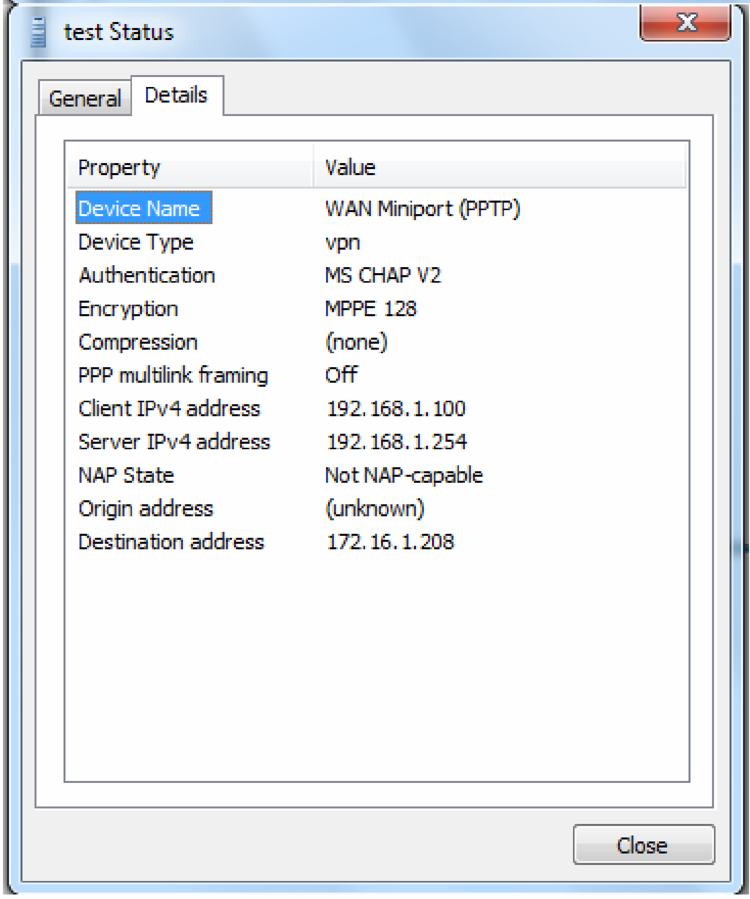
EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types.

□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

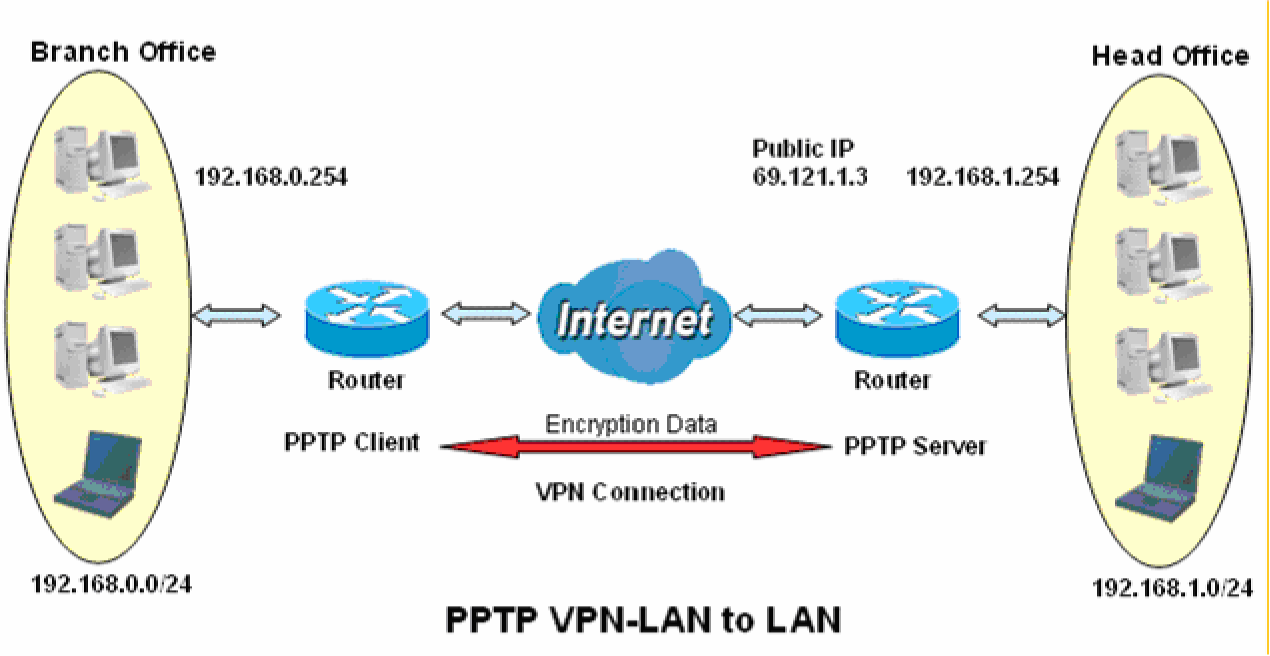
□ Automatically use my Windows logon name and password (and domain, if any)



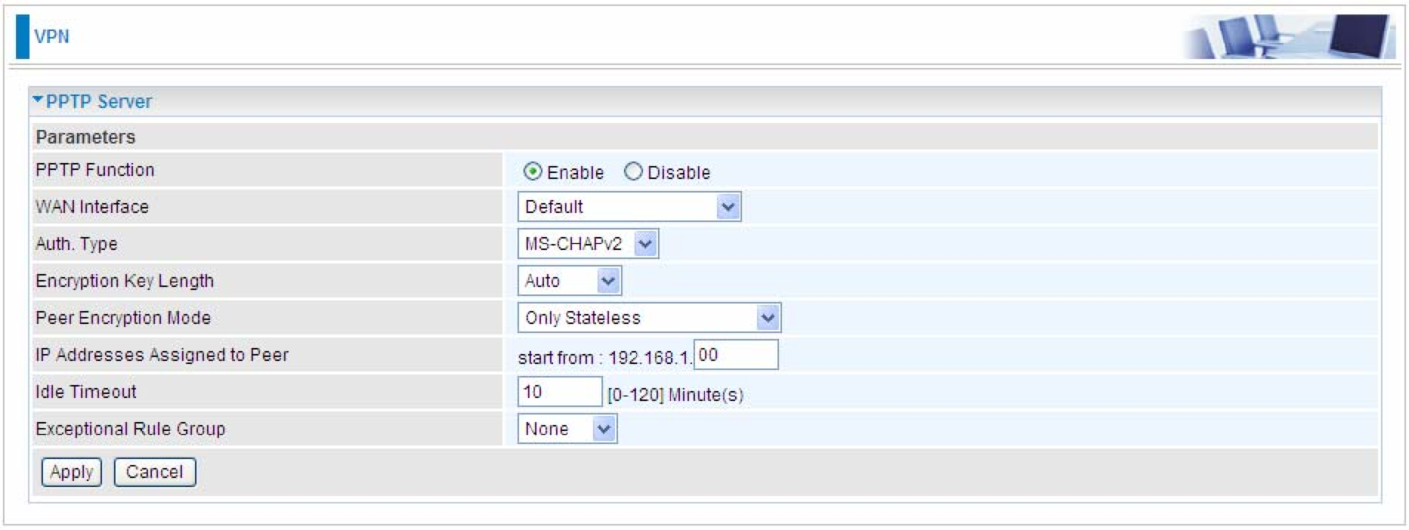
Property	Value
Device Name	WAN Miniport (PPTP)
Device Type	vpn
Authentication	MS CHAP V2
Encryption	MPPE 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	192.168.1.100
Server IPv4 address	192.168.1.254
NAP State	Not NAP-capable
Origin address	(unknown)
Destination address	172.16.1.208

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

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



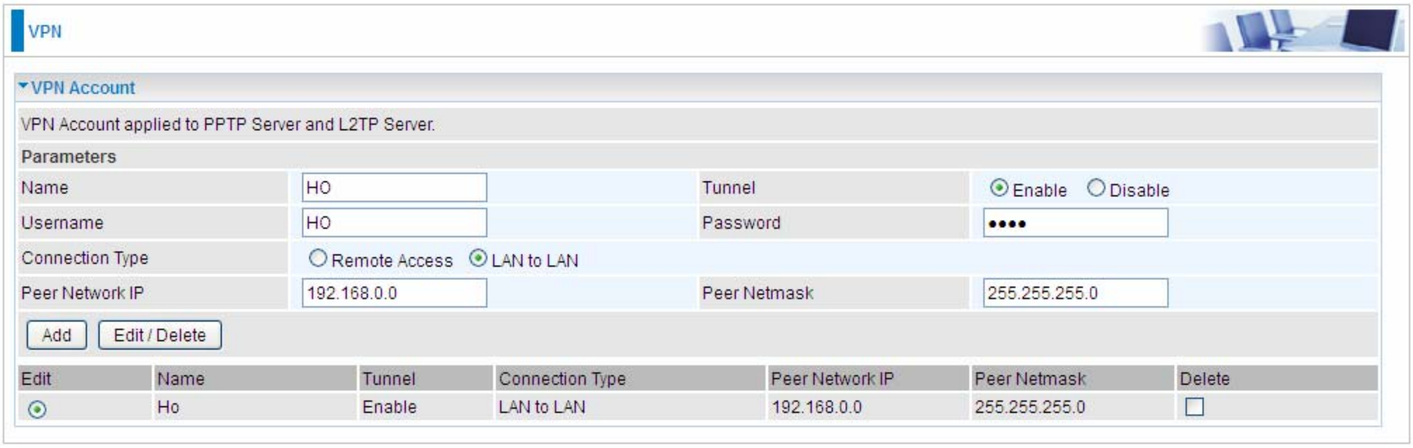
Server side: Head Office



Parameters	
PPTP Function	● Enable ○ Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1. 00
Idle Timeout	10 [0-120] Minute(s)
Exceptional Rule Group	None

The above is the common setting for PPTP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then the PPTP Account.



VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

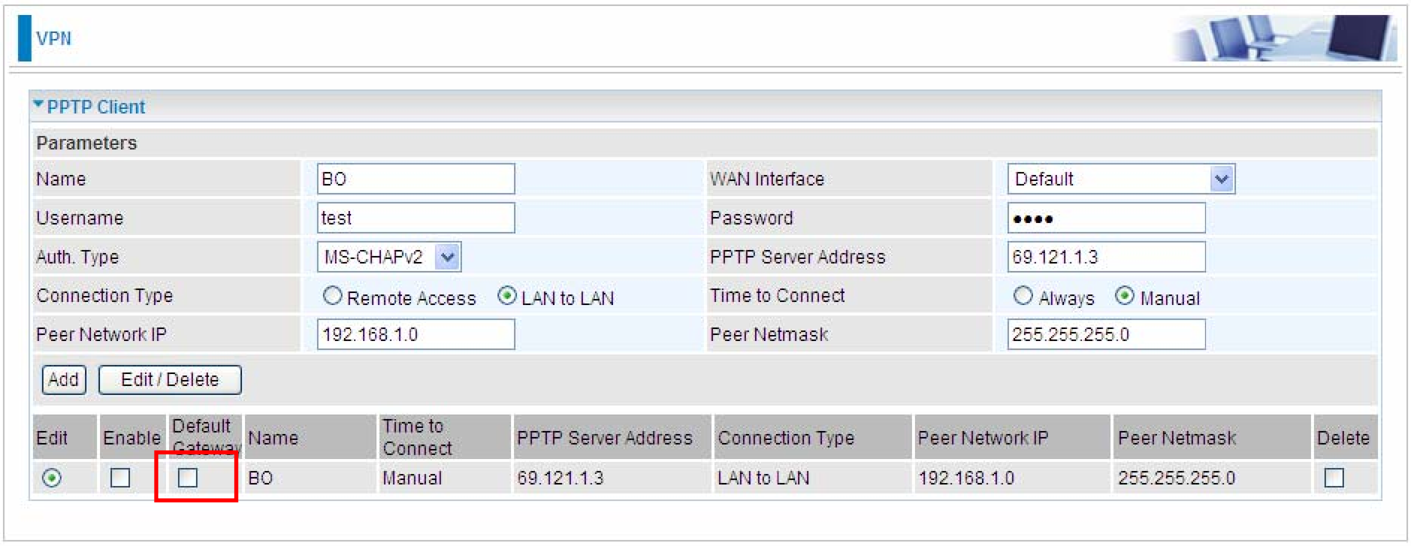
Parameters			
Name	HO	Tunnel	● Enable ○ Disable
Username	HO	Password	••••
Connection Type	○ Remote Access ● LAN to LAN		
Peer Network IP	192.168.0.0	Peer Netmask	255.255.255.0

Add | Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
●	Ho	Enable	LAN to LAN	192.168.0.0	255.255.255.0	□

Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.



VPN

PPTP Client

Parameters			
Name	BO	WAN Interface	Default
Username	test	Password	••••
Auth. Type	MS-CHAPv2	PPTP Server Address	69.121.1.3
Connection Type	○ Remote Access ● LAN to LAN	Time to Connect	○ Always ● Manual
Peer Network IP	192.168.1.0	Peer Netmask	255.255.255.0

Add | Edit / Delete

Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
●	□	□	BO	Manual	69.121.1.3	LAN to LAN	192.168.1.0	255.255.255.0	□

Note: users can see the “Default Gateway” item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

L2TP

The **Layer 2 Tunneling Protocol** (L2TP) is a Layer2 tunneling protocol for implementing virtual private networks.

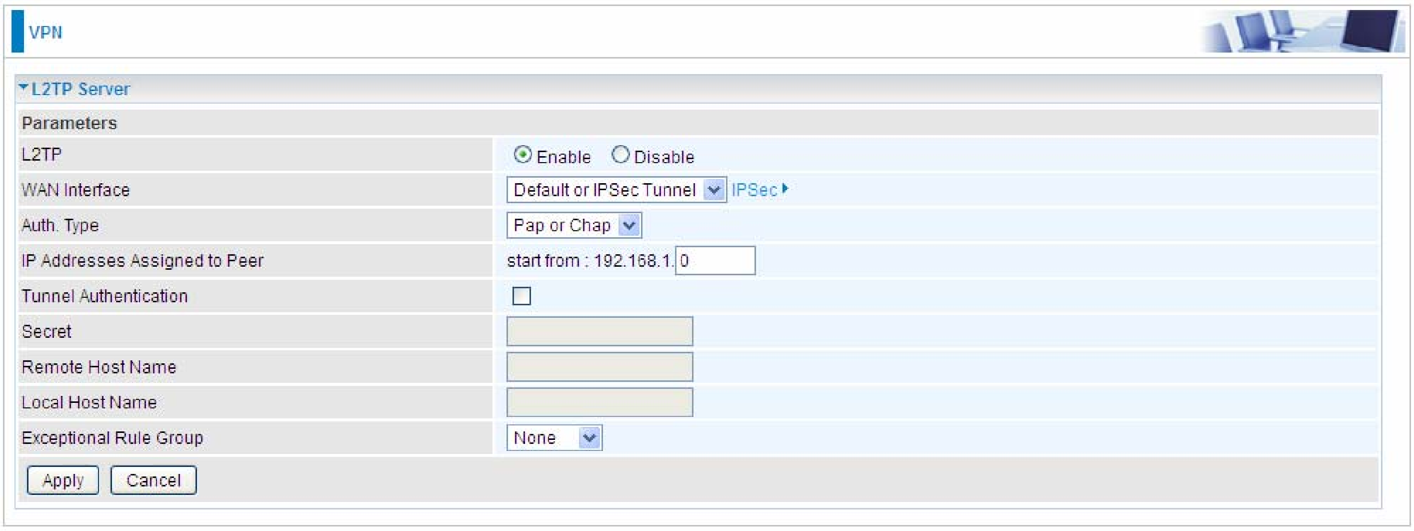
L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity. The combination of these two protocols is generally known as L2TP/IPsec.

In L2TP section, both pure L2TP and L2TP/IPSec are supported. Users can choose your preferable option for your own needs.

Note: 4 sessions for Client and only one for Server respectively.

L2TP Server

In L2TP session, users can set the bassic parameters(authentication, encyption, peer address, etc) for L2TP Server, and accounts in the page of VPN Account. They both constitutes the complete L2TP Server settings.



Parameters	
L2TP	● Enable ○ Disable
WAN Interface	Default or IPSec Tunnel IPSec▸
Auth. Type	Pap or Chap
IP Addresses Assigned to Peer	start from : 192.168.1. 0
Tunnel Authentication	□
Secret	
Remote Host Name	
Local Host Name	
Exceptional Rule Group	None

L2TP: Select **Enable** to activate L2TP Server. **Disable** to deactivate L2TP Server.

WAN Interface: Select the exact WAN interface configured as source for the tunnel. Select different interfaces, you will decide whether to use L2TP over IPSec or the pure L2TP.

- ⓘ **L2TP over IPSec**, Select “Default or IPSec Tunnel” only when there is IPSec for L2TP rule in place.
- ⓘ **Pure L2TP**, Select Default (there is no IPSec for L2TP in place) or other interface to activate the pure L2TP.

Auth. Type: The authentication type, Pap or Chap, PaP, Chap. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

IP Addresses Assigned to Peer: 192.168.1.x: please input the IP assigned range from 1~ 254.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication. Enable it if needed and set the same in the client side.

Secret: Enter the secretly pre-shared password for tunnel authentication.

Remote Host Name: Enter the remote host name (of peer) featuring the destination of the L2TP tunnel.

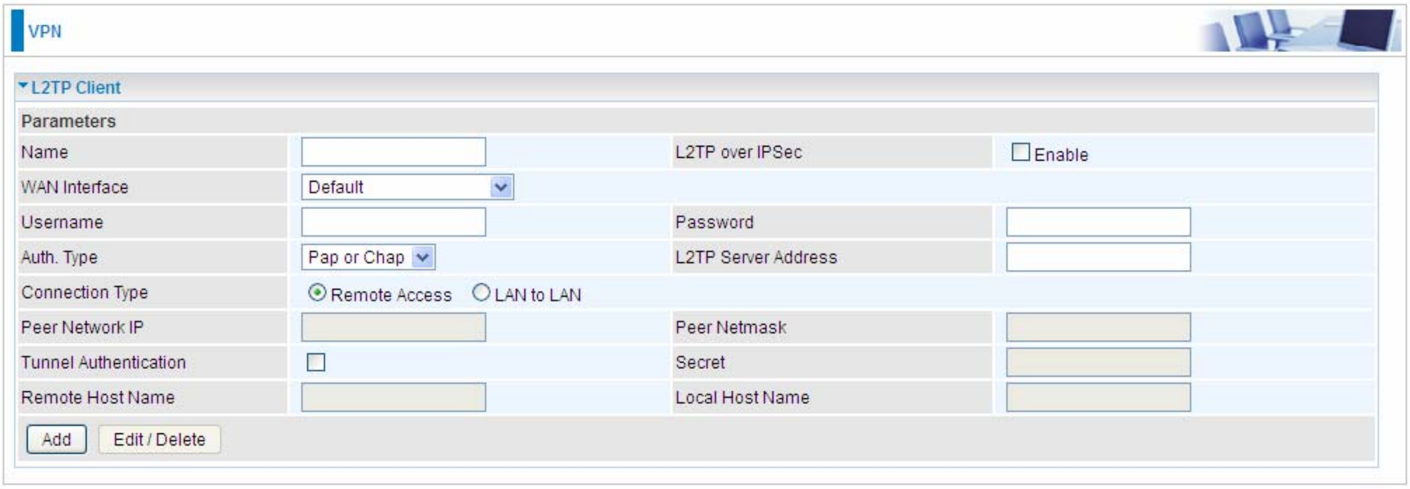
Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Exceptional Rule Group: Select to grant or block access to a group of IPs to the L2TP server. See Exceptional Rule Group. If there is not any restriction, select none.

Click **Apply** to submit your L2TP Server basic settings.

L2TP Client

L2TP client can help you dial-in the L2TP server to establish L2TP tunnel over Internet.



VPN

▾L2TP Client

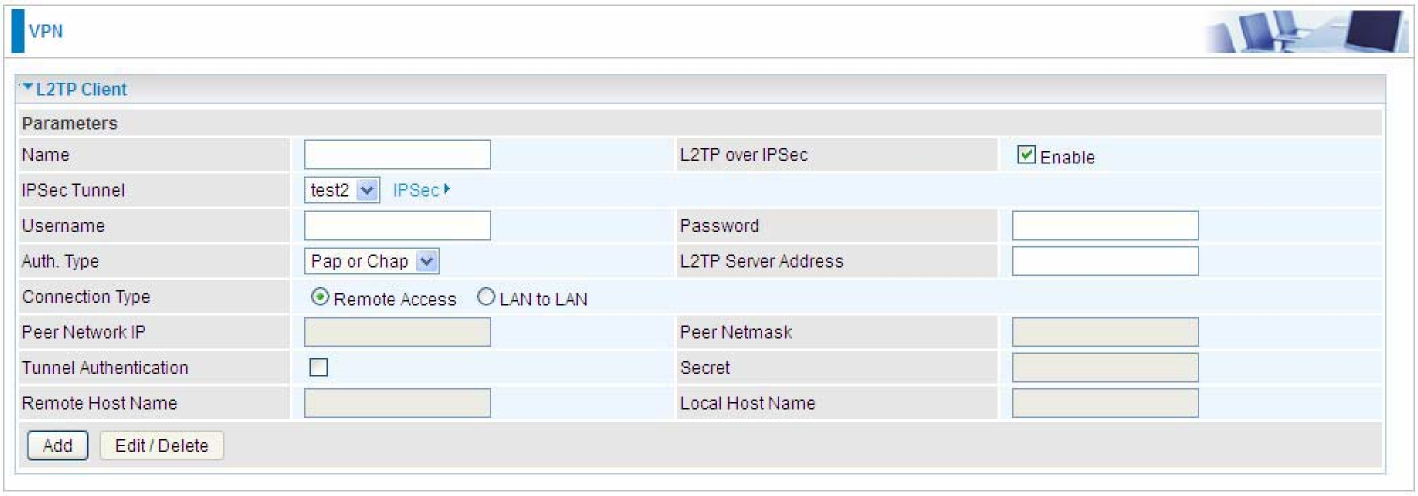
Parameters

Name		L2TP over IPSec	□ Enable
WAN Interface	Default		
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	● Remote Access ○ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	□	Secret	
Remote Host Name		Local Host Name	

Name: user-defined name for identification.

L2TP over IPSec: If your L2TP server has used L2TP over IPSec feature, please enable this item. under this circumstance, client and server communicate using L2TP over IPSec.

ⓘ **Enable**



VPN

▾L2TP Client

Parameters

Name		L2TP over IPSec	☑ Enable
IPSec Tunnel	test2 IPSec ▸		
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	● Remote Access ○ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	□	Secret	
Remote Host Name		Local Host Name	

IPSec Tunnel: Select the appropriate IPSec for L2TP rule configured for the L2TP Client.

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

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

L2TP Server Address: Enter the IP address of the L2TP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for Server.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

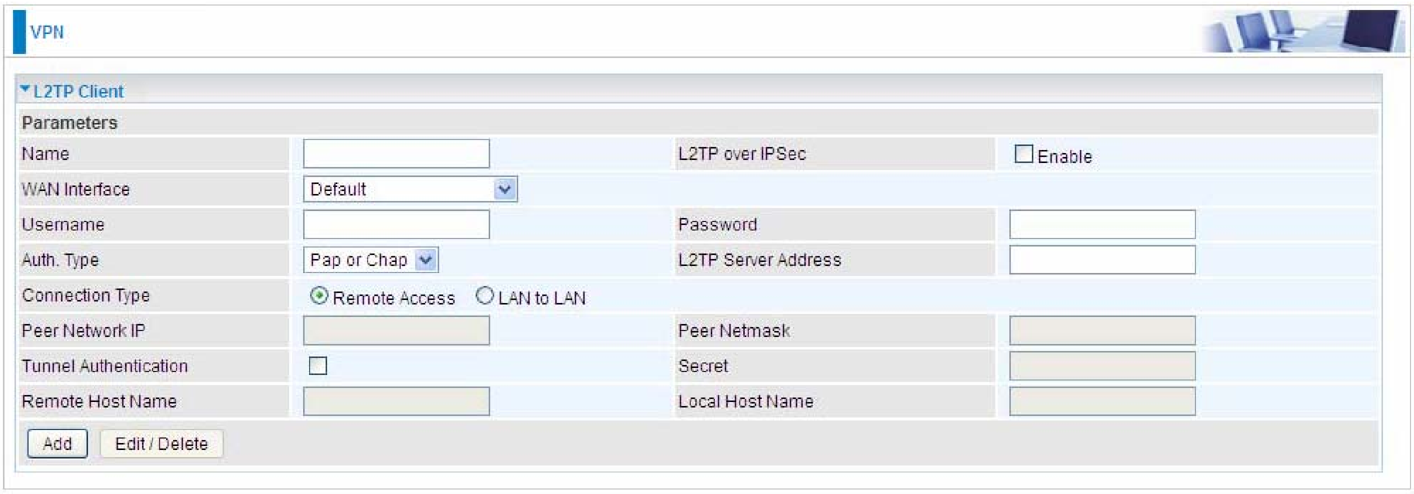
Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

Click **Add** button to save your changes.

Disable



VPN

▾L2TP Client

Parameters			
Name		L2TP over IPSec	□ Enable
WAN Interface	Default		
Username		Password	
Auth. Type	Pap or Chap	L2TP Server Address	
Connection Type	● Remote Access ○ LAN to LAN		
Peer Network IP		Peer Netmask	
Tunnel Authentication	□	Secret	
Remote Host Name		Local Host Name	

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel. Under this circumstance, client and server communicate through pure L2TP server.

Username: Enter the username provided by your L2TP Server.

Password: Enter the password provided by your L2TP Server.

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

L2TP Server Address: Enter the IP address of the L2TP server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Peer Network IP: Please input the subnet IP for Server.

Peer Netmask: Please input the Netmask for server.

Tunnel Authentication: Select whether to enable L2TP tunnel authentication, if the server side enables this feature, please follow.

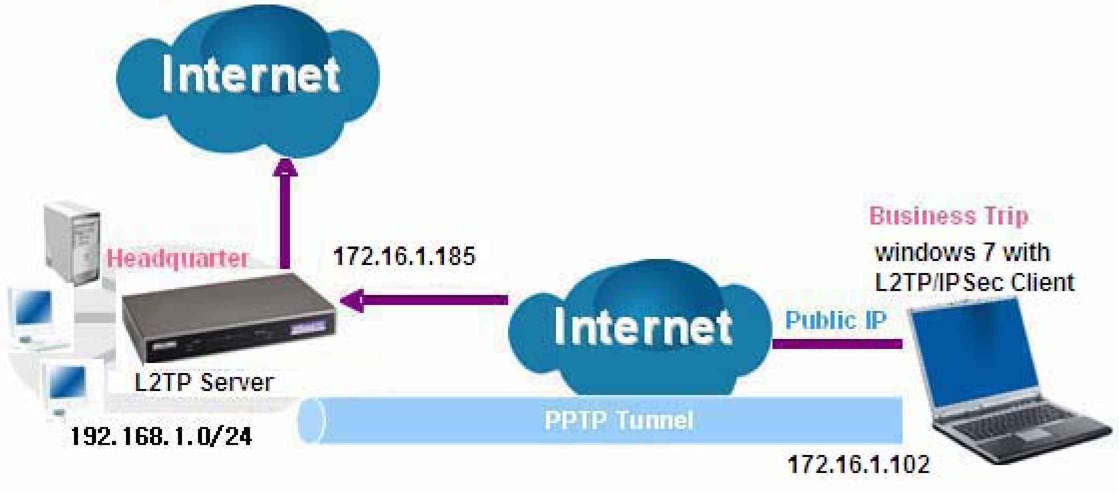
Secret: Enter the set secret password in the server side.

Remote Host Name: Enter the remote host name featuring the destination of the L2TP tunnel.

Local Host Name: Enter the local host name featuring the source of the L2TP tunnel.

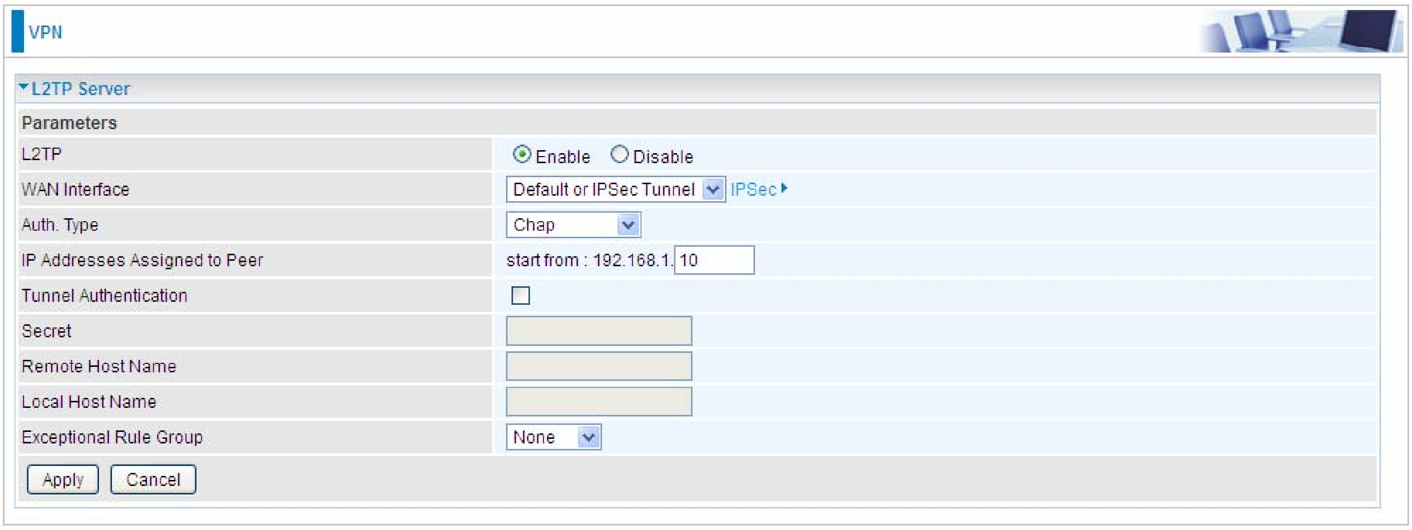
Click **Add** button to save your changes.

Example: L2TP over IPSec Remote Access with Windows7
(Note: inside test with 172.16.1.185, just an example for illustration)



Server Side:

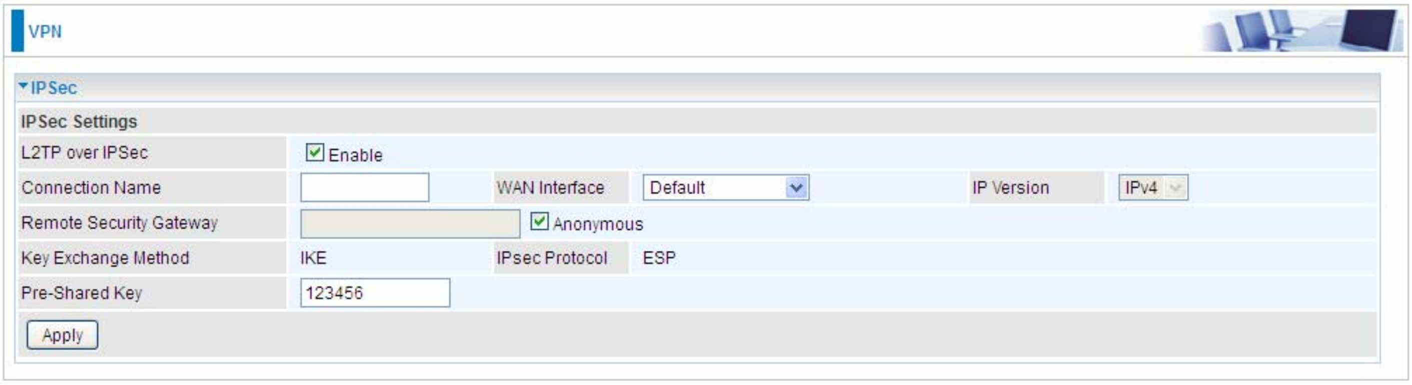
1. Configuration > **VPN** > **L2TP** and Enable the L2TP function, Click **Apply**.



▾L2TP Server

Parameters	
L2TP	● Enable ○ Disable
WAN Interface	Default or IPSec Tunnel IPSec▸
Auth. Type	Chap
IP Addresses Assigned to Peer	start from : 192.168.1. 10
Tunnel Authentication	□
Secret	
Remote Host Name	
Local Host Name	
Exceptional Rule Group	None

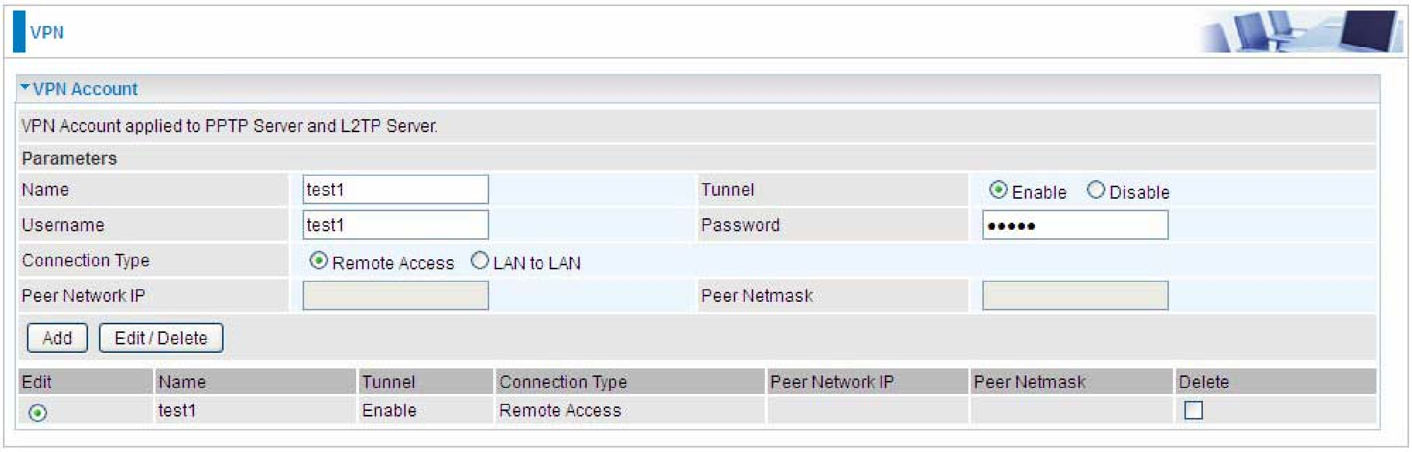
The IPSec for L2TP rule



▾IPSec

IPSec Settings					
L2TP over IPSec	☑ Enable				
Connection Name		WAN Interface	Default	IP Version	IPv4
Remote Security Gateway	☑ Anonymous				
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				

2. Create a L2TP Account “test1”.


VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

Parameters

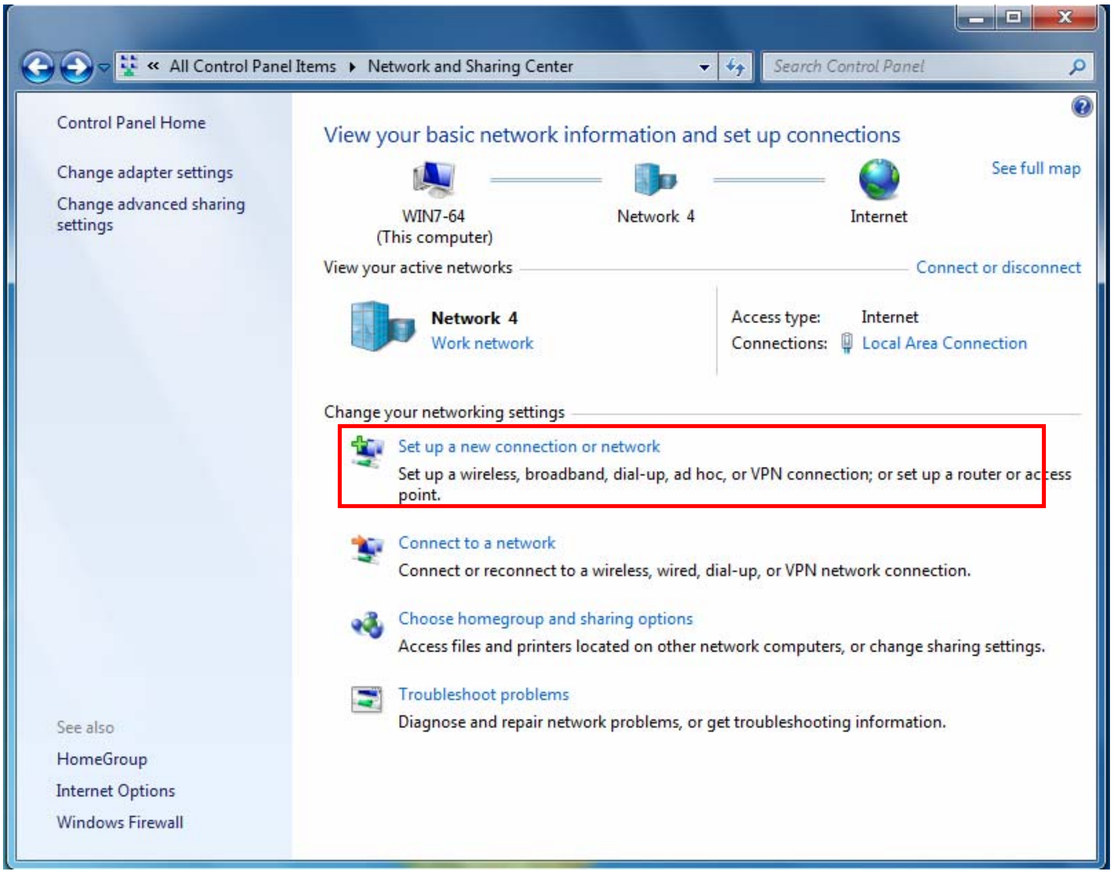
Name	test1	Tunnel	● Enable ○ Disable
Username	test1	Password	•••••
Connection Type	● Remote Access ○ LAN to LAN		
Peer Network IP		Peer Netmask	

Add | Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
●	test1	Enable	Remote Access			□

Client Side:

1. In Windows7 click **Start** > **Control Panel**> **Network and Sharing Center,** Click **Set up a new connection network**.



View your basic network information and set up connections

View your active networks

Network 4
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

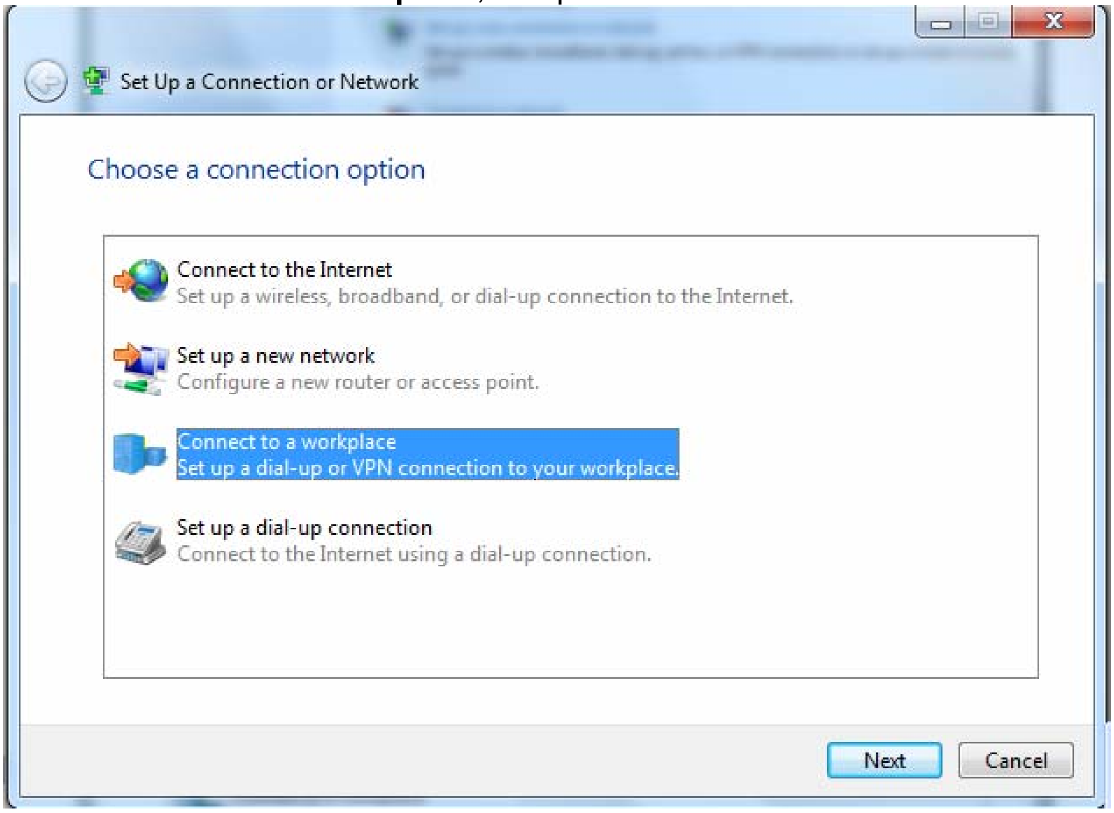
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2. Click **Connect to a workplace**, and press **Next**.



Set Up a Connection or Network

Choose a connection option

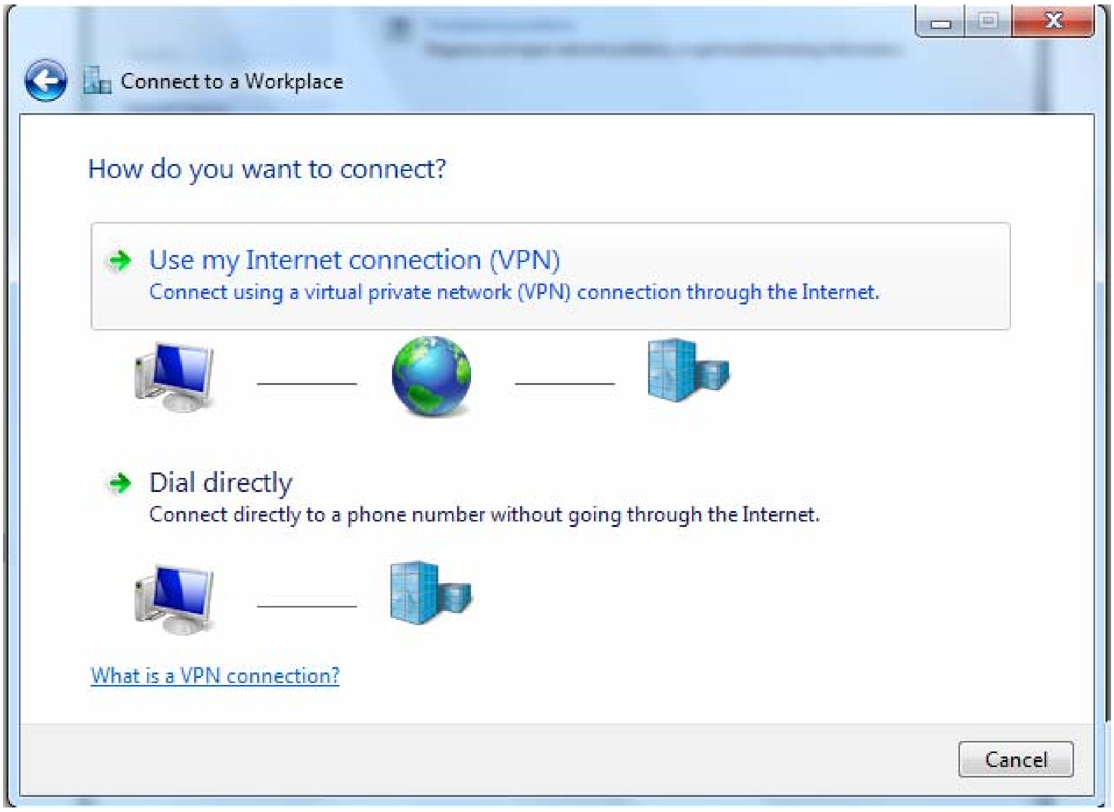
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

3. Select **Use my Internet connection (VPN)** and press **Next**.



Connect to a Workplace

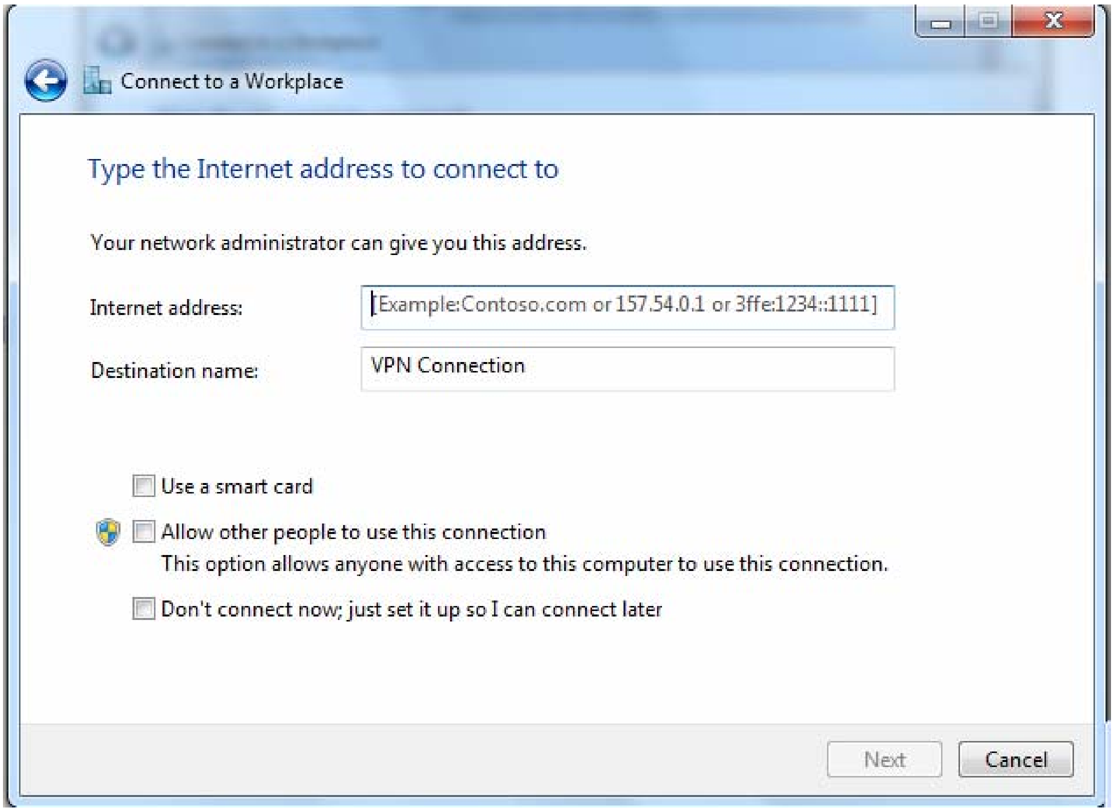
How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

What is a VPN connection?

4. Input **Internet address** and **Destination name** for this connection and press **Next**.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

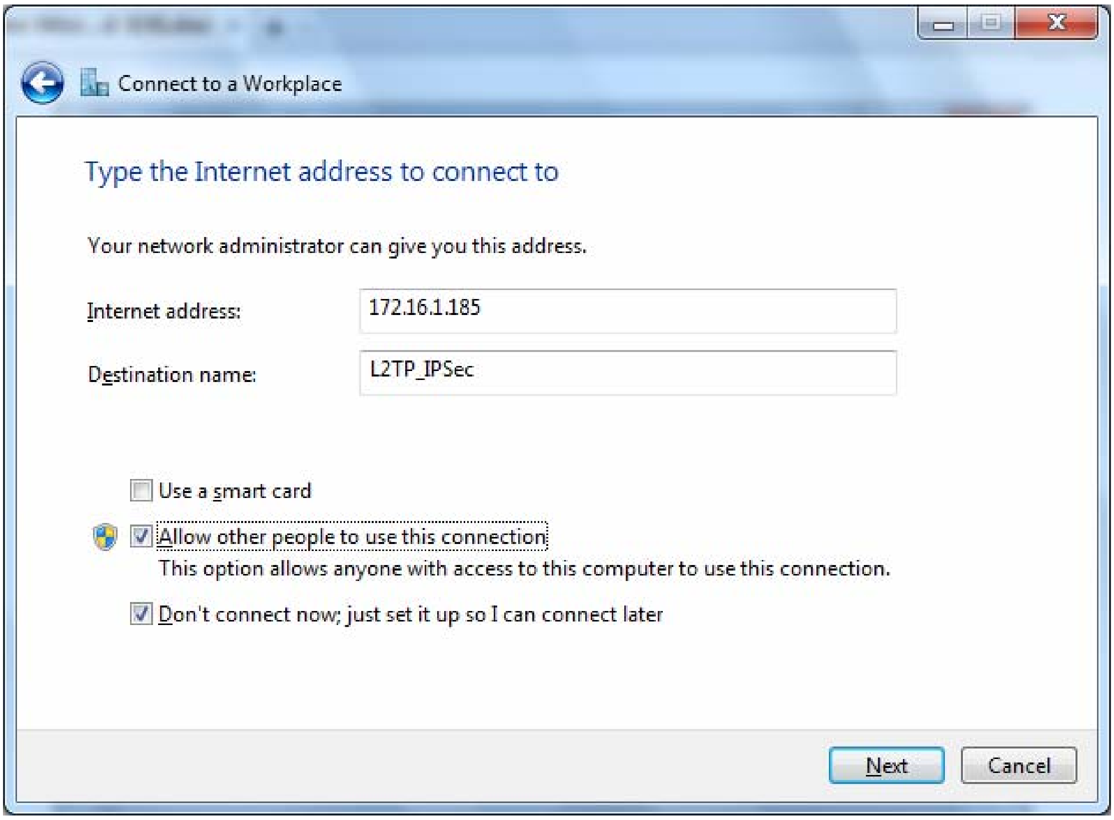
Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection

□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

□ Don't connect now; just set it up so I can connect later



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.185

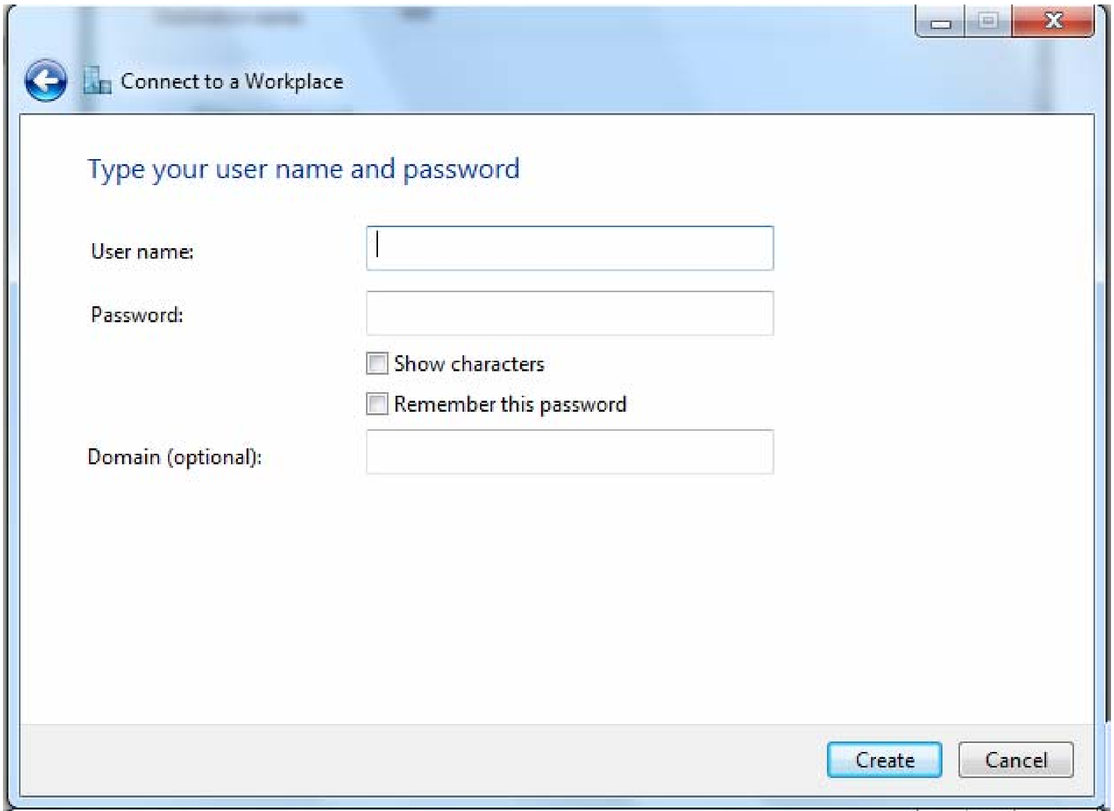
Destination name: L2TP_IPSec

□ Use a smart card

☑ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

5. Input the account (**user name** and **password**) and press **Create**.



Connect to a Workplace

Type your user name and password

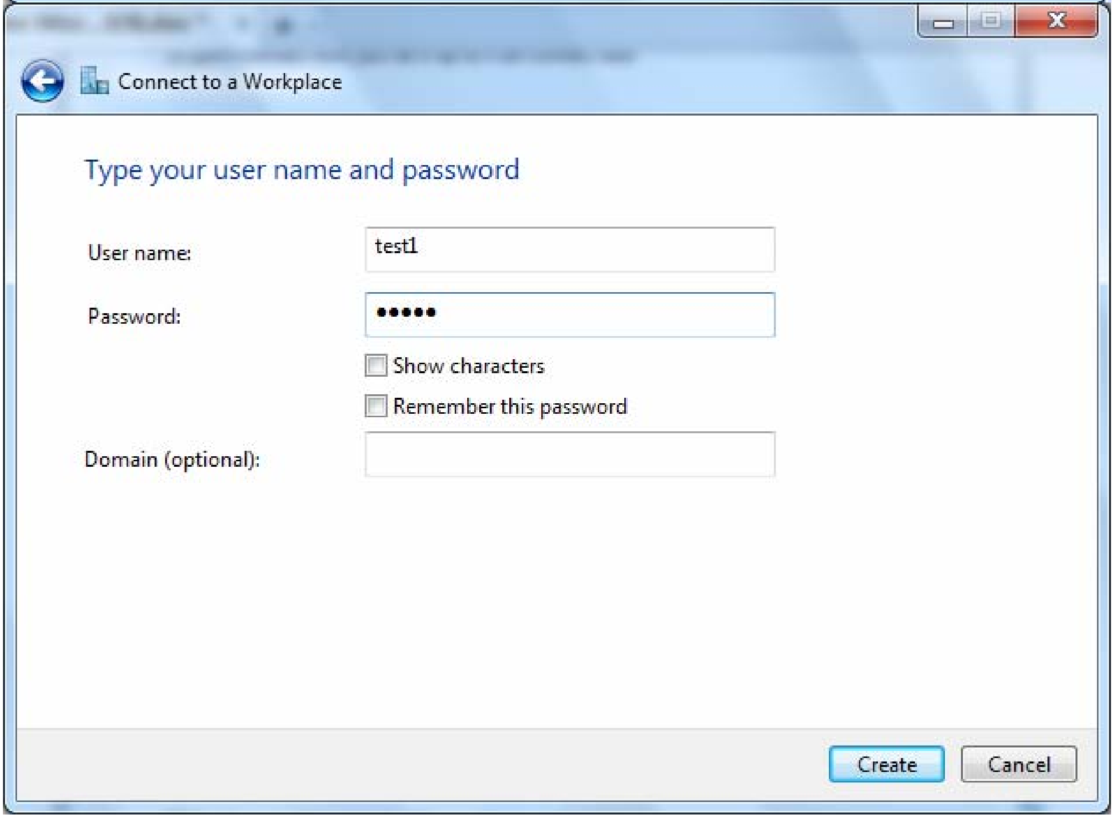
User name:

Password:

□ Show characters

□ Remember this password

Domain (optional):



Connect to a Workplace

Type your user name and password

User name: test1

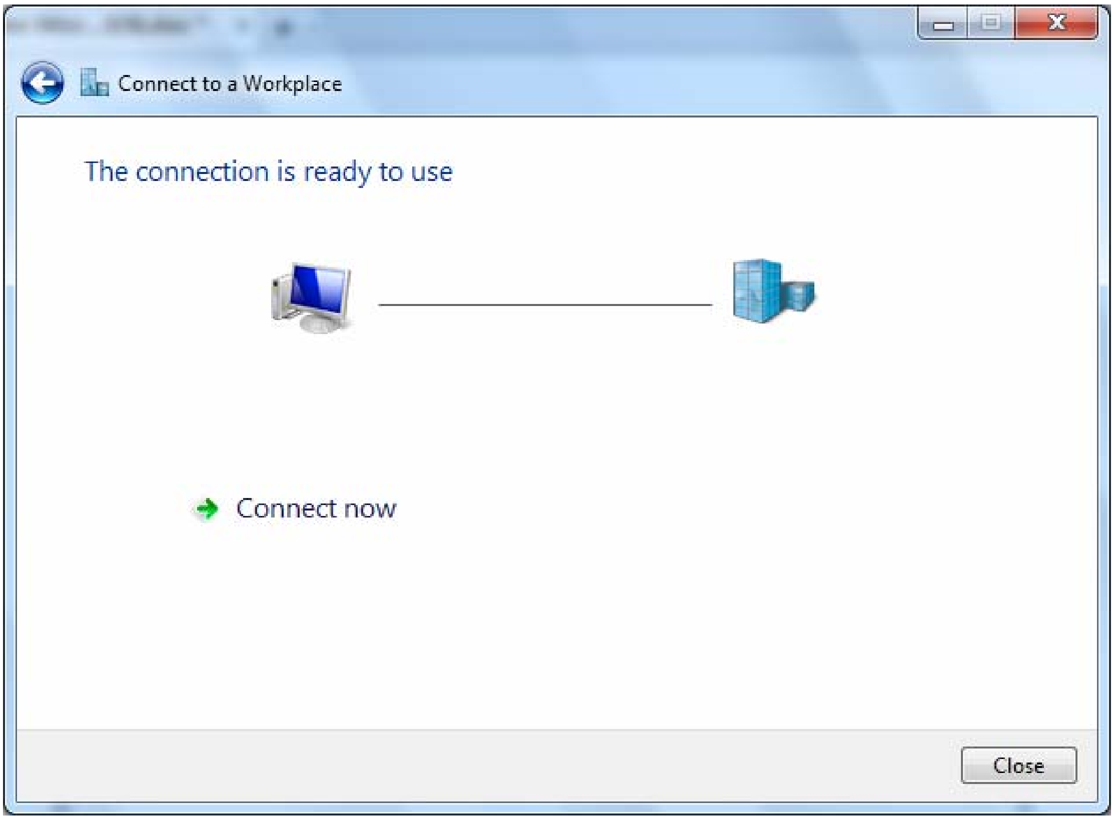
Password: •••••

□ Show characters

□ Remember this password

Domain (optional):

6. Connection created. Press **Close**.

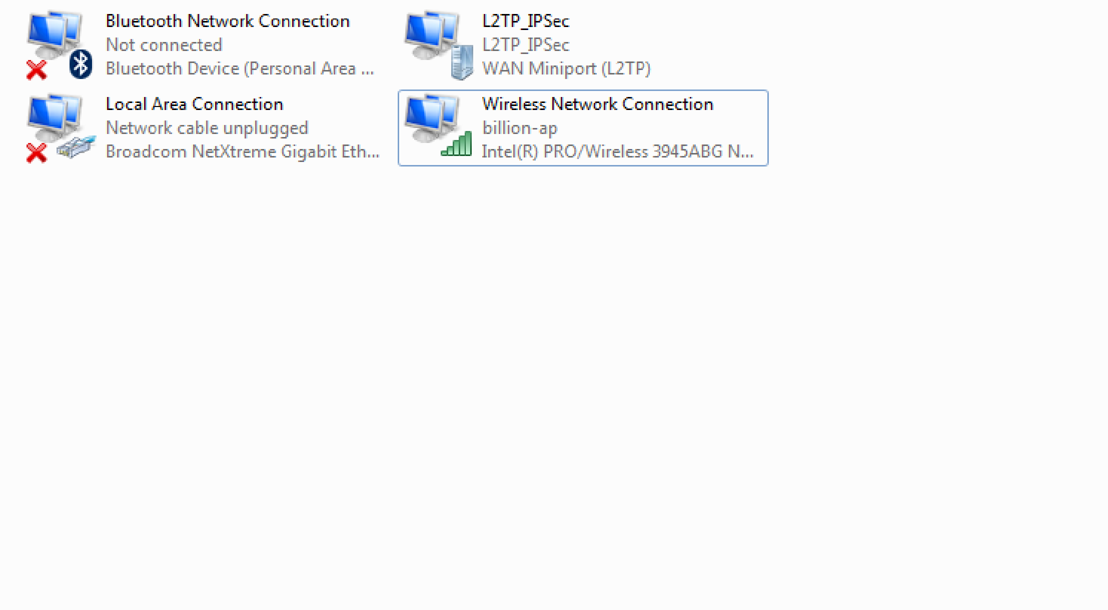


Connect to a Workplace

The connection is ready to use

Connect now

7. Go to **Network Connections** shown below to check the detail of the connection. Right click "L2TP_IPSec" icon, and select "**Properties**" to change the security parameters.



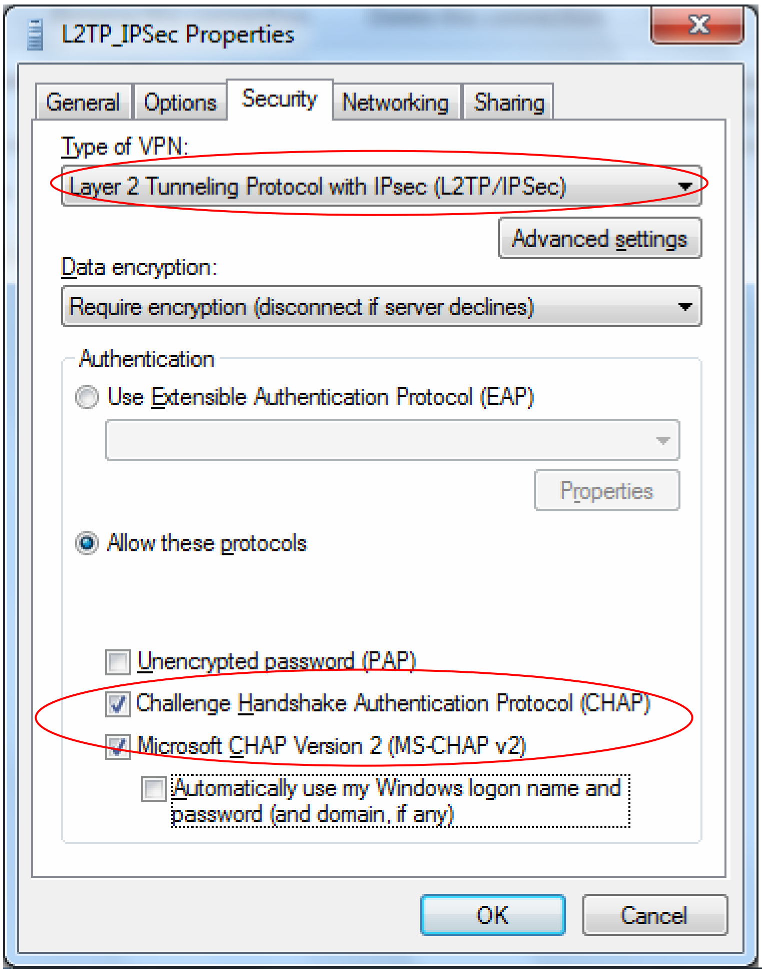
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

L2TP_IPSec
L2TP_IPSec
WAN Miniport (L2TP)

Local Area Connection
Network cable unplugged
Broadcom NetXtreme Gigabit Eth...

Wireless Network Connection
billion-ap
Intel(R) PRO/Wireless 3945ABG N...

8. Chang the type of VPN to “**Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)**” and Click Advanced Settings to set the pre-shared (set in IPSec) key for authentication.



L2TP_IPSec Properties

Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption:
Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

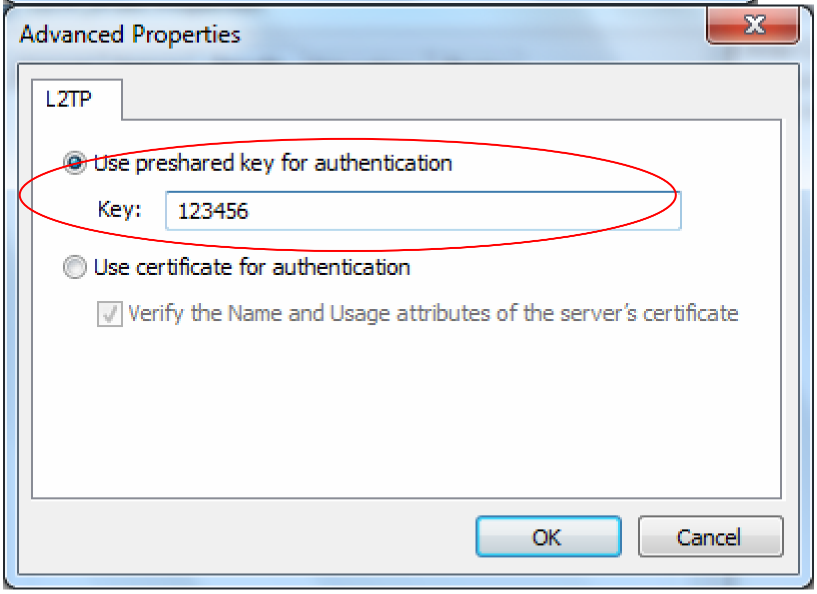
● Allow these protocols

□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)



Advanced Properties

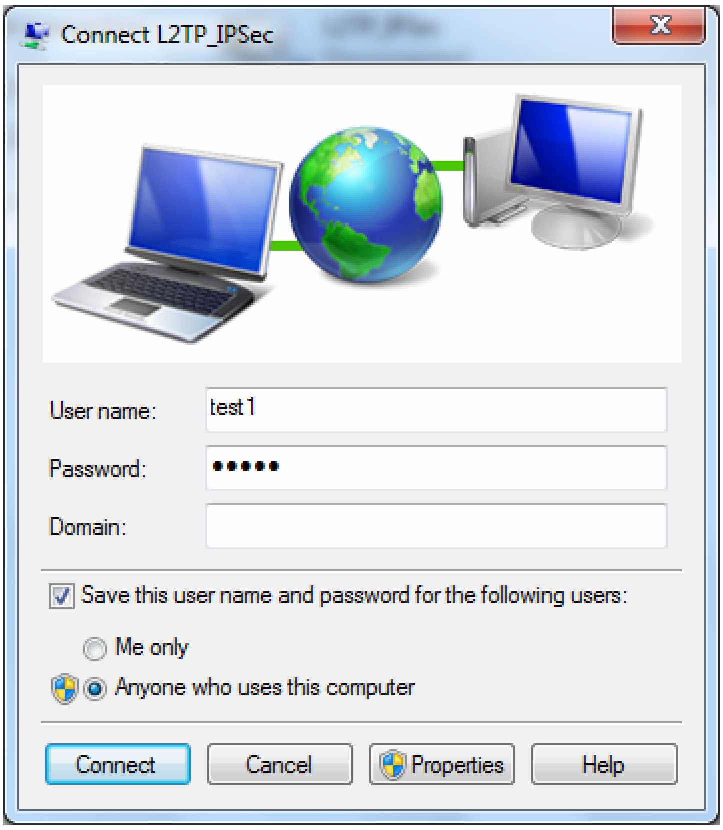
● Use preshared key for authentication

Key: 123456

○ Use certificate for authentication

☑ Verify the Name and Usage attributes of the server’s certificate

9. Go to **Network connections**, enter username and password to connect L2TP_IPSec and check the connection status.



User name: test1

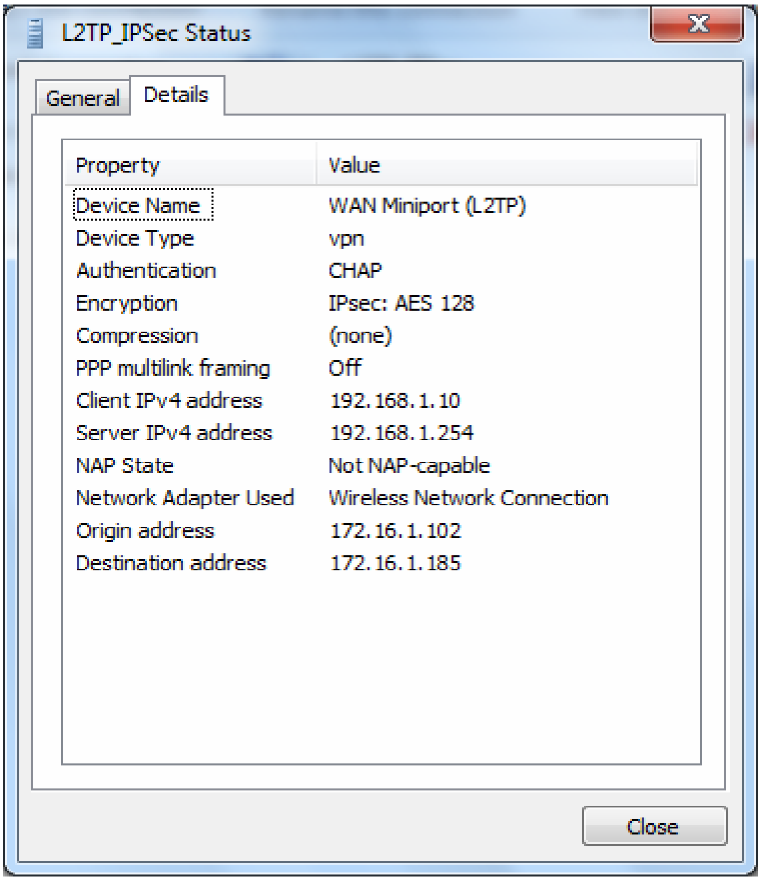
Password: •••••

Domain:

☑ Save this user name and password for the following users:

○ Me only

● Anyone who uses this computer

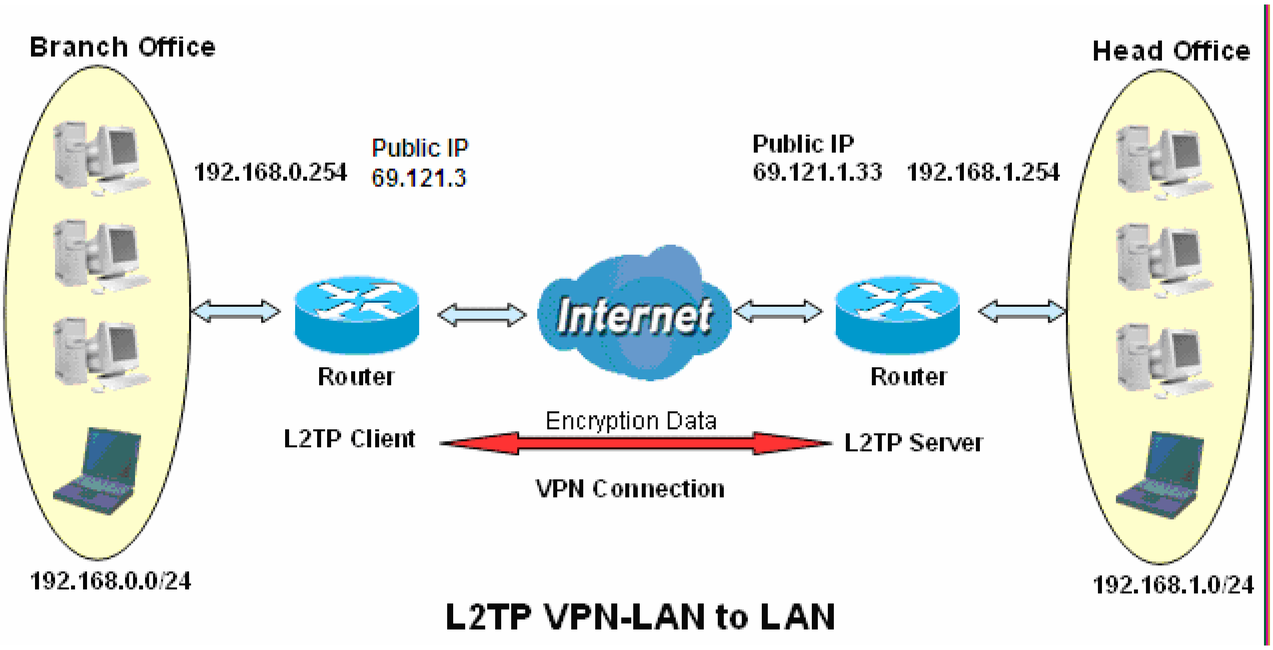


Property	Value
Device Name	WAN Miniport (L2TP)
Device Type	vpn
Authentication	CHAP
Encryption	IPsec: AES 128
Compression	(none)
PPP multilink framing	Off
Client IPv4 address	192.168.1.10
Server IPv4 address	192.168.1.254
NAP State	Not NAP-capable
Network Adapter Used	Wireless Network Connection
Origin address	172.16.1.102
Destination address	172.16.1.185

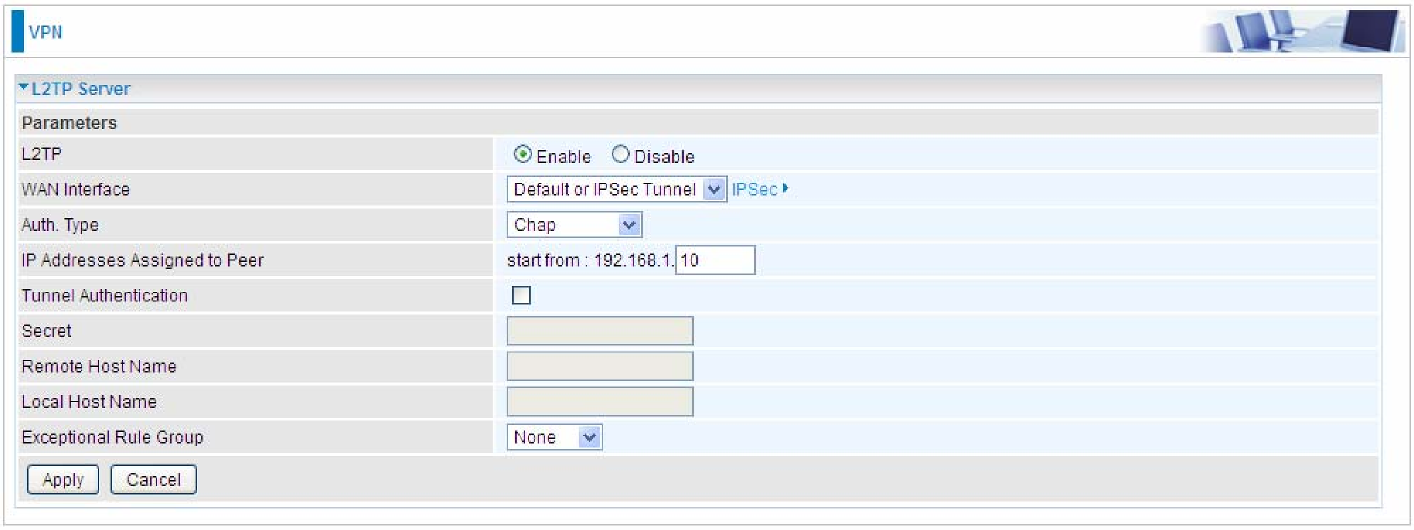
Example: Configuring L2TP LAN-to-LAN VPN Connection

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

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.

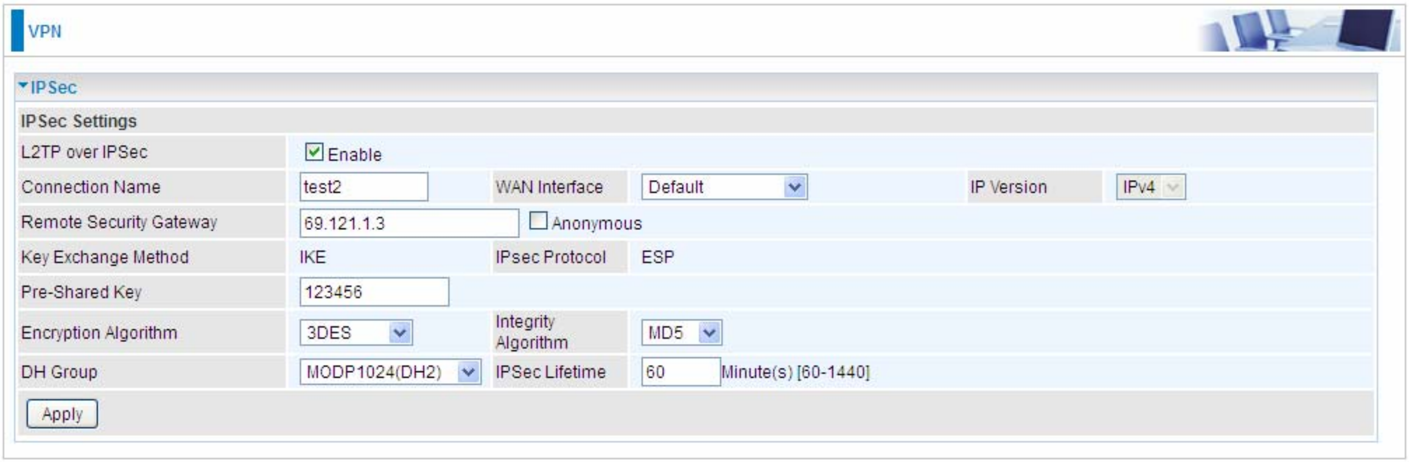


Server side: Head Office



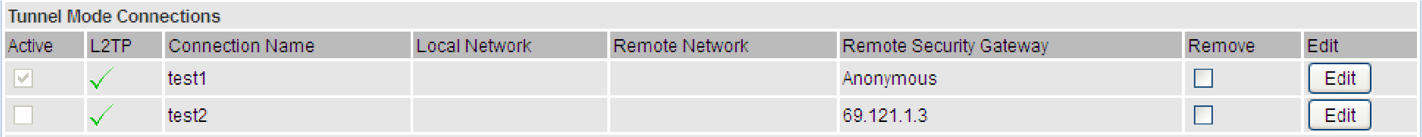
Parameters

L2TP	● Enable ○ Disable
WAN Interface	Default or IPSec Tunnel IPSec ▸
Auth. Type	Chap
IP Addresses Assigned to Peer	start from : 192.168.1. 10
Tunnel Authentication	□
Secret	
Remote Host Name	
Local Host Name	
Exceptional Rule Group	None



IPSec Settings

L2TP over IPSec	☑ Enable				
Connection Name	test2	WAN Interface	Default	IP Version	IPv4
Remote Security Gateway	69.121.1.3 □ Anonymous				
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	123456				
Encryption Algorithm	3DES	Integrity Algorithm	MD5		
DH Group	MODP1024(DH2)	IPSec Lifetime	60 Minute(s) [60-1440]		

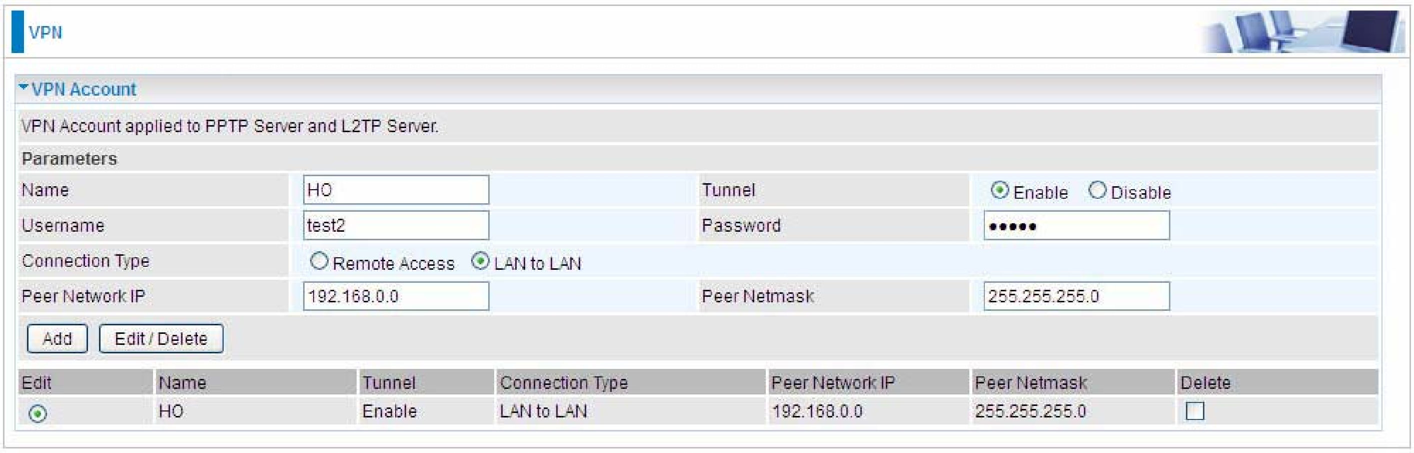


Tunnel Mode Connections

Active	L2TP	Connection Name	Local Network	Remote Network	Remote Security Gateway	Remove	Edit
☑	✓	test1			Anonymous	□	Edit
□	✓	test2			69.121.1.3	□	Edit

The above is the commonly setting for L2TP Server, set as you like for authentication and encryption. The settings in Client side should be in accordance with settings in Server side.

Then account the L2TP Account.



VPN

VPN Account

VPN Account applied to PPTP Server and L2TP Server.

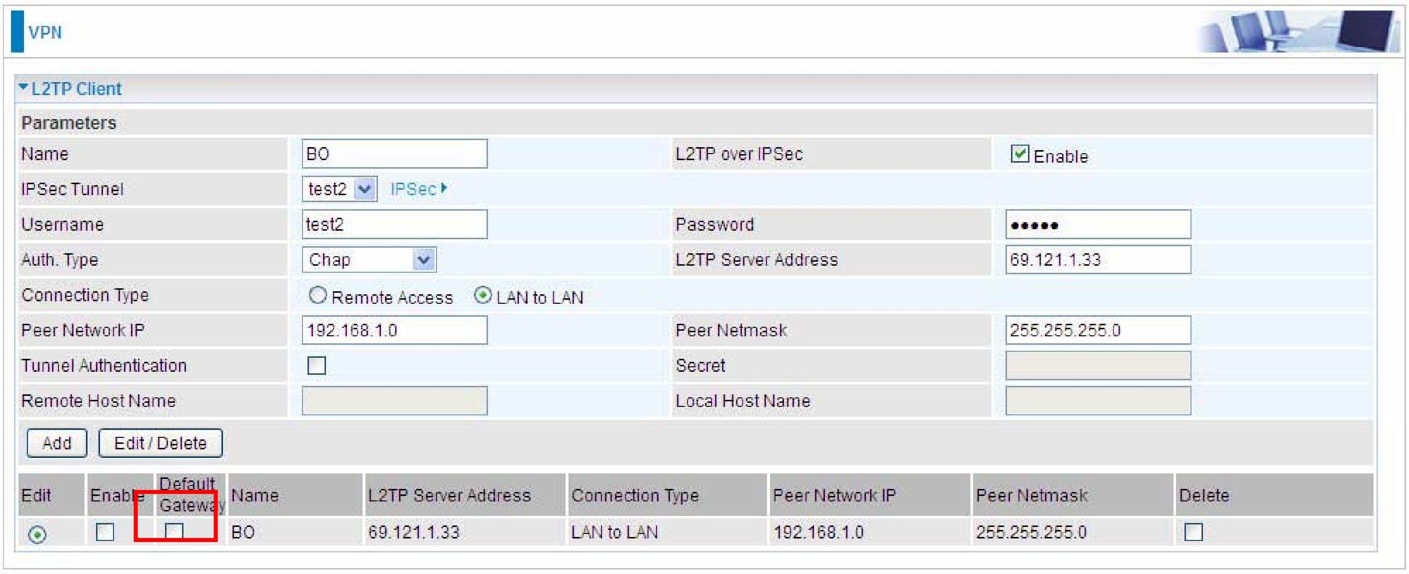
Parameters

Name	HO	Tunnel	● Enable ○ Disable
Username	test2	Password	•••••
Connection Type	○ Remote Access ● LAN to LAN		
Peer Network IP	192.168.0.0	Peer Netmask	255.255.255.0

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
●	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	□

Client Side: Branch Office

The client user can set up a tunnel connecting to the PPTP server, and can also set the tunnel as the default route for all outgoing traffic.



▾L2TP Client

Parameters

Name	BO	L2TP over IPSec	☑ Enable
IPSec Tunnel	test2 IPSec ▸		
Username	test2	Password	●●●●●
Auth. Type	Chap	L2TP Server Address	69.121.1.33
Connection Type	○ Remote Access ● LAN to LAN		
Peer Network IP	192.168.1.0	Peer Netmask	255.255.255.0
Tunnel Authentication	□	Secret	
Remote Host Name		Local Host Name	

Add | Edit / Delete

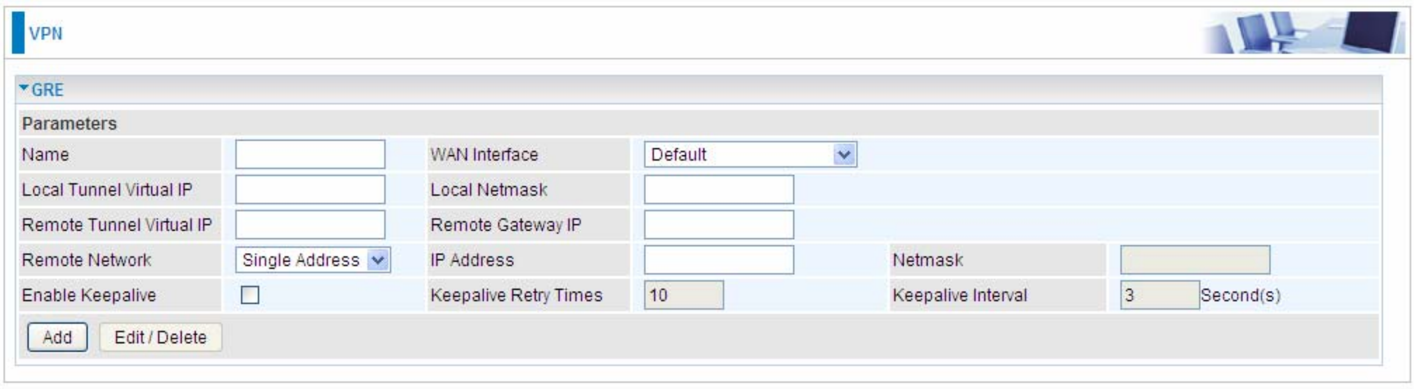
Edit	Enable	Default Gateway	Name	L2TP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
●	□	□	BO	69.121.1.33	LAN to LAN	192.168.1.0	255.255.255.0	□

Note: users can see the "Default Gateway" item in the bar, and user can check to select the tunnel as the default gateway (default route) for traffic. If selected, all outgoing traffic will be forwarded to this tunnel and routed to the next hop.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an Internet Protocol (IP) network. And the common use can be GRE over IPSec.

Note: up to 8 tunnels can be added, but only 4 can be activated.



VPN

GRE

Parameters

Name		WAN Interface	Default		
Local Tunnel Virtual IP		Local Netmask			
Remote Tunnel Virtual IP		Remote Gateway IP			
Remote Network	Single Address	IP Address		Netmask	
Enable Keepalive	□	Keepalive Retry Times	10	Keepalive Interval	3 Second(s)

Name: User-defined identification.

WAN Interface: Select the exact WAN interface configured for the tunnel as the source tunnel IP. Select Default to use the now-working WAN interface for the tunnel.

Local Tunnel Virtual IP: Please input the virtual IP for the local tunnel.

Local Netmask: Input the netmask for the local tunnel.

Remote Tunnel Virtual IP: Please input the virtual destination IP for tunnel.

Remote Gateway IP: Set the destination IP for the tunnel.

Remote Network: Select the peer topology, Single address (client) or Subnet.

IP Address: Set the IP address if the peer is a client. If the peer is a subnet, please enter the IP and netmask.

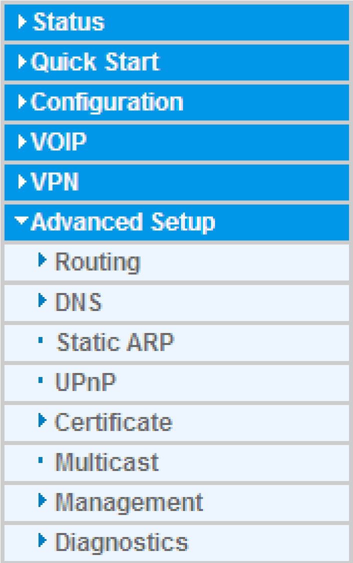
Enable Keepalive: Normally, the tunnel interface is always up. Enable keepalive to determine when the tunnel interface is to be closed. The local router sends keepalive packets to the peer router, if keepalive response is not received from peer router within the allowed time ('retry time' multiply 'interval', based on default settings, the time interval can be 30 seconds), the local router will shut up its tunnel interface.

Keepalive Retry Times: Set the keepalive retry times, default is 10.

Keepalive Interval: Set the keepalive Interval, unit in seconds. Default is 3 seconds.

Advanced Setup

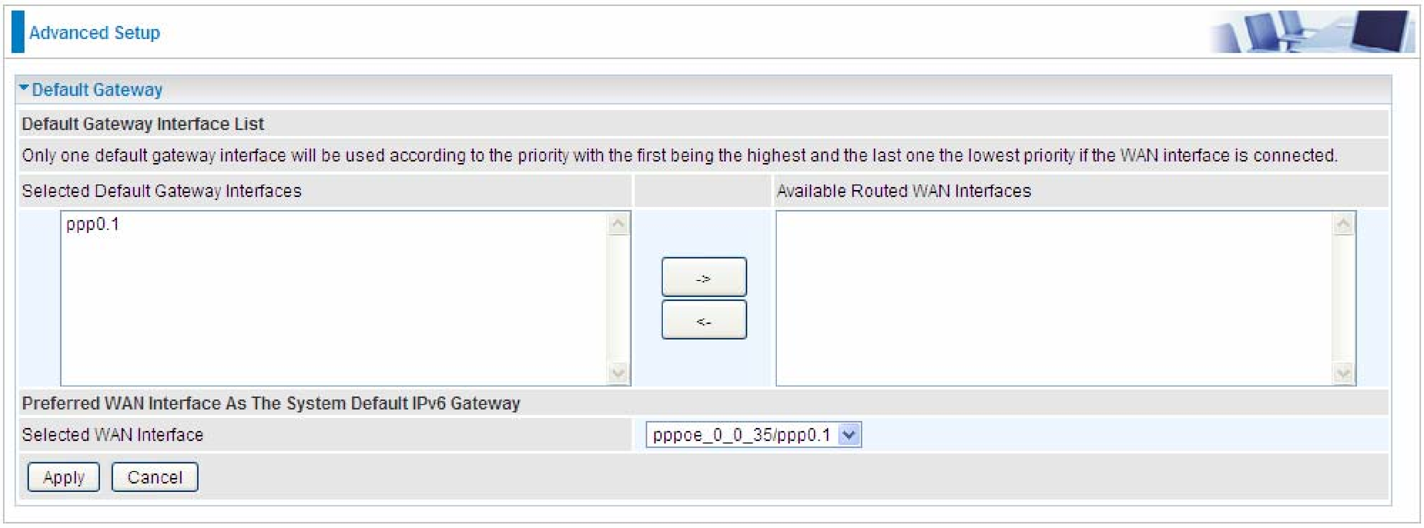
There are sub-items within the System section: **Routing**, **DNS**, **Static ARP, UPnP**, **Certificate**, **Multicast**, **Management**, and **Diagnostics.**



(7800VDOX)

Routing

Default Gateway



Default Gateway Interface List

Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Selected Default Gateway Interfaces	Available Routed WAN Interfaces
ppp0.1	

Preferred WAN Interface As The System Default IPv6 Gateway

Selected WAN Interface: pppoe_0_0_35/ppp0.1

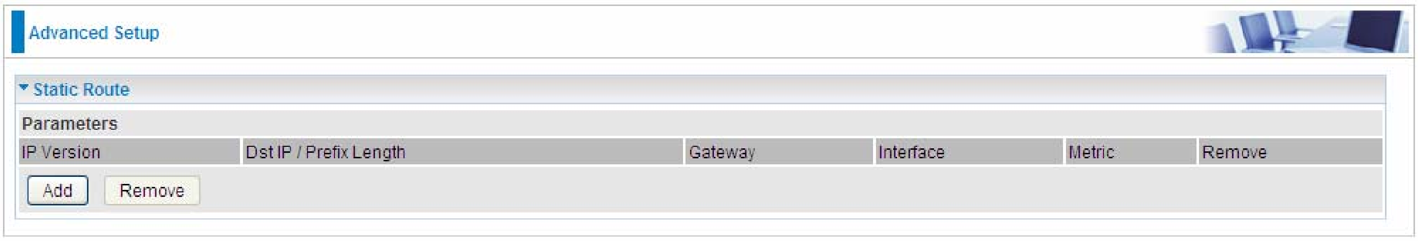
WAN port: Select the port this gateway applies to.

To set ***Default Gateway*** and ***Available Routed WAN Interface***. This interfaces are the ones you have set in WAN section, here select the one you want to be the default gateway by moving the interface via -> or <-. And select a Default IPv6 Gateway from the drop-down menu.

Note: Only one default gateway interface will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Static Route

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



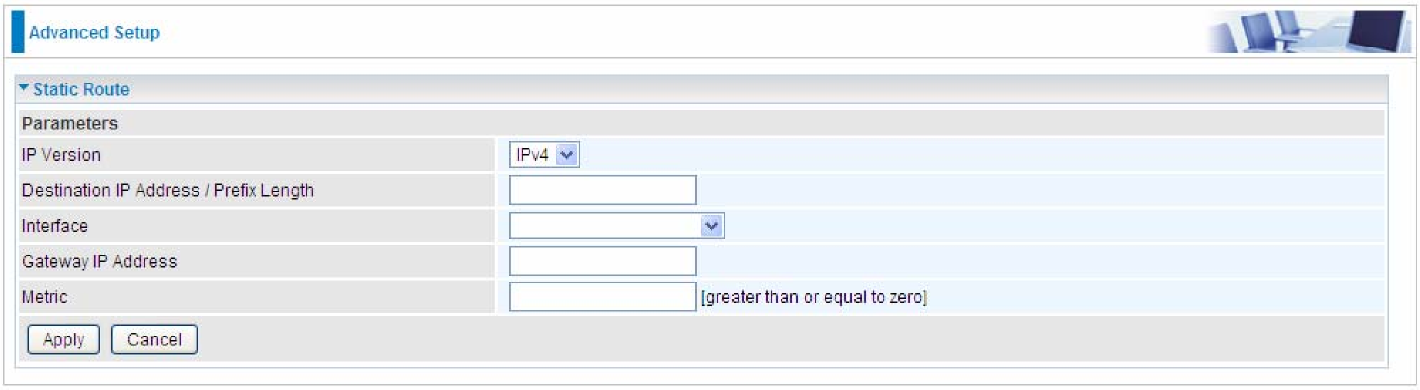
Advanced Setup

Static Route

Parameters

IP Version	Dst IP / Prefix Length	Gateway	Interface	Metric	Remove

Above is the static route listing table, click **Add** to create static routing.



Advanced Setup

Static Route

Parameters

IP Version	IPv4
Destination IP Address / Prefix Length	
Interface	
Gateway IP Address	
Metric	[greater than or equal to zero]

IP Version: Select the IP version, IPv4 or IPv6.

Destination IP Address / Prefix Length: Enter the destination IP address and the prefix length. For IPv4, the prefix length means the number of '1' in the submask, it is another mode of presenting submask. One IPv4 address,192.168.1.0/24, submask is 255.255.255.0. While in IPv6, IPv6 address composes of two parts, thus, the prefix and the interface ID, the prefix is like the net ID in IPv4, and the interface ID is like the host ID in IPv4. The prefix length is to identify the net ID in the address. One IPv6 address, 3FFE:FFFF:0:CD30:0:0:0:0 / 64, the prefix is 3FFE:FFFF:0:CD3.

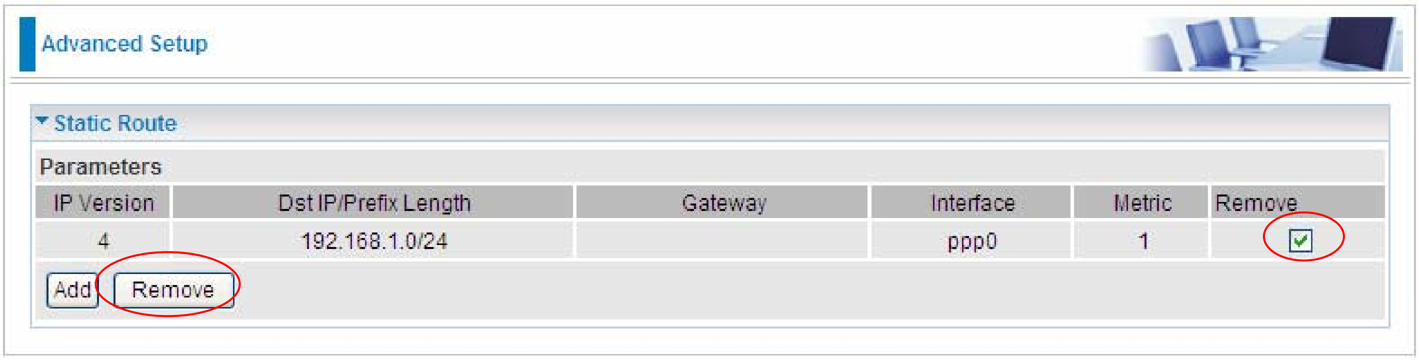
Interface: Select an interface this route associated.

Gateway IP Address: Enter the gateway IP address.

Metric: Metric is a policy for router to commit router, to determine the optimal route. Enter one number greater than or equal to 0.

Click **Apply** to apply this route and it will be listed in the route listing table.

In listing table you can remove the one you don't want by checking the checking box and press **Remove** button.



Advanced Setup

Static Route

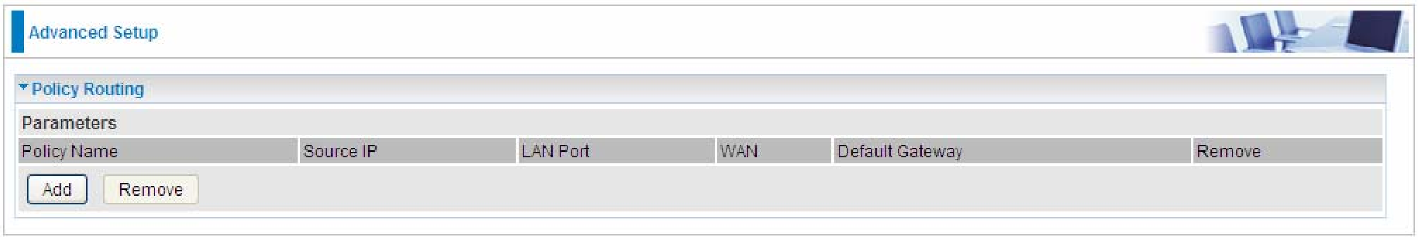
Parameters

IP Version	Dst IP/Prefix Length	Gateway	Interface	Metric	Remove
4	192.168.1.0/24		ppp0	1	☑

Policy Routing

Here users can set a route for the host (source IP) in a LAN interface to access outside through a specified Default Gateway or a WAN interface.

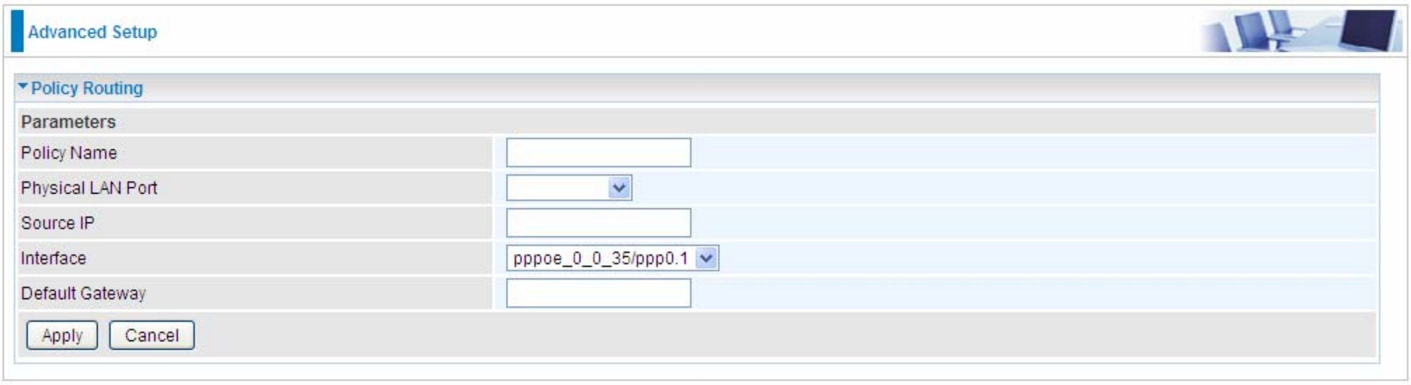
The following is the policy Routing listing table.



Parameters

Policy Name	Source IP	LAN Port	WAN	Default Gateway	Remove

Click **Add** to create a policy route.



Parameters

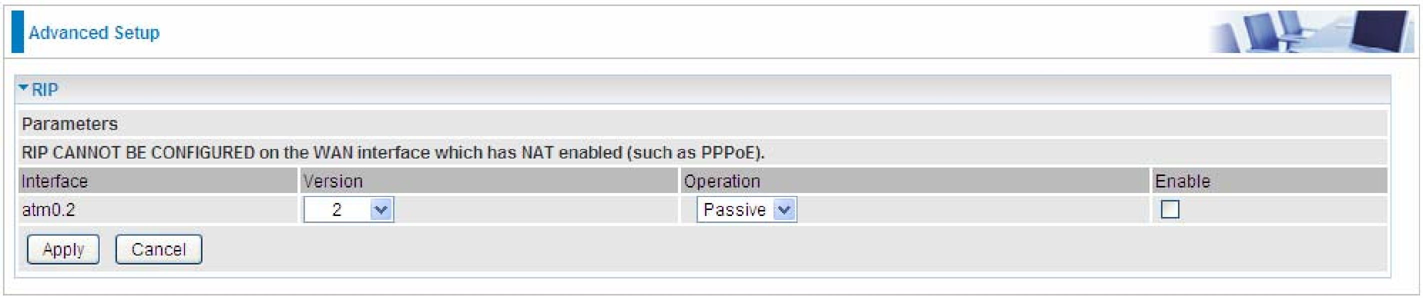
Policy Name	
Physical LAN Port	
Source IP	
Interface	pppoe_0_0_35/ppp0.1
Default Gateway	

Policy Name: User-defined name.
Physical LAN Port: Select the LAN port.
Source IP: Enter the Host Source IP.
Interface: Select the WAN interface which you want the Source IP to access outside through.
Default Gateway: Enter the default gateway which you want the Source IP to access outside through.

Click **Apply** to apply your settings. And the item will be listed in the policy Routing listing table. Here if you want to remove the route, check the remove checkbox and press **Remove** to delete it.

RIP

RIP, Router Information Protocol, is a simple Interior Gateway Protocol (IGP). RIP has two versions, RIP-1 and RIP-2.



Parameters

RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

Interface	Version	Operation	Enable
atm0.2	2	Passive	□

Interface: the interface the rule applies to.

Version: select the RIP version, there are two versions, RIP-1 and RIP-2.

Operation: RIP has two operation mode.

- **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- **Active:** working in this mode, the router sends and receives RIP routing information and modifies routing table according to the received information.

Enable: check the checkbox to enable RIP rule for the interface.

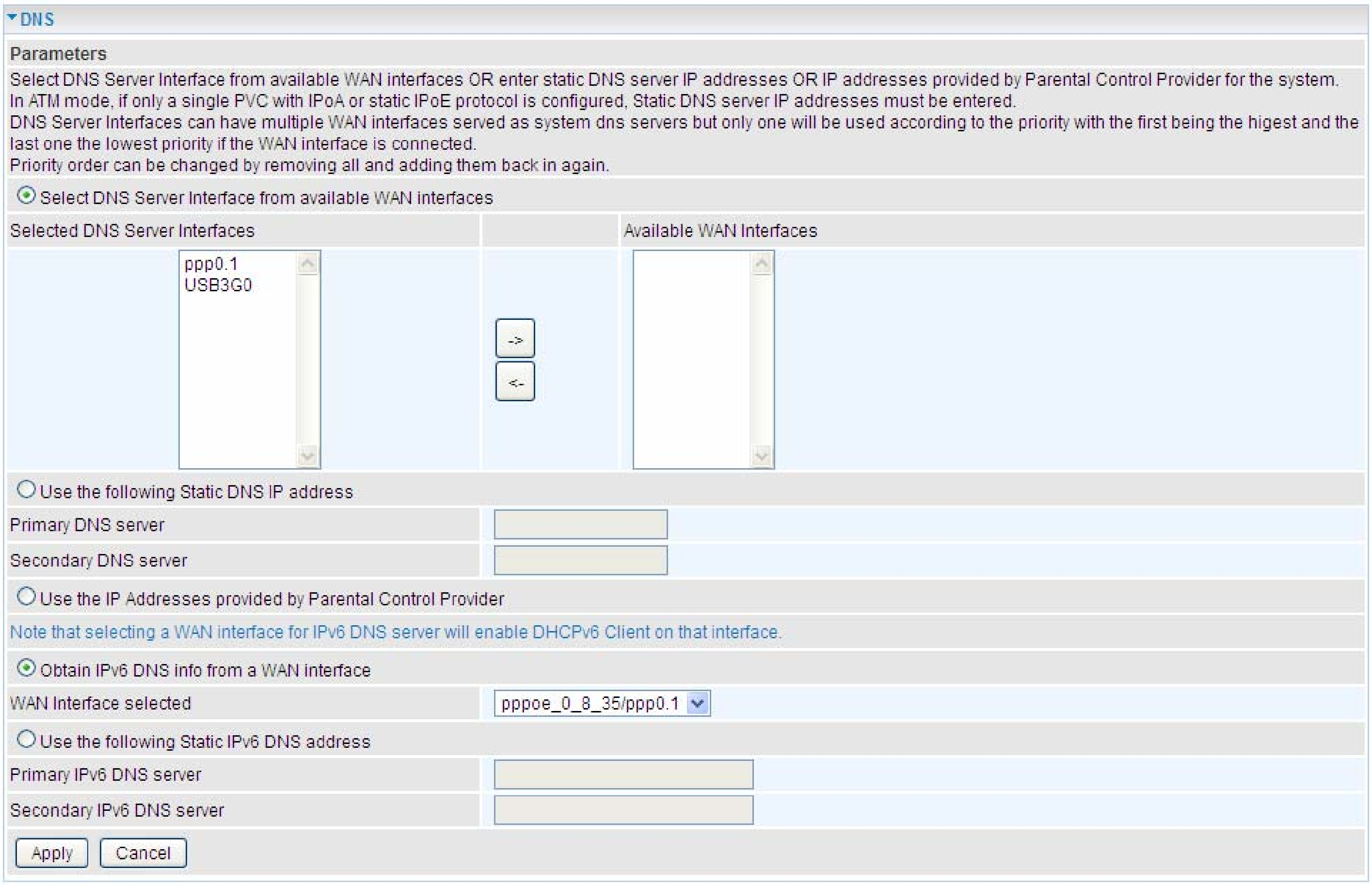
Note: RIP can't be configured on the WAN interface which has NAT enabled (such as PPPoE).

Click **Apply** to apply your settings.

DNS

DNS, Domain Name System, is a distributed database of TCP/IP application. DNS provides translation from Domain name to IP.

DNS



▾DNS

Parameters

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses OR IP addresses provided by Parental Control Provider for the system.
In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.
Priority order can be changed by removing all and adding them back in again.

● Select DNS Server Interface from available WAN interfaces

Selected DNS Server Interfaces		Available WAN Interfaces
ppp0.1 USB3G0	-> <-	

○ Use the following Static DNS IP address

Primary DNS server	
Secondary DNS server	

○ Use the IP Addresses provided by Parental Control Provider

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

● Obtain IPv6 DNS info from a WAN interface

WAN Interface selected	pppoe_0_8_35/ppp0.1

○ Use the following Static IPv6 DNS address

Primary IPv6 DNS server	
Secondary IPv6 DNS server	

Apply Cancel

➤ IPv4

Three ways to set an IPv4 DNS server

- **Select DNS server from available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- **User the following Static DNS IP address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- **Use the IP address provided by Parental Control Provider:** If user registers and gets an DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at Parental Control Provider).

➤ IPv6:

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

Obtain IPv6 DNS info from a WAN interface

WAN Interface selected: Select one configured IPv6 WAN connection from the drop-down menu to be as an IPv6 DNS.

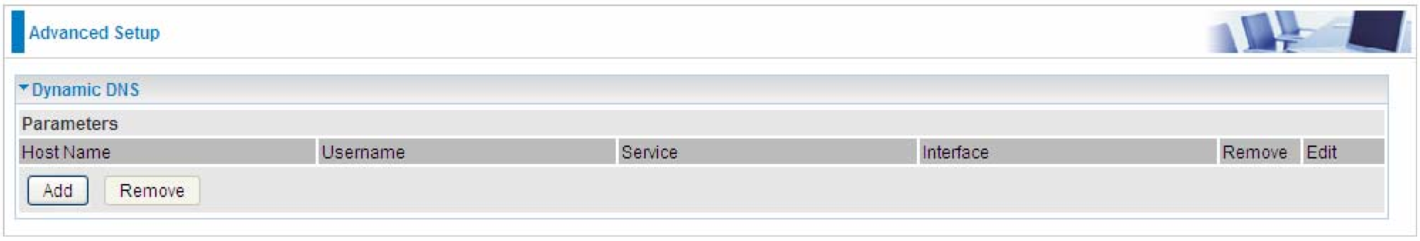
Use the following Static IPv6 DNS address

Primary IPv6 DNS Server / Secondary IPv6 DNS Server: Type the specific primary and secondary IPv6 DNS Server address.

Dynamic DNS

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

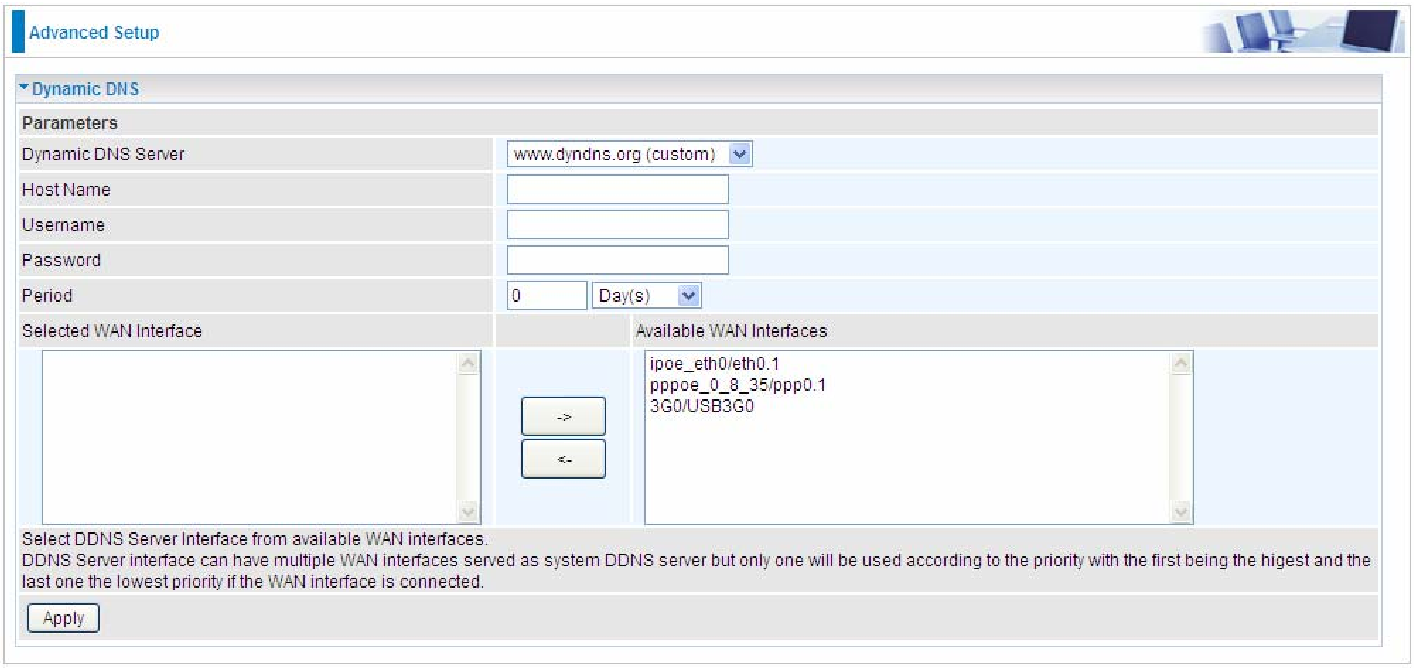
Here users can register different WAN interfaces with different DNS(es).



Parameters

Host Name	Username	Service	Interface	Remove	Edit

Click **Add** to register a WAN interface with the exact DNS.



Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	
Username	
Password	
Period	0 Day(s)

Selected WAN Interface	Available WAN Interfaces
	ipoe_eth0/eth0.1 pppoe_0_8_35/ppp0.1 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.

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

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

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

Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

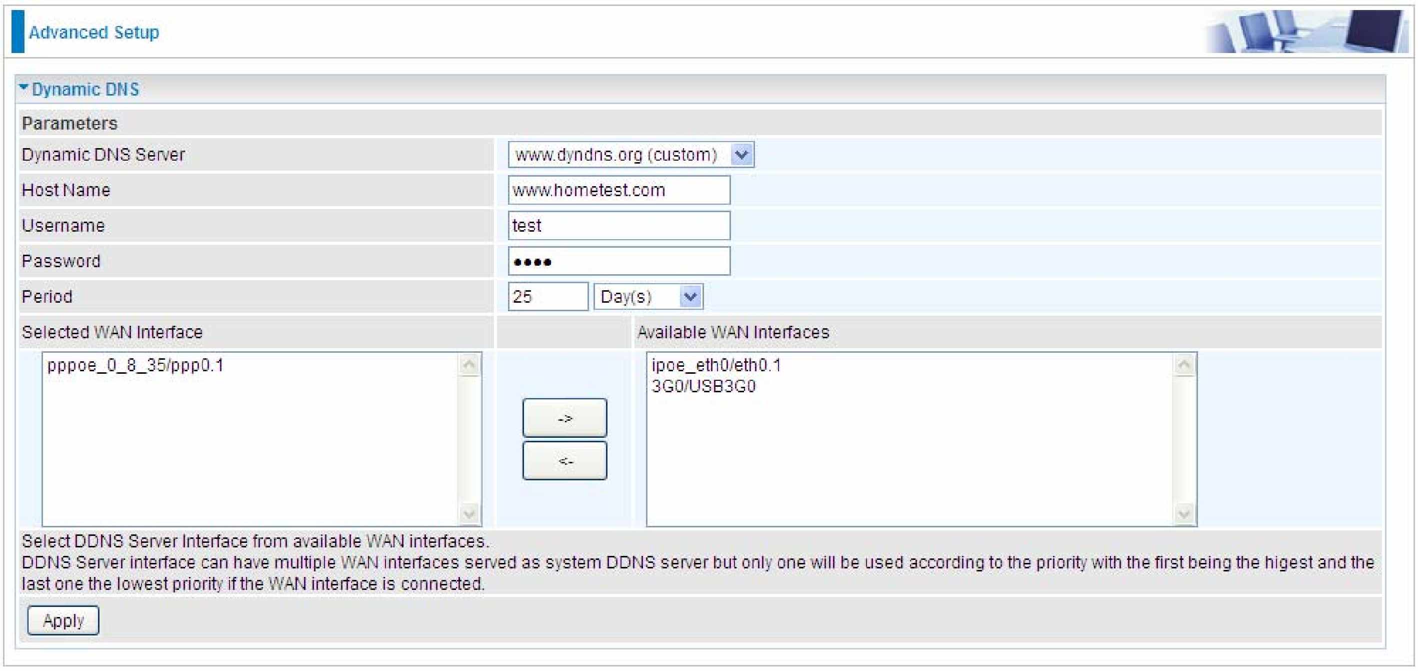
Selected WAN Interface: Select the Interface that is bound to the registered Domain name.

User can register different DDNS to different interfaces.

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User ***test*** register two Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

1. pppoe_0_8_35 with DDNS: www.hometest.com using username/password test/test



Advanced Setup

Dynamic DNS

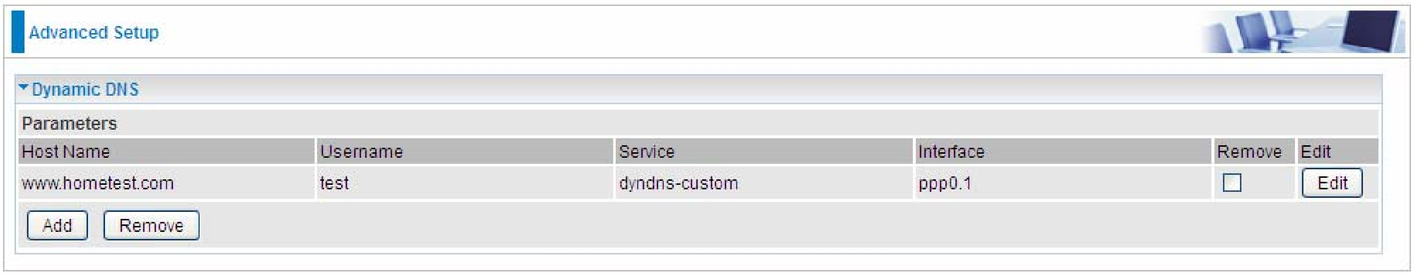
Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest.com
Username	test
Password	••••
Period	25 Day(s)

Selected WAN Interface		Available WAN Interfaces
pppoe_0_8_35/ppp0.1	-> <-	ipoe_eth0/eth0.1 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.

Apply



Advanced Setup

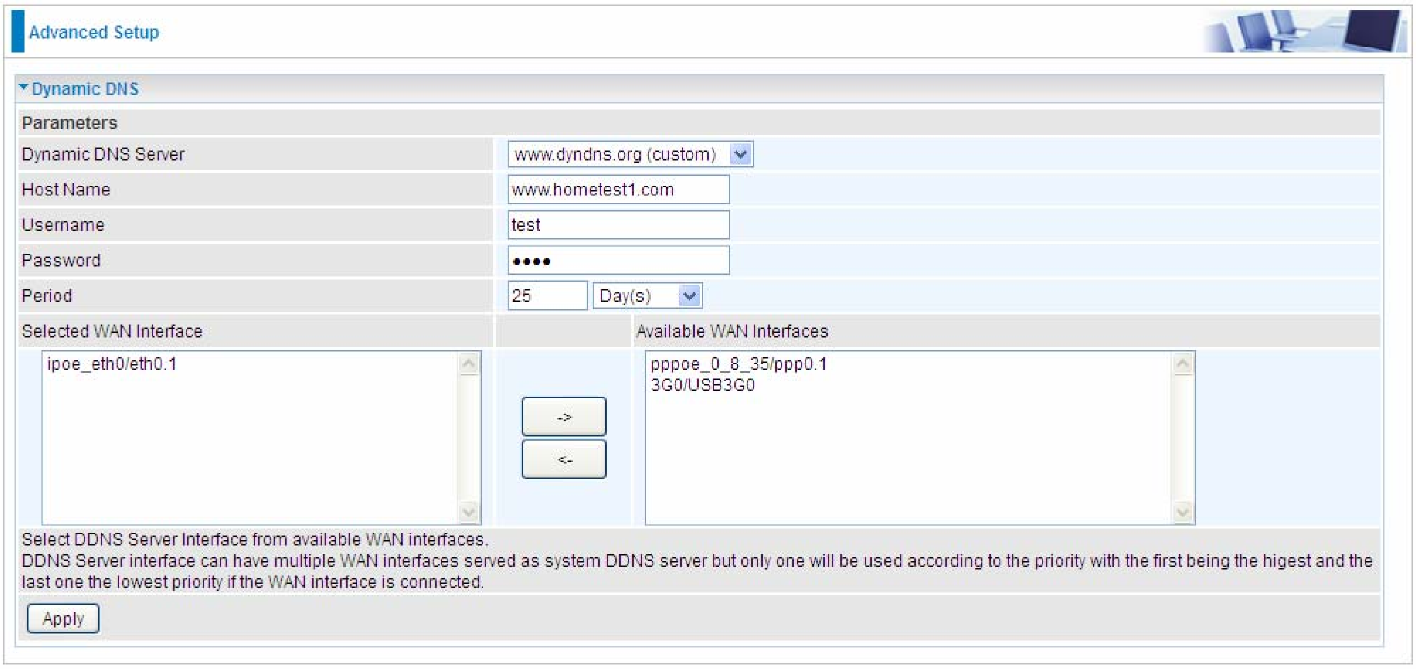
Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	□	Edit

Add Remove

2. ipoe_eth0 with DDNS: www.hometest1.com using username/password test/test.



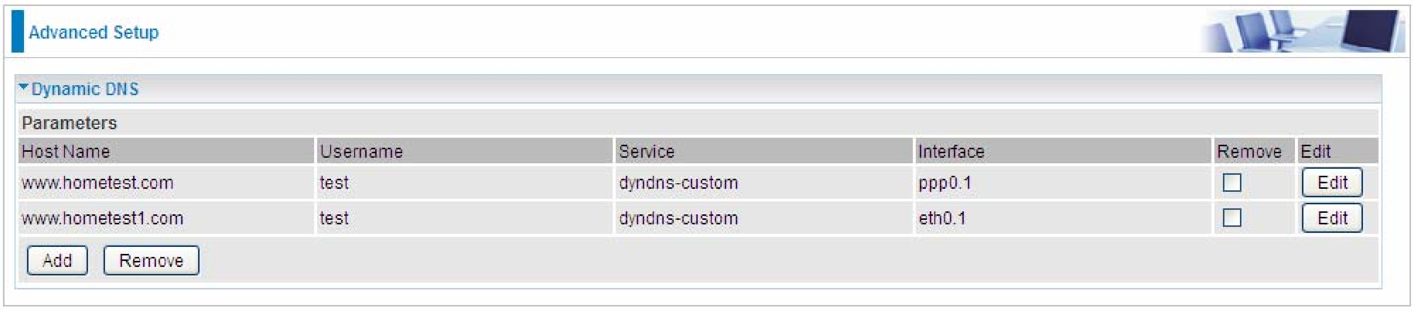
Advanced Setup

Dynamic DNS

Parameters	
Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest1.com
Username	test
Password	••••
Period	25 Day(s)

Selected WAN Interface		Available WAN Interfaces
ipoe_eth0/eth0.1	-> <-	pppoe_0_8_35/ppp0.1 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected.



Advanced Setup

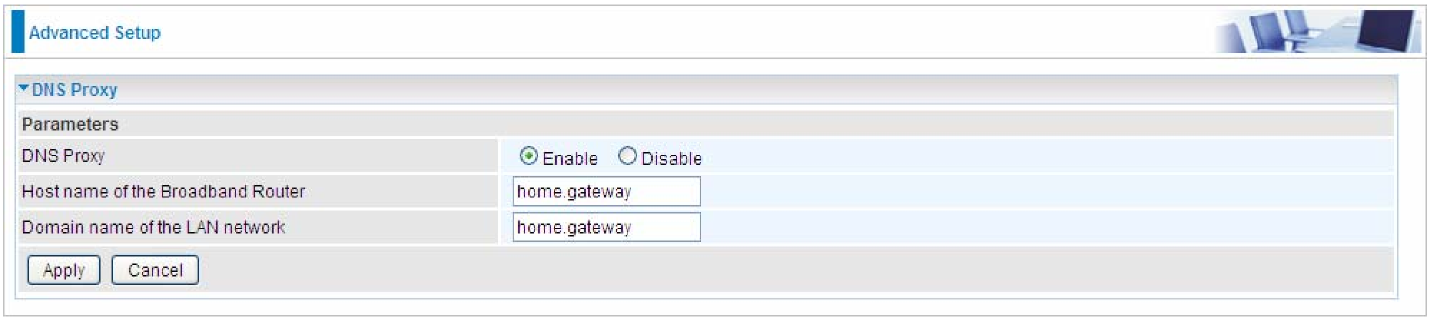
Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	□	Edit
www.hometest1.com	test	dyndns-custom	eth0.1	□	Edit

DNS Proxy

DNS proxy is used to forward request and response message between DNS Client and DNS Server. Hosts in LAN can use router serving as a DNS proxy to connect to the DNS Server in public to correctly resolve Domain name to access the internet.



Parameters	
DNS Proxy	● Enable ○ Disable
Host name of the Broadband Router	home.gateway
Domain name of the LAN network	home.gateway

DNS Proxy: Select whether to enable or disable DNS Proxy function, default is enabled.

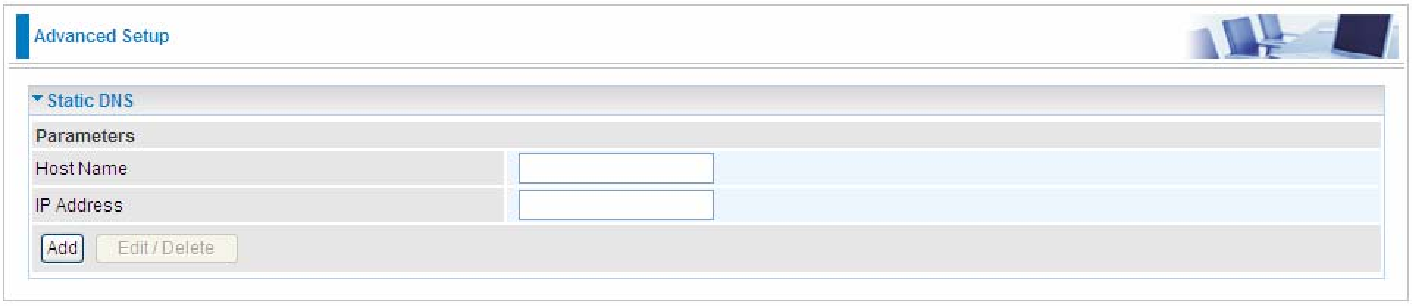
Host name of the Broadband Router: Enter the host name of the router. Default is home.gateway.

Domain name of the LAN network: Enter the domain name of the LAN network. home.gateway.

Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.



Advanced Setup

▾ Static DNS

Parameters	
Host Name	
IP Address	

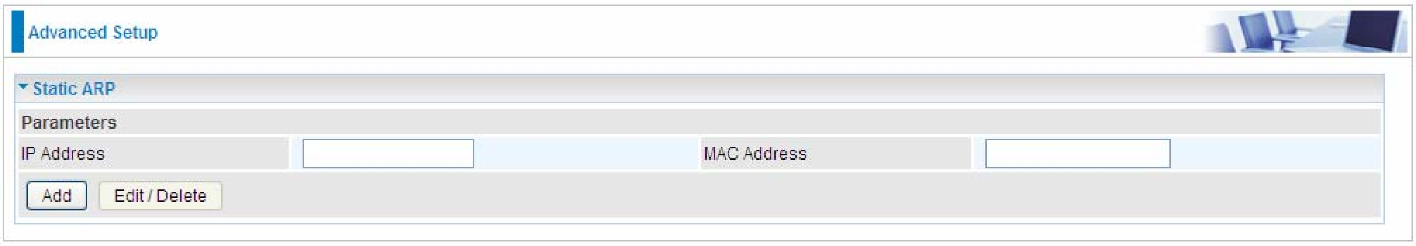
Host Name: Type the domain name (host name) for the specific IP .

IP Address: Type the IP address bound to the set host name above.

Click **Add** to save your settings.

Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.



IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

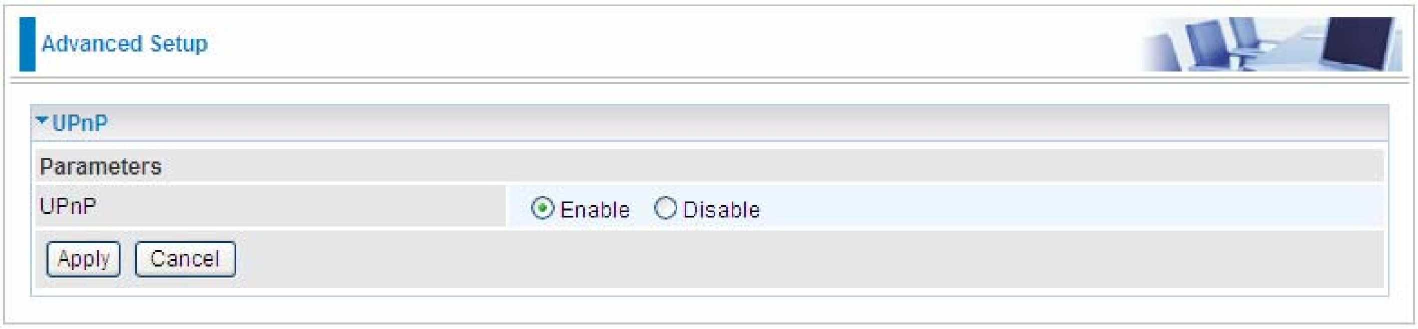
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click **Add** to confirm the settings.

UPnP

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

Both the user’s Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows Me natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



Advanced Setup

UPnP

Parameters

UPnP ● Enable ○ Disable

UPnP:

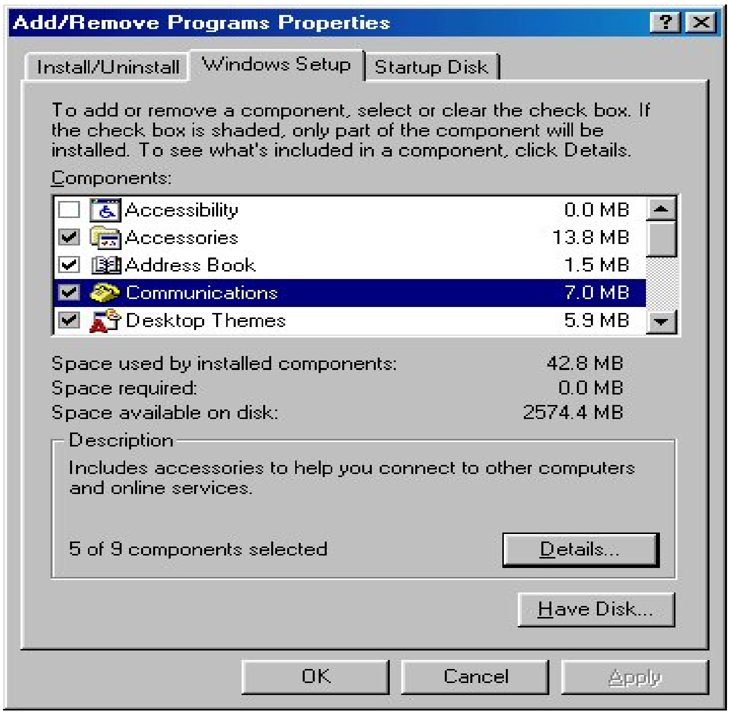
- **Enable:** Check to enable the router’s UPnP functionality.
- **Disable:** Check to disable the router’s UPnP functionality.

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

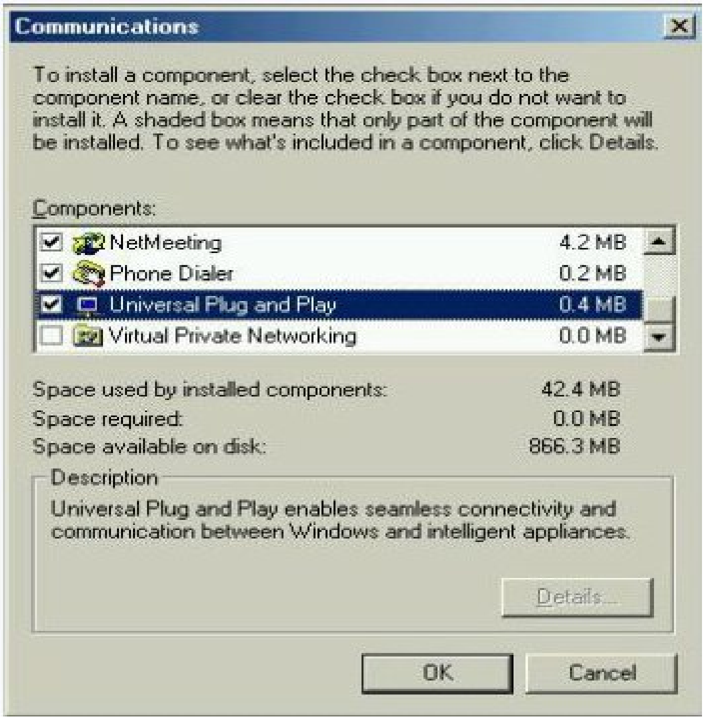
Space used by installed components:	42.8 MB
Space required:	0.0 MB
Space available on disk:	2574.4 MB

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

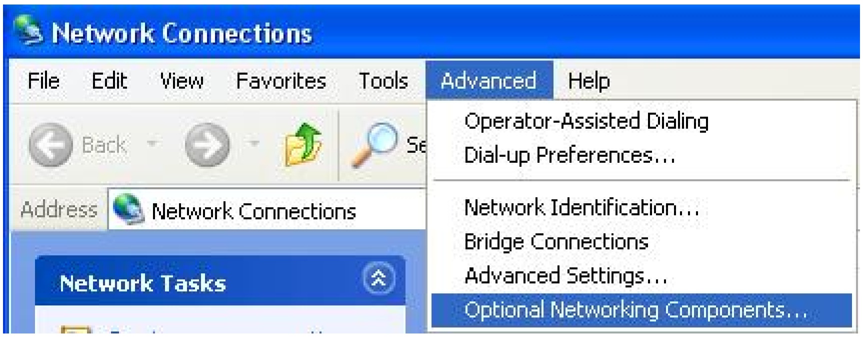
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

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

Step 5: Restart the computer when prompted.

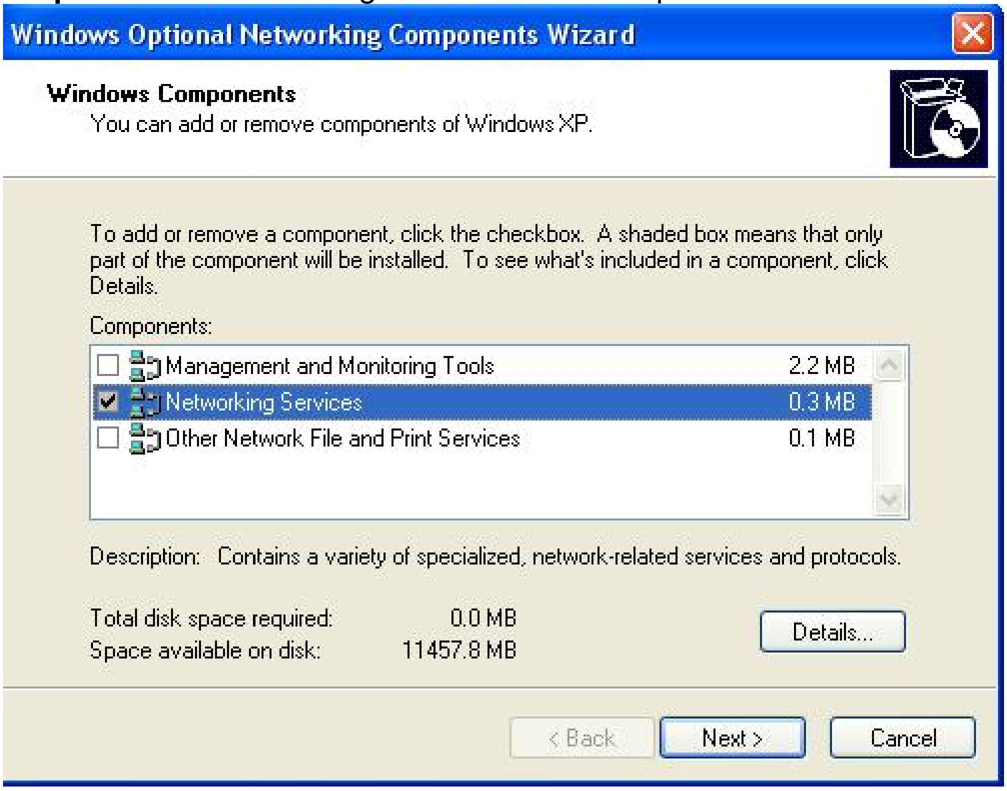
Follow the steps below to install the UPnP in Windows XP.

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 ….



The Windows Optional Networking Components Wizard window displays.

Step 4: Select Networking Service in the Components selection box and click Details.



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.

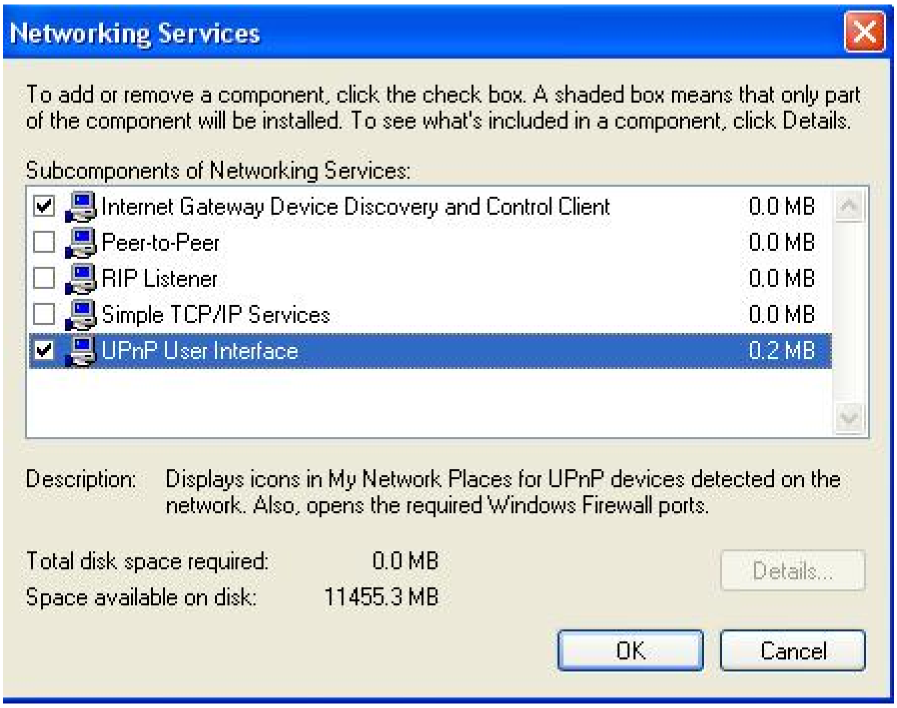
Components:

☐	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

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**.



Networking Services

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

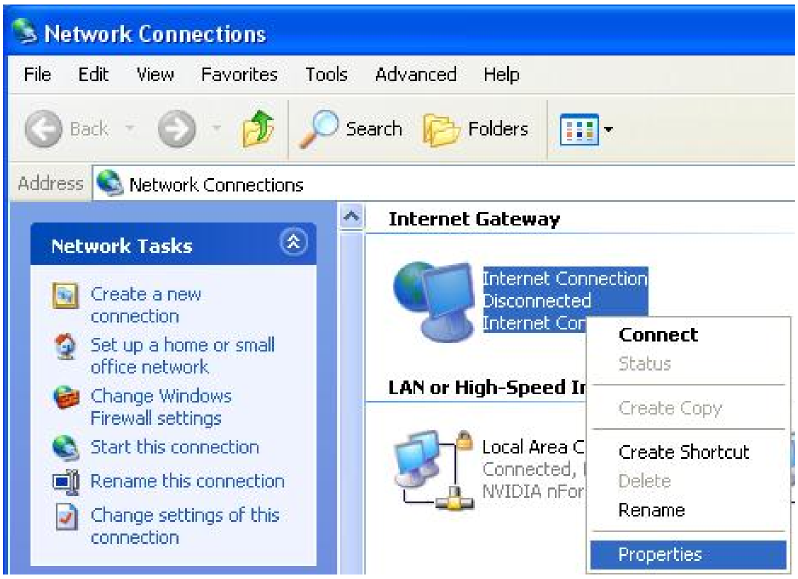
Description: Displays icons in My Network Places for UPnP devices detected on the network. Also, opens the required Windows Firewall ports.

Total disk space required: 0.0 MB

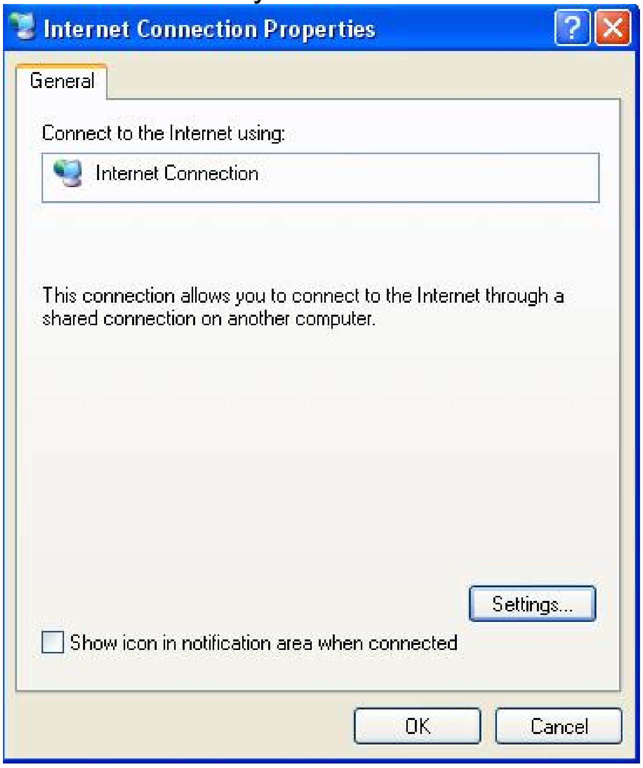
Space available on disk: 11455.3 MB

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

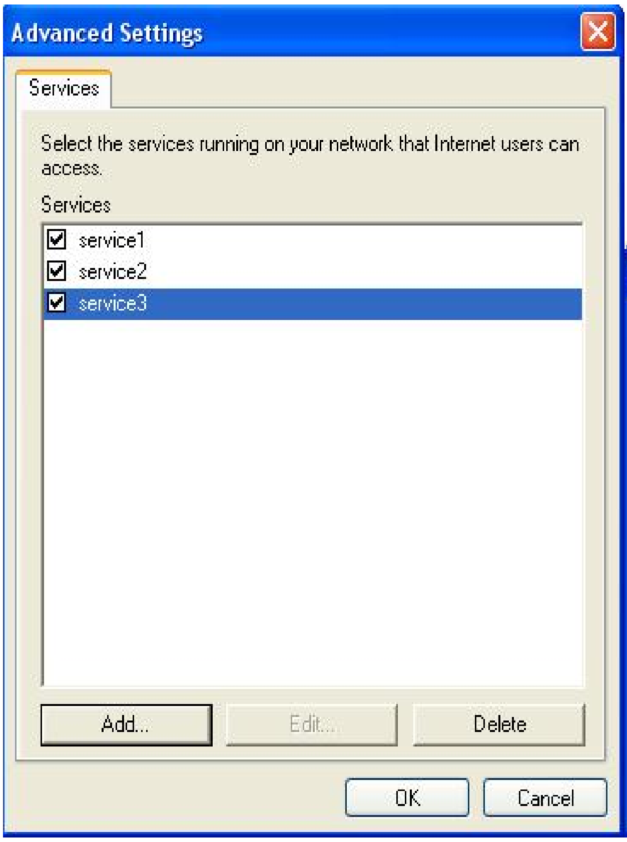
Connect to the Internet using:

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.



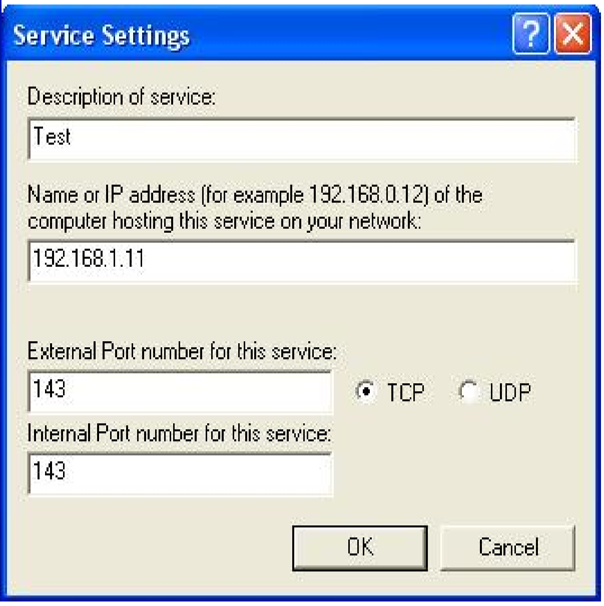
Advanced Settings

Services

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

Services

☑ service1
☑ service2
☑ service3



Service Settings

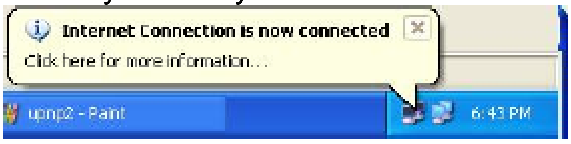
Description of service: Test

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

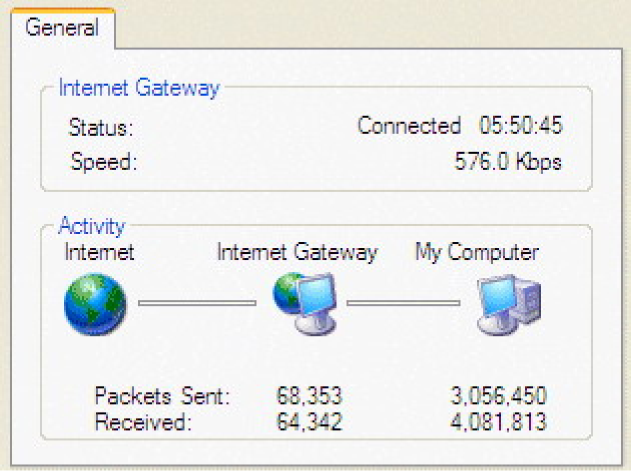
Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray



Internet Connection is now connected

Click here for more information...

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



General

Internet Gateway

Status: Connected 05:50:45

Speed: 576.0 Kbps

Activity

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

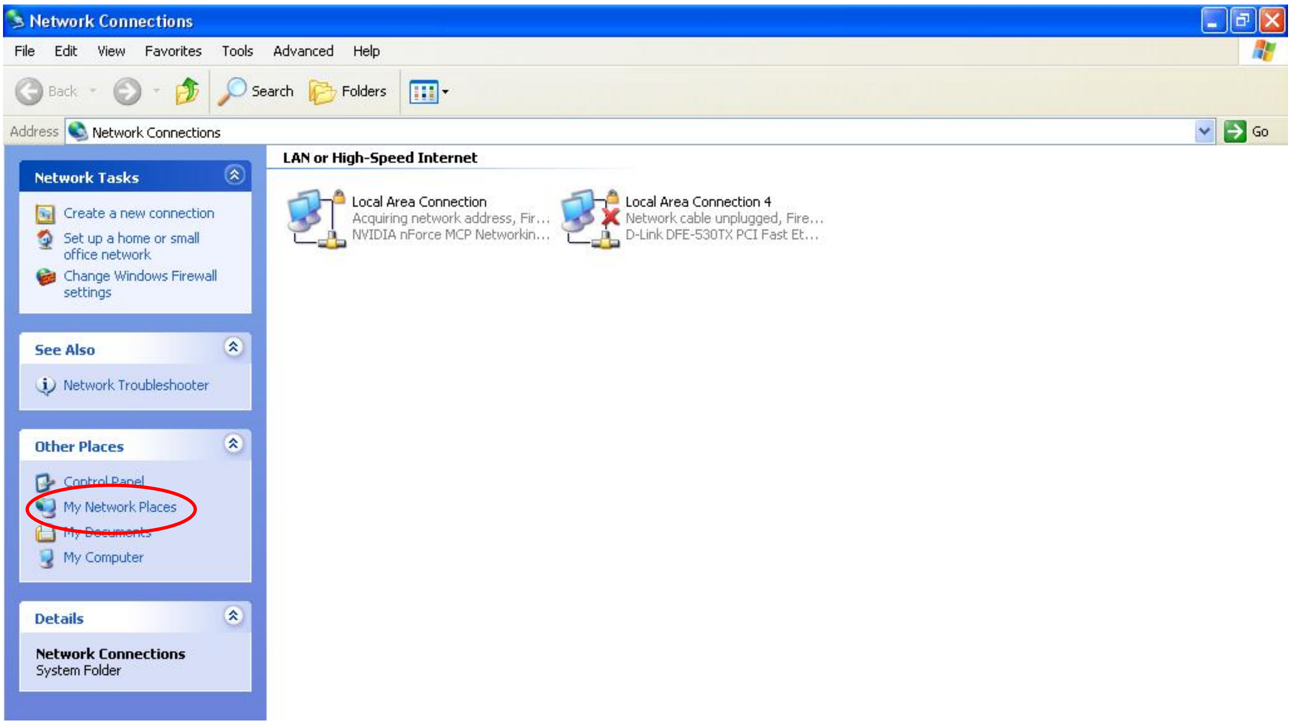
Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7800VDP(O)X 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.



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

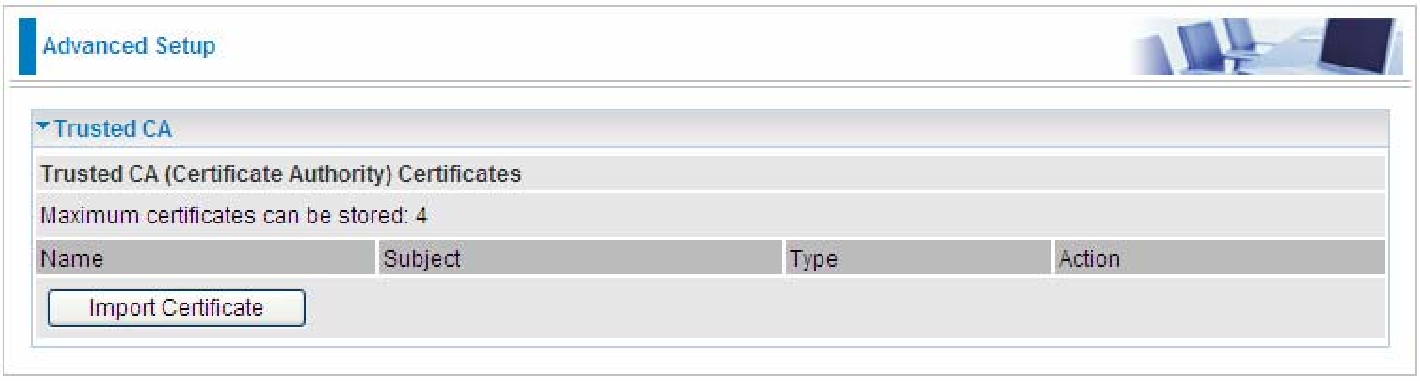
Step 5: Right-click on the icon of your BiPAC 7800VDP(O)X and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 7800VDP(O)X and select Properties. A properties window displays basic information about the BiPAC 7800VDP(O)X.

Certificate

This feature is used for TR069 ACS Server authentication of the device using certificate, if necessary. If the imported certificate doesn't match the authorized certificate of the ACS Server, the device will have no access to the server.

Trusted CA



Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action

Certificate Name: The certificate identification name.

Subject: The certificate subject.

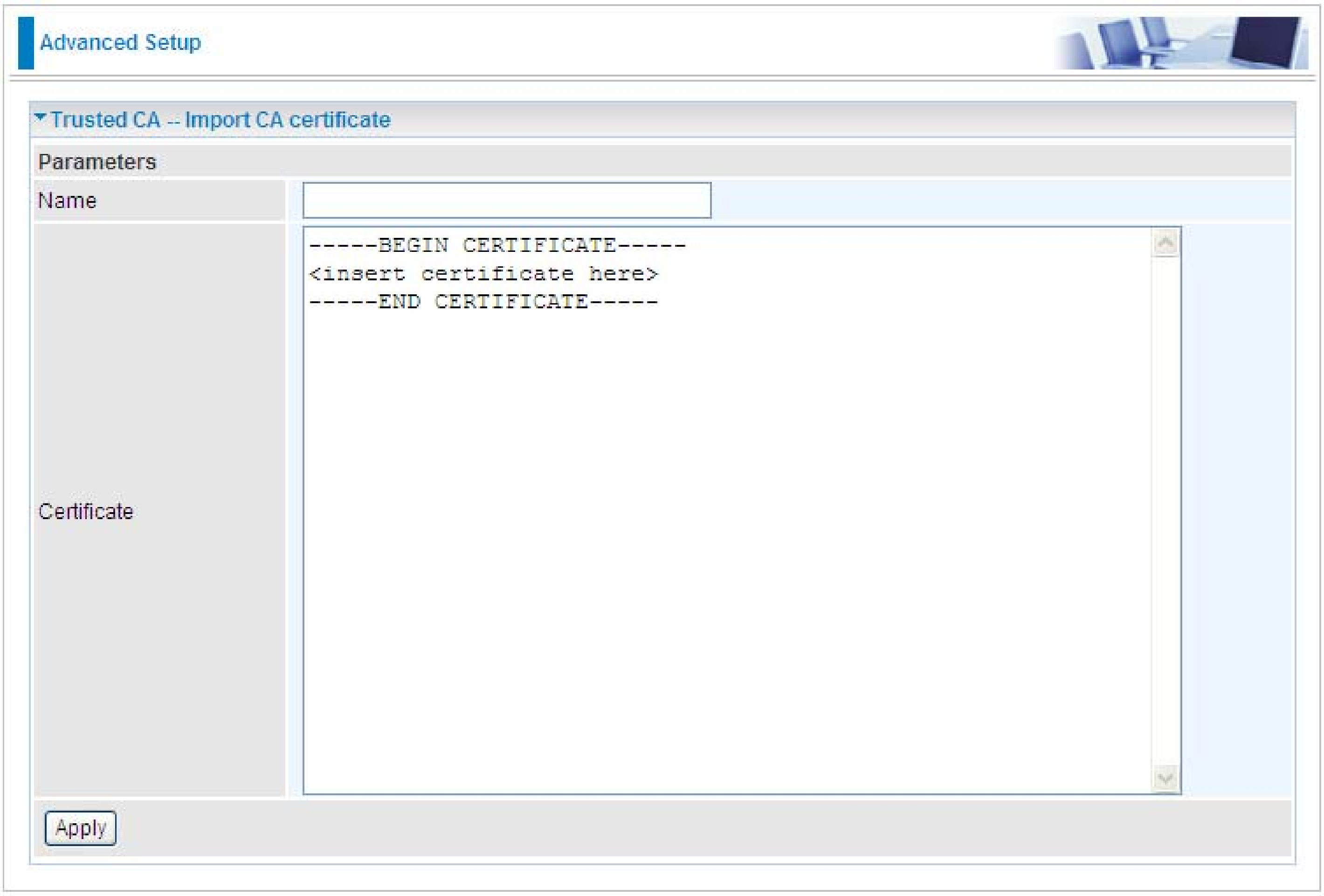
Type: The certificate type information. "ca", indicates that the certificate is a CA-signed certificate. "self", indicates that the certificate is a certificate owner signed one.

"x.509", indicates the certificate is the one created and signed according to the definition of Public-Key System suggested by x.509.

Action:

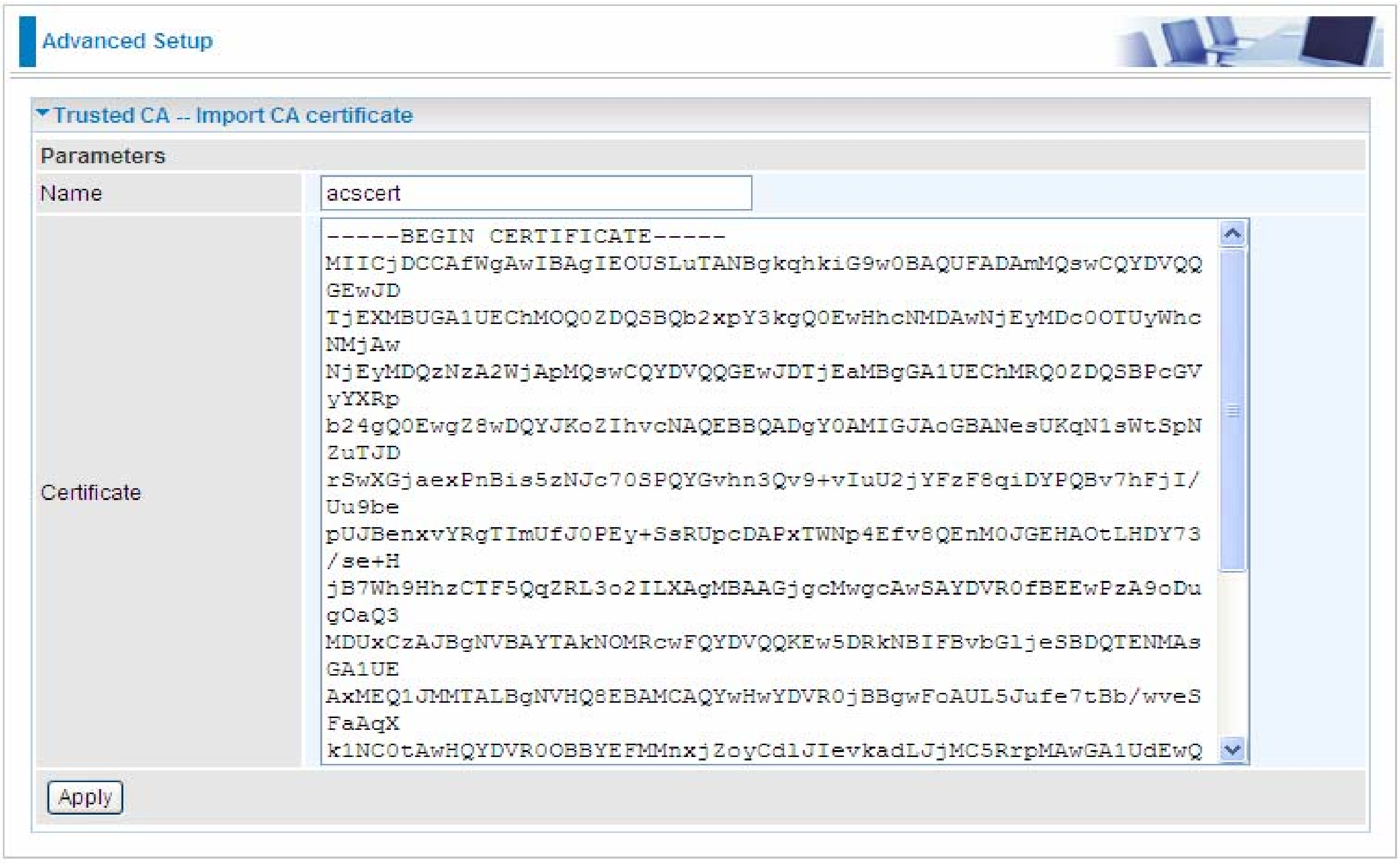
- View: view the certificate.
- Remove: remove the certificate.

Click **Import Certificate** button to import your certificate.



Name	
Certificate	-----BEGIN CERTIFICATE----- <insert certificate here> -----END CERTIFICATE-----

Enter the certificate name and insert the certificate.

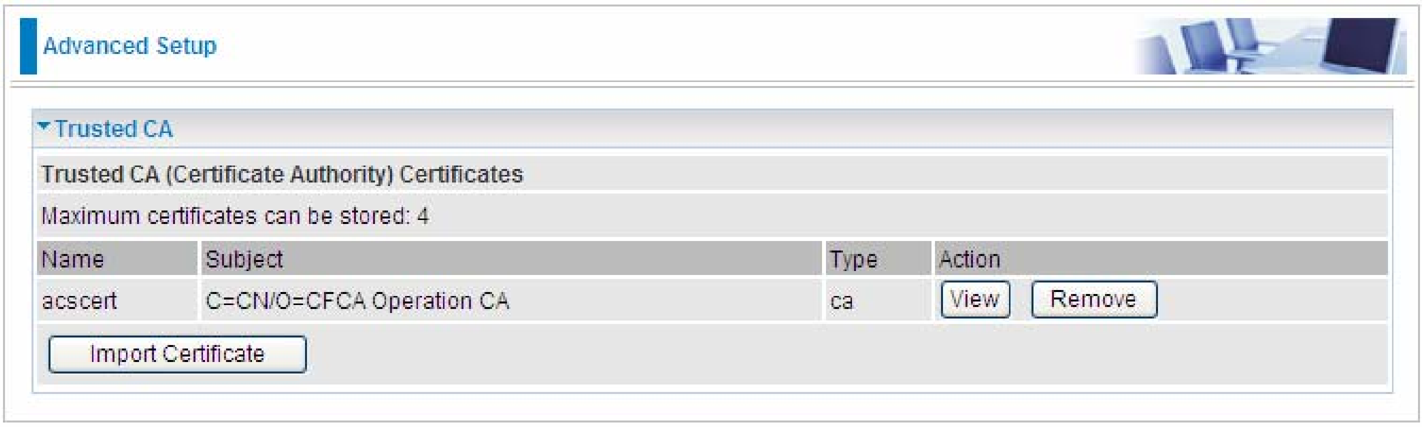


Name: acscert

Certificate:

```
-----BEGIN CERTIFICATE-----
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQ
GEwJD
TjEXMBUGA1UEChMOQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc
NMjAw
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBgGA1UEChMRQ0ZDQSBPcGV
yYXRp
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN
ZuTJD
rSwXGjaexPnBis5zNJc70SPQYGvhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/
Uu9be
pUJBenxvYRgTImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73
/se+H
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVR0fBEEwPzA9oDu
gOaQ3
MDUxCzAJBgNVBAYTAkNOMRcwFQYDVQQKEw5DRkNBIFBvbGljeSBDQTENMAs
GA1UE
AxMEQ1JMMTALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUL5Jufe7tBb/wveS
FaAqX
k1NC0tAwHQYDVR0OBBYEFMMnxjZoyCdlJIevkadLJjMC5RrpMAwGA1UdEwQ
```

Click **Apply** to confirm your settings.



Advanced Setup

▼Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action
acscert	C=CN/O=CFCA Operation CA	ca	View Remove

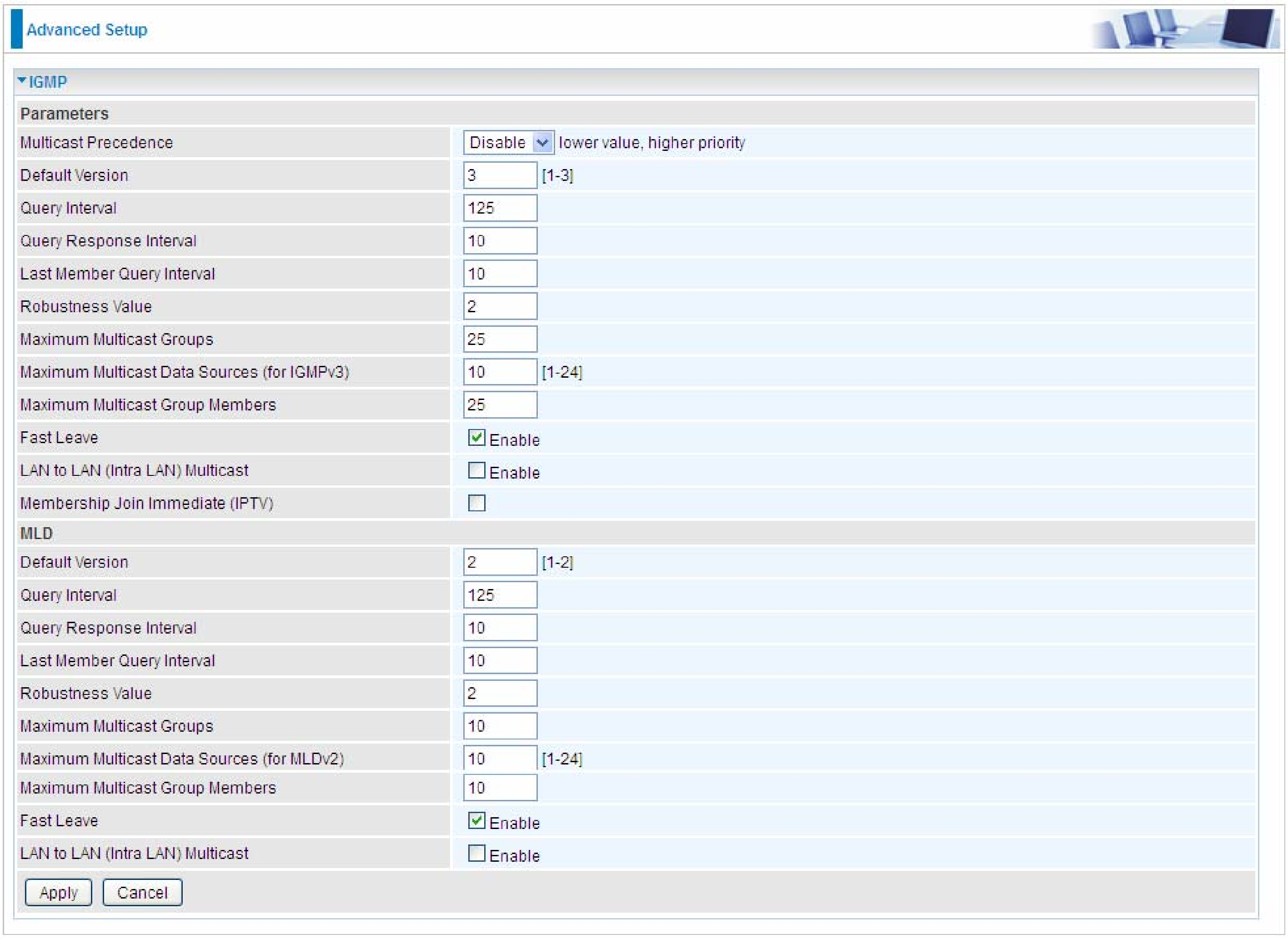
Import Certificate

Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router.

IGMP stands for **Internet Group Management Protocol,** it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP, that is IGMPv1, IGMPv2 and IGMPv3.

MLD, short for **Multicast Listener Discovery** protocol, is a component if the Internet Protocol version 6(IPv6) suite. MLD is used by IPv6 to discover multicast listeners on a directly attached link, much as IGMP used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3.



Parameters	
Multicast Precedence	Disable ▾ lower value, higher priority
Default Version	3 [1-3]
Query Interval	125
Query Response Interval	10
Last Member Query Interval	10
Robustness Value	2
Maximum Multicast Groups	25
Maximum Multicast Data Sources (for IGMPv3)	10 [1-24]
Maximum Multicast Group Members	25
Fast Leave	☑ Enable
LAN to LAN (Intra LAN) Multicast	□ Enable
Membership Join Immediate (IPTV)	□
MLD	
Default Version	2 [1-2]
Query Interval	125
Query Response Interval	10
Last Member Query Interval	10
Robustness Value	2
Maximum Multicast Groups	10
Maximum Multicast Data Sources (for MLDv2)	10 [1-24]
Maximum Multicast Group Members	10
Fast Leave	☑ Enable
LAN to LAN (Intra LAN) Multicast	□ Enable

IGMP

Multicast Precedence: It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v3.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for IGMP v3): Enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

LAN to LAN (Intra LAN) Multicast: Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Membership Join Immediate (IPTV): When a host joins a multicast session, it sends unsolicited join report to its upstream router immediately. The Startup Query Interval has been set to 1/4 of the General Query value to enable the faster join at startup.

MLD

Default Version: Enter the supported MLD version, 1-2, default is MLDv2.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

Last Member Query Interval: Enter the interval time (sec) the multicast router query the specified group after it has received leave message.

Robustness Value: Enter the router robustness parameter, default is 2, the greater the robustness value, the more robust the Querier is.

Maximum Multicast Groups: Enter the Maximum Multicast Groups.

Maximum Multicast Data Sources(for MLDv2): Enter the Maximum Multicast Data Sources,1-24.

Maximum Multicast Group Members: Enter the Maximum Multicast Group Members.

Fast leave: Check to determine whether to support fast leave. If this value is enabled, MLD proxy removes the membership of a group member immediately without sending an MLD membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

LAN to LAN (Intra LAN) Multicast: Check to determine whether to support LAN to LAN (Intra LAN) Multicast. If user want to have a multicast data source on LAN side and he want to get MLD snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

Management

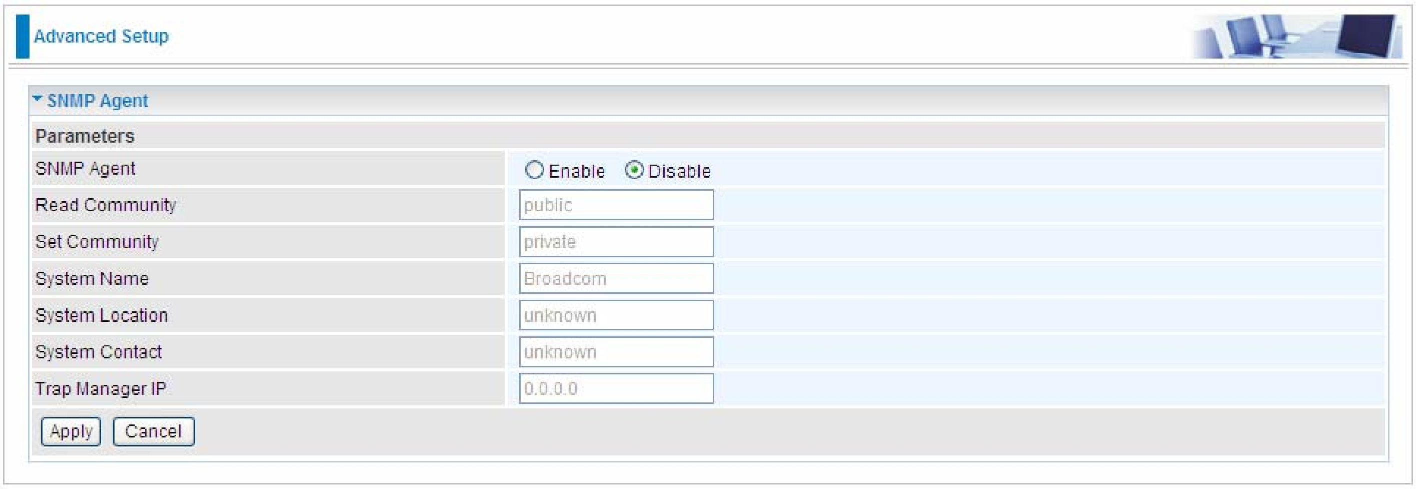
SNMP Agent

SNMP, Simple Network Management Protocol, is the most popular one in network. It consists of SNMP Manager，SNMP Agent and MIB. Every network device supporting SNMP will have a SNMP Agent which is a management software running in the device.

SNMP Manager, the management software running on the server, it uses SNMP protocol to send GetRequest、GetNextRequest, SetRequest message to Agent to view and change the information of the device.

SNMP Agents, the management software running in the device, accepts the message from the manager, Reads or Writes the management variable in MIB accordingly and then generates Response message to send it to the manager. Also, agent will send Trap message to the manager when agent finds some exceptions.

Trap message, is the message automatically sent by the managed device without request to the manager about the emergency events.



SNMP Agent

Parameters

SNMP Agent	○ Enable ● Disable
Read Community	public
Set Community	private
System Name	Broadcom
System Location	unknown
System Contact	unknown
Trap Manager IP	0.0.0.0

SNMP Agent: enable or disable SNMP Agent.

Read Community: Type the Get Community, which is the authentication for the incoming Get-and GetNext requests from the management station.

Set Community: Type the Set Community, which is the authentication for incoming Set requests from the management station.

System Name: here it refers to your router.

System Location: user-defined location.

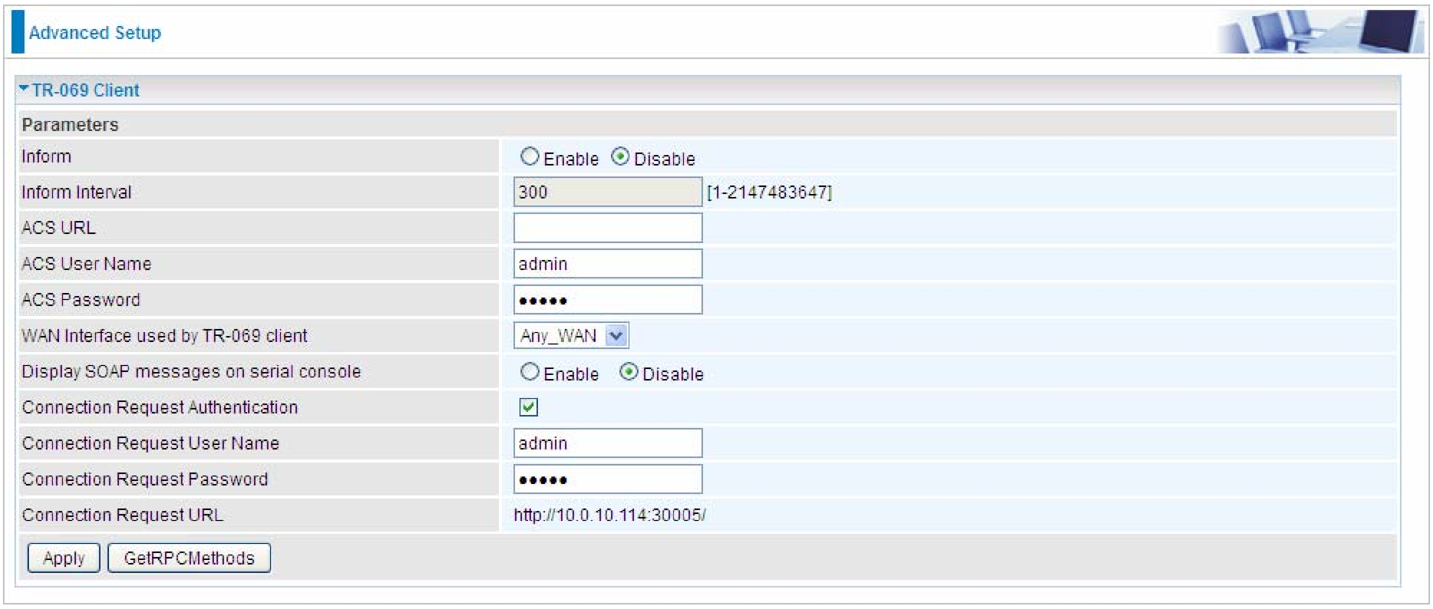
System Contact: user-defined contact message.

Trap manager IP: enter the IP address of the server receiving the trap sent by SNMP agent.

TR- 069 Client

TR-069 (short for Technical Report 069) is a DSL Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Advanced Setup

TR-069 Client

Parameters	
Inform	○ Enable ● Disable
Inform Interval	300 [1-2147483647]
ACS URL	
ACS User Name	admin
ACS Password	•••••
WAN Interface used by TR-069 client	Any_WAN
Display SOAP messages on serial console	○ Enable ● Disable
Connection Request Authentication	☑
Connection Request User Name	admin
Connection Request Password	•••••
Connection Request URL	http://10.0.10.114:30005/

Inform: select enable to let CPE be authorized to send Inform message to automatically connect to ACS.

Inform Interval: Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

ACS URL: Enter the ACS server login name.

ACS User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

ACS password: Enter the ACS server login password.

WAN interface used by TR-069: select the interface used by TR-069.

Display SOAP message on serial console: select whether to display SOAP message on serial console.

Connection Request Authentication: Check to enable connection request authentication feature.

Connection Request User Name: Enter the username for ACS server to make connection request.

Connection Request User Password: Enter the password for ACS server to make connection request.

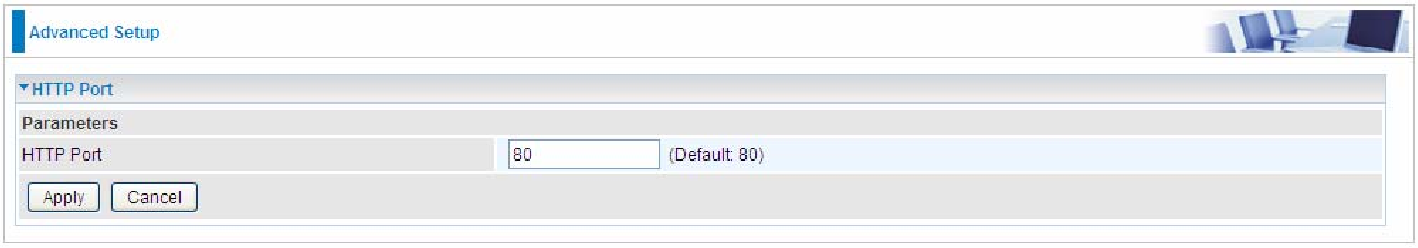
Connection Request URL: Automatically match the URL for ACS server to make connection request.

GetRPCMethods： Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.

Http Port

The device equips user to change the embedded web server accessing port. Default is 80.


Advanced Setup

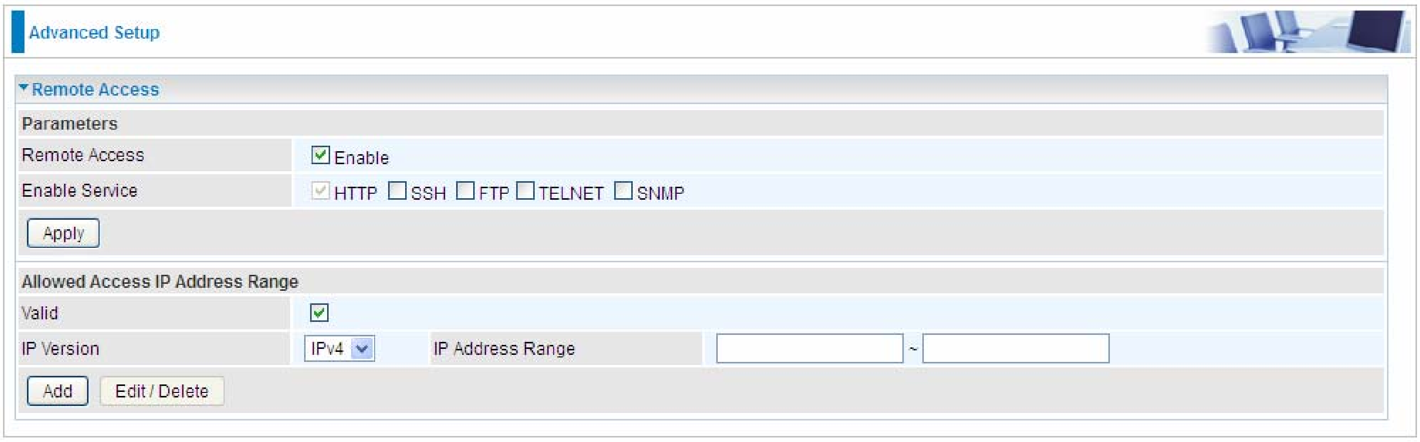
HTTP Port

Parameters

HTTP Port 80 (Default: 80)

Remote Access

It is to allow remote access to the router to view or configure.



Parameters

Remote Access	☑ Enable
Enable Service	☑ HTTP □ SSH □ FTP □ TELNET □ SNMP

Allowed Access IP Address Range

Valid	☑		
IP Version	IPv4	IP Address Range	~

Remote Access: Select “Enable” to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

Enable Service: Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit your settings.

"**Allowed Access IP Address Range**" was used to restrict which IP address could login to access system web GUI.

Valid: Enable/Disable Allowed Access IP Address Range

IP Address Range: Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

Click **Add** to add an IP Range to allow remote access.

Note: **1.** If user wants to grant remote access to IPs, first enable **Remote Access**.

2. Remote Access enabled:

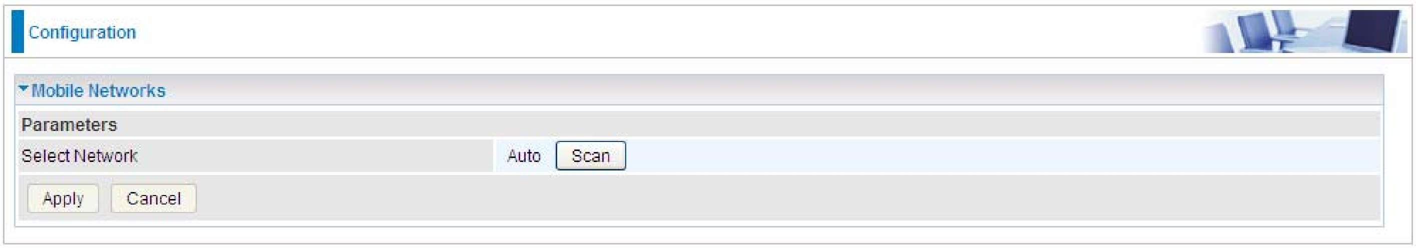
1) Enable ***Valid*** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.

2) Disable ***Valid*** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.

3) No listing of IP range is to allow any IP(s) to remote access the router.

Mobile Network

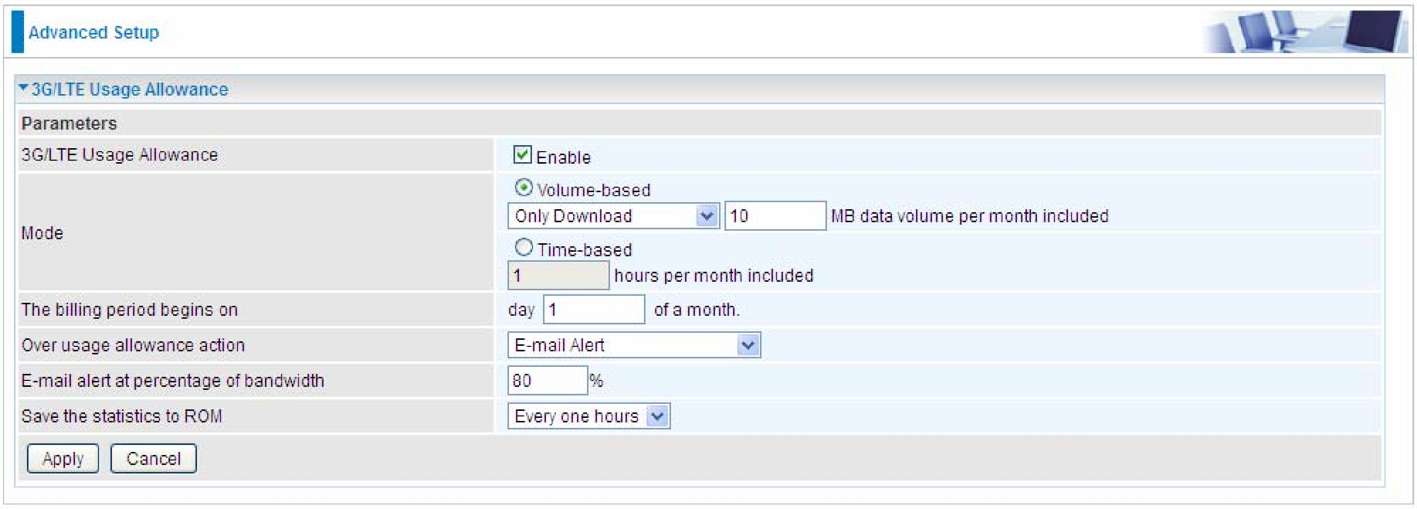
User can press **Scan** to discover available 3G/LTE mobile network.



Select Network Auto

3G/LTE Usage Allowance

3G/LTE usage allowance is designated for users to monitor and control the 3G flow usage.



▾3G/LTE Usage Allowance

Parameters	
3G/LTE Usage Allowance	☑ Enable
Mode	● Volume-based Only Download ▾ 10 MB data volume per month included ○ Time-based 1 hours per month included
The billing period begins on	day 1 of a month.
Over usage allowance action	E-mail Alert ▾
E-mail alert at percentage of bandwidth	80 %
Save the statistics to ROM	Every one hours ▾

Mode: include Volume-based and Time-based control.

- **Volume-based** include “only Download”, ”only Upload” and “Download and Upload” to limit the flow.
- **Time-based** control the flow by providing specific hours per month.

The billing period begins on: The beginning day of billing each month.

Over usage allowance action: What to do when the flow is over usage allowance, the available methods are “E-mail Alert”, ”Email Alert and Disconnect” and “Disconnect”.

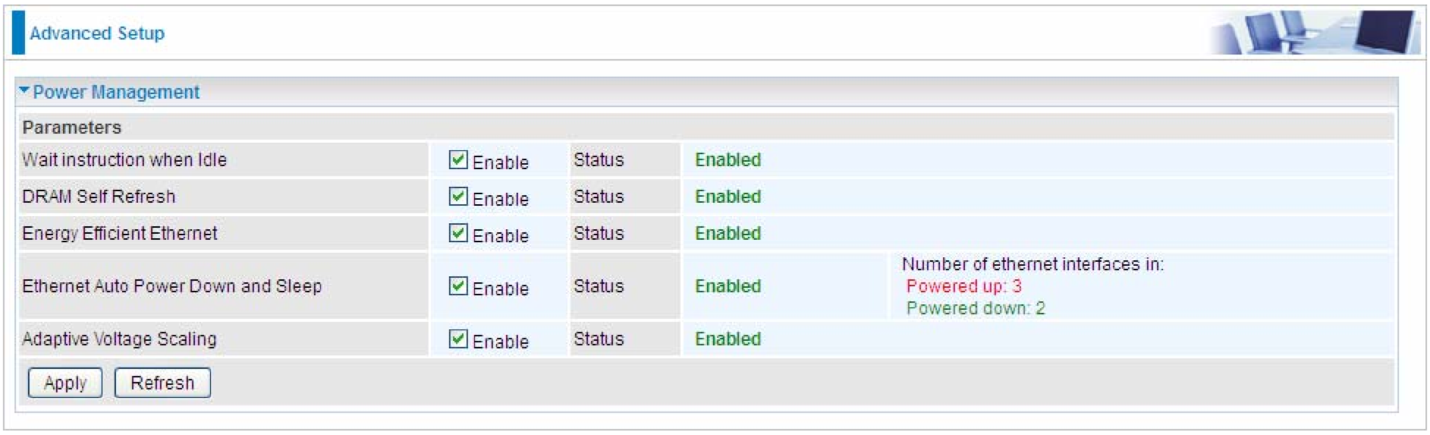
E-mail alert at percentage of bandwidth: When the used bandwidth exceeds the set proportion, the system will send email to alert.

Save the statistics to ROM: To save the statistics to ROM system.

Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.

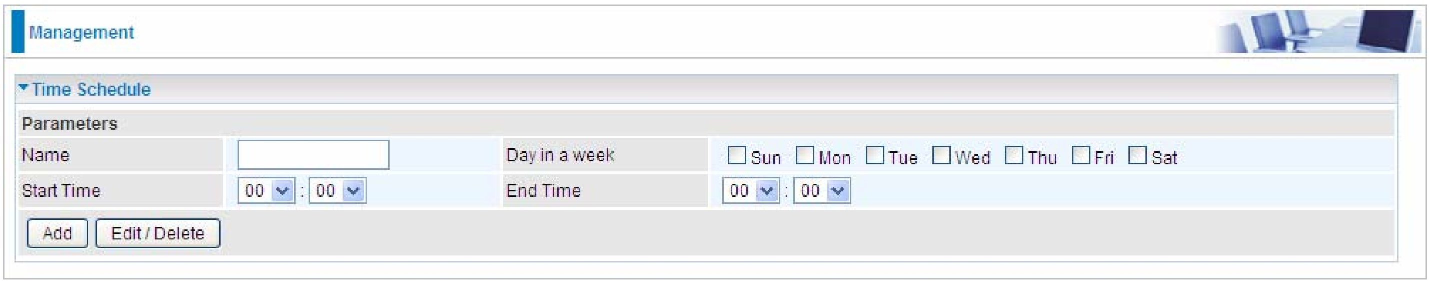


Parameters				
Wait instruction when Idle	☑ Enable	Status	Enabled	
DRAM Self Refresh	☑ Enable	Status	Enabled	
Energy Efficient Ethernet	☑ Enable	Status	Enabled	
Ethernet Auto Power Down and Sleep	☑ Enable	Status	Enabled	Number of ethernet interfaces in: Powered up: 3 Powered down: 2
Adaptive Voltage Scaling	☑ Enable	Status	Enabled	

Time Schedule

The Time Schedule supports up to **32** timeslots 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.



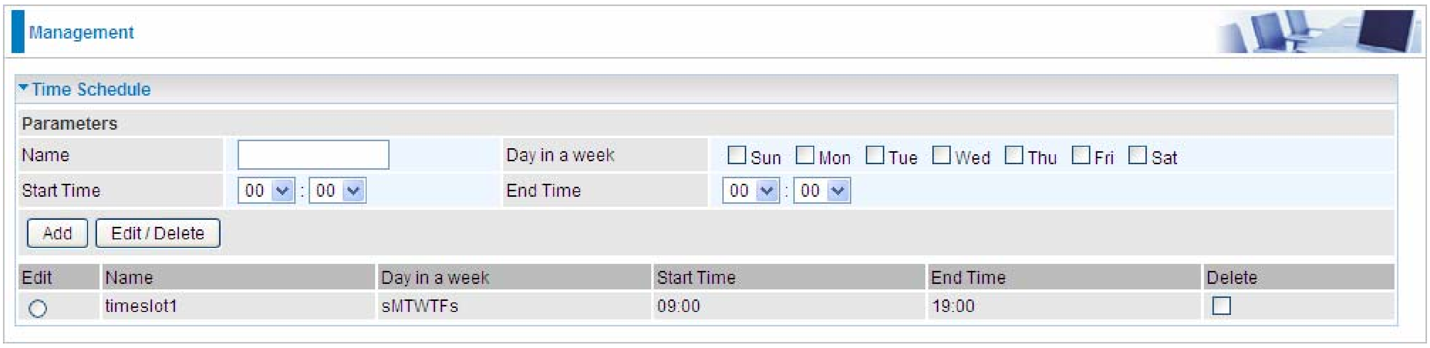
Management

▾Time Schedule

Parameters

Name		Day in a week	□Sun □Mon □Tue □Wed □Thu □Fri □Sat
Start Time	00 : 00	End Time	00 : 00

For example, user can add a timeslot named "timeslot1" which features a period of 9:00-19:00 on every weekday.



Management

▾Time Schedule

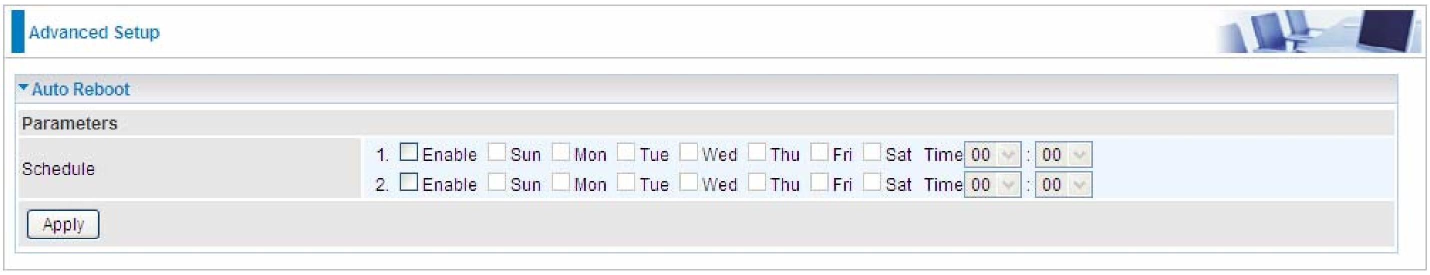
Parameters

Name		Day in a week	□Sun □Mon □Tue □Wed □Thu □Fri □Sat
Start Time	00 : 00	End Time	00 : 00

Edit	Name	Day in a week	Start Time	End Time	Delete
○	timeslot1	sMTWTFs	09:00	19:00	□

Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.



Advanced Setup

Auto Reboot

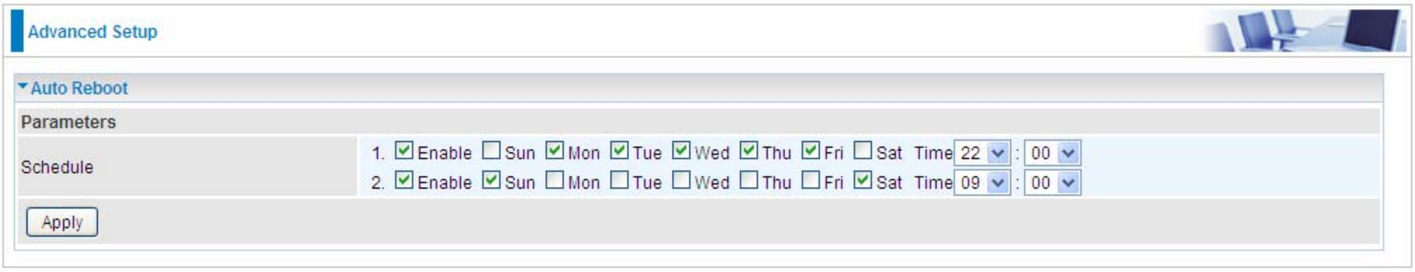
Parameters

Schedule

1. □ Enable □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat Time 00 : 00
2. □ Enable □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat Time 00 : 00

Enable to set the time schedule for rebooting.

For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:



Advanced Setup

Auto Reboot

Parameters

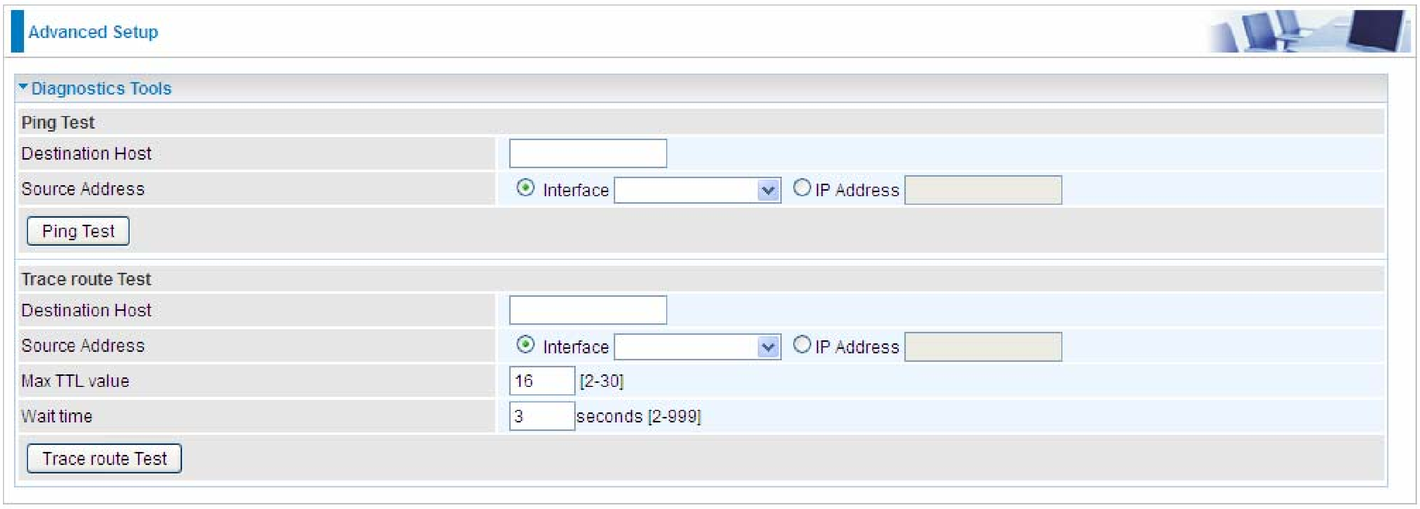
Schedule

1. ☑ Enable □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat Time 22 : 00
2. ☑ Enable ☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri ☑ Sat Time 09 : 00

Diagnostics

Diagnostics Tools

BiPAC 7800VDP(O)X offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.



Ping Test	
Destination Host	
Source Address	● Interface ○ IP Address
Ping Test	
Trace route Test	
Destination Host	
Source Address	● Interface ○ IP Address
Max TTL value	16 [2-30]
Wait time	3 seconds [2-999]
Trace route Test	

Ping Test: to verify the connectivity between source and destination.

Destination Host: Enter the destination host (IP, domain name) to be checked for connectivity.

Source Address: Select or set the source address to test the connectivity from the source to the destination.

Ping Test: Press this button to proceed ping test.

Trace route Test: to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

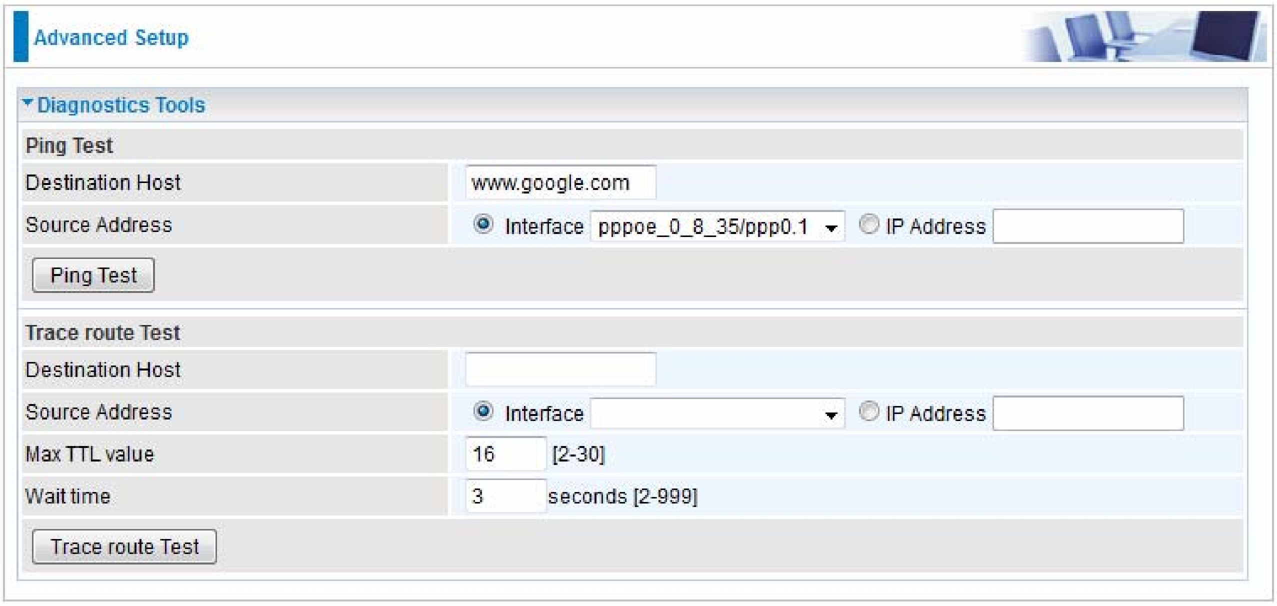
Destination Host: Set the destination host (IP, domain name) to be traced.

Source Address: Select or set the source address to trace the route from the source to the destination.

Max TTL value: Set the max Time to live (TTL) value.

Wait time: Set waiting time for each response in seconds.

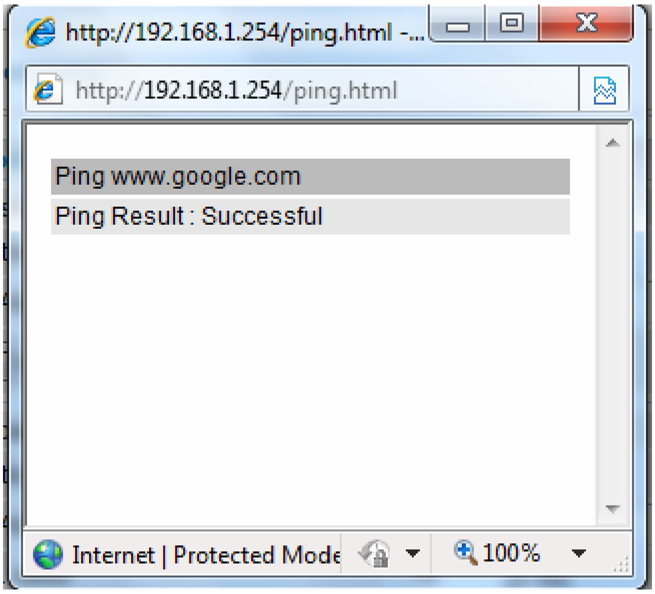
Example: Ping www.google.com



Advanced Setup

Diagnostics Tools

Ping Test	
Destination Host	www.google.com
Source Address	● Interface pppoe_0_8_35/ppp0.1 ○ IP Address
Ping Test	
Trace route Test	
Destination Host	
Source Address	● Interface ○ IP Address
Max TTL value	16 [2-30]
Wait time	3 seconds [2-999]
Trace route Test	



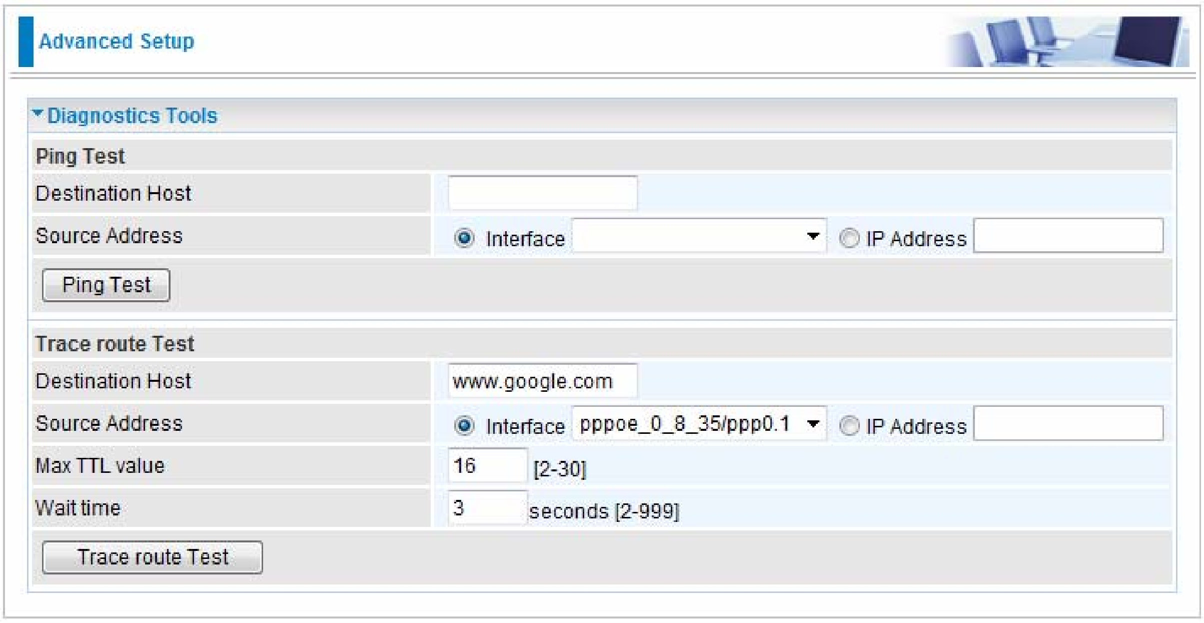
http://192.168.1.254/ping.html -...

http://192.168.1.254/ping.html

Ping www.google.com

Ping Result : Successful

Example: “trace” www.google.com



Advanced Setup

Diagnostics Tools

Ping Test

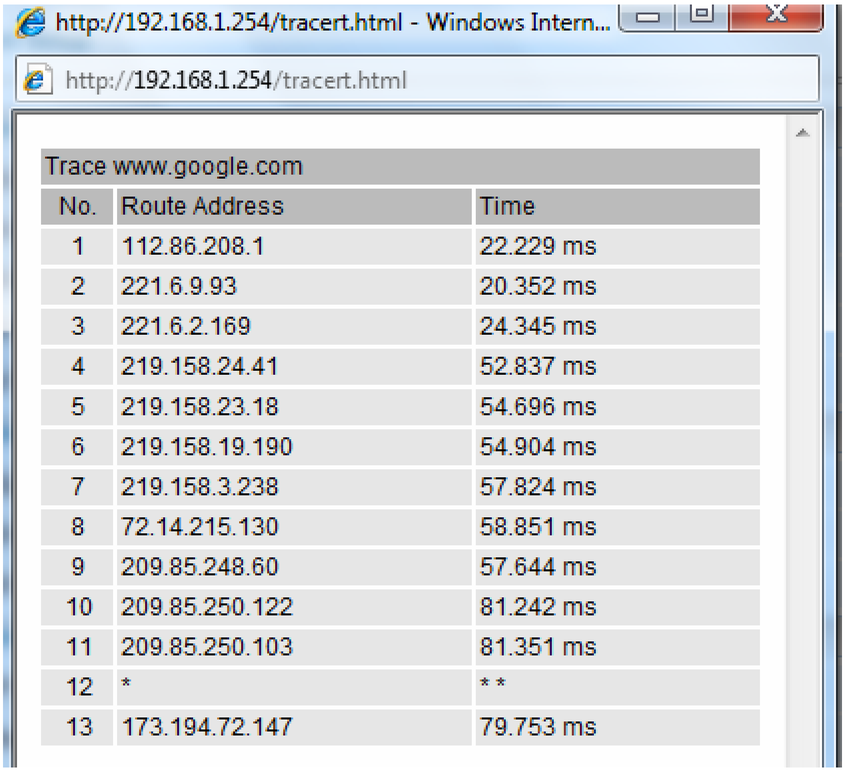
Destination Host	
Source Address	● Interface ▾ ○ IP Address

Ping Test

Trace route Test

Destination Host	www.google.com
Source Address	● Interface pppoe_0_8_35/ppp0.1 ▾ ○ IP Address
Max TTL value	16 [2-30]
Wait time	3 seconds [2-999]

Trace route Test



http://192.168.1.254/tracert.html - Windows Intern...

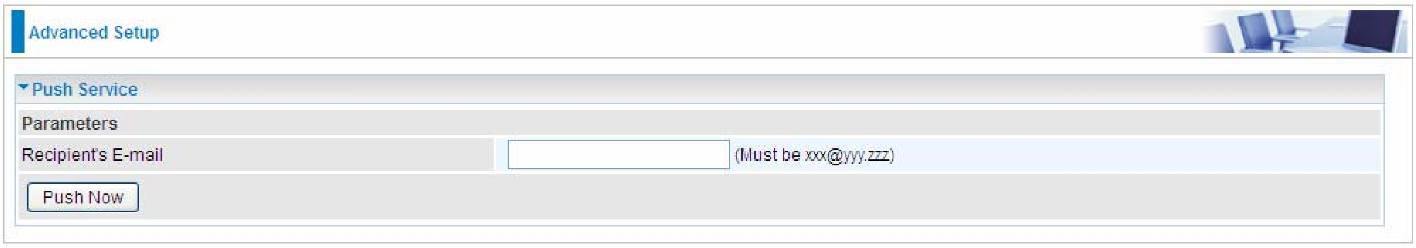
http://192.168.1.254/tracert.html

Trace www.google.com

No.	Route Address	Time
1	112.86.208.1	22.229 ms
2	221.6.9.93	20.352 ms
3	221.6.2.169	24.345 ms
4	219.158.24.41	52.837 ms
5	219.158.23.18	54.696 ms
6	219.158.19.190	54.904 ms
7	219.158.3.238	57.824 ms
8	72.14.215.130	58.851 ms
9	209.85.248.60	57.644 ms
10	209.85.250.122	81.242 ms
11	209.85.250.103	81.351 ms
12	*	* *
13	173.194.72.147	79.753 ms

Push Service

With push service, the system can send email messages with consumption data and system information.



▾Push Service

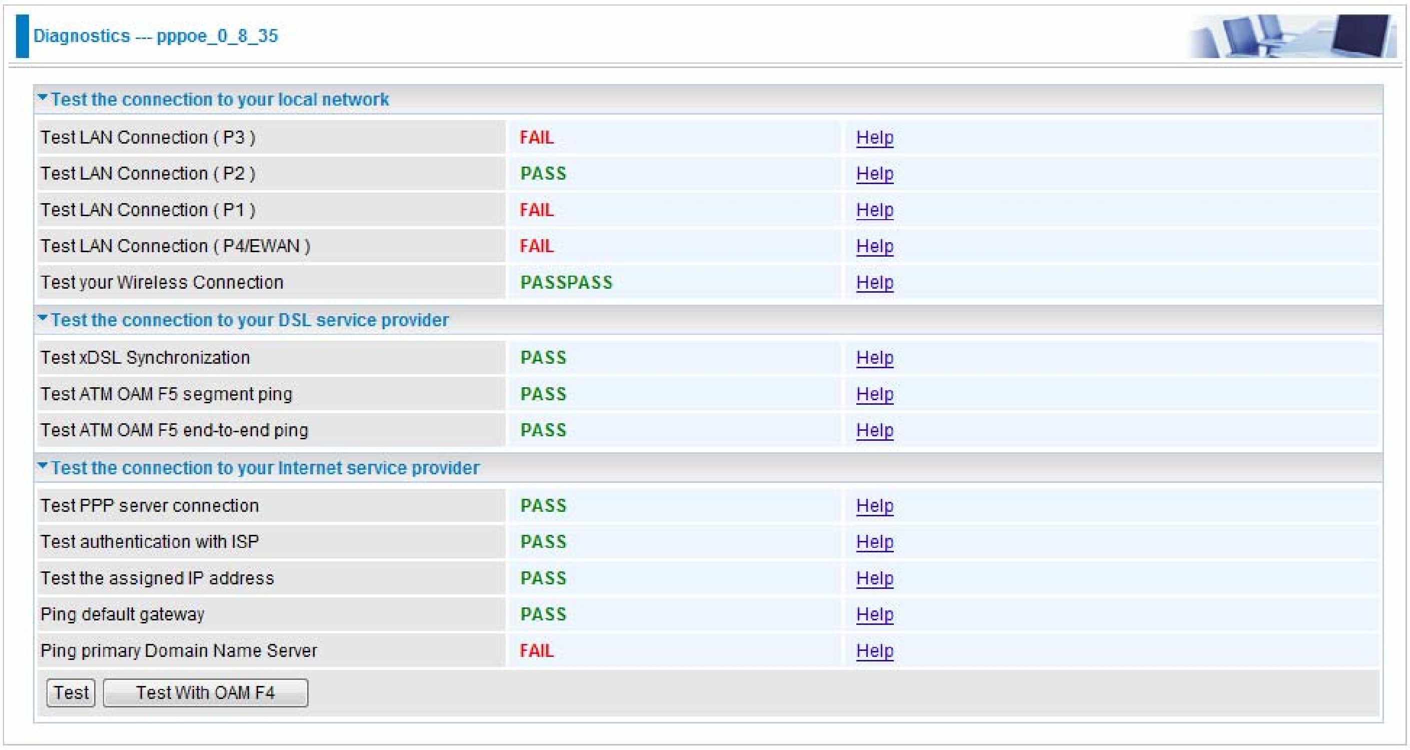
Parameters	
Recipient's E-mail	(Must be xxx@yyy.zzz)

Recipient’s E-mail: Enter the destination mail address. The email is used to receive ***system log*** ，***system configuration***， ***security log*** sent by the device when the **Push Now** button is pressed (information sent only when pressing the button), but the mail address is not remembered.

Note: Please first set correct the SMTP server parameters in Mail Alert.

Diagnostics

Check the connections, including Ethernet connection, Internet Connection and wireless connection. Click ***Help*** link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

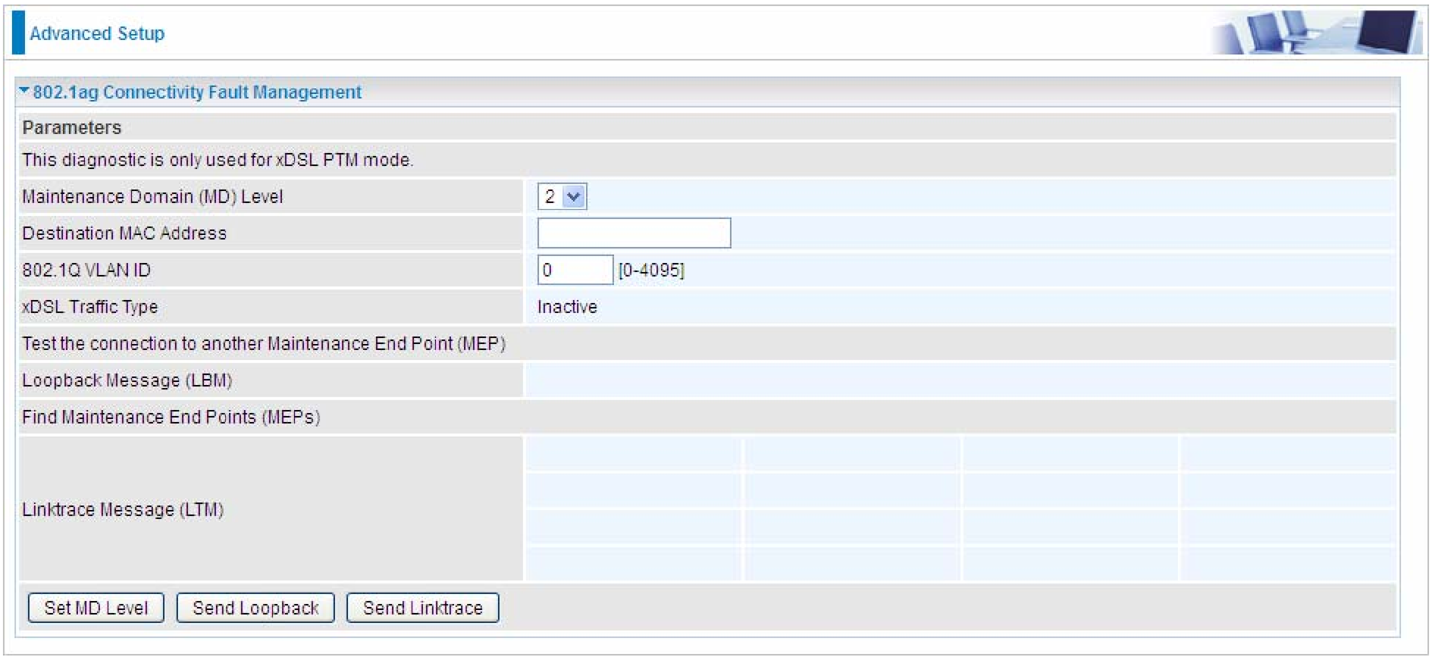


Diagnostics --- pppoe_0_8_35

▼ Test the connection to your local network		
Test LAN Connection (P3)	FAIL	Help
Test LAN Connection (P2)	PASS	Help
Test LAN Connection (P1)	FAIL	Help
Test LAN Connection (P4/EWAN)	FAIL	Help
Test your Wireless Connection	PASSPASS	Help
▼ Test the connection to your DSL service provider		
Test xDSL Synchronization	PASS	Help
Test ATM OAM F5 segment ping	PASS	Help
Test ATM OAM F5 end-to-end ping	PASS	Help
▼ Test the connection to your Internet service provider		
Test PPP server connection	PASS	Help
Test authentication with ISP	PASS	Help
Test the assigned IP address	PASS	Help
Ping default gateway	PASS	Help
Ping primary Domain Name Server	FAIL	Help

Fault Management

IEEE 802.1ag Connectivity Fault Management (CFM) is a standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Fault Management is to uniquely test the VDSL PTM connection; Push service



Parameters

This diagnostic is only used for xDSL PTM mode.

Maintenance Domain (MD) Level	2
Destination MAC Address	
802.1Q VLAN ID	0 [0-4095]
xDSL Traffic Type	Inactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM)

Find Maintenance End Points (MEPs)

Linktrace Message (LTM)

Maintenance Domain (MD) Level: Maintenance Domains (MDs) are management spaces on a network, typically owned and operated by a single entity. MDs are configured with Names and Levels, where the eight levels range from 0 to 7. A hierarchal relationship exists between domains based on levels. The larger the domain, the higher the level value.

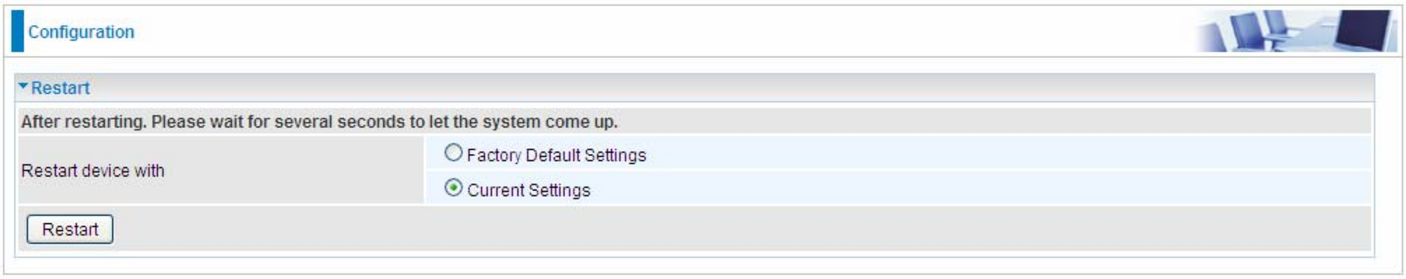
Maintenance End Point: Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

Link Trace: Link Trace messages otherwise known as Mac Trace Route are Multicast frames that a MEP transmits to track the path (hop-by-hop) to a destination MEP which is similar in concept to User Datagram Protocol (UDP) Trace Route. Each receiving MEP sends a Trace route Reply directly to the Originating MEP, and regenerates the Trace Route Message.

Loop-back: Loop-back messages otherwise known as MaC ping are Unicast frames that a MEP transmits, they are similar in concept to an Internet Control Message Protocol (ICMP) Echo (Ping) messages, sending Loopback to successive MIPs can determine the location of a fault. Sending a high volume of Loopback Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loopback to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

Restart

This section lets you restart your router if necessary. Click Restart in the low right corner of each configuration page.



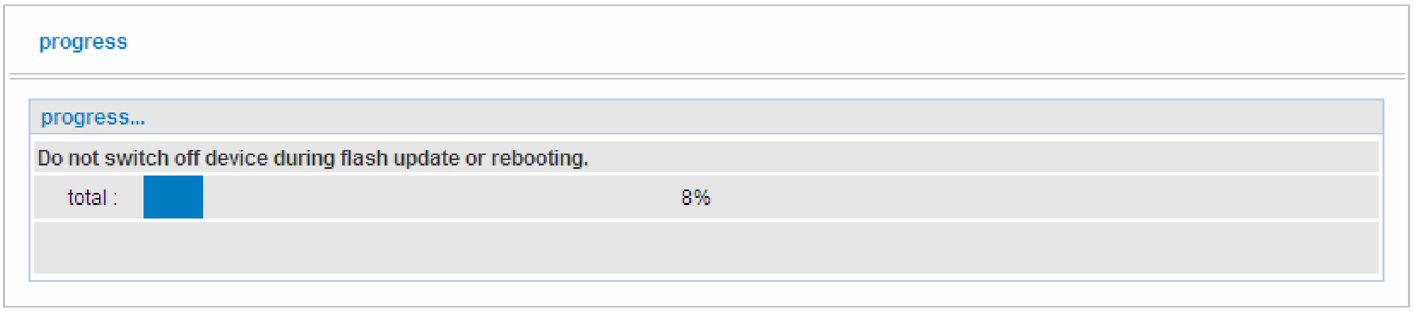
▾Restart

After restarting. Please wait for several seconds to let the system come up.

Restart device with ○ Factory Default Settings ● Current Settings

Restart

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings. Or you just want to restart after the current setting, the select the Current Settings, and Click Restart.



progress...

Do not switch off device during flash update or rebooting.

total : 8%

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 is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problems with WAN interface

Problem	Suggested Action
Frequent loss of ADSL line sync (disconnections)	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections. If you have a back-to-base alarm system you should contact your security provider for a technician to make any necessary changes.

Problem with LAN interface

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

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference
(2) This device must accept any interference received, including interference that may cause undesired operation.
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.