



# **BiPAC 7800(N)X(L)**

**3G/4G LTE (Wireless-N) (VPN)  
ADSL2+/Fibre Broadband Router**

## **User Manual**



# Notice

Please read this notice before moving on next.

You are now reading an all-in-one document on instructions about three different routers with similar and up-to-date features -7800X, 7800NX, and 7800NXL. The three models are the most recent models offered by our company, with concrete features placed in the next chapters.

The major difference lies in whether the model is with support of wireless and VPN. Please check the diagram below:

Model	WAN	Ethernet	Wireless	VPN
<a href="#">7800X</a>	ADSL, EWAN, 3G/4G LTE	10/100/1000M x4 (#4 can be configured as EWAN)	NA	IPSec, PPTP, GRE
<a href="#">7800NXL</a>	ADSL, EWAN, 3G/4G LTE	10/100/1000M x4 (#4 can be configured as EWAN)	11n	NA
<a href="#">7800NX</a>	ADSL, EWAN, 3G/4G LTE	10/100/1000M x4 (#4 can be configured as EWAN)	11n	IPSec, PPTP, GRE

For details, users can follow the User Manual.



# Table of Contents

Chapter 1: Introduction .....	1
Introduction to your Router .....	1
Features.....	3
ADSL Compliance .....	3
Network Protocols and Features.....	4
Firewall.....	4
Quality of Service Control .....	4
ATM, PTM and PPP Protocols.....	4
IPTV Application .....	5
Wireless LAN ( <i>BiPAC 7800NX(L) only</i> ) .....	5
USB Application Server .....	5
Virtual Private Network (VPN) ( <i>7800(N)X only</i> ).....	5
Management.....	6
Hardware Specifications .....	7
Physical Interface .....	7
Chapter 2: Installing the Router .....	8
Package Contents .....	8
Important note for using this router .....	10
Device Description .....	11
The Front LEDs .....	11
The Rear Ports .....	13
Cabling.....	15
Chapter 3: Basic Installation.....	16
Connecting Your Router .....	17
Network Configuration .....	21
Configuring a PC in Windows 7 .....	21
Configuring a PC in Windows Vista.....	24
Configuring a PC in Windows XP.....	27
Configuring PC in Windows 2000 .....	29
Configuring PC in Windows 95/98/Me .....	30
Configuring PC in Windows NT4.0 .....	31
Factory Default Settings .....	32
Information from your ISP .....	34
Easy Sign On (EZSO).....	35
Chapter 4: Configuration.....	44
Configuration via Web Interface .....	44
Status .....	46
Summary .....	47
WAN .....	48
Statistics .....	49
LAN .....	49
WAN Service.....	50
xTM .....	50
xDSL.....	51
Bandwidth Usage .....	54
LAN .....	54
WAN Service.....	56
3G/LTE Status .....	58
Route .....	59
ARP .....	60



DHCP .....	61
IPSec (7800(N)X only) .....	62
PPTP (7800(N)X only) .....	63
Log .....	64
System Log .....	64
Security Log .....	65
Quick Start .....	66
Quick Start .....	66
Configuration .....	73
LAN - Local Area Network .....	74
Ethernet .....	74
IPv6 Autoconfig .....	77
Interface Grouping .....	81
Wireless (7800NX(L) only) .....	84
Basic .....	85
Security .....	87
MAC Filter .....	99
Wireless Bridge .....	100
Advanced .....	102
Station Info .....	104
WAN-Wide Area Network .....	105
WAN Service .....	105
DSL .....	105
Ethernet .....	116
3G/LTE .....	123
DSL .....	126
SNR .....	127
System .....	128
Internet Time .....	128
Firmware Upgrade .....	129
Backup / Update .....	130
Access Control .....	131
Mail Alert .....	132
Configure Log .....	133
USB .....	134
Storage Device Info .....	134
User Account .....	135
Print Server .....	140
DLNA .....	146
IP Tunnel .....	148
IPv6inIPv4 .....	148
IPv4inIPv6 .....	150
Security .....	151
IP Filtering Outgoing .....	151
IP Filtering Incoming .....	153
MAC Filtering .....	155
Blocking WAN PING .....	156
Time Restriction .....	157
URL Filter .....	159
QoS - Quality of Service .....	162
NAT .....	167
Virtual Servers .....	167
ALG .....	170
Port Triggering .....	171



DMZ Host .....	174
One-to-One NAT .....	175
Wake On LAN .....	176
Advanced Setup .....	177
Routing .....	178
Default Gateway .....	178
Static Route .....	179
Policy Routing .....	181
RIP .....	182
DNS .....	183
DNS .....	183
Dynamic DNS .....	184
DNS Proxy .....	186
Static ARP .....	187
UPnP .....	188
VPN (7800(N)X only) .....	195
IPSec .....	195
PPTP .....	204
PPTP Account .....	205
PPTP Client .....	206
GRE .....	217
Certificate .....	218
Trusted CA .....	218
Multicast .....	221
Management .....	223
SNMP Agent .....	223
TR-069 Client .....	224
Remote Access .....	226
Power Management .....	227
Time Schedule .....	228
Diagnostics .....	229
Push Service .....	229
Diagnostics .....	230
Fault Management .....	231
Restart .....	232
Chapter 5: Troubleshooting .....	233
Appendix: Product Support & Contact .....	235



# Chapter 1: Introduction

## Introduction to your Router

The BiPAC 7800(N)X(L) is a fibre-ready ADSL2+ modem, an all-in-one advanced device integrating Wireless-N 300Mbps (*7800NX(L) only*), Gigabit Ethernet, 3G/4G LTE, and NAS(Network Attached Storage) in one unit. As well as being IPv6-capable, the BiPAC 7800(N)X(L) ADSL2+ router supports super fast fibre connections via dual-WAN connectivity through a Gigabit Ethernet WAN port. Also, it also has a USB port, allowing the device to act as a print server as well as a NAS (Network Attached Storage) device with DLNA (Digital Living Network Alliance). Moreover, the USB port can host a 3G/4G LTE modem connecting to the 3G/4G LTE network for Internet access. With an array of advanced features, the BiPAC 7800(N)X(L) delivers a future-proof solution for ADSL2+ connections, super fast FTTC and ultra-speed FTTH (Fibre-To-The-Home) network deployment and services.

### Maximum wireless performance (*7800NX(L) only*)

With an integrated 802.11n Wireless Access Point, the router delivers up to 6 times the speed of an 802.11a/b/g network device. It supports a data rate of up to 300Mbps and is also compatible with 802.11a/b/g equipment. The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over wireless LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any external wires or cables.

### 3G/4G LTE Mobility and Always-on Connectivity

With 3G/4G LTE-based Internet connection (requires an additional 3G/4GLTE USB modem plugged into the built-in USB port), user can access internet through 3G/4G LTE, whether you are seated at your desk or taking a cross-country trip. The auto fail-over feature ensures optimum connectivity and minimum interruption by quickly and smoothly connecting to a 3G/4G LTE network in the event that you ADSL/Fibre/Cable line fails. The BiPAC 7800(N)X(L) will then automatically reconnect to the ADSL/Fibre/Cable connection when it is restored, reducing connection costs. These features are perfect for office situations when a constant and smooth WAN connection is critical.

### 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  $3.4 \times 10^{38}$ ) 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.

The BiPAC 7800(N)X(L) fully supports IPv6 (Internet Protocol Version 6), launched as the current IPv4 range is filling up, and IPv6 is gradually becoming the indispensable addressing system for savvy cloud computing users. Dual stack means the router is capable of running IPv4 and IPv6 in parallel during the transition period. With Billion IPv6 enabled devices, three major transition mechanisms such as Dual-Stack, Dual-Stack Lite, and 6RD (IPv6 rapid deployment) are supported to be adapted easily into service provider's IPv4/IPv6 network



## **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 data 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.

## **Gigabit Ethernet**

The BiPAC 7800(N)X(L) has four Gigabit Ethernet Ports and the fourth port can be configured as a WAN port if requested. This EWAN offers another broadband connectivity option for connecting to a cable, VDSL, fibre or second ADSL modem. The BiPAC 7800(N)X(L) again offers users convenience and optimal network performance with data rates reaching 1 Gbps.

## **Virtual AP (7800NX(L) only)**

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

- Triple-WAN ports for 3G/4G LTE, ADSL2+, Gigabit Ethernet WAN (EWAN) for broadband connectivity
- Gigabit WAN and LAN
- Fibre (FTTC/FTTP/FTTH) ready with high WAN throughput
- IPv6 ready (IPv4/IPv6 dual stack)
- 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) (*BiPAC 7800NX(L) only*)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support (*BiPAC 7800NX(L) only*)
- Secured IPSec VPN with powerful DES/ 3DES/ AES (*BiPAC 7800(N)X only*)
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication (*BiPAC 7800(N)X only*)
- GRE tunnel (*BiPAC 7800(N)X only*)
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization and Bandwidth management
- Universal Plug and Play (UPnP) Compliance
- Supports IPTV Application<sup>\*2</sup>
- USB port for print server, NAS(Samba), DLNA media server, and 3G/4G LTE USB modem
- Ease of Use with Quick Installation Wizard (EZSO)

## 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

## **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<sup>\*2</sup>**

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

## **Wireless LAN (*BiPAC 7800NX(L) only*)**

- Compliant with IEEE 802.11 a/ b/ g/ n standards
- 2.4 GHz radio band for wireless
- Up to 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/4G LTE dongle support
- Storage/NAS: Samba server, DLNA media server
- Printer Server

## **Virtual Private Network (VPN) (*7800(N)X only*)**

- IKE key management
- DES, 3DES and AES encryption for 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\*<sup>1</sup> supports remote management
- Available Syslog
- Mail alert for WAN IP changed
- Auto failover and fallback
- Push Service



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 4dbi detachable antennas (*BiPAC 7800NX(L) only*)
- DSL: ADSL port
- USB 2.0 port for storage service, printer server and 3G/4G LTE dongle
- 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

### 7800NX and 7800NXL

- BiPAC 7800NX(L) 3G/4G LTE Wireless-N ADSL2+ (VPN)/ Fibre Broadband Router
- Quick Start Guide
- CD containing the on-line manual
- RJ-45 Cat. 5e STP Ethernet cable
- RJ-11 ADSL/ telephone cable
- Power adapter
- Splitter / Micro-filter (Optional)

**ADSL2+ Router**



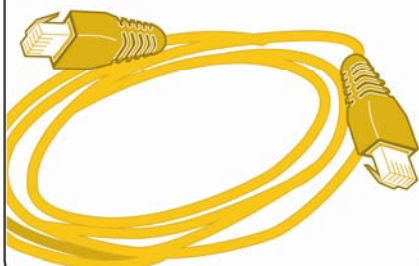
**Quick Start Guide**



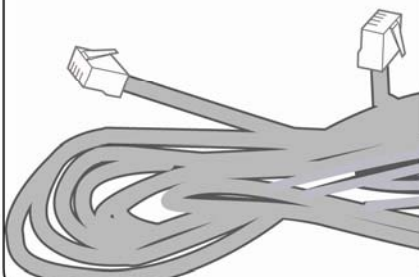
**CD**



**RJ-45 Cat. 5e STP Ethernet cable**

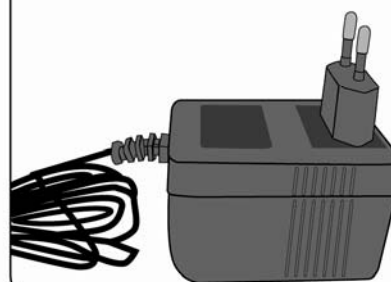


**RJ-11 Phone cable**



**Power Adapter**

(The type may differ by different country)





## 7800X

- BiPAC 7800X 3G/4G LTE ADSL2+ VPN/ Fibre Broadband Router
- Quick Start Guide
- CD containing the on-line manual
- RJ-45 Cat. 5e STP Ethernet cable
- RJ-11 ADSL/ telephone cable
- Power adapter
- Splitter / Micro-filter (Optional)

**ADSL2+ Router**



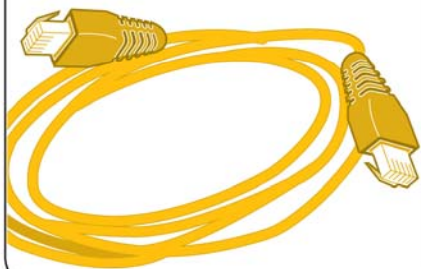
**Quick Start Guide**



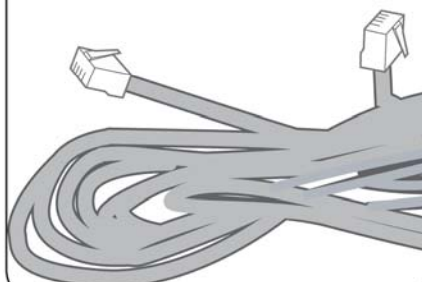
**CD**



**RJ-45 Cat. 5e STP  
Ethernet cable**

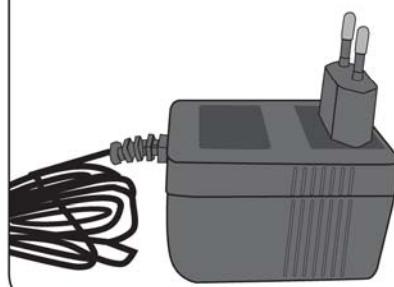


**RJ-11  
Phone cable**



**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

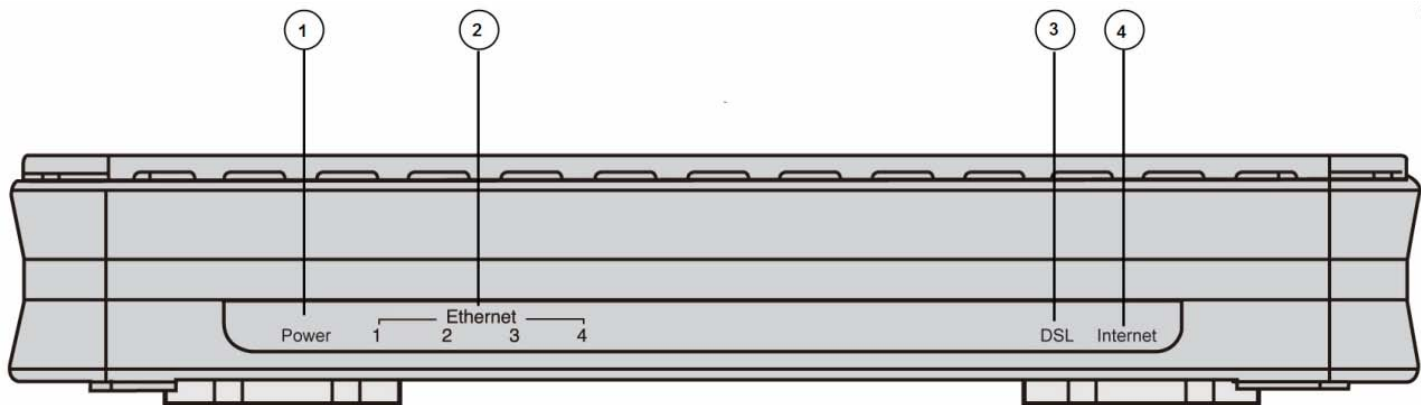
1. Place the router on a stable surface.
2. Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.



# Device Description

## The Front LEDs

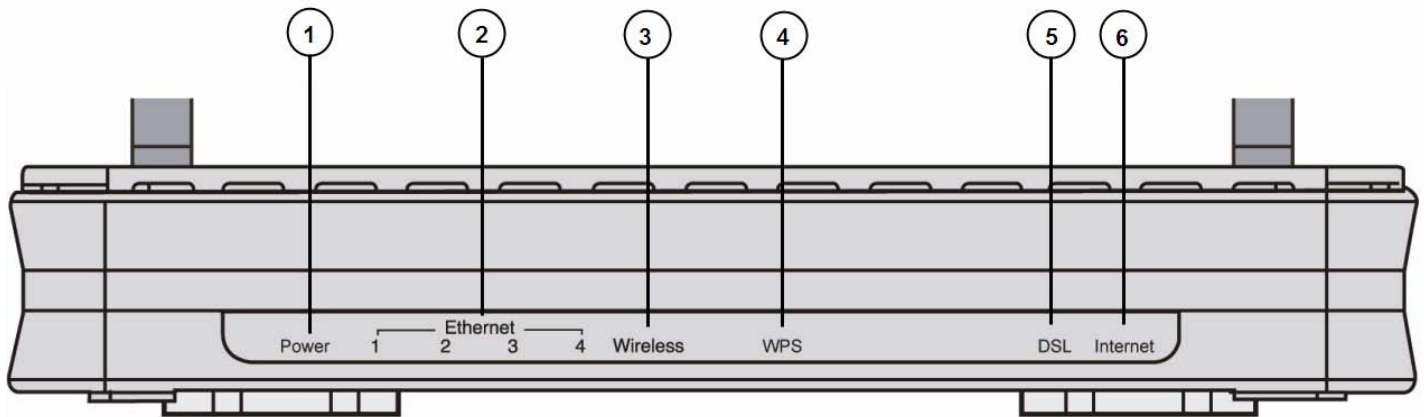
7800X



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	DSL	Green Blinking	DSL synchronizing or waiting for DSL synchronizing
		Green	Successfully connected to an ADSL DSLAM (Line Sync).
		Off	DSL cable unplugged
4	Internet	Red	Obtaining IP failure
		Green	Having obtained an IP address successfully
		Off	Router in bridge mode or DSL connection not present.



## 7800NX and 7800NXL

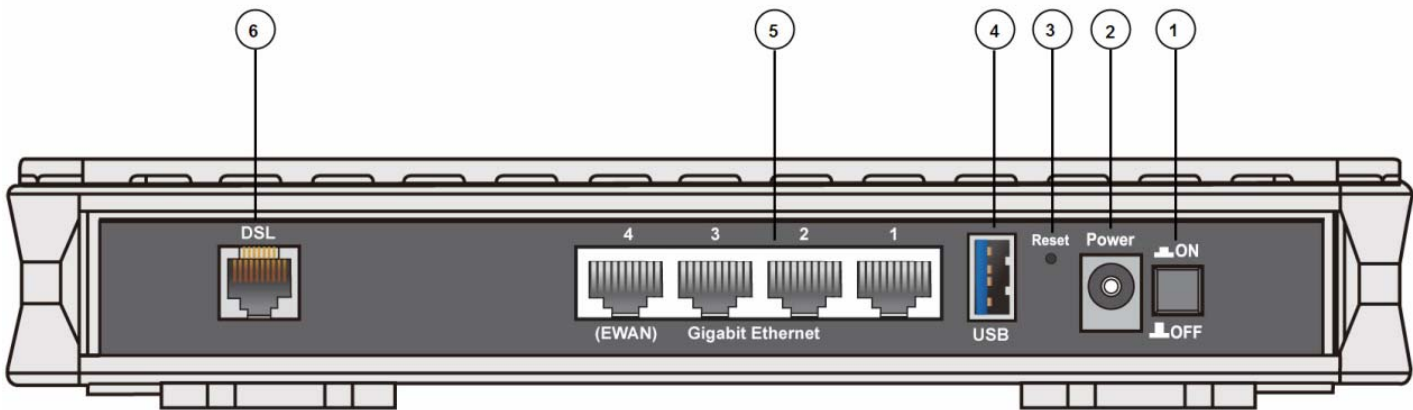


LED		Status	Meaning
1	Power	Red	Boot failure or in emergency mode
		Green	System ready
2	Ethernet Port 1-4 (EWAN)	Green	Transmission speed hitting 1000Mbps
		Orange	Transmission speed hitting 10/100Mbps
		Blinking	Data being transmitted/received
3	Wireless	Green	Wireless connection established
		Green blinking	Sending/receiving data
4	WPS	Green blinking	WPS configuration being in progress
		Off	WPS process completed or WPS is off
5	DSL	Green Blinking	DSL synchronizing or waiting for DSL synchronizing
		Green	Successfully connected to an ADSL DSLAM (Line Sync).
		Off	DSL cable unplugged
6	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

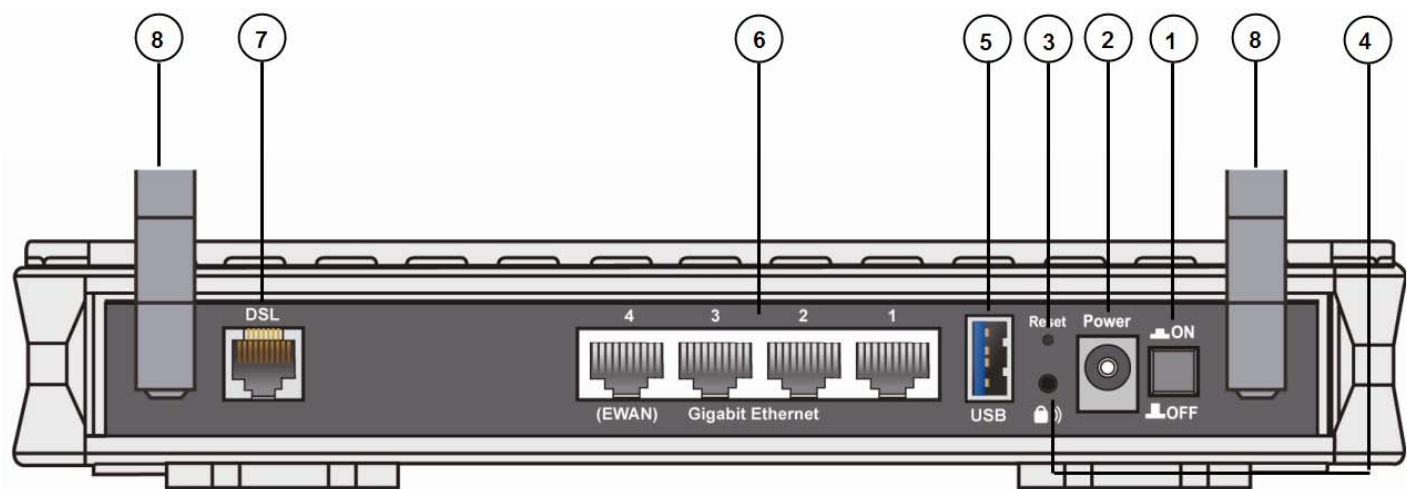
7800X



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 <b>5 seconds or above</b> : to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password)
4	USB	Connect the USB device (Printer, USB 2.0 storage, 3G/4G LTE USB modem) to this port.
5	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. <b>Note:</b> Port #4 can be configured as a WAN Interface for Broadband connectivity.
6	DSL	Connect this port to the DSL network with the RJ-11 cable (telephone) provided.



7800NX and 7800NXL



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 <b>5 seconds or above</b> : to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password)
4	WPS	Push WPS button to trigger Wi-Fi Protected Setup function.
5	USB	Connect the USB device (Printer, USB 2.0 storage, 3G/4G LTE 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. <b>Note:</b> Port #4 can be configured as a WAN Interface for Broadband connectivity.
7	DSL	Connect this port to the DSL network with the RJ-11 cable (telephone) provided.
8	Antenna	The detachable 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.



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.

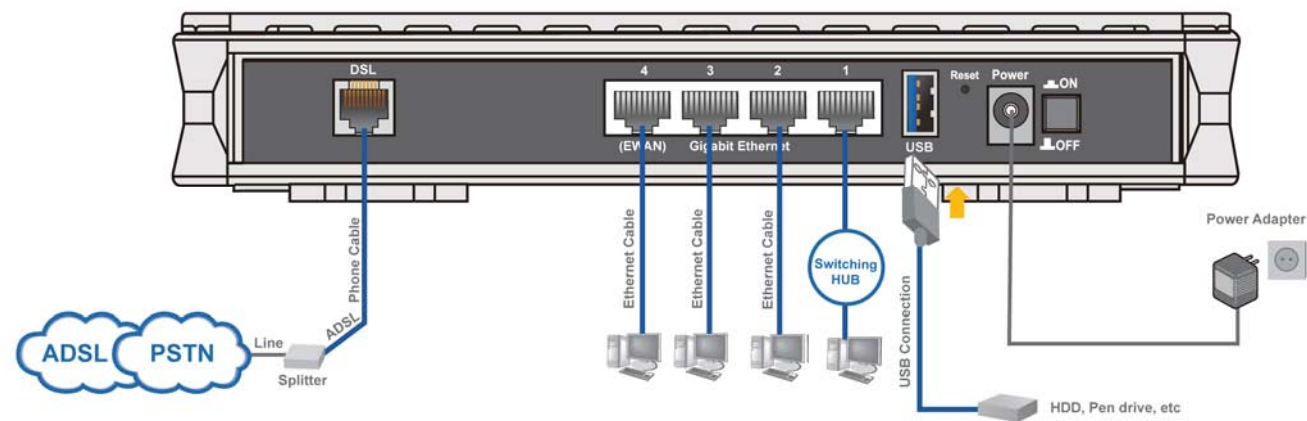


# Connecting Your Router

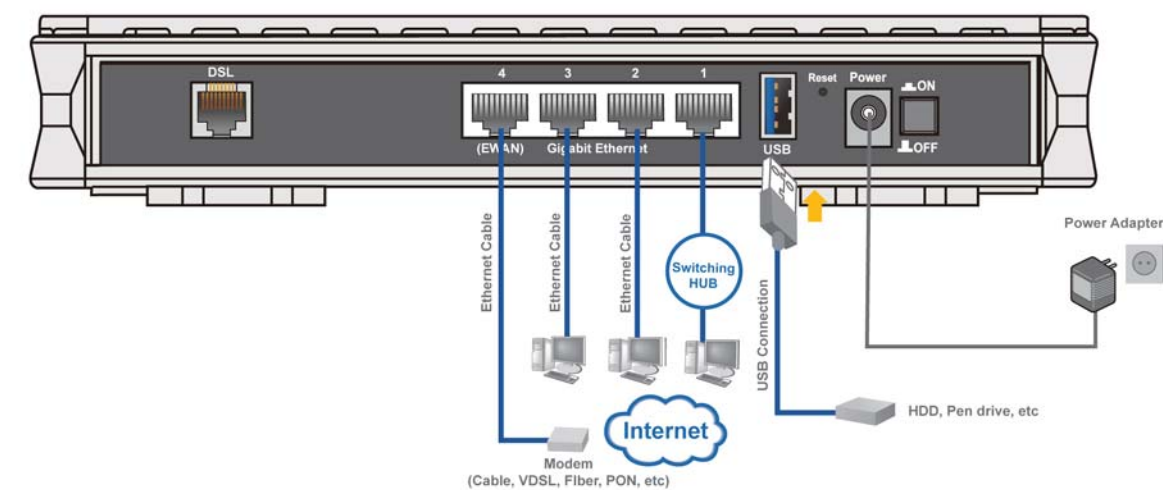
Users can connect the ADSL2+ router as the following.

7800X

ADSL Router mode:

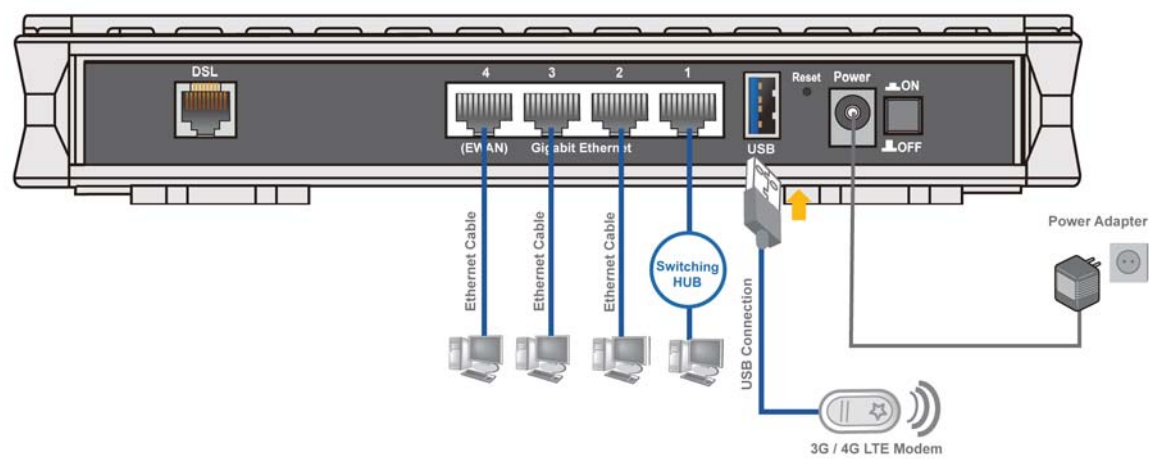


Broadband Router mode:





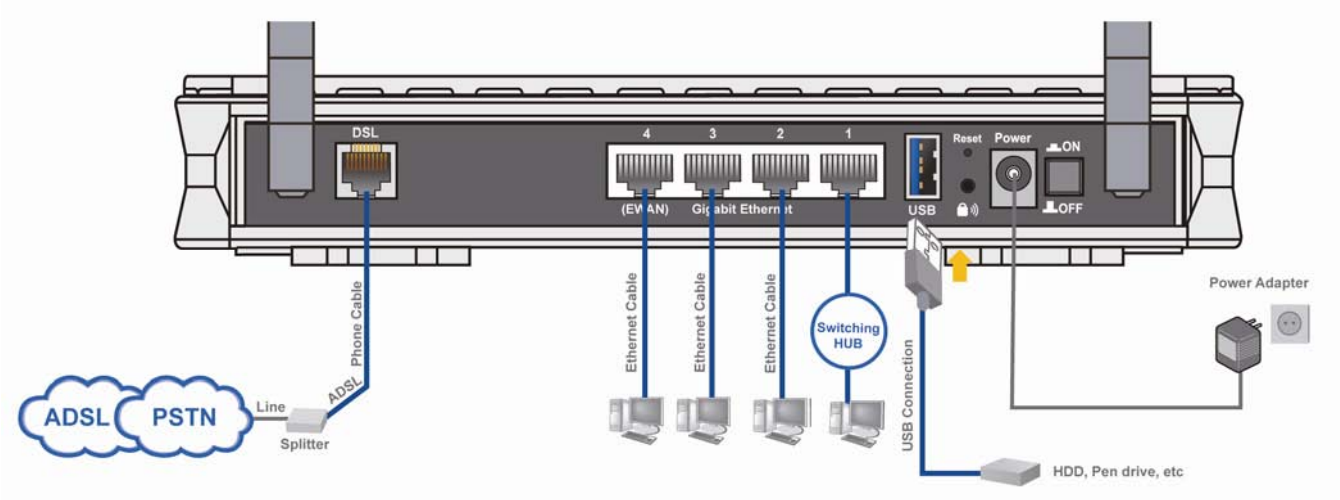
3G/LTE Router mode



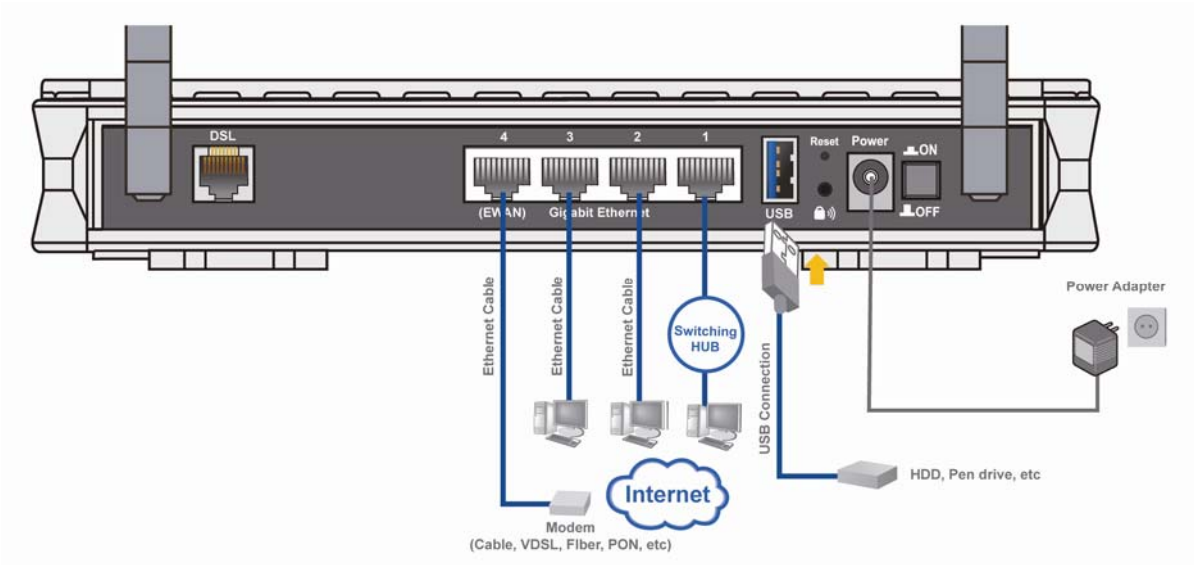


7800NX and 7800NXL

ADSL Router mode:

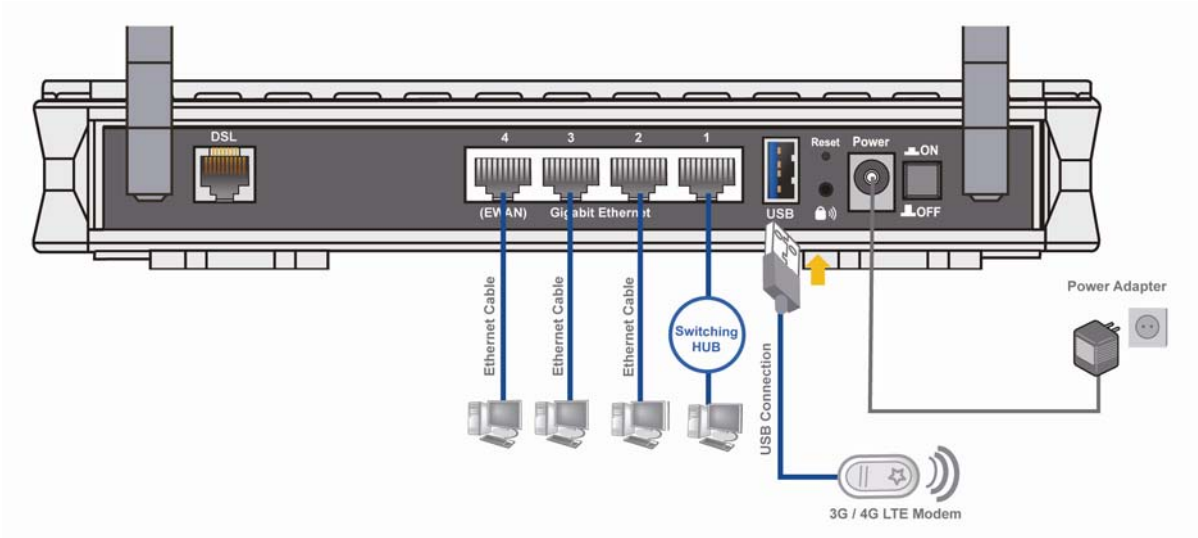


Broadband Router mode:





3G/LTE Router mode

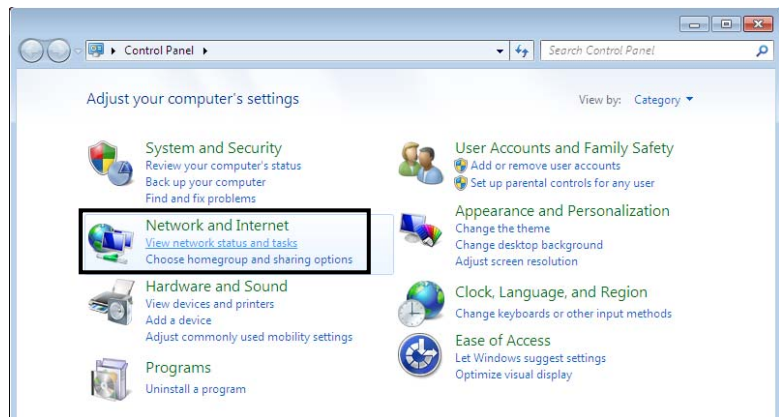




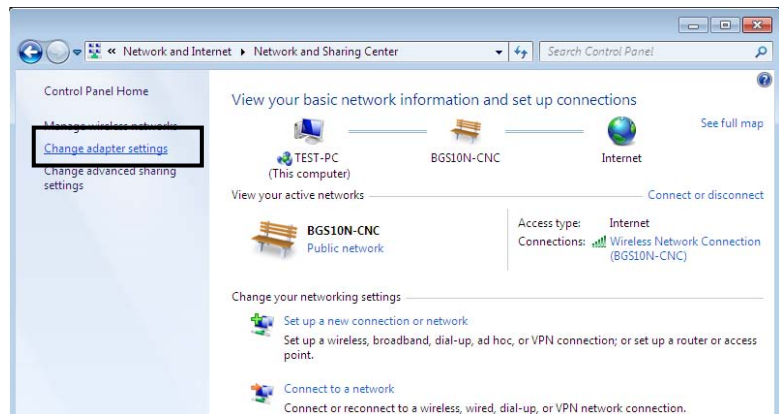
# Network Configuration

## Configuring a PC in Windows 7

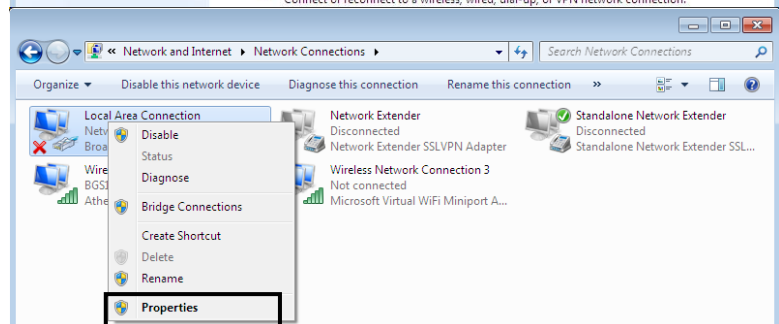
1. Go to **Start**. Click on **Control Panel**. Then click on **Network and Internet**.



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



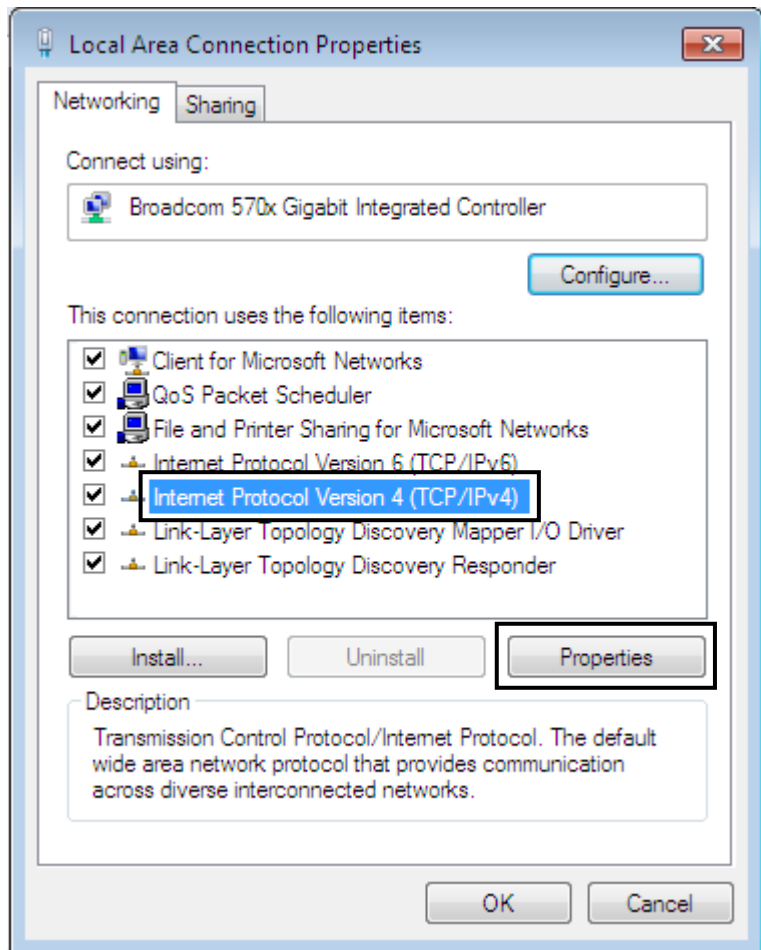
3. Select the **Local Area Connection**, and right click the icon to select **Properties**.



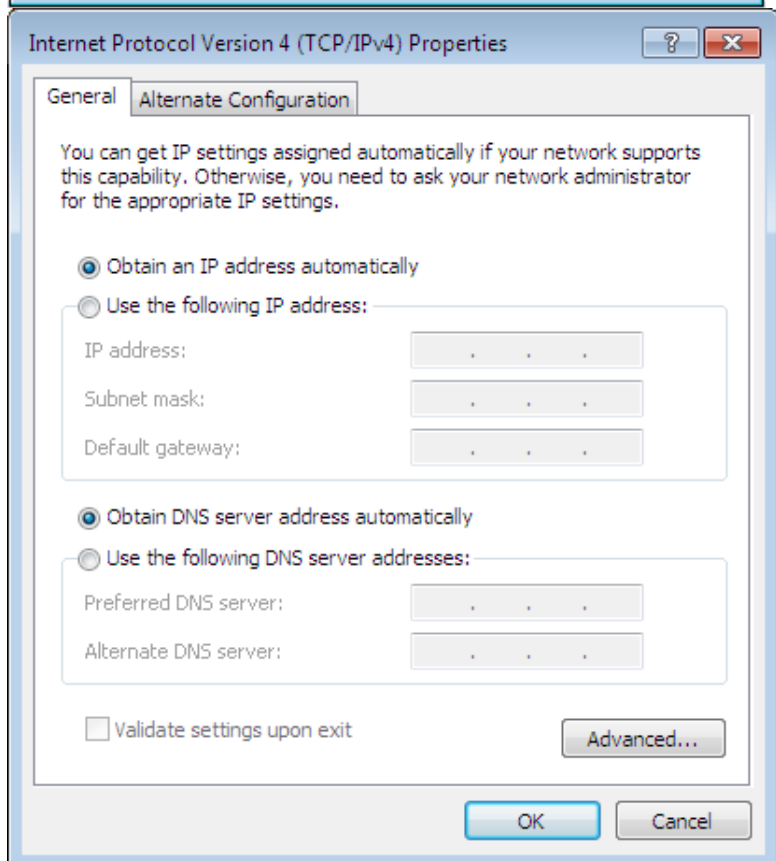


## IPv4:

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



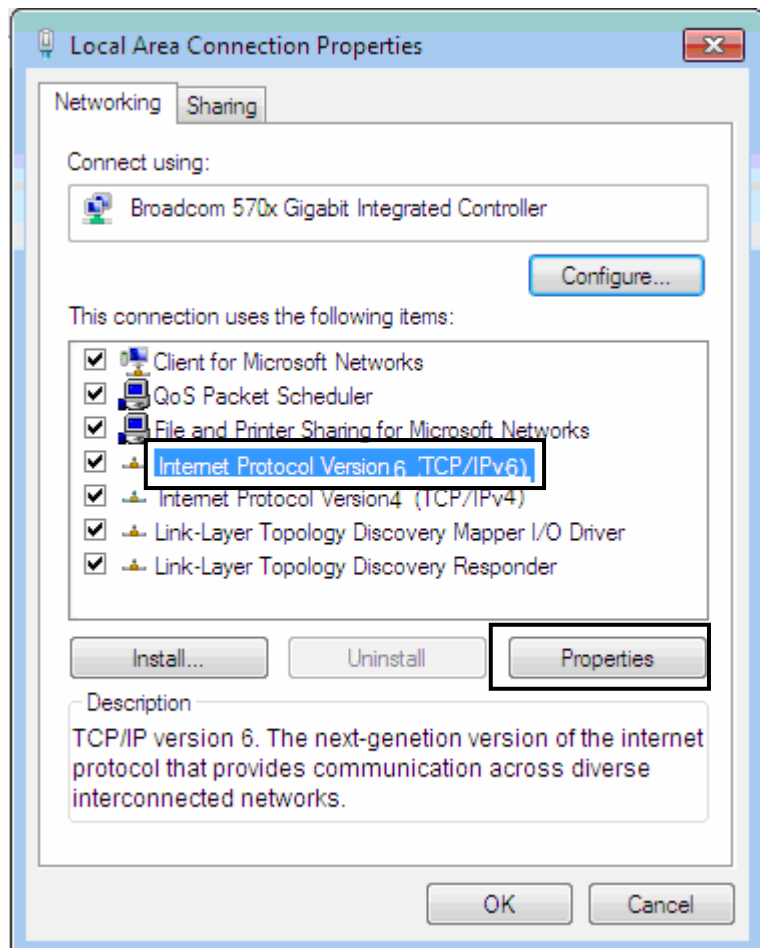
5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



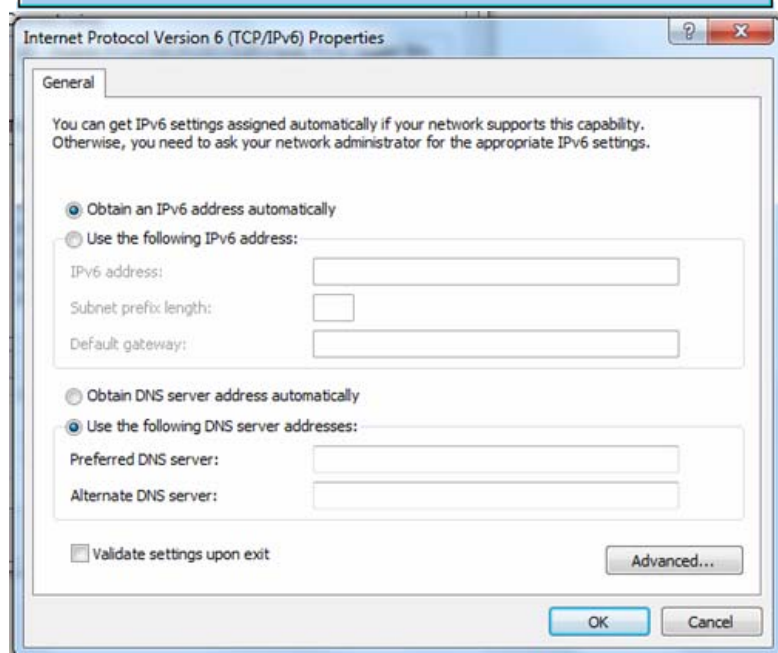


## IPv6:

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



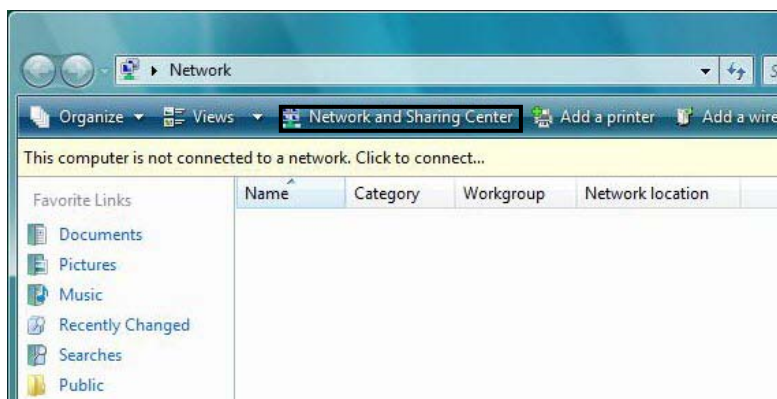
5. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



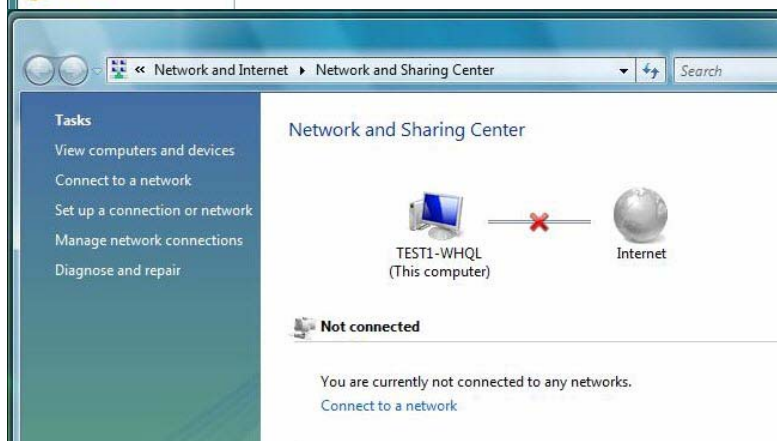


# Configuring a PC in Windows Vista

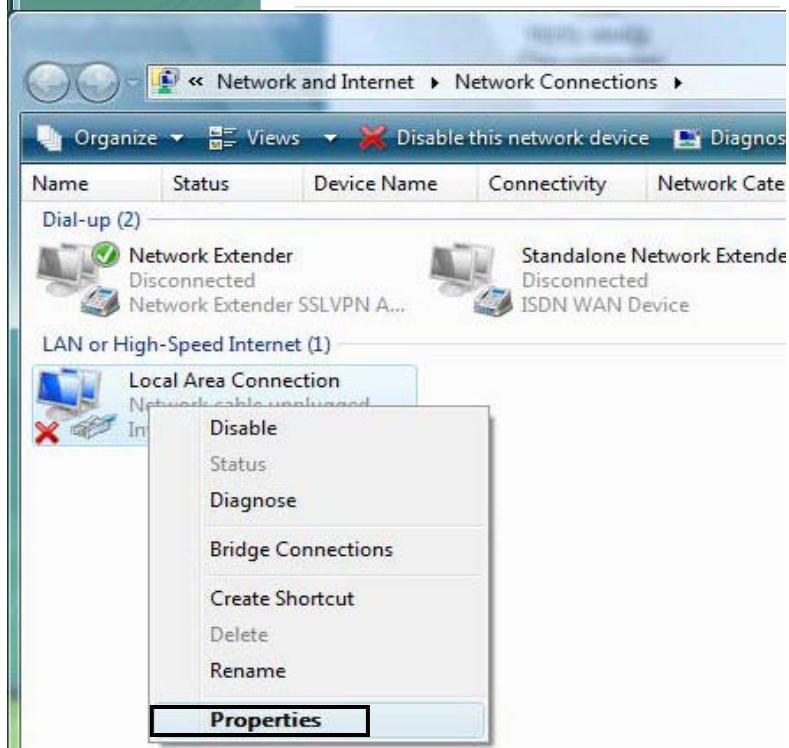
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



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



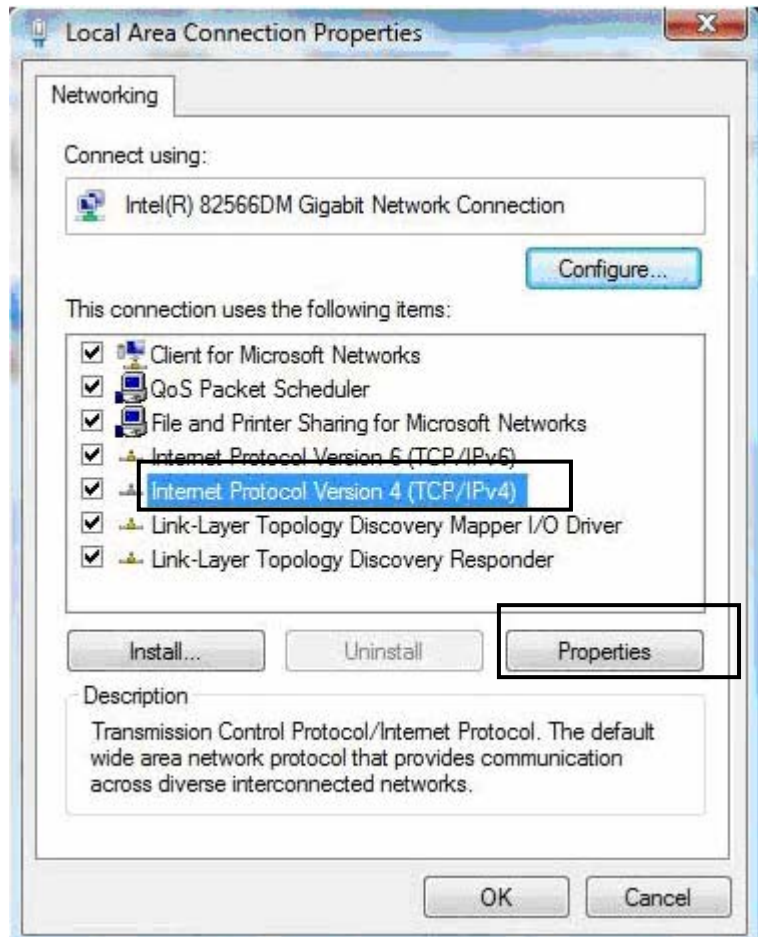
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



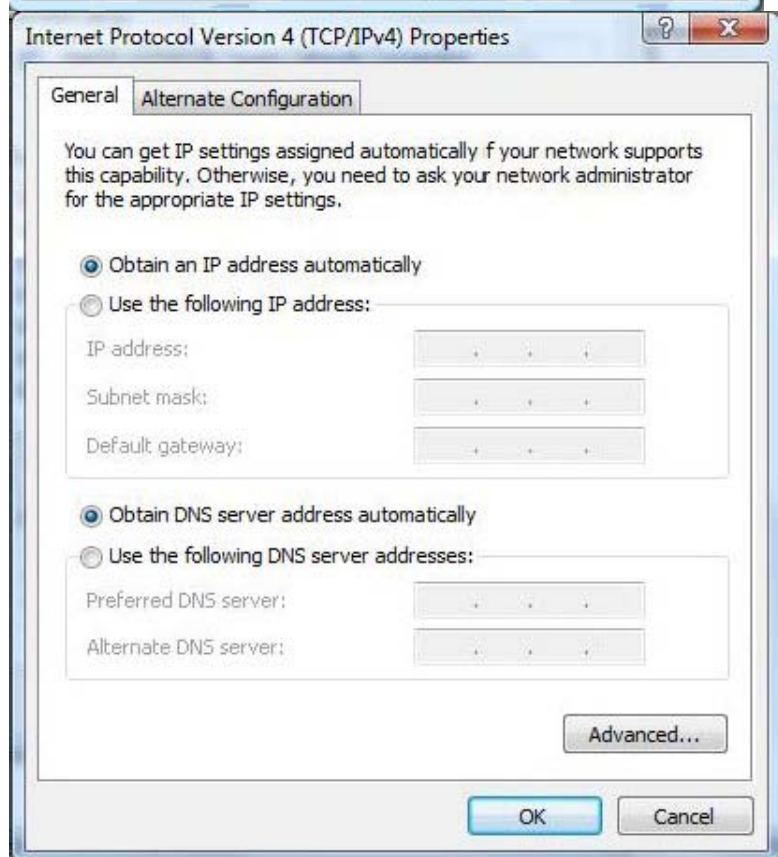


## IPv4:

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



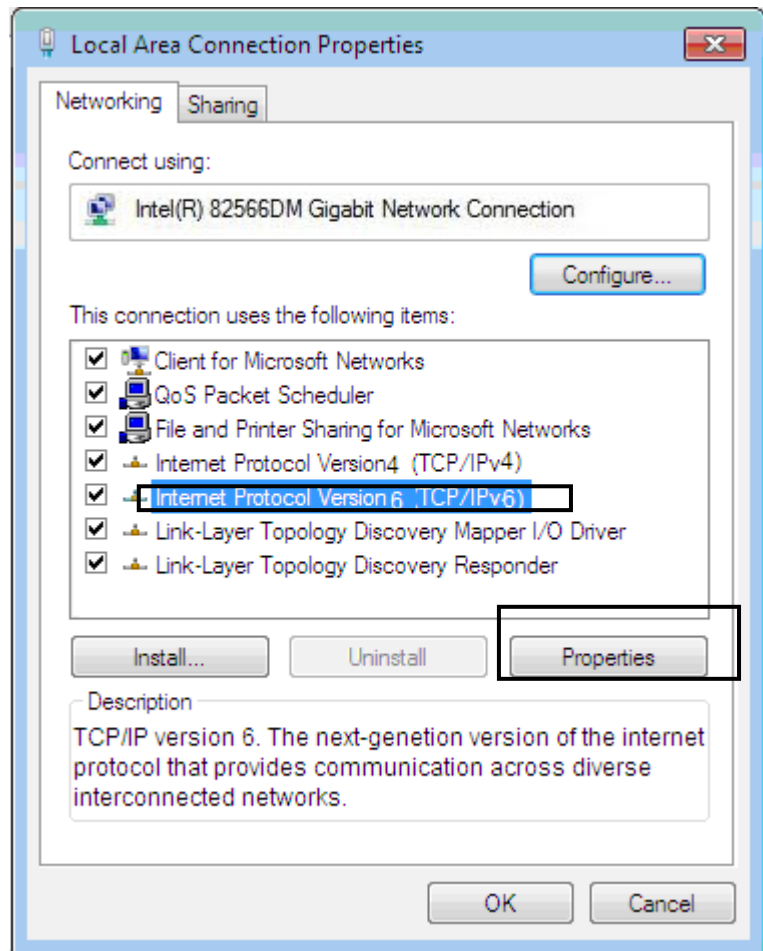
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.





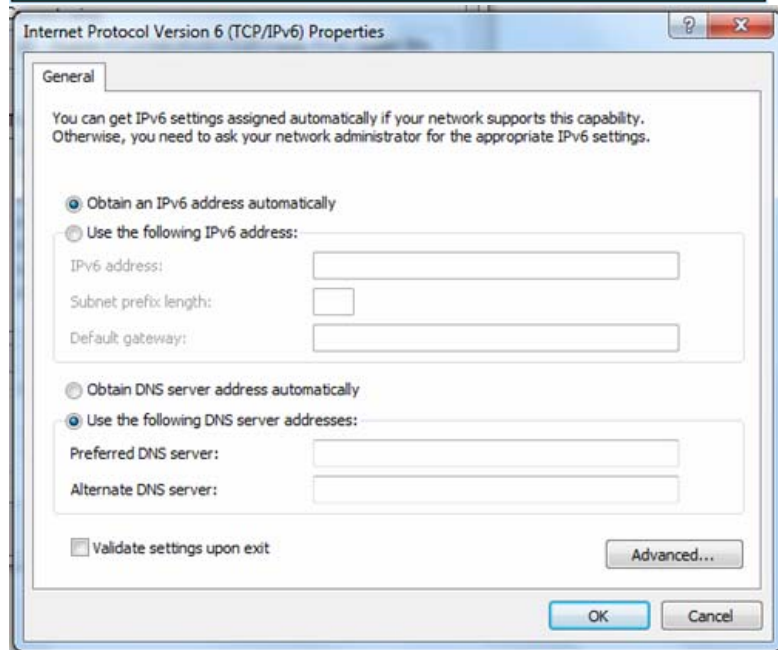
## IPv6:

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



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.

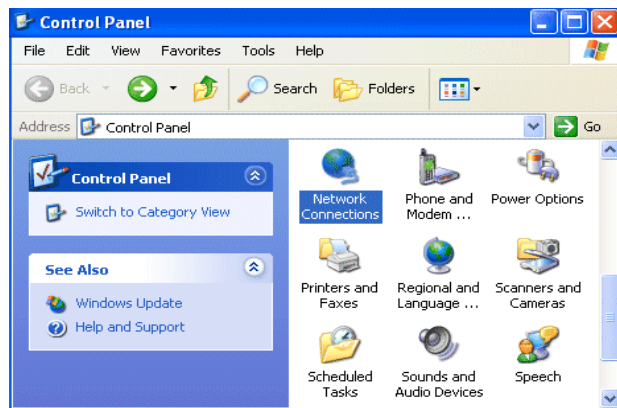




# Configuring a PC in Windows XP

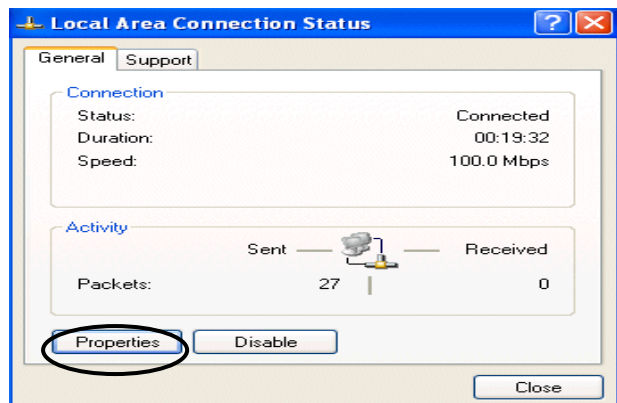
## IPv4:

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

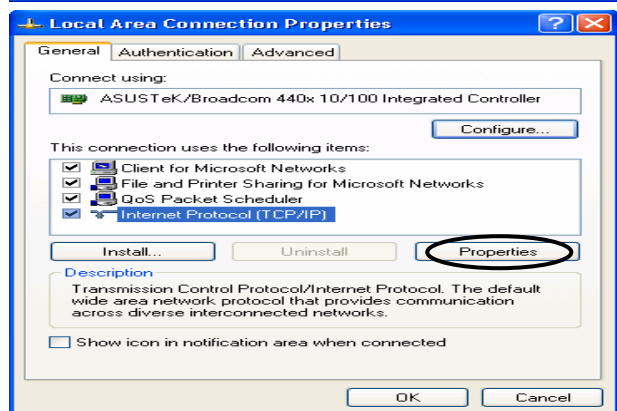


2. Double-click **Local Area Connection**.

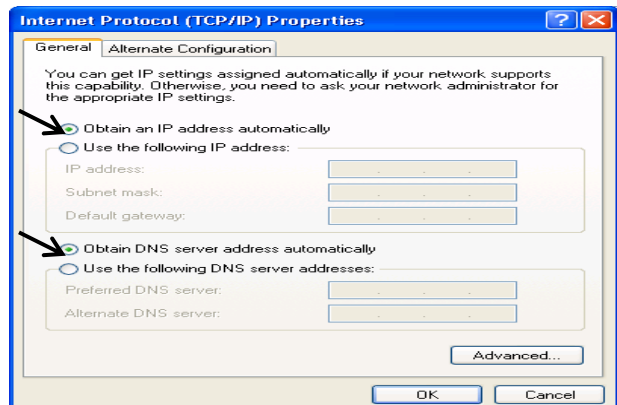
3. In the **Local Area Connection Status** window, click **Properties**.



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



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



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

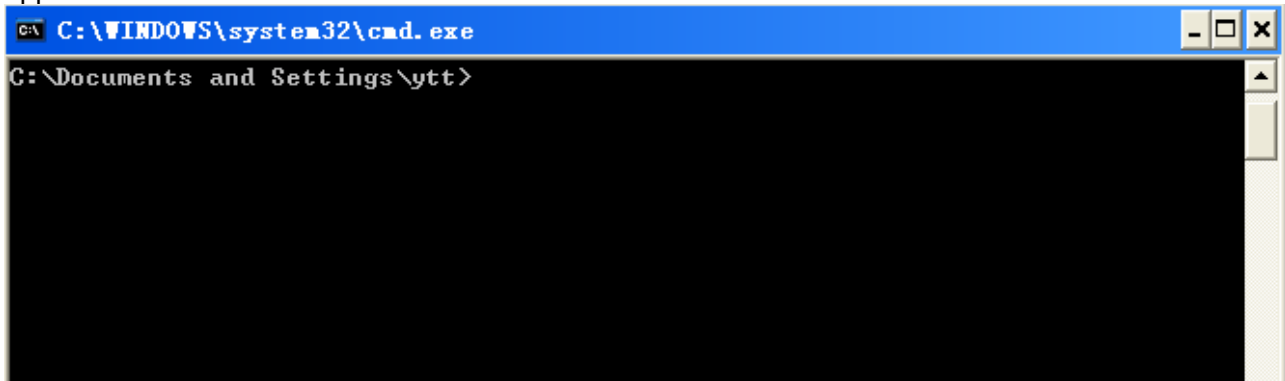


## IPv6:

IPv6 is supported by Windows XP, but you should install it first.

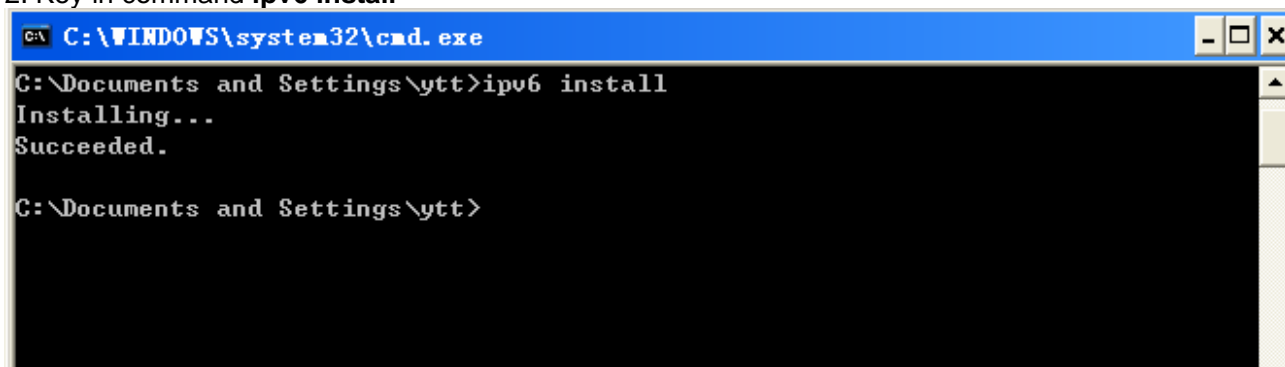
Act as shown below:

1. On the desktop, Click Start > Run, type cmd, then press Enter key in the keyboard, the following screen appears.



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



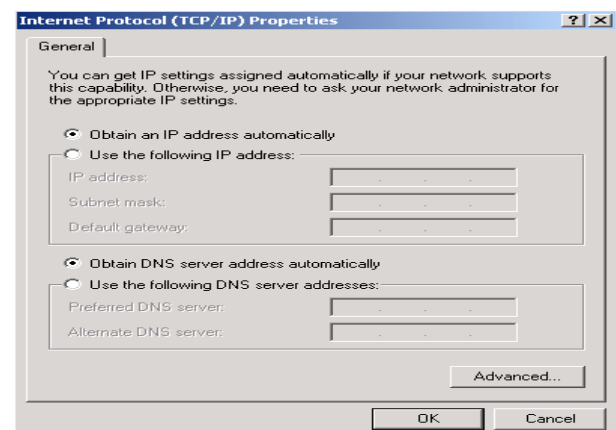
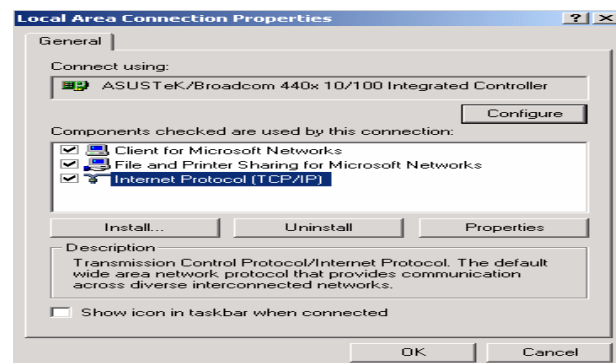
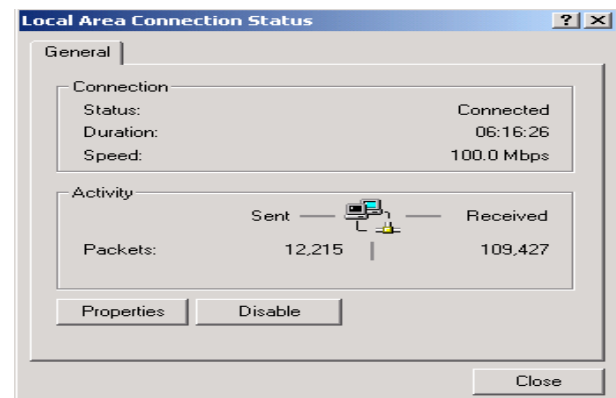
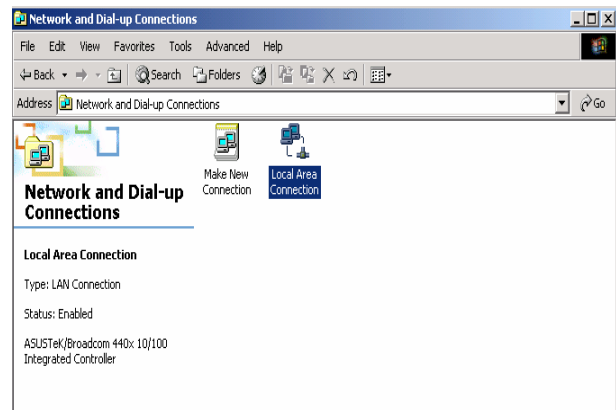
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.
C:\Documents and Settings\ytt>
```

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



# Configuring PC in Windows 2000

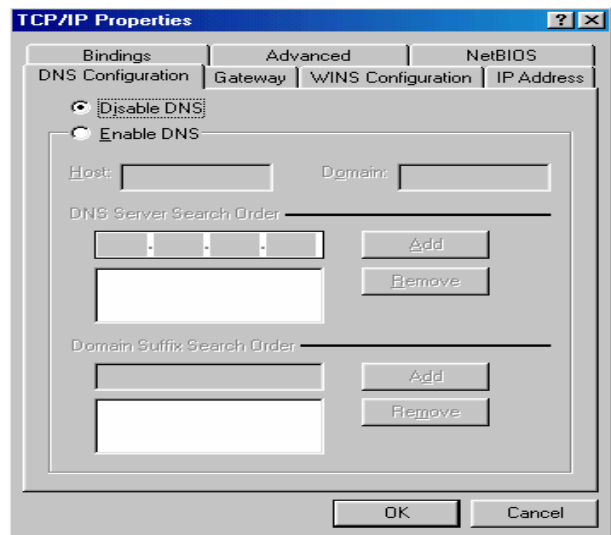
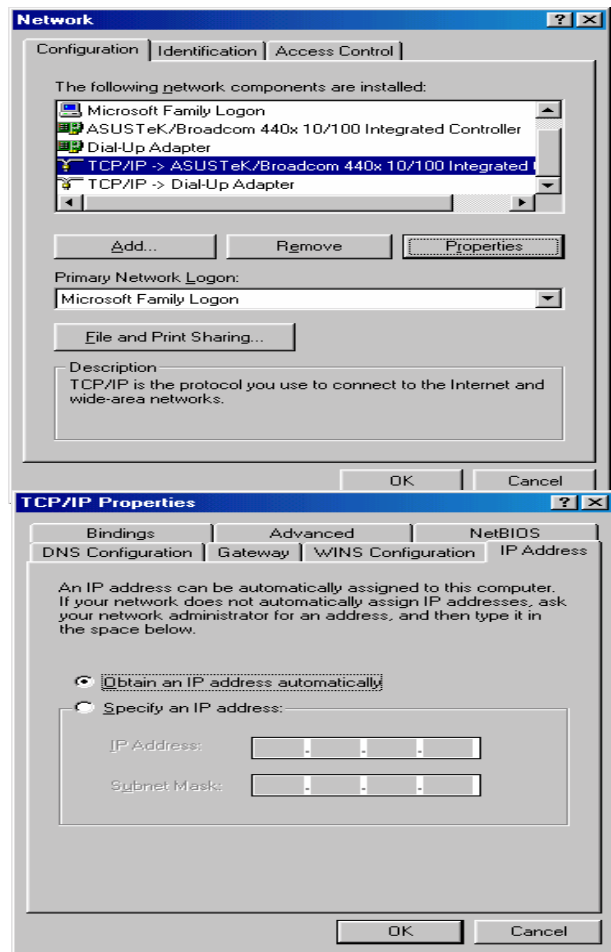
1. Go to Start > Settings > Control Panel.  
In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.
3. In the Local Area Connection Status window click Properties.
4. Select Internet Protocol (TCP/IP) and click Properties.
5. Select the Obtain an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





# Configuring PC in Windows 95/98/Me

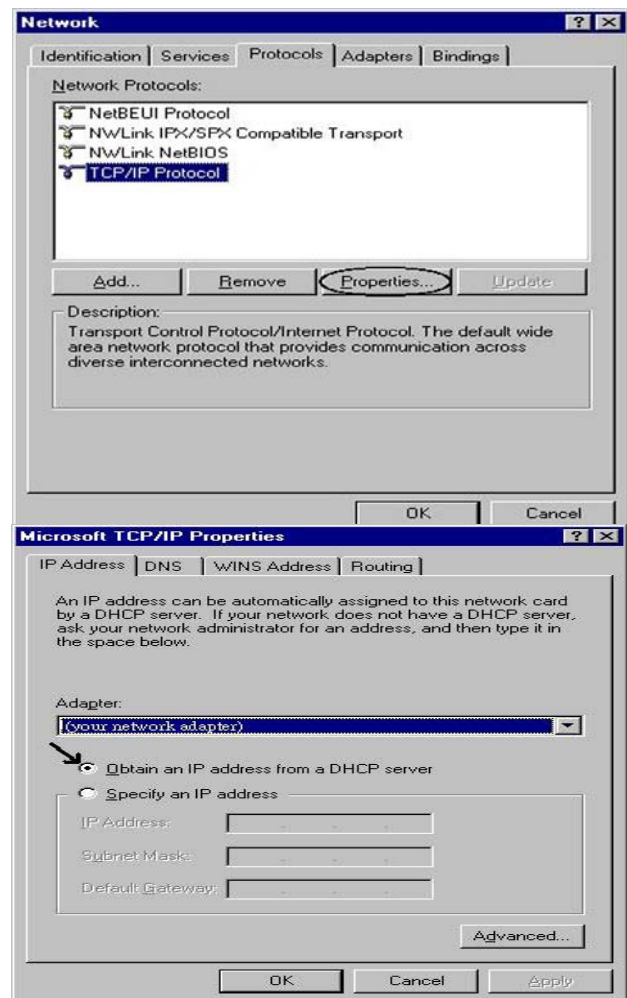
1. Go to Start > Settings > Control Panel.  
In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.
3. Select the Obtain an IP address automatically radio button.
4. Then select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





## Configuring PC in Windows NT4.0

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





# Factory Default Settings

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

## Web Interface (Username and Password)

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.



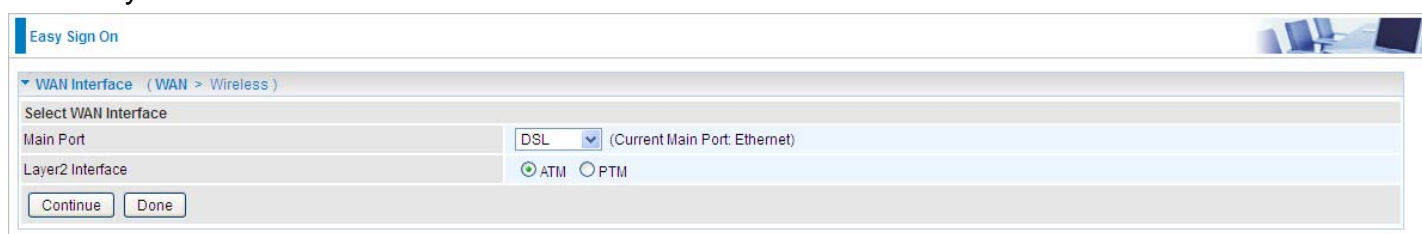
# Easy Sign On (EZSO)

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.

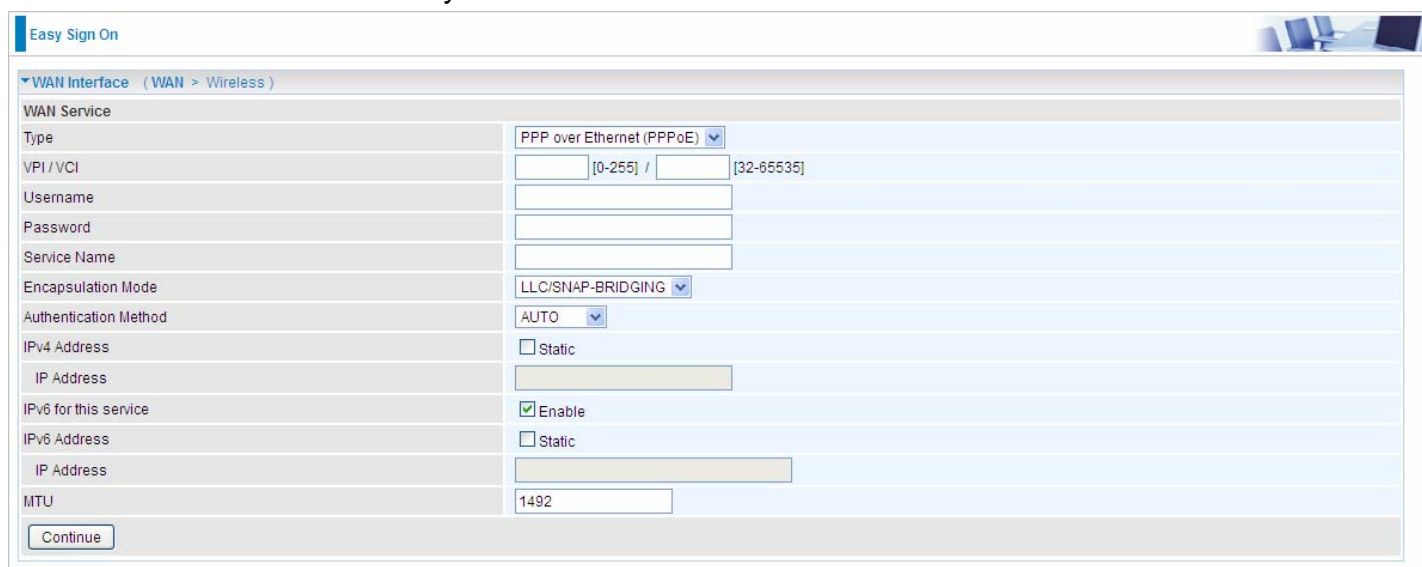
## DSL mode

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



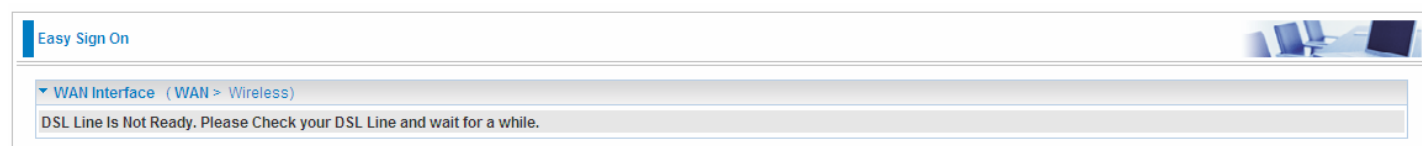
The screenshot shows the 'Easy Sign On' window with the 'WAN Interface' tab selected. Under 'Select WAN Interface', the 'Main Port' is set to 'DSL' (Current Main Port: Ethernet). The 'Layer2 Interface' has radio buttons for 'ATM' (selected) and 'PTM'. 'Continue' and 'Done' buttons are at the bottom.

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.



The screenshot shows the 'Easy Sign On' window with the 'WAN Service' tab selected. Fields include: '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 checkbox), 'IP Address', 'IPv6 for this service' (Enable checkbox, checked), 'IPv6 Address' (Static checkbox), 'IP Address', and 'MTU' (1492). A 'Continue' button is at the bottom.

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



The screenshot shows the 'Easy Sign On' window with the 'WAN Interface' tab selected. A message box at the bottom states: '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 )

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 )

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. Enable the wireless 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 )

Parameters

Wireless	<input checked="" type="checkbox"/> Enable
SSID	<input type="text" value="wlan-ap"/>
WPA Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

[Continue](#)

Easy Sign On


▼ Wireless ( WAN > Wireless )

Please wait while the device is configured.



## 6. Success in configuring the EZSO.

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](http://192.168.1.254)  
2. Continue to [wpad.home.gateway/wpad.dat](http://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 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 31M 33S
Date/Time	Tue Jan 15 07:11:51 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

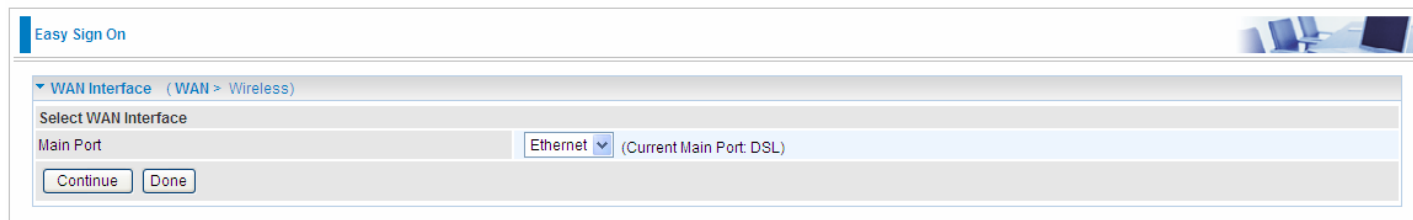
▼ WAN

Line Rate - Upstream (Kbps)	1315
Line Rate - Downstream (Kbps)	27431
Default Gateway	ppp0.1 (DSL)
Connection Time	00:01:57
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (DSL)

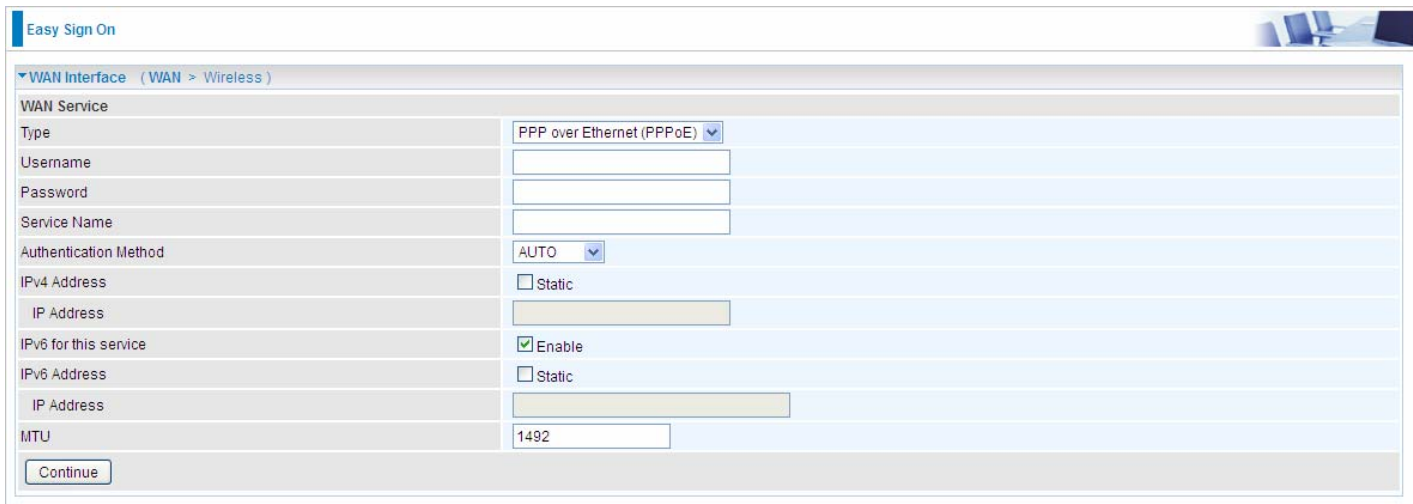


## Ethernet mode

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



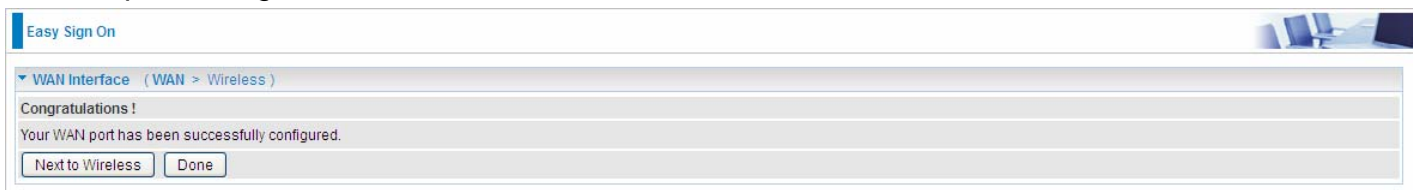
2. Enter the username, password from your ISP, for IP and DNS settings, also refer to your ISP. Here IPv6 service is enabled by default.



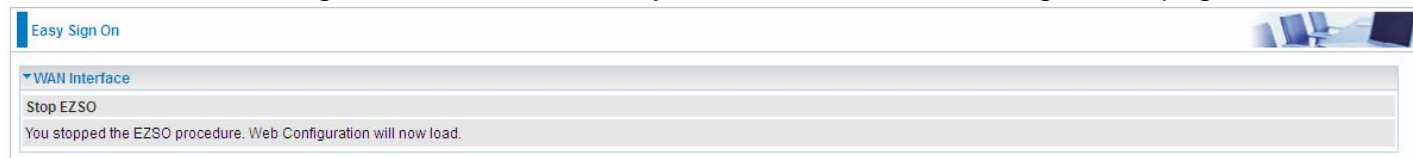
3. Wait while the device is configured.



4. WAN port configuration is success.



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





5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless 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).

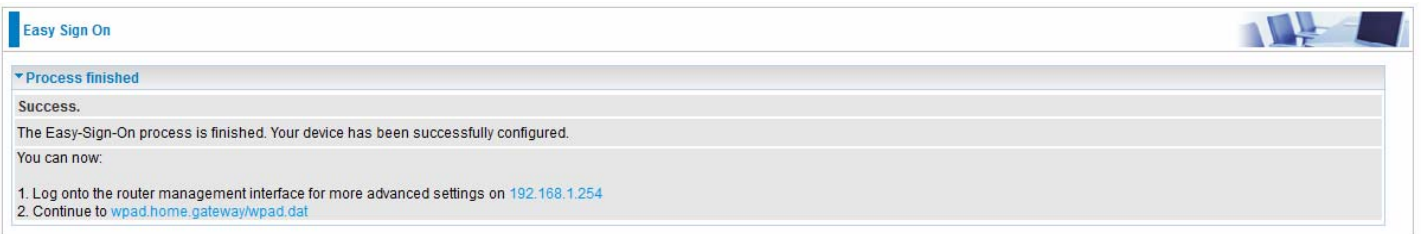


The screenshot shows the 'Easy Sign On' configuration page. At the top, there's a header 'Easy Sign On' with a small graphic of a laptop and chair. Below the header, a navigation bar shows 'Wireless (WAN > Wireless)'. The main content area is titled 'Parameters' and contains three rows: 'Wireless' with a checked 'Enable' checkbox, 'SSID' with a text box containing 'wlan-ap', and 'WPA Pre-Shared Key' with an empty text box and a link 'Click here to display'. A 'Continue' button is at the bottom left.



The screenshot shows the 'Easy Sign On' configuration page. At the top, there's a header 'Easy Sign On' with a small graphic of a laptop and chair. Below the header, a navigation bar shows 'Wireless (WAN > Wireless)'. The main content area displays the message 'Please wait while the device is configured.'

6. Success in configuring the EZSO.




The screenshot shows the 'Easy Sign On' configuration page. At the top, there's a header 'Easy Sign On' with a small graphic of a laptop and chair. Below the header, a navigation bar shows 'Process finished'. The main content area is titled 'Success.' and contains the text 'The Easy-Sign-On process is finished. Your device has been successfully configured. You can now:' followed by two numbered steps: '1. Log onto the router management interface for more advanced settings on 192.168.1.254' and '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 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 34M 39S
Date/Time	Tue Jan 15 07:14:58 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

▼ WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp0.1 (Ethernet)
Connection Time	00:00:46
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (Ethernet)



## 3G/LTE

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

Easy Sign On

WAN Interface (WAN > Wireless)

Select WAN Interface

Main Port 3G/LTE (Current Main Port: 3G/LTE)

Username

APN internet

Continue Done

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

Easy Sign On

WAN Interface (WAN > Wireless)

Parameters

Mode Use 3G/LTE dongle settings

APN internet

Username

Password

Authentication Method AUTO

PIN

Obtain DNS ☒ Automatic

Primary DNS / Secondary DNS

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

Continue

3. Wait while the device is configured.

Easy Sign On

WAN Interface (WAN > Wireless)

Please wait while the device is configured.

4. WAN port configuration is success.

Easy Sign On

WAN Interface (WAN > Wireless)

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. Enable wireless 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 )

Parameters

Wireless

SSID

WPA Pre-Shared Key

☒ Enable

Continue

[Click here to display](#)

7. Success in configuring the EZSO.

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/](http://www.sohu.com/)




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

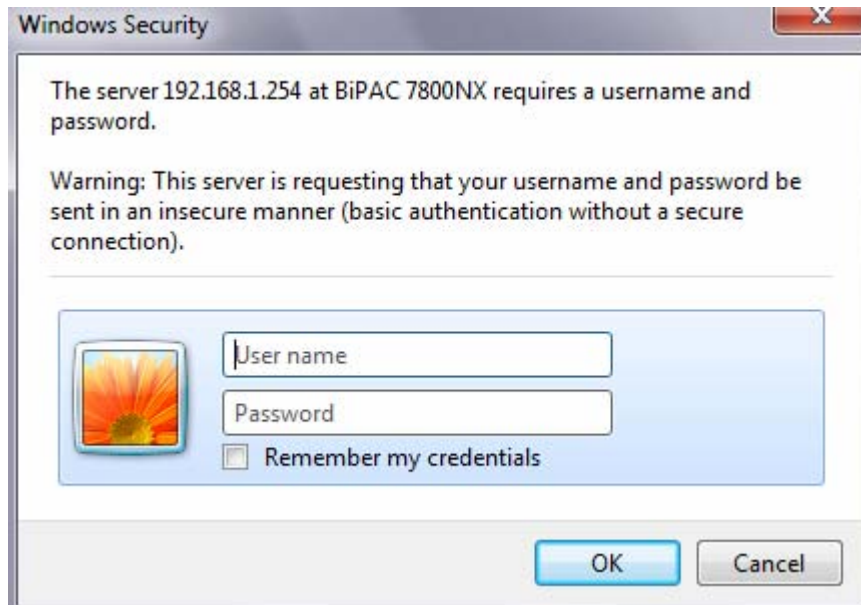
Status	
▼ Device Information	
Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 36M 16S
Date/Time	Tue Jan 15 07:16:35 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:feec:ffd0/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4
▼ WAN	
Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp3g0 (3G/LTE)
Connection Time	00:04:28
Primary DNS Server	221.6.4.66
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway	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.



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



Once you have logged on to your BiPAC 7800(N)X(L) 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, Route, 3G/LTE Status, Route, ARP, DHCP, Log)

● **Quick Start** (Quick Start)

● **Configuration** (LAN, Wireless *(7800NX and 7800NXL only)*, WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)

● **Advanced Setup** (Routing, DNS, Static ARP, UPnP, VPN *(7800NX and 7800X only)*, Certificate, Multicast, Management, Diagnostics)



# 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](#), [IPSec](#), [PPTP](#) and [Log](#) subsections are included.

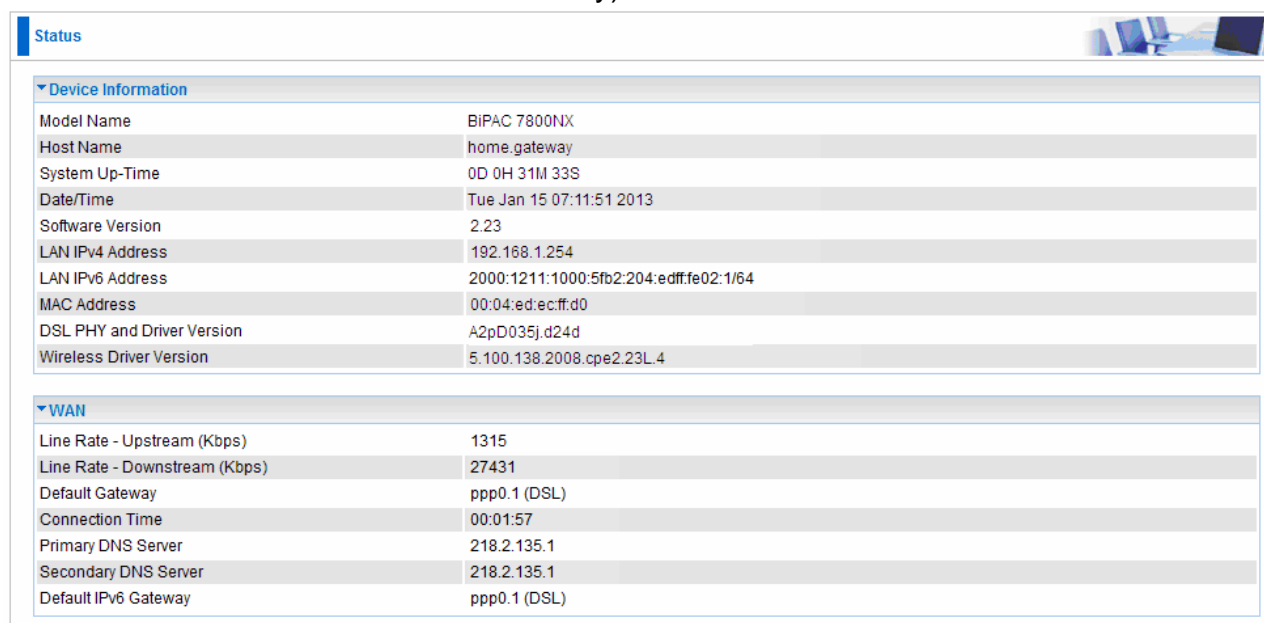
▼ Status
▪ Summary
▪ WAN
▶ Statistics
▶ Bandwidth Usage
▪ 3G/LTE Status
▪ Route
▪ ARP
▪ DHCP
▪ IPSec
▪ PPTP
▶ Log
▪ Quick Start
▶ Configuration
▶ Advanced Setup

(7800NX)



# Summary

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



The screenshot shows the 'Status' page of a router. It features a 'Status' tab at the top right. Below the tab, there are two expandable sections: 'Device Information' and 'WAN'. The 'Device Information' section lists various system details, and the 'WAN' section lists network configuration details.

Device Information	
Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 31M 33S
Date/Time	Tue Jan 15 07:11:51 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

WAN	
Line Rate - Upstream (Kbps)	1315
Line Rate - Downstream (Kbps)	27431
Default Gateway	ppp0.1 (DSL)
Connection Time	00:01:57
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (DSL)

## 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.

**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):** Displays Upstream line Rate in Kbps.

**Line Rate – Downstream (Kbps):** Displays Downstream line Rate in Kbps.

**Default Gateway:** Displays Default Gateway.

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

**Primary DNS Server:** Displays IPV4 address of Primary DNS Server.

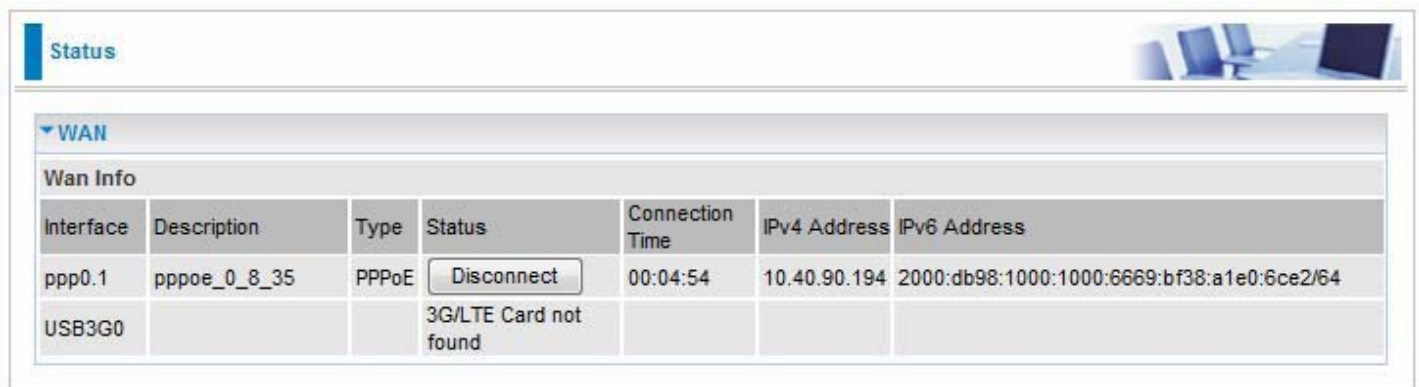
**Secondary DNS Server:** Displays IPV4 address of Secondary DNS Server.

**Default IPv6 Gateway:** Displays the IPv6 Gateway used.



# WAN

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



The screenshot shows a 'Status' window with a 'WAN' section expanded. It contains a table titled 'Wan Info' with columns for Interface, Description, Type, Status, Connection Time, IPv4 Address, and IPv6 Address. Two rows are visible: one for 'ppp0.1' (PPPoE) which is connected with a 'Disconnect' button, and another for 'USB3G0' (3G/LTE) which is not found.

Wan Info						
Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address
ppp0.1	pppoe_0_8_35	PPPoE	<button>Disconnect</button>	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64
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.



# 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.

Status

LAN Statistics

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

Reset

(DSL)

Status

LAN Statistics

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P3	0	0	0	0	0	0	0	0
P2	81681997	191880	0	0	198896059	237800	0	0
P1	0	0	0	0	0	0	0	0
wl0	1179834	10153	0	0	2506888	12190	0	0

Reset

(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.

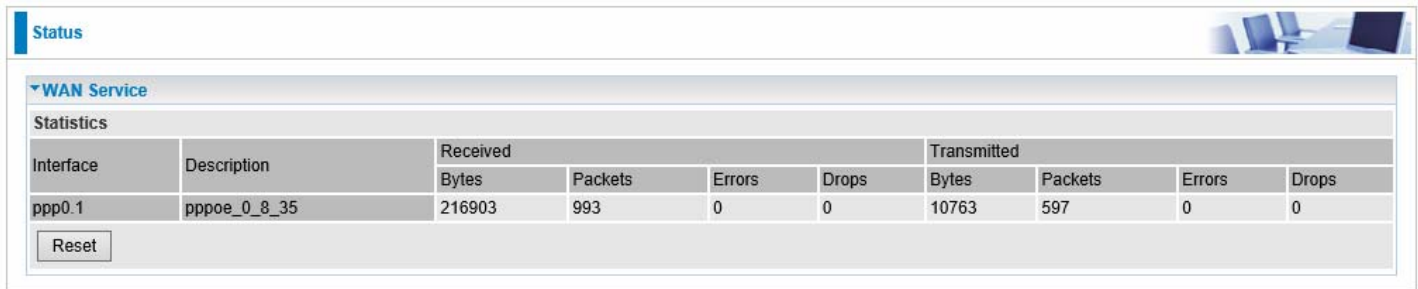
**Drops:** Display the statistics of drops arising in Receiving or Transmitting data.

**Reset:** Press this button to refresh the statistics.



## WAN Service

The table shows the statistics of WAN.



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

Reset

**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 Packets.

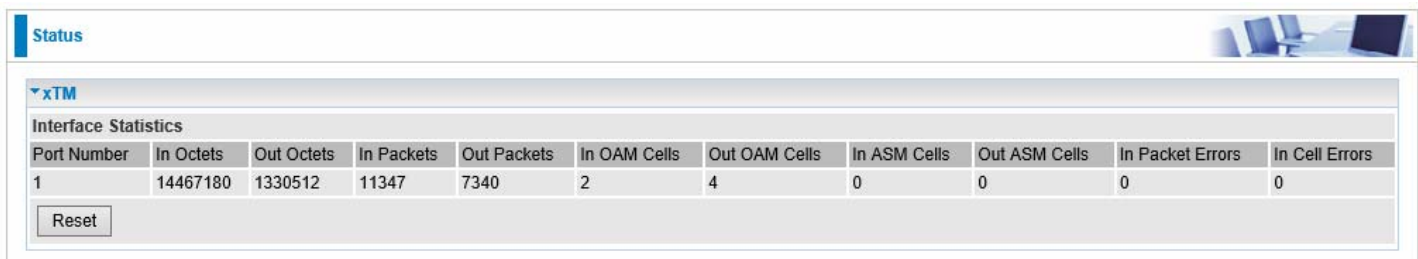
**Errors:** Display the statistics of errors arising in Receiving or Transmitting data.

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

**Reset:** Press this button to refresh the statistics.

## xTM

The Statistics-xTM screen displays all the xTM 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

Reset

**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 (0.1 dB)	71	74
Attenuation (0.1 dB)	0	8
Output Power (0.1 dBm)	72	93
Attainable Rate (Kbps)	28008	1331
Rate (Kbps)	27403	1303
MSGc (# of bytes in overhead channel message)	51	27
B (# of bytes in Mux Data Frame)	243	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)	0.2846	1.9878
L (# of bits in PMD Data Frame)	6858	330
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	1553346
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	0	0
OCD Errors	0	0
LCD Errors	0	0
Total Cells	54842488	2595079
Data Cells	2543	1681
Bit Errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	1869	1869
<div><div>xDSL BER Test</div><div>Reset</div></div>		

**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 (0.1 dB):** show the Signal to Noise Ratio(SNR) margin.

**Attenuation (0.1 dB):** This is estimate of average loop attenuation of signal.

**Output Power (0.1 dBm):** show the output power.

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

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



**K (number of bytes in DMT frame):** show the number of bytes in DMT frame.

**R (number of check bytes in RS code word):** show the number of check bytes in RS code word.

**S (RS code word size in DMT frame):** show the RS code word size in DMT 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

Start Close

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

ADSL BER Test -- Running

The xDSL BER test is in progress.

Connection Speed 8000 Kbps

The test will run for 20 seconds

Stop Close



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	0x0000000008A31680
Error Ratio	0.00e+00

Close

**Reset:** Click this button to reset the statistics.

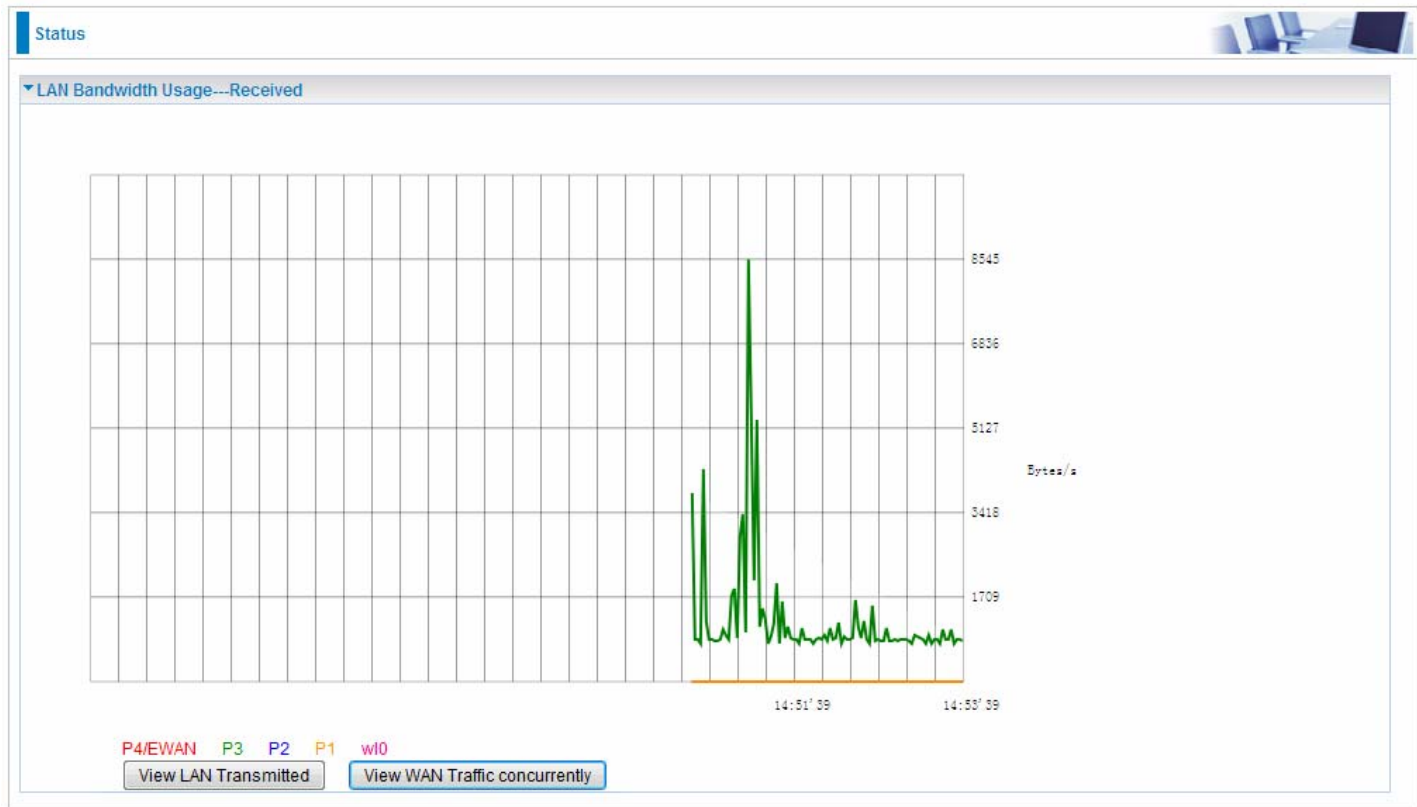


# Bandwidth Usage

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.

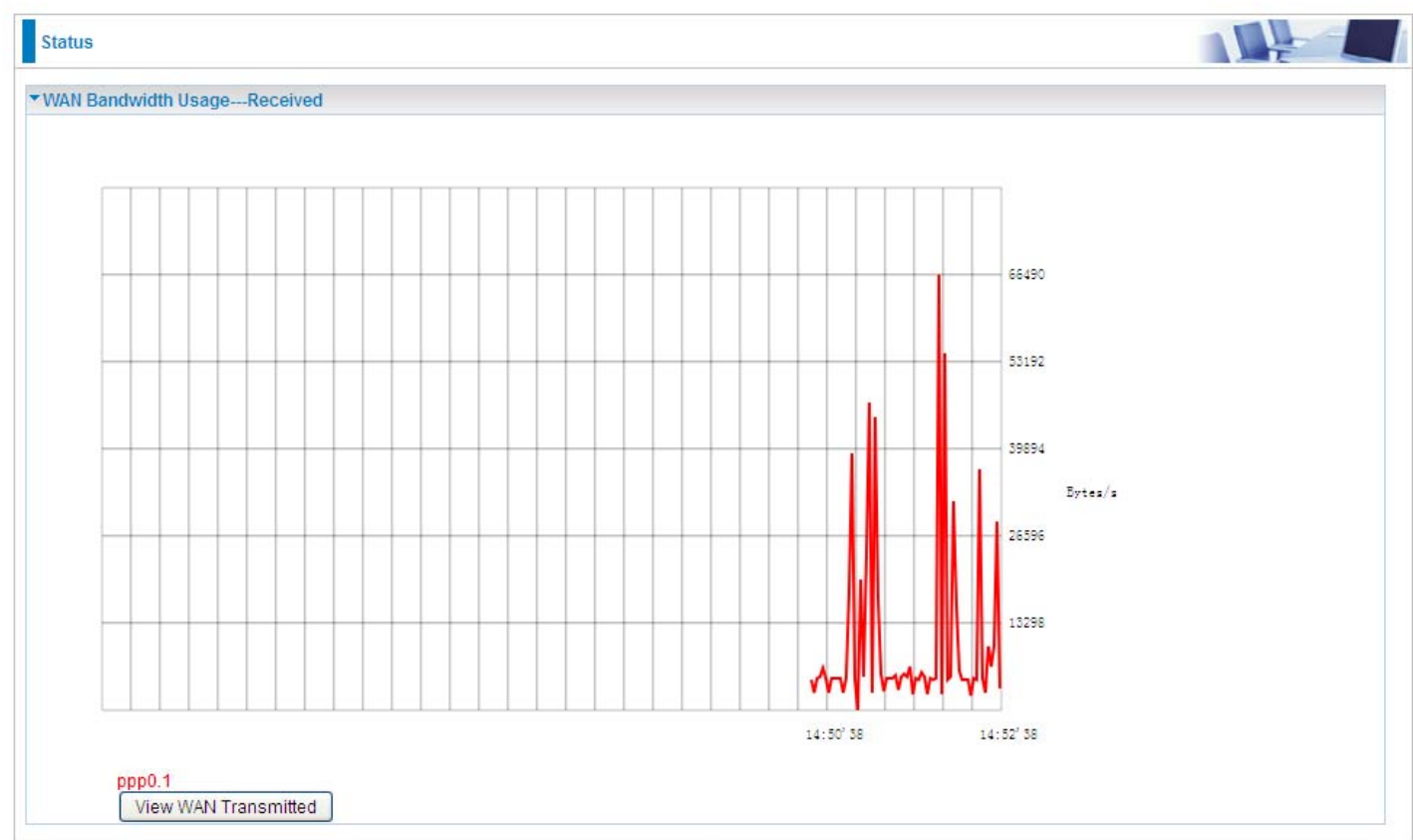


(DSL)

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.)

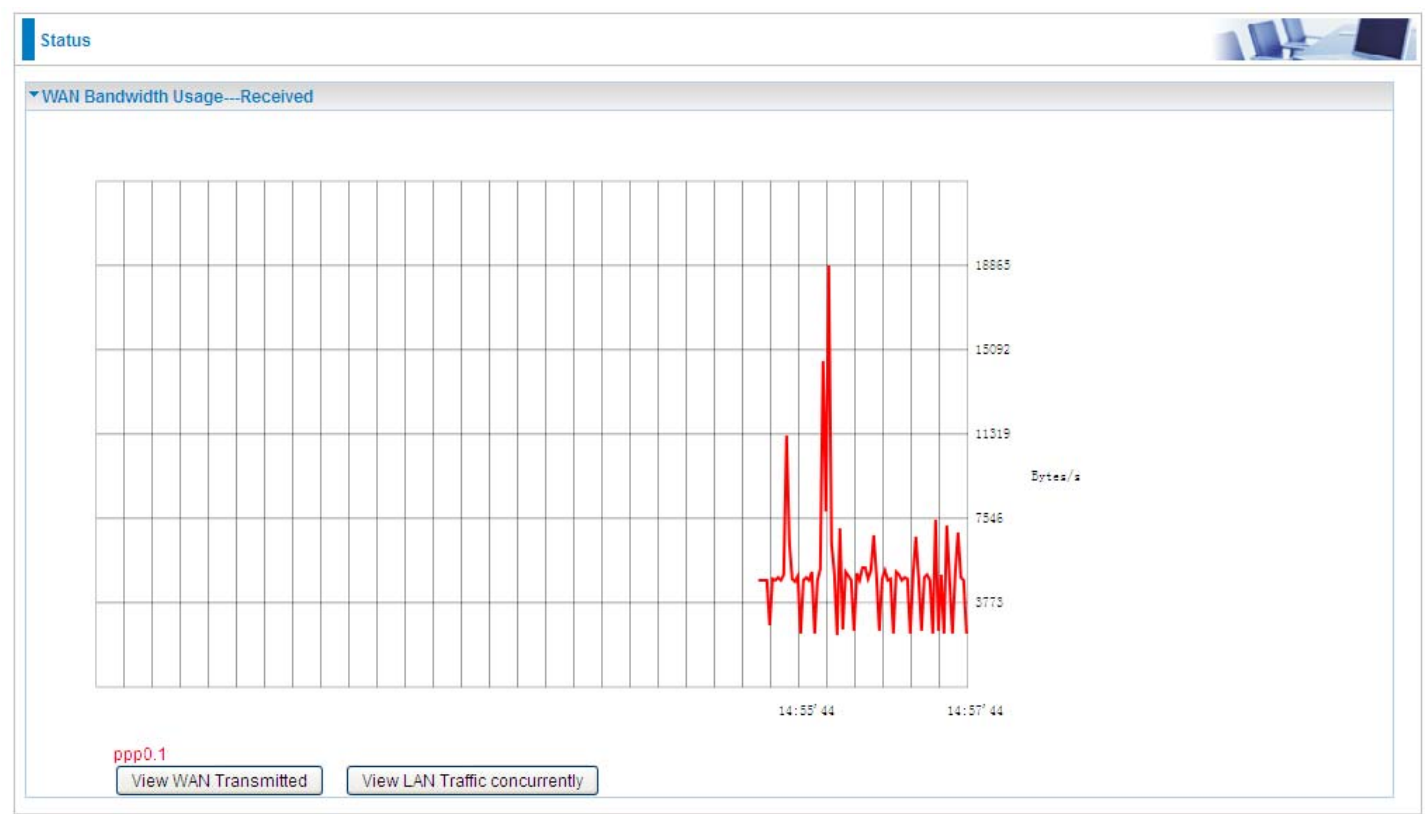


When you press **View WAN Traffic concurrently** button, the WAN Bandwidth Usage pops up so that users can view the WAN traffic concurrently.





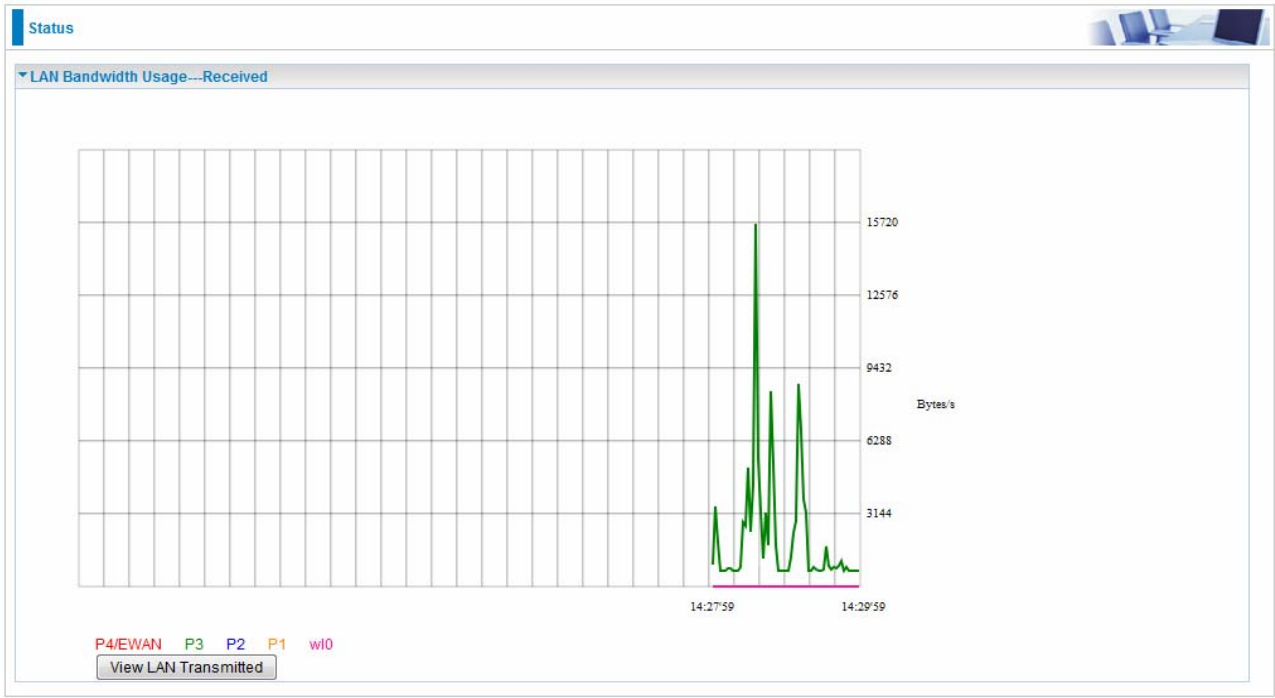
WAN Service



Press **View WAN Transmitted** button to change the diagram to the statistics from a Received Bytes of view.




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





## 3G/LTE Status

Status	
▼ 3G/LTE Status	
Parameters	
Status	Up
Signal Strength	
Network Name	China Unicom
Network Mode	UMTS
Card Name	K4505-Z
Card Firmware	BD_P680A2V1.0.0B05

**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.



# 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.

- ① **U:** Show the route is activated or enabled.
- ① **H (host):** destination is host not the subnet.
- ① **G:** Show that the outside gateway is needed to forward packets in this route.
- ① **R:** Show that the route is reinstated from dynamic routing.
- ① **D:** Show that the route is dynamically installed by daemon or redirecting.
- ① **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 Filtering** function. Here IPv6 Neighbor Table, listed with IPv6 address-MAC mapping, is supported.

Device Info			
▼ ARP			
ARP Table			
IP Address	Flag	MAC Address	Device
192.168.1.1	Incomplete	00:00:00:00:00:00	br0
192.168.1.100	Complete	00:22:64:1b:6ffd	br0
Neighbor Cache Table			
IPv6 Address		MAC Address	Device
fe80::d160:5adb:9009:87ae		00:22:64:1b:6ffd	br0
2000:1211:1002:4f0b:bd94:aa1e:3567:9759		00:22:64:1b:6ffd	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.

- ① Complete: the route resolving is processing well.
- ① M(Marked as permanent entry): the route is permanent.
- ① 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”.

## Neighbor Cache Table

**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”.



# DHCP

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

Status			
▼ DHCP			
Leased Table			
Host Name	MAC Address	IP Address	Expires In
billion-17bc6f1	18:a9:05:38:04:03	192.168.1.1	21 hours, 19 minutes, 7 seconds
ytt-PC	00:16:d4:a7:54:4a	192.168.1.2	23 hours, 26 minutes, 20 seconds

**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.

**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.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

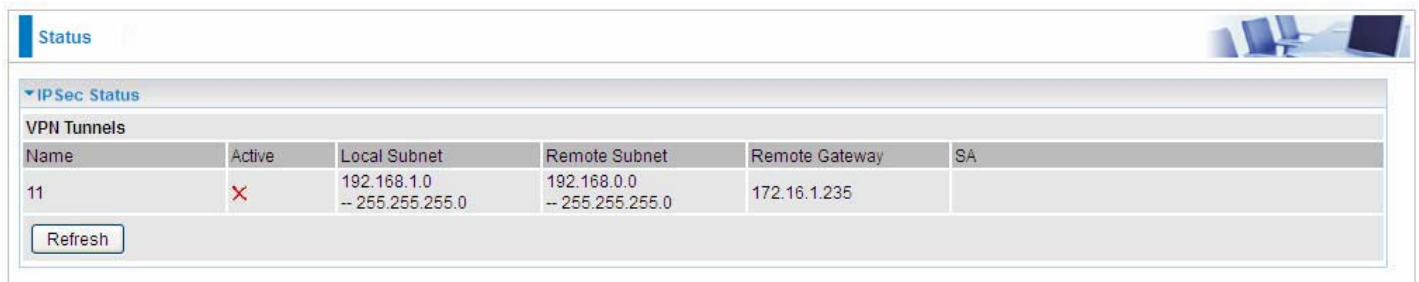
Pinging billion-17bc6f1.home.gateway [192.168.1.1] with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64


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>
```



## IPSec (7800(N)X only)

A screenshot of a network management interface. At the top left is a 'Status' tab. To the right is a small graphic of a computer desk. Below the tab is a section titled 'IPSec Status' with a dropdown arrow. Underneath is a table with the heading 'VPN Tunnels'. The table has six columns: 'Name', 'Active', 'Local Subnet', 'Remote Subnet', 'Remote Gateway', and 'SA'. There is one data row with the name '11'. The 'Active' column shows a red 'X' icon. The 'Local Subnet' column shows '192.168.1.0' and '-- 255.255.255.0'. The 'Remote Subnet' column shows '192.168.0.0' and '-- 255.255.255.0'. The 'Remote Gateway' column shows '172.16.1.235'. The 'SA' column is empty. Below the table is a 'Refresh' button.

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	
<input type="button" value="Refresh"/>					

**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 (7800(N)X only)

Status						
▼ PPTP Status						
PPTP Server ▼						
Name ▼	Enable	Status	Connection Type	Peer Network IP	Connect By	Action
test	✓	Connected	Remote Access		172.16.1.207	<button>Drop</button>
PPTP Client ▼						
Name	Enable	Status	Connection Type	Peer Network IP	Client IP	Action
<button>Refresh</button>						

### 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.

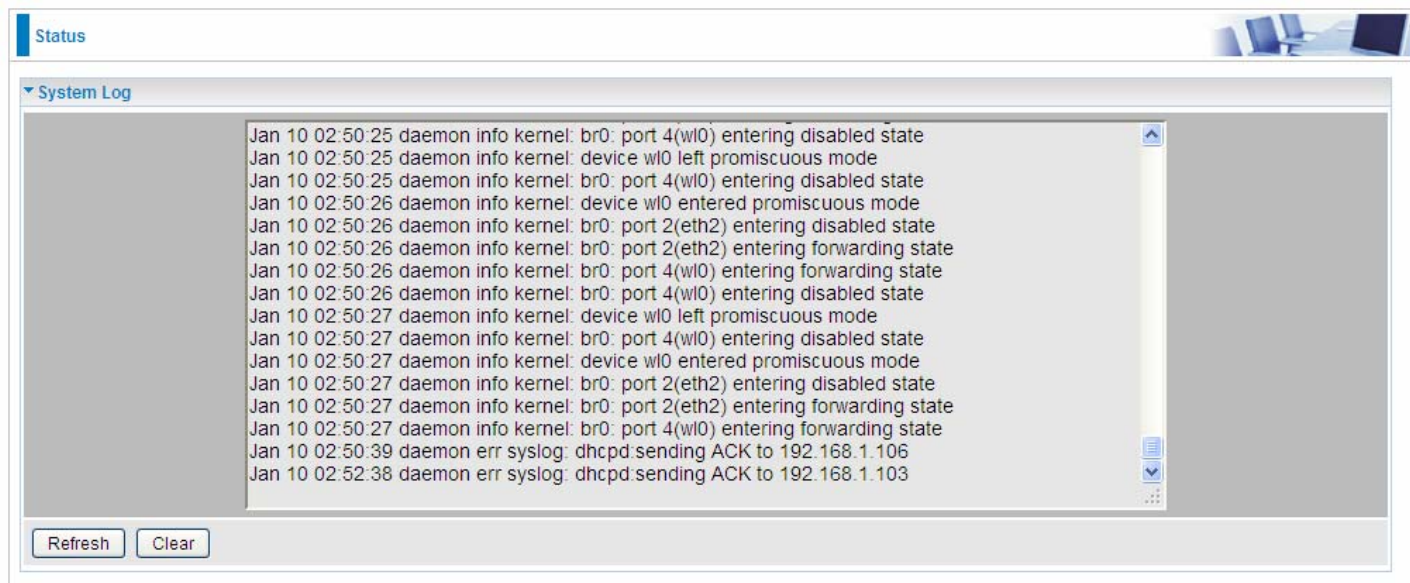
**Refresh:** Click this button to refresh the connection status.



# 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.



The screenshot shows a web interface for viewing system logs. At the top, there is a 'Status' tab. Below it, the 'System Log' section is expanded, displaying a list of log entries. The entries are timestamped and include details about network interface states and DHCP acknowledgments. At the bottom of the log list, there are two buttons: 'Refresh' and 'Clear'.

```
Jan 10 02:50:25 daemon info kernel: br0: port 4(wl0) entering disabled state
Jan 10 02:50:25 daemon info kernel: device wl0 left promiscuous mode
Jan 10 02:50:25 daemon info kernel: br0: port 4(wl0) entering disabled state
Jan 10 02:50:26 daemon info kernel: device wl0 entered promiscuous mode
Jan 10 02:50:26 daemon info kernel: br0: port 2(eth2) entering disabled state
Jan 10 02:50:26 daemon info kernel: br0: port 2(eth2) entering forwarding state
Jan 10 02:50:26 daemon info kernel: br0: port 4(wl0) entering forwarding state
Jan 10 02:50:26 daemon info kernel: br0: port 4(wl0) entering disabled state
Jan 10 02:50:27 daemon info kernel: device wl0 left promiscuous mode
Jan 10 02:50:27 daemon info kernel: br0: port 4(wl0) entering disabled state
Jan 10 02:50:27 daemon info kernel: device wl0 entered promiscuous mode
Jan 10 02:50:27 daemon info kernel: br0: port 2(eth2) entering disabled state
Jan 10 02:50:27 daemon info kernel: br0: port 2(eth2) entering forwarding state
Jan 10 02:50:27 daemon info kernel: br0: port 4(wl0) entering forwarding state
Jan 10 02:50:39 daemon err syslog: dhcpd: sending ACK to 192.168.1.106
Jan 10 02:52:38 daemon err syslog: dhcpd: sending ACK to 192.168.1.103
```

Refresh Clear

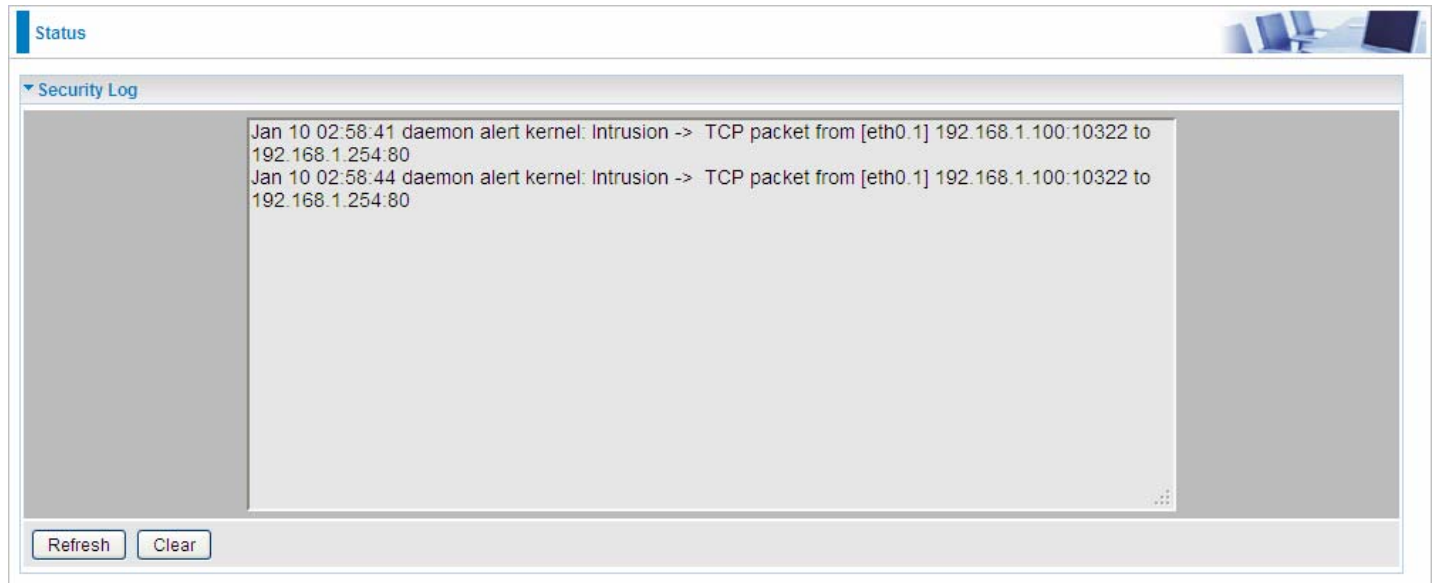
**Refresh:** Click to update the system log.

**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.



# 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)

Select WAN Interface

Main Port

DSL

(Current Main Port: 3G/LTE)

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)

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)

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

66



3. Wait while the device is configured.

Quick Start

WAN Interface ( WAN > Wireless )

Please wait while the device is configured.

4. WAN port configuration is successful.

Quick Start

WAN Interface ( WAN > Wireless )

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless 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 )

Parameters

Wireless

SSID

WPA Pre-Shared Key

☒ Enable

[Click here to display](#)

Continue

Quick Start

Wireless ( WAN > Wireless )

Please wait while the device is configured.

6. Success.

Quick Start

Process finished

Success.



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

Status	
▼ Device Information	
Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 31M 33S
Date/Time	Tue Jan 15 07:11:51 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4
▼ WAN	
Line Rate - Upstream (Kbps)	1315
Line Rate - Downstream (Kbps)	27431
Default Gateway	ppp0.1 (DSL)
Connection Time	00:01:57
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (DSL)



Ethernet mode

1. Select **Ethernet**, press **Continue** to go on to next step, or if you only want to configure Wireless, press **Jump to Wireless setting**.

Quick Start

▼ WAN Interface ( WAN > Wireless )

Select WAN Interface

Main Port

Ethernet (Current Main Port: 3G/LTE)

Continue

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 )

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

Continue

3. Wait while the device is configured.

Quick Start

▼ WAN Interface ( WAN > Wireless )

Please wait while the device is configured.

4. WAN port configuration is successful.

Quick Start

▼ WAN Interface ( WAN > Wireless )

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless



5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless 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 )

Parameters

Wireless

SSID

WPA Pre-Shared Key

☒ Enable

wlan-ap

[Click here to display](#)

Continue

Quick Start

Wireless ( WAN > Wireless )

Please wait while the device is configured.

6. Success.

Quick Start

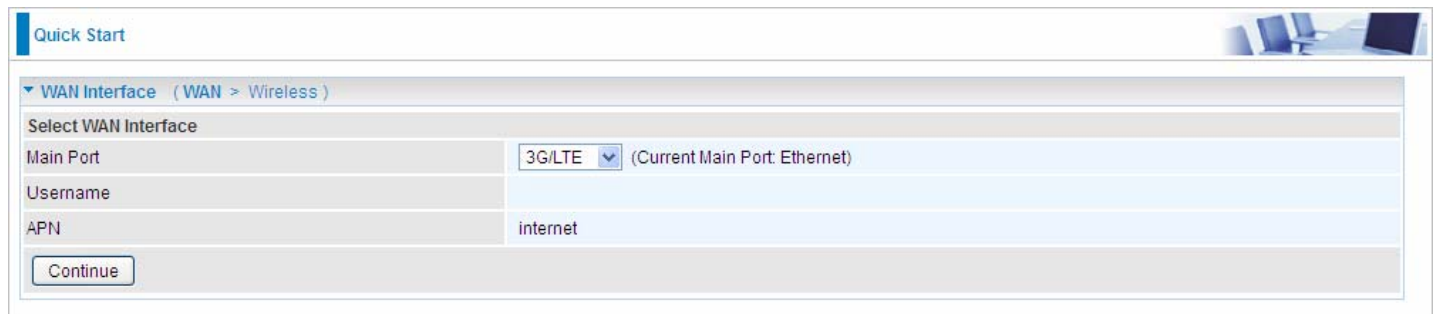
Process finished

Success.



## 3G/LTE

1. Select **3G/LTE**, press **Continue** to go on to next step, or if you only want to configure Wireless, press **Jump to Wireless setting**.



Quick Start

▼ WAN Interface (WAN > Wireless)

Select WAN Interface

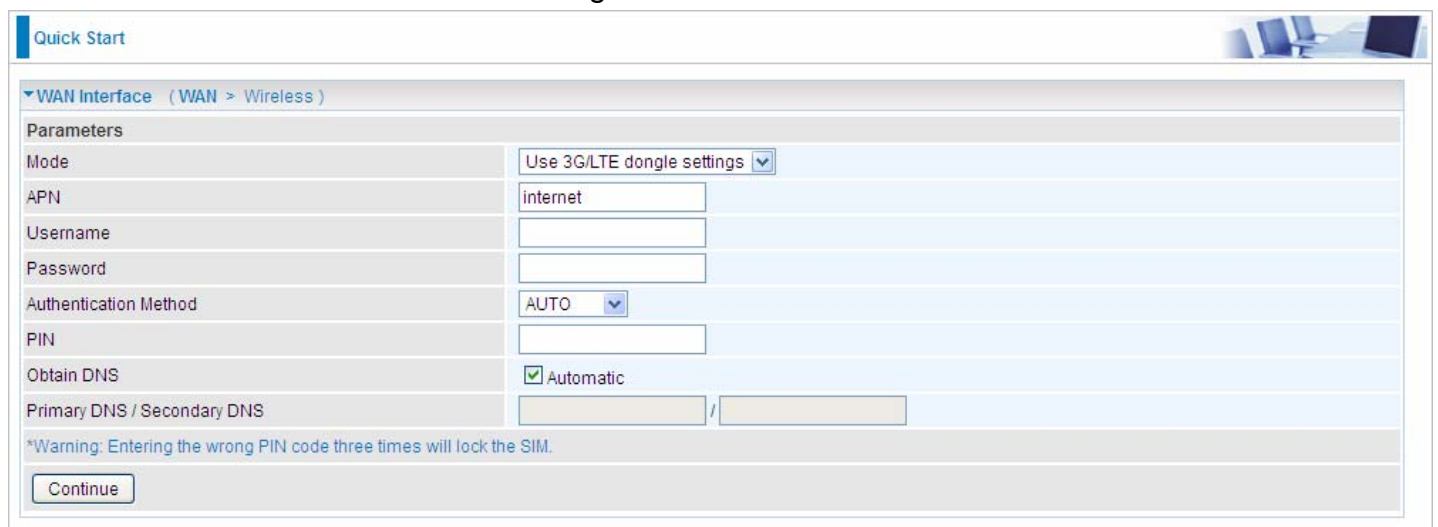
Main Port: 3G/LTE (Current Main Port: Ethernet)

Username:

APN: internet

Continue

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)

Parameters

Mode: Use 3G/LTE dongle settings

APN: internet

Username:

Password:

Authentication Method: AUTO

PIN:

Obtain DNS: ☒ Automatic

Primary DNS / Secondary DNS: /

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

Continue

3. Wait while the device is configured.

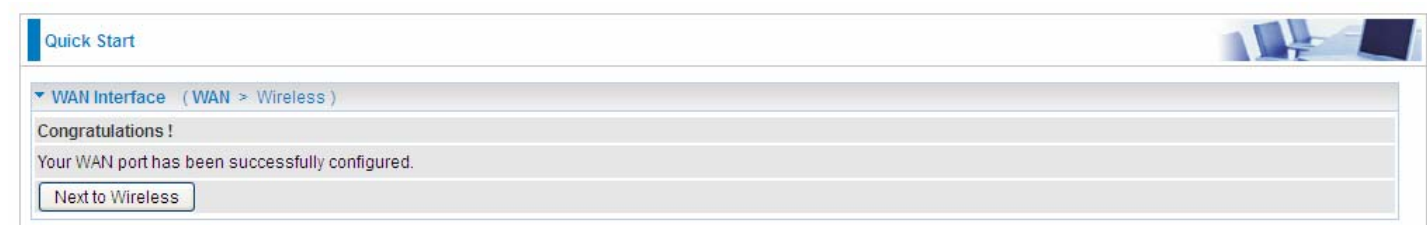


Quick Start

▼ WAN Interface (WAN > Wireless)

Please wait while the device is configured.

4. WAN port configuration is successful.



Quick Start

▼ WAN Interface (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless



5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless 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)

Parameters

Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap
WPA Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Continue



Quick Start

Wireless (WAN > Wireless)

Please wait while the device is configured.

## 6. Success.

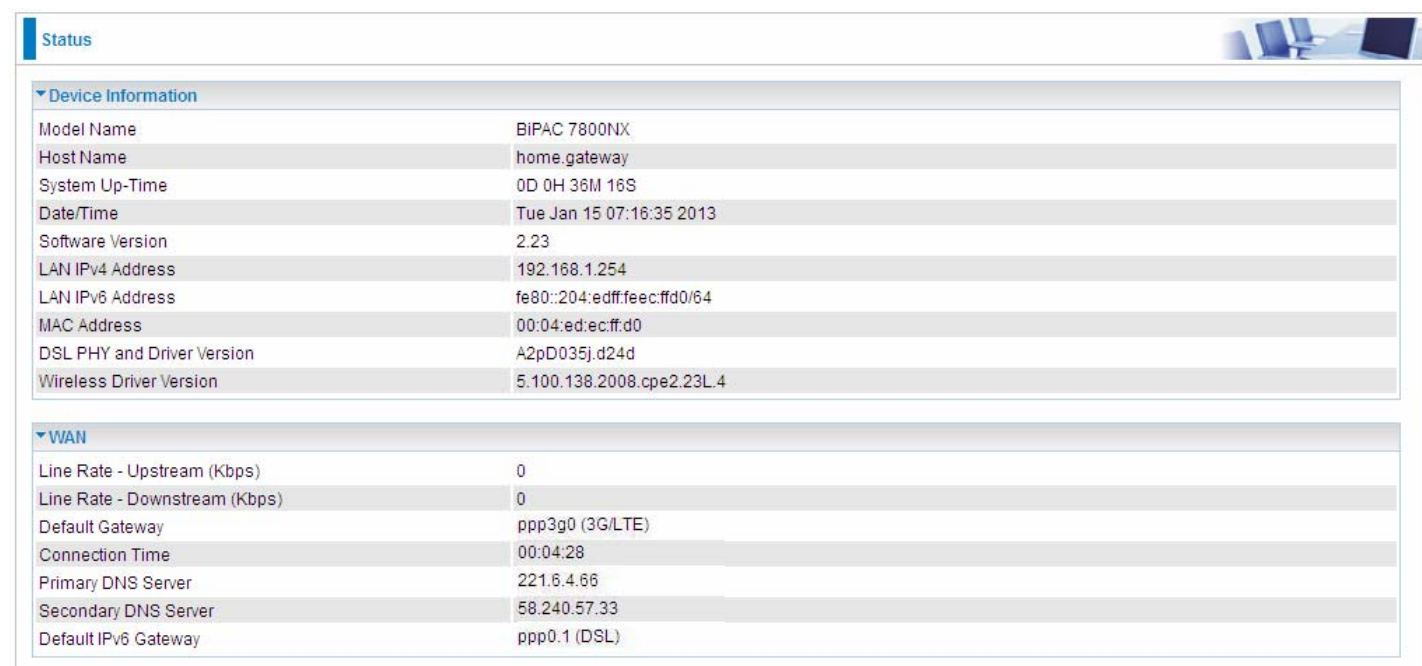


Quick Start

Process finished

Success.

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



Status

Device Information

Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 36M 16S
Date/Time	Tue Jan 15 07:16:35 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:feec:ffd0/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp3g0 (3G/LTE)
Connection Time	00:04:28
Primary DNS Server	221.6.4.66
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway	ppp0.1 (DSL)



# 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](#), [WAN](#), [System](#), [USB](#), [IP Tunnel](#), [Security](#), [Quality of Service](#), [NAT](#) and [Wake On LAN](#).

▸ Status
▸ Quick Start
▾ Configuration
▸ LAN
▸ Wireless
▸ WAN
▸ System
▸ USB
▸ IP Tunnel
▸ Security
▸ Quality of Service
▸ NAT
▸ Wake On LAN
▸ Advanced Setup

(7800NX)

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

The screenshot shows a web-based configuration interface for LAN settings. At the top, there's a 'Configuration' tab. Below it, a 'LAN' section is expanded. The 'Parameters' section includes fields for Group Name (Default), IP Address (192.168.1.254), Subnet Mask (255.255.255.0), IGMP Snooping (checked), IGMP Snooping Mode (Blocking Mode selected), LAN side firewall (unchecked), and DHCP Server (Enabled). Below these are fields for DHCP Server Start IP Address (192.168.1.100), End IP Address (192.168.1.199), Leased Time (24 hours), and Option 66 (unchecked). A 'Static IP Lease List' table has columns for Host Label, MAC Address, IP Address, Remove, and Edit, with an 'Add' button below it. An 'IP Alias' section has an 'IP Alias' field (unchecked), and fields for IP Address and Subnet Mask. At the bottom are 'Apply' and 'Cancel' buttons.

## 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:

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **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.

❶ Disable

DHCP Server	
DHCP Server	Disable

Disable the DHCP Server function.

❷ 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	<input type="checkbox"/> Enable

**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.

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
<input type="button" value="Add"/>				

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

Configuration

Static IP

Parameters

Host Label	<input type="text"/>
MAC Address	<input type="text"/>
IP Address	<input type="text"/>

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	<input type="checkbox"/>	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	<input type="checkbox"/> Enable
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
<div>Apply Cancel</div>	

- 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.

Configuration

IPv6 Autoconfig

Parameters

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

Apply Cancel

**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.

- ① Randomly Generated
- ① 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.

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **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.

- ① With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv6 Server	<input type="checkbox"/> Enable
Issue Router Advertisements	<input checked="" type="checkbox"/> 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.

- ② With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start interface ID	<input type="text" value="0:0:0:2"/>
End interface ID	<input type="text" value="0:0:0:254"/>
Leased Time (hour)	<input type="text" value="24"/>
Issue Router Advertisements	<input checked="" type="checkbox"/> 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.

① With only DHCPv6 enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input type="radio"/> Stateless <input checked="" type="radio"/> Stateful
Start interface ID	<input type="text" value="0:0:0:2"/>
End interface ID	<input type="text" value="0:0:0:254"/>
Leased Time (hour)	<input type="text" value="24"/>
Issue Router Advertisements	<input type="checkbox"/> Enable

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

① With both DHCPv6 and Issue Router Advertisement Enabled

DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input type="radio"/> Stateless <input checked="" type="radio"/> Stateful
Start interface ID	<input type="text" value="0:0:0:2"/>
End interface ID	<input type="text" value="0:0:0:254"/>
Leased Time (hour)	<input type="text" value="24"/>
Issue Router Advertisements	<input checked="" type="checkbox"/> 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.)

Configuration

Interface Grouping

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	

Add

Remove



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\_0\_35/ppp0.1

Grouped LAN Interfaces

Available LAN Interfaces

P4/EWAN  
P3  
P2  
P1  
wlan-ap

Automatically Add Clients With the following DHCP Vendor IDs

Apply

Cancel

**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.

82



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

Configuration

▼Interface Grouping

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	
test	<input type="checkbox"/>	ppp0.1	P2	

Add

Remove

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

Configuration

▼Interface Grouping

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	
test	<input checked="" type="checkbox"/>	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.



# Wireless (7800NX(L) only)

This section provides you ways to configure wireless access. The BiPAC 7800NX(L) supports wireless on the 2.4GHz for users. This part has sub-items as [Basic](#), [Security](#), [MAC Filter](#), [Wireless Bridge](#), [Advanced](#) and [Station Info](#) here.

▶ Status
▪ Quick Start
▼ Configuration
▶ LAN
▼ Wireless
▪ Basic
▪ Security
▪ MAC Filter
▪ Wireless Bridge
▪ Advanced
▪ Station Info
▶ WAN
▶ System
▶ USB
▶ IP Tunnel
▶ Security
▪ Quality of Service
▶ NAT
▪ Wake On LAN
▶ Advanced Setup

(7800NX)



## 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	<input checked="" type="checkbox"/> Enable
Hide SSID	<input type="checkbox"/> Enable
Clients Isolation	<input type="checkbox"/> Enable
Disable WMM Advertise	<input type="checkbox"/> Enable
Wireless Multicast Forwarding (WMMF)	<input type="checkbox"/> Enable
SSID	wlan-ap
BSSID	00:04:ED:EC:FF:D0
Country	UNITED STATES
Max Clients	16 [1-16]

**Wireless - Guest/Virtual Access Points**

SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMMF	Max Clients	BSSID	Enable
wl0_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A	<input type="checkbox"/>
wl0_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A	<input type="checkbox"/>
wl0_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A	<input type="checkbox"/>

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 (WMMF):** 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" to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the 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.

Configuration

▼ 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

Network Authentication

Open

WEP Encryption

Disabled

Apply

Cancel

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

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.



## ① 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.

## ① 802.1x

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.



## ① WPA

Network Authentication	WPA	▼
WPA Group Rekey Interval	0	[0-2147483647]
RADIUS Server IP Address	0.0.0.0	
RADIUS Port	1812	
RADIUS Key		
WPA/WAPI Encryption	TKIP+AES	▼
WEP Encryption	Disabled	▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

**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.

## ① WPA-PSK / WPA2-PSK

Network Authentication	WPA-PSK	▼
WPA/WAPI passphrase	●●●●●●●●	<a href="#">Click here to display</a>
WPA Group Rekey Interval	0	[0-2147483647]
WPA/WAPI Encryption	TKIP+AES	▼
WEP Encryption	Disabled	▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

**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.



## ① WPA2

Network Authentication	WPA2
WPA2 Preauthentication	Enable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	0 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	AES
WEP Encryption	Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**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.

## ① Mixed WPA2/WPA

Network Authentication	Mixed WPA2/WPA
WPA2 Preauthentication	Enable
Network Re-auth Interval	36000 [0-2147483647]
WPA Group Rekey Interval	0 [0-2147483647]
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WPA/WAPI Encryption	TKIP+AES
WEP Encryption	Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**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.

① **Mixed WPA2/WPA-PSk**

Network Authentication	Mixed WPA2/WPA -PSK
WPA/WAPI passphrase	..... <a href="#">Click here to display</a>
WPA Group Rekey Interval	0 [0-2147483647]
WPA/WAPI Encryption	TKIP+AES
WEP Encryption	Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**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.



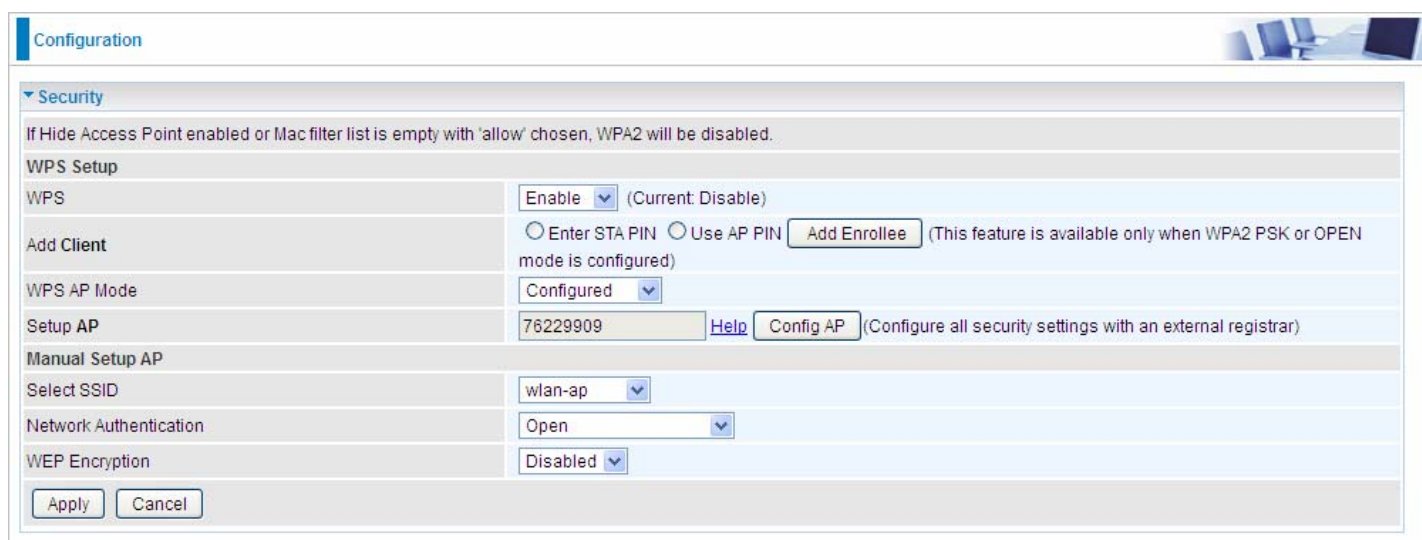
## WPS Setup

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.



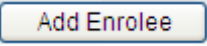
The screenshot shows a web-based configuration interface for WPS Setup. The page is titled "Configuration" and has a "Security" tab selected. A warning message states: "If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled." The "WPS Setup" section includes a "WPS" dropdown menu set to "Enable" (Current: Disable). Below it, there are radio buttons for "Enter STA PIN" and "Use AP PIN", with an "Add Enrollee" button. A note indicates that this feature is only available when WPA2 PSK or OPEN mode is configured. The "WPS AP Mode" dropdown is set to "Configured". The "Setup AP" field contains the PIN "76229909", with "Help" and "Config AP" buttons. A note explains that "Config AP" is used to configure all security settings with an external registrar. The "Manual Setup AP" section includes a "Select SSID" dropdown set to "wlan-ap", a "Network Authentication" dropdown set to "Open", and a "WEP Encryption" dropdown set to "Disabled". At the bottom, there are "Apply" and "Cancel" buttons.

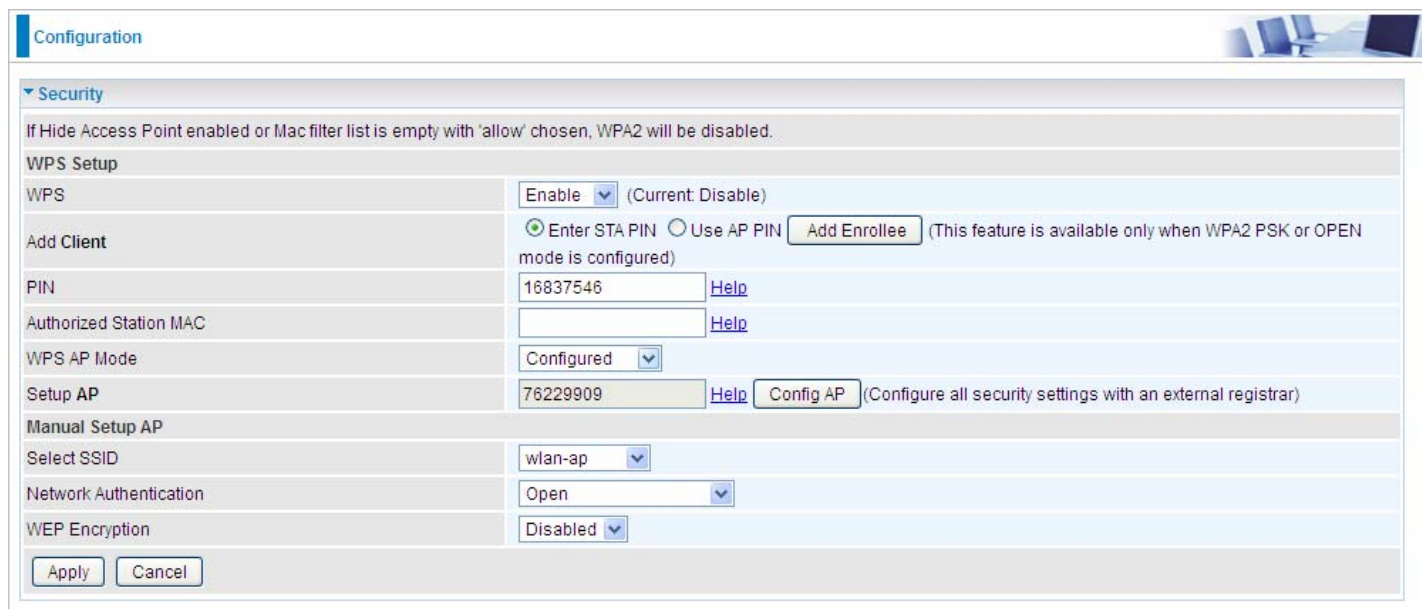
Configuration	
▼ Security	
If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.	
WPS Setup	
WPS	Enable (Current: Disable)
Add Client	<input type="radio"/> Enter STA PIN <input type="radio"/> Use AP PIN <input type="button" value="Add Enrollee"/> (This feature is available only when WPA2 PSK or OPEN mode is configured)
WPS AP Mode	Configured
Setup AP	76229909 <input type="button" value="Help"/> <input type="button" value="Config AP"/> (Configure all security settings with an external registrar)
Manual Setup AP	
Select SSID	wlan-ap
Network Authentication	Open
WEP Encryption	Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



## 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 .




Configuration

Security

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

WPS Setup

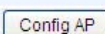
WPS  (Current: Disable)

Add Client ☒ Enter STA PIN ☐ Use AP PIN  (This feature is available only when WPA2 PSK or OPEN mode is configured)

PIN  [Help](#)

Authorized Station MAC  [Help](#)

WPS AP Mode



Setup AP  [Help](#)  (Configure all security settings with an external registrar)

Manual Setup AP

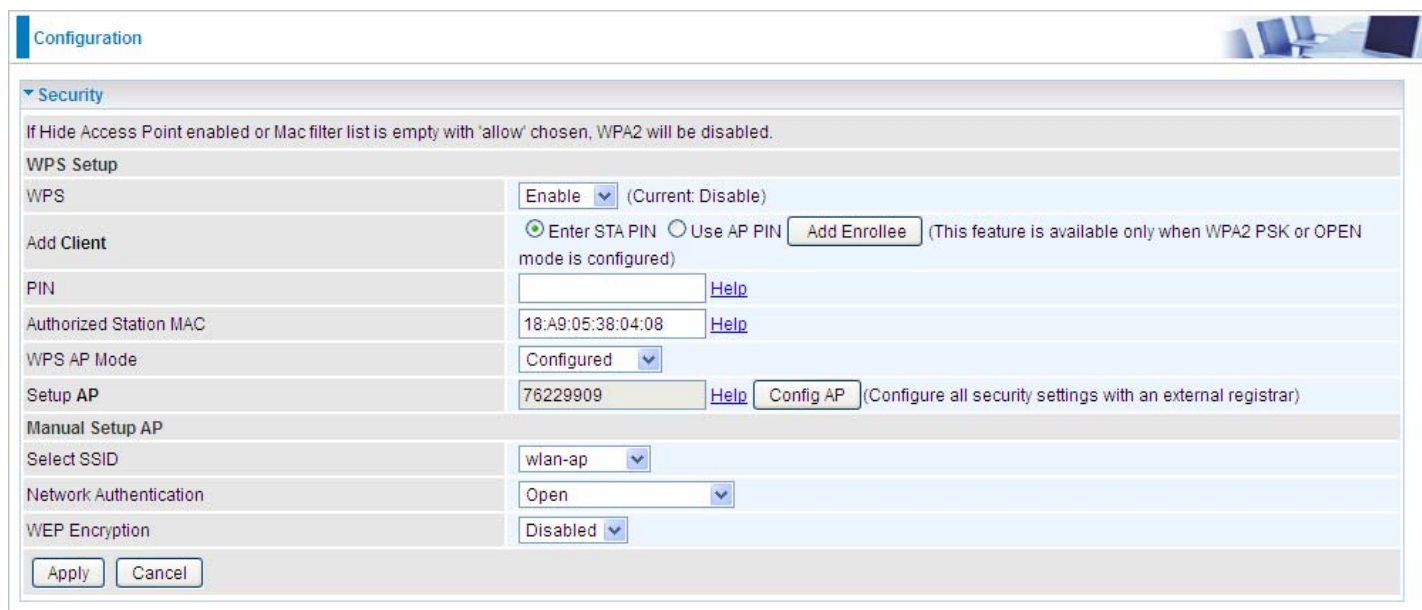
Select SSID

Network Authentication

WEP Encryption

(Station PIN)



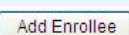
Configuration

Security

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

WPS Setup

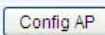
WPS  (Current: Disable)

Add Client ☒ Enter STA PIN ☐ Use AP PIN  (This feature is available only when WPA2 PSK or OPEN mode is configured)

PIN  [Help](#)

Authorized Station MAC  [Help](#)

WPS AP Mode



Setup AP  [Help](#)  (Configure all security settings with an external registrar)

Manual Setup AP

Select SSID

Network Authentication

WEP Encryption

(Station MAC)

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



- 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) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

The screenshot displays the WPS utility interface with the following components:

- Top Navigation Bar:** Profile, Network, Advanced, Statistics, WMM, WPS (highlighted), Radio On/Off, About.
- WPS AP List:**

ID	AP Name	MAC Address	Count
ID : 0x0000	wlan-ap	00-04-ED-EC:FF:D0	1
ID :	11	00-04-ED-00-00-01	1
- WPS Profile List:** (Empty list)
- Buttons:** PIN, PBC, WPS Associate IE (checked), WPS Probe IE (checked), Progress >> 0%, WPS status is disconnected.
- Right Panel:** Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Status & Extra Info:**
  - Status >> Disconnected
  - Extra Info >>
  - Channel >>
  - Authentication >>
  - Encryption >>
  - Network Type >>
  - IP Address >>
  - Sub Mask >>
  - Default Gateway >>
- Link Quality & Signal Strength:**
  - Link Quality >> 0%
  - Signal Strength 1 >> 0%
  - Signal Strength 2 >> 0%
  - Noise Strength >> 0%
- Transmit & Receive Performance:**
  - Transmit: Link Speed >> Max, Throughput >> 0.000 Kbps
  - Receive: Link Speed >> Max, Throughput >> 0.000 Kbps
- HT (High Throughput) Section:**
  - BW >> n/a, SNR0 >> n/a, GI >> n/a, MCS >> 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.

The screenshot displays a network configuration interface with a top navigation bar containing icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The WPS tab is selected.

**WPS AP List**

ID	MAC	Count
11	00-04-ED-01-00-01	1
wlan-ap	00:04:ED:EC:FF:D0	1

**WPS Profile List**

wlan-ap

**WPS Configuration**

- ☒ WPS Associate IE
- ☒ WPS Probe IE

Progress >> 100%

PIN - Get WPS profile successfully.

**WPS Status and Performance**

**Status >> wlan-ap <--> 00:04:ED:EC:FF:D0**

**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

**HT**

**Transmit**

Link Speed >> 270.0 Mbps

Throughput >> 5.600 Kbps

**Receive**

Link Speed >> 54.0 Mbps

Throughput >> 81.608 Kbps

**Link Quality >> 100%**

**Signal Strength 1 >> 64%**

**Signal Strength 2 >> 34%**

**Noise Strength >> 26%**

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**” and Click “**Config AP**” button.

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)

WPS AP Mode

Unconfigured ▼

Setup AP

76229909 [Help](#) Config AP (Configure all security settings with an external registrar)

Manual Setup AP

Select SSID

wlan-ap ▼

Network Authentication

Open ▼

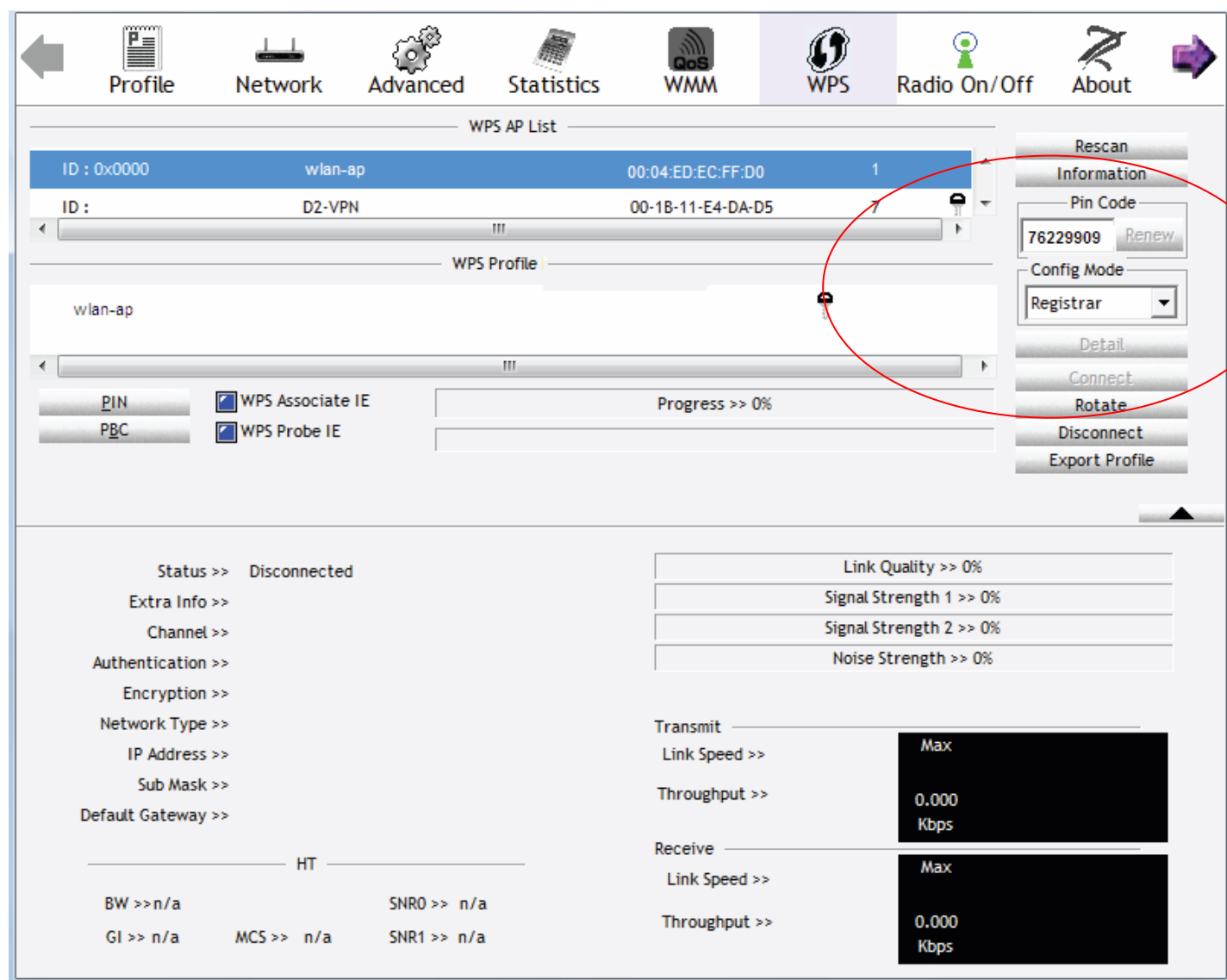
WEP Encryption

Disabled ▼

Apply Cancel



2. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as **Registrar**. Enter the **PIN** number (76229909 (device) for example) in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.





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

The screenshot displays the WinBox WPS configuration page. At the top, navigation tabs include Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The WPS tab is active, showing the WPS AP List and WPS Profile List. The WPS AP List shows a single entry with ID 11, Name wlan-ap, and MAC 00:04:ED:EC:FF:D0. The WPS Profile List shows a single profile named wlan-ap. Below the profile list, there are checkboxes for WPS Associate IE and WPS Probe IE, both of which are checked. A progress bar indicates 100% completion, and a message states 'PIN - Get WPS profile successfully.' To the right of the profile list, there are buttons for Rescan, Information, Pin Code (76229909), Renew, Config Mode (Registrar), Detail, Connect, Rotate, Disconnect, Export Profile, and Delete. Below the profile list, there is a section for the profile's status and configuration. The status section shows 'Status >> wlan-ap <-> 00:04:ED:EC:FF:D0'. The extra info section shows 'Link is Up [TxPower:100%]'. The channel section shows 'Channel >> 1 <-> 2412 MHz; central channel : 3'. The authentication section shows 'Authentication >> Open'. The encryption section shows 'Encryption >> NONE'. The network type section shows 'Network Type >> Infrastructure'. The IP address section shows 'IP Address >> 192.168.1.100'. The sub mask section shows 'Sub Mask >> 255.255.255.0'. The default gateway section shows 'Default Gateway >> 192.168.1.254'. The HT section shows 'HT BW >> 40', 'GI >> long', 'MCS >> 15', 'SNR0 >> 19', and 'SNR1 >> n/a'. On the right side of the status section, there are two graphs showing Link Quality and Signal Strength. The Link Quality graph shows a value of 100%. The Signal Strength graph shows two values: 64% and 34%. The Noise Strength graph shows a value of 26%. Below the graphs, there are two sections for Transmit and Receive link speed and throughput. The Transmit section shows 'Link Speed >> 270.0 Mbps' and 'Throughput >> 5.600 Kbps'. The Receive section shows 'Link Speed >> 54.0 Mbps' and 'Throughput >> 81.608 Kbps'.

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



## MAC Filter



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

### MAC Restrict Mode:

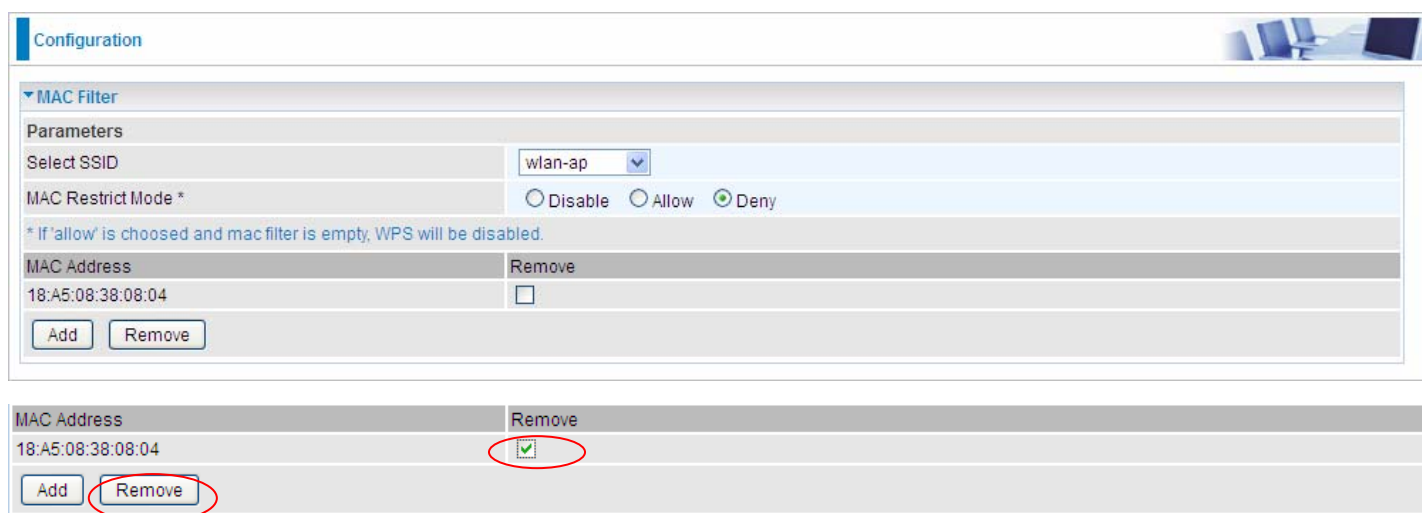
- ① **Disable:** disable the MAC Filter function.
- ① **Allow:** allow the hosts with the following listed MACs to access the wireless network.
- ① **Deny:** deny the hosts with the following listed MACs to access the wireless network.

Click **Add** to add the MACs.



**MAC Address:** enter 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.



If you don't need a rule, check the remove checkbox and press **Remove** to delete it.



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).

Configuration

Wireless Bridge

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

Apply

Refresh

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

- ① **Access Point:** The gateway communicates with both clients and bridges.
- ① **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:

- ① **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

Apply

Refresh

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

- ① **Enabled (Scan):** To enable wireless bridge restriction. Only those scanned by the gateway can communicate.

Bridge Restrict

Enabled(Scan)

	SSID	BSSID
<input type="checkbox"/>	CMB	C4:CA:D9:7C:11:51
<input type="checkbox"/>	ChinaNet	C4:CA:D9:7C:11:50
<input type="checkbox"/>	wlan-ap4	00:04:ED:D7:33:CB



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

- ① **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.

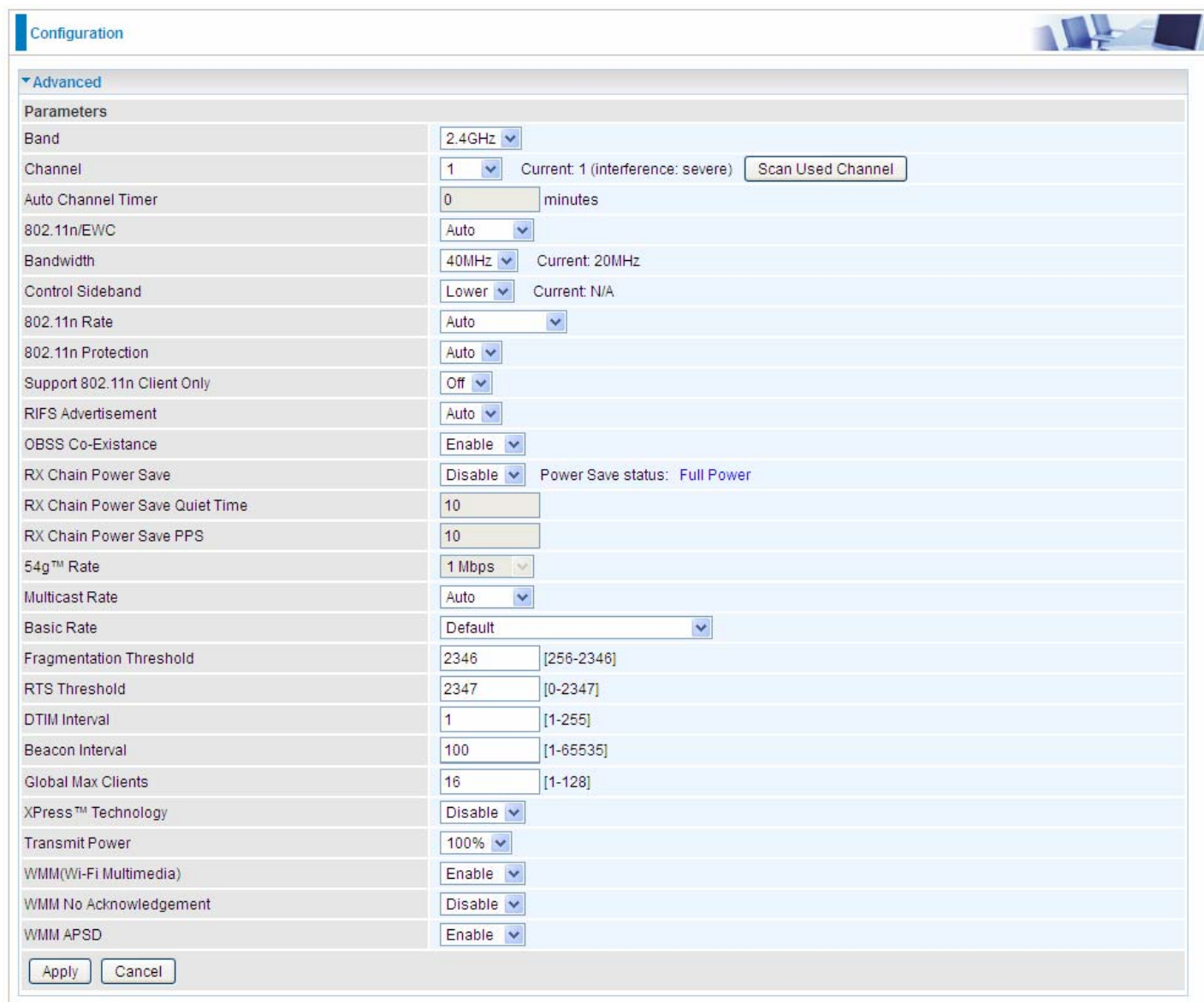
Bridge Restrict	Disable ▼
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

Click **Apply** to apply your settings.



## Advanced

Here users can set some advanced parameters about wireless.



The screenshot shows a web-based configuration interface for wireless settings. The title bar at the top left says 'Configuration'. The main content area is titled 'Advanced' and contains a list of parameters with their current values and controls. The parameters are: Band (2.4GHz), Channel (1), Auto Channel Timer (0 minutes), 802.11n/EWC (Auto), Bandwidth (40MHz), Control Sideband (Lower), 802.11n Rate (Auto), 802.11n Protection (Auto), Support 802.11n Client Only (Off), RIFS Advertisement (Auto), OBSS Co-Existence (Enable), RX Chain Power Save (Disable), 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), RTS Threshold (2347), DTIM Interval (1), Beacon Interval (100), Global Max Clients (16), XPress™ Technology (Disable), Transmit Power (100%), WMM(Wi-Fi Multimedia) (Enable), WMM No Acknowledgement (Disable), and WMM APSD (Enable). There are 'Apply' and 'Cancel' buttons at the bottom left. A 'Scan Used Channel' button is next to the Channel parameter. The current status for Power Save is 'Full Power'.

Parameter	Value	Current
Band	2.4GHz	
Channel	1	Current: 1 (interference: severe)
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-Existence	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. 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.



Configuration				
▼ Station Info				
Associated Stations				
MAC Address	Associated	Authorized	SSID	Interface
00:18:DE:CE:8F:5B	Yes		wlan-ap	wl0
<input type="button" value="Refresh"/>				

**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.

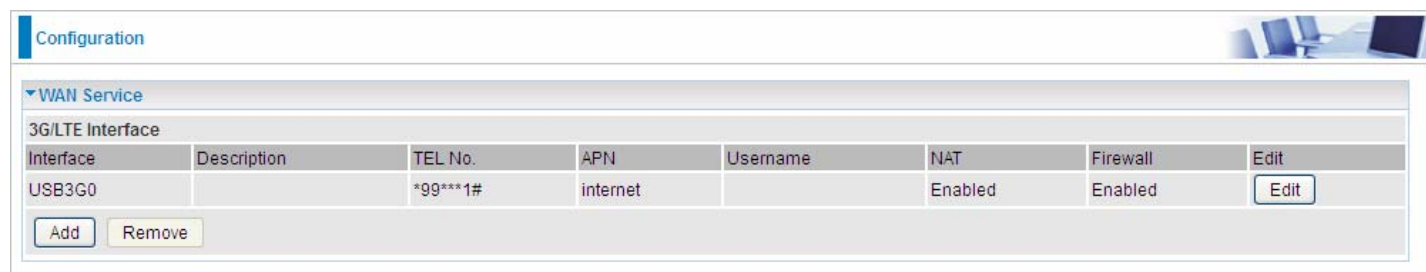


# WAN-Wide Area Network

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

## WAN Service

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



The screenshot shows the 'Configuration' page with the 'WAN Service' tab selected. It displays a table of existing WAN connections. The table has columns for Interface, Description, TEL No., APN, Username, NAT, Firewall, and Edit. There is one entry for 'USB3G0' with a description, TEL No. '\*99\*\*\*1#', APN 'internet', and NAT and Firewall both set to 'Enabled'. Below the table are 'Add' and 'Remove' buttons.

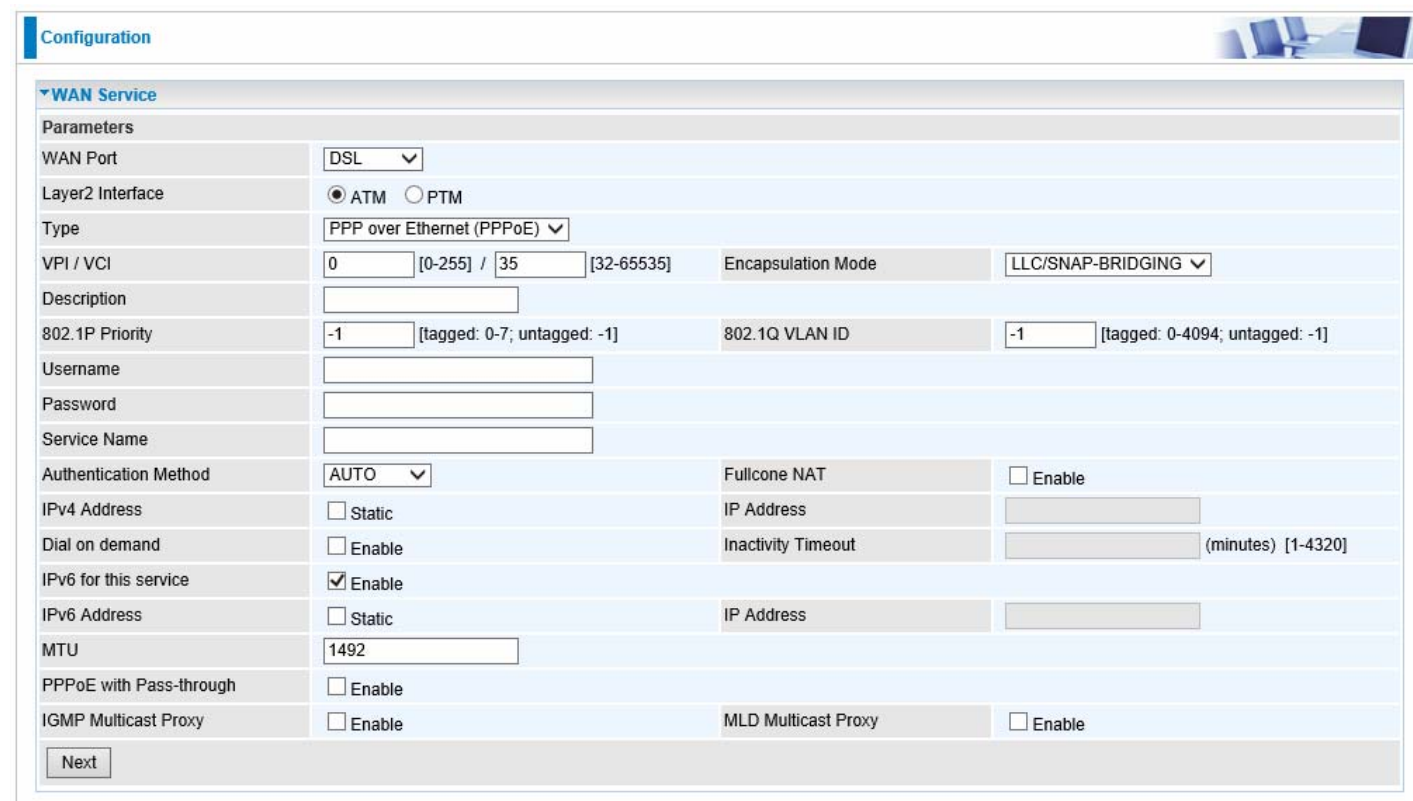
Interface	Description	TEL No.	APN	Username	NAT	Firewall	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	<a href="#">Edit</a>

[Add](#) [Remove](#)

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

### ① 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.



The screenshot shows the 'Configuration' page with the 'WAN Service' tab selected. It displays the configuration form for a new WAN connection. The form is divided into sections: Parameters, Layer2 Interface, and Authentication Method. The 'Parameters' section includes fields for WAN Port (DSL), Layer2 Interface (ATM selected), Type (PPP over Ethernet (PPPoE)), VPI / VCI (0 / 35), Encapsulation Mode (LLC/SNAP-BRIDGING), Description, 802.1P Priority (-1), 802.1Q VLAN ID (-1), Username, Password, Service Name, Authentication Method (AUTO), Fullcone NAT (unchecked), IPv4 Address (Static), IP Address, Dial on demand (unchecked), Inactivity Timeout (minutes) [1-4320], IPv6 for this service (checked), IPv6 Address (Static), IP Address, MTU (1492), PPPoE with Pass-through (unchecked), IGMP Multicast Proxy (unchecked), and MLD Multicast Proxy (unchecked). A 'Next' button is at the bottom.

**Parameters**

WAN Port:

Layer2 Interface: ☒ ATM ☐ PTM

Type:

VPI / VCI:  [0-255] /  [32-65535] Encapsulation Mode:

Description:

802.1P Priority:  [tagged: 0-7; untagged: -1] 802.1Q VLAN ID:  [tagged: 0-4094; untagged: -1]

Username:

Password:

Service Name:

Authentication Method:  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:

PPPoE with Pass-through: ☐ Enable

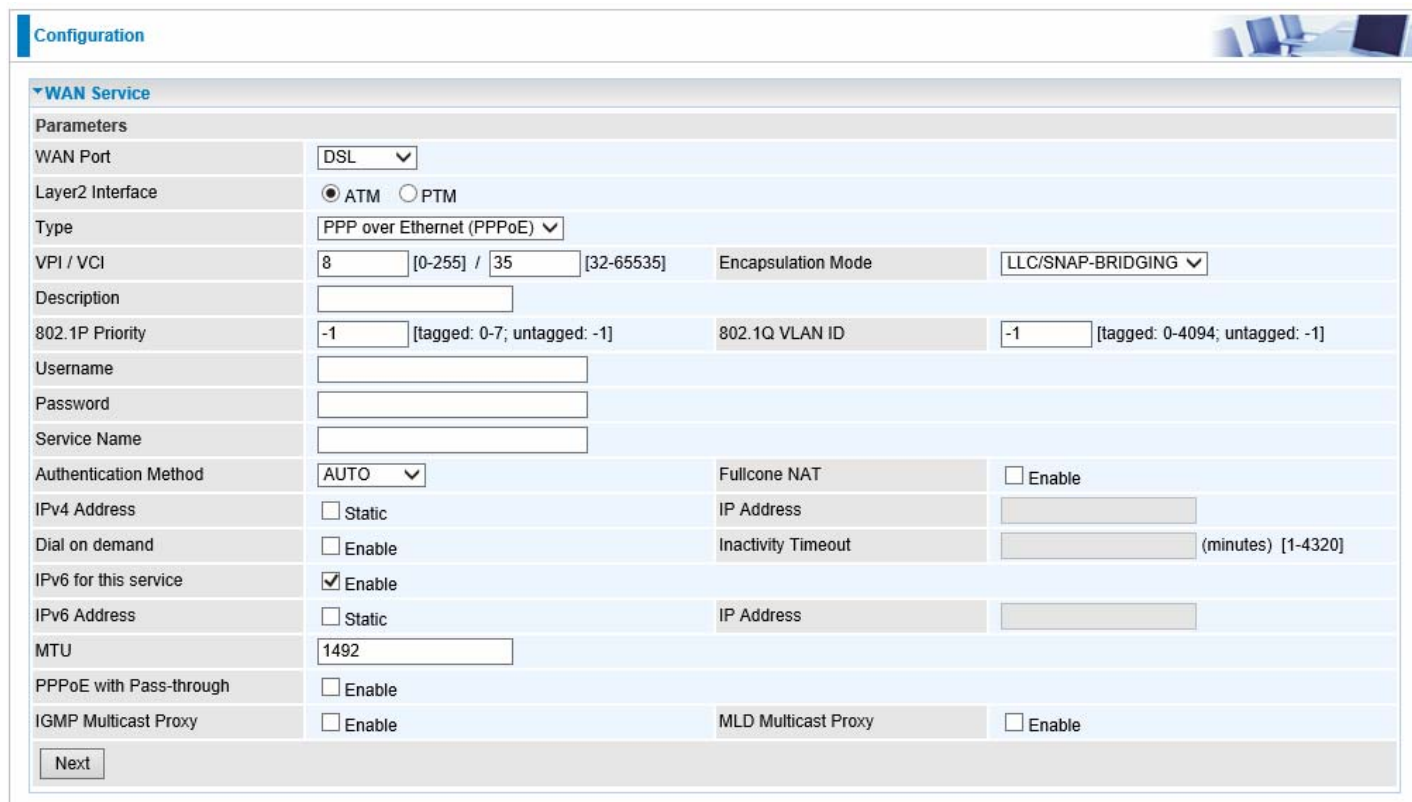
IGMP Multicast Proxy: ☐ Enable MLD Multicast Proxy: ☐ Enable

[Next](#)

**Layer2 Interface:** 2 transfer mode, ATM or PTM.



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



The image shows a configuration window titled "Configuration" with a sub-tab "WAN Service". The window contains a form with various fields for configuring a WAN service. The fields are organized into sections: Parameters, WAN Port, Layer2 Interface, Type, VPI / VCI, Encapsulation Mode, Description, 802.1P Priority, 802.1Q VLAN ID, Username, Password, Service Name, Authentication Method, Fullcone NAT, IPv4 Address, IP Address, Dial on demand, Inactivity Timeout, IPv6 for this service, IPv6 Address, IP Address, MTU, PPPoE with Pass-through, IGMP Multicast Proxy, MLD Multicast Proxy, and a Next button.

WAN Service Configuration			
<b>Parameters</b>			
WAN Port	DSL		
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM		
Type	PPP over Ethernet (PPPoE)		
VPI / VCI	8 [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	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1492		
PPPoE with Pass-through	<input type="checkbox"/> Enable		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> Enable
<input type="button" value="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.

**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 (**I**nternet **G**roup **M**anagement **P**rotocol) 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 (**M**ulticast **L**istener **D**iscovery **P**rotocol) 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

ppp0.1

Available Routed WAN Interfaces

Selected WAN Interface As The System Default IPv6 Gateway

pppoe\_0\_8\_35/ppp0.1

DNS

DNS Server Interface

Selected DNS Server Interfaces

ppp0.1

Available WAN Interfaces

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

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

Either IPv4 or IPv6, you can choose static setting or select from available interfaces.

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 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	Icmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8 / 35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	Edit

3G/LTE Interface

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

Add


Remove



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 (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
ppp0.1	pppoe_0_8_35	PPPoE	<a href="#">Disconnect</a>	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64
USB3G0			3G/LTE Card not found			

Status





▼ Device Information

Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 31M 33S
Date/Time	Tue Jan 15 07:11:51 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edff:fe02:1/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

▼ WAN

Line Rate - Upstream (Kbps)	1315
Line Rate - Downstream (Kbps)	27431
Default Gateway	ppp0.1 (DSL)
Connection Time	00:01:57
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (DSL)



**WAN Service**

Parameters

WAN Port	DSL		
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM		
Type	PPPoA		
VPI / VCI	0	[0-255] / 35	[32-65535]
Encapsulation Mode	VC/MUX		
Description			
Username			
Password			
Authentication Method	AUTO	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1500		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> 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.

**Username:** Enter the account obtained from the ISP.

**Password:** Enter the password obtained from the ISP.

**Service Name:** The item is for identification purposes, user can define this.

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

**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 (**I**nternet **G**roup **M**anagement **P**rotocol) 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 (**M**ulticast **L**istener **D**iscovery **P**rotocol) 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

WAN Service

Parameters

WAN Port	DSL		
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> 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	<input checked="" type="checkbox"/> Enable		
Option 60 Vendor ID			
Option 61 IAID		8 hexadecimal digits	
Option 61 DUID		hexadecimal digits	
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
Obtain an IPv6 address automatically	<input checked="" type="checkbox"/> Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
Firewall	<input checked="" type="checkbox"/> Enable	IGMP Multicast	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> 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.

**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 IAID:** Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

**Option 61 DUID:** Enter the associated information provided by your ISP. You should input hexadecimal number(s).



**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 (**I**nternet **G**roup **M**embership 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 (**M**ulticast **L**istener **D**iscovery 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


WAN Service

Parameters

WAN Port	DSL		
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM		
Type	IPoA		
VPI / VCI	0	[0-255] / 35	[32-65535]
Encapsulation Mode	LLC/SNAP-ROUTING		
Description			
WAN IP Address			
WAN Subnet Mask			
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
Firewall	<input checked="" type="checkbox"/> Enable	IGMP Multicast	<input type="checkbox"/> 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.

**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.



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]

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.



## ① Ethernet

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

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	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1492		
PPPoE with Pass-through	<input type="checkbox"/> Enable		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> Enable

Next

## ● 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	Fullcone NAT	<input type="checkbox"/> Enable
IPv4 Address	<input type="checkbox"/> Static	IP Address	
Dial on demand	<input type="checkbox"/> Enable	Inactivity Timeout	(minutes) [1-4320]
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
IPv6 Address	<input type="checkbox"/> Static	IP Address	
MTU	1492		
PPPoE with Pass-through	<input type="checkbox"/> Enable		
IGMP Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Proxy	<input type="checkbox"/> 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.

**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.

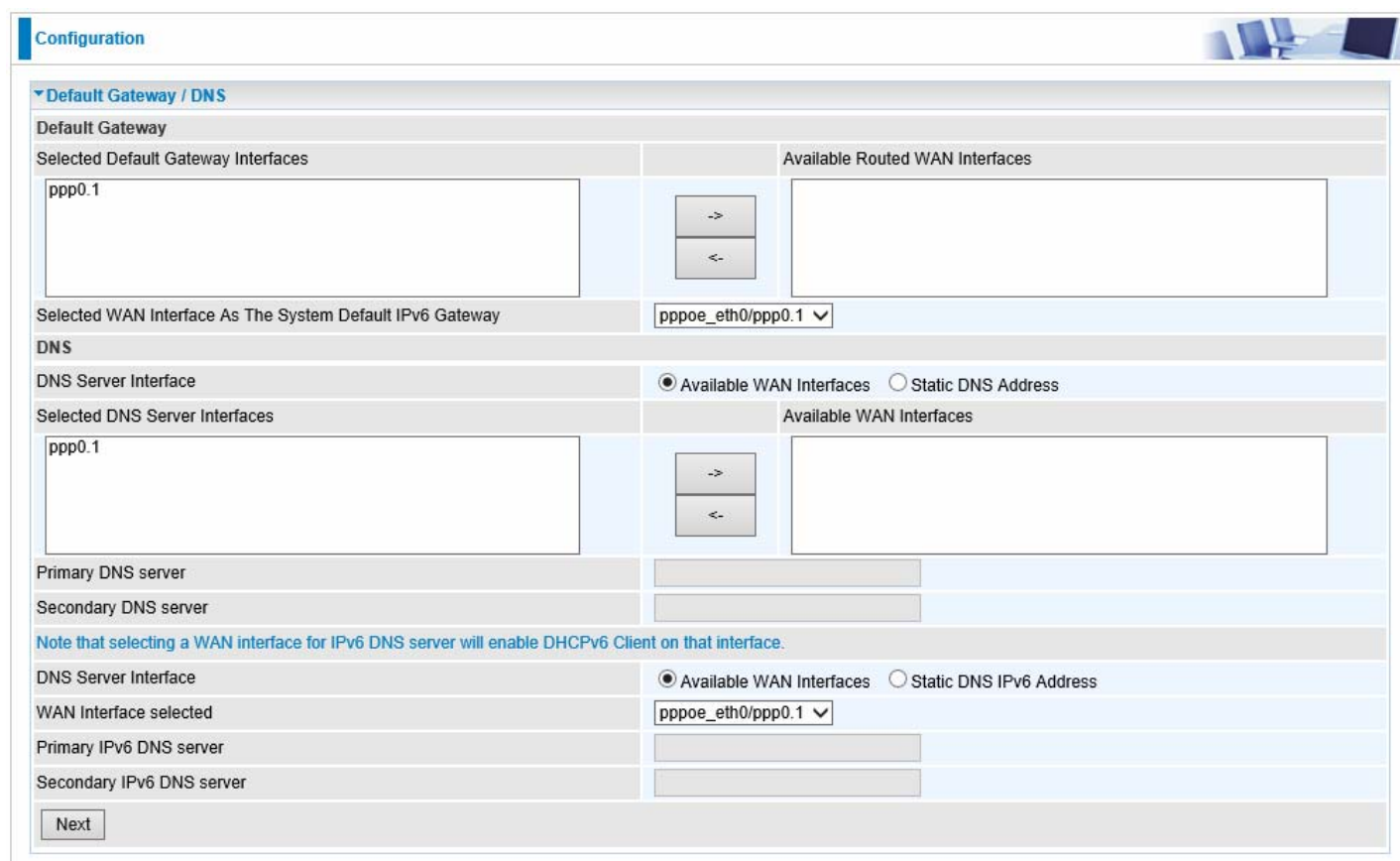
**PPPoE with Pass-through:** Enable or disable PPPoE pass-through. If it is enabled, PCs behind the router can dial itself.

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) 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 (**M**ulticast **L**istener **D**iscovery **P**rotocol) 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.



The screenshot shows a web-based configuration interface. At the top, there's a 'Configuration' header. Below it, a section titled 'Default Gateway / DNS' is expanded. The 'Default Gateway' section has two columns: 'Selected Default Gateway Interfaces' (containing 'ppp0.1') and 'Available Routed WAN Interfaces' (empty). Between them are two buttons: '->' and '<-. Below this, a dropdown menu for 'Selected WAN Interface As The System Default IPv6 Gateway' is set to 'pppoe\_eth0/ppp0.1'. The 'DNS' section follows, with a radio button selection for 'Available WAN Interfaces' (selected) and 'Static DNS Address'. It has two columns: 'Selected DNS Server Interfaces' (containing 'ppp0.1') and 'Available WAN Interfaces' (empty), with '->' and '<- buttons between them. Below these are input fields for 'Primary DNS server' and 'Secondary DNS server'. A blue note states: 'Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.' This is followed by another radio button selection for 'Available WAN Interfaces' and 'Static DNS IPv6 Address'. Below this is a dropdown for 'WAN Interface selected' set to 'pppoe\_eth0/ppp0.1', and input fields for 'Primary IPv6 DNS server' and 'Secondary IPv6 DNS server'. At the bottom left is a 'Next' button.

## Default Gateway

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

## DNS

Either IPv4 or IPv6, you can choose a static setting or select from available interfaces.

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 menu to be as an IPv6 DNS.

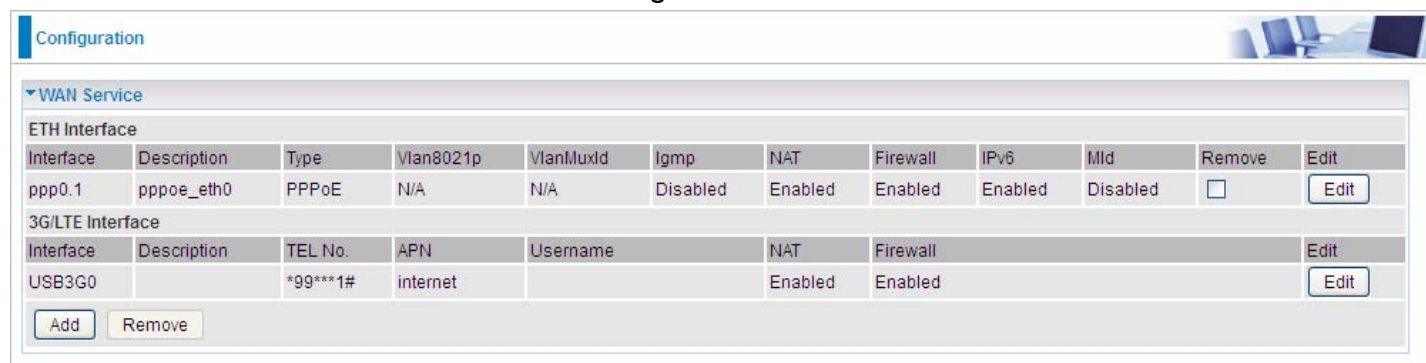
### Static DNS IPv6 Address

**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.



The screenshot shows the 'Configuration' page with a 'WAN Service' section. It contains two tables: 'ETH Interface' and '3G/LTE Interface'. The 'ETH Interface' table has columns for Interface, Description, Type, Vlan8021p, VlanMuxId, Igmp, NAT, Firewall, IPv6, Mld, Remove, and Edit. The '3G/LTE Interface' table has columns for Interface, Description, TEL No., APN, Username, NAT, Firewall, and Edit. Below the tables are 'Add' and 'Remove' buttons.

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	<input type="checkbox"/>	Edit

3G/LTE Interface							
Interface	Description	TEL No.	APN	Username	NAT	Firewall	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Edit

Add Remove

Here the corresponding WAN Service have 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).

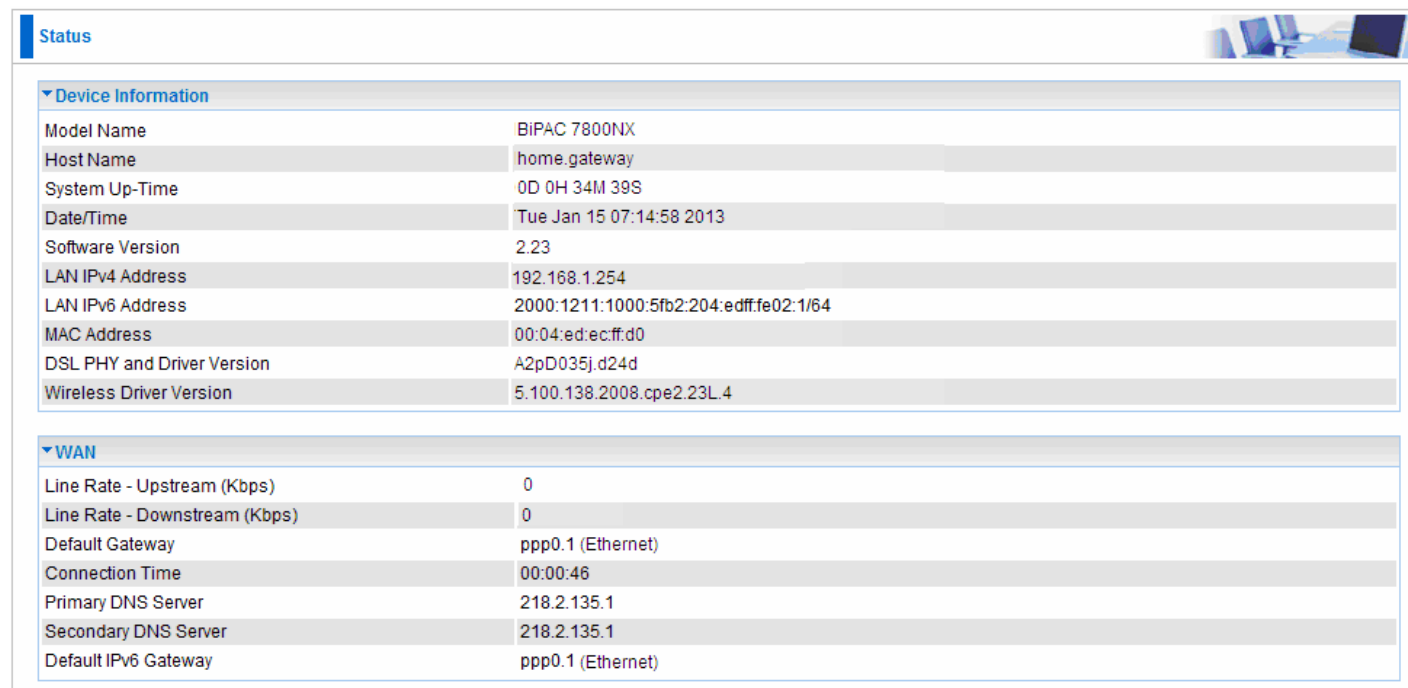
(IPv4 or IPv6)



The screenshot shows the 'Status' page with a 'WAN' section. It contains a 'Wan Info' table with columns for Interface, Description, Type, Status, Connection Time, IPv4 Address, and IPv6 Address. The 'Status' column has a 'Disconnect' button for the ppp0.1 interface.

Wan Info						
Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address
ppp0.1	pppoe_eth0	PPPoE	Disconnect	00:04:54	10.40.90.194	2000:db98:1000:1000:6669:bf38:a1e0:6ce2/64
USB3G0			3G/LTE Card not found			

The device summary information




The screenshot shows the 'Status' page with a 'Device Information' section. It contains a table with various system and network parameters. Below it is a 'WAN' section with a table showing connection statistics and settings.

Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 34M 39S
Date/Time	Tue Jan 15 07:14:58 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:5fb2:204:edffe02:1/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp0.1 (Ethernet)
Connection Time	00:00:46
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway	ppp0.1 (Ethernet)



Configuration


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	<input checked="" type="checkbox"/> Enable		
Option 60 Vendor ID			
Option 61 IAID		8 hexadecimal digits	
Option 61 DUID		hexadecimal digits	
Option 125	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		
WAN IP Address			
WAN Subnet Mask			
WAN gateway IP Address			
IPv6 for this service	<input checked="" type="checkbox"/> Enable		
Obtain an IPv6 address automatically	<input checked="" type="checkbox"/> Enable		
WAN IPv6 Address/Prefix Length			
WAN Next-Hop IPv6 Address			
NAT	<input checked="" type="checkbox"/> Enable	Fullcone NAT	<input type="checkbox"/> Enable
Firewall	<input checked="" type="checkbox"/> Enable	IGMP Multicast	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> 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.

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 IAID:** Enter the associated information provided by your ISP. You should input 8 hexadecimal numbers.

**Option 61 DUID:** Enter the associated information provided by your ISP. You should input hexadecimal number(s).

**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 (**I**nternet **G**roup **M**embership 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 (**M**ulticast **L**istener **D**iscovery 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.



Configuration


WAN Service

Parameters

WAN Port	Ethernet ▾		
Type	Bridging ▾		
Description	<input type="text"/>		
802.1P Priority	<input type="text" value="-1"/> [tagged: 0-7; untagged: -1]	802.1Q VLAN ID	<input type="text" value="-1"/> [tagged: 0-4094; untagged: -1]

Next

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

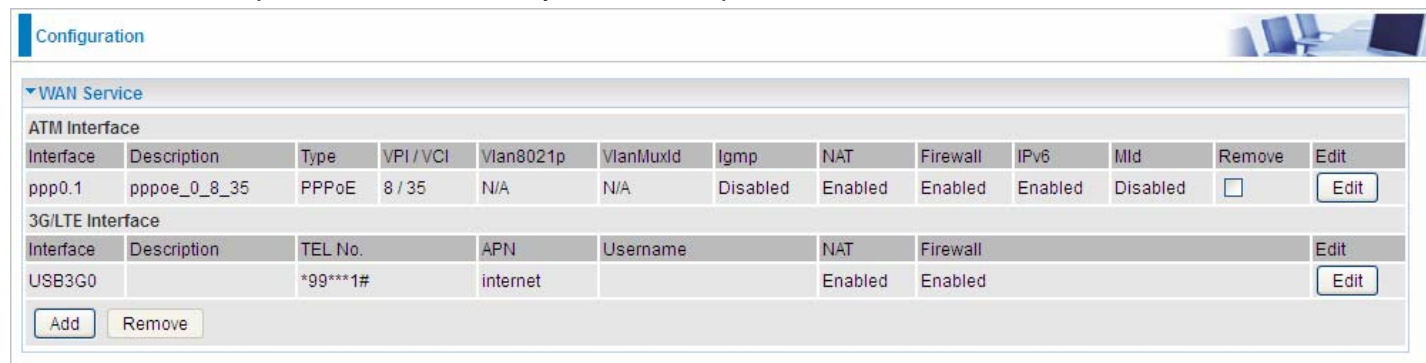
**802.1P Priority:** The parameter indicates the frame priority level from 0 (lowest) to 7 (highest), which can be used to prioritize different classes of traffic (voice, video, data, etc). Enter the priority identification, tagged: 0-1, untagged: -1.

**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.



## 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

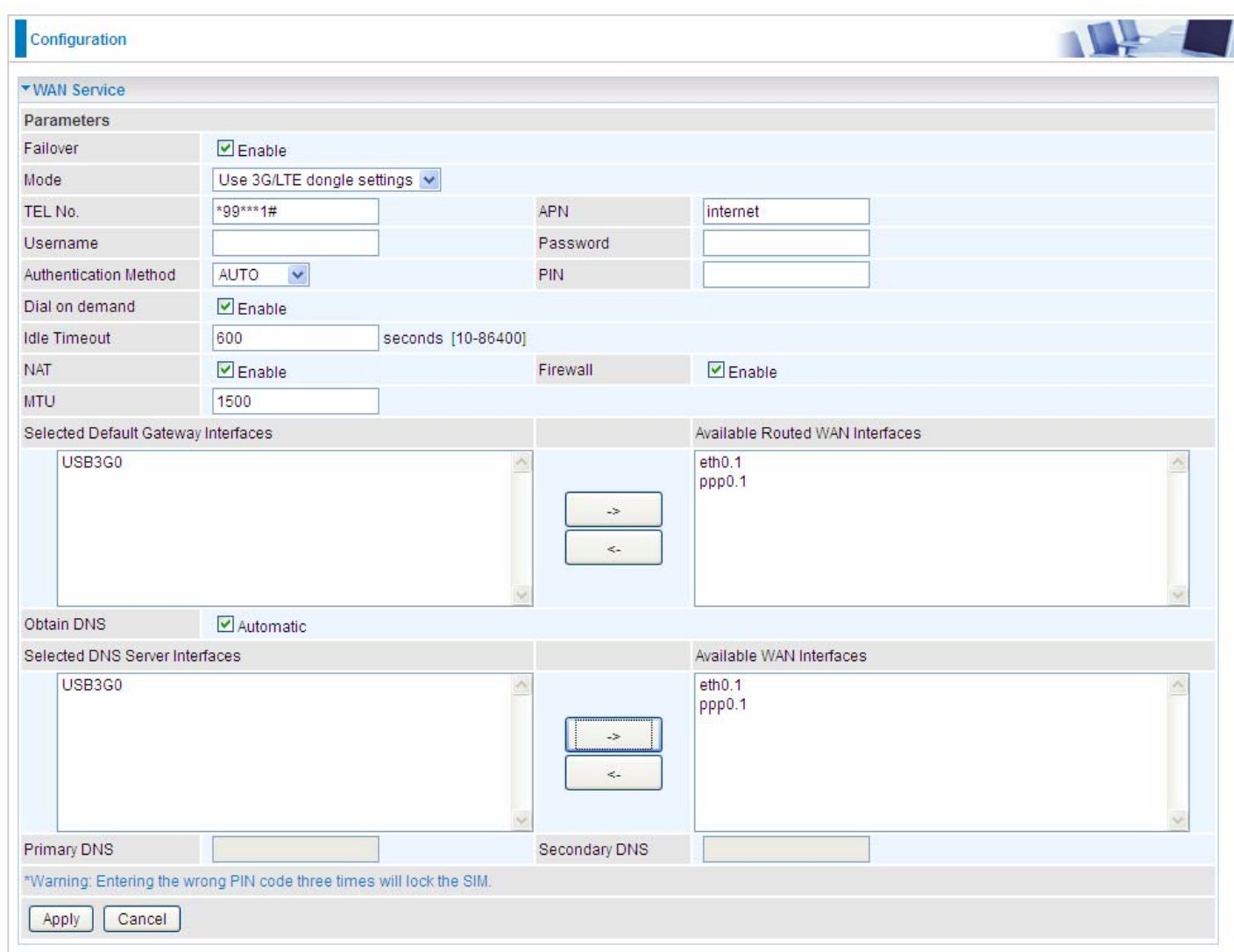
Interface	Description	Type	VPI / VCI	Vlan8021p	VlanMuxId	Icmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_0_8_35	PPPoE	8 / 35	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	Edit

3G/LTE Interface

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

Add Remove

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

Idle Timeout 600 seconds [10-86400]

NAT ☒ Enable Firewall ☒ Enable

MTU 1500

Selected Default Gateway Interfaces Available Routed WAN Interfaces

USB3G0 eth0.1 ppp0.1

Obtain DNS ☒ Automatic

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.

Apply Cancel

**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.

- ① **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	<input checked="" type="checkbox"/> Enable
Idle Timeout	600 seconds [10-86400]

- ① **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	<input type="checkbox"/> Enable
Keep Alive	<input checked="" type="checkbox"/> 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:** Select the IP addresses of the DNS servers.

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
ppp0.1	pppoe_0_8_35	PPPoE	Unconfigured			
ppp3g0	3G0	PPP	Failover / Connected	00:01:10	10.44.183.197	

Status

▼ Device Information

Model Name	BIPAC 7800NX
Host Name	home.gateway
System Up-Time	0D 0H 36M 16S
Date/Time	Tue Jan 15 07:16:35 2013
Software Version	2.23
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:feec:ffd0/64
MAC Address	00:04:ed:ec:ff:d0
DSL PHY and Driver Version	A2pD035j.d24d
Wireless Driver Version	5.100.138.2008.cpe2.23L.4

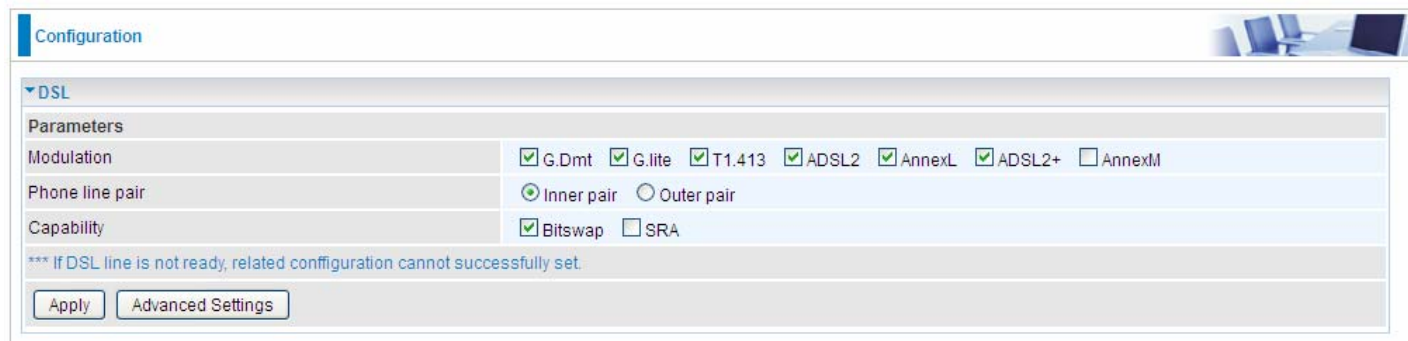
▼ WAN

Line Rate - Upstream (Kbps)	0
Line Rate - Downstream (Kbps)	0
Default Gateway	ppp3g0 (3G/LTE)
Connection Time	00:04:28
Primary DNS Server	221.6.4.66
Secondary DNS Server	58.240.57.33
Default IPv6 Gateway	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.



The image shows a web-based configuration interface for DSL settings. At the top, there is a 'Configuration' tab. Below it, a section titled 'DSL' is expanded. Under 'Parameters', there are three rows: 'Modulation' with checkboxes for G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+, and AnnexM; 'Phone line pair' with radio buttons for Inner pair and Outer pair; and 'Capability' with checkboxes for Bitswap and SRA. A warning message states: '\*\*\* If DSL line is not ready, related configuration cannot successfully set.' At the bottom of the section are 'Apply' and 'Advanced Settings' buttons.

**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.

① Bitswap Enable: Allows bitswaping function.

① SRA Enable: Allows seamless rate adaptation.

Click Apply to confirm the settings.

Click [Advanced Settings](#) to future configure DSL.



The image shows the 'DSL Advanced Settings' screen. It has a 'Configuration' tab at the top. The 'DSL Advanced Settings' section is expanded. Under 'Parameters', there is a 'Test Mode' row with radio buttons for Normal, Reverb, Medley, No Retrain, and L3. At the bottom of the section are 'Apply' and 'Tone Selection' buttons.

Select the Test Mode, or leave it as default.

**Tone Selection:** This should be left as default or be configured by an advanced user.

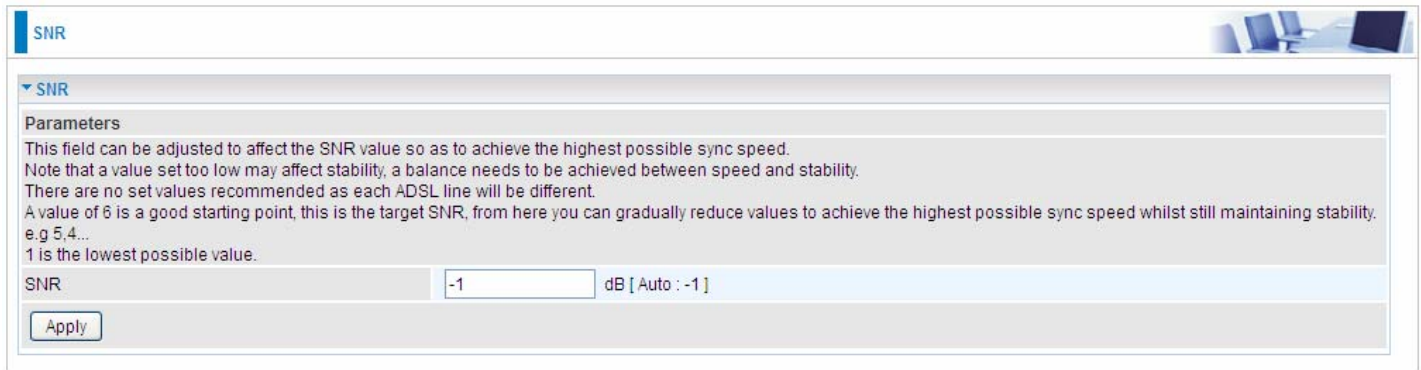
The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart.

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.



The screenshot shows a configuration window titled "SNR" with a sub-section "Parameters". The text in the Parameters section explains that the SNR value can be adjusted to affect the sync speed, but a balance between speed and stability is needed. It notes that there are no set values recommended for ADSL lines and that a value of 6 is a good starting point. It also mentions that 1 is the lowest possible value. Below the text, there is a text input field labeled "SNR" containing the value "-1", followed by the unit "dB [ Auto : -1 ]". An "Apply" button is located at the bottom left of the configuration area.

SNR

▼ SNR

**Parameters**

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  dB [ Auto : -1 ]

Apply

**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	<input checked="" type="checkbox"/> Enable
First NTP time server	Other <input type="text" value="192.43.244.18"/>
Second NTP time server	Other <input type="text" value="128.138.140.44"/>
Third NTP time server	Other <input type="text" value="129.6.15.29"/>
Fourth NTP time server	Other <input type="text" value="131.107.1.10"/>
Fifth NTP time server	None <input type="text"/>
Time zone offset	(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London <input type="text"/>

Apply

Cancel

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.

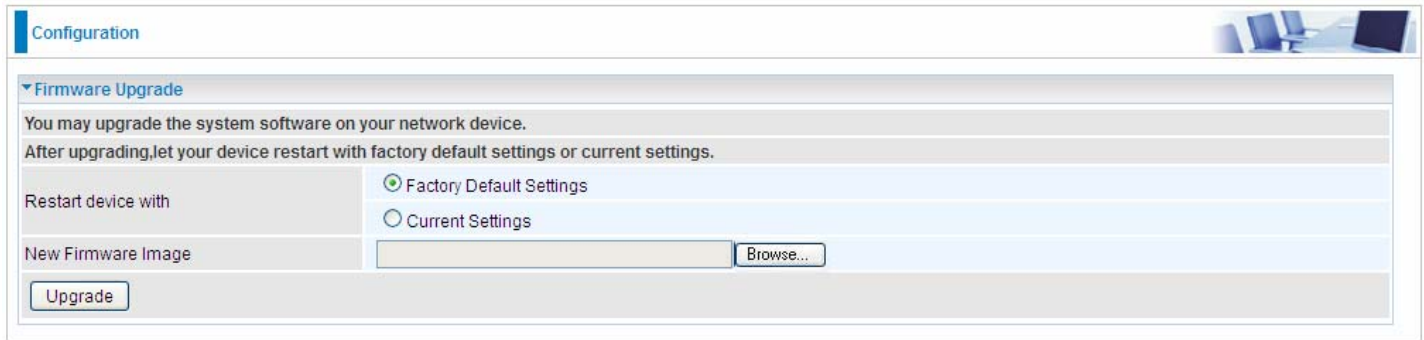
Choose your local time zone from the drop-down menu. After a successful connection to the Internet, the router will retrieve the correct local time from the NTP server you have specified. If you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their 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.



The screenshot shows the 'Configuration' tab of a router's web interface. Under the 'Firmware Upgrade' section, there is a heading 'You may upgrade the system software on your network device.' followed by the instruction 'After upgrading, let your device restart with factory default settings or current settings.' Below this, there are two radio buttons: 'Factory Default Settings' (which is selected) and 'Current Settings'. To the left of these radio buttons is the label 'Restart device with'. Below the radio buttons is a text input field for 'New Firmware Image' with a 'Browse...' button next to it. At the bottom left of the section is an 'Upgrade' button.

### Restart device with:

- ① **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.
- ① **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 upgrading 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.

Backup Settings

Restore Configuration

Configuration File

Browse...

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

Update Settings

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...

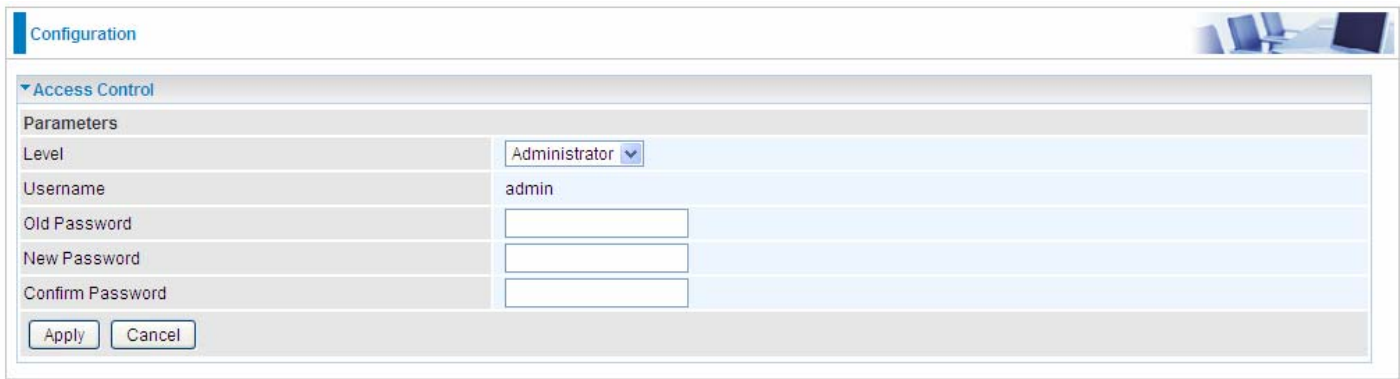
Do not switch off device during flash update or rebooting.

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.



The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Administrator'. The 'Username' is 'admin'. There are three empty text boxes for 'Old Password', 'New Password', and 'Confirm Password'. At the bottom are 'Apply' and 'Cancel' buttons.

**Level:** select which level you want to change password to. There are three default levels.

- ① **Administrator:** the root user, corresponding default username and password are admin and admin respectively.
- ① **Remote:** username for the remote user to login, corresponding default username and password are support and support respectively.
- ① **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.

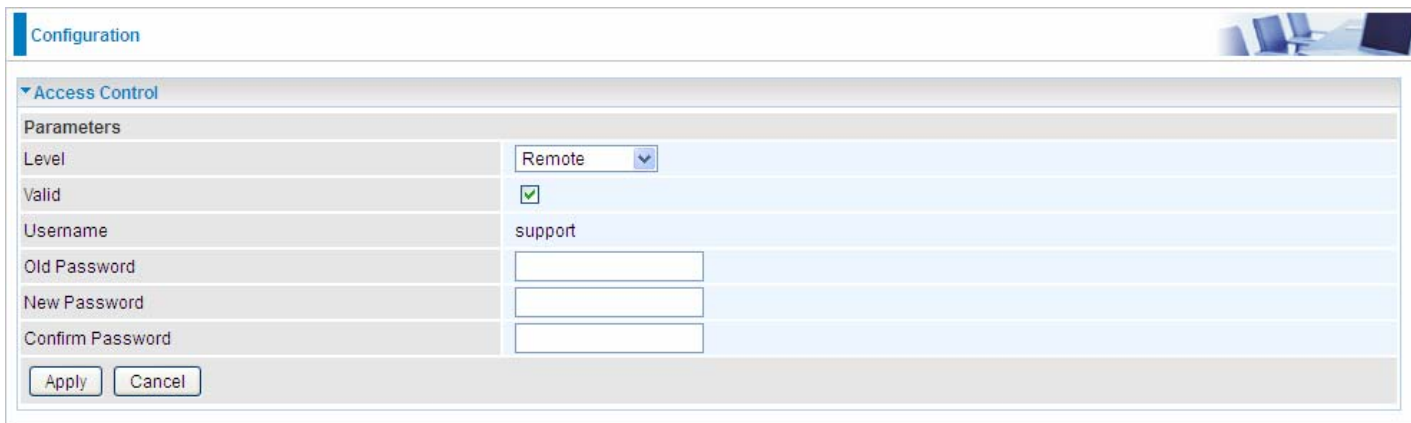
**Username:** the default username for each user level.

**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.



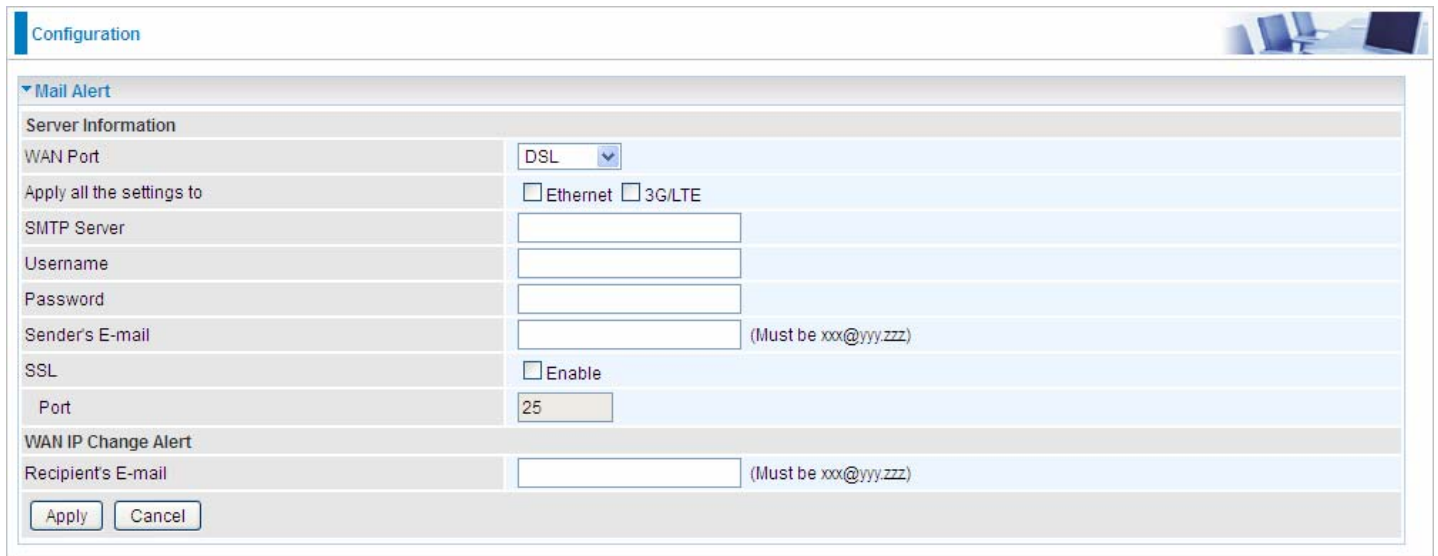
The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Remote'. The 'Valid' checkbox is checked. The 'Username' is 'support'. There are three empty text boxes for 'Old Password', 'New Password', and 'Confirm Password'. At the bottom are 'Apply' and 'Cancel' buttons.

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.



The screenshot shows a web-based configuration interface for 'Mail Alert'. At the top, there is a 'Configuration' tab and a small graphic of a server room. The main section is titled 'Mail Alert' and contains several fields for configuration. Under 'Server Information', there is a 'WAN Port' dropdown menu currently set to 'DSL'. Below it, there are checkboxes for 'Ethernet' and '3G/LTE'. The 'Apply all the settings to' checkbox is also present. There are input fields for 'SMTP Server', 'Username', 'Password', and 'Sender's E-mail' (with a note '(Must be xxx@yyy.zzz)'). There is a checkbox for 'SSL' and a 'Port' field set to '25'. Under 'WAN IP Change Alert', there is a 'Recipient's E-mail' field (also with a note '(Must be xxx@yyy.zzz)'). At the bottom, there are 'Apply' and 'Cancel' buttons.

Mail Alert	
<b>Server Information</b>	
WAN Port	DSL
Apply all the settings to	<input type="checkbox"/> Ethernet <input type="checkbox"/> 3G/LTE
SMTP Server	
Username	
Password	
Sender's E-mail	(Must be xxx@yyy.zzz)
SSL	<input type="checkbox"/> Enable
Port	25
<b>WAN IP Change Alert</b>	
Recipient's E-mail	(Must be xxx@yyy.zzz)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**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.

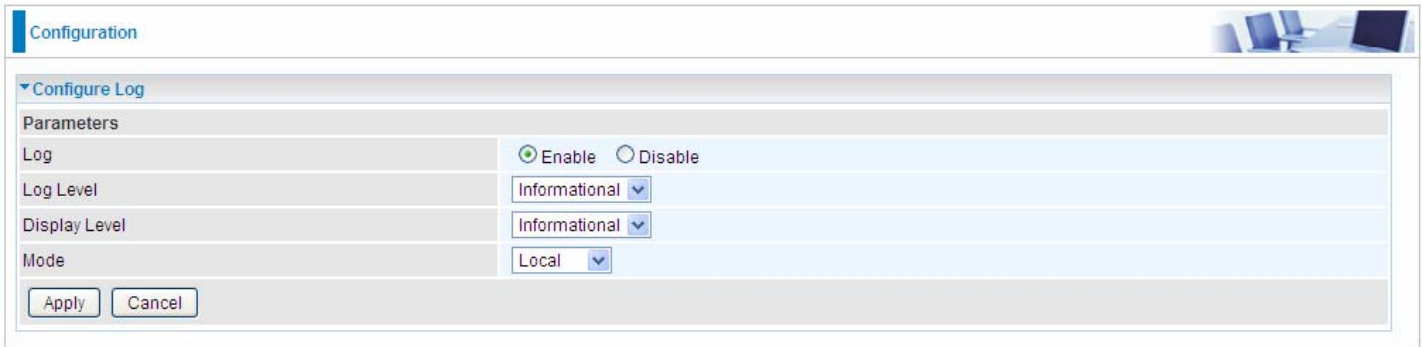
**SSL:** check to whether to enable SSL encryption feature.

**Port:** the port, default is 25.

**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.



## Configure Log



**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:

- ① **Emergency** = system is unusable
- ① **Alert** = action must be taken immediately
- ① **Critical** = critical conditions
- ① **Error** = error conditions
- ① **Warning** = warning conditions
- ① **Notice** = normal but significant conditions
- ① **Informational** = information events
- ① **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.

- ① **Local:** Select this mode to store the logs in the router's local memory.
- ① **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.
- ① **Both:** Logs stored adopting above two ways.

Click **Apply** to save your settings.

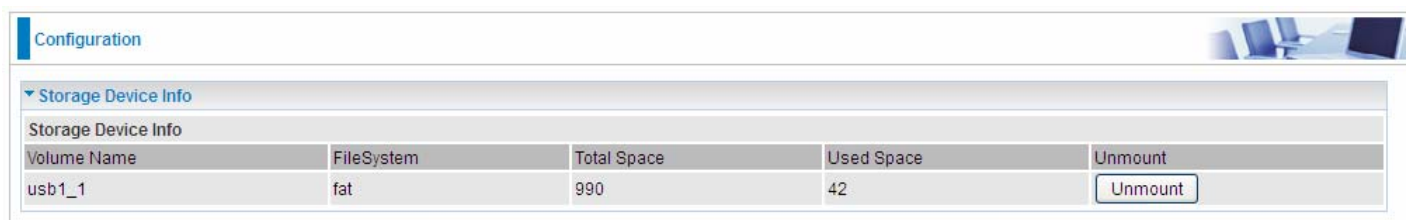


# USB

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.



The screenshot shows a web interface with a 'Configuration' tab. Under the 'Storage Device Info' section, there is a table with the following data:

Volume Name	FileSystem	Total Space	Used Space	Unmount
usb1_1	fat	990	42	<button>Unmount</button>

**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.

Configuration

User Accounts

User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove
admin	/	

Add

Remove

Click **Add** button, enter the user account-adding page:

Configuration

User Accounts

Parameters

Username	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Volume Name	usb1_1

Apply

Cancel

**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.

Configuration

User Accounts

User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove
admin	/	
test	usb1_1/test	<input type="checkbox"/>

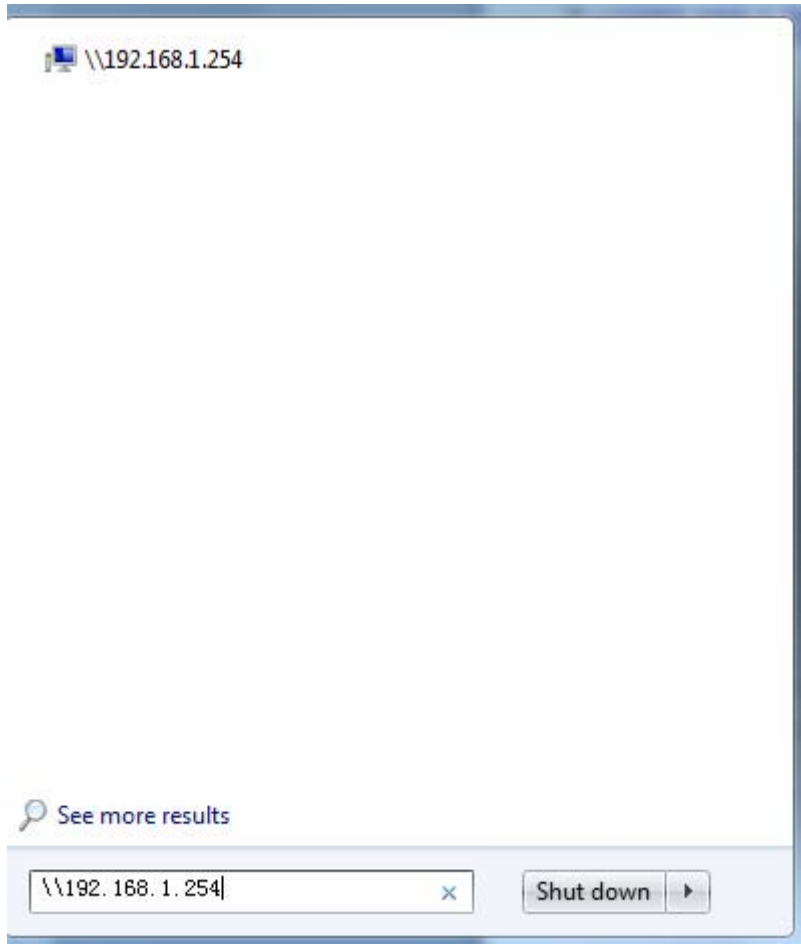
Add

Remove



## Accessing mechanism of Storage:

In your computer, Click **Start** > **Run**, enter [\\192.168.1.254](http://192.168.1.254)



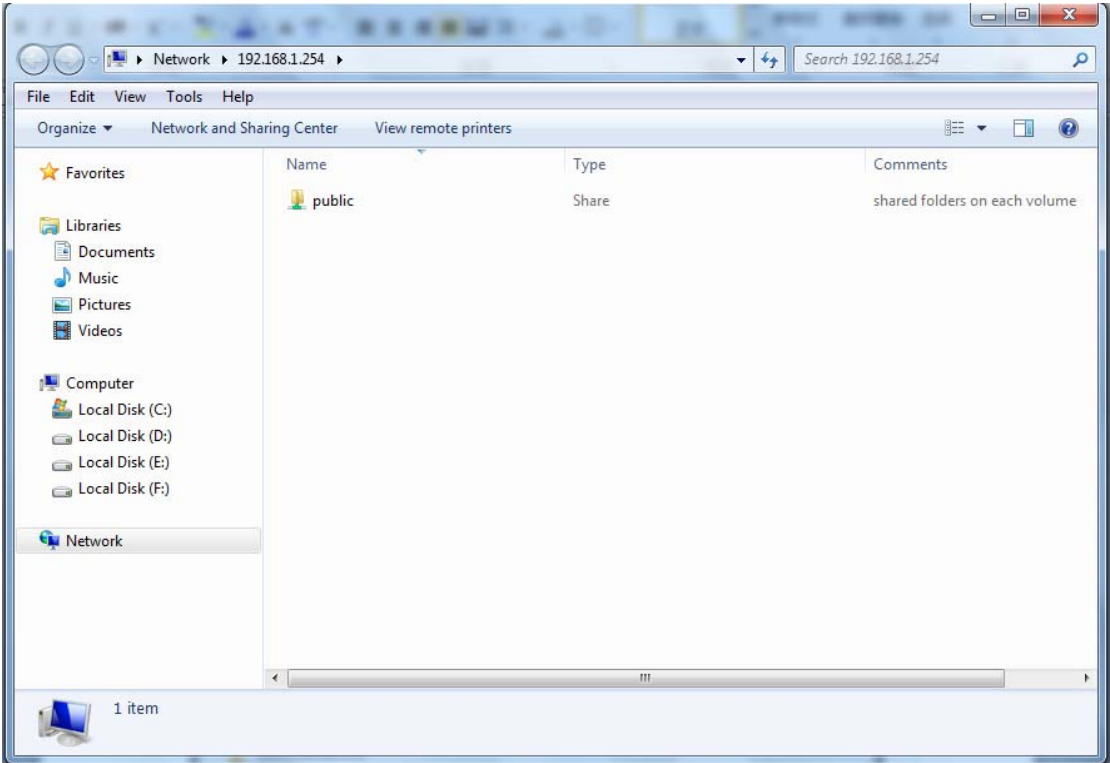


When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

When first logged on to the network folder, you will see the “**public**” folder.

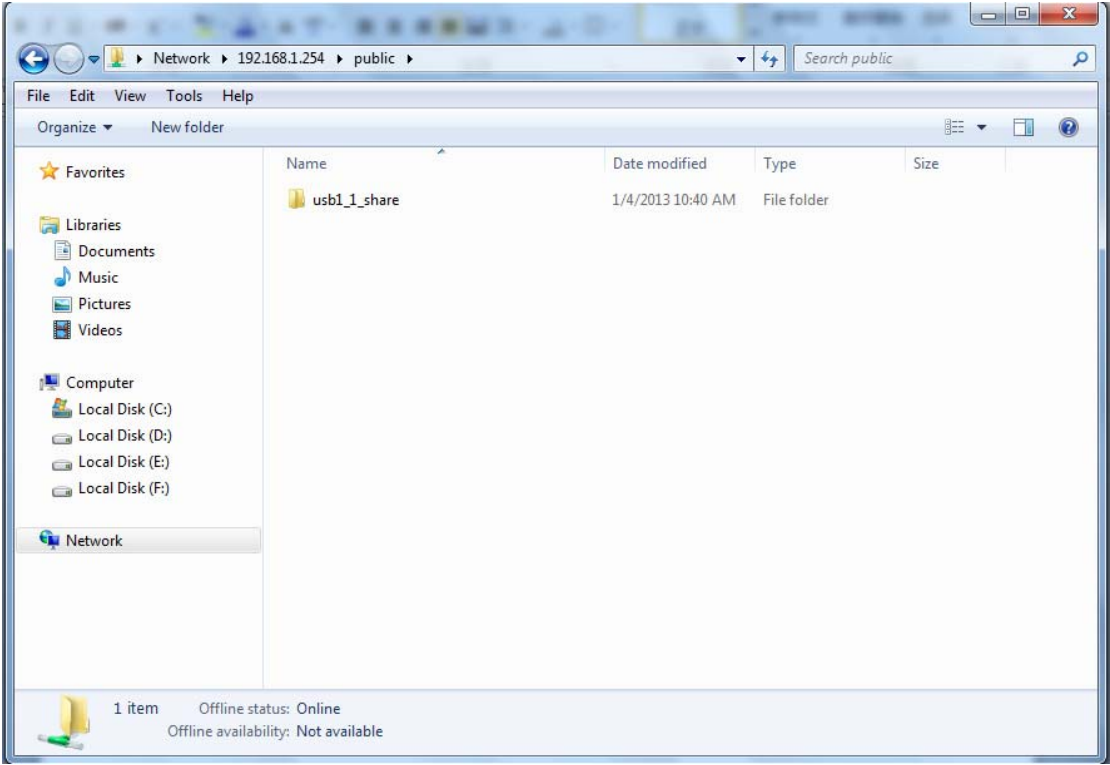
**Public:** The public sharing space for each user in the USB Storage.

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.



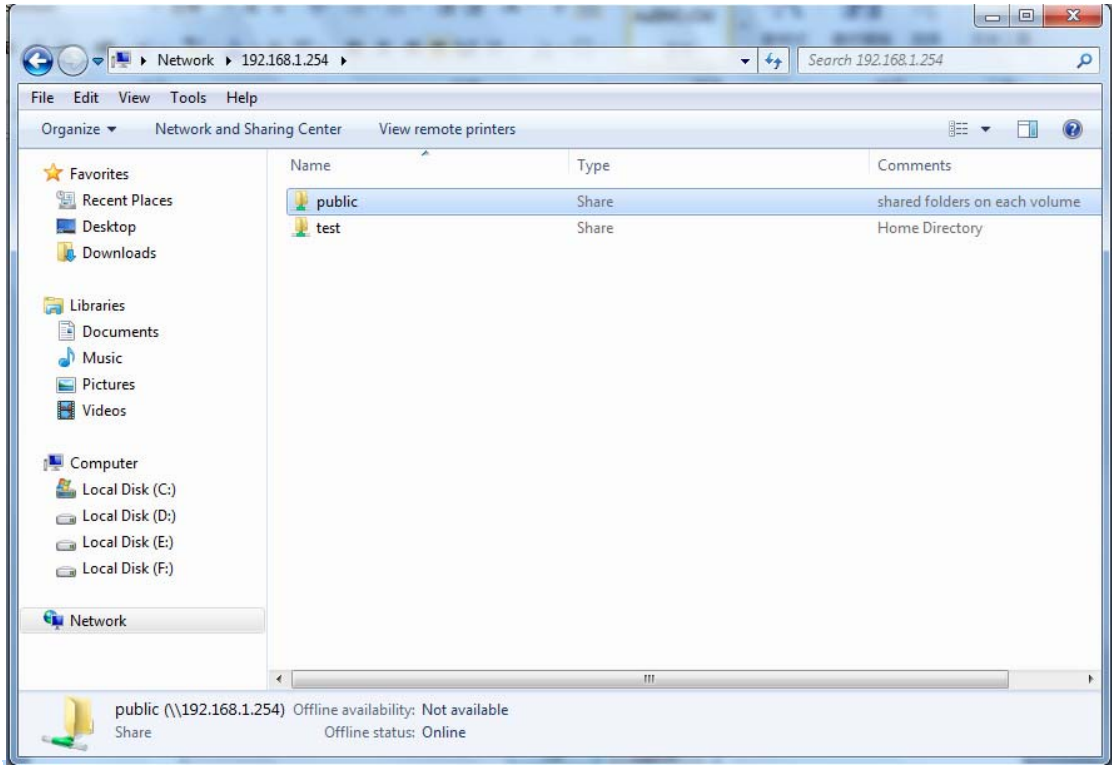


Access the folder *public*.





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.





## 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 7800(N)X(L). 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 (7800NX for example)

1. Connect the printer to the 7800NX's USB port
2. Enable the print server on the 7800NX
3. Install the printer drivers on the PC you want to print from



The screenshot shows a 'Configuration' window with a 'Print Server' section. Under 'Parameters', there are three fields: 'On-board Print Server' with a checked 'Enable' checkbox, 'Printer Name' with the text 'OfficePrinter', and 'Make And Model' with the text 'Epson Stylus Photo R2!'. At the bottom of the section are 'Apply' and 'Cancel' buttons.

**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*

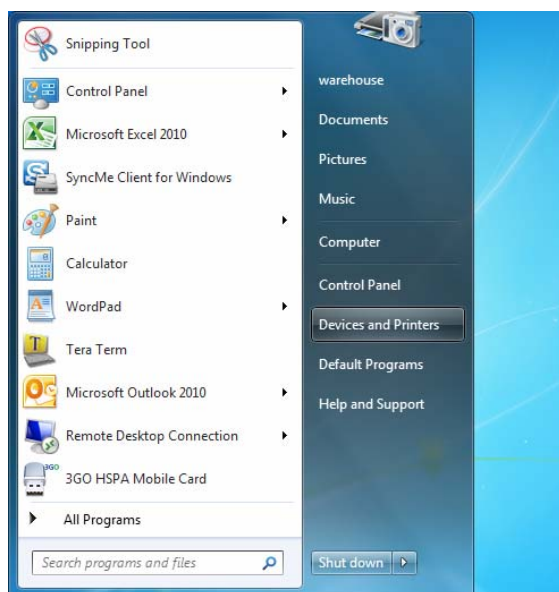
### Note:

The **Printer name** can be any text string up to **40** characters. It cannot contain spaces.

The **Make and Model** 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"

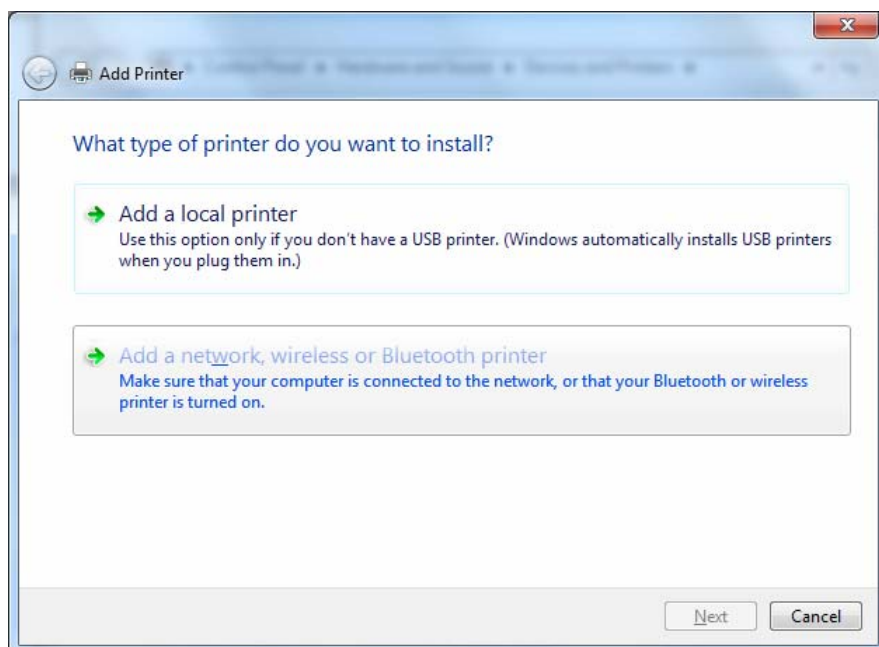




**Step 2:** Click “Add a Printer”.

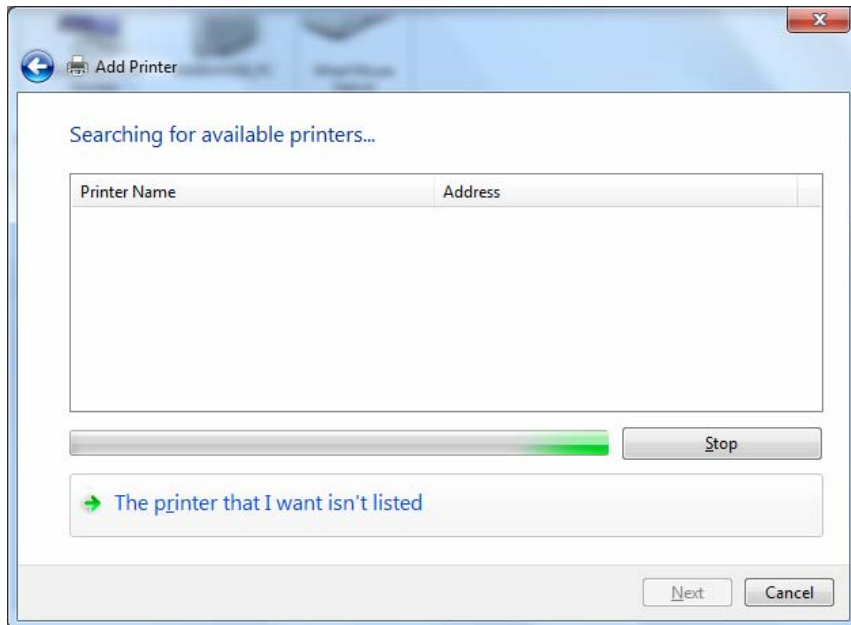


**Step 3:** Click “Add a network, wireless or Bluetooth printer





**Step 4:** Click “The printer that I want isn’t listed”



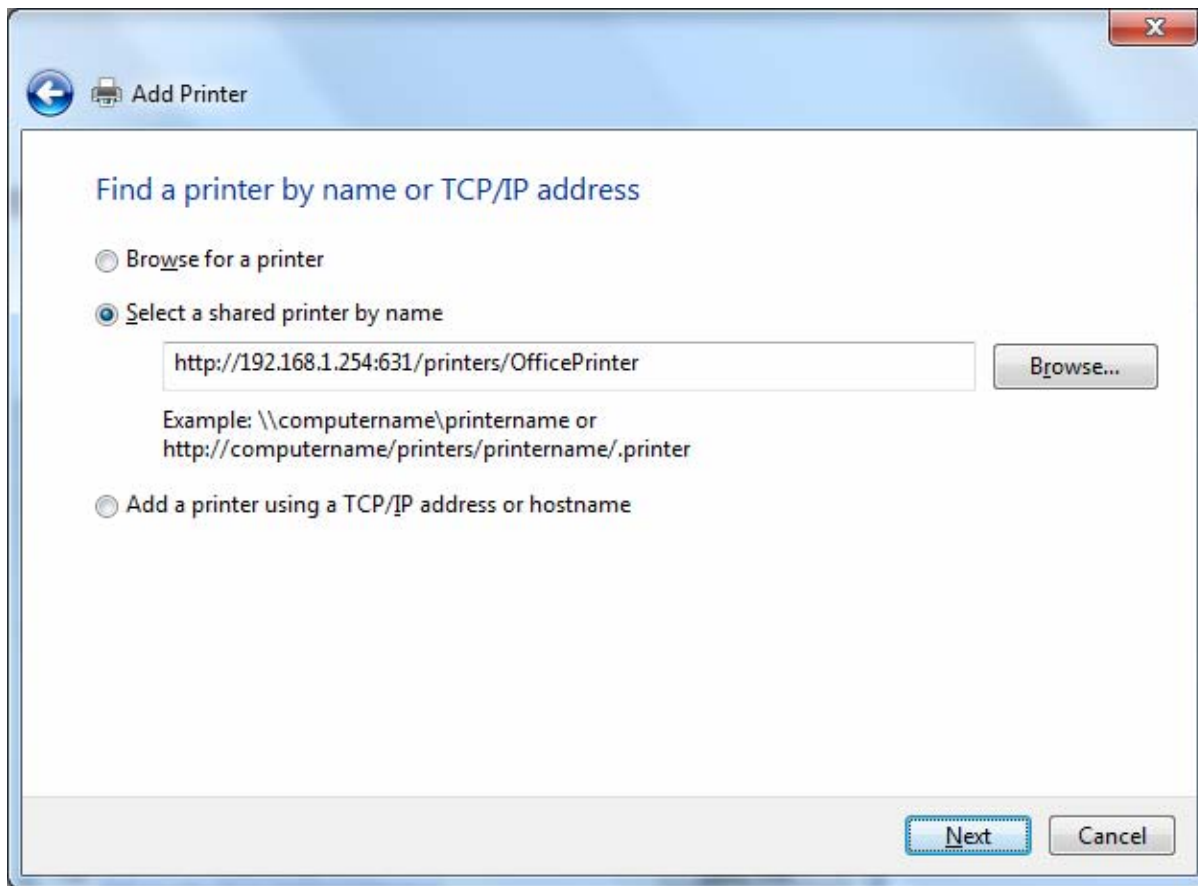
**Step 5:** Select “Select a shared printer by name”

Enter `http://7800NX- LAN-IP:631/printers/printer-name` or. Make sure printer’s name is the same as what you set in the 7800NX earlier

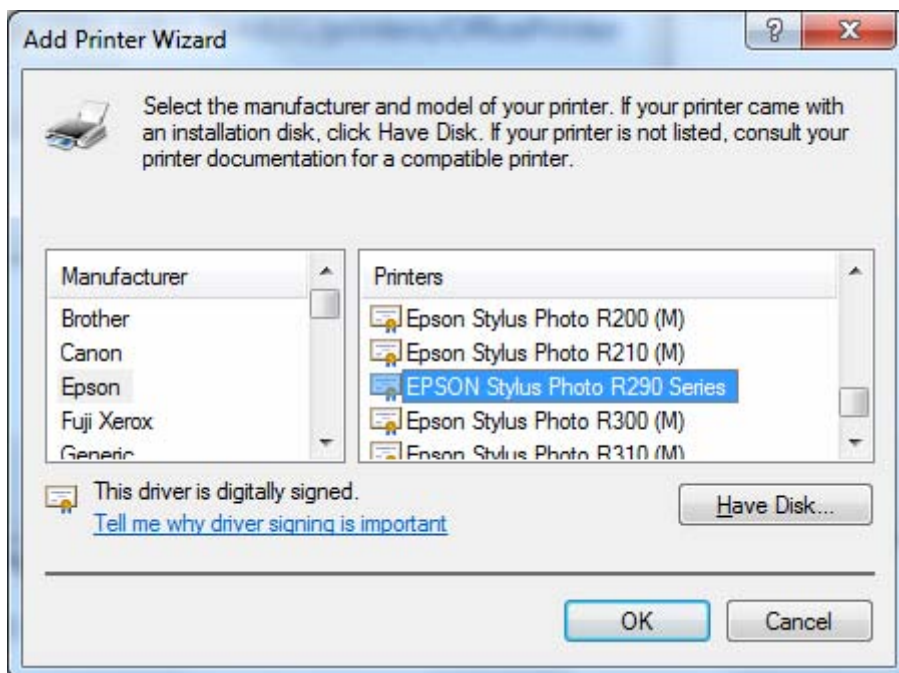
For Example: `http://192.168.1.254:631/printers/OfficePrinter`

OfficePrinter is the Printer Name we setup earlier



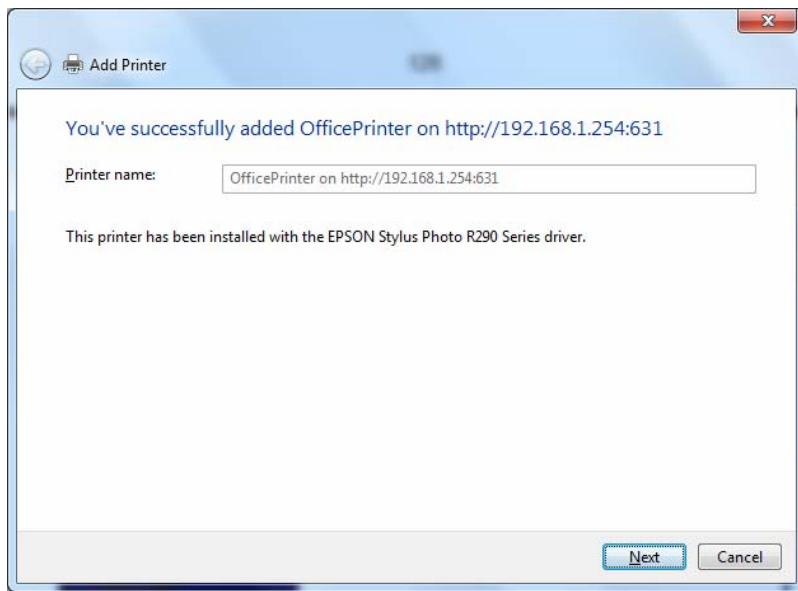


**Step 6:** Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.

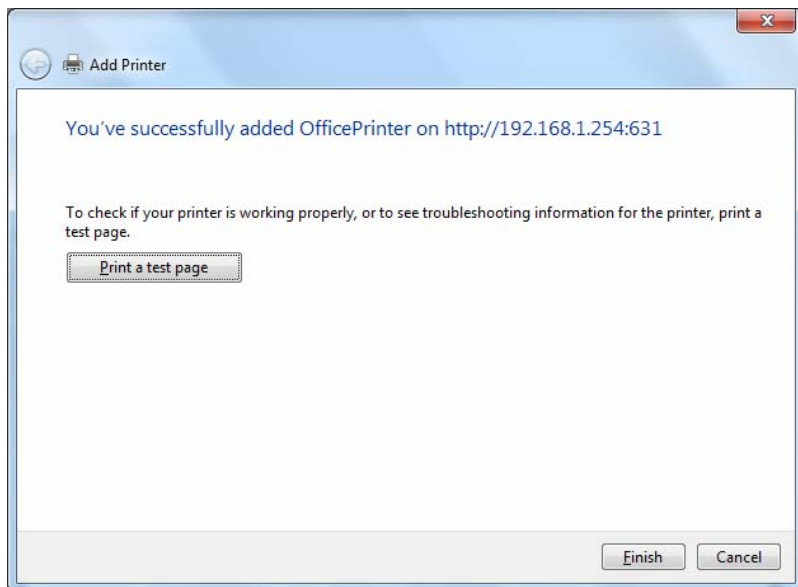


**Step 7:** Click “Next”



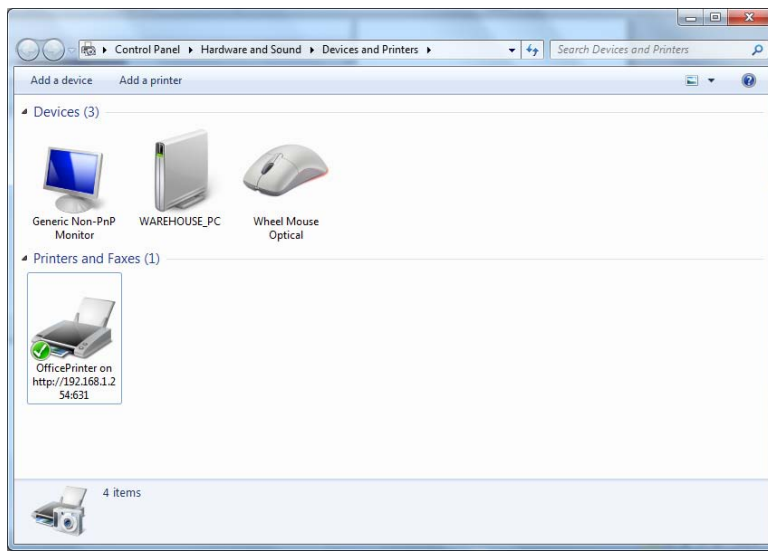


**Step 8:** Click “Next” and you are done



You will now be able to see your printer on the Devices and Printers Page







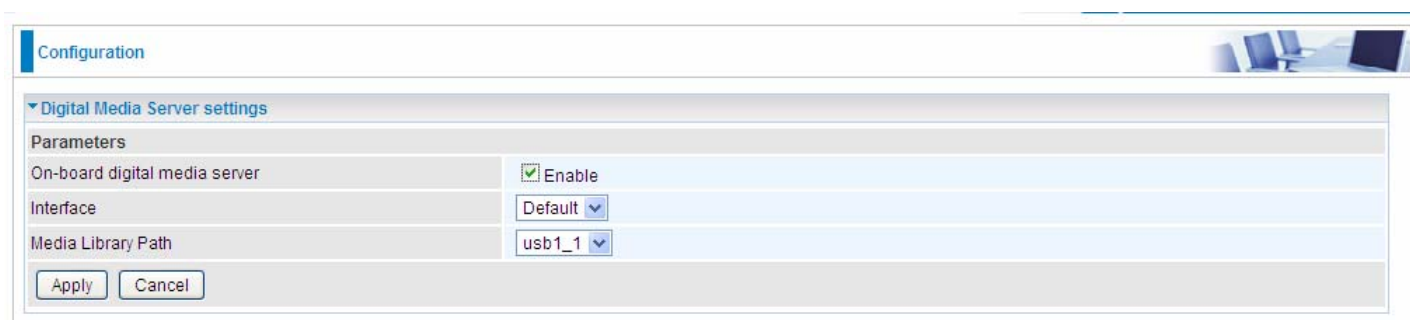
## DLNA

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, 7800(N)X(L) can serve as a DLNA server.



The screenshot shows a 'Configuration' window with a 'Digital Media Server settings' section. Under 'Parameters', there are three settings: 'On-board digital media server' is checked and set to 'Enable'; 'Interface' is set to 'Default'; and 'Media Library Path' is set to 'usb1\_1'. At the bottom of the settings section are 'Apply' and 'Cancel' buttons.

Parameters	
On-board digital media server	<input checked="" type="checkbox"/> Enable
Interface	Default
Media Library Path	usb1_1

Apply Cancel

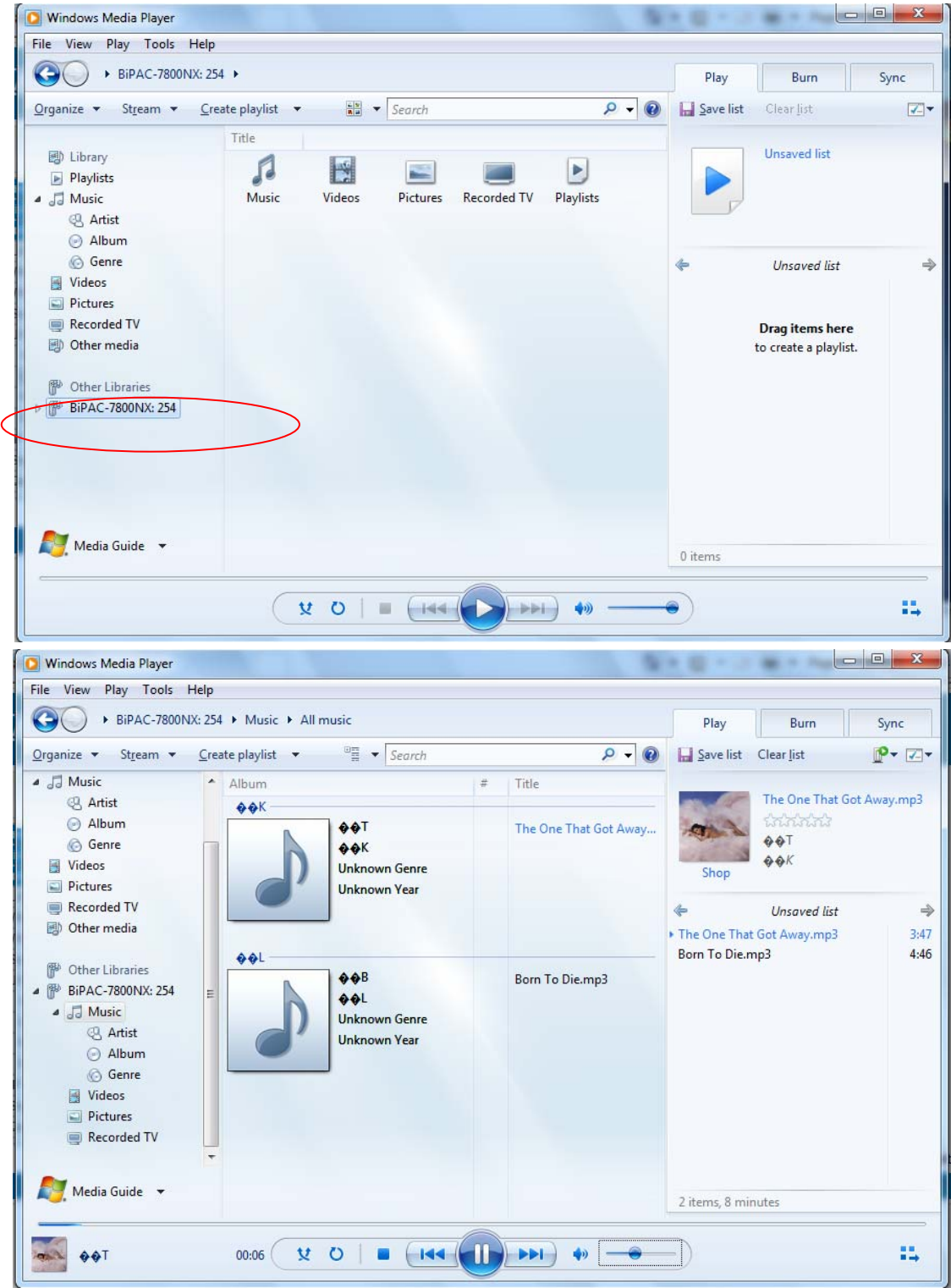
**On-board digital media server:** Enable to share the device as a DLNA server.

**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 .





# 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:

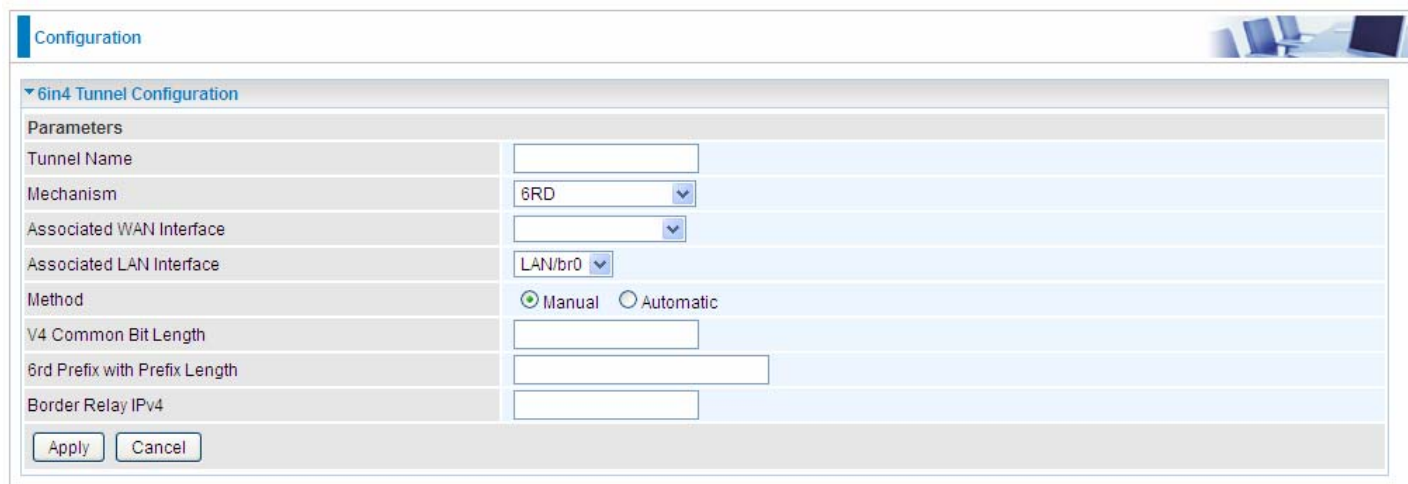
6RD is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of internet service providers (ISPs).

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.



The screenshot shows a configuration window titled "Configuration" with a sub-tab "IPv6inIPv4". Below this is the "6in4 Tunnel Configuration" section, which contains a table with columns: Name, WAN, LAN, Dynamic, V4 Common Bit Length, 6rd Prefix with Prefix Length, Border Relay Address, and Remove. The table is currently empty. Below the table are "Add" and "Remove" buttons.

Click **Add** button to manually add the 6in4 rules.



The screenshot shows the "6in4 Tunnel Configuration" window. It has a "Parameters" section with the following fields: Tunnel Name (text input), Mechanism (dropdown menu set to "6RD"), Associated WAN Interface (dropdown menu), Associated LAN Interface (dropdown menu set to "LAN/br0"), Method (radio buttons for "Manual" and "Automatic", with "Manual" selected), V4 Common Bit Length (text input), 6rd Prefix with Prefix Length (text input), and Border Relay IPv4 (text input). At the bottom are "Apply" and "Cancel" buttons.

**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 encapsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.



## IPv4inIPv6

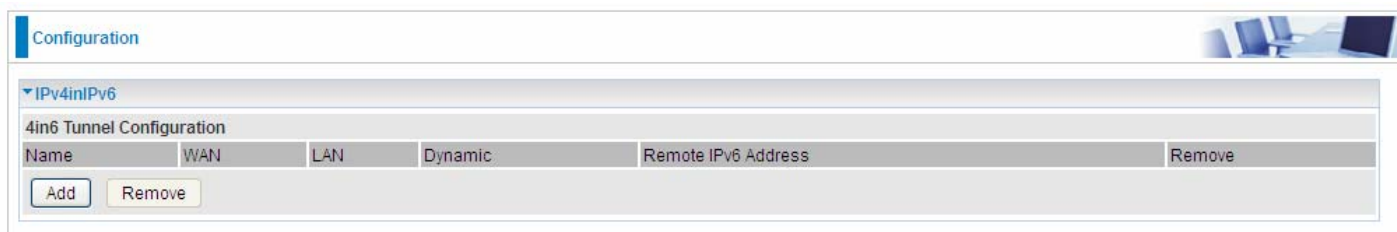
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

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

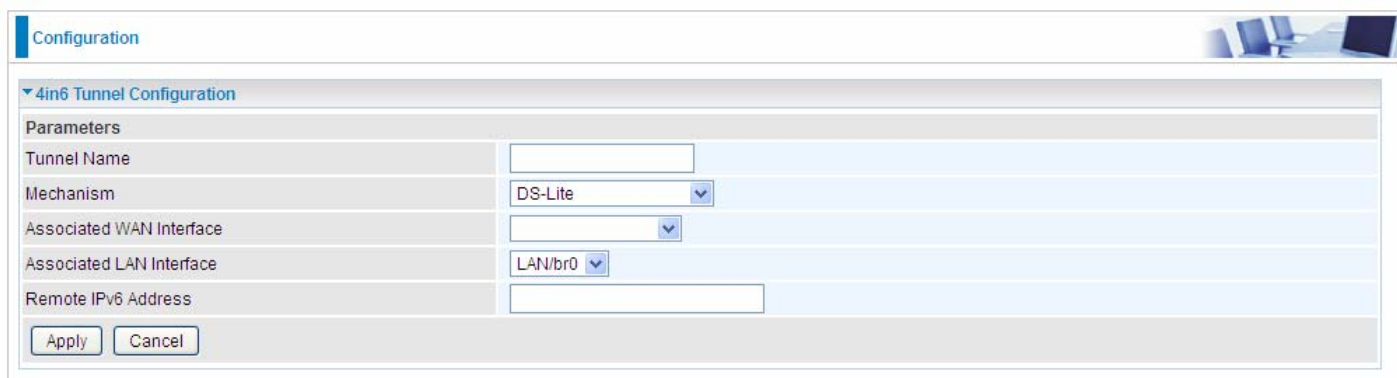
DS – Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

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.



The screenshot shows a web interface titled "Configuration" with a sub-section "IPv4inIPv6". Below this is a "4in6 Tunnel Configuration" section containing a table with columns: Name, WAN, LAN, Dynamic, Remote IPv6 Address, and Remove. The table is currently empty. Below the table are "Add" and "Remove" buttons.

Click **Add** button to manually add the 4in6 rules.



The screenshot shows the "4in6 Tunnel Configuration" form. It includes the following fields and controls:

- Tunnel Name:** A text input field.
- Mechanism:** A dropdown menu with "DS-Lite" selected.
- Associated WAN Interface:** A dropdown menu.
- Associated LAN Interface:** A dropdown menu with "LAN/br0" selected.
- Remote IPv6 Address:** A text input field.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

**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.

**Remote IPv6 Address:** Specify the remote IPv6 address. The remote relay is used to unwrap encapsulated IPv6 packets into IPv4 packets, and do the NAT before sending them to the IPv4 network.



# 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

Filter Name	IP Version	Protocol	Source IP address	Source Port	Log	Remove	Edit
			Destination IP address	Destination Port			
Add	Remove						

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

:

00

To

00

:

00

:

00

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 ) 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 of Sun to 19:00 of 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:** 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

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Filter Name	IP Version	Protocol	Source IP address	Source Port	Log	Remove	Edit
			Destination IP address	Destination Port			
FTP	4	TCP	Any	Any	Disable	<input type="checkbox"/>	Edit
			Any	21			

Add

Remove



## 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	Source Port	Destination IP address	Destination Port	Log	Remove	Edit
-------------	------------	------------	----------	-------------------	-------------	------------------------	------------------	-----	--------	------

Add Remove

Click **Add** button to enter the exact rule setting page.

Configuration

Incoming IP Filtering Setup

Parameters

Filter Name: [text box] << --type or select from listbox-- >>

IP Version: IPv4

Protocol: TCP/UDP

Protocol Number: [text box] [0 - 254]

Source IP address: [text box] ~ [text box]

Source Port: [text box] [port or port:port]

Destination IP address: [text box] ~ [text box]

Destination Port: [text box] [port or port:port]

Interfaces: ☒ All ☒ ipoe\_eth0/eth0.1 ☒ br0/br0

Time Schedule: Always On [dropdown] ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat From [00]:[00] To [00]:[00]

Log: ☐

Apply Remove

**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 ) 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 of Sun to 19:00 of 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:** check the check-box to record the security log. To check the log, users can turn to [Security Log](#).

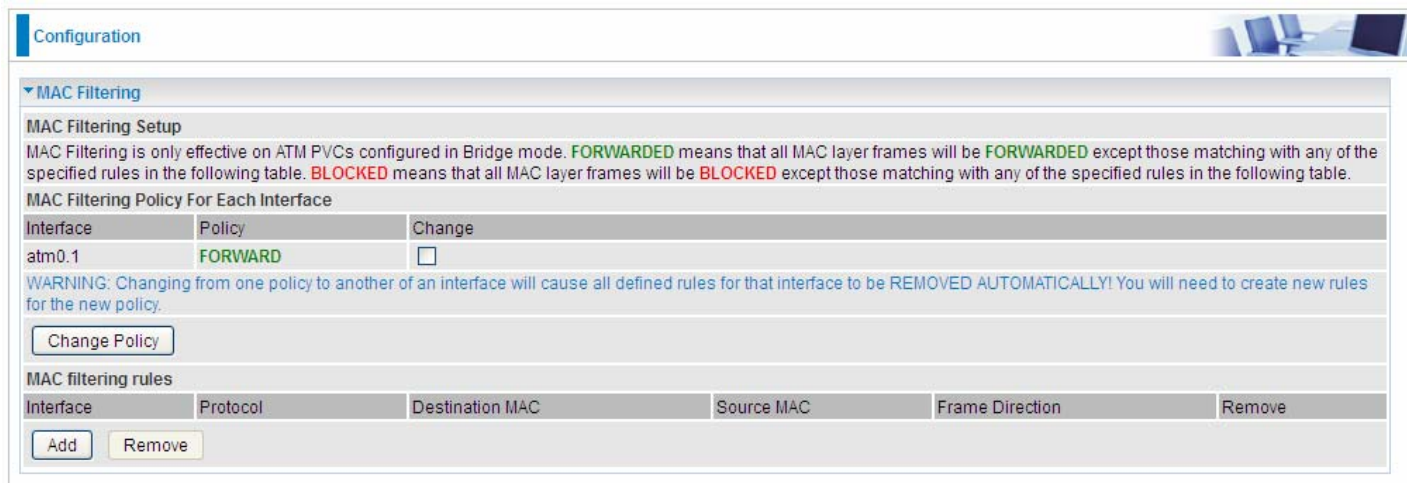


## MAC Filtering

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	<input type="checkbox"/>

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.

Change Policy

MAC filtering rules

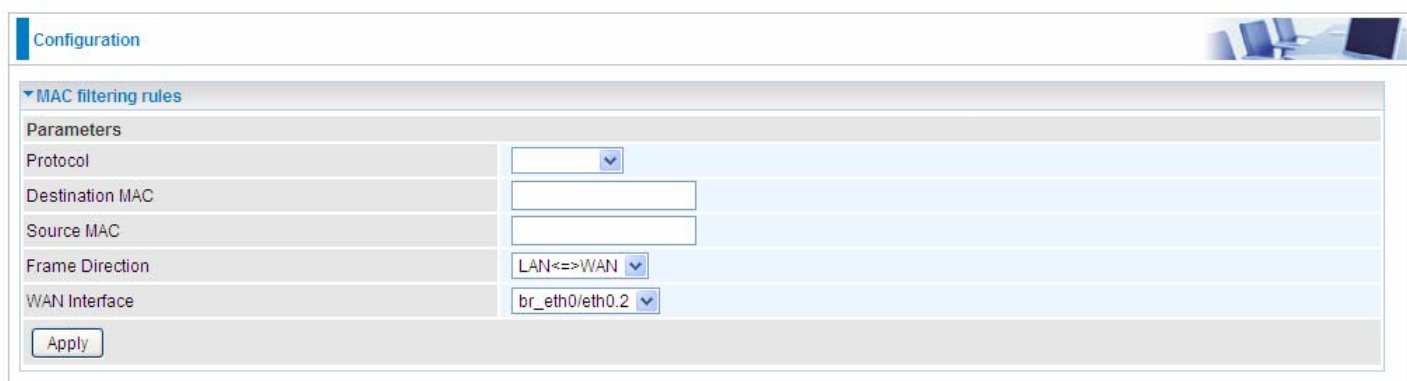
Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
-----------	----------	-----------------	------------	-----------------	--------

Add 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

WAN Interface

Apply

**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.

Configuration

▼Block WAN PING

Parameters

Block WAN PING	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block WAN (IPv6) PING	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Cancel

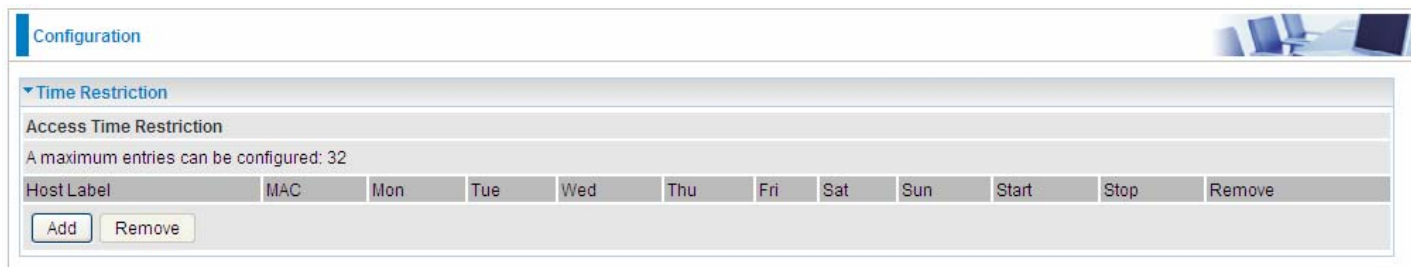


## Time Restriction

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.

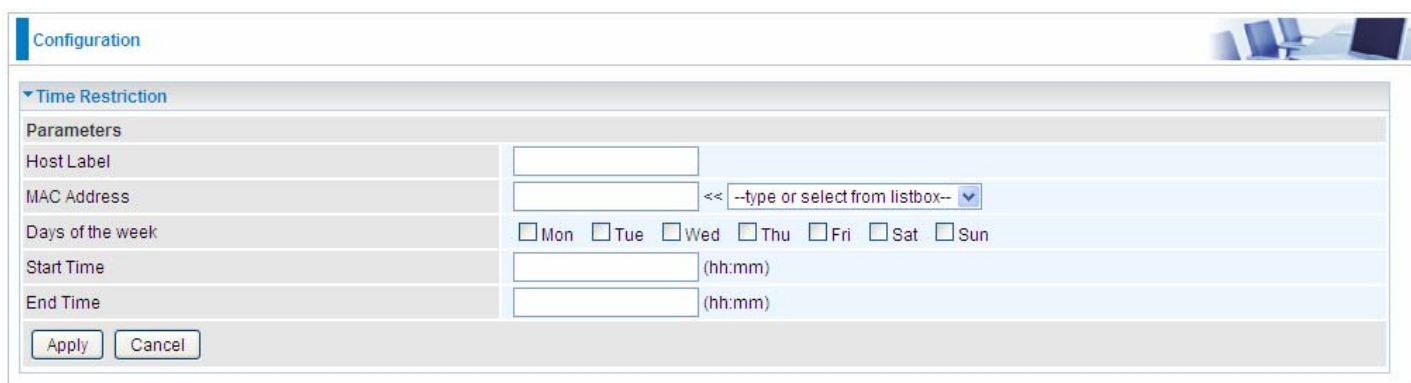
This page adds time of day restriction to a special LAN device connected to the router. To **Restrict** LAN device(s), please click Add button to add the device(s) from accessing internet under some set time. To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

**Note:** The maximum entries configured: 32.



The screenshot shows the 'Configuration' page with a 'Time Restriction' section. It includes a table with columns: Host Label, MAC, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start, Stop, and Remove. Below the table are 'Add' and 'Remove' buttons. A note states: 'A maximum entries can be configured: 32'.

Click **Add** to add the rules.



The screenshot shows the 'Parameters' section of the 'Time Restriction' configuration. It includes fields for Host Label, MAC Address (with a dropdown menu), Days of the week (checkboxes for Mon-Sun), Start Time (hh:mm), and End Time (hh:mm). Below these fields are 'Apply' and 'Cancel' buttons.

**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.

**Days of the week:** Select the days of a week the rule takes efforts.

**Start Time:** Enter the start time of each day in hh:mm format. Leaving it empty means 00:00.

**End Time:** Enter the end time of each day in hh:mm format. Leaving it empty means 23:59.

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	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
child_use	18:a9:05:04:12:23	x	x	x	x	x			0:0	23:59	<input type="checkbox"/>

Add

Remove

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.

If you needn't this rule, you can check the box, press Remove, it will be OK.

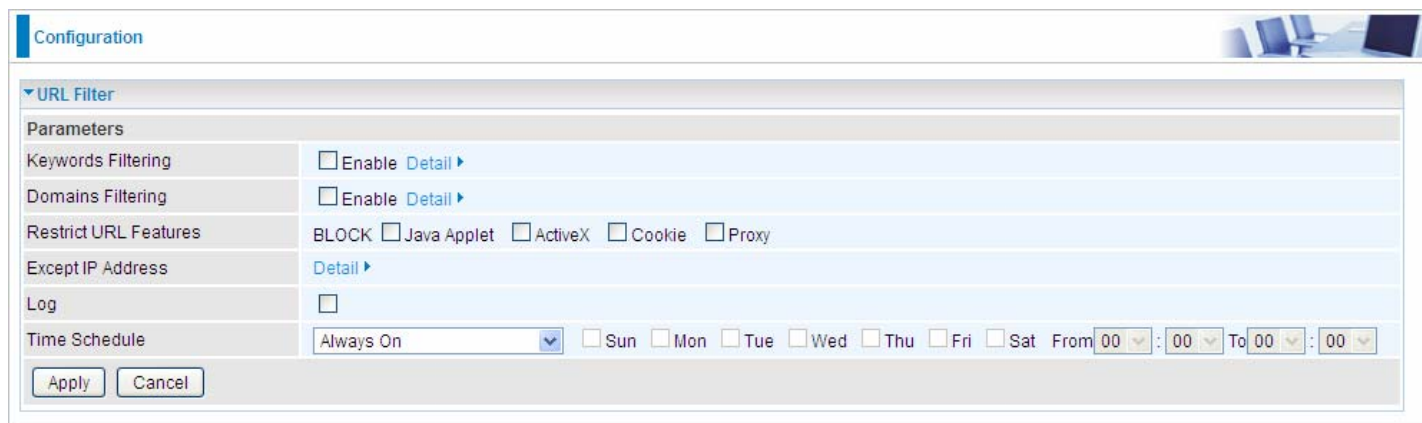


## URL Filter

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.



The screenshot shows the 'Configuration' window for the 'URL Filter'. It contains several settings:

- 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 (dropdown), ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat, From  :  :  To  :  :

Buttons: [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 of Sun to 19:00 of 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](#).

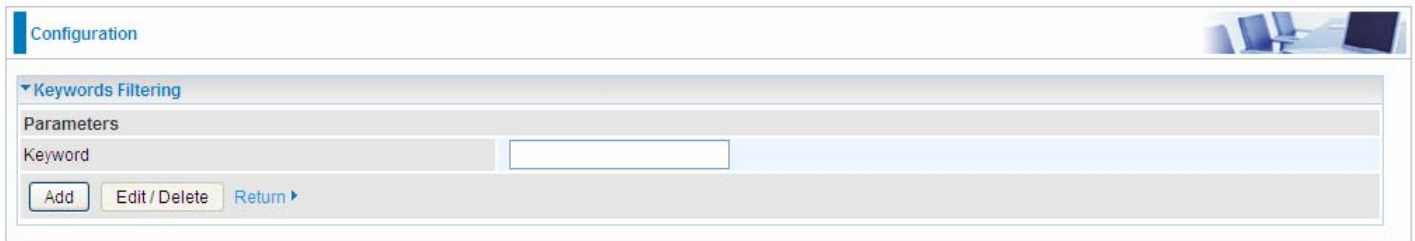
**Log:** Select Enable for this option if you will like to capture the logs for this URL filter policy. To check the log, users can turn to [Security Log](#).



## Keywords Filtering

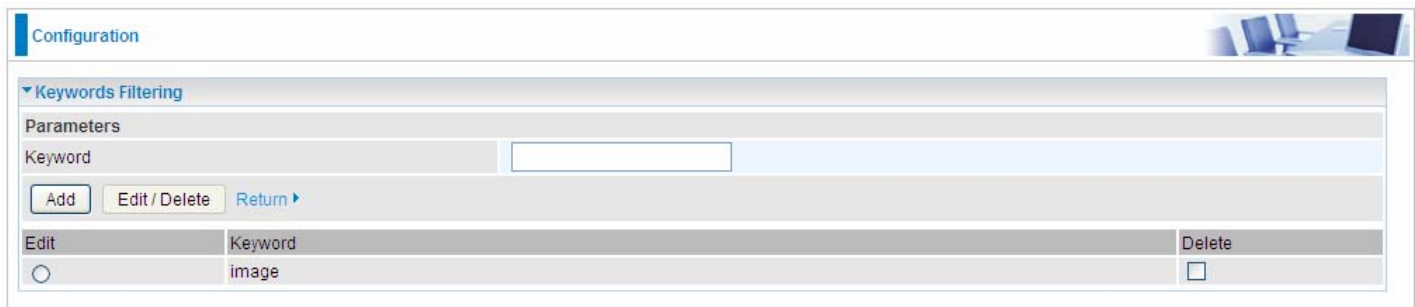
**Note:** Maximum number of entries: 32.

Click [Detail ▶](#) to add the keywords.



The screenshot shows the 'Configuration' window with the 'Keywords Filtering' section expanded. Under 'Parameters', there is a 'Keyword' text field and three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

Enter the Keyword, for example image, and then click **Add**.



The screenshot shows the 'Keywords Filtering' section with a list of keywords. The list has columns for 'Edit', 'Keyword', and 'Delete'. One entry is visible with the keyword 'image' and an unchecked 'Delete' checkbox.


Edit	Keyword	Delete
<input type="radio"/>	image	<input type="checkbox"/>

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.



The screenshot shows the 'Configuration' window with the 'Domains Filtering' section expanded. Under 'Parameters', there is a 'Domains Filtering' text field, a 'Type' dropdown menu set to 'Forbidden Domain', and three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

**Domain Filtering:** enter the domain you want this filter to apply.

**Type:** select the action this filter deals with the Domain.

- ❶ **Forbidden Domain:** The domain is forbidden access.
- ❷ **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.



The screenshot shows a web interface for configuration. At the top, there's a 'Configuration' tab. Below it, a section titled 'Except IP Address' is expanded. Under 'Parameters', there are two rows: 'IP Version' with a dropdown menu set to 'IPv4', and 'Internal IP Address' with two empty text input fields separated by a tilde '~'. At the bottom of this section are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

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.

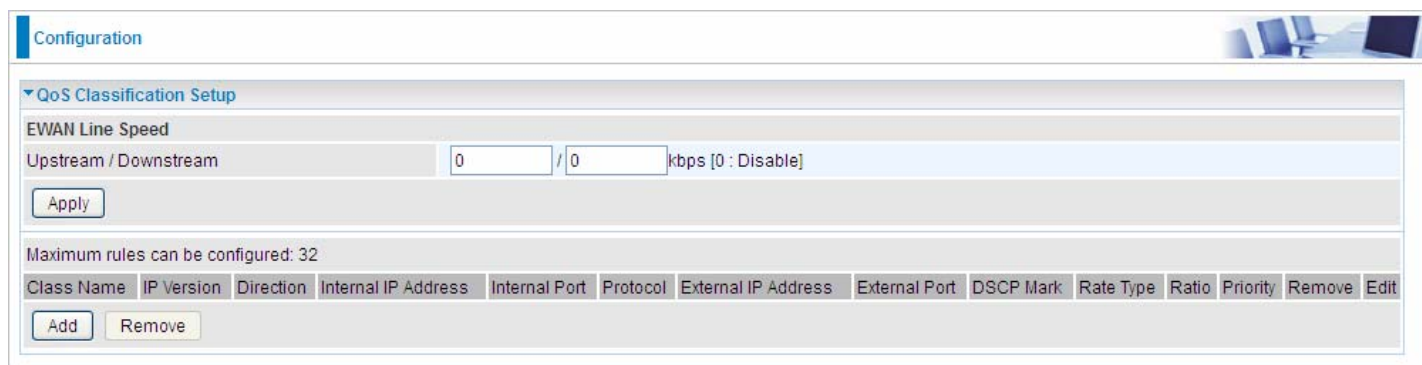
At the URL Filter page, press **Apply** to confirm your settings.



# QoS - 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.

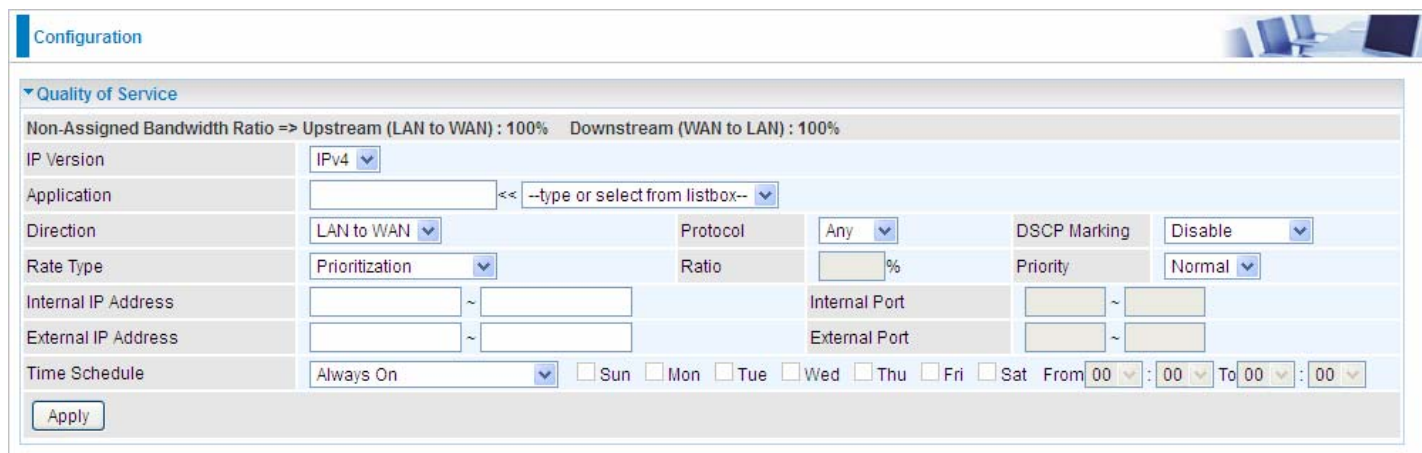


The screenshot shows the 'Configuration' page with the 'QoS Classification Setup' section expanded. It includes a 'EWAN Line Speed' section with 'Upstream / Downstream' rate inputs (both set to 0) and a unit dropdown set to 'kbps [0 : Disable]'. Below this is an 'Apply' button. A message states 'Maximum rules can be configured: 32'. At the bottom is a table header for QoS rules with columns: Class Name, IP Version, Direction, Internal IP Address, Internal Port, Protocol, External IP Address, External Port, DSCP Mark, Rate Type, Ratio, Priority, Remove, and Edit. There are 'Add' and 'Remove' buttons below the table.

## 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.



The screenshot shows the 'Configuration' page with the 'Quality of Service' section expanded. It displays 'Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%'. The configuration fields include: IP Version (IPv4), Application (empty), Direction (LAN to WAN), Protocol (Any), DSCP Marking (Disable), Rate Type (Prioritization), Ratio (empty), Priority (Normal), Internal IP Address (empty), Internal Port (empty), External IP Address (empty), External Port (empty), and Time Schedule (Always On). There are checkboxes for days of the week and a time range selector. An 'Apply' button is at the bottom.

**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.

- ① **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.
- ① **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** or **Prioritization**.

- ① **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.
- ① **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.

**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  $20\% \times 256 \times 0.9 = 46\text{kbps}$ . (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.

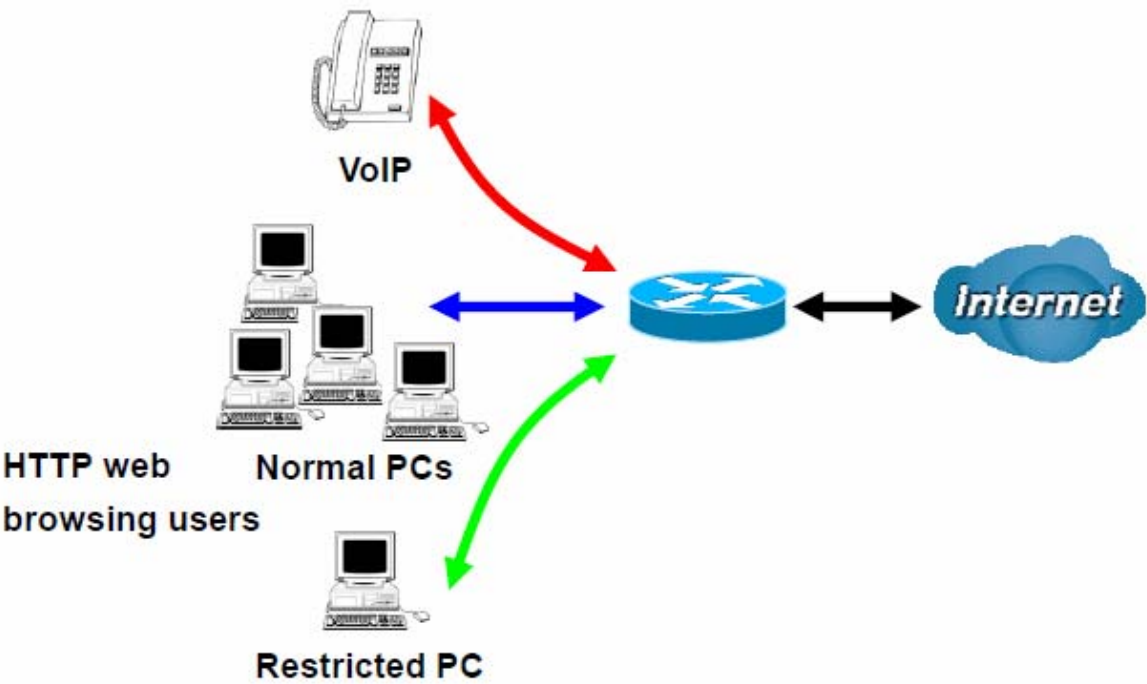
**External Port:** The Port number on the remote / WAN side.



**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 of Sun to 19:00 of 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](#).



**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	
Rate Type	Prioritization	Ratio	%	
Internal IP Address			DSCP Marking	EF(101110)
External IP Address			Priority	High
Time Schedule	timeslot1 <input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> 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	
Rate Type	Limited (Maximum)	Ratio	20 %	
Internal IP Address			DSCP Marking	Disable
External IP Address			Priority	Normal
Time Schedule	timeslot1 <input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> 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
Rate Type	Prioritization	Ratio	%
Internal IP Address	~		Internal Port
External IP Address	~		External Port
Time Schedule	timeslot1 <input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat    From 00 : 00 To 09 : 19		
<div>Apply</div>			

Other applications, like FTP, Mail access, users can use QoS to control based on need.



# 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.

## 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.

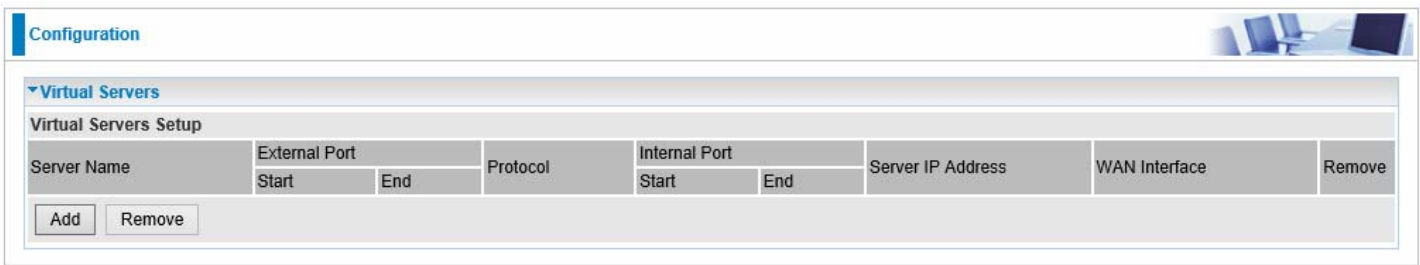
If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing 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.



It is virtual server listing table as you see, Click **Add** to move on.



The following configuration page will appear to let you configure.

Configuration

Virtual Servers

Parameters

Interface

pppoe\_0\_0\_35/ppp0.1

Server Name

Custom Service

Custom Service

Server IP Address

<< --type or select from listbox--

External Port

Start

End

Protocol

Internal Port

Start

End

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

TCP

Apply

Cancel

**Interface:** select from the drop-down menu the interface you want the virtual server(s) to apply.

**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**

- ① **Start:** Enter a port number as the external starting number for the range you want to give access to internal network.
- ① **End:** Enter a port number as the external ending number for the range you want to give access to internal network.

**Internal Port**

- ① **Start:** Enter a port number as the internal starting number.
- ① **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.



## 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.

Configuration

Virtual Servers

Parameters

Interface

pppoe\_0\_0\_35/ppp0.1

Server Name

Age of Empires

Custom Service

Server IP Address

192.168.1.10

<< 192.168.1.100

External Port

Start

End

Protocol

Internal Port

Start

End

47624	47624	TCP	47624	47624
6073	6073	TCP	6073	6073
2300	2400	TCP	2300	2400
2300	2400	UDP	2300	2400
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Apply

Cancel

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

Configuration

Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Remove
	Start	End		Start	End			
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.10	ppp0.1	<input type="checkbox"/>
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.10	ppp0.1	<input type="checkbox"/>
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.10	ppp0.1	<input type="checkbox"/>
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.10	ppp0.1	<input type="checkbox"/>

Add

Remove



## 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	Remove
	Start	End		Start	End			
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.10	ppp0.1	<input type="checkbox"/>
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.10	ppp0.1	<input type="checkbox"/>
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.10	ppp0.1	<input type="checkbox"/>
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.10	ppp0.1	<input checked="" type="checkbox"/>

Add

Remove

## ALG

The ALG Controls enable or disable protocols over application layer.

Configuration

ALG

Parameters

SIP

☒ Enable ☐ Disable

Apply

Cancel



## 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.

Application	Trigger		Open			WAN Interface	Remove
	Protocol	Port Range	Protocol	Port Range			
		Start End		Start	End		
<div>Add Remove</div>							

Click **Add** to add a port triggering rule.

Configuration

Port Triggering

Parameters

Interface:

Application:

Custom Application:

Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Apply

**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

① **Start:** Enter a port number as the triggering port starting number.

① **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

① **Start:** Enter a port number as the open port starting number.

① **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\_0\_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
		TCP			TCP

Apply

2. Press **Apply** to conform, and the items will be list in the **Virtual Servers Setup** table.

Configuration

Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove
	Protocol	Start	End	Protocol	Start	End		
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	<input type="checkbox"/>

Add Remove



**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**.

Advanced Setup

Port Triggering

Port Triggering Setup

Application	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		
Aim Talk	TCP	4099	4099	TCP	5191	5191	ppp0.1	<input type="checkbox"/>

Add

Remove



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

Time Schedule

Apply

Cancel

**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 of Sun to 19:00 of Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to “Disable”, the rule is disabled. See [Time Schedule](#).

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

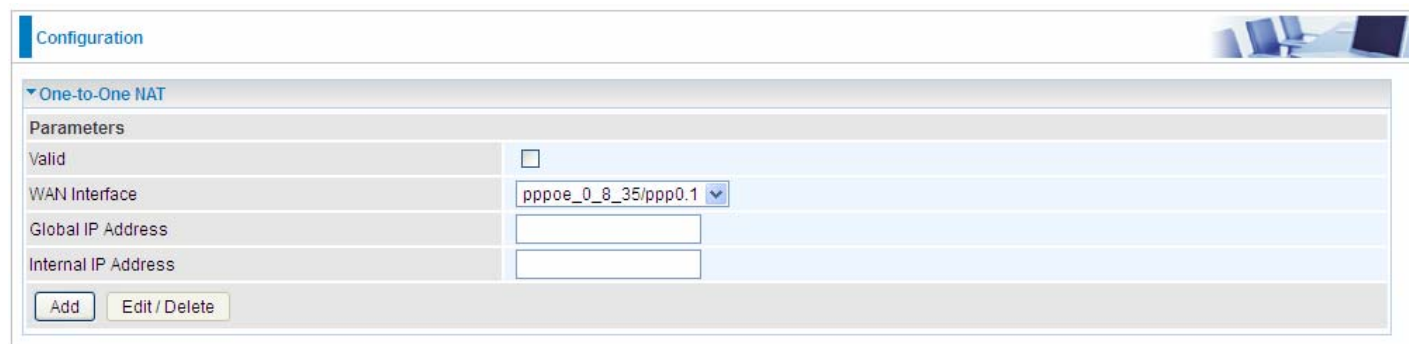
If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

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.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, a section titled 'One-to-One NAT' is expanded. Under this section, there is a 'Parameters' table. The table has four rows: 'Valid' with a checkbox, 'WAN Interface' with a dropdown menu showing 'pppoe\_0\_8\_35/ppp0.1', 'Global IP Address' with an empty text input field, and 'Internal IP Address' with an empty text input field. At the bottom of the table, there are two buttons: 'Add' and 'Edit / Delete'.

Parameters	
Valid	<input type="checkbox"/>
WAN Interface	pppoe_0_8_35/ppp0.1
Global IP Address	<input type="text"/>
Internal IP Address	<input type="text"/>

**Valid:** Check whether to validate 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.

**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.



# 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)

Add

Edit / Delete

- Host Label:** Enter identification for the host.
- Select:** Select MAC address of the computer that you want to wake up or turn on remotely.
- Add:** After selecting, click Add then you can perform the Wake-up action.
- Edit/Delete:** Click to edit or delete the selected MAC address.
- Ready:**
- “**Yes**” indicating the remote computer is ready for your waking up.
- “**No**” indicating the machine is not ready for your waking up.
- Delete:** Delete the selected MAC address.

Configuration

Wake On LAN

Parameters

Host Label

MAC Address

<< --select--

(type or select from listbox)

Add

Edit / Delete

Edit	Action	Host Label	MAC Address	Ready	Delete
<input type="radio"/>	<div>Wake Up</div>	billion-17bc6f1	18:A9:05:38:04:03	Yes	<input type="checkbox"/>



# Advanced Setup

There are sub-items within the System section: [Routing](#), [DNS](#), [Static ARP](#), [UPnP](#), [VPN \(7800NX and 7800X only\)](#), [Certificate](#), [Multicast](#), [Management](#), and [Diagnostics](#).

▸ Status
▸ Quick Start
▸ Configuration
▼ Advanced Setup
▸ Routing
▸ DNS
▸ Static ARP
▸ UPnP
▸ VPN
▸ Certificate
▸ Multicast
▸ Management
▸ Diagnostics

(7800NX)



# Routing

## Default Gateway

Advanced Setup

▼ 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

Apply

Cancel

**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
<div>Add Remove</div>					

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]
<div>Apply Cancel</div>	

**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	<input checked="" type="checkbox"/>

Add

Remove



## 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.

Advanced Setup

Policy Routing

Parameters

Policy Name	Source IP	LAN Port	WAN	Default Gateway	Remove
-------------	-----------	----------	-----	-----------------	--------

Add

Remove

Click **Add** to create a policy route.

Advanced Setup

Policy Routing

Parameters

Policy Name	<input type="text"/>
Physical LAN Port	<div><div></div><div></div></div>
Source IP	<input type="text"/>
Interface	<div>pppoe_0_0_35/ppp0.1<div></div></div>
Default Gateway	<input type="text"/>

Apply

Cancel

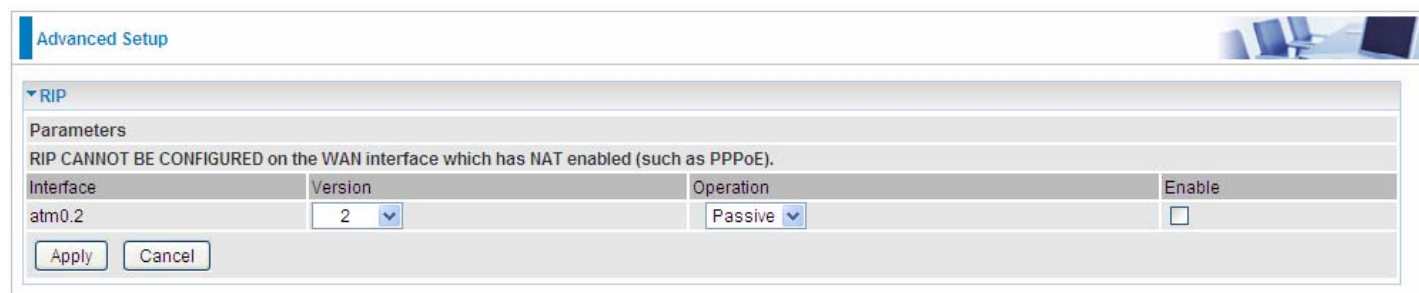
- Policy Name:** User-defined name.
- Physical LAN Port:** Select the LAN port.
- Source IP:** Enter the Host Source IP.
- Interface:** Select the WAN interface which you want the Source IP to access outside through.
- Default Gateway:** Enter the default gateway which you want the Source IP to access 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.



The screenshot shows the 'Advanced Setup' window for configuring RIP. It includes a warning message and a table for interface settings.

Advanced Setup

▼ RIP

Parameters

RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

Interface	Version	Operation	Enable
atm0.2	2	Passive	<input type="checkbox"/>

Apply Cancel

**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.

- ① **Passive:** only receive the routing information broadcasted by other routers and modifies its routing table according to the received information.
- ① **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 of Domain name to IP.

## DNS

IPv6 DNS Server's operation is similar to IPv4 DNS server. There are two modes to get DNS server address: Auto and Static mode.

Advanced Setup

▼ DNS

Parameters

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses 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 highest 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

ppp0.1

Available WAN Interfaces

→

←

☐ Use the following Static DNS IP address

Primary DNS server

Secondary DNS server

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\_0\_35/ppp0.1

☐ Use the following Static IPv6 DNS address

Primary IPv6 DNS server

Secondary IPv6 DNS server

Apply

Cancel

### 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

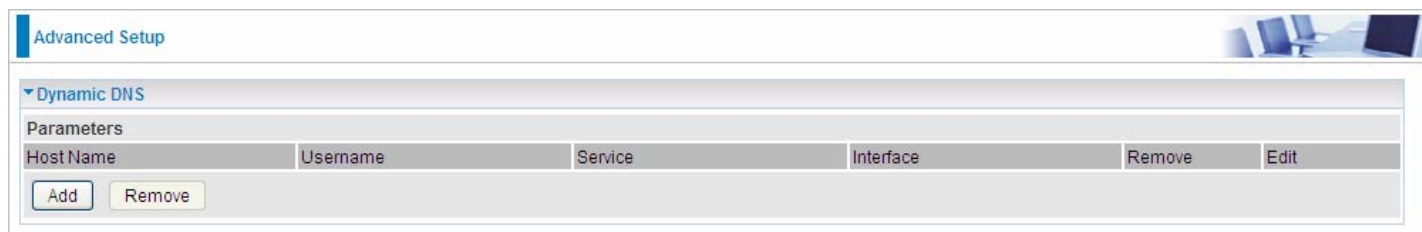
**Primary IPv6 DNS Server / Secondary IPv6 DNS Server:** type the specific primary and secondary IPv6 DNS Server address.



## 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).



Advanced Setup

Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
-----------	----------	---------	-----------	--------	------

Add Remove

Click **Add** to register a WAN interface with the exact DNS.



Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server: www.dyndns.org (custom)

Host Name:

Interface: pppoe\_0\_0\_35/ppp0.1

Username:

Password:

Apply

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.

**Interface:** Select the Interface that is bound to the registered Domain name.

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



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\_0\_35 with DDNS: [www.hometest.com](http://www.hometest.com) using username/password test/test

Advanced Setup

Dynamic DNS -- Add

Parameters

Dynamic DNS Server

www.dyndns.org (custom)

Host Name

www.hometest.com

Interface

pppoe\_0\_0\_35/ppp0.1

Username

test

Password

....

Apply

Advanced Setup

Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	<input type="checkbox"/>	Edit

Add

Remove

2. ipoe\_eth0 with DDNS: [www.hometest1.com](http://www.hometest1.com) using username/password test/test.

Advanced Setup

Dynamic DNS -- Add

Parameters

Dynamic DNS Server

www.dyndns.org (custom)

Host Name

www.hometest1.com

Interface

ipoe\_eth0/eth0.1

Username

test

Password

....

Apply

Advanced Setup

Dynamic DNS

Parameters

Host Name	Username	Service	Interface	Remove	Edit
www.hometest.com	test	dyndns-custom	ppp0.1	<input type="checkbox"/>	Edit
www.hometest1.com	test	dyndns-custom	eth0.1	<input type="checkbox"/>	Edit


Add

Remove



## 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.



Advanced Setup

▼ DNS Proxy

Parameters	
DNS Proxy	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Host name of the Broadband Router	<input type="text" value="home.gateway"/>
Domain name of the LAN network	<input type="text" value="home.gateway"/>

**DNS Proxy:** Select whether to enable or disable DNS Proxy function, default is enabled.

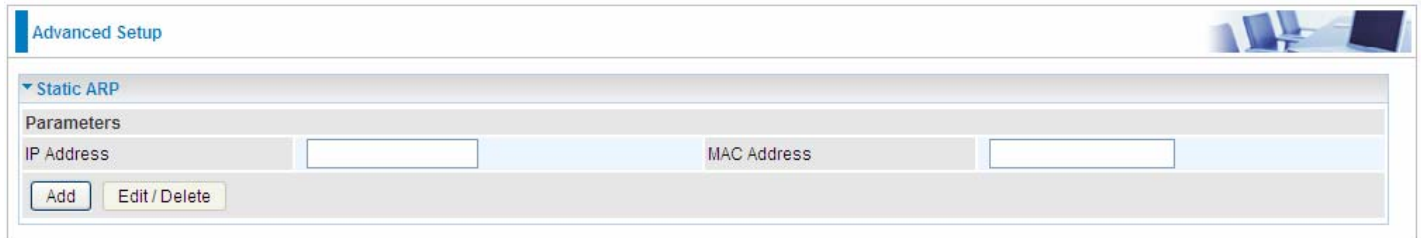
**Host name of the Broadband Router:** Enter the host name of the router. Default is home.gateway.

**Domain name of the LAN network:** Enter the domain name of the LAN network. home.gateway.



## Static 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.



The screenshot shows a web-based configuration interface for Static ARP. At the top, there is a tab labeled "Advanced Setup" with a small icon of a desk and chairs to its right. Below the tab is a section titled "Static ARP" with a dropdown arrow. Under this section, there is a "Parameters" label. Below the label, there are two input fields: "IP Address" and "MAC Address". The "IP Address" field is on the left and the "MAC Address" field is on the right. Below these fields are two buttons: "Add" and "Edit / Delete".

**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.

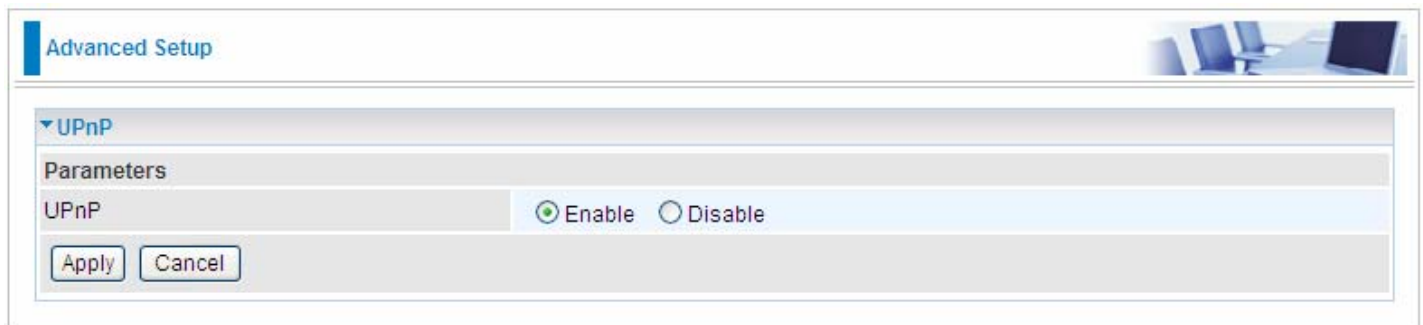
Click **Add** to confirm the settings.



## 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.



### UPnP:

- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

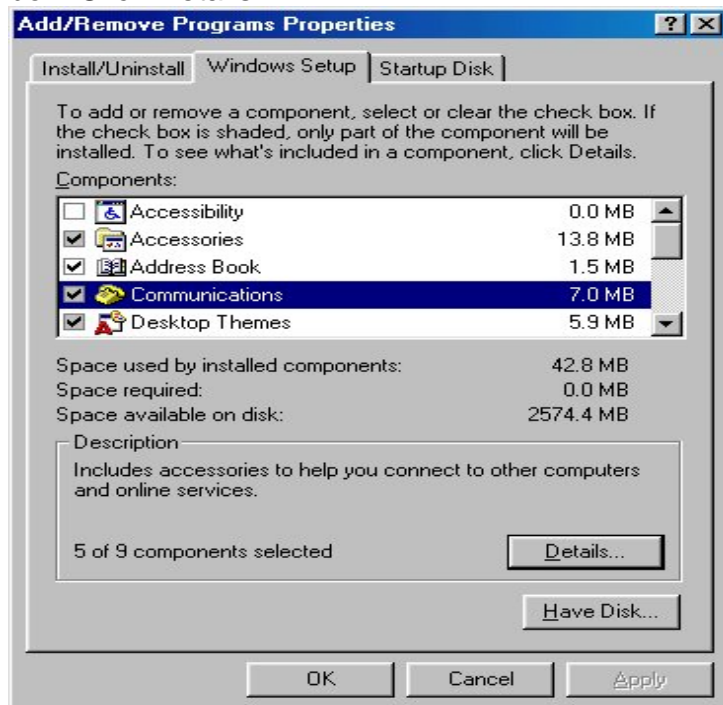


## Installing UPnP in Windows Example

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.



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



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



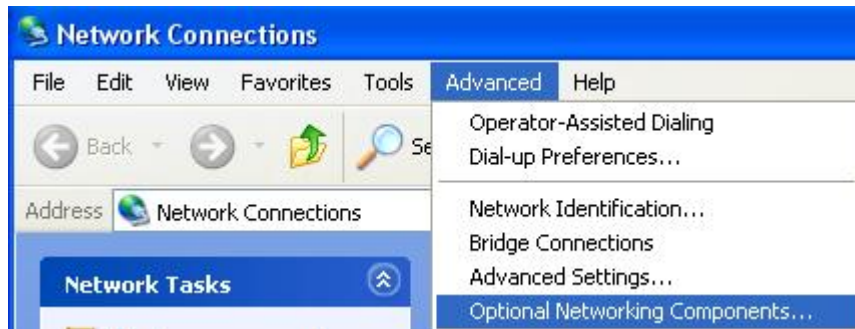
**Step 5:** Restart the computer when prompted.

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

**Step 1:** Click Start and Control Panel.

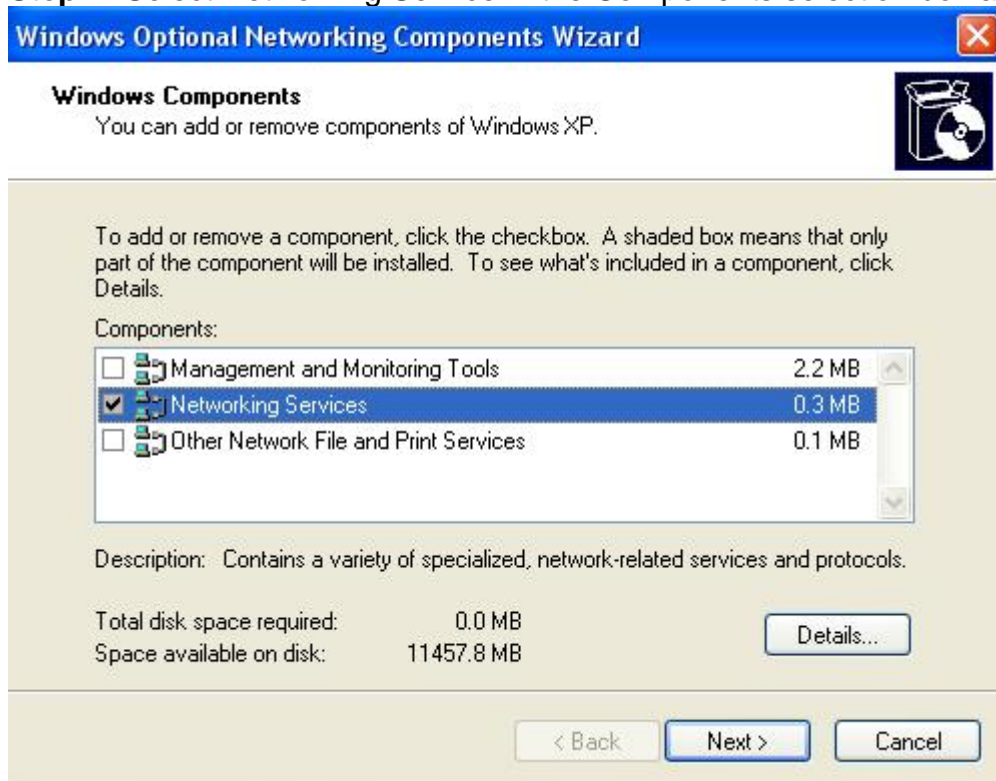
**Step 2:** Double-click Network Connections.

**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.

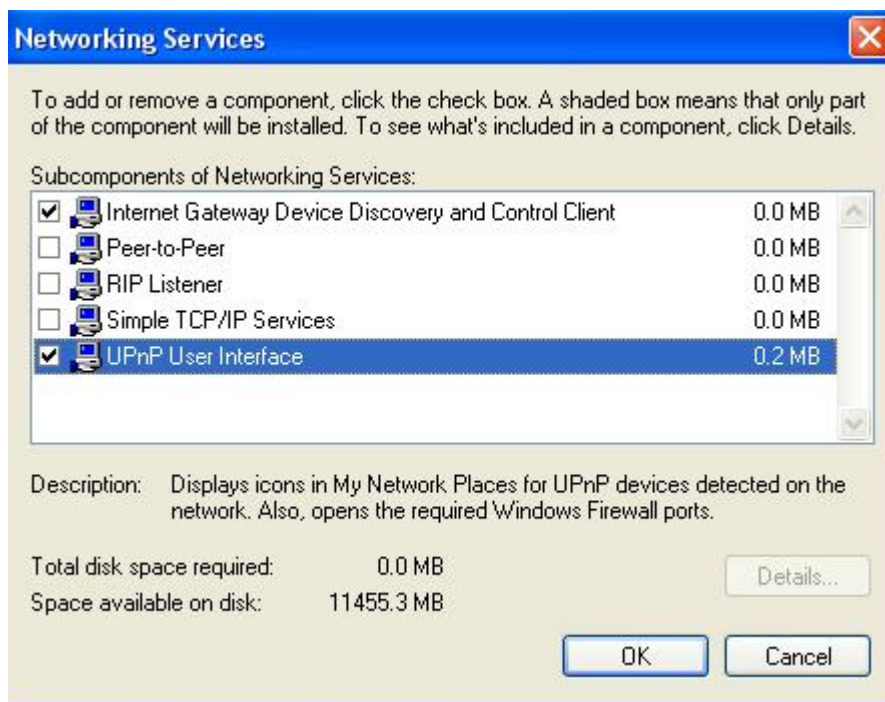
**Step 4:** Select Networking Service in the Components selection box and click Details.





**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**.



## 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.

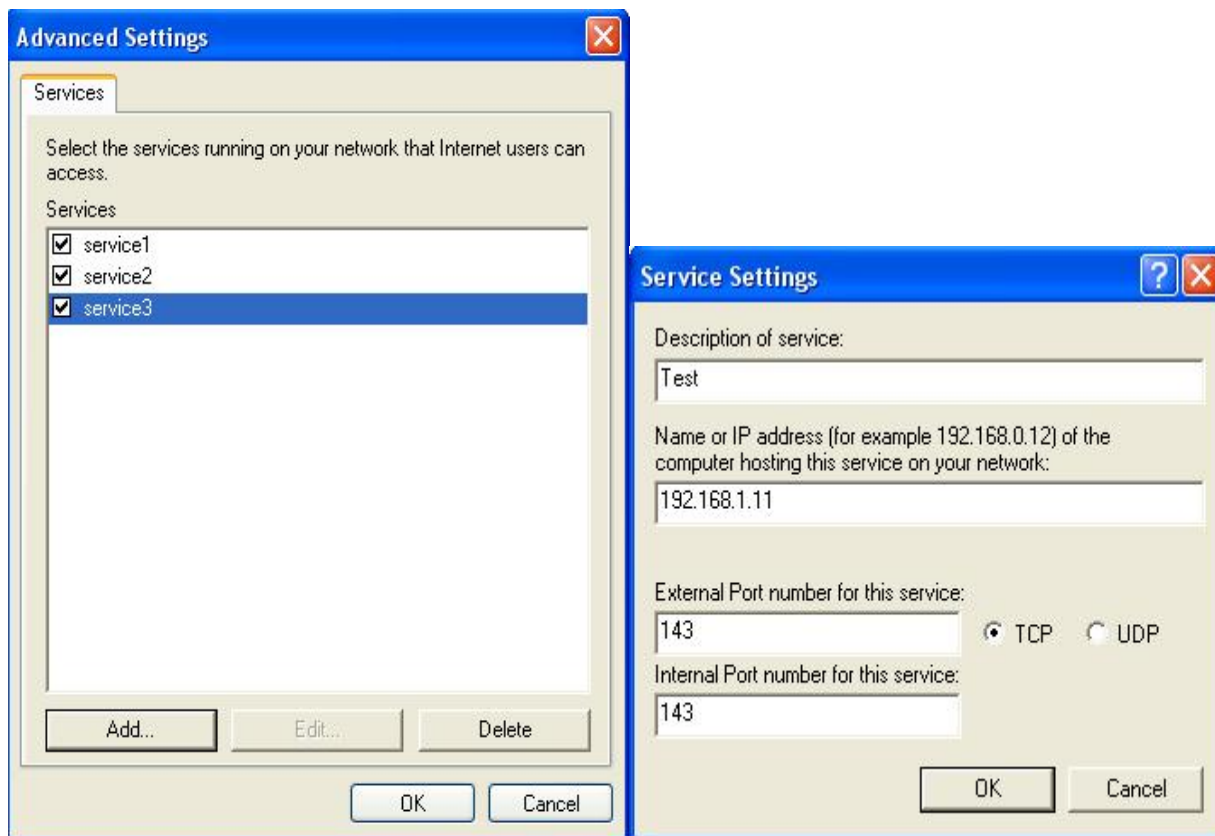




**Step 3:** In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.



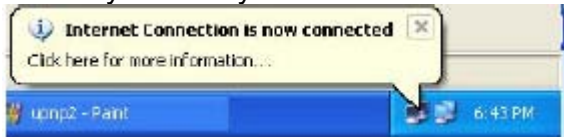
**Step 4:** You may edit or delete the port mappings or click Add to manually add port mappings.



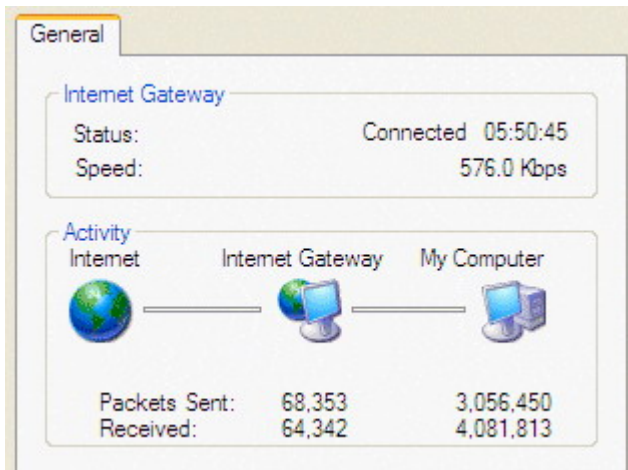
**Step 5:** Select Show icon in notification area when connected option and click OK. An icon displays



in the system tray



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





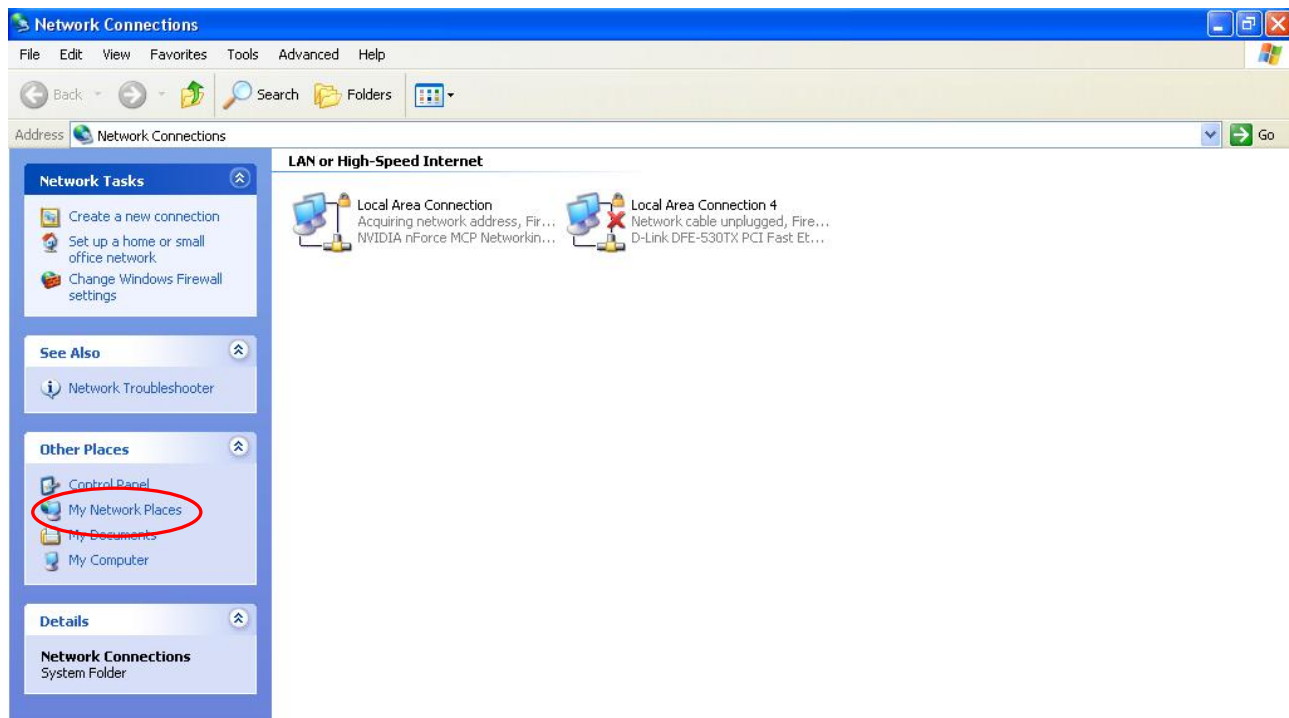
## Web Configurator Easy Access

With UPnP, you can access web-based configuration for the BiPAC 7800(N)X(L) 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 7800(N)X(L) and select Invoke. The web configuration login screen displays.

**Step 6:** Right-click on the icon of your BiPAC 7800(N)X(L) and select Properties. A properties window displays basic information about the BiPAC 7800(N)X(L).



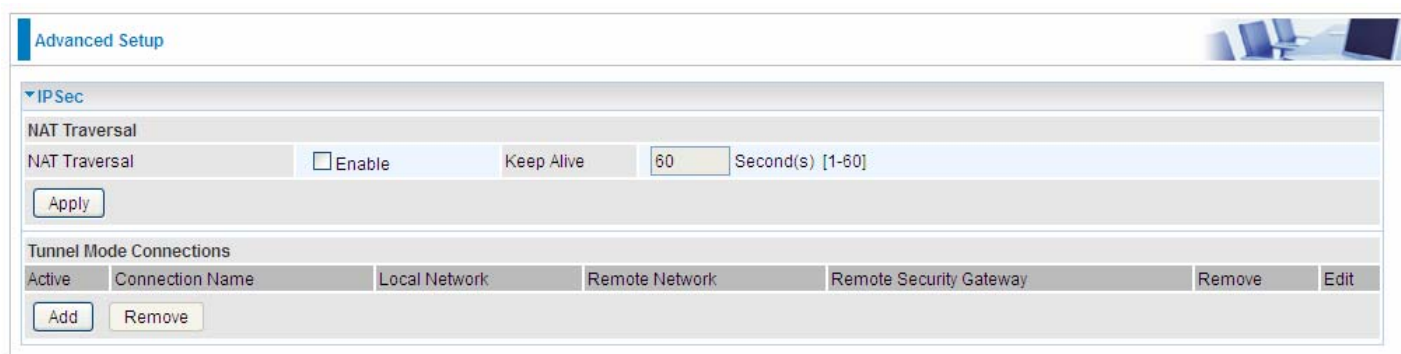
## VPN (7800(N)X only)

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*).



The screenshot shows the 'Advanced Setup' window for IPSec configuration. It includes a 'NAT Traversal' section with an 'Enable' checkbox, a 'Keep Alive' interval of 60 seconds, and an 'Apply' button. Below this is a 'Tunnel Mode Connections' table with columns for Active, Connection Name, Local Network, Remote Network, Remote Security Gateway, Remove, and Edit. There are 'Add' and 'Remove' buttons at the bottom of the table.

Active	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.

**Advanced Setup**

**IPsec**

**IPsec Settings**

Connection Name	<input type="text"/>	WAN Interface	Default	IP Version	IPv4
Local Network	Subnet	IP Address	<input type="text"/>	Netmask	<input type="text"/>
Remote Security Gateway	<input type="text"/>	<input type="checkbox"/> Anonymous			
Remote Network	Single Address	IP Address	<input type="text"/>	Netmask	<input type="text"/>
Key Exchange Method	IKE	IPsec Protocol	ESP		
Pre-Shared Key	<input type="text"/>				
Local ID Type	Default	ID Content	<input type="text"/>		
Remote ID Type	Default	ID Content	<input type="text"/>		

**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]	

**DPD Setting**

DPD Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Detection Interval	180	Second(s)	Idle Timeout	5	Consecutive times [5-99]

## IPsec Settings

**Connection Name:** A given name for the connection (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.

- ① **Single Address:** The IP address of the local host, for establishing an IPsec connection between a security gateway and a host (*network-to-host*).
- ① **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.

- ① **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.
- ① **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.

- ① **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56\*3) bits as an encryption method.
- ① **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.

- ① **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ① **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). There are 8 modes. 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). There are 8 modes. 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.

## **DPD Setting**

**DPD Function:** Check **Enable** to enable the function.

**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.

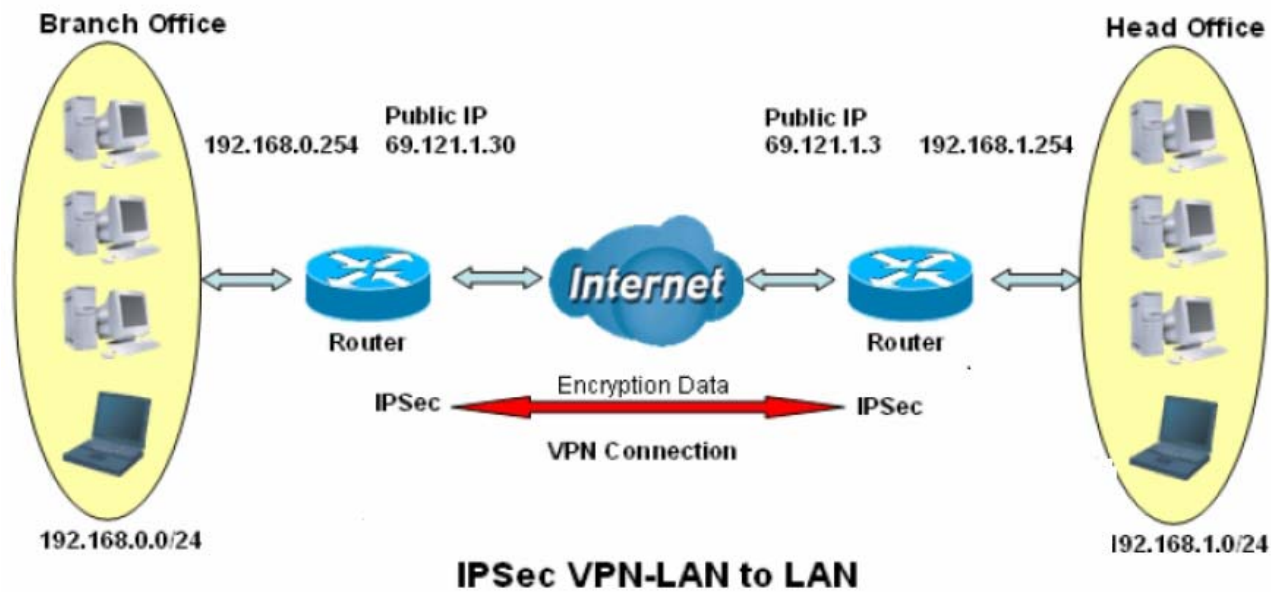


Examples (7800NX for example):

1. LAN-to-LAN connection

Two BiPAC 7800NXs want to setup a secure IPSec VPN tunnel

**Note:** The IPSec Settings shall be consistent between the two routers.



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

#### IPSec Settings

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	<input type="checkbox"/> 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	Integrity Algorithm	MD5
Encryption Algorithm	3DES	SA Lifetime	480 Minute(s) [60-1440]
DH Group	MODP1024(DH2)		

#### Phase 2

Encryption Algorithm	3DES	Integrity Algorithm	MD5
DH Group	None	IPSec Lifetime	60 Minute(s) [60-1440]

#### DPD Setting

DPD Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]



## 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		Branch Office network
	Subnet		
	IP Address	192.168.0.0	
	Netmask	255.255.255.0	
3	Remote Secure Gateway Address(Hostname)	69.121.1.3	IP address of the Head office router (on WAN side)
4	Remote Network		Head office network
	Subnet		
	IP Address	192.168.1.0	
	Netmask	255.255.255.0	
5	Proposal		Security Plan
	Method	ESP	
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	

Advanced Setup

IPsec

IPSec Settings

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]

DPD Setting

DPD Function

☐ Enable ☒ Disable

Detection Interval

180

Second(s) [180-86400]

Idle Timeout

5

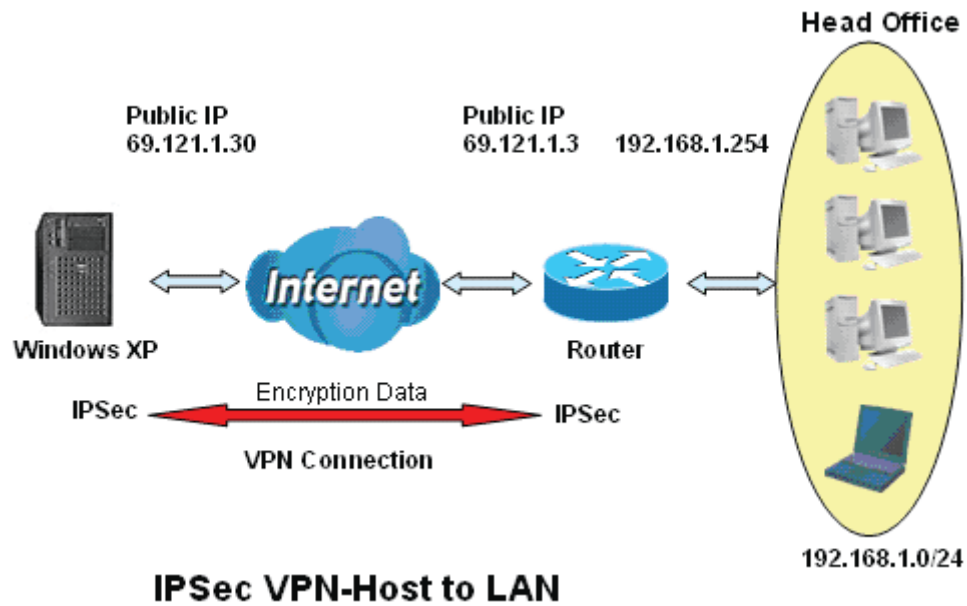
Consecutive times [5-99]

Apply



## 2. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



Item	Function		Description
1	Connection Name	Headoffice-to-Host	Give a name for IPSec connection
2	Local Network		Head Office network
	Subnet		
	IP Address	192.168.1.0	
	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		Host
	Single Address	69.121.1.30	
5	Proposal		Security Plan
	Method	ESP	
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	





### IPsec

#### IPSec Settings

Connection Name	B-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	<input type="checkbox"/> 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]

#### DPD Setting

DPD Function	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		
Detection Interval	180 Second(s) [180-86400]	Idle Timeout	5 Consecutive times [5-99]



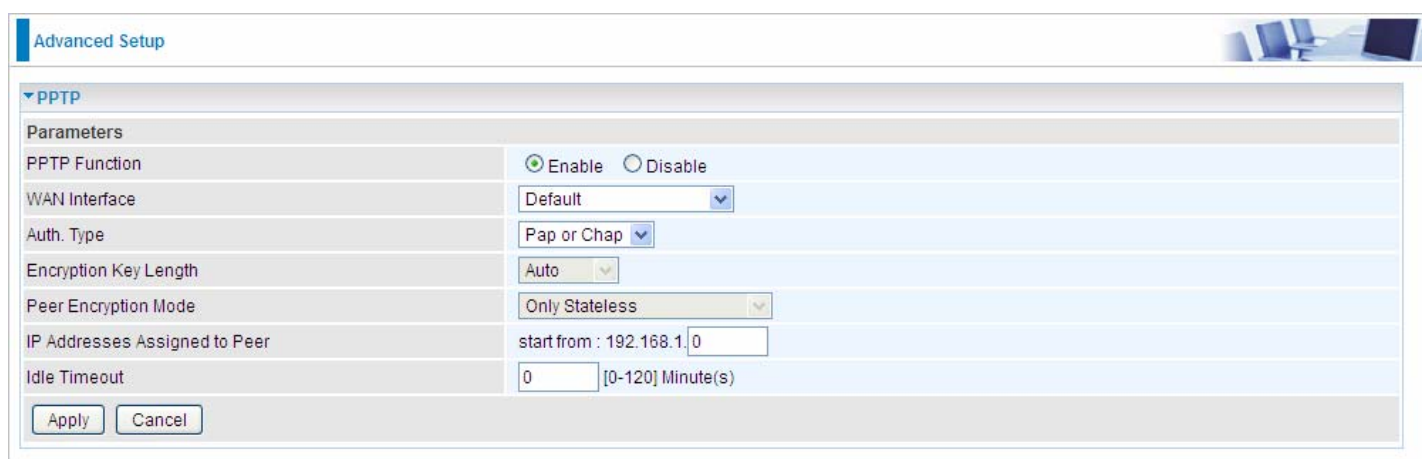
## PPTP

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.

In PPTP session, users can set the basic parameters(authentication, encryption, peer address, etc) for PPTP Server, and accounts in the next page of PPTP Account. They both constitutes the PPTP Server setting.



The screenshot shows the 'Advanced Setup' window for PPTP configuration. The 'PPTP' section is expanded, showing the following parameters:

Parameters	
PPTP Function	<input checked="" type="radio"/> Enable <input type="radio"/> 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)

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

**PPTP Function:** 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 "Stateful" or "Allow Stateless and Stateful" mode. The key will be changed every 256 packets when you select Stateful 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.

Click **Apply** to submit your PPTP Server basic settings.



## PPTP Account



The screenshot shows a web-based configuration interface for PPTP accounts. At the top, there is a tab labeled "Advanced Setup" and a small icon of a computer desk. Below this is a section titled "PPTP Account" with a dropdown arrow. Underneath is a "Parameters" section containing several input fields and controls:

Parameters	
Name	<input type="text"/>
Username	<input type="text"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN
Peer Network IP	<input type="text"/>
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Password	<input type="password"/>
Peer Netmask	<input type="text"/>

At the bottom of the parameters section are two buttons: "Add" and "Edit / Delete".

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

**Tunnel:** Select **Enable** to activate the account. PPTP 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.

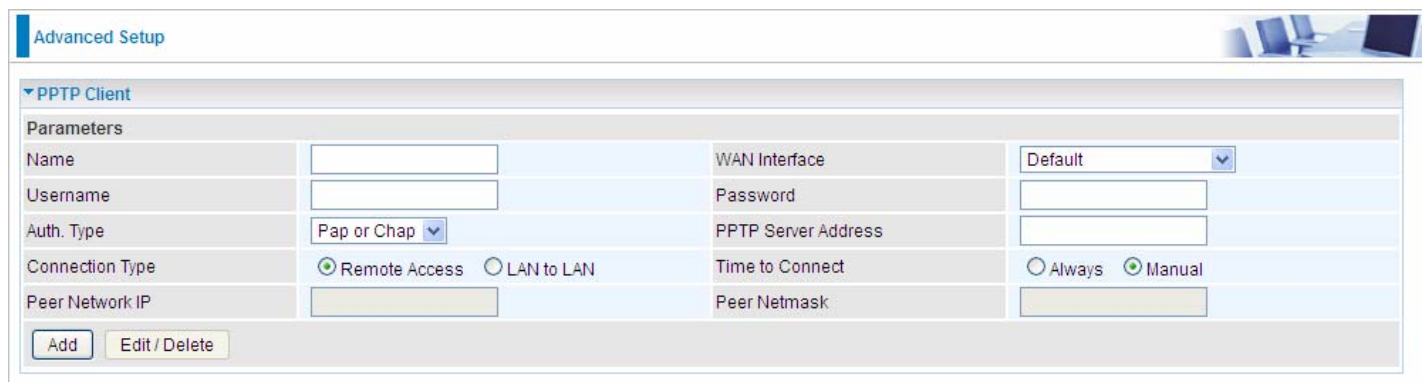
**Peer Network IP:** Please input the subnet IP for remote network.

**Peer Netmask:** Please input the Netmask for remote network.



## PPTP Client

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet.



The screenshot shows the 'Advanced Setup' page with the 'PPTP Client' section expanded. It contains a 'Parameters' table with the following fields:

Parameters	
Name	<input type="text"/>
Username	<input type="text"/>
Auth. Type	Pap or Chap <input type="button" value="v"/>
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN
Peer Network IP	<input type="text"/>
WAN Interface	Default <input type="button" value="v"/>
Password	<input type="password"/>
PPTP Server Address	<input type="text"/>
Time to Connect	<input type="radio"/> Always <input checked="" type="radio"/> Manual
Peer Netmask	<input type="text"/>

At the bottom of the form are two buttons: 'Add' and 'Edit / Delete'.

**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.

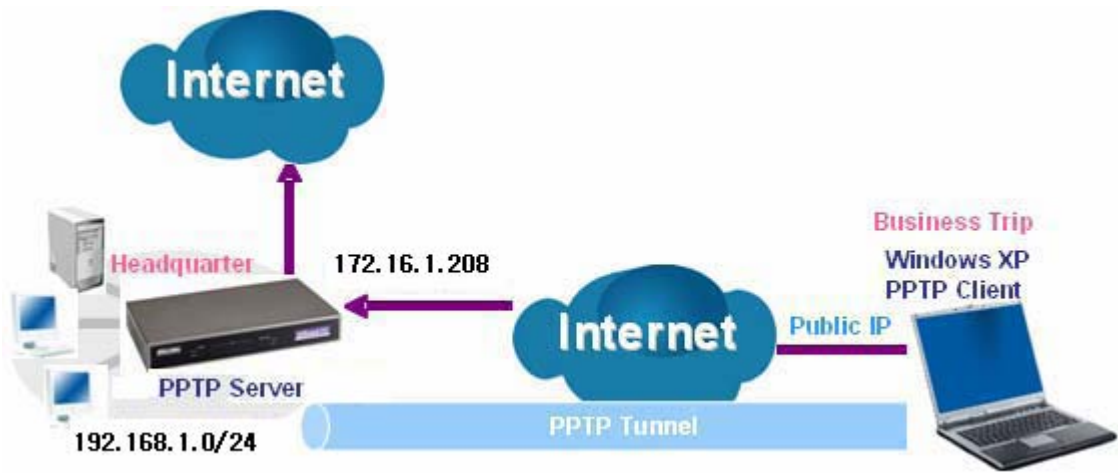
**Peer Network IP:** Please input the subnet IP for Server peer.

**Peer Netmask:** Please input the Netmask for server peer.

Click **Edit/Delete** 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**.

Advanced Setup

▼ PPTP

Parameters

PPTP Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.100
Idle Timeout	10 [0-120] Minute(s)

Apply Cancel

2: Create a PPTP Account “test”.

Advanced Setup

▼ PPTP Account

Parameters

Name	test	Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test	Password	.....
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN		
Peer Network IP		Peer Netmask	

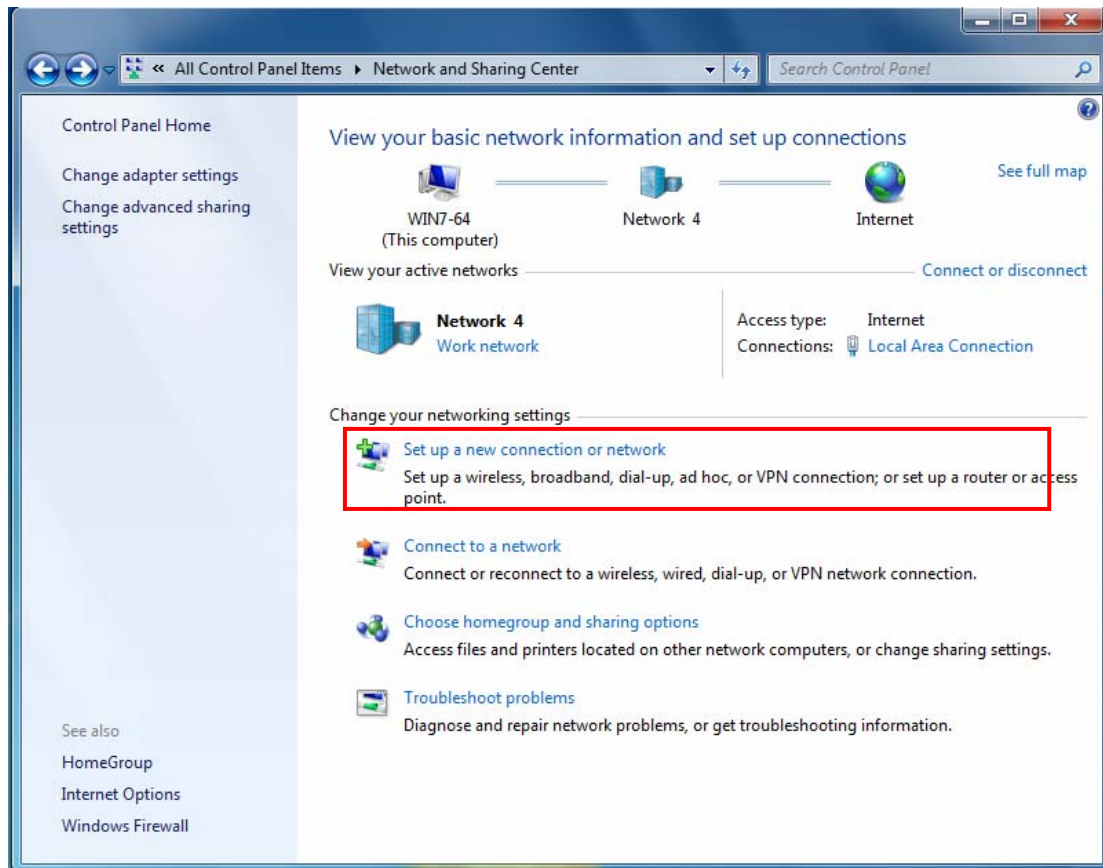
Add Edit / Delete

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input checked="" type="radio"/>	test	Enable	Remote Access			<input type="checkbox"/>



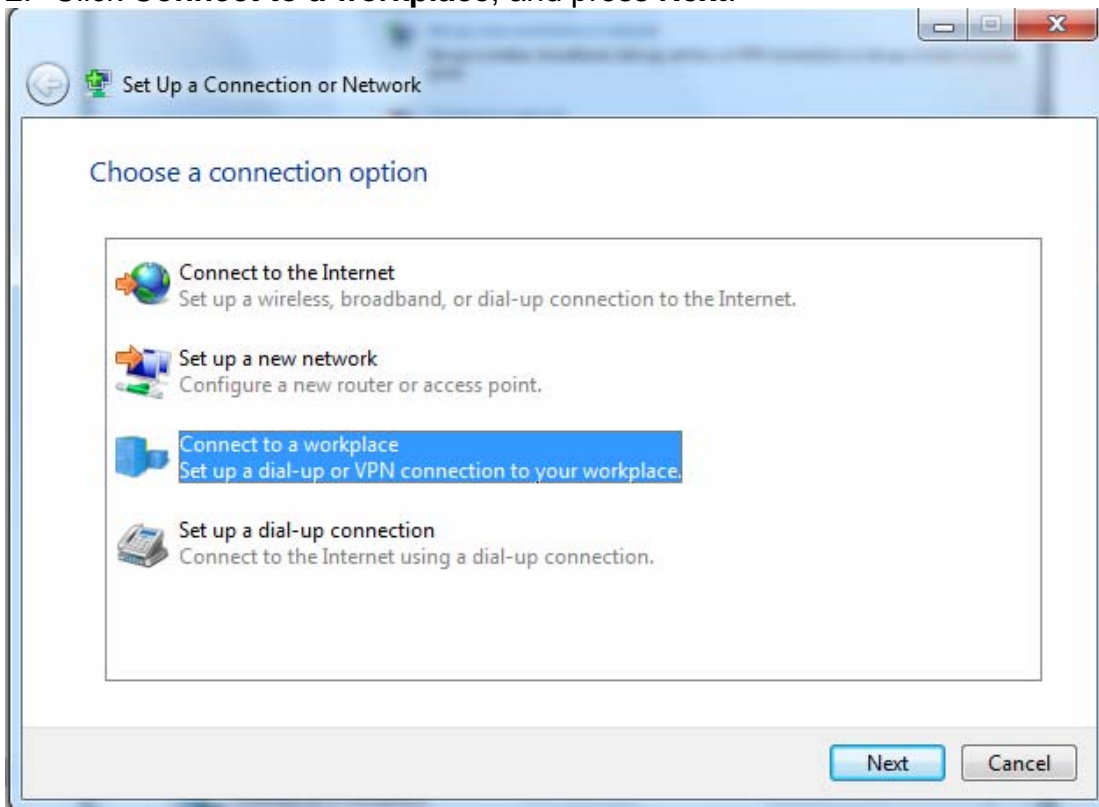
## Client Side:

1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection network**.





2. Click **Connect to a workplace**, and press **Next**.



3. Select **Use my Internet connection (VPN)** and press **Next**.





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

Next Cancel

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

Next Cancel



5. Input the account (**user name** and **password**) and press **Create**.

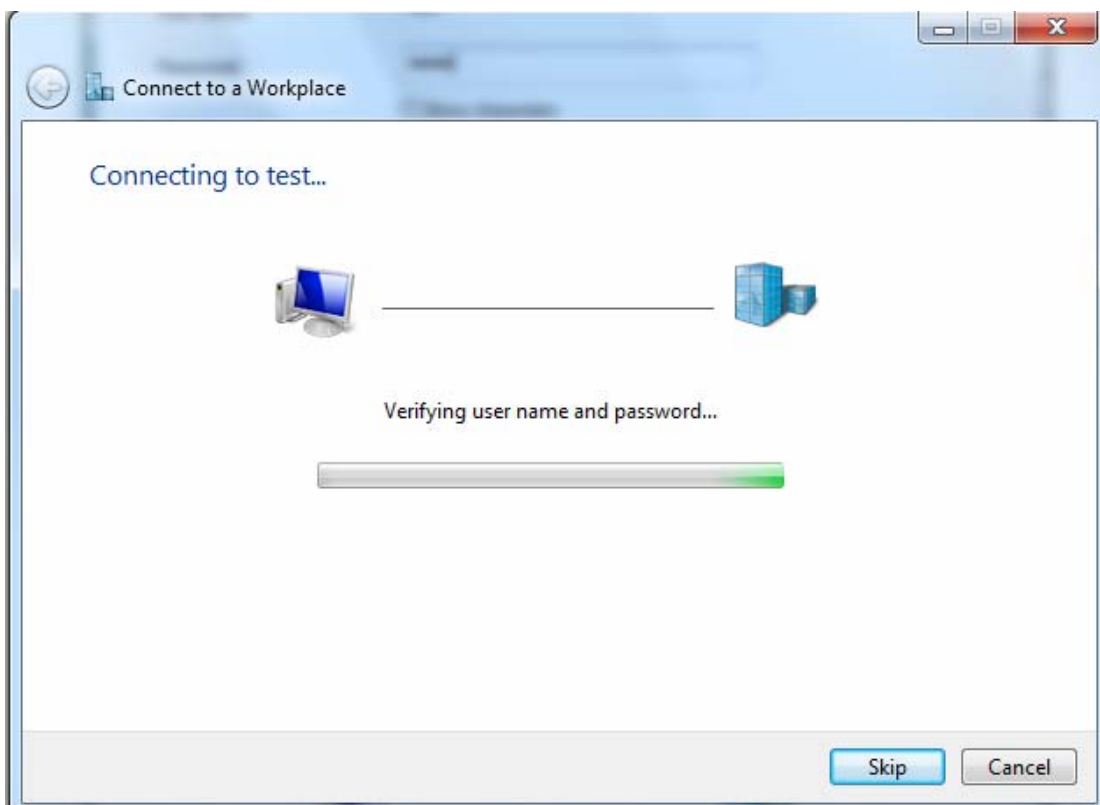
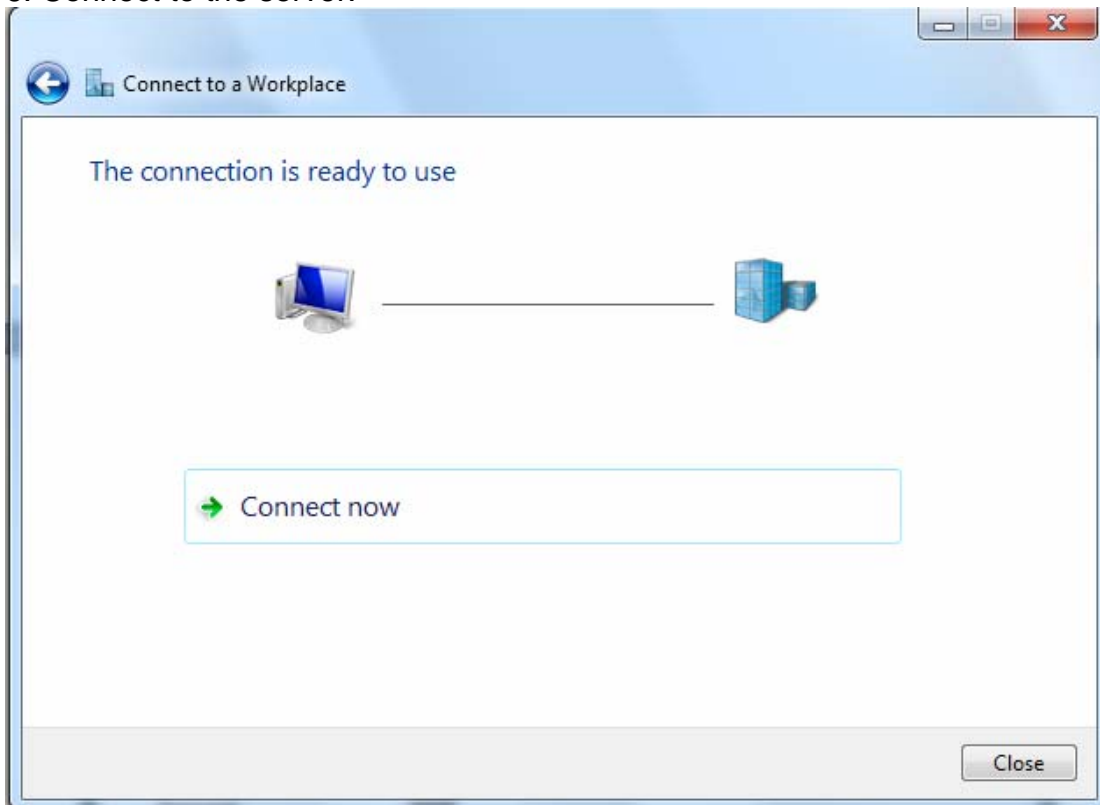
The image displays two sequential screenshots of a 'Connect to a Workplace' dialog box. The dialog box has a title bar with a back arrow icon and the text 'Connect to a Workplace'. The main content area is titled 'Type your user name and password'. It contains three input fields: 'User name:', 'Password:', and 'Domain (optional):'. The 'Password:' field has two checkboxes below it: 'Show characters' and 'Remember this password'. At the bottom right, there are 'Create' and 'Cancel' buttons.

**Top Screenshot:** The 'User name:' field is empty. The 'Password:' field is empty. The 'Domain (optional):' field is empty. The 'Show characters' and 'Remember this password' checkboxes are unchecked.

**Bottom Screenshot:** The 'User name:' field contains the text 'test'. The 'Password:' field contains masked characters '....'. The 'Domain (optional):' field is empty. The 'Show characters' and 'Remember this password' checkboxes are unchecked.

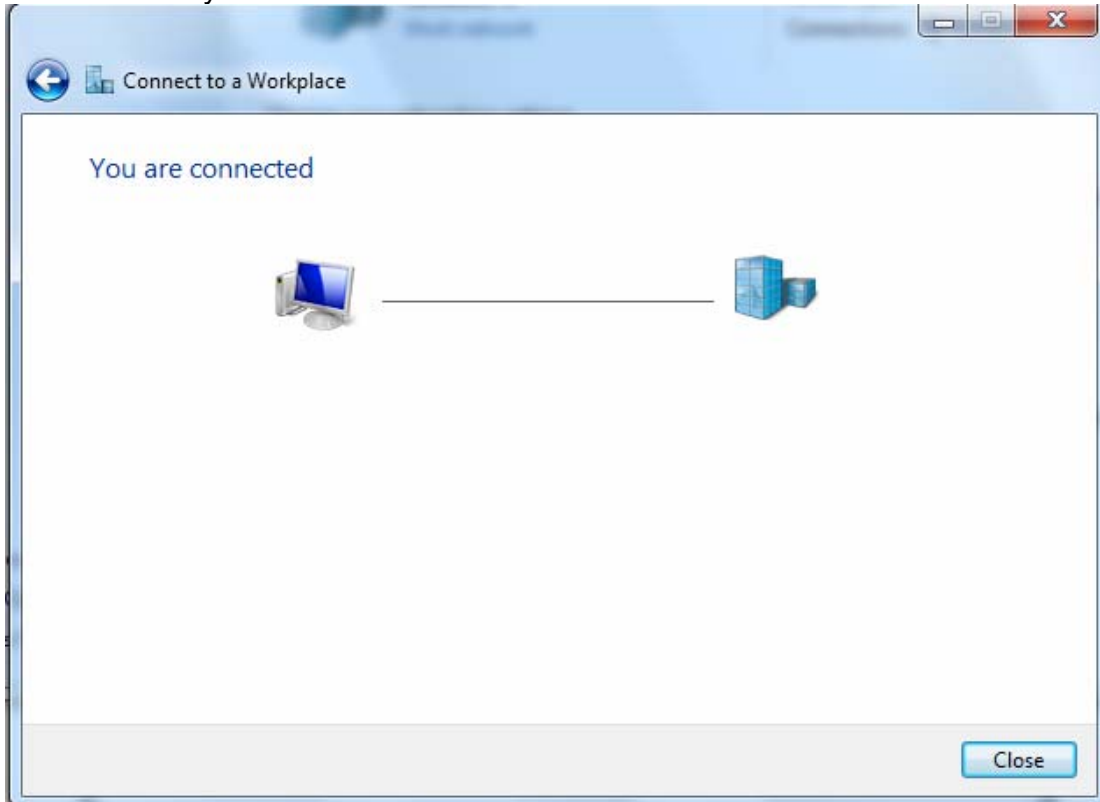


6. Connect to the server.





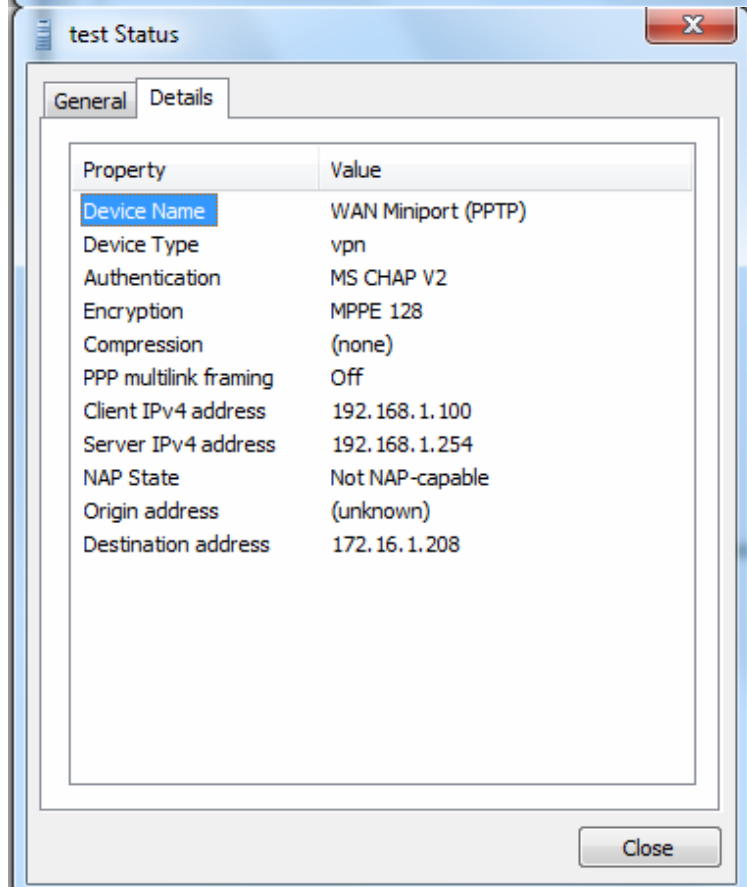
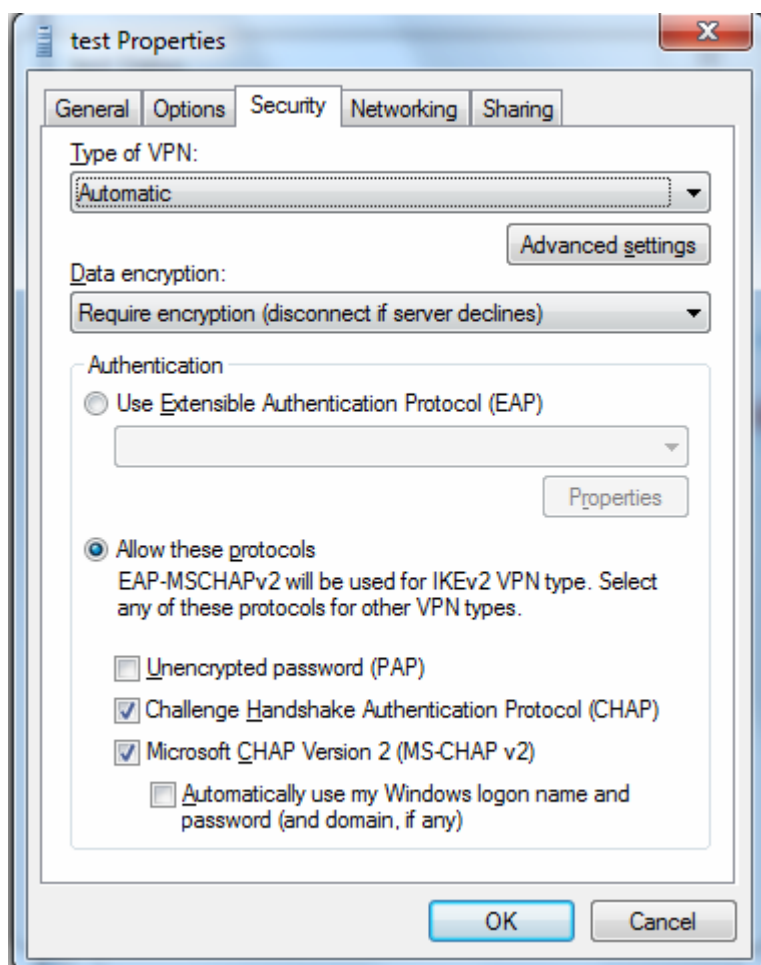
7. Successfully connected.



**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)



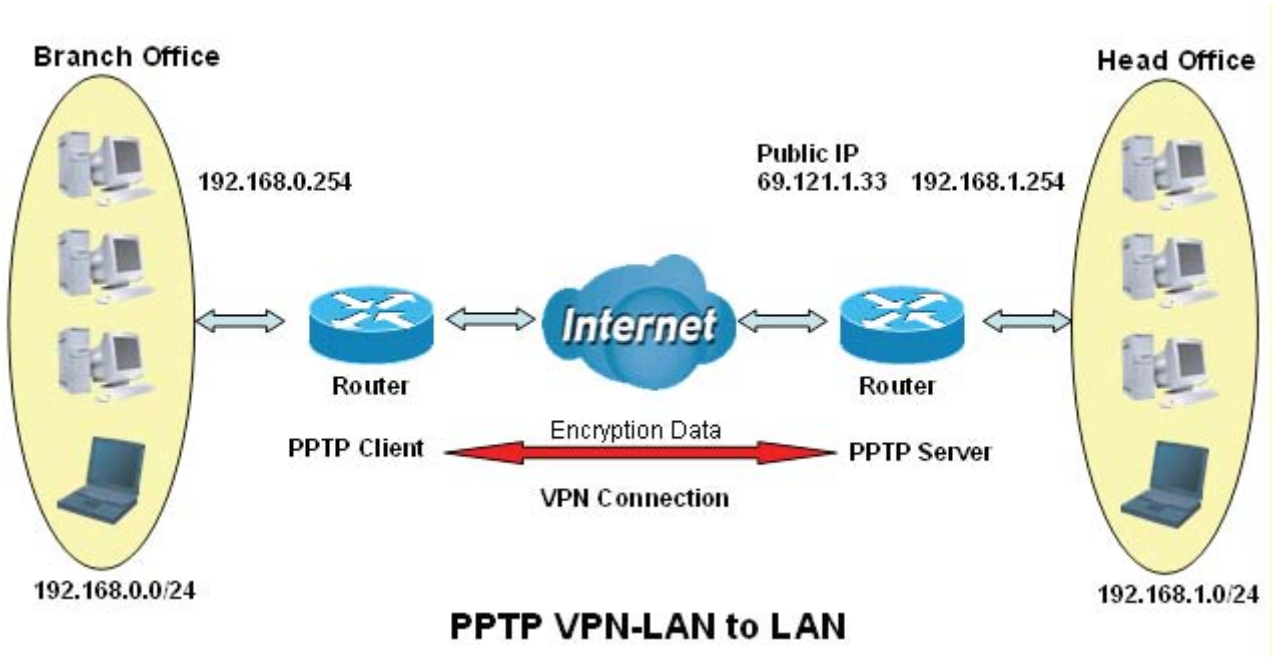






Example: Configuring a LAN-to-LAN PPTP VPN Connection

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

Advanced Setup

▼ PPTP

Parameters

PPTP Function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
WAN Interface	Default
Auth. Type	MS-CHAPv2
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	start from : 192.168.1.100
Idle Timeout	10 [0-120] Minute(s)

Apply Cancel

The above is the commonly 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 account the PPTP Account.

Advanced Setup

▼ PPTP Account

Parameters

Name	HO	Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test	Password	....
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> 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
<input type="radio"/>	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>



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.

Advanced Setup

PPTP Client

Parameters

Name	BO	WAN Interface	Default
Username	test	Password	••••
Auth. Type	MS-CHAPv2	PPTP Server Address	69.121.1.3
Connection Type	<input type="radio"/> Remote Access <input checked="" type="radio"/> LAN to LAN		Time to Connect <input type="radio"/> Always <input checked="" type="radio"/> Manual
Peer Network IP	192.168.1.0	Peer Netmask	255.255.255.0

Add

Edit / Delete

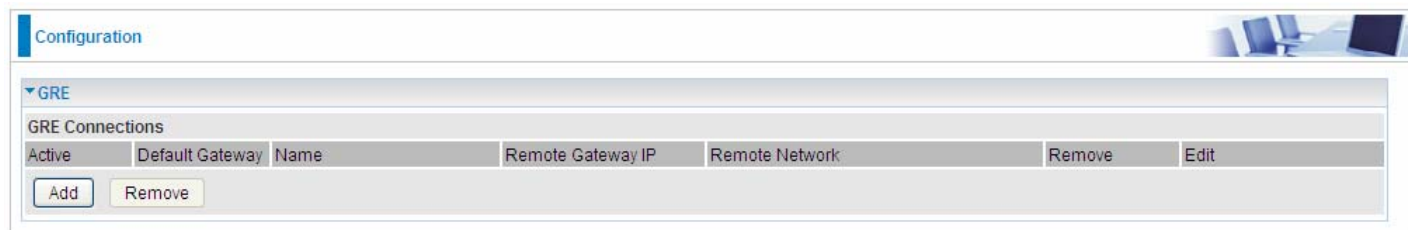
Edit	Enable	Default Gateway	Name	Time to Connect	PPTP Server Address	Connection Type	Peer Network IP	Peer Netmask	Delete
<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>	BO	Manual	69.121.1.3	LAN to LAN	192.168.1.0	255.255.255.0	<input type="checkbox"/>

**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.



The screenshot shows the 'Configuration' page with a 'GRE' section. It features a table titled 'GRE Connections' with columns: 'Active', 'Default Gateway', 'Name', 'Remote Gateway IP', 'Remote Network', 'Remove', and 'Edit'. Below the table are 'Add' and 'Remove' buttons.

Active	Default Gateway	Name	Remote Gateway IP	Remote Network	Remove	Edit
--------	-----------------	------	-------------------	----------------	--------	------

Click **Add** to set up new GRE tunnels.



The screenshot shows the 'Configuration' page with a 'GRE' section. It features a 'Parameters' form with fields for 'Name', 'WAN Interface' (set to 'Default'), 'Remote Gateway IP', 'Remote Network' (set to 'Single Address'), and 'IP Address'. An 'Apply' button is at the bottom.

**Parameters**

Name:

WAN Interface:

Remote Gateway IP:

Remote Network:

IP Address:

**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.

**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.



# 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

Advanced Setup

Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 4

Name	Subject	Type	Action
<div>Import Certificate</div>			



**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.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name

Certificate

-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----

Apply

Enter the certificate name and insert the certificate.

Advanced Setup

Trusted CA -- Import CA certificate

Parameters

Name

acscert

Certificate

-----BEGIN CERTIFICATE-----  
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQGEwJD  
TjEXMBUGA1UEChMQQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc  
NMjAw  
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBGGA1UEChMRQ0ZDQSBPcGV  
yYXRp  
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN  
ZuTJD  
rSwXGjaexPnBis5zNJc70SPQYgVhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/  
Uu9be  
pUJBenxvYRgTIImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73  
/se+H  
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVROfBEEwPzA9oDu  
gOaQ3  
MDUxCzAJBgNVBAYTAkNOMRcwFQYDVQQKEw5DRkNBIFBvbGljeSBBDQITENMA  
GA1UE  
AxMEQ1JMTALBgNVHQ8EBAMCAQYwHwYDVROjBBgwFoAUL5Jufe7tBb/wveS  
FaAqX  
k1NC0tAwHQYDVRO0BBYEFMMnxjZoyCd1JIevkadLJjMC5RrpMAwGA1UdEwQ

Apply



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	<div>ViewRemove</div>

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.

Advanced Setup

IGMP

Parameters

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	<input checked="" type="checkbox"/> Enable	
LAN to LAN (Intra LAN) Multicast	<input type="checkbox"/> Enable	
Mebership Join Immediate (IPTV)	<input type="checkbox"/>	

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	<input checked="" type="checkbox"/> Enable	
LAN to LAN (Intra LAN) Multicast	<input checked="" type="checkbox"/> Enable	

Apply

Cancel

## IGMP

**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

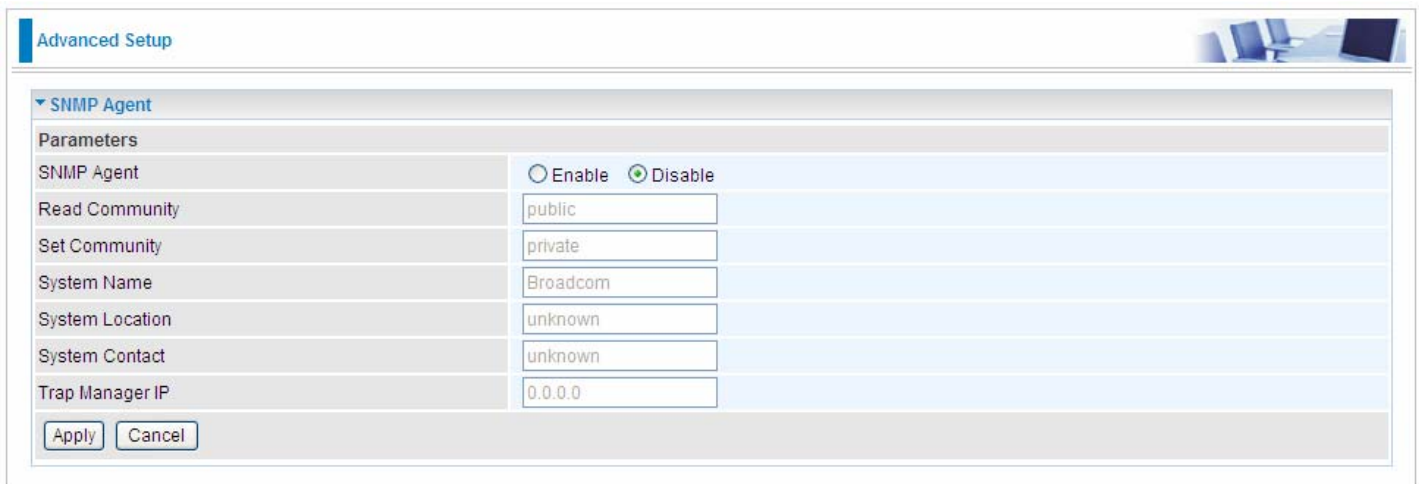
## SNMP Agent

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.



The screenshot shows a web interface titled "Advanced Setup" with a sub-section for "SNMP Agent". Under "Parameters", there are several configuration fields:

Parameters	
SNMP Agent	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Read Community	<input type="text" value="public"/>
Set Community	<input type="text" value="private"/>
System Name	<input type="text" value="Broadcom"/>
System Location	<input type="text" value="unknown"/>
System Contact	<input type="text" value="unknown"/>
Trap Manager IP	<input type="text" value="0.0.0.0"/>

At the bottom of the configuration area are two buttons: "Apply" and "Cancel".

**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.

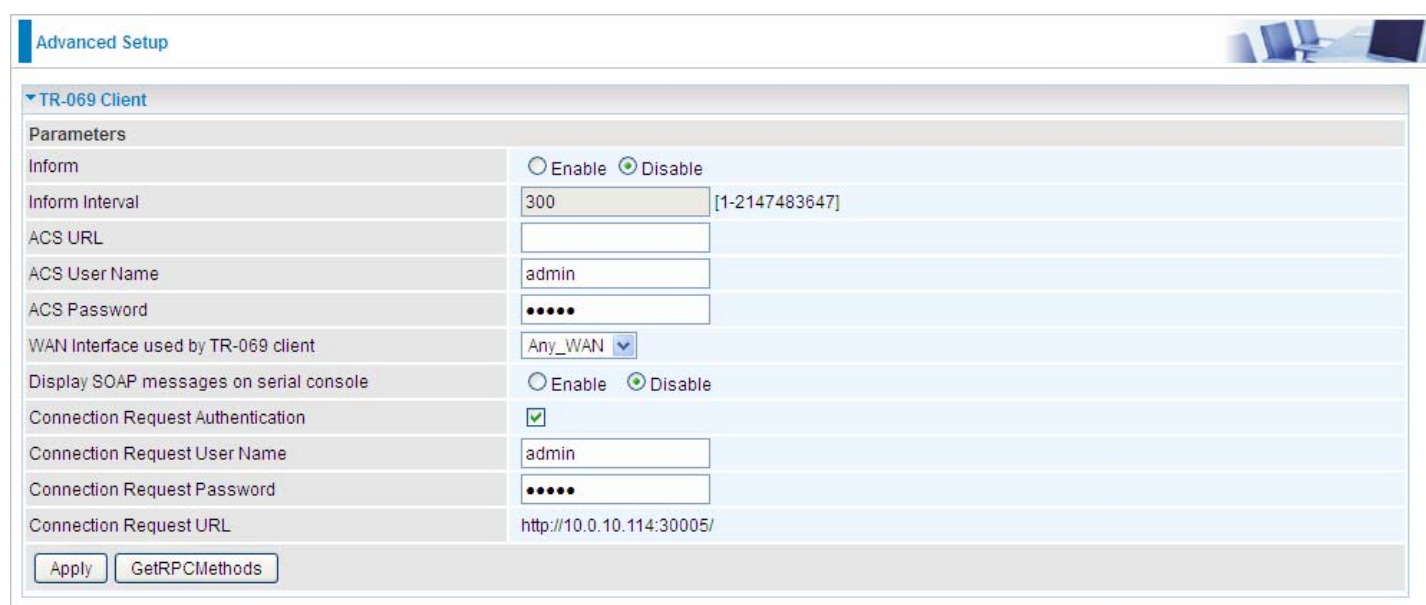
**Trap manager IP:** enter the IP address of the server receiving the trap sent by SNMP agent.



## 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.



The screenshot shows a web-based configuration interface titled "Advanced Setup". Under the "TR-069 Client" section, there is a "Parameters" table. The "Inform" parameter has radio buttons for "Enable" and "Disable", with "Disable" selected. The "Inform Interval" is set to 300, with a range of [1-2147483647] shown. The "ACS URL" is empty. The "ACS User Name" is "admin". The "ACS Password" is masked with dots. The "WAN Interface used by TR-069 client" is set to "Any\_WAN" via a dropdown. The "Display SOAP messages on serial console" has radio buttons for "Enable" and "Disable", with "Disable" selected. The "Connection Request Authentication" is checked. The "Connection Request User Name" is "admin". The "Connection Request Password" is masked with dots. The "Connection Request URL" is "http://10.0.10.114:30005/". At the bottom, there are "Apply" and "GetRPCMethods" buttons.

Parameters	
Inform	<input type="radio"/> Enable <input checked="" type="radio"/> 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	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connection Request Authentication	<input checked="" type="checkbox"/>
Connection Request User Name	admin
Connection Request Password	.....
Connection Request URL	http://10.0.10.114:30005/

Apply GetRPCMethods

**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.



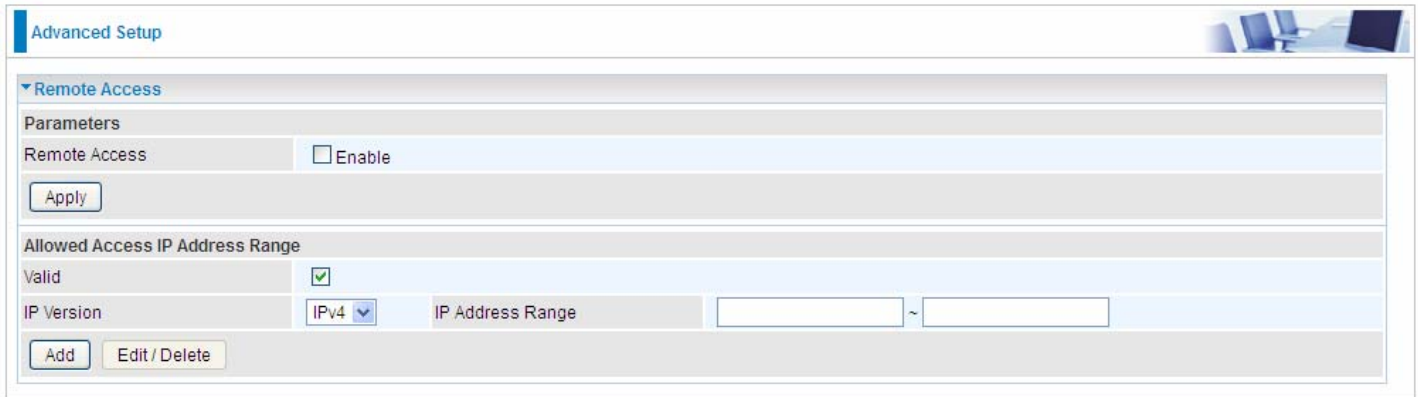
**GetRPCMethods:** Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.



## Remote Access

It is to allow remote access to the router to view or configure.



The screenshot shows the 'Advanced Setup' page with the 'Remote Access' section expanded. Under 'Parameters', there is a 'Remote Access' checkbox labeled 'Enable' which is currently unchecked. Below this is an 'Apply' button. The 'Allowed Access IP Address Range' section contains a 'Valid' checkbox which is checked. Below that, there is a table with columns for 'IP Version' (set to 'IPv4') and 'IP Address Range' (with two empty input fields separated by a tilde '~'). At the bottom of this section are 'Add' and 'Edit / Delete' buttons.

**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.

"**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.



# 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.

Advanced Setup

Power Management

Parameters

MIPS CPU Clock divider when Idle	<input checked="" type="checkbox"/> Enable	Status	Enabled
Wait instruction when Idle	<input checked="" type="checkbox"/> Enable	Status	Enabled
DRAM Self Refresh	<input checked="" type="checkbox"/> Enable	Status	Enabled
Ethernet Auto Power Down	<input checked="" type="checkbox"/> Enable	Status	Enabled
Adaptive Voltage Scaling	<input checked="" type="checkbox"/> Enable	Status	Enabled

Apply

Refresh

Number of ethernet interfaces in:  
Full power mode: 1  
Low power mode: 3



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. Refer to **Internet Times** for details. You router time should correspond

Management

Time Schedule

Parameters

Name

Day in a week

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Start Time

00 : 00

End Time

00 : 00

Add

Edit / Delete

For example, user can add a timeslot named “timeslot1” features a period from 9:00 of Monday to 19:00 of Friday.

Management

Time Schedule

Parameters

Name

Day in a week

☐ Sun

☐ Mon

☐ Tue

☐ Wed

☐ Thu

☐ Fri

☐ Sat

Start Time

00 : 00

End Time

00 : 00

Add

Edit / Delete

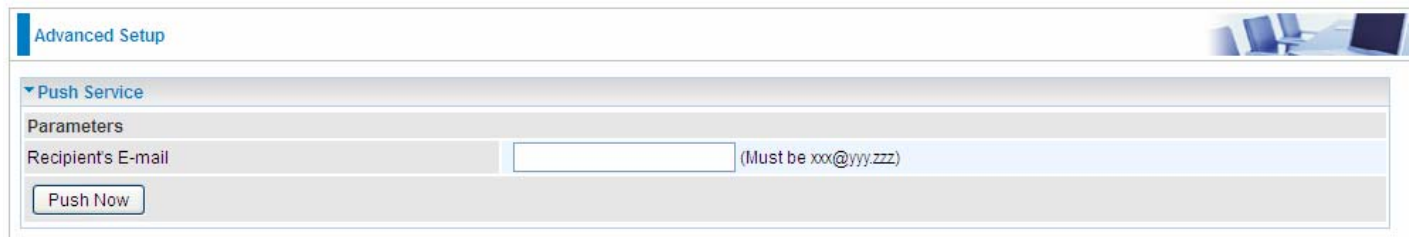
Edit	Name	Day in a week	Start Time	End Time	Delete
<input type="radio"/>	timeslot1	sMTWTFs	09:00	19:00	<input type="checkbox"/>



# Diagnostics

## Push Service

With push service, the system can send email messages with consumption data and system information.



The screenshot shows a web interface titled "Advanced Setup" in the top left corner. Below the title bar, there is a section labeled "Push Service" with a downward-pointing arrow. Underneath, a "Parameters" section contains a label "Recipient's E-mail" followed by a text input field. To the right of the input field is a placeholder text "(Must be xxx@yyy.zzz)". Below the input field is a button labeled "Push Now".

**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	<a href="#">Help</a>
Test LAN Connection ( P2 )	PASS	<a href="#">Help</a>
Test LAN Connection ( P1 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P4/EWAN )	FAIL	<a href="#">Help</a>
Test your Wireless Connection	PASSPASS	<a href="#">Help</a>
▼ Test the connection to your DSL service provider		
Test xDSL Synchronization	PASS	<a href="#">Help</a>
Test ATM OAM F5 segment ping	PASS	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping	PASS	<a href="#">Help</a>
▼ Test the connection to your Internet service provider		
Test PPP server connection	PASS	<a href="#">Help</a>
Test authentication with ISP	PASS	<a href="#">Help</a>
Test the assigned IP address	PASS	<a href="#">Help</a>
Ping default gateway	PASS	<a href="#">Help</a>
Ping primary Domain Name Server	FAIL	<a href="#">Help</a>
<div>Test    Test With OAM F4</div>		



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

Advanced Setup

802.1ag Connectivity Fault Management

Parameters

This diagnostic is only used for VDSL PTM mode.

Maintenance Domain (MD) Level2

Destination MAC Address

802.1Q VLAN ID0[0-4095]

VDSL Traffic TypeInactive

Test the connection to another Maintenance End Point (MEP)

Loopback Message (LBM)

Find Maintenance End Points (MEPs)

Linktrace Message (LTM)

Set MD LevelSend LoopbackSend Linktrace

**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.

Configuration

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

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
<b>None of the LEDs is on when you turn on the router</b>	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.
<b>You have forgotten your login username or password</b>	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
<b>Frequent loss of ADSL line sync (disconnections)</b>	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>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows Me, Windows XP and Windows Vista are registered Trademarks of Microsoft Corporation.