



# **BiPAC 8700NEXL R2**

**Wireless-N 3G/4G LTE VDSL2/ADSL2+  
Firewall Router**

**User Manual**

# Table of Contents

Chapter 1: Introduction .....	1
Introduction to your Router.....	1
Features .....	3
VDSL2/ADSL2+ Compliance .....	3
Network Protocols and Features .....	4
Firewall.....	4
Quality of Service Control .....	5
ATM and PPP Protocols .....	5
IPTV Applications .....	5
USB Application Server .....	5
Wireless LAN .....	5
Management.....	6
Hardware Specifications .....	7
Physical Interface .....	7
Chapter 2: Installing the Router.....	8
Package Contents.....	8
Important note for using this router .....	9
Device Description .....	10
The Front LEDs .....	10
The Rear Ports.....	11
Cabling.....	13
Chapter 3: Basic Installation .....	14
Connecting Your Router.....	15
Network Configuration .....	17
Configuring a PC in Windows 7/ 8 .....	17
Configuring a PC in Windows Vista .....	20
Configuring a PC in Windows XP .....	23
Factory Default Settings.....	25
Information from your ISP .....	27
Easy Sign On (EZSO) .....	28
Chapter 4: Configuration .....	35
Configuration via Web Interface.....	35
Status .....	37
Summary .....	38
WAN .....	39
Statistics .....	40
LAN.....	40
WAN Service.....	41
xTM .....	41
xDSL.....	42
Bandwidth Usage .....	45
LAN.....	45
WAN Service.....	47
3G/4G LTE Status .....	49
Route.....	50
ARP .....	51
DHCP .....	52
Log.....	53
System Log .....	53

Security Log.....	54
Quick Start.....	55
Configuration .....	61
LAN - Local Area Network.....	62
Ethernet .....	62
IPv6 Autoconfig.....	65
Interface Grouping.....	69
Wireless.....	72
Basic .....	73
Security .....	75
MAC Filter .....	86
Wireless Bridge.....	87
Advanced.....	88
Station Info.....	90
Schedule Control.....	91
WAN-Wide Area Network.....	92
WAN Service.....	92
DSL.....	92
Ethernet .....	103
3G/4G LTE .....	110
DSL.....	113
SNR.....	114
System.....	115
Internet Time .....	115
Firmware Upgrade .....	116
Backup / Update .....	117
Access Control.....	118
Mail Alert .....	119
SMS Alert.....	120
Configure Log .....	121
USB.....	122
Storage Device Info .....	122
User Account.....	123
Print Server .....	128
DLNA .....	133
IP Tunnel .....	135
IPv6inIPv4.....	135
IPv4inIPv6.....	137
Security .....	138
IP Filtering Outgoing .....	138
IP Filtering Incoming .....	141
MAC Filtering .....	143
Blocking WAN PING .....	144
Time Restriction .....	145
URL Filter.....	147
Parental Control Provider.....	150
QoS - Quality of Service .....	151
Quality of Service .....	151
QoS Port Shaping .....	156
NAT.....	157
Exceptional Rule Group.....	157
Virtual Servers.....	158
DMZ Host .....	162

One-to-One NAT .....	163
Port Triggering .....	164
ALG .....	167
Wake On LAN .....	168
Advanced Setup .....	169
Routing .....	170
Default Gateway .....	170
Static Route .....	171
Policy Routing .....	173
RIP .....	174
DNS .....	175
DNS .....	175
Dynamic DNS .....	177
DNS Proxy .....	180
Static DNS .....	181
Static ARP .....	182
UPnP .....	183
Certificate .....	189
Trusted CA .....	189
Multicast .....	192
Management .....	194
SNMP Agent .....	194
TR- 069 Client .....	195
HTTP Port .....	197
Remote Access .....	198
Mobile Networks .....	199
3G/4G LTE Usage Allowance .....	200
Power Management .....	201
Time Schedule .....	202
Auto Reboot .....	203
Diagnostics .....	204
Diagnostics Tools .....	204
Push Service .....	207
Diagnostics .....	208
Fault Management .....	209
Restart .....	210
Chapter 5: Troubleshooting .....	211
Appendix: Product Support & Contact .....	213

# Chapter 1: Introduction

## Introduction to your Router

The Billion BiPAC 8700NEXL R2, a multi service VDSL2/ADSL2+ Router, features fibre-ready triple-WAN VDSL2 supports backward compatibility to ADSL2+ for a longer reach distance, an all-in-one advanced device equipped with 802.11n (2.4GHz) 300Mbps, Gigabit EWAN, connections to 3G/4G LTE. As well as being IPv6-capable, the BiPAC 8700NEXL R2 VDSL2 router supports super-fast fibre connections via a Gigabit Ethernet WAN port. It also has one 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) and FTP (File Transfer Protocol) access. 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 Billion BiPAC 8700NEXL R2 delivers a future-proof solution for VDSL2 connections, super-fast FTTC and ultra-speed FTTH (Fibre-To-The-Home) network deployment and services.

### Flexible Deployment Options

The BiPAC 8700NEXL R2 provides users with flexible, scalable deployment options optimized to both reduce costs and provide the longest possible lifespan for the investment. The BiPAC 8700NEXL R2 integrates dual WAN options; a VDSL2/ADSL2+ interface and a second 10/100/1000 Ethernet WAN interface which can be used for broadband connectivity to any other Ethernet broadband device. SOHO or small office users can even deploy the BiPAC 8700NEXL R2 for FTTx (Fiber-to-the-building, node, or home) applications over a fibre device connection. Operators can now deploy one device to support current and future network migration.

### 3G/4G LTE mobility

With 3G/4G LTE-based Internet connection (requires an additional 3G/4G LTE 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 8700NEXL R2 will then automatically reconnect to the xDSL/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.

### Optimal wireless performance

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.

## **Experience Gigabit**

The BiPAC 8700NEXL R2 one Gigabit WAN port. This EWAN offers another broadband connectivity option for connecting to a cable, DSL, fibre modem. The BiPAC 8700NEXL R2 again offers users convenience and optimal network performance with data rates reaching up to 1Gbps.

## **Pathway to the IPv6 future**

The BiPAC 8700NEXL R2 fully support IPv4 and IPv6 dual stack. Dual Stack means the router is capable of running IPv4 and IPv6. 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..

## **Virtual AP**

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

## **Web Based GUI**

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

## **Firmware Upgradeable**

Device can be upgraded to the latest firmware through the WEB based GUI.

# Features

- Compliant with all ADSL2+/VDSL2 standards
- IPv6 ready (IPv4/IPv6 dual stack)
- Triple WAN approach – VDSL2/ADSL2+, 3G/4G LTE mobile connection, and Ethernet WAN for Broadband Connectivity
- 5-port Ethernet switch
- 1-port (Port#5) Gigabit Ethernet WAN (EWAN) port for broadband connectivity.
- 1 USB ports for 3G/4G LTE USB modem
- IEEE 802.11 b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- Supports WDS repeater function
- SNR adjustments to achieve highest sync speeds
- Monitoring of individual LAN/WAN traffic
- Universal Plug and Play (UPnP) Compliance
- QoS for traffic prioritization and bandwidth management
- SOHO firewall security
- Auto failover
- Supports IPTV application<sup>\*2</sup>
- Ease of use with quick installation wizard (EZSO)
- Broadcom chipset for better stability
- Ideal for Home and SOHO users

## VDSL2/ADSL2+ Compliance

- Compliant with xDSL Standard
  - Full-rate ANSI T1.413 Issue 2
  - ITU-T G.993.2 (VDSL2, supporting profile 8a, 8b,8c, 8d, 12a, 12b, 17a)
  - ITU-T G.992.1 (G.dmt)
  - ITU-T G.992.2 (G.lite)
  - ITU-T G.992.3 (G.dmt.bis)
  - ITU-T G.992.3 Annex M (ADSL2 Annex M)
  - ITU-T G.992.4 (G.lite.bis),
  - ITU-T G.992.5 (G.dmt.bis plus)

- ITU-T G.992.5 Annex M (ADSL2+ Annex M)
- ITU-T G.994.1 (G.hs)
- Supports VDSL2 band plan: 997 and 998

## **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
- 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
- Support port-based Interface Grouping (VLAN)

## **Firewall**

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- Packet Filtering (v4/v6) - port, source IP address, destination IP address
- MAC Filter
- URL Content Filtering (v4/v6) – string or domain name detection in URL string
- Remote access control for web base access
- 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
- Password protection for system management



## Quality of Service Control

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

## ATM 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
- Interface Grouping (VLAN)
- Quality of Service (QoS)

## USB Application Server

- 3G/4G LTE dongle support
- Storage/NAS: FTP server, Samba server, DLNA
- Printer Server

## Wireless LAN

- Compliant with IEEE 802.11 b/ g/ n standards
- 2.4-2.484GHz 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
- Multiple wireless SSIDs with wireless guest access and client isolation
- WDS repeater function support

- 802.1x radius authentication supported

## 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
- Push Service for diagnostics and debug usage



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

### 8700NEXL R2

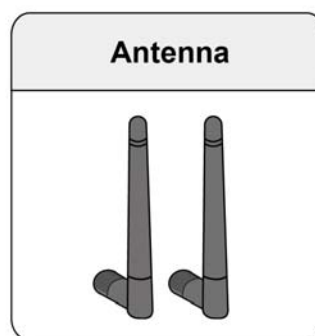
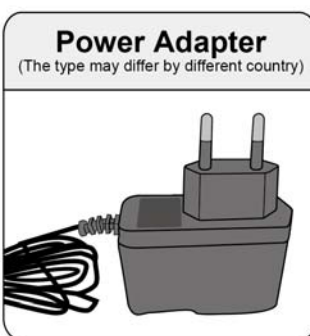
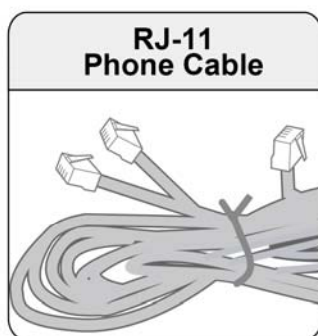
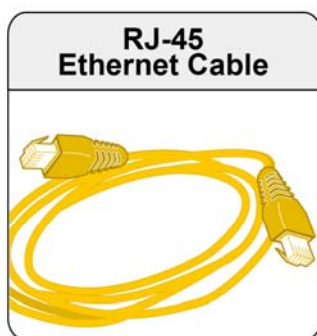
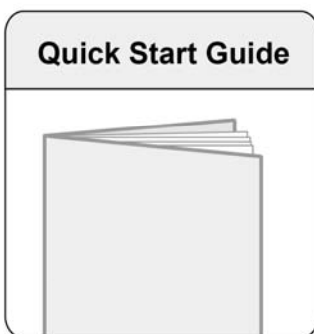
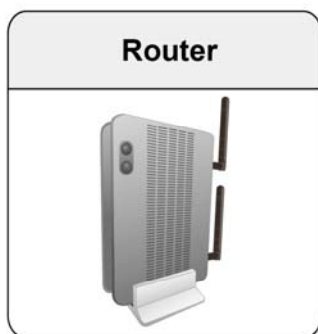
- WLAN: Two external Wi-Fi Antennas
- DSL: xDSL port
- USB 2.0: 1-port USB 2.0 interface for storage service and printer server and 3G/4G LTE dongle
- Ethernet: 4-port 10 / 100 Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: 1 Gigabit Ethernet port (port#5) connecting directly to Fiber/ xDSL/ Cable modem, also serving as an Ethernet port#5 when not in EWAN use
- Power jack
- Power switch
- Wi-Fi on/off button and WPS push button
- Factory default reset button

# Chapter 2: Installing the Router

## Package Contents

### 8700NEXL R2

- BiPAC 8700NEXL R2 Wireless-N 3G/4G LTE VDSL2/ADSL2+ Firewall Router
- This Quick Start Guide
- CD containing User Manual
- RJ-45 Cat. 5e STP Ethernet Cable
- RJ-11 xDSL/ telephone Cable
- Vertical Stand
- Two detachable Wi-Fi Antennas
- Power adaptor
- Splitter/ Micro-filter (Optional)



## Important note for using this router



### Warning

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



### Attention

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

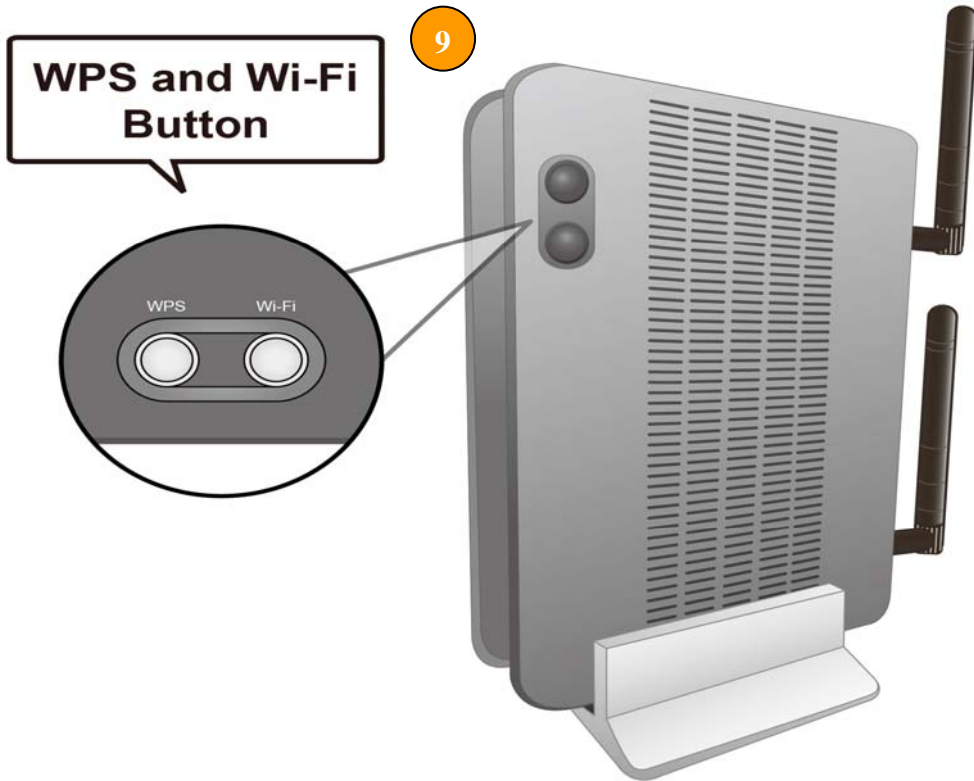
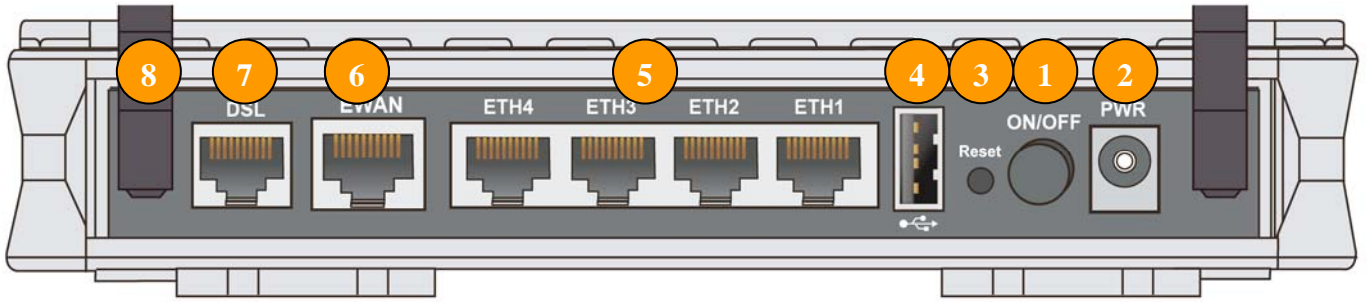
# Device Description

## The Front LEDs



LED	STATUS	DESCRIPTION
PWR	Green	System is up and ready
	Off	No Power
ETH1/2/3/4	Green	LAN link established and active via LAN port.
	Blinking	Data transmitting or receiving over LAN.
	Off	No LAN link via LAN port.
Gigabit EWAN/ETH5	Green	EWAN port link established and active
	Blinking	EWAN port data activity occurs
	Off	No EWAN port link active
WLAN	Green	The wireless module is ready and idle
	Blinking	Data transmitting or receiving over WLAN
	Off	The wireless function is disabled.
WPS	Green	WPS connection is established
	Blinking	Trying to establish a WPS connection
	Off	WPS function is off or no WPS connection
DSL	Green	DSL link established and active
	Quick Blinking	DSL is trying to establish a connection
	Off	No DSL link
INET	Green	IP connected.
	Blinking	IP connected and IP traffic is passing through the device.
	Off	No internet IP address obtained.
USB	Green	USB connection is established.
	Off	No USB port connected.

# The Rear Ports



PORT		MEANING
1	Power ON/OFF	Power ON/OFF switch.
2	PWR (Power)	Connect the supplied Power Adapter to this port.
3	Reset	Push and hold the reset button for 5 seconds to restore to its factory default settings (this is used when you cannot login to the router, e.g. forgot your password).
4	USB	Connect to a Printer or USB storage device.
5	ETH1/2/3/4	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.
6	Gb EWAN	Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable, for broadband connectivity.  <b>Note: Ethernet #5 (EWAN) is a LAN / WAN Configurable Port ; it can be configured as a WAN Interface for Broadband connectivity</b>
7	DSL	Connect the device to a DSL telephone jack or splitter using a RJ-11 telephone cable.
8	Antennas	Connect to the detachable antennas.
9	WPS / Wi-Fi On/Off	By controlling the pressing time, users can achieve two different effects:  (1) <b>WPS*</b> : Press & hold the button for <b>2 seconds</b> to trigger WPS function  (2) <b>Wireless ON/OFF button</b> : Press & hold the button for <b>more than 6 seconds</b> to enable/disable wireless  <b>* For WPS configuration, please refer to the WPS section in the User Manual.</b>



## 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 8, Windows 8 /7 /XP /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.

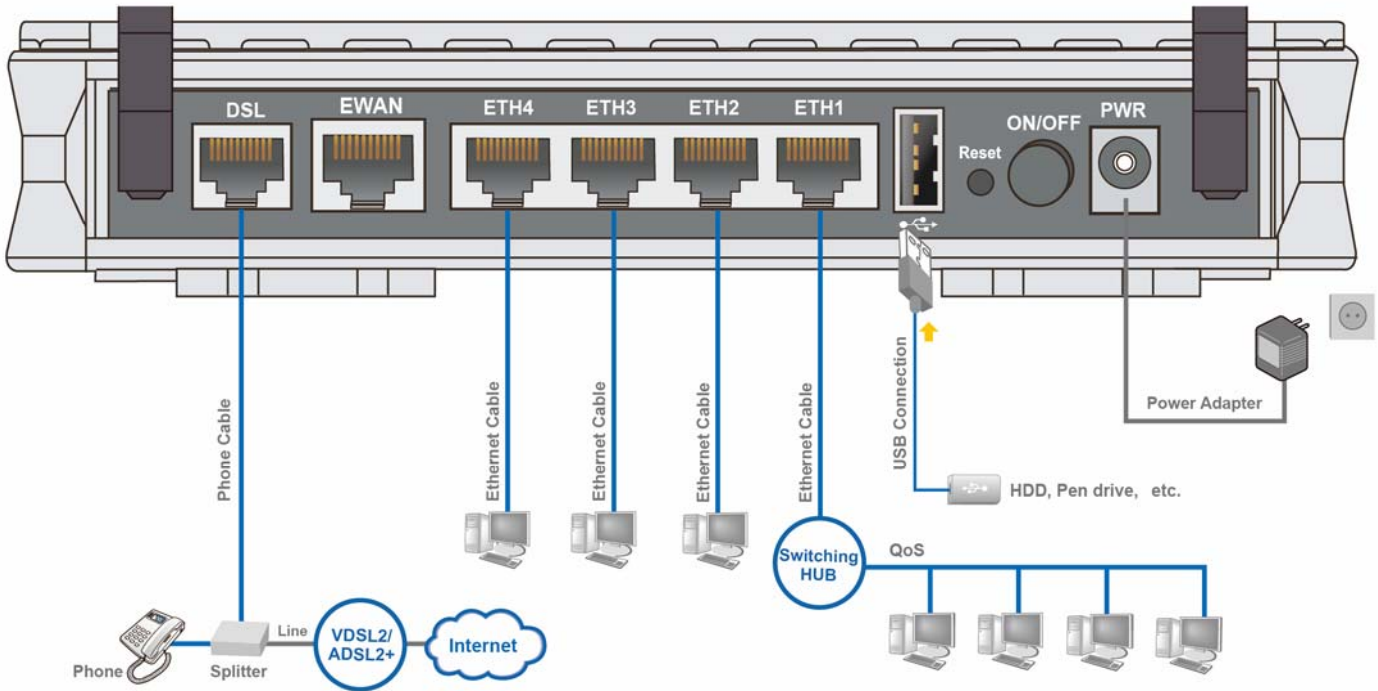


Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

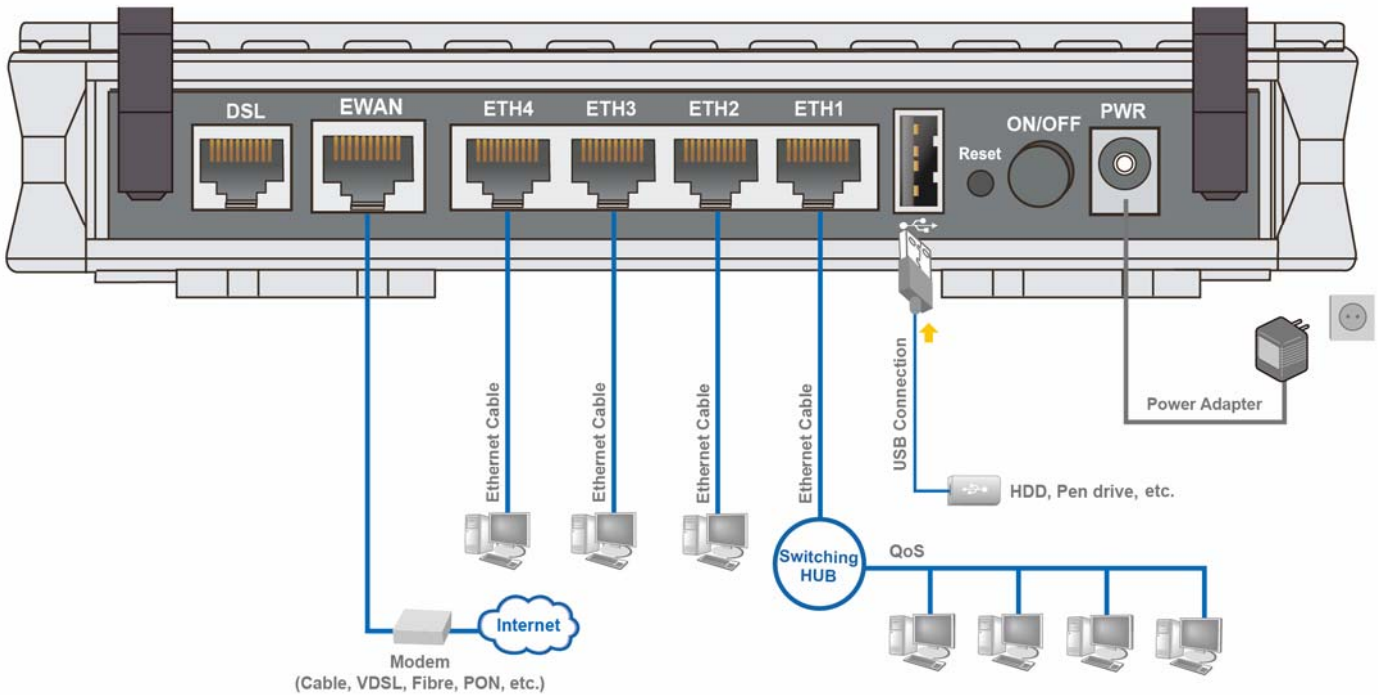
# Connecting Your Router

Users can connect the ADSL2+/VDSL2 router as the following

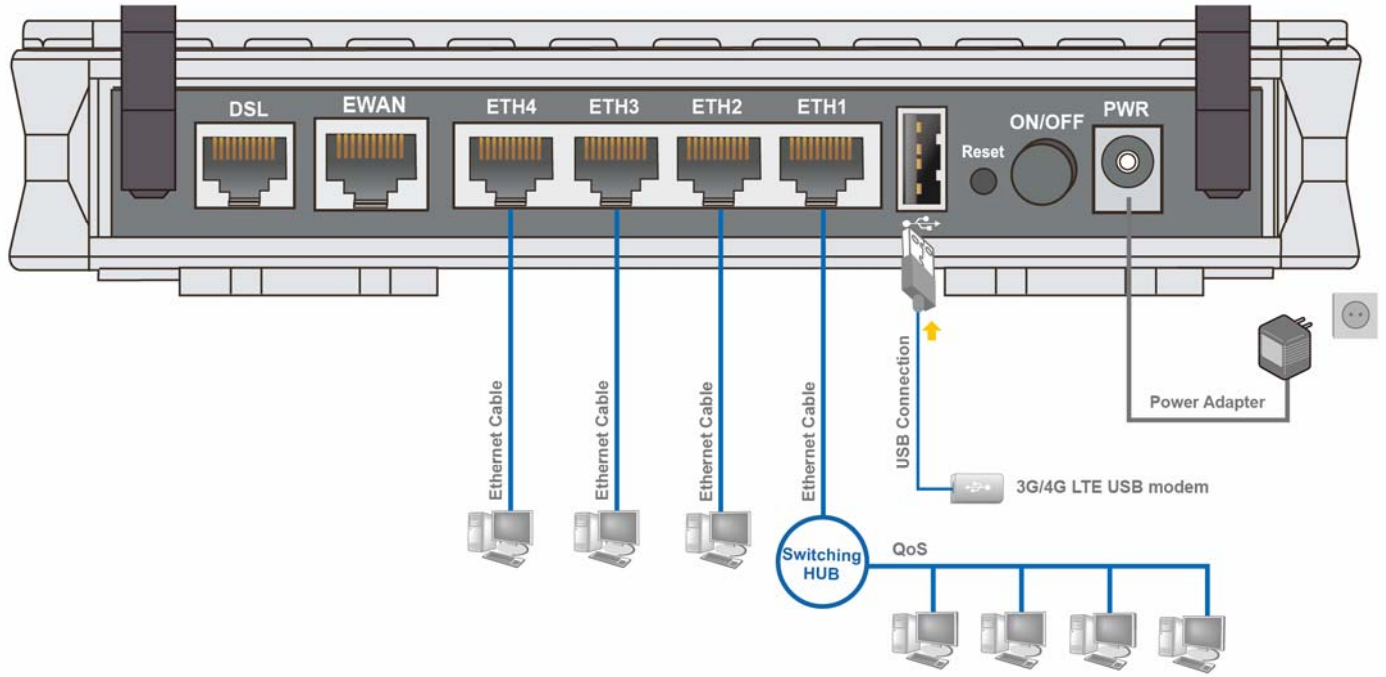
**DSL Router mode:**



**Broadband Router mode:**



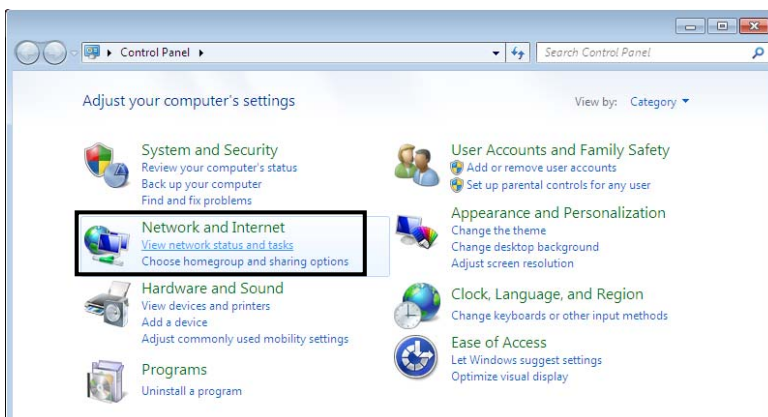
# 3G/4G LTE Router Mode



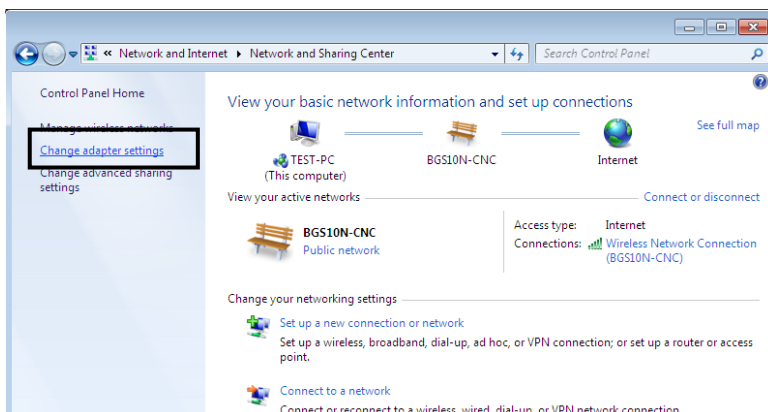
# Network Configuration

## Configuring a PC in Windows 7 / 8

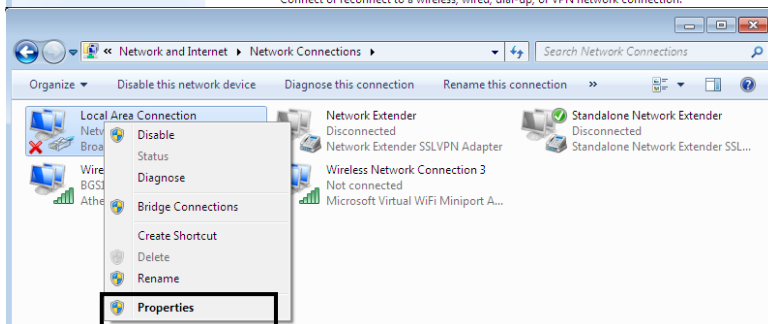
1. Go to **Start**. Click on **Control Panel**. Then click on **Network and Internet**.



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

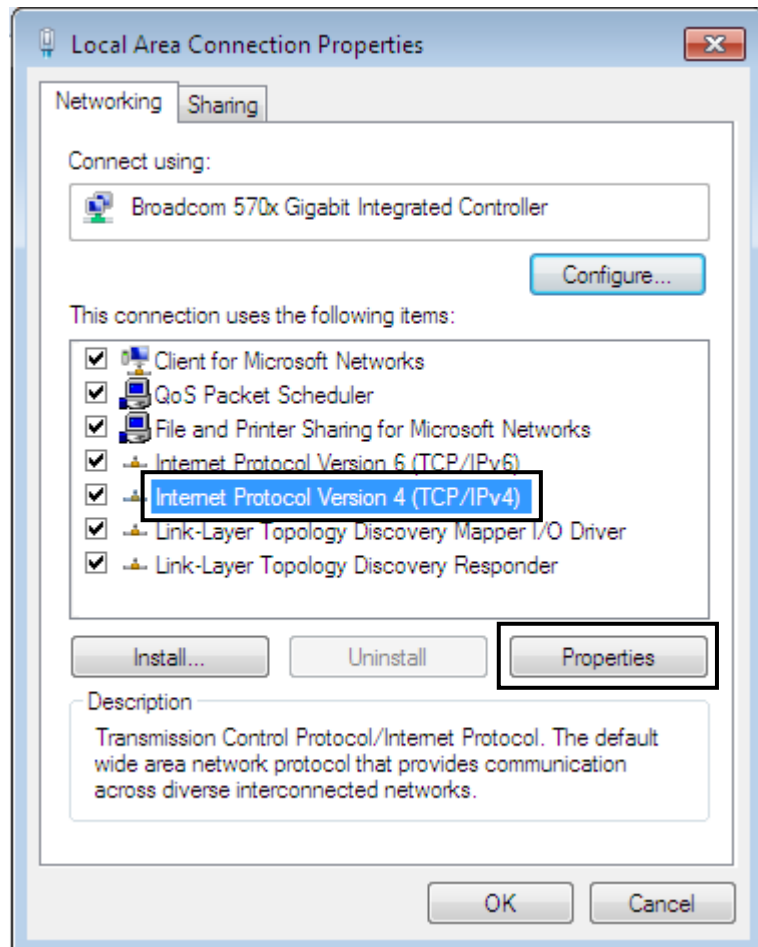


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

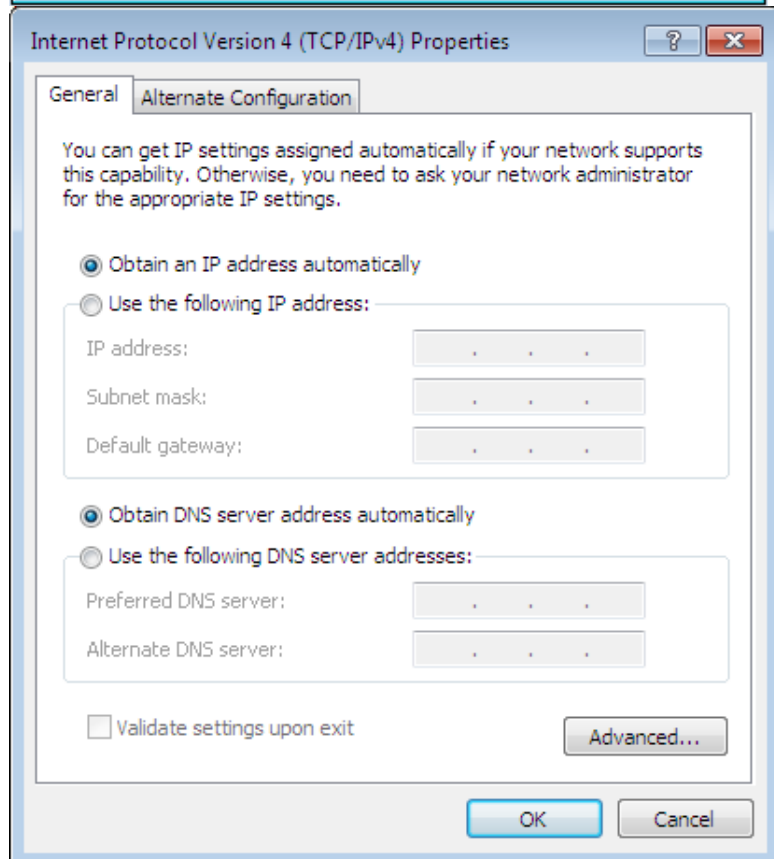


## IPv4:

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

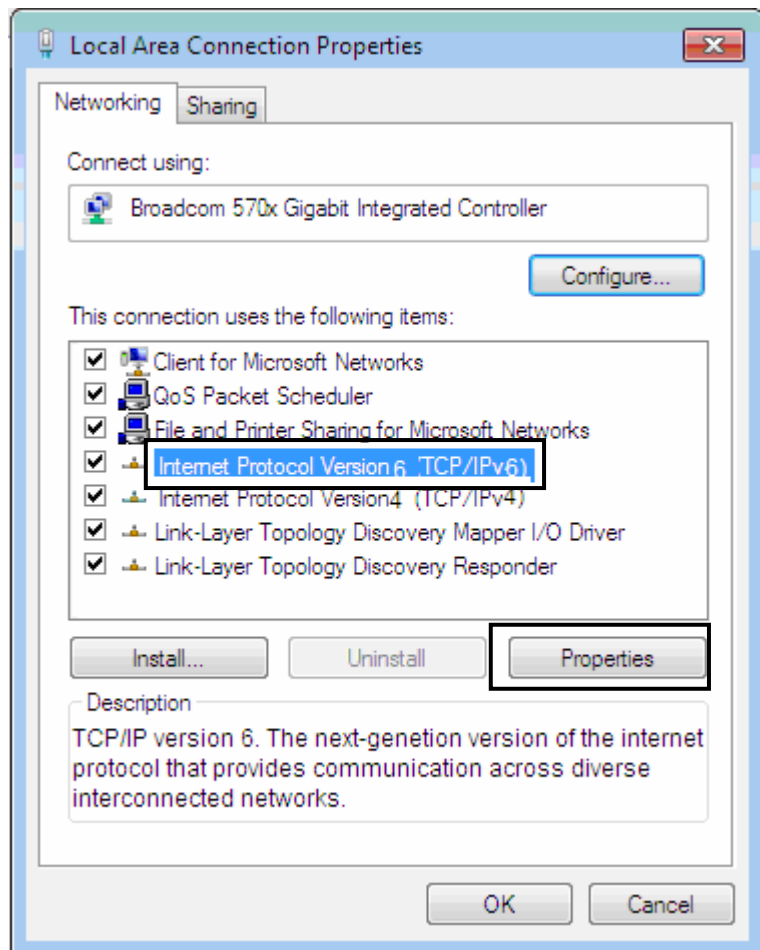


5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

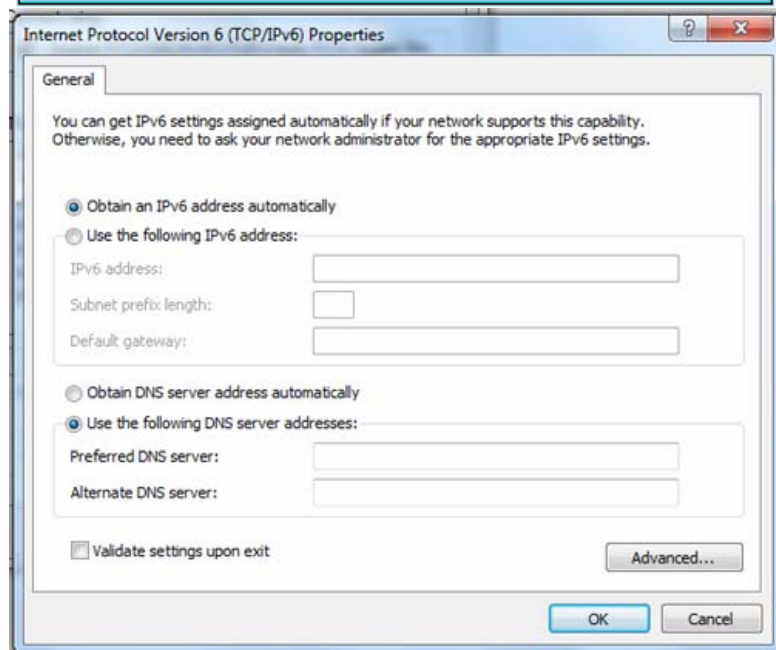


## IPv6:

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

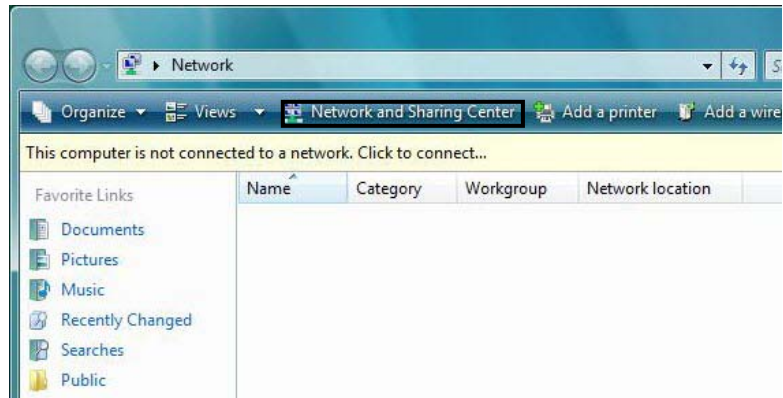


5. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



# Configuring a PC in Windows Vista

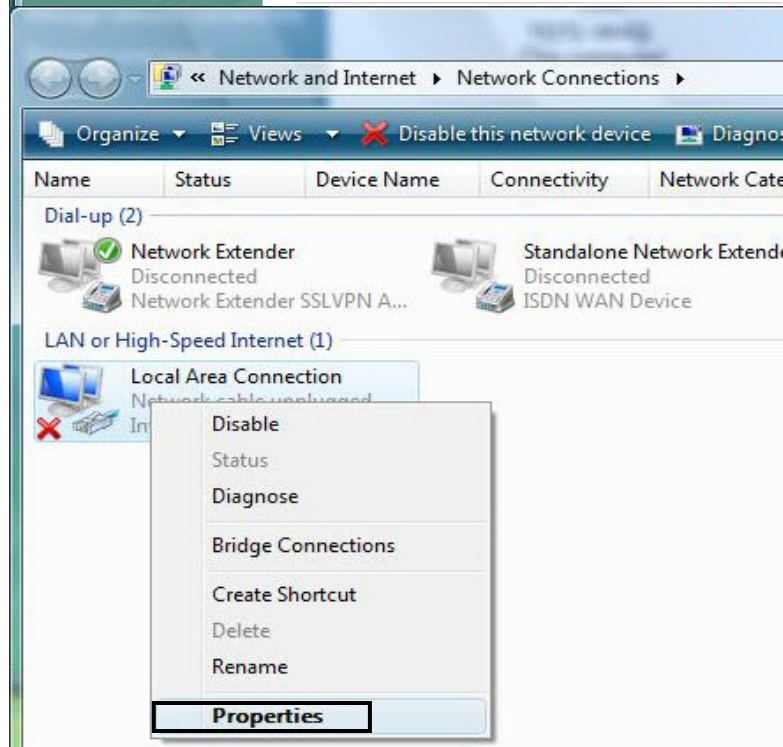
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.



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



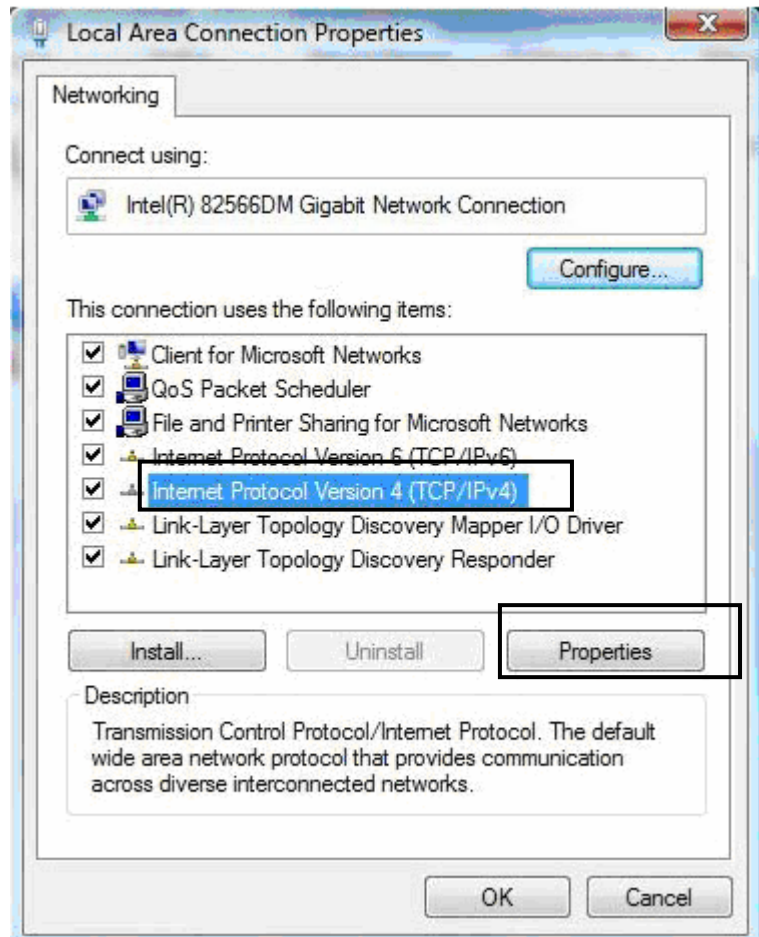
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.





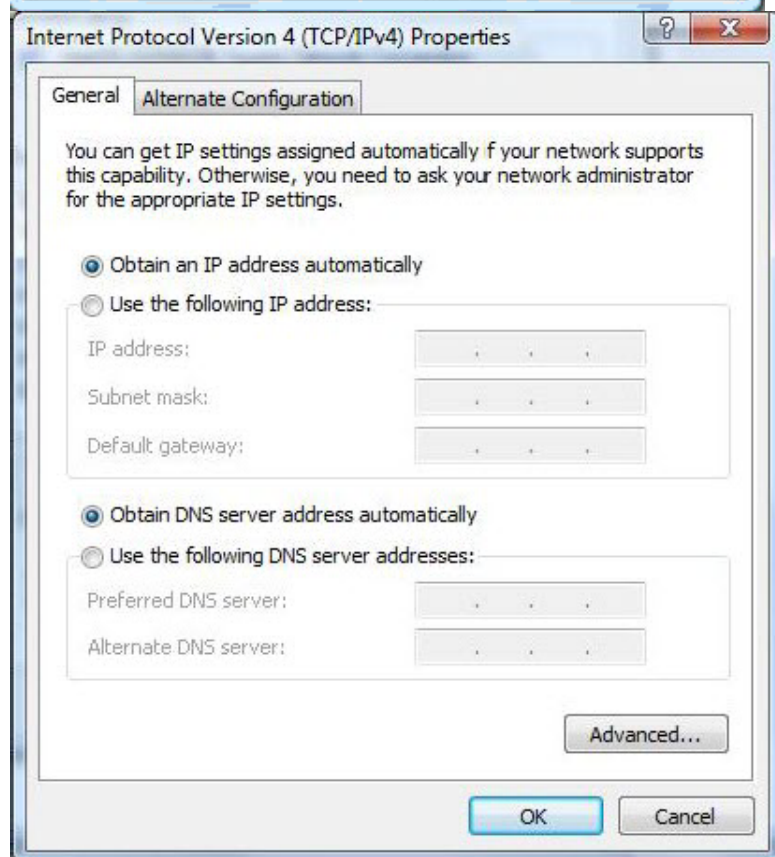
## IPv4:

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



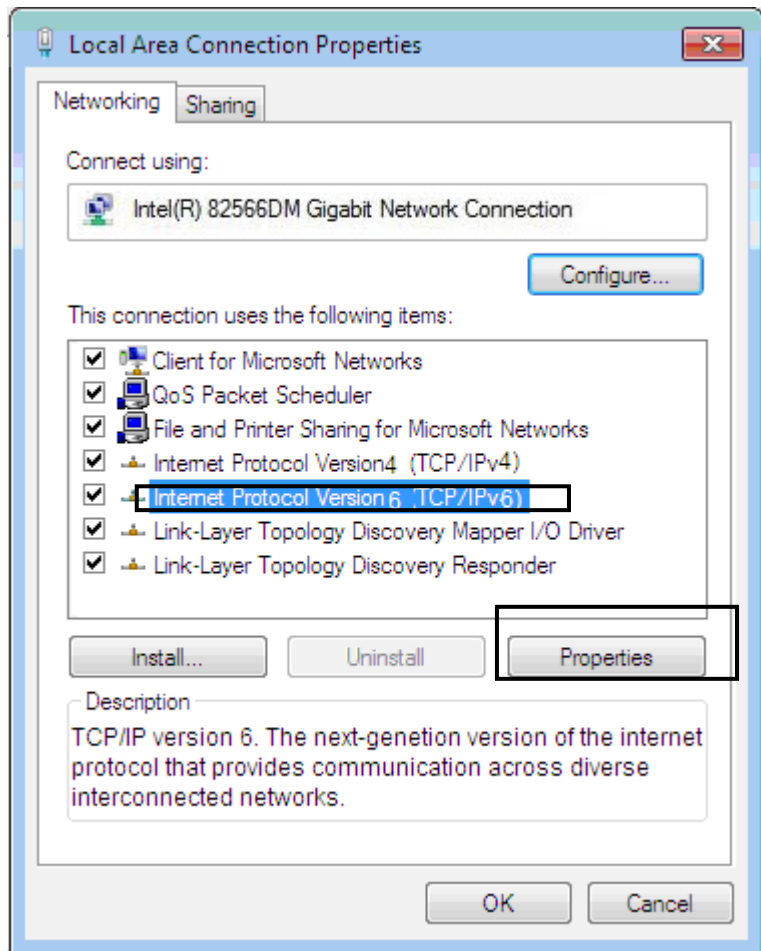
6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



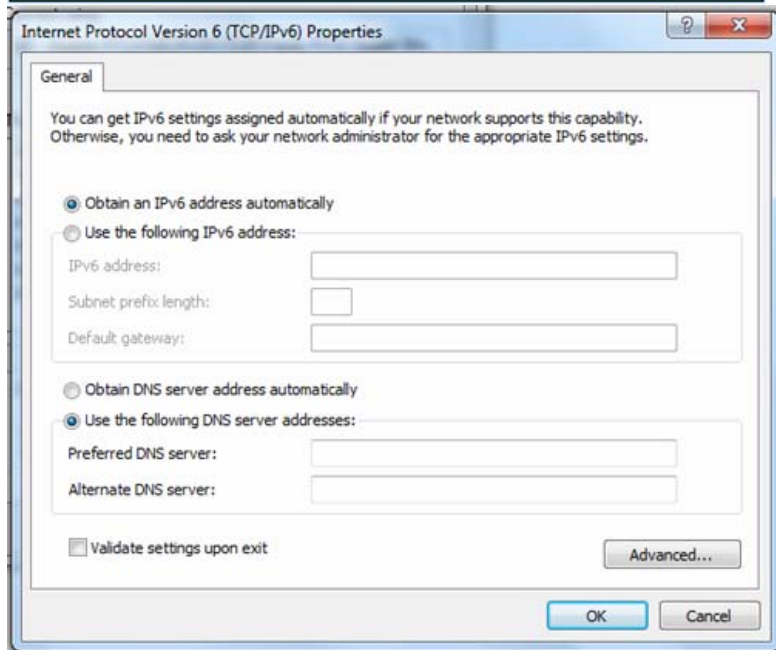
## IPv6:

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.

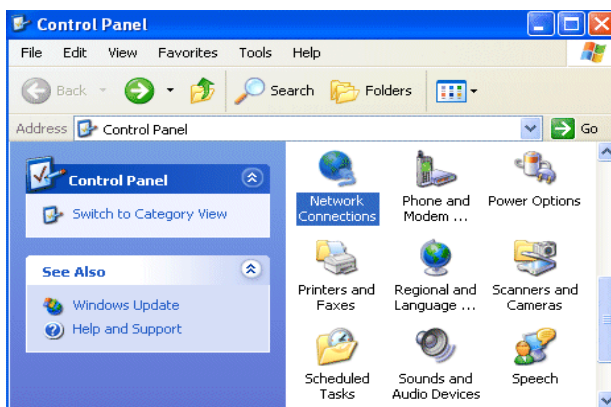
10. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



# Configuring a PC in Windows XP

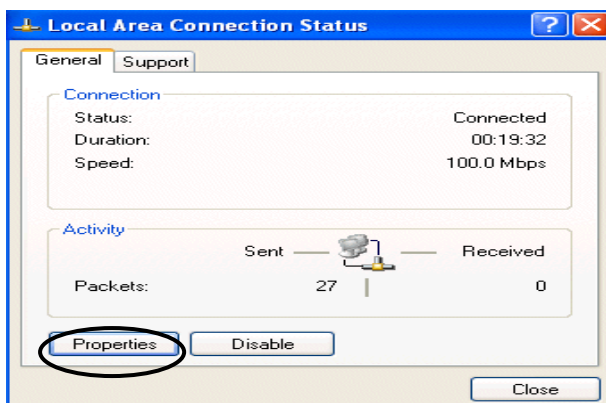
## IPv4:

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

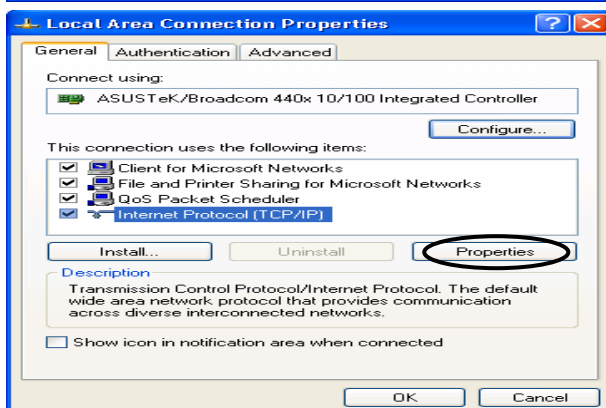


2. Double-click **Local Area Connection**.

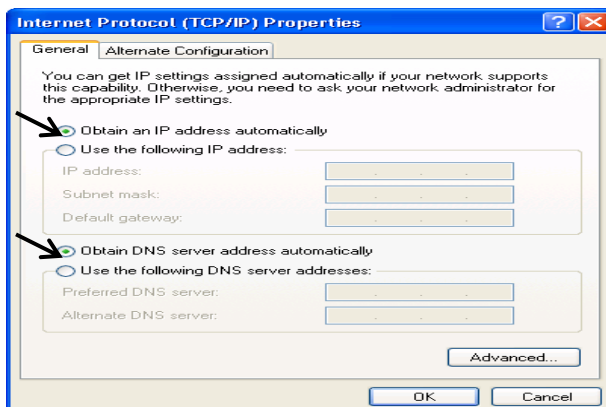
3. In the **Local Area Connection Status** window, click **Properties**.



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.



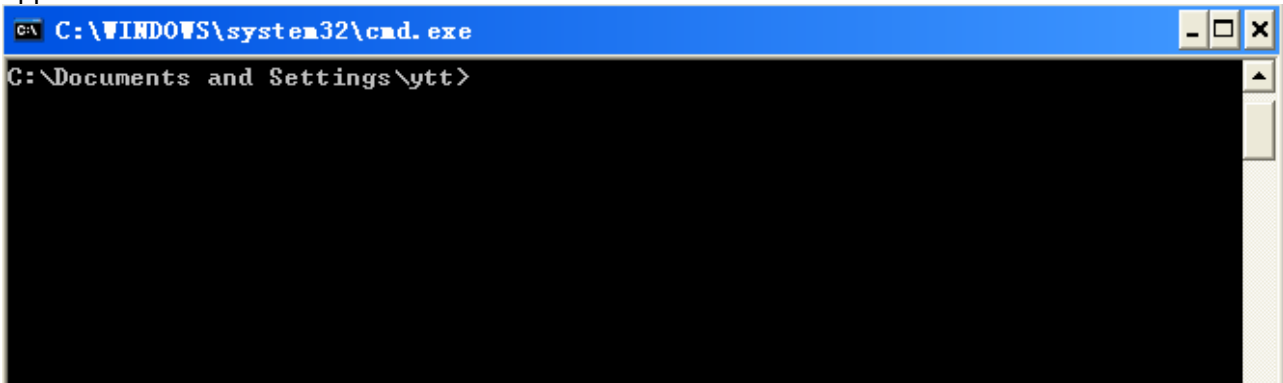
6. Click **OK** to finish the configuration.

## IPv6:

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

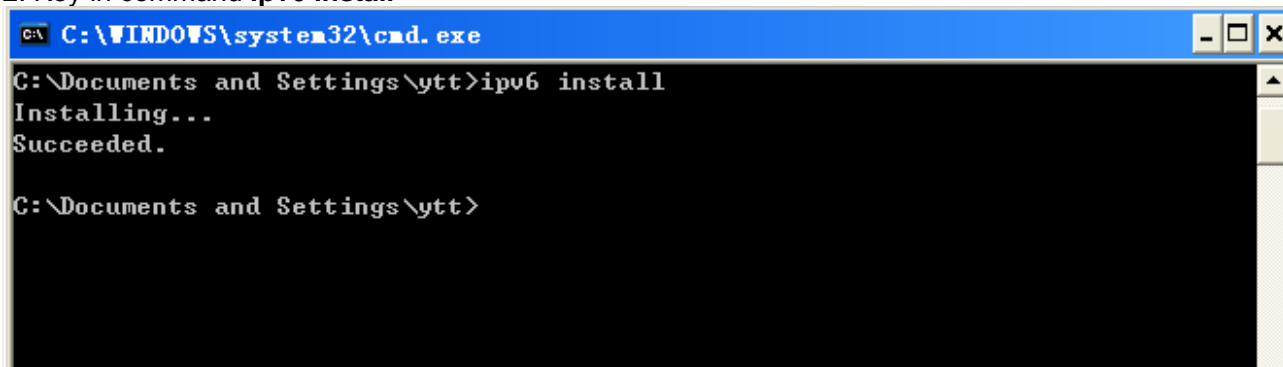
Act as shown below:

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.

# 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: 192.168.1.254
- ▶ IP pool counts: 100

## LAN and WAN Port Addresses

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

### IPv4

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

### IPv6

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

## Information from your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided.

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

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

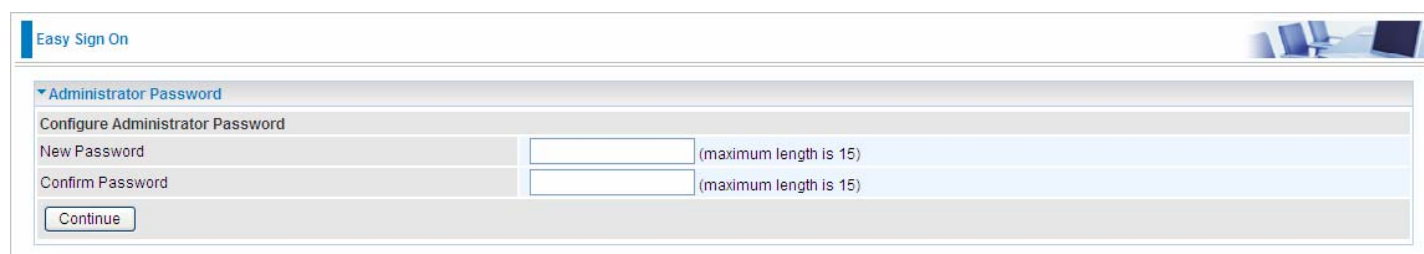
# Easy Sign On (EZSO)

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

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


## EZSO window pops up:

**Step1:** Set the administration password.



The screenshot shows the 'Easy Sign On' window with the 'Administrator Password' section expanded. It contains two input fields: 'New Password' and 'Confirm Password', both with a note '(maximum length is 15)'. A 'Continue' button is located at the bottom left of the section.

**Step 2:** Set the Time Zone.



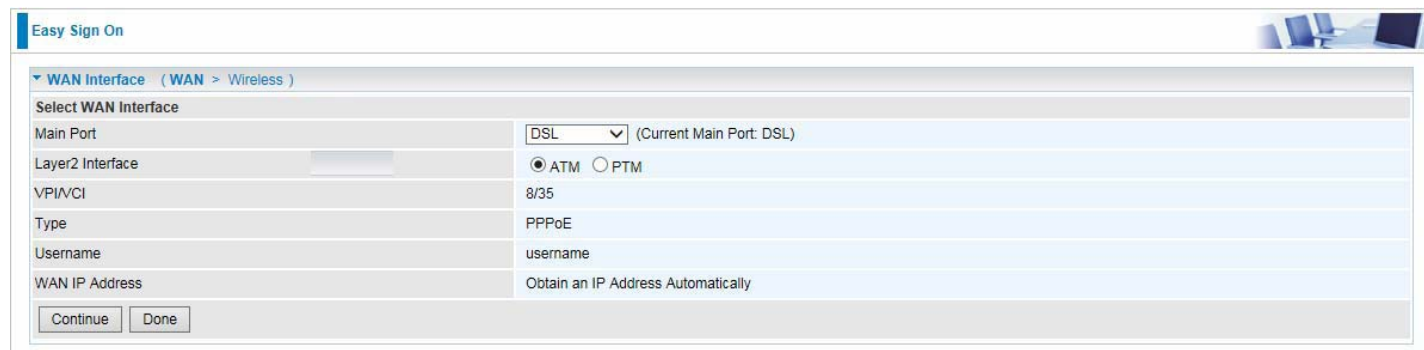
The screenshot shows the 'Easy Sign On' window with the 'Time Zone' section expanded. It contains a dropdown menu for 'Time zone offset' with the selected option '(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. A 'Continue' button is located at the bottom left of the section.

**Step 3:** Configure the WAN interface.

## DSL mode (ADSL mode, please choose ATM; VDSL, please choose PTM)

Here take ADSL for example.

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' section expanded. It contains several configuration options: 'Main Port' set to 'DSL', 'Layer2 Interface' with radio buttons for 'ATM' (selected) and 'PTM', 'VPI/VCI' set to '8/35', 'Type' set to 'PPPoE', 'Username' set to 'username', and 'WAN IP Address' set to 'Obtain an IP Address Automatically'. 'Continue' and 'Done' buttons are at the bottom left.

**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' interface with the 'WAN Interface (WAN > Wireless)' section expanded. The 'WAN Service' configuration is as follows:

Type	PPP over Ethernet (PPPoE)
VPI / VCI	8 [0-255] / 35 [32-65535]
Username	username
Password	••••••••
Service Name	
Encapsulation Mode	LLC/SNAP-BRIDGING
Authentication Method	AUTO
IPv4 Address	<input type="checkbox"/> Static
IP Address	
IPv6 for this service	<input checked="" type="checkbox"/> Enable
IPv6 Address	<input type="checkbox"/> Static
IP Address	
MTU	1492

A 'Continue' button is located at the bottom left of the configuration area.

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

The screenshot shows the 'Easy Sign On' interface with the 'WAN Interface (WAN > Wireless)' section expanded. A warning message is displayed:

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

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

The screenshot shows the 'Easy Sign On' interface with the 'WAN Interface (WAN > Wireless)' section expanded. A message is displayed:

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**.

The screenshot shows the 'Easy Sign On' interface with the 'WAN Interface (WAN > Wireless)' section expanded. A success message is displayed:

Congratulations !  
Your WAN port has been successfully configured.

Buttons for 'Next to Wireless' and 'Done' are visible at the bottom.

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

The screenshot shows the 'Easy Sign On' interface with the 'WAN Interface' section expanded. A message is displayed:

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).



The screenshot shows the 'Easy Sign On' interface for configuring wireless settings. The page title is 'Easy Sign On'. Below the title, there is a breadcrumb trail: 'Wireless (WAN > Wireless)'. The main content area is titled 'Parameters' and contains the following fields:

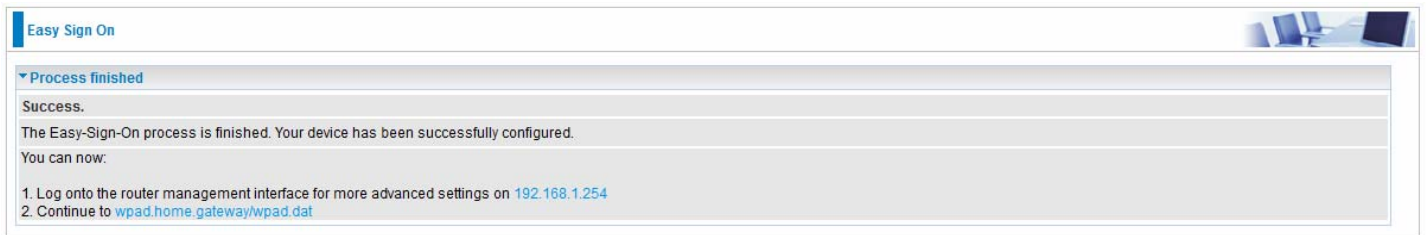
- Wireless:** A checkbox labeled 'Enable' which is checked.
- SSID:** A text input field containing the value 'wlan-ap'.
- WPA2 Pre-Shared Key:** A text input field that is empty, with a link 'Click here to display' next to it.

At the bottom of the configuration area, there is a 'Continue' button.



The screenshot shows the 'Easy Sign On' interface during the configuration process. The page title is 'Easy Sign On'. Below the title, there is a breadcrumb trail: 'Wireless (WAN > Wireless)'. The main content area displays the message: 'Please wait while the device is configured.'

6. Success in configuring the EZSO.



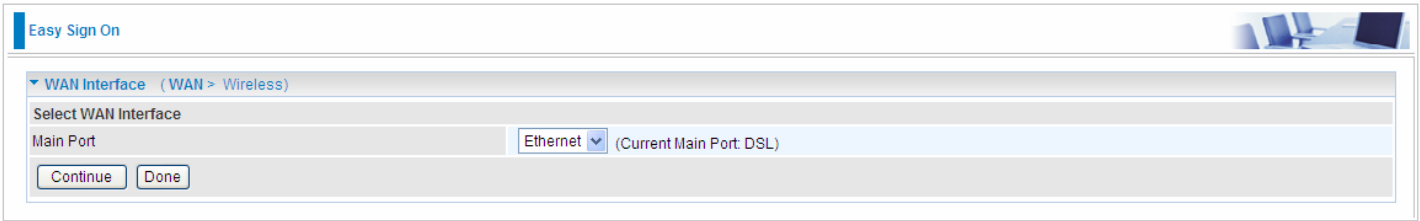
The screenshot shows the 'Easy Sign On' interface after successful configuration. The page title is 'Easy Sign On'. Below the title, there is a breadcrumb trail: 'Process finished'. The main content area displays the following text:

**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)

## Ethernet mode

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



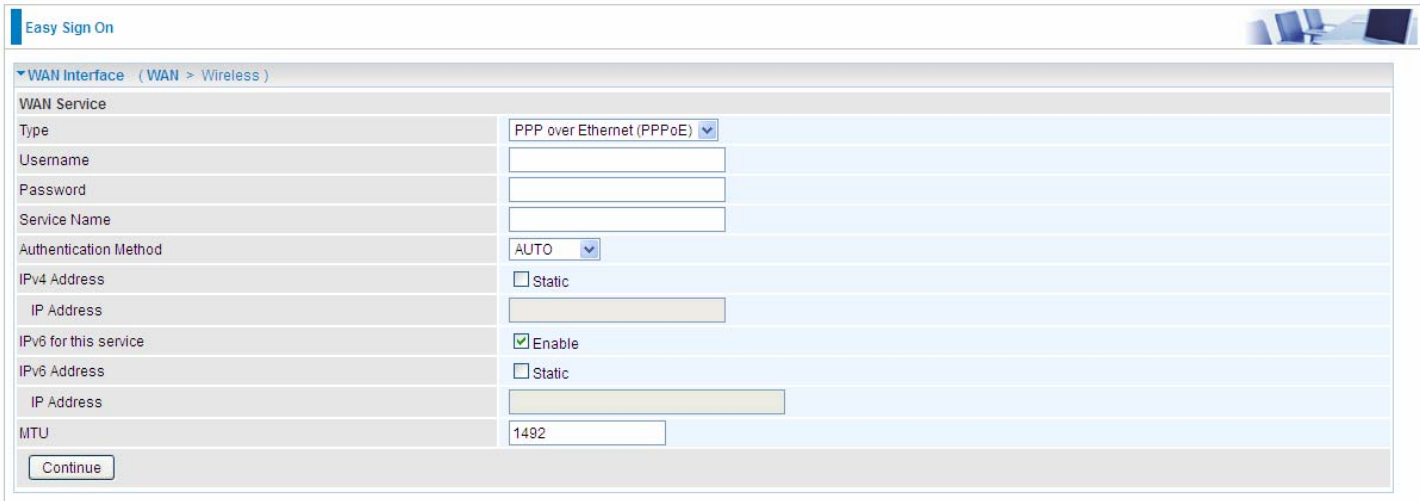
Easy Sign On

WAN Interface (WAN > Wireless)

Select WAN Interface

Main Port Ethernet (Current Main Port: DSL)

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



Easy Sign On

WAN Interface (WAN > Wireless)

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

3. Wait while the device is configured.

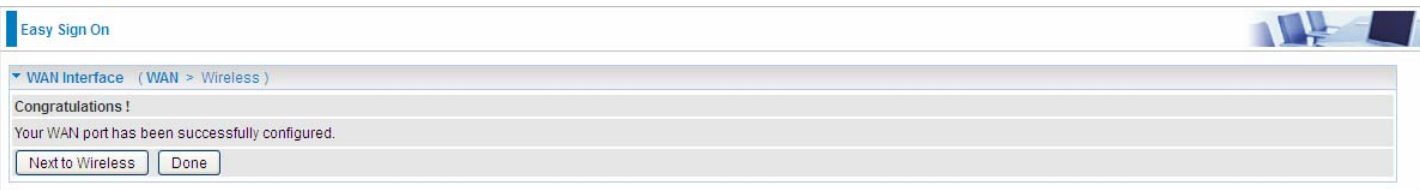


Easy Sign On

WAN Interface (WAN > Wireless)

Please wait while the device is configured.

4. WAN port configuration is successful.



Easy Sign On

WAN Interface (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

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



Easy Sign On

WAN Interface

Stop EZSO

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

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. 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' interface for configuring wireless settings. The 'Wireless' section is expanded, showing a 'Parameters' table with the following fields:

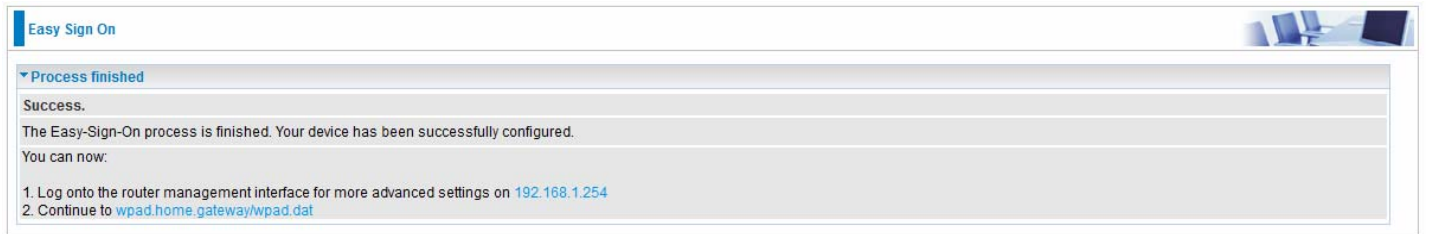
Parameters	
Wireless	<input checked="" type="checkbox"/> Enable
SSID	<input type="text" value="wlan-ap"/>
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

At the bottom of the configuration area, there is a 'Continue' button.



The screenshot shows the 'Easy Sign On' interface with the 'Wireless' section expanded. The main content area displays the message: 'Please wait while the device is configured.'

6. Success in configuring the EZSO.



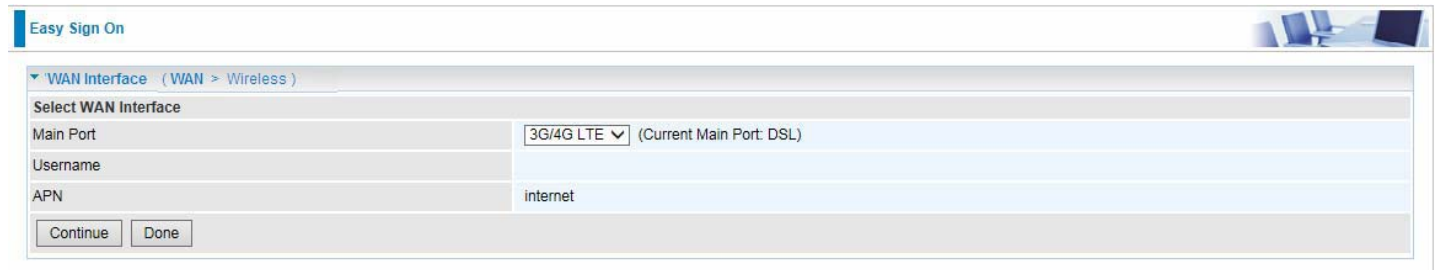
The screenshot shows the 'Easy Sign On' interface with the 'Process finished' section expanded. The main content area displays the following text:

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)

## 3G/4G LTE

1. Select **3G/4G LTE**, press **Continue** to go on to next step.



Easy Sign On

▼ WAN Interface (WAN > Wireless)

Select WAN Interface

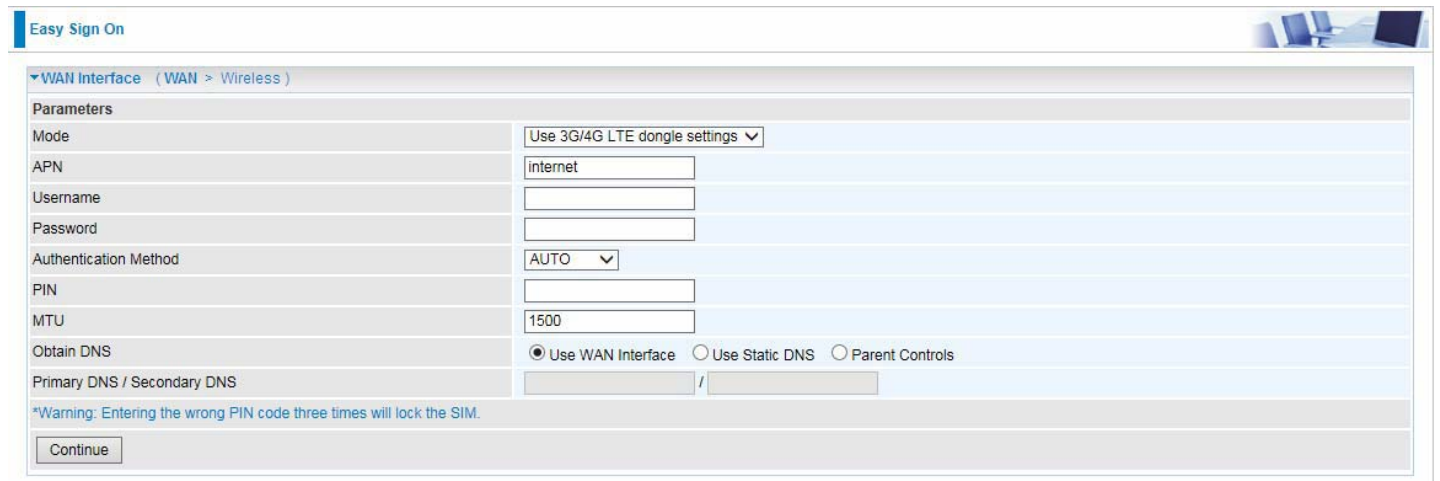
Main Port: 3G/4G LTE (Current Main Port: DSL)

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/4G LTE dongle settings

APN: internet

Username:

Password:

Authentication Method: AUTO

PIN:

MTU: 1500

Obtain DNS:  Use WAN Interface  Use Static DNS  Parent Controls

Primary DNS / Secondary DNS: /

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

Continue

3. Wait while the device is configured.

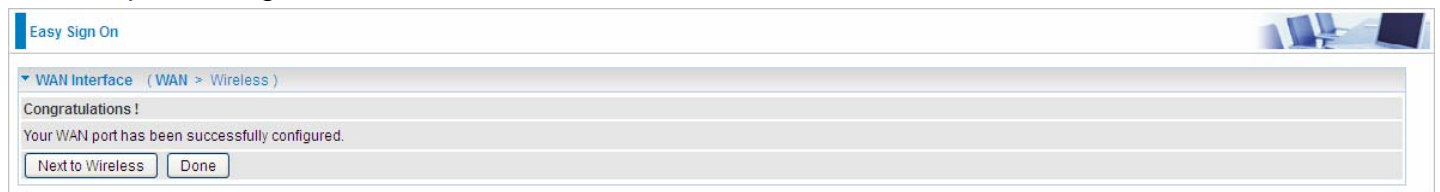


Easy Sign On

▼ Wireless (WAN > Wireless)

Please wait while the device is configured.

4. WAN port configuration is successful.



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).



The screenshot shows the 'Easy Sign On' interface for configuring wireless settings. The 'Wireless' section is expanded, showing a 'Parameters' table with the following fields:

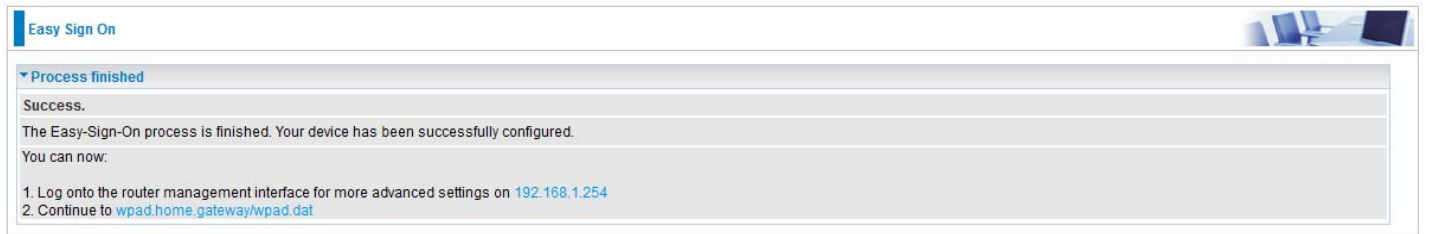
Parameters	
Wireless	<input checked="" type="checkbox"/> Enable
SSID	<input type="text" value="wlan-ap"/>
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

At the bottom of the configuration area, there is a 'Continue' button.



The screenshot shows the 'Easy Sign On' interface with the 'Wireless' section expanded. 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' interface with the 'Process finished' section expanded. The main content area displays the following text:

**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)

# 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 xDSL2+ Router!**

Once you have logged on to your BiPAC 8700NEXL R2 Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Status** (Summary, WAN, Statistics, Bandwidth Usage, 3G/4G LTE Status, Route, ARP, DHCP, Log)
- **Quick Start** (Quick Start)
- **Configuration** (LAN, Wireless, WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)
- **Advanced Setup** (Routing, DNS, Static ARP, UPnP, Certificate, Multicast, Management, Diagnostics)



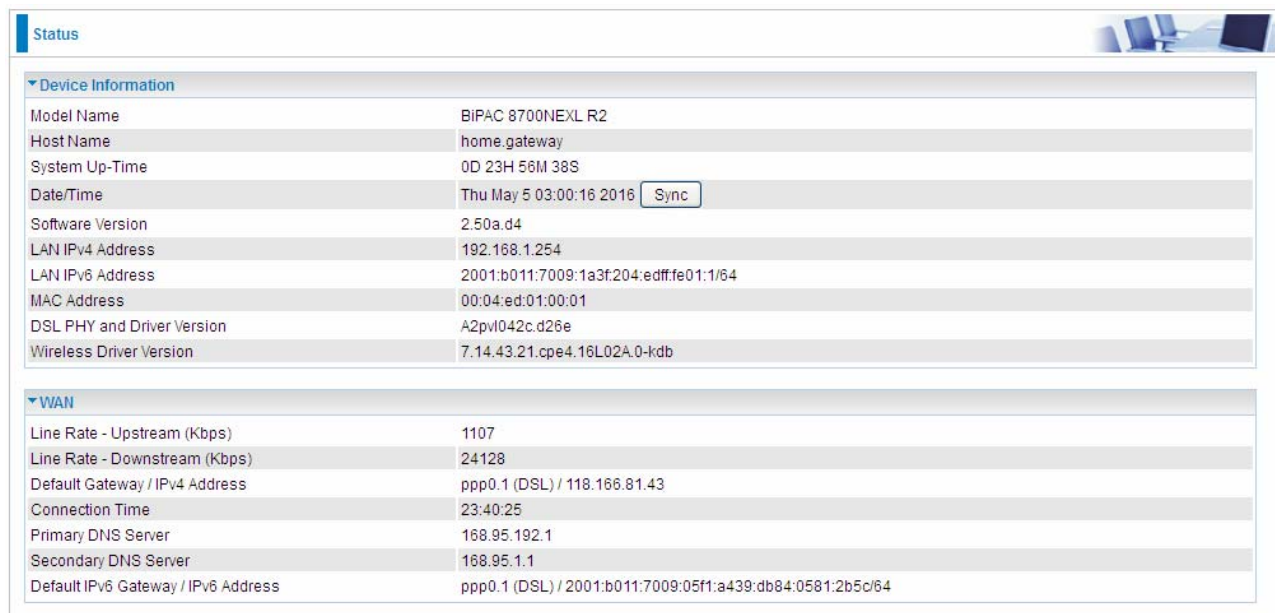
# Status

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/4G LTE Status](#), [Route](#), [ARP](#), [DHCP](#) and [Log](#) subsections are included.

▼ Status
▪ Summary
▪ WAN
▶ Statistics
▶ Bandwidth Usage
▪ 3G/4G LTE Status
▪ Route
▪ ARP
▪ DHCP
▶ Log
• Quick Start
▶ Configuration
▶ Advanced Setup

# Summary

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



The screenshot shows a web interface for a router's status page. It is divided into two main sections: 'Device Information' and 'WAN'. The 'Device Information' section lists various system parameters such as Model Name, Host Name, System Up-Time, Date/Time, Software Version, LAN IPv4 and IPv6 addresses, MAC Address, DSL PHY and Driver Version, and Wireless Driver Version. The 'WAN' section displays connection statistics and settings, including Line Rate (Upstream/Downstream), Default Gateway, Connection Time, DNS Servers, and Default IPv6 Gateway.

Device Information	
Model Name	BIPAC 8700NEXL R2
Host Name	home.gateway
System Up-Time	0D 23H 56M 38S
Date/Time	Thu May 5 03:00:16 2016 <input type="button" value="Sync"/>
Software Version	2.50a.d4
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2001:b011:7009:1a3f:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pvl042c.d26e
Wireless Driver Version	7.14.43.21.cpe4.16L02A.0-kdb

WAN	
Line Rate - Upstream (Kbps)	1107
Line Rate - Downstream (Kbps)	24128
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 118.166.81.43
Connection Time	23:40:25
Primary DNS Server	168.95.192.1
Secondary DNS Server	168.95.1.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2001:b011:7009:05f1:a439:db84:0581:2b5c/64

## Device Information

**Model Name:** Displays the model name.

**Host Name:** Displays the name of the router.

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

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

**Software Version:** Firmware version.

**LAN IPv4 Address:** Displays the LAN IPv4 address.

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

**MAC Address:** Displays the MAC address.

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

**Wireless Driver Version:** Displays wireless driver version.

## WAN

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

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

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

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

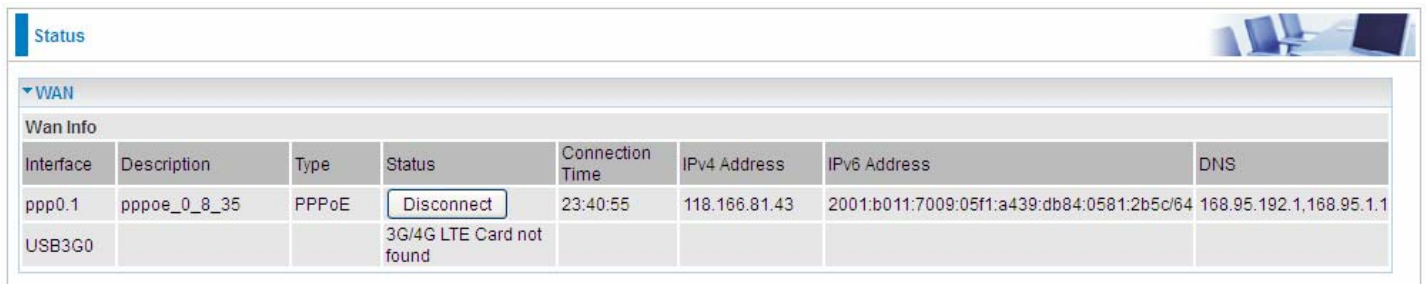
**Primary DNS Server:** Displays IPV4 address of Primary DNS Server.

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

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

# WAN

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



Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	23:40:55	118.166.81.43	2001:b011:7009:05f1:a439:db84:0581:2b5c/64	168.95.192.1,168.95.1.1
USB3G0			3G/4G LTE Card not found				

**Interface:** The WAN connection interface.

**Description:** The description of this connection.

**Type:** The protocol used by this connection.

**Status:** To disconnect or connect the link.

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

**IPv4 Address:** The WAN IPv4 Address the device obtained.

**IPv6 Address:** The WAN IPv6 Address the device obtained.

**DNS:** The DNS address the device obtained.

# Statistics

## LAN

The table shows the statistics of LAN.

**Note:** P5 can be configured as EWAN, and when the device is in EWAN profile, there is no P5/EWAN interface as P5 is working as a WAN port.

LAN Statistics																
Interface	Received								Transmitted							
	Total				Multicast	Unicast	Broadcast	Total				Multicast	Unicast	Broadcast		
	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
P1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P4	18324245	86321	0	0	0	29294	54940	2087	10310169	62537	0	0	0	4619	57904	14
P5/EWAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wi0	0	0	0	0	0	0	0	0	11873874	34545	0	0	0	32493	0	2398

(DSL)

LAN Statistics																
Interface	Received								Transmitted							
	Total				Multicast	Unicast	Broadcast	Total				Multicast	Unicast	Broadcast		
	Bytes	Packets	Errors	Drops	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Packets	Packets	Packets		
P1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P2	77435845	362447	0	0	134637	198486	29324	113085406	224505	0	0	11191	213164	150		
P3	197319	1929	0	0	347	1437	145	959634	1944	0	0	412	1440	92		
P4	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
wi0	165174	2135	0	0	1	2127	7	66771179	179679	0	0	137981	12289	29409		

(EWAN)

**Interface:** List each LAN interface. P1-P5 indicates the LAN interfaces (P5 can be configured as EWAN).

**Bytes:** Display the total Received and Transmitted traffic statistics in Bytes for each interface.

**Packets:** Display the total Received and Transmitted traffic statistics in Packets for each interface.

**Errors:** Display the total statistics of errors arising in Receiving or Transmitting data for each interface.

**Drops:** Display the total statistics of drops arising in Receiving or Transmitting data for each interface.

**Multicast (packets):** Display the Received and Transmitted multicast Packets for each interface.

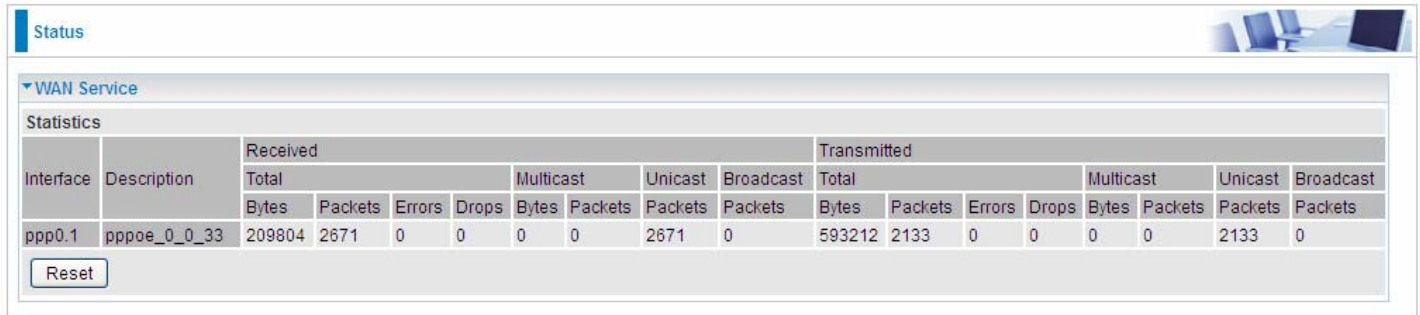
**Unicast (packets):** Display the Received and Transmitted unicast Packets for each interface.

**Broadcast (packets):** Display the Received and Transmitted broadcast Packets for each interface.

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

## WAN Service

The table shows the statistics of WAN.



The screenshot shows a web interface with a 'Status' tab and a 'WAN Service' section. Under 'WAN Service', there is a 'Statistics' table. The table has columns for 'Interface' and 'Description', and two main sections: 'Received' and 'Transmitted'. Each section has sub-columns for 'Total', 'Multicast', 'Unicast', and 'Broadcast'. The 'Total' sub-section further breaks down into 'Bytes', 'Packets', 'Errors', and 'Drops'. A 'Reset' button is located below the table.

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
ppp0.1	pppoe_0_0_33	209804	2671	0	0	0	0	2671	0	593212	2133	0	0	0	0	2133	0

**Interface:** Display the connection interface.

**Description:** The description for the connection.

**Bytes:** Display the Received and Transmitted traffic statistics in Bytes for every WAN interface.

**Packets:** Display the Received and Transmitted traffic statistics in Packests for every WAN interface.

**Errors:** Display the statistics of errors arising in Receiving or Transmitting data for every WAN interface.

**Drops:** Display the statistics of drops arising in Receiving or Transmitting data for every WAN interface.

**Multicast (packets):** Display the Received and Transmitted multicast Packets for every WAN interface.

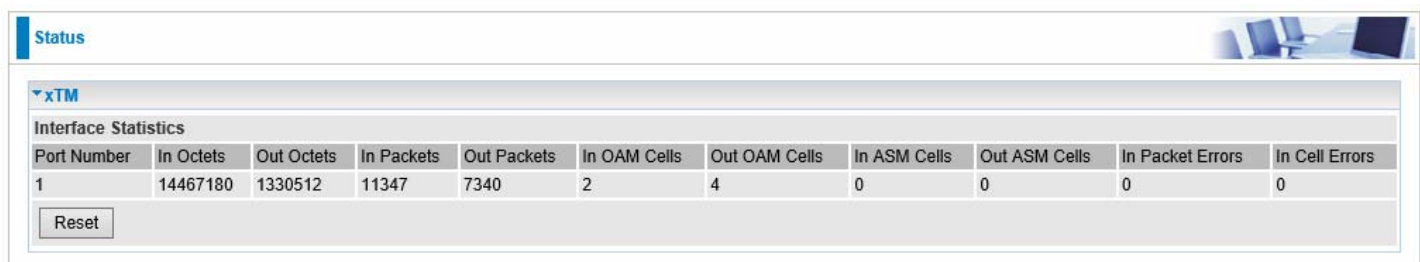
**Unicast (packets):** Display the Received and Transmitted unicast Packets for every WAN interface.

**Broadcast (packets):** Display the Received and Transmitted broadcast Packets for every WAN interface.

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

## xTM

The Statistics-xTM screen displays all the xTM statistics



The screenshot shows a web interface with a 'Status' tab and an 'xTM' section. Under 'xTM', there is an 'Interface Statistics' table. The table has columns for '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', and 'In Cell Errors'. A 'Reset' button is located below the table.

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

**Port Number:** Shows number of the port for xTM.

**In Octets:** Number of received octets over the interface.

**Out Octets:** Number of transmitted octets over the interface.

**In Packets:** Number of received packets over the interface.

**Out Packets:** Number of transmitted packets over the interface.

**In OAM Cells:** Number of OAM cells received.

**Out OAM Cells:** Number of OAM cells transmitted.

**In ASM Cells:** Number of ASM cells received.


**Out ASM Cells:** Number of ASM cells transmitted.

**In Packet Errors:** Number of received packets with errors.

**In Cell Errors:** Number of received cells with errors.

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

## xDSL

Status 

▼ xDSL

xDSL		
Mode	ADSL_2plus	
Traffic Type	ATM	
Status	Up	
Link Power State	L0	
	Downstream	Upstream
Line Coding (Trellis)	On	On
SNR Margin (dB)	6.4	6.0
Attenuation (dB)	2.0	0.7
Output Power (dBm)	17.6	2.6
Attainable Rate (Kbps)	24452	1104
Rate (Kbps)	24328	1071
MSGc (# of bytes in overhead channel message)	58	66
B (# of bytes in Mux Data Frame)	254	33
M (# of Mux Data Frames in FEC Data Frame)	1	1
T (Mux Data Frames over sync bytes)	3	1
R (# of check bytes in FEC Data Frame)	0	0
S (ratio of FEC over PMD Data Frame length)	0.3349	0.9855
L (# of bits in PMD Data Frame)	6090	276
D (interleaver depth)	1	1
Delay (msec)	0	0
INP (DMT symbol)	0.00	0.00
Super Frames	0	0
Super Frame Errors	39	3
RS Words	0	1722778
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	1215	2
OCD Errors	15	0
LCD Errors	15	0
Total Cells	420733366	402229838
Data Cells	878484	358776
Bit Errors	67717	0
Total ES	30	3
Total SES	0	0
Total UAS	23	23

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

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

**Status:** Show the status of DSL link.

**Link Power State:** Show link output power state.

**Line Coding (Trellis):** Trellis on/off.

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

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

**Output Power (dBm):** Show the output power.

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

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

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

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

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

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

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

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

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

**D (interleaver depth):** Show the interleaver depth.

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

**INP (DMT symbol):** Show the DMT symbol.

**Super Frames:** The total number of super frames.

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

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

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

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

**HEC Errors:** Total number of Header Error Checksum errors.

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

**LCD Errors:** Total number of Loss of Cell Delineation.

**Total Cells:** Total number of cells.

**Data Cells:** Total number of data cells.

**Bit Errors:** Total number of bit errors.

**Total ES:** Total Number of Errored Seconds.

**Total SES:** Total Number of Severely Errored Seconds.

**Total UAS:** Total Number of Unavailable Seconds.

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

**ADSL BER Test -- Start**

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

Tested Time (sec)

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

**ADSL BER Test -- Running**

The xDSL BER test is in progress.

Connection Speed 27447 Kbps

The test will run for 20 seconds

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

**ADSL BER Test -- Result**

The ADSL BER test completed successfully.

Test Time 20 seconds

Total Transferred Bits 0x000000001DA1F500

Error Ratio 0.00e+00

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



## Bandwidth Usage

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

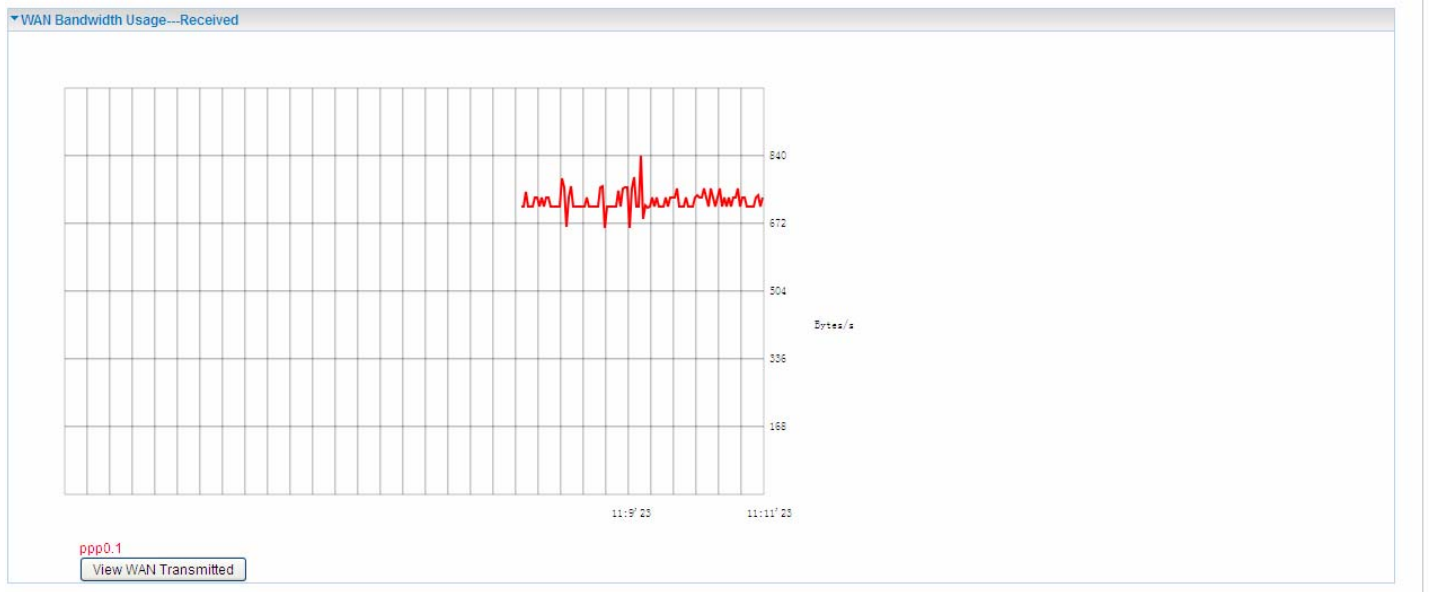
### LAN

**Note:** P5 can be configured as EWAN, and when the device is in EWAN profile, there is no P5/EWAN interface as P5 is working as a WAN port.

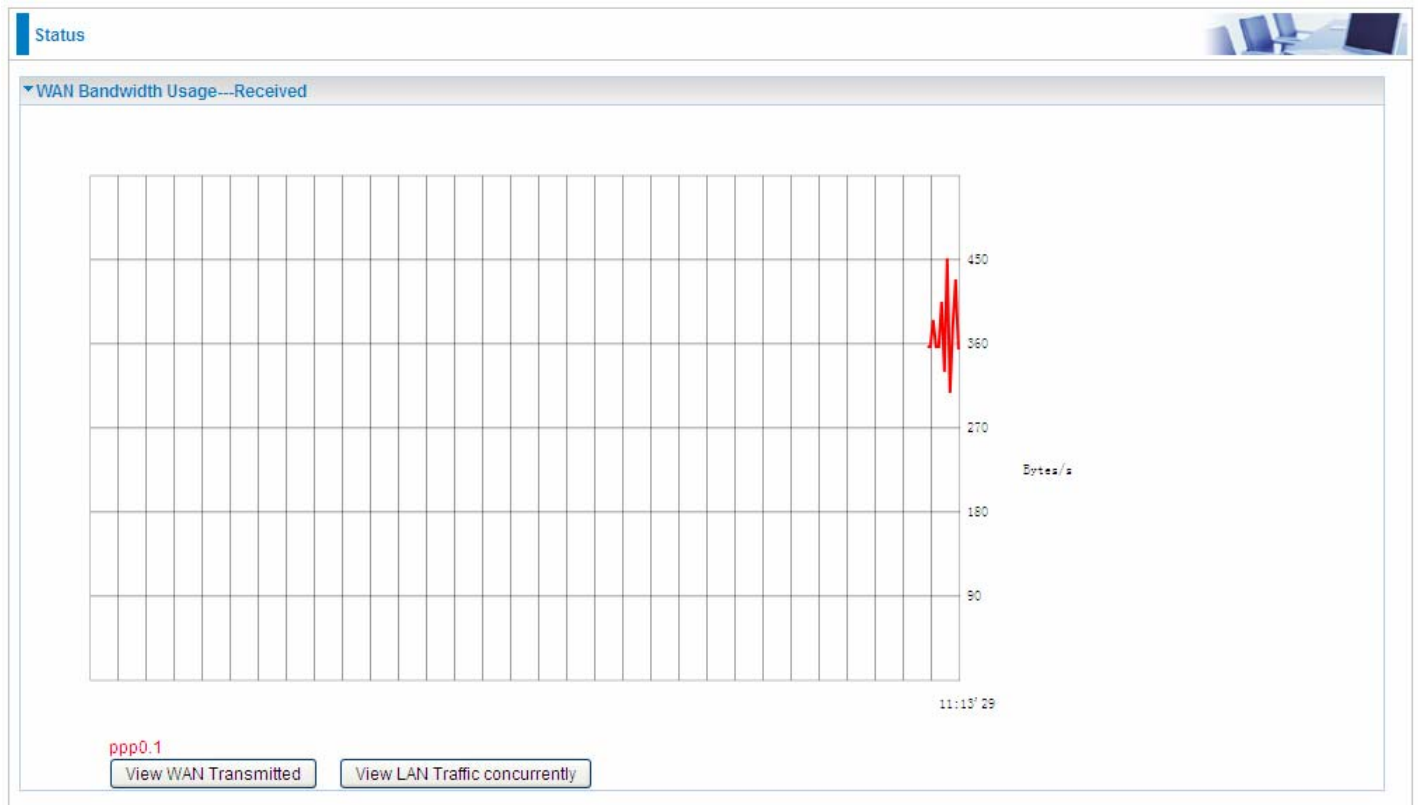


Press **View LAN Transmitted** button to change the diagram to the statistics of the LAN Transmitted Bytes. (**Note:** P4 means Ethernet port #4, and the traffic information of the port #4 is identified with orange, the same color with P4 in the diagram; other ports all take the same mechanism.)

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

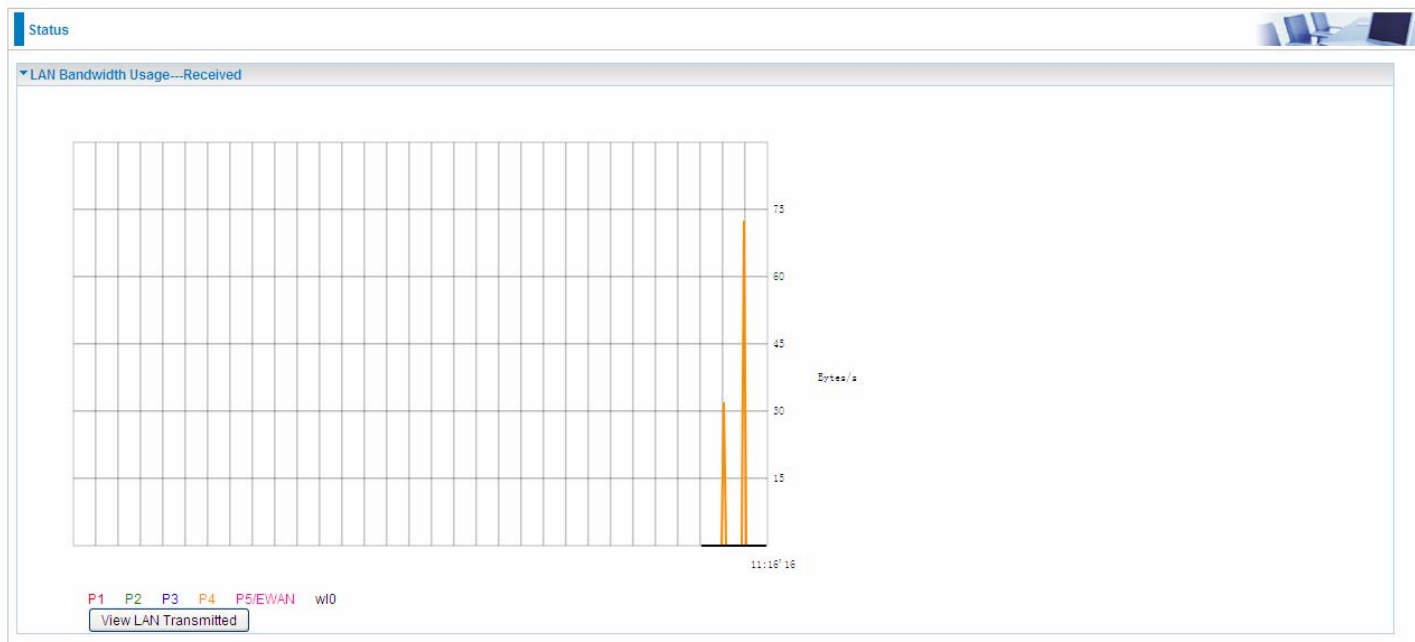


## WAN Service

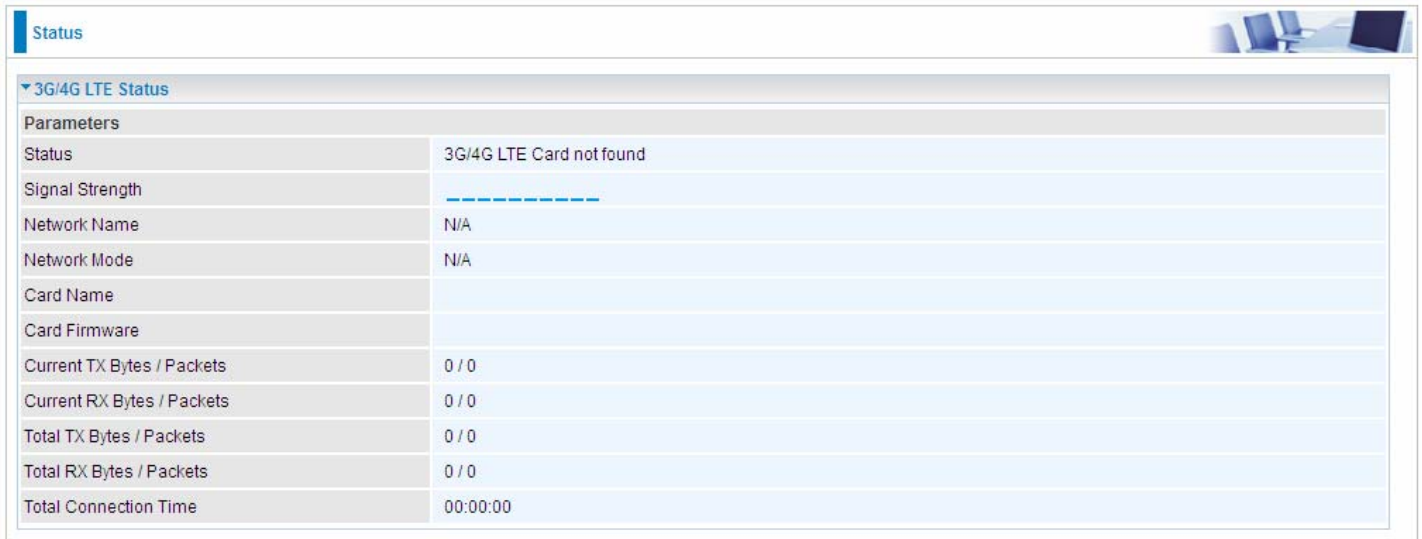


Press **View WAN Transmitted** button to change the diagram to the statistics of the WAN Transmitted Bytes.

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



# 3G/4G LTE Status



Parameters	
Status	3G/4G LTE Card not found
Signal Strength	-----
Network Name	N/A
Network Mode	N/A
Card Name	
Card Firmware	
Current TX Bytes / Packets	0 / 0
Current RX Bytes / Packets	0 / 0
Total TX Bytes / Packets	0 / 0
Total RX Bytes / Packets	0 / 0
Total Connection Time	00:00:00

**Status:** The current status of the 3G/4G LTE connection.

**Signal Strength:** The signal strength bar and dBm value indicates the current 3G/4G-LTE signal strength. The front panel 3G/4G LTE Signal Strength LED indicates the signal strength as well.

**Network Name:** The name of the 3G/4G LTE network the router is connecting to.

**Network Mode:** The current operation mode for 3G/4G LTE module, it depends on service provider and card's limitation, GSM or UMTS.

**Card Name:** Given a name for the embedded 3G/4G LTE module.


**Card Firmware:** Current used FW in the 3G/4G LTE module.

**Current Received (RX) /Transmitted (TX) Bytes:** Current Rx/TX (receive/transmit) packets in Byte

**Total Received (RX) /Transmitted (TX) Bytes:** The total Rx/TX (receive/transmit) packets in Byte

**Total Connection Time:** The total of 3G/4G LTE dongle connection time since the 3G/4G LTE is up and running

# 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
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe_0_0_33	ppp0.1
168.95.98.254	0.0.0.0	255.255.255.255	UH	0	pppoe_0_0_33	ppp0.1
168.95.192.1	0.0.0.0	255.255.255.255	UH	0	pppoe_0_0_33	ppp0.1
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

**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.

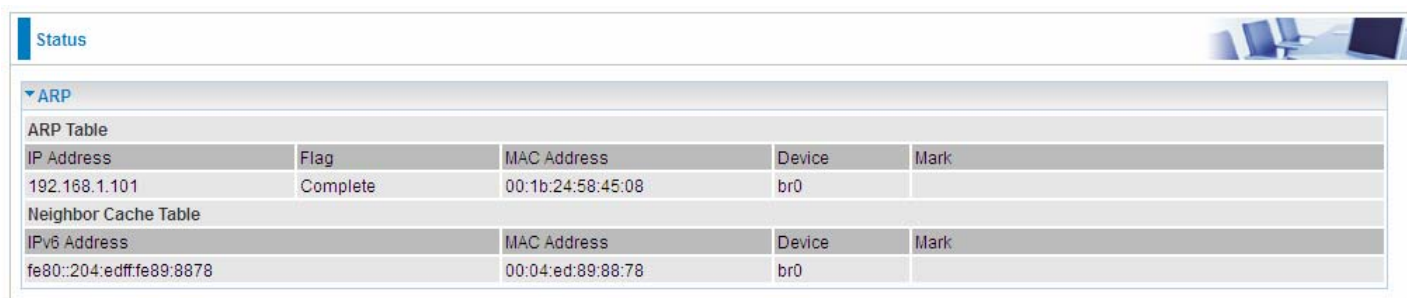
**Metric:** Display the number of hops counted as the Metric of the route.

**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.



The screenshot shows a web interface with a 'Status' tab. Underneath, there is a section for 'ARP' which contains two tables. The first table is the 'ARP Table' and the second is the 'Neighbor Cache Table'. Both tables have columns for IP/IPv6 Address, Flag, MAC Address, Device, and Mark.

IP Address	Flag	MAC Address	Device	Mark
192.168.1.101	Complete	00:1b:24:58:45:08	br0	

IPv6 Address	MAC Address	Device	Mark
fe80::204:edff:fe89:8878	00:04:ed:89:88:78	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".

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

## 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".

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

# DHCP

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



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

**Host Name:** The Host Name of DHCP client.

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

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

**Expires in:** Show the remaining time after registration.

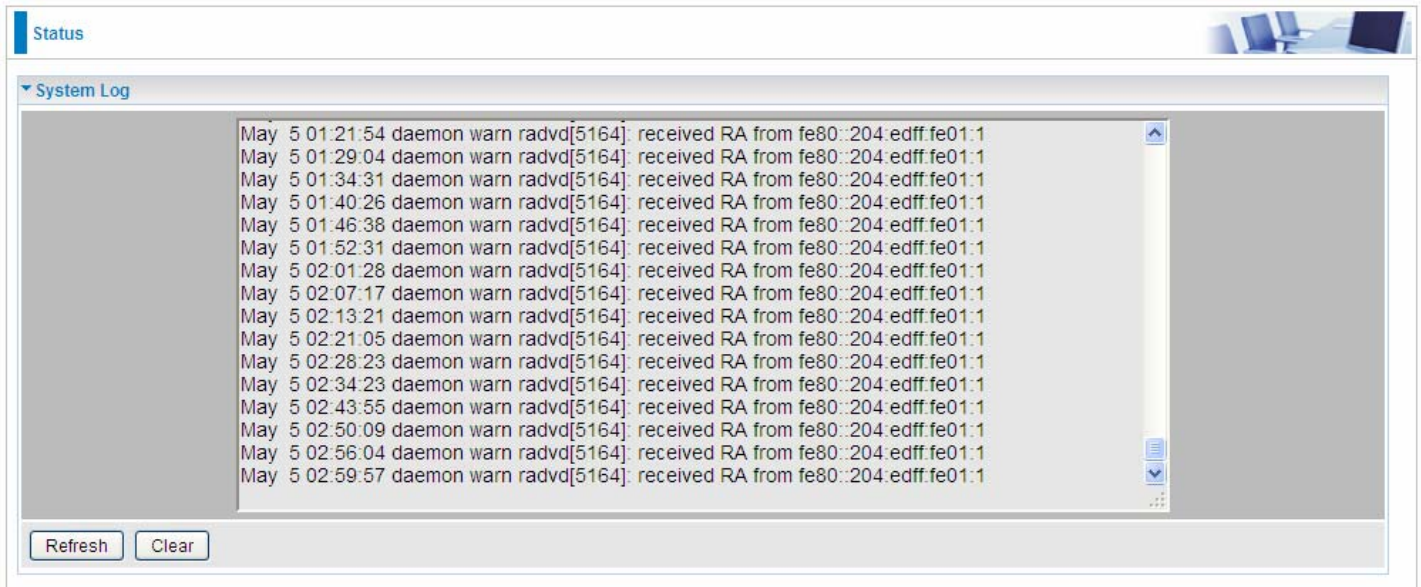
**Mark:** Show clearly the SSID (WLAN) the device is in.



# 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.



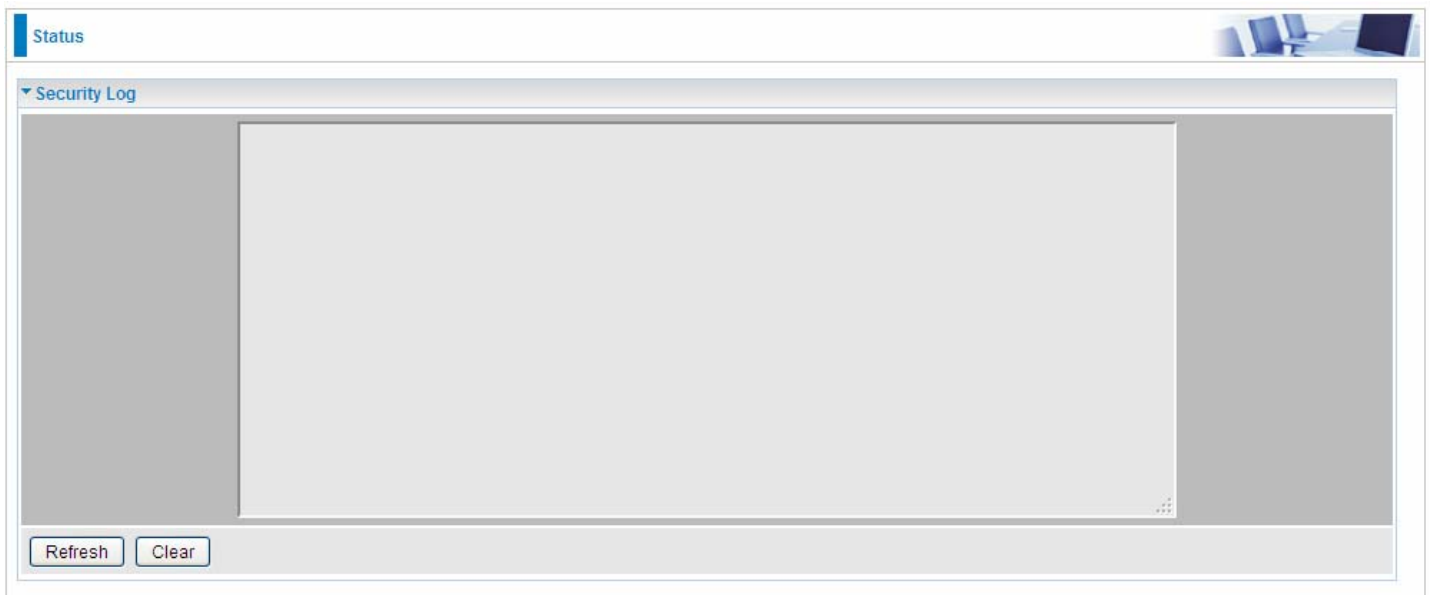
The screenshot shows a web interface for viewing system logs. At the top left, there is a 'Status' tab. Below it, a 'System Log' section is expanded, displaying a list of log entries. Each entry follows the format: 'May 5 01:21:54 daemon warn radvd[5164]: received RA from fe80::204:edff:fe01:1'. The list contains 17 entries. At the bottom of the log area, there are two buttons: 'Refresh' and 'Clear'. On the right side of the log area, there are navigation icons for scrolling and a refresh icon.

**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 security log.

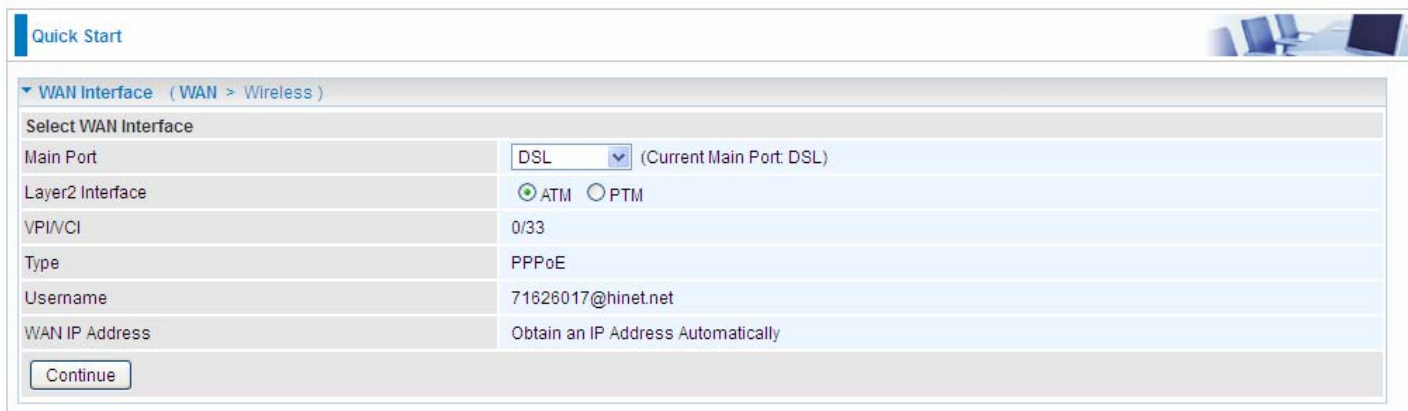
**Clear:** Click to clear the current log from the screen.

# Quick Start

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

## DSL mode (ADSL mode, please choose ATM; VDSL, please choose PTM)

Here take ADSL for example.



Quick Start

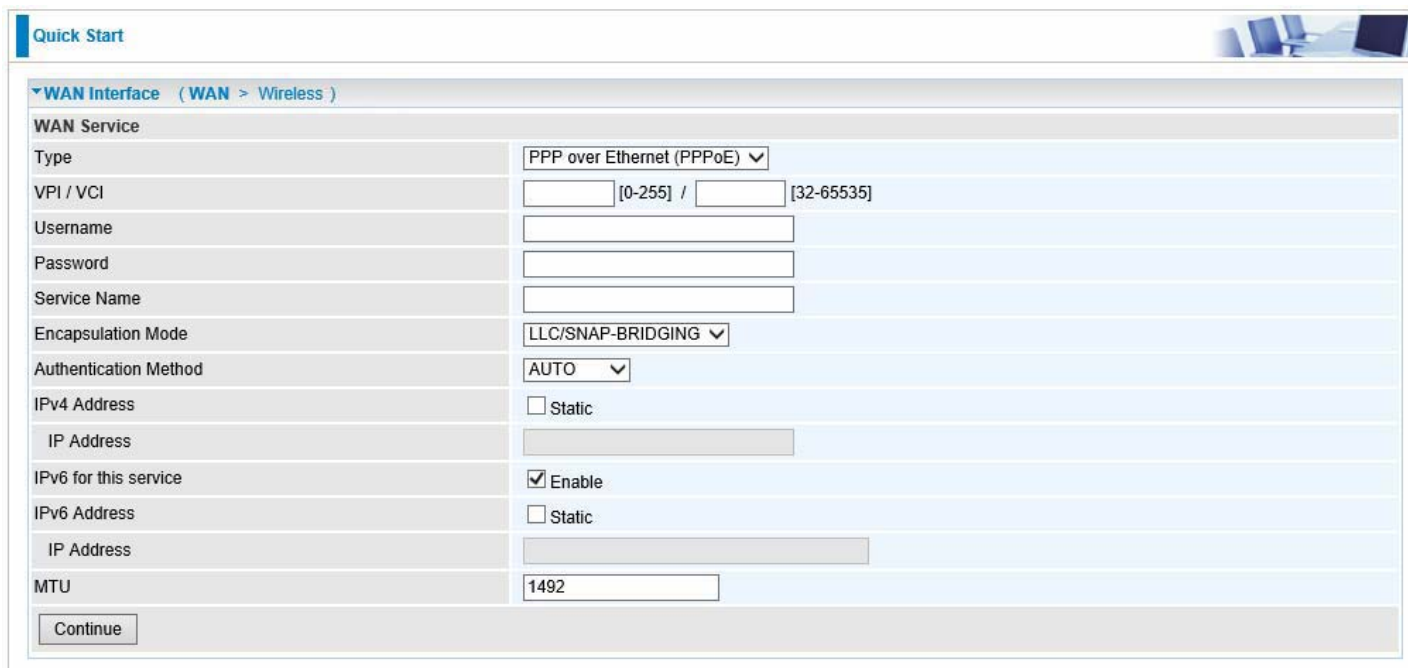
WAN Interface (WAN > Wireless)

Select WAN Interface

Main Port	DSL (Current Main Port: DSL)
Layer2 Interface	<input checked="" type="radio"/> ATM <input type="radio"/> PTM
VPI/VCI	0/33
Type	PPPoE
Username	71626017@hinet.net
WAN IP Address	Obtain an IP Address Automatically

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	<input type="checkbox"/> Static
IP Address	
IPv6 for this service	<input checked="" type="checkbox"/> Enable
IPv6 Address	<input type="checkbox"/> 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.

#### 4. Wait while the device is configured.

Quick Start

▼ WAN Interface ( WAN > Wireless )

Please wait while the device is configured.

#### 5 WAN port configuration is successful.

Quick Start

▼ WAN Interface ( WAN > Wireless )

Congratulations !  
Your WAN port has been successfully configured.

Next to Wireless

#### 6. 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).

Quick Start

▼ Wireless ( WAN > Wireless )

Parameters

Wireless	<input checked="" type="checkbox"/> Enable
SSID	<input type="text" value="wlan-ap"/>
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Continue

Quick Start

▼ WAN Interface ( WAN > Wireless )

Please wait while the device is configured.

#### 7. Success.


Quick Start

▼ Process finished

Success.

## Ethernet mode

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



Quick Start

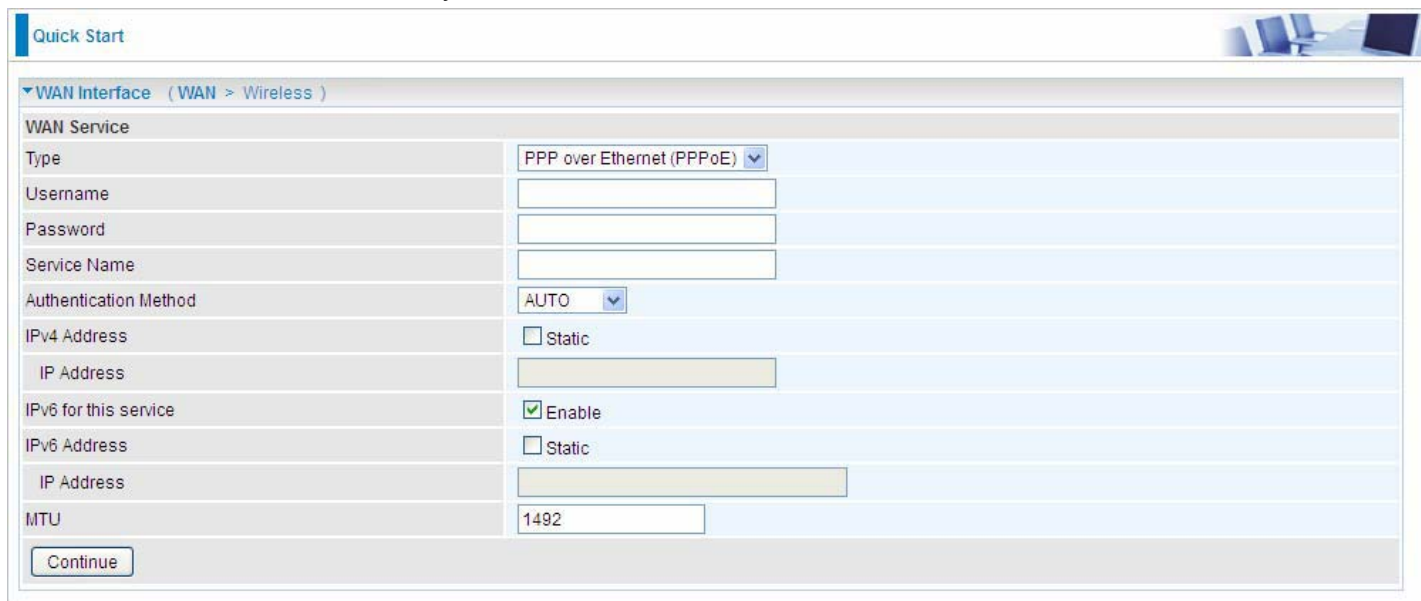
WAN Interface (WAN > Wireless)

Select WAN Interface

Main Port: Ethernet (Current Main Port: DSL)

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: [Text Field]

Password: [Text Field]

Service Name: [Text Field]

Authentication Method: AUTO

IPv4 Address:  Static

IP Address: [Text Field]

IPv6 for this service:  Enable

IPv6 Address:  Static

IP Address: [Text Field]

MTU: 1492

Continue

3. Wait while the device is configured.

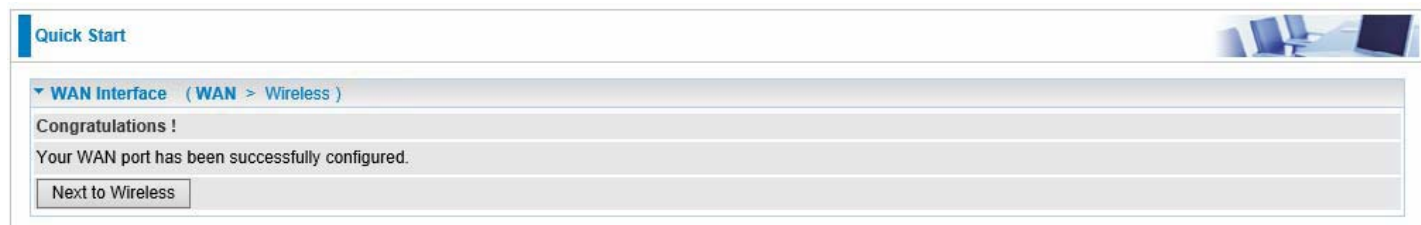


Quick Start

WAN Interface (WAN > Wireless > VOIP)

Please wait while the device is configured.

4. WAN port configuration is successful.



Quick Start


WAN Interface (WAN > Wireless)

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 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).

Quick Start 

▼ **Wireless** ( WAN > Wireless )

Parameters

Wireless	<input checked="" type="checkbox"/> Enable
SSID	<input type="text" value="wlan-ap"/>
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Quick Start 

▼ **WAN Interface** ( WAN > Wireless )

Please wait while the device is configured.

## 6. Success.

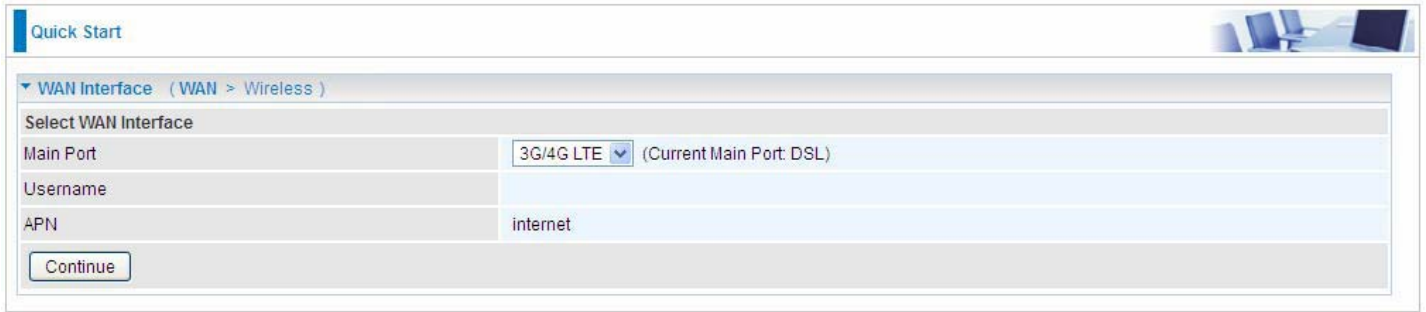
Quick Start 

▼ **Process finished**

Success.

## 3G/4G LTE

1. Select **3G/4G LTE**, press **Continue** to go on to next step.



Quick Start

WAN Interface (WAN > Wireless)

Select WAN Interface

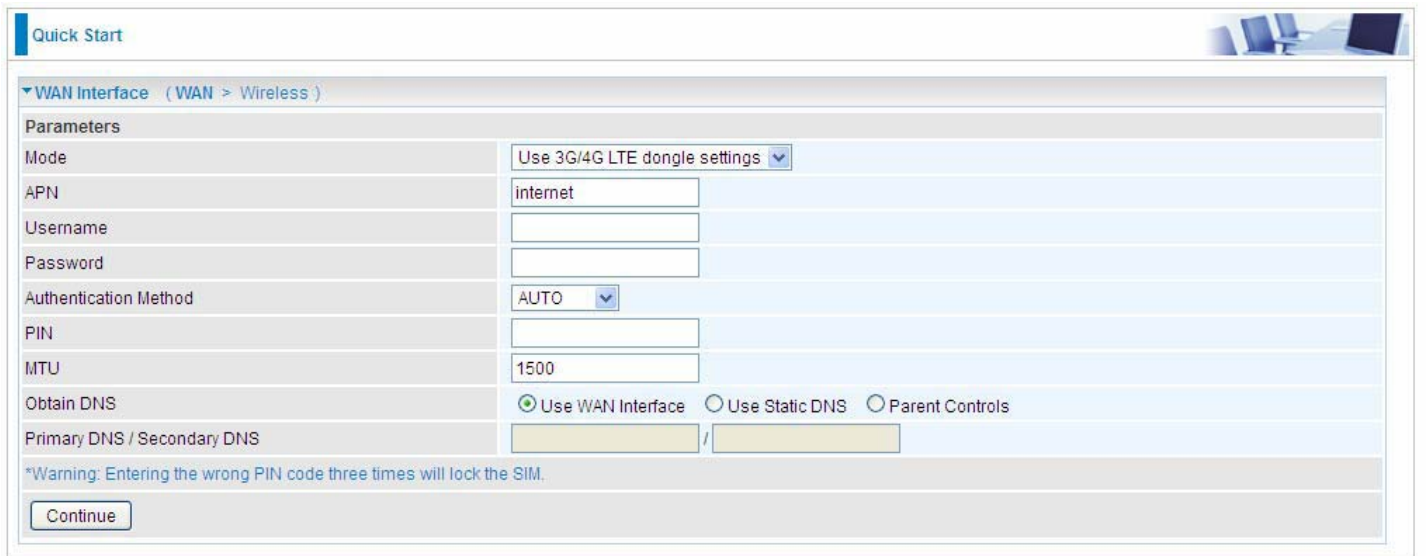
Main Port: 3G/4G LTE (Current Main Port: DSL)

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/4G LTE dongle settings

APN: internet

Username:

Password:

Authentication Method: AUTO

PIN:

MTU: 1500

Obtain DNS:  Use WAN Interface  Use Static DNS  Parent Controls

Primary DNS / Secondary DNS: /

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

Continue

3. Wait while the device is configured.

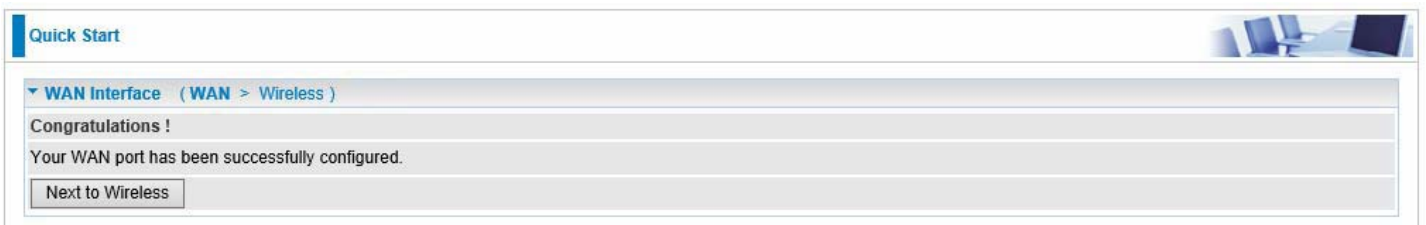


Quick Start

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 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).

Quick Start 

▼ **Wireless** ( WAN > Wireless )

Parameters

Wireless	<input checked="" type="checkbox"/> Enable
SSID	<input type="text" value="wlan-ap"/>
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Quick Start 

▼ **WAN Interface** ( WAN > Wireless )

Please wait while the device is configured.

## 6. Success.

Quick Start 

▼ **Process finished**

Success.



# 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
▶ VPN
▶ Advanced Setup

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 'Configuration' window for LAN settings. It includes sections for 'Parameters' and 'DHCP Server'. The 'Parameters' section has 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), IGMP LAN to LAN Multicast (unchecked), and LAN side firewall (unchecked). The 'DHCP Server' section has fields for DHCP Server (Enabled), Start IP Address (192.168.1.100), End IP Address (192.168.1.199), Leased Time (24), Option 66 (unchecked), and Use Router's setting as DNS Server (checked). There are also fields for Primary and Secondary DNS servers. Below these is a 'Static IP Lease List' table with columns for Host Label, MAC Address, IP Address, Remove, and Edit. At the bottom, there is an 'IP Alias' section with fields for IP Alias (unchecked), IP Address, and Subnet Mask. 'Apply' and 'Cancel' buttons are at the bottom left.

### 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.

**IGMP LAN to 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 wants to get IGMP snooping enabled, then this LAN-to-LAN multicast feature should be enabled.

**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
Use Router's setting as DNS Server	<input checked="" type="checkbox"/>
Primary DNS server	
Secondary DNS server	

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

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

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

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

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

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

### ❸ DHCP Server Relay

DHCP Server	
DHCP Server	DHCP Server Relay
DHCP Server IP Address	


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

## Static IP List

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

Static IP Lease List				
Host Label	MAC Address	IP Address	Remove	Edit
<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"/>	<input type="button" value="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"/>

**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.

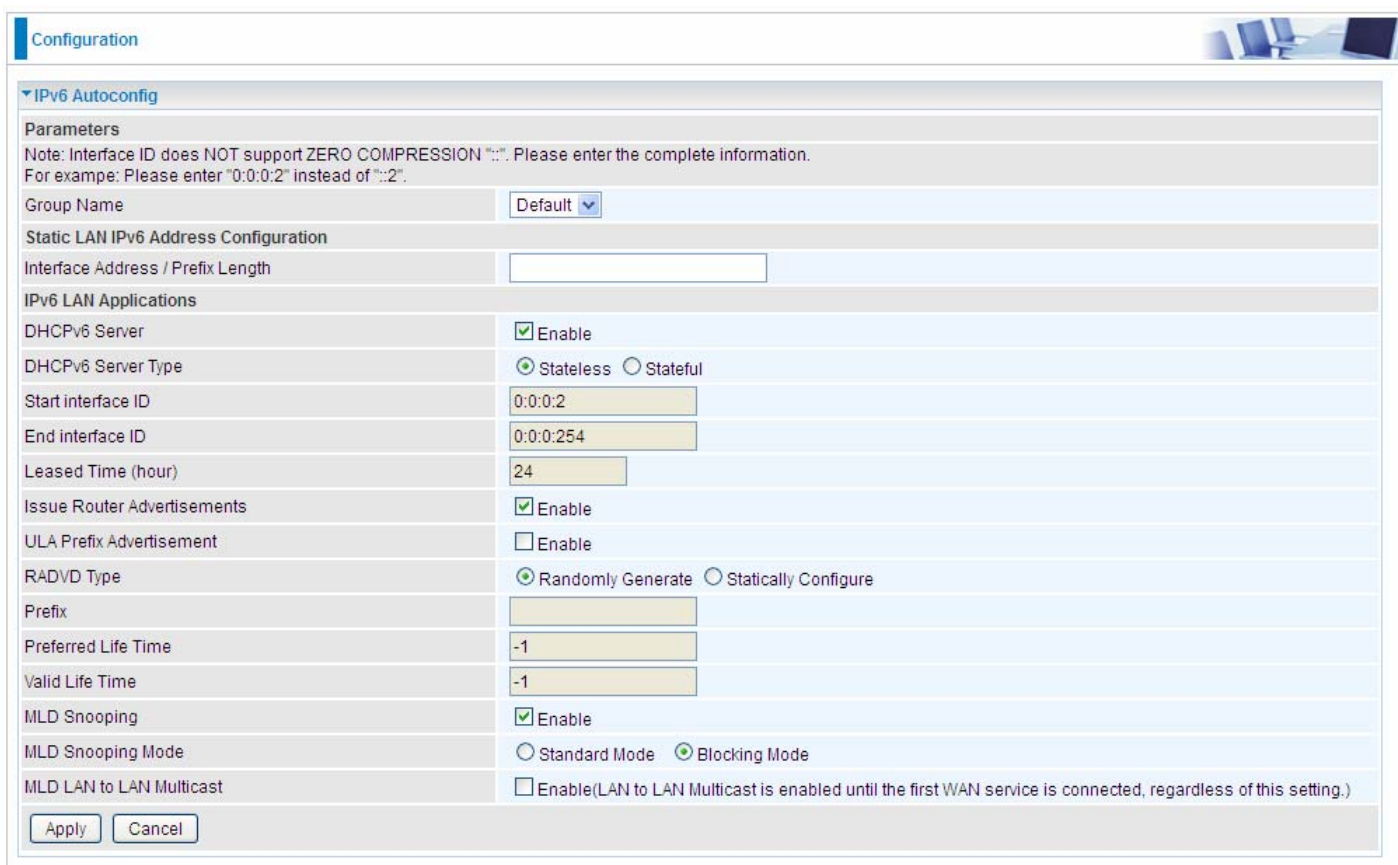
Click **Apply** to apply your settings.

## 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.



The screenshot shows a configuration page titled "Configuration" with a sub-section for "IPv6 Autoconfig". It includes a note about interface ID formatting, a "Group Name" dropdown set to "Default", and a "Static LAN IPv6 Address Configuration" section with an empty input field. Below that is the "IPv6 LAN Applications" section, which contains various settings:

Parameter	Value
DHCPv6 Server	<input checked="" type="checkbox"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start interface ID	0:0:0:2
End interface ID	0:0:0:254
Leased Time (hour)	24
Issue Router Advertisements	<input checked="" type="checkbox"/> Enable
ULA Prefix Advertisement	<input type="checkbox"/> Enable
RADVD Type	<input checked="" type="radio"/> Randomly Generate <input type="radio"/> Statically Configure
Prefix	
Preferred Life Time	-1
Valid Life Time	-1
MLD Snooping	<input checked="" type="checkbox"/> Enable
MLD Snooping Mode	<input type="radio"/> Standard Mode <input checked="" type="radio"/> Blocking Mode
MLD LAN to LAN Multicast	<input type="checkbox"/> Enable(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

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

**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.

**MLD LAN to 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

## 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.

- ① 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**: P5 can be configured as EWAN, and when the device is in EWAN profile, there is no P5/EWAN interface as P5 is working as a WAN port.)

Configuration

▼ Interface Grouping

Groups Isolation  Enable

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	P1	
			P2	
			P3	
			P4	
			wlan-ap	
		P5/EWAN		

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

Click **Add** to add groups.

Configuration

▼ Interface grouping Configuration

Parameters

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

Group Name

Grouped WAN Interfaces

Available WAN Interfaces

pppoe\_0\_8\_35/ppp0.1

Grouped LAN Interfaces

Available LAN Interfaces

P1  
P2  
P3  
P4  
wlan-ap  
P5/EWAN

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.

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

Configuration

Interface Grouping

Groups Isolation Enable

Apply

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default	<input type="checkbox"/>		P1	
			P3	
			P4	
			wlan-ap	
test	<input checked="" type="checkbox"/>	ppp0.1	P5/EWAN	
			P2	

Add Remove

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

Configuration

Interface Grouping

Groups Isolation Enable

Apply

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default	<input type="checkbox"/>		P1	
			P3	
			P4	
			wlan-ap	
test	<input checked="" type="checkbox"/>	ppp0.1	P5/EWAN	
			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.

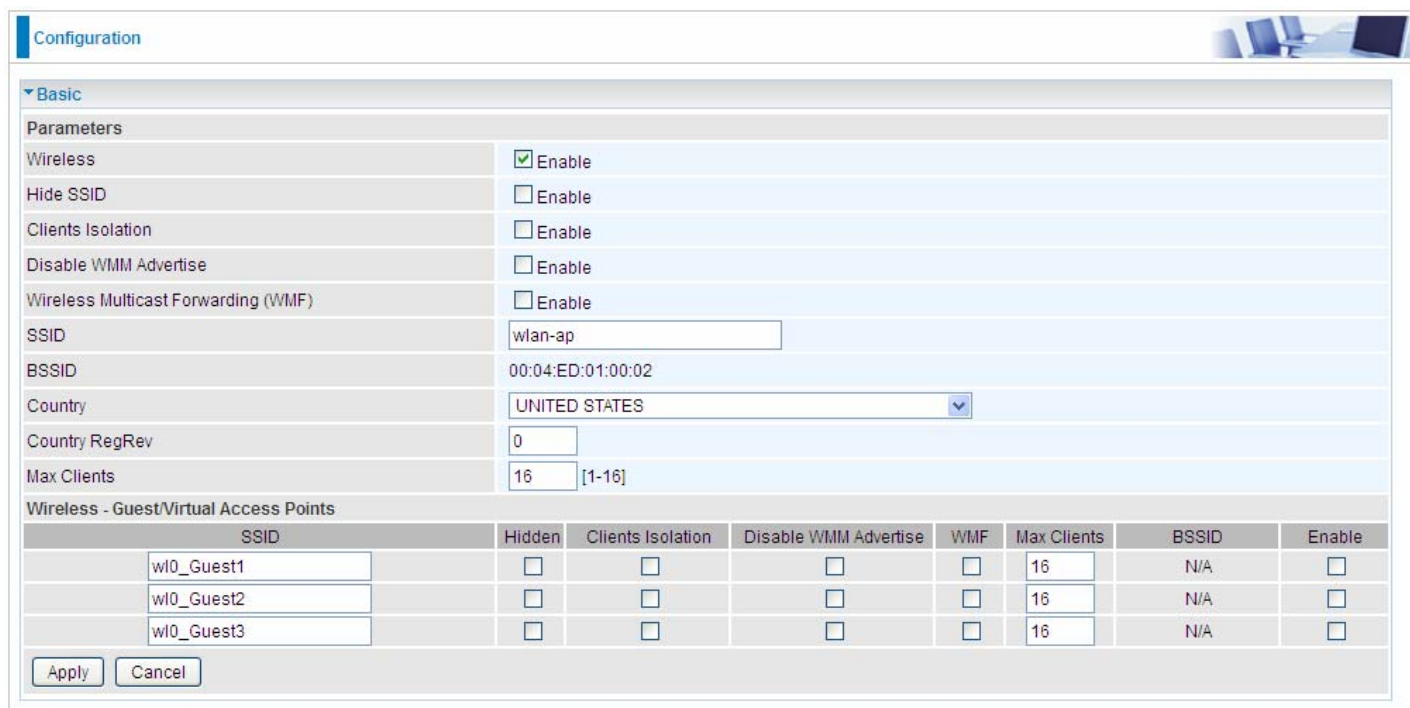
# Wireless

This section provides you ways to configure wireless access. The BiPAC 8700NEXL R2 supports wireless on the 2.4GHz for users. This part has sub-items as [Basic](#), [Security](#), [MAC Filter](#), [Wireless Bridge](#), [Advanced](#), [Station Info](#) and [Schedule Control](#) here.

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

## Basic

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



The screenshot shows the 'Configuration' page for a wireless access point. The 'Basic' section is expanded, showing the following parameters:

- Wireless:  Enable
- Hide SSID:  Enable
- Clients Isolation:  Enable
- Disable WMM Advvertise:  Enable
- Wireless Multicast Forwarding (WMF):  Enable
- SSID: wlan-ap
- BSSID: 00:04:ED:01:00:02
- Country: UNITED STATES
- Country RegRev: 0
- Max Clients: 16 [1-16]

Below the parameters is a table for 'Wireless - Guest/Virtual Access Points':

SSID	Hidden	Clients Isolation	Disable WMM Advvertise	WMF	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"/>

At the bottom of the configuration page are 'Apply' and 'Cancel' buttons.

**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 Advvertise:** Stop the router from 'advertising' its Wireless Multimedia (WMM) functionality, which provides basic quality of service for time-sensitive applications (e.g. VoIP, Video). Check to disable or enable this function.

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

**SSID:** The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security purpose, change the default wlan-ap 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

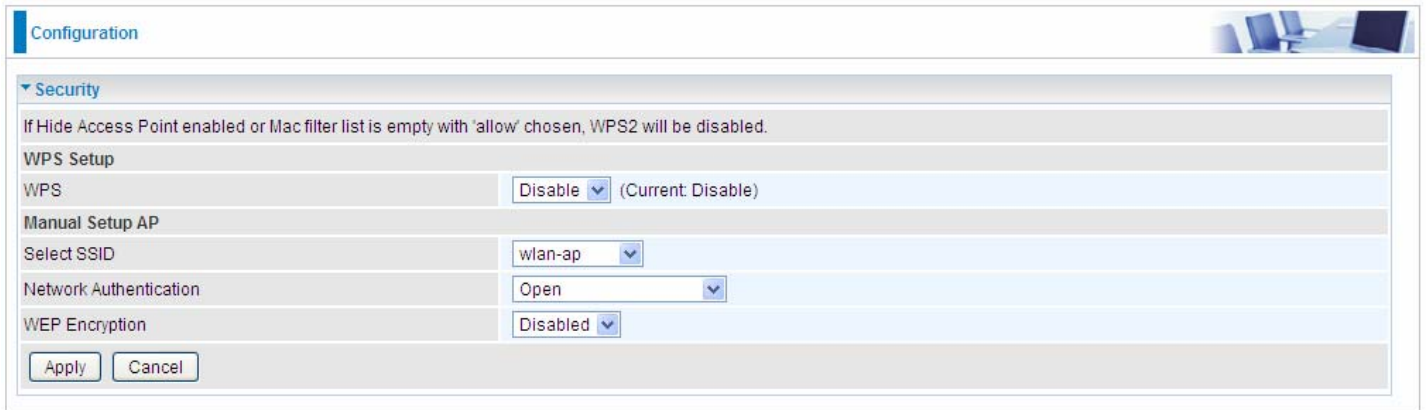
but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing 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.



The screenshot shows a web interface for configuring wireless security. The 'Security' section is expanded, showing a warning: 'If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.' Below this, the 'WPS Setup' section has 'WPS' set to 'Disable' (Current: Disable). The 'Manual Setup AP' section has 'Select SSID' set to 'wlan-ap', 'Network Authentication' set to 'Open', and 'WEP Encryption' set to 'Disabled'. 'Apply' and 'Cancel' buttons are at the bottom.

### Note:

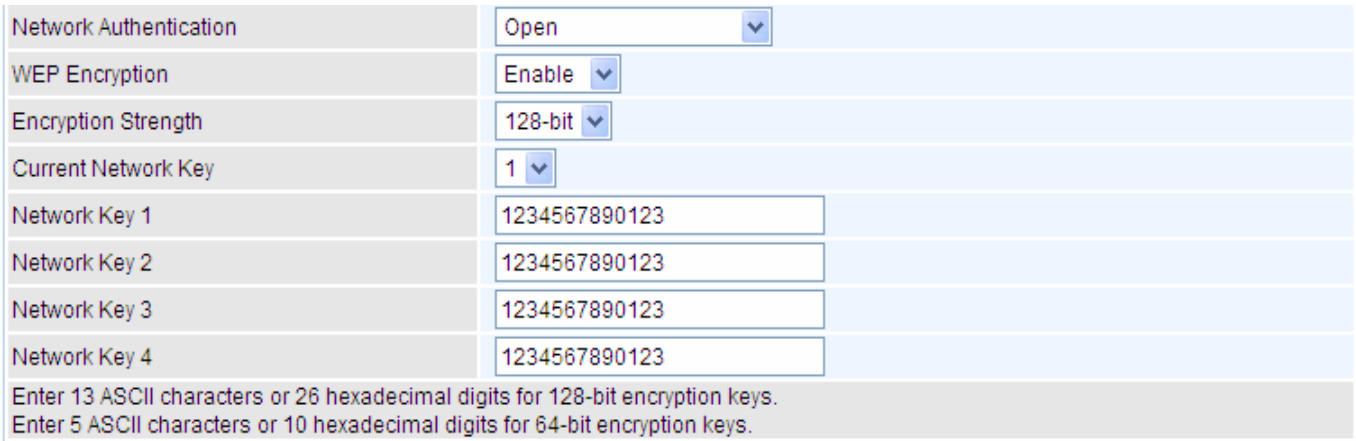
The WPS feature will also be unavailable when the security setting is not WPA2 PSK or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

## Manual Setup AP

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

### Network Authentication

#### ① Open



The screenshot shows the 'Network Authentication' configuration page. The 'Network Authentication' dropdown is set to 'Open'. Below it, 'WEP Encryption' is set to 'Enable', 'Encryption Strength' is set to '128-bit', and 'Current Network Key' is set to '1'. There are four text input fields for 'Network Key 1', 'Network Key 2', 'Network Key 3', and 'Network Key 4', all containing the value '1234567890123'. A note at the bottom states: '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 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 WPA2

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

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

**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 WPA2-PSK

Network Authentication	WPA2 -PSK
Protected Management Frames	Disable
WPA/WAPI passphrase	..... <a href="#">Click here to display</a>
WPA Group Rekey Interval	3600 [0-2147483647]
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

**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 Mixed WPA2/WPA

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

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

**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
Protected Management Frames	Disable
WPA/WAPI passphrase	..... <a href="#">Click here to display</a>
WPA Group Rekey Interval	3600 [0-2147483647]
WPA/WAPI Encryption	AES
WEP Encryption	Disabled

**Protected Management Frame:** Select whether to enable protected management frame mechanism. By default, it is disabled. If enabled, the network adapter of the attempting wireless client should also support this feature.

**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.

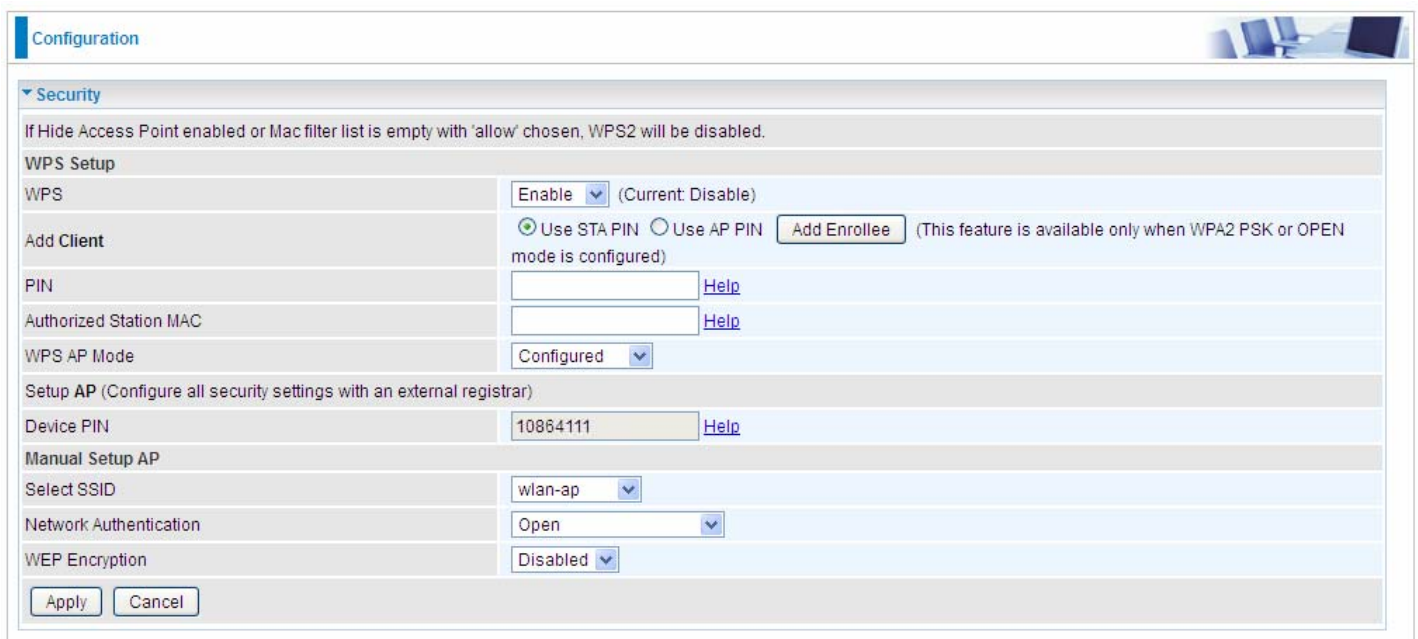
## WPS Setup

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:

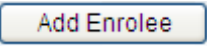
- 1) WPS feature is only available when in WPA2 PSK or OPEN mode in security settings.
- 2) Here wireless can be configured as **Registrar** and **Enrollee** mode respectively. When AP is configured as Registrar, you should select “Configured” in the WPS AP Mode below, and default WPS AP Mode is “Configured”. When AP is configured as Enrollee, the WPS AP Mode below should be changed to “Unconfigured”. Follow the following steps.

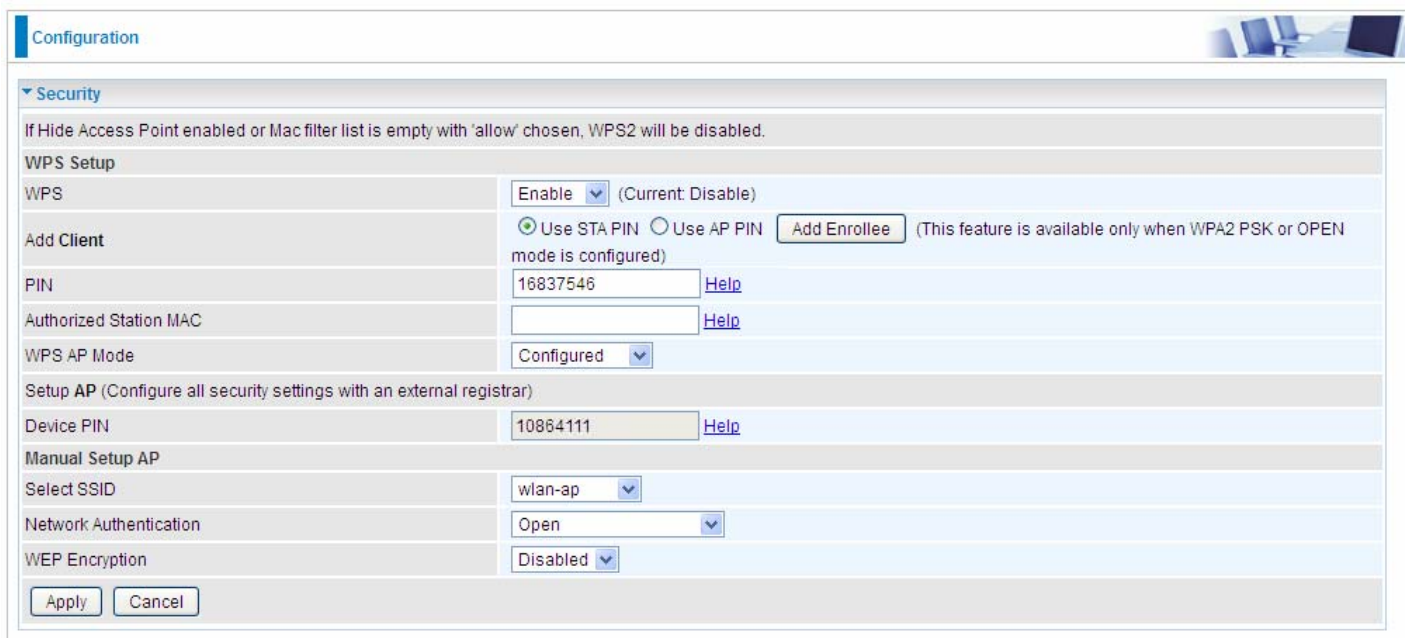


The screenshot shows a web-based configuration interface for WPS. The page is titled "Configuration" and has a "Security" section expanded. A warning message states: "If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled." The "WPS Setup" section includes a "WPS" dropdown menu set to "Enable" (Current: Disable). Below it are radio buttons for "Use STA PIN" (selected) and "Use AP PIN", along with an "Add Enrollee" button and a note: "(This feature is available only when WPA2 PSK or OPEN mode is configured)". There are input fields for "PIN" and "Authorized Station MAC", each with a "Help" link. The "WPS AP Mode" dropdown is set to "Configured". The "Setup AP (Configure all security settings with an external registrar)" section has a "Device PIN" input field with the value "10864111" and a "Help" link. 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 are "Apply" and "Cancel" buttons.

## Configure AP as Registrar

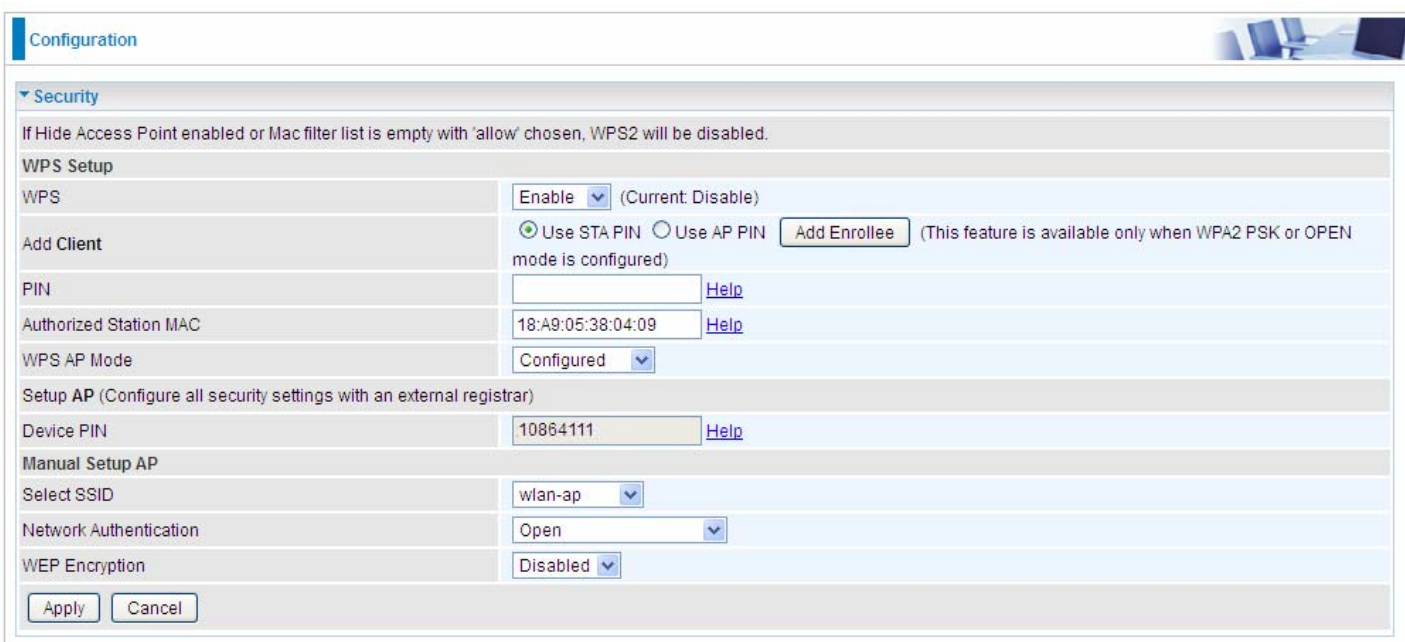
### Add Enrollee with PIN method

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 .



The screenshot shows the 'Configuration' page with the 'Security' section expanded. Under 'WPS Setup', the 'WPS' dropdown is set to 'Enable'. The 'Add Client' section has 'Use STA PIN' selected. The 'PIN' field contains '16837546'. The 'Authorized Station MAC' field is empty. The 'WPS AP Mode' is set to 'Configured'. Below this, the 'Setup AP' section has 'Device PIN' set to '10864111'. The 'Manual Setup AP' section has 'Select SSID' set to 'wlan-ap', 'Network Authentication' set to 'Open', and 'WEP Encryption' set to 'Disabled'. 'Apply' and 'Cancel' buttons are at the bottom.

(Station PIN)



The screenshot shows the same 'Configuration' page. In the 'Add Client' section, 'Use STA PIN' is still selected, but the 'PIN' field is empty. The 'Authorized Station MAC' field now contains '18:A9:05:38:04:09'. All other settings remain the same as in the previous screenshot.

(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:

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

ID	AP Name	MAC Address	Count
0x0000	wlan-ap	00-04-ED-EC:FF:D0	1
11		00-04-ED-00-00-01	1
- WPS Profile List:** (Empty)
- WPS Configuration:**
  - WPS Associate IE
  - WPS Probe IE
  - 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 & Metrics:**
  - Status >> Disconnected
  - Link Quality >> 0%
  - Signal Strength 1 >> 0%
  - Signal Strength 2 >> 0%
  - Noise Strength >> 0%
  - Transmit:
    - Link Speed >> Max
    - Throughput >> 0.000 Kbps
  - Receive:
    - Link Speed >> Max
    - Throughput >> 0.000 Kbps
  - HT:
    - BW >> n/a
    - SNRO >> 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 several sections:

- Navigation Bar:** Profile, Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, About.
- WPS AP List:** A table with columns for ID, MAC address, and a count. Two entries are visible: ID 11 with MAC 00-04-ED-01-00-01, and ID wlan-ap with MAC 00:04:ED:EC:FF:D0.
- WPS Profile List:** A dropdown menu showing 'wlan-ap' selected.
- WPS Configuration:** Includes buttons for PIN and PBC, checkboxes for 'WPS Associate IE' and 'WPS Probe IE' (both checked), a progress bar at 100%, and a message: 'PIN - Get WPS profile successfully.'
- Right Panel:** A vertical stack of buttons: Rescan, Information, Pin Code (16837546, Renew), Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Status Section:** A red circle highlights the following information:
  - 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 Section:** HT (High Throughput) parameters:
  - BW >> 40
  - GI >> long
  - MCS >> 15
  - SNRO >> 19
  - SNR1 >> n/a
- Link Quality Metrics:** A series of colored bars showing:
  - Link Quality >> 100% (green)
  - Signal Strength 1 >> 64% (yellow)
  - Signal Strength 2 >> 34% (red)
  - Noise Strength >> 26% (green)
- Transmit Section:** Transmit Link Speed >> 270.0 Mbps, Throughput >> 5.600 Kbps. Includes a spectrum graph with a peak at 38.624 Kbps.
- Receive Section:** Receive Link Speed >> 54.0 Mbps, Throughput >> 81.608 Kbps. Includes a spectrum graph with a peak at 146.840 Kbps.

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

## Configure AP as Enrollee

### ● Add Registrar with PIN Method

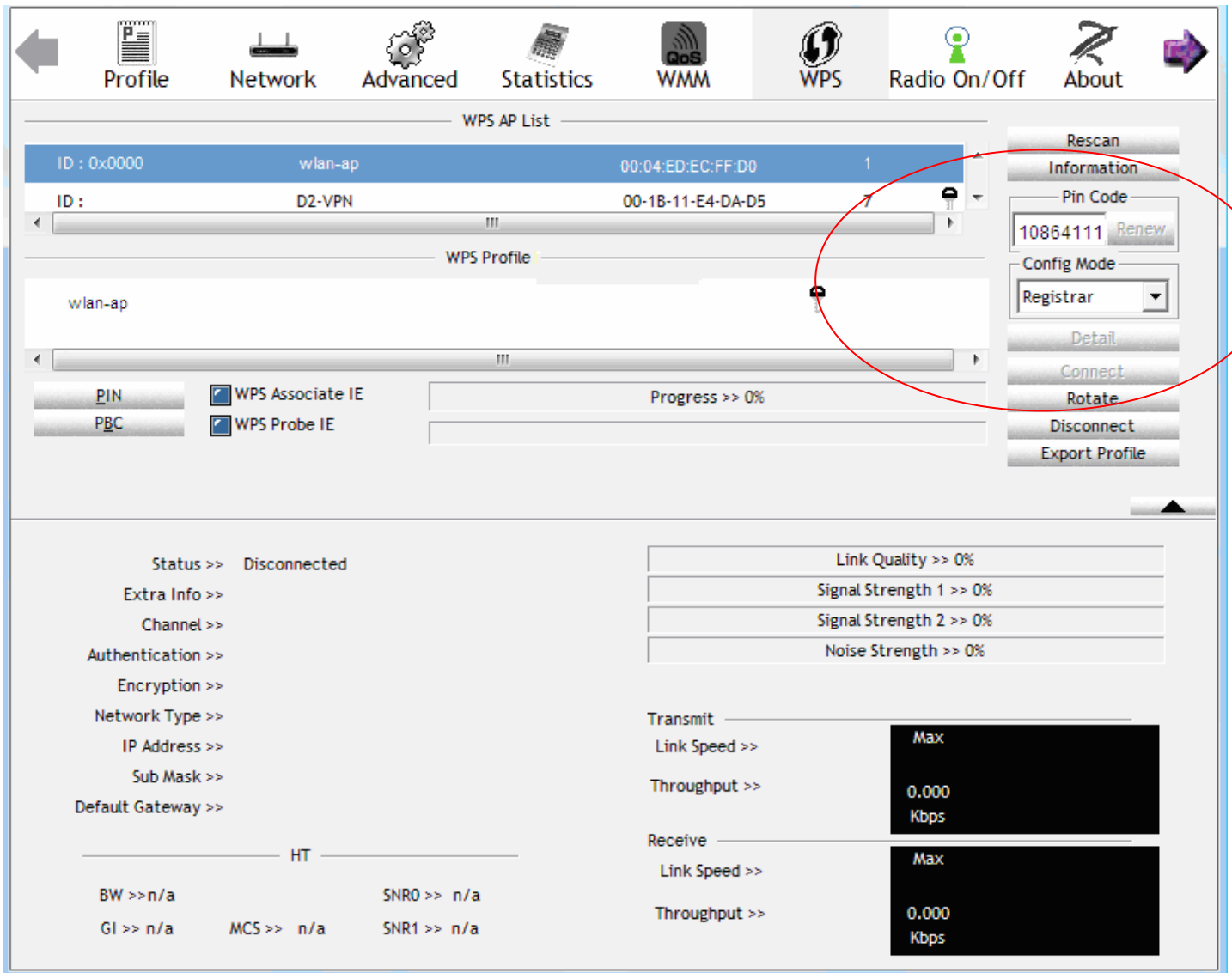
1. Set AP to “*Unconfigured Mode*”.



The screenshot shows the Configuration page for an Access Point. The 'Security' section is expanded to show 'WPS Setup'. The 'WPS' dropdown is set to 'Enable' (Current: Disable). The 'Add Client' section has 'Use AP PIN' selected, and an 'Add Enrollee' button is visible. The 'WPS AP Mode' dropdown is set to 'Unconfigured'. The 'Manual Setup AP' section shows 'Device PIN' as '10864111', 'Select SSID' as 'wlan-ap', 'Network Authentication' as 'Open', and 'WEP Encryption' as 'Disabled'. 'Apply' and 'Cancel' buttons are at the bottom.

Configuration	
▼ Security	
If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.	
WPS Setup	
WPS	Enable (Current: Disable)
Add Client	<input type="radio"/> Use STA PIN <input checked="" type="radio"/> Use AP PIN <a href="#">Add Enrollee</a> (This feature is available only when WPA2 PSK or OPEN mode is configured)
WPS AP Mode	Unconfigured
Setup AP (Configure all security settings with an external registrar)	
Device PIN	10864111 <a href="#">Help</a>
Manual Setup AP	
Select SSID	wlan-ap
Network Authentication	Open
WEP Encryption	Disabled
<a href="#">Apply</a> <a href="#">Cancel</a>	

2. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as **Registrar**. Enter the **PIN** number (10864111 (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 WPS configuration interface. At the top, there are navigation tabs: Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The main content area is divided into several sections:

- WPS AP List:** A table with columns for ID, MAC address, and a count. It lists two entries: ID '11' with MAC '00-04-ED-01-00-01' and ID 'wlan-ap' with MAC '00:04:ED:EC:FF:D0'.
- WPS Profile List:** A list containing the profile name 'wlan-ap'.
- Configuration Options:** Includes fields for PIN and PBC, checkboxes for 'WPS Associate IE' and 'WPS Probe IE', and a progress bar showing 'Progress >> 100%'. A message below reads 'PIN - Get WPS profile successfully.'
- Right-Hand Panel:** Contains buttons for 'Rescan', 'Information', 'Pin Code' (with input '10864111' and 'Renew' button), 'Config Mode' (set to 'Registrar'), 'Detail', 'Connect', 'Rotate', 'Disconnect', 'Export Profile', and 'Delete'.
- Status Section (circled in red):**
  - 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
- Performance Metrics:**
  - Link Quality >> 100%
  - Signal Strength 1 >> 64%
  - Signal Strength 2 >> 34%
  - Noise Strength >> 26%
  - Transmit: Link Speed >> 270.0 Mbps, Throughput >> 5.600 Kbps
  - Receive: Link Speed >> 54.0 Mbps, Throughput >> 81.608 Kbps
- HT Section:**
  - BW >> 40, SNR0 >> 19
  - GI >> long, MCS >> 15, SNR1 >> n/a

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

## MAC Filter



Configuration

MAC Filter

Parameters

Select SSID: wlan-ap

MAC Restrict Mode \*:  Disable  Allow  Deny

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

MAC Address	Remove	Edit
-------------	--------	------

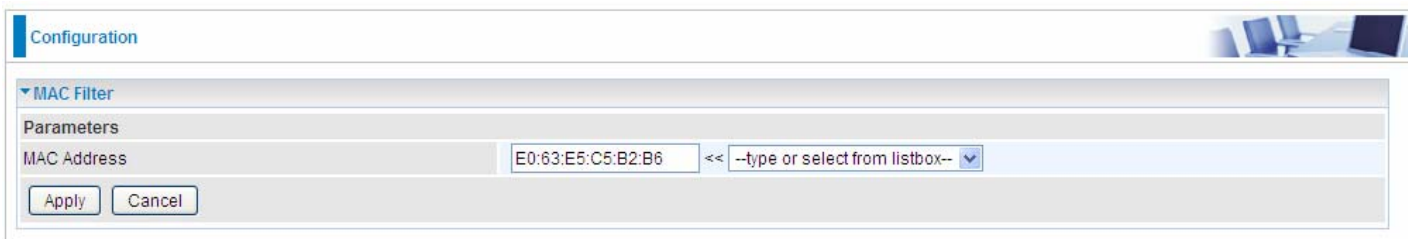
Add Remove

**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.



Configuration

MAC Filter

Parameters

MAC Address: E0:63:E5:C5:B2:B6 << --type or select from listbox--

Apply Cancel

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

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



Configuration

MAC Filter

Parameters

Select SSID: wlan-ap

MAC Restrict Mode \*:  Disable  Allow  Deny

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

MAC Address	Remove	Edit
E0:63:E5:C5:B2:B6	<input type="checkbox"/>	Edit

Add Remove

## Wireless Bridge

WDS (wireless distributed system) is a system enabling the wireless interconnection of 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.

Configuration

Wireless Bridge

Parameters

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.

Bridge Restrict: Enable

Remote Bridges MAC Address

Apply Refresh

**Bridge Restrict:** It 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)

Remote Bridges MAC Address	SSID	BSSID
<input type="checkbox"/>	wlan-ap	00:04:ED:14:27:13

Apply Refresh

**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

Apply Refresh

Click **Apply** to apply your settings..

## Advanced

Here users can set some advanced parameters about wireless.

Advanced	
Parameters	
Band	2.4GHz
Channel	1 Current: 1 (interference: acceptable) <input type="button" value="Scan Used Channel"/>
Auto Channel Timer	15 minutes
802.11n/EWC	Auto
Bandwidth	20MHz / 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 Coexistence	Enable
RX Chain Power Save	Enable Power Save status: Low 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:** In the 2.4 GHz radio frequency.

**Channel:** Choose a channel to use. Here is a list of available channels or select Auto mode instead.

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

**Auto Channel Timer (min):** Available when Auto Channel is selected. The auto channel times length it takes to scan in minutes.

**802.11n/EWC:** Select to auto enable or disable 802.11n.

**Bandwidth:** The higher the bandwidth the better the performance will be but greater interference with other wireless devices. Select **20MHz** for lessen radio interference.

**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.

**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 an 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 duration of Quiet Time, described above, before the Rx Chain Power Save feature activates itself.

**54g™ Rate:** Available after changing **802.11n Rate** to “Use 54g Rate” in **802.11n Rate**. It is used to limit 11n speed to a specific rate, e.g. 1M, 6M, 12M, 24M, 48M, etc.

**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.

**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.



**MAC Address:** The MAC address of the wireless clients.

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

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

**SSID:** Show the current SSID of the client.

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

**Refresh:** To get the latest information.

## Schedule Control

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

The Wireless schedule only functions whilst Wireless is enabled.

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

For detail setting the timeslot, user can turn to [Time Schedule](#) .

Configuration

**Schedule Control**

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

wlan-ap Enable

Time Schedule

1. Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

2.  check or select from listbox  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

Wireless - Guest/Virtual Access Points

wl0\_Guest1 Disable

Time Schedule

1. Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

2.  check or select from listbox  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

wl0\_Guest2 Disable

Time Schedule

1. Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

2.  check or select from listbox  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

wl0\_Guest3 Disable

Time Schedule

1. Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

2.  check or select from listbox  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

Apply

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

For example: user wants the SSID “wlan-ap” to work on weekdays except for Wednesday, under this circumstance, user can set as shown below. (8700NEXL R2 offers a optimal way to set two separate timeslots when user needs to activate the SSID during separate intervals. )

wlan-ap Enable

Time Schedule

1. check or select from listbox  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 23 : 59

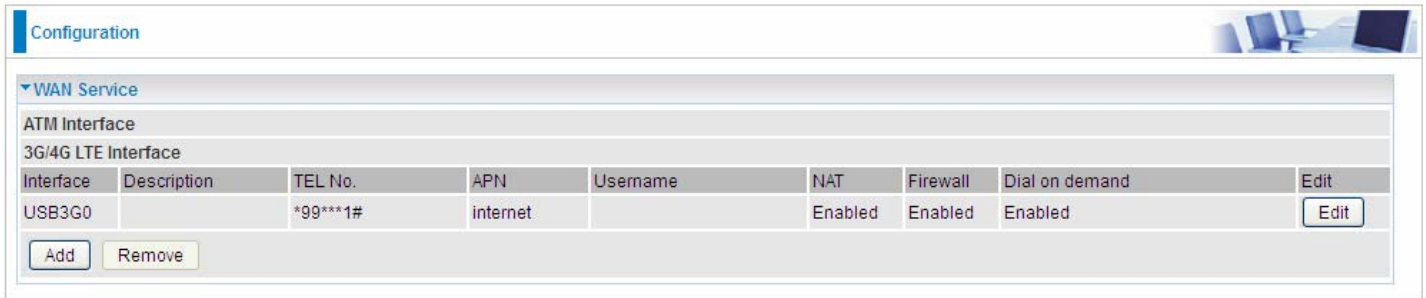
2.  check or select from listbox  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 23 : 59

# 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

Three WAN interfaces are provided for WAN connection: DSL (VDSL/ADSL), Ethernet and 3G/4G LTE.



The screenshot shows the 'Configuration' page for 'WAN Service'. Under the '3G/4G LTE Interface' section, there is a table with the following data:

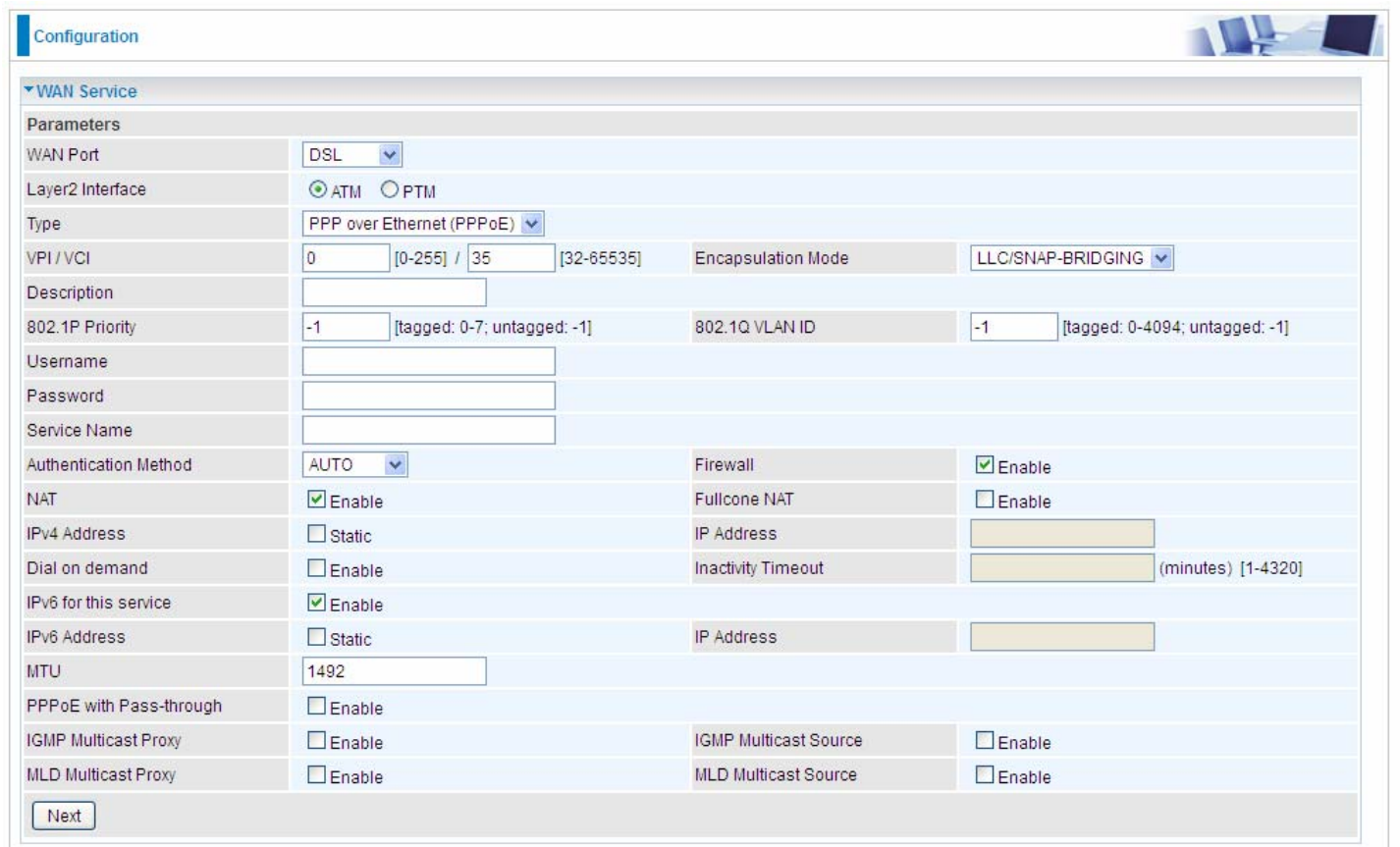
Interface	Description	TEL No.	APN	Username	NAT	Firewall	Dial on demand	Edit
USB3G0		*99***1#	internet		Enabled	Enabled	Enabled	<input type="button" value="Edit"/>

Below the table are 'Add' and 'Remove' buttons.

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 (ADSL)** and **PTM (VDSL)** configuration of PTM mode is similar as ATM mode, here take ATM mode WAN configuration for example.



The screenshot shows the 'Configuration' page for 'WAN Service' with the 'Parameters' section expanded. The configuration is as follows:

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

A 'Next' button is located at the bottom left of the configuration area.



**Layer2 Interface:** 2 transfer mode, **ATM (ADSL)** or **PTM (VDSL)**.

## ● PPPoE

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

The screenshot shows the configuration page for a WAN Service. The 'Parameters' section is expanded, showing various settings for the service. The 'WAN Port' is set to 'DSL'. The 'Layer2 Interface' is set to 'ATM'. The 'Type' is 'PPP over Ethernet (PPPoE)'. The 'VPI/VCI' is set to '0' and '35'. The 'Encapsulation Mode' is 'LLC/SNAP-BRIDGING'. The 'Description' field is empty. The '802.1P Priority' is '-1' and the '802.1Q VLAN ID' is '-1'. The 'Username', 'Password', and 'Service Name' fields are empty. The 'Authentication Method' is 'AUTO'. The 'Firewall' is checked. The 'NAT' is checked, and 'Fullcone NAT' is unchecked. The 'IPv4 Address' is set to 'Static' (unchecked), and the 'IP Address' field is empty. The 'Dial on demand' is unchecked, and the 'Inactivity Timeout' field is empty. The 'IPv6 for this service' is checked, and the 'IPv6 Address' is set to 'Static' (unchecked), with the 'IP Address' field empty. The 'MTU' is '1492'. The 'PPPoE with Pass-through' is unchecked. The 'IGMP Multicast Proxy' is unchecked, and the 'IGMP Multicast Source' is unchecked. The 'MLD Multicast Proxy' is unchecked, and the 'MLD Multicast Source' is unchecked. A 'Next' button is located at the bottom left of the configuration area.

**VPI/VCI:** Enter the VPI/VCI 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 purposes, user can define this.

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

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

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

**Fullcone NAT:** Enable or disable fullcone NAT. Fullcone is a kind of NAT, in this mode, all requests

from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

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

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

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

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

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

**IPv6 for this service:** Enable to use IPv6 service.

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

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

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

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

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**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.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**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.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

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

The screenshot shows a configuration interface with two main sections: 'Default Gateway / DNS' and 'DNS'.  
In the 'Default Gateway / DNS' section, 'Selected Default Gateway Interfaces' contains 'ppp0.1'. 'Available Routed WAN Interfaces' contains '3G0/USB3G0'. Below these, 'Selected WAN Interface As The System Default IPv6 Gateway' is set to 'pppoe\_0\_8\_35/ppp0.1'.  
The 'DNS' section has three radio buttons: 'Available WAN Interfaces' (selected), 'Static DNS Address', and 'Parent Controls'. Below, 'Selected DNS Server Interfaces' contains 'ppp0.1' and 'Available WAN Interfaces' contains '3G0/USB3G0'.  
There are input fields for 'Primary DNS server' and 'Secondary DNS server'. A note states: 'Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.'  
Below the note, 'DNS Server Interface' has radio buttons for 'Available WAN Interfaces' (selected) and 'Static DNS IPv6 Address'. 'WAN Interface selected' is set to 'pppoe\_0\_8\_35/ppp0.1'. There are also input fields for 'Primary IPv6 DNS server' and 'Secondary IPv6 DNS server'.  
A 'Next' button is located at the bottom left of the configuration area.

## Default Gateway

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

## DNS

### ➤ IPv4

#### Three ways to set an IPv4 DNS server

- ① **Available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

### ➤ IPv6

#### Obtain IPv6 DNS info from a WAN interface

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

#### Static DNS IPv6 Address

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

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

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

**Configuration**

▼ WAN Service

ATM Interface

Interface	Description	Type	VPI / VCI	Vlan8021p	VlanMuxId	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/4G LTE Interface

Interface	Description	TEL No.	APN	Username	NAT	Firewall	Dial on demand	Edit
USB3G0		*99***1#	internet		Enabled	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	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	23:50:29	118.166.81.43	2001:b011:7009:05f1:a439:db84:0581:2b5c/64	168.95.192.1,168.95.1.1
USB3G0			3G/4G LTE Card not found				

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

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

**Description:** User-defined description for the connection.

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

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

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

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

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

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

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

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

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

**Dial on demand:** It is a parameter to let users to dial for connection to internet themselves. It is

useful when saving internet fees.

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

**IPv6 for this service:** Enable to use IPv6 service.

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

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

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

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**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.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**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.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

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

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

**Option 125:** Option 125 is a complementary standard of DHCP protocol, it is used to encapsulate

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

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

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

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

**IPv6 for this service:** Enable to use IPv6 service.

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

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

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

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

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

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

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

**IGMP Multicast 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.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**No Multicast VLAN Filter:** Enable to deactivate the multicast VLAN filter which allows users to filter on all multicast packets or on specific multicast groups.

**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. **Note:** It works only on MLD version 2.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system.

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

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

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



The screenshot shows a configuration window titled 'Configuration' with a sub-section 'WAN Service'. Under 'Parameters', the following settings are visible:

- WAN Port:** DSL (dropdown)
- Layer2 Interface:** ATM (radio button selected), PTM (radio button unselected)
- Type:** IPoA (dropdown)
- VPI / VCI:** 0 [0-255] / 35 [32-65535]
- Encapsulation Mode:** LLC/SNAP-ROUTING (dropdown)
- Description:** (empty text field)
- WAN IP Address:** (empty text field)
- WAN Subnet Mask:** (empty text field)
- NAT:**  Enable. A sub-section 'Fullcone NAT' has  Enable.
- Firewall:**  Enable.

A 'Next' button is located at the bottom left of the configuration area.

**VPI/VCI:** Enter the VPI/VCI 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.

The screenshot shows a configuration page for 'WAN Service'. Under the 'Parameters' section, the following settings are visible:

- WAN Port:** DSL
- Layer2 Interface:** ATM (selected), PTM
- Type:** Bridging
- VPI / VCI:** 0 [0-255] / 35 [32-65535]
- Encapsulation Mode:** LLC/SNAP-BRIDGING
- Description:** (empty text box)
- 802.1P Priority:** -1 [tagged: 0-7; untagged: -1]
- 802.1Q VLAN ID:** -1 [tagged: 0-4094; untagged: -1]
- Allow as IGMP Multicast Source:**  Enable
- Allow as MLD Multicast Source:**  Enable

A 'Next' button is located at the bottom left of the configuration area.

**VPI/VCI:** Enter the VPI/VCI 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: 0-7, untagged: -1.

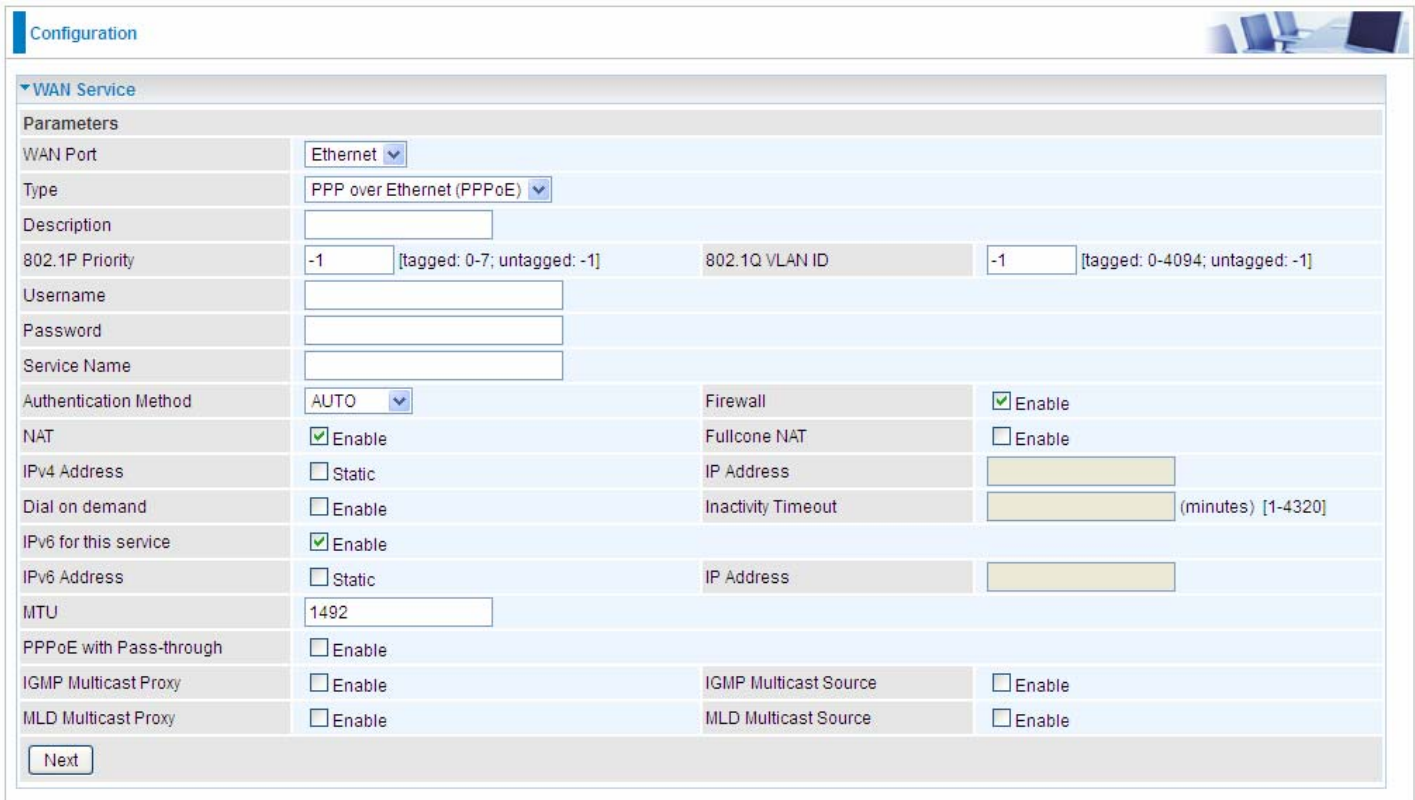
**802.1Q VLAN ID:** It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4094, untagged : -1.

**Allow as IGMP Multicast Source:** Enable to support the “source filtering” which is the ability for a system to report interest in receiving packets “only ” from specific source address(es), or “all but” specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**Allow as MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

## ① Ethernet

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



Configuration

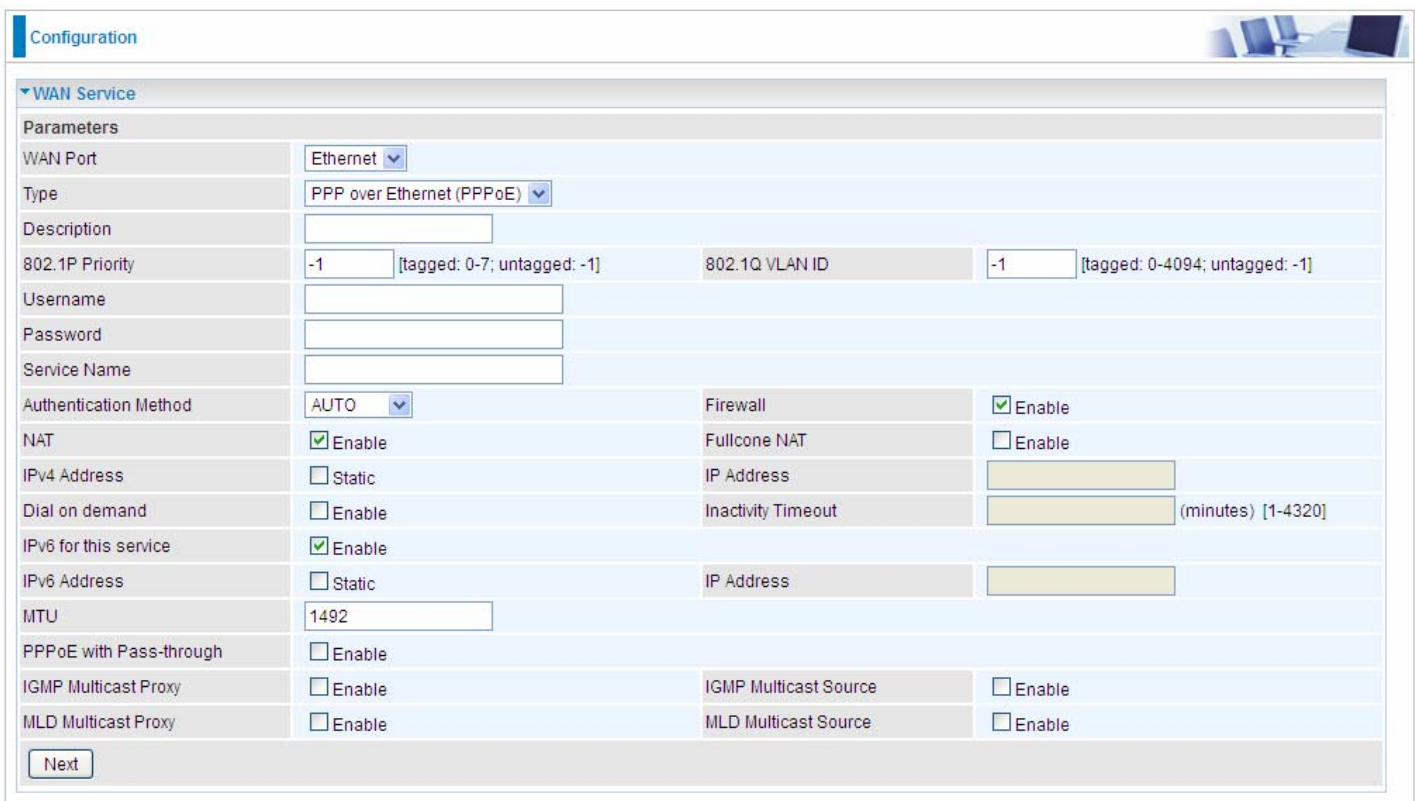
WAN Service

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	Firewall	<input checked="" type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable	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	IGMP Multicast Source	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Source	<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	Firewall	<input checked="" type="checkbox"/> Enable
NAT	<input checked="" type="checkbox"/> Enable	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	IGMP Multicast Source	<input type="checkbox"/> Enable
MLD Multicast Proxy	<input type="checkbox"/> Enable	MLD Multicast Source	<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.

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

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

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

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

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

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

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

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

**IPv6 for this service:** Enable to use IPv6 service.

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

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

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

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

**IGMP Multicast Proxy:** Check whether to enable this feature. IGMP (**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.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**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.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

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

The screenshot shows a configuration interface with the following sections:

- Default Gateway / DNS**
  - Default Gateway**
    - Selected Default Gateway Interfaces: ppp0.1
    - Available Routed WAN Interfaces: 3G0/USB3G0
    - Selected WAN Interface As The System Default IPv6 Gateway: pppoe\_eth0/ppp0.1
  - DNS**
    - DNS Server Interface:  Available WAN Interfaces,  Static DNS Address,  Parent Controls
    - Selected DNS Server Interfaces: ppp0.1
    - Available WAN Interfaces: 3G0/USB3G0
    - Primary DNS server: [Empty text box]
    - Secondary DNS server: [Empty text box]
    - Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.
    - DNS Server Interface:  Available WAN Interfaces,  Static DNS IPv6 Address
    - WAN Interface selected: pppoe\_eth0/ppp0.1
    - Primary IPv6 DNS server: [Empty text box]
    - Secondary IPv6 DNS server: [Empty text box]

A "Next" button is located at the bottom left of the configuration area.

## Default Gateway

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

## DNS

### ➤ IPv4

#### Three ways to set an IPv4 DNS server

- ① **Available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **Static DNS Address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

### ➤ IPv6

#### Obtain IPv6 DNS info from a WAN interface

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

#### Static DNS IPv6 Address

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

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

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

**Configuration**

▼ WAN Service

ETH Interface

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Remove	Edit
ppp0.1	pppoe_eth4	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	<input type="checkbox"/>	Edit

3G/4G LTE Interface

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

**Status**

▼ WAN

Wan Info

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Disconnect	23:52:32	118.166.81.43	2001:b011:7009:05f1:a439:db84:0581:2b5c/64	168.95.192.1,168.95.1.1
USB3G0			3G/4G LTE Card not found				

The screenshot shows the 'Configuration' page for 'WAN Service'. The 'Parameters' section includes the following fields and options:

- WAN Port:** Ethernet (dropdown)
- Type:** IP over Ethernet (dropdown)
- Description:** (text input)
- 802.1P Priority:** -1 (text input, with help text: [tagged: 0-7; untagged: -1])
- 802.1Q VLAN ID:** -1 (text input, with help text: [tagged: 0-4094; untagged: -1])
- Obtain an IP address automatically:**  Enable
- Option 60 Vendor ID:** (text input)
- Option 61 Client ID:** (text input)
- Option 125:**  Disable  Enable
- WAN IP Address:** (text input)
- WAN Subnet Mask:** (text input)
- WAN gateway IP Address:** (text input)
- IPv6 for this service:**  Enable
- Obtain an IPv6 address automatically:**  Enable
- WAN IPv6 Address/Prefix Length:** (text input)
- WAN Next-Hop IPv6 Address:** (text input)
- NAT:**  Enable
- Fullcone NAT:**  Enable
- Firewall:**  Enable
- IGMP Multicast Proxy:**  Enable
- IGMP Multicast Source:**  Enable
- No Multicast VLAN Filter:**  Enable
- MLD Multicast Proxy:**  Enable
- MLD Multicast Source:**  Enable
- MTU:** 1500 (text input)
- MAC Spoofing:** (text input)

A 'Next' button is located at the bottom left of the configuration area.

**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 ClientID:** Enter the associated information provided by your ISP.

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

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

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

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

**IPv6 for this service:** Enable to use IPv6 service.

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

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

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

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

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

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

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

**IGMP Multicast:** IGMP (**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.

**IGMP Multicast Source:** Enable to support the "source filtering" which is the ability for a system to report interest in receiving packets "only " from specific source address(es), or "all but" specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**No Multicast VLAN Filter:** Enable to deactivate the multicast VLAN filter which allows users to filter on all multicast packets or on specific multicast groups.

**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.

**MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

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

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



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]
Allow as IGMP Multicast Source	<input type="checkbox"/> Enable	Allow as MLD Multicast Source	<input type="checkbox"/> Enable

**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.

**Allow as IGMP Multicast Source:** Enable to support the “source filtering” which is the ability for a system to report interest in receiving packets “only ” from specific source address(es), or “all but” specific source address(es), sent to a particular multicast address. **Note:** It works only on IGMP version 3.

**Allow as MLD Multicast Source:** Used in a similar way by IPv6 system as IGMP Multicast source in IPv4 system. Enable it to support the source filtering functionality for IPv6 system. **Note:** It works only on MLD version 2.

## ① 3G/4G LTE

Select 3G/4G LTE to configure the route to enjoy the mobility. By default the 3G/4G LTE interface is on, user can edit the parameters to meet your own requirements.

Configuration

---

**WAN Service**

**ATM Interface**

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

**3G/4G LTE Interface**

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

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

Click **Edit** button to enter the 3G/4G LTE configuration page.

Configuration

---

**WAN Service**

**Parameters**

Dial on demand  Enable

Mode [Use 3G/4G LTE dongle settings](#)

Use PPP  Enable

TEL No.  APN

Username  Password

Authentication Method [AUTO](#) PIN

Dial on demand  Enable

Keep Alive  Enable  seconds [1-86400]

IP Address

MTU

NAT  Enable Firewall  Enable

Selected Default Gateway Interfaces  Available Routed WAN Interfaces

Obtain DNS  Use WAN Interface  Use Static DNS  Parent Controls

Selected DNS Server Interfaces  Available WAN Interfaces

Primary DNS  Secondary DNS

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

[Apply](#) [Cancel](#)

**Dial on demand:** If enabled, the 3G/4G LTE will work in dial on demand and be brought up only when there is no active default route. In this mode, 3G/4G LTE work as a backup for the WAN connectivity. While if disabled, 3G/4G 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/4G LTE 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/4G 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	<input type="text" value="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 <input type="text" value="7"/> seconds [1-86400]
IP Address	<input type="text" value="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 USB3G0.

**Selected DNS Server Interfaces:** Three ways to set a DNS server.

- ① **Available WAN interfaces:** Select a desirable WAN interface as the DNS server.
- ① **Static DNS Address:** To specify DNS server manually by entering your primary and

secondary DNS server addresses.

- ① **Parental Controls:** If user registers and gets a DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

Click **Apply** to confirm the settings.

Here you can configure WAN Service, if it is OK, you can access the internet. You can go to **Status >WAN** or **Summary** to view the WAN connection information.

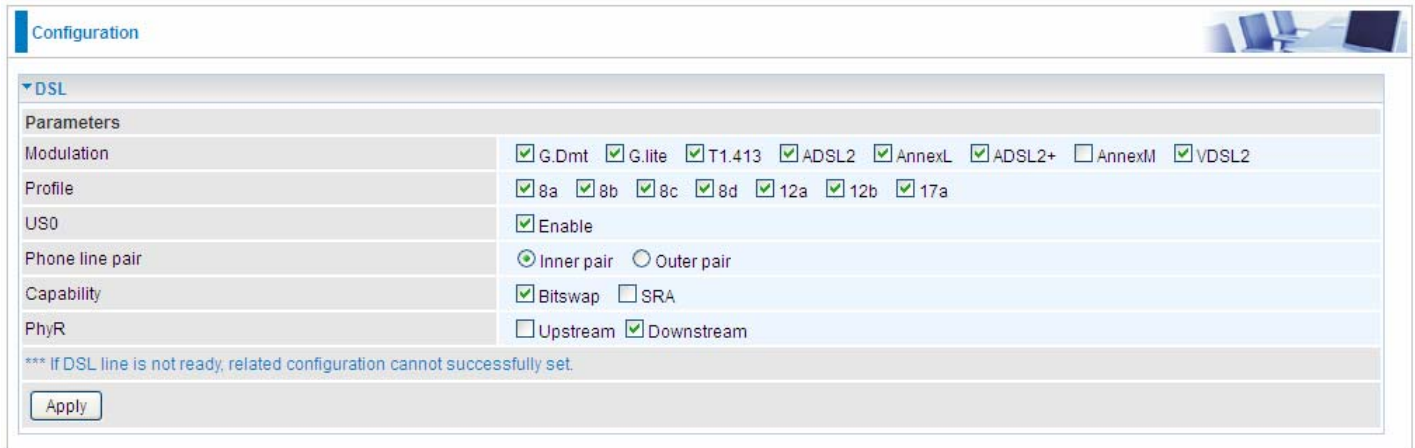


The screenshot shows a web interface with a 'Status' tab selected. Underneath, there is a section for 'WAN' with a 'Wan Info' table. The table has columns for Interface, Description, Type, Status, Connection Time, IPv4 Address, IPv6 Address, and DNS. Two rows are visible: one for 'ppp0.1' which is 'Unconfigured', and one for 'USB3G0' which is 'Connected' with an IPv4 address of 10.44.183.197 and a DNS of 221.5.4.55.

Interface	Description	Type	Status	Connection Time	IPv4 Address	IPv6 Address	DNS
ppp0.1	pppoe_0_8_35	PPPoE	Unconfigured				
USB3G0	3G0	PPP	Connected	00:01:10	10.44.183.197		221.5.4.55

## 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 screenshot shows a web-based configuration page for DSL settings. The page has a header 'Configuration' and a sub-section 'DSL'. Below this, there is a table of parameters with their respective settings:

Parameters	
Modulation	<input checked="" type="checkbox"/> G.Dmt <input checked="" type="checkbox"/> G.lite <input checked="" type="checkbox"/> T1.413 <input checked="" type="checkbox"/> ADSL2 <input checked="" type="checkbox"/> AnnexL <input checked="" type="checkbox"/> ADSL2+ <input type="checkbox"/> AnnexM <input checked="" type="checkbox"/> VDSL2
Profile	<input checked="" type="checkbox"/> 8a <input checked="" type="checkbox"/> 8b <input checked="" type="checkbox"/> 8c <input checked="" type="checkbox"/> 8d <input checked="" type="checkbox"/> 12a <input checked="" type="checkbox"/> 12b <input checked="" type="checkbox"/> 17a
US0	<input checked="" type="checkbox"/> Enable
Phone line pair	<input checked="" type="radio"/> Inner pair <input type="radio"/> Outer pair
Capability	<input checked="" type="checkbox"/> Bitswap <input type="checkbox"/> SRA
PhyR	<input type="checkbox"/> Upstream <input checked="" type="checkbox"/> Downstream

\*\*\* If DSL line is not ready, related configuration cannot successfully set.

Apply

**Modulation:** There are 8 modes “G.Dmt”, “G.lite”, “T1.413”, “ADSL2”, “AnnexL”, “ADSL2+”, “AnnexM”, that user can select for this connection.

**Profile:** VDSL profiles up to 17a.

**US0:** Select to enable US0. In VDSL mode, profiles like 8a, 8b, 8c, 8d and 12a need users to enable US0 band.

**Phone line pair:** This is for reserved only. You can choose "Inner Pair" or "Outer Pair".

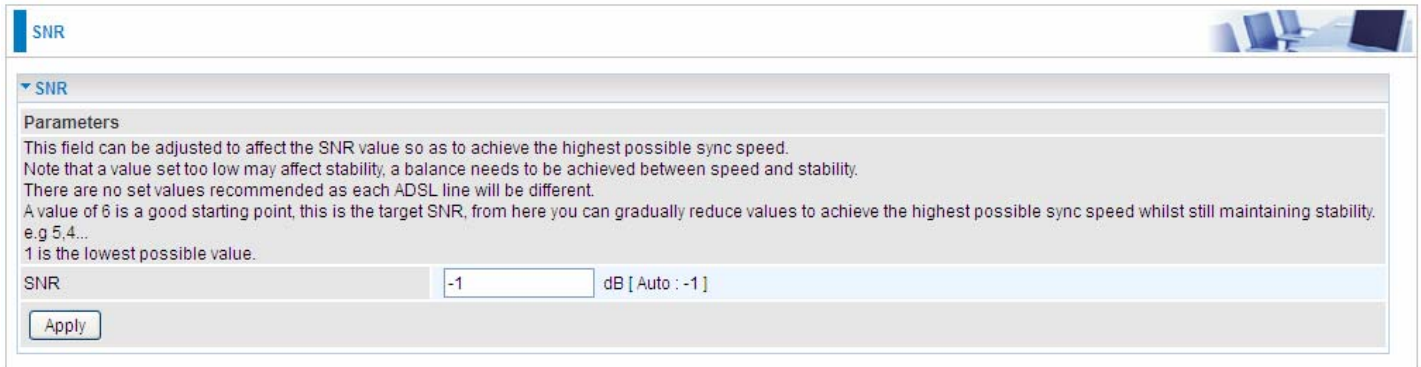
**Capability:** There are 2 options “Bitswap Enable” and “SRA Enable” that user can select for this connection.

- ① Bitswap Enable: Allows bitswaping function.
- ① SRA Enable: Allows seamless rate adaptation.

**PhyR:** A new technology to control impulse and noise to improve the BER and DSL data quality. Click **Apply** to confirm the settings.

## 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". At the top right, there is a small image of a computer workstation. Below the title bar, there is a section labeled "Parameters" with the following text: "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." Below this text, there is a text input field labeled "SNR" containing the value "-1", followed by the unit "dB [ Auto : -1 ]". At the bottom left of the configuration area, there is an "Apply" button.

**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.

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

Apply Cancel

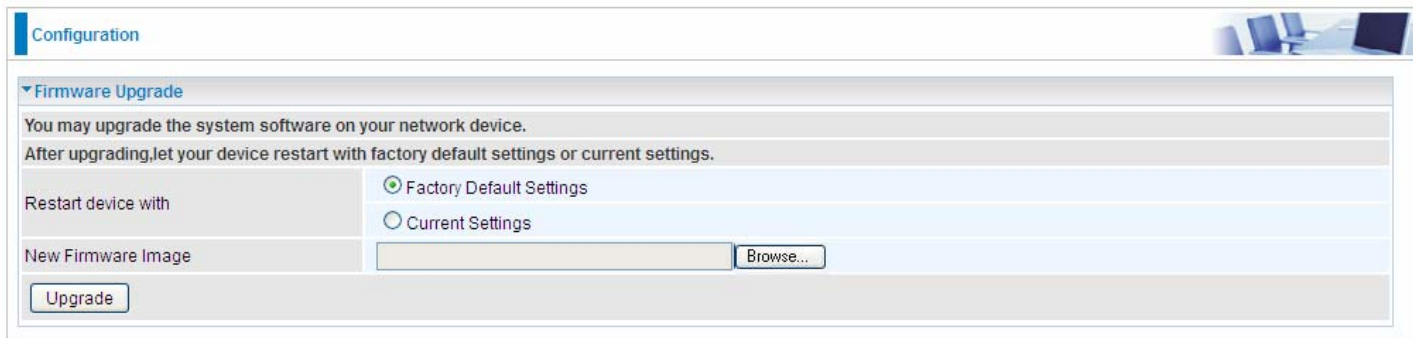
Choose the NTP time server from the drop-down menu, if you prefer to specify an NTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

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 a web interface for configuring a router's firmware upgrade. At the top, there is a 'Configuration' tab. Below it, the 'Firmware Upgrade' section is expanded. The text reads: 'You may upgrade the system software on your network device. After upgrading, let your device restart with factory default settings or current settings.' There are two radio button options: 'Factory Default Settings' (which is selected) and 'Current Settings'. Below these is a text input field for 'New Firmware Image' with a 'Browse...' button next to it. At the bottom left of the form 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.



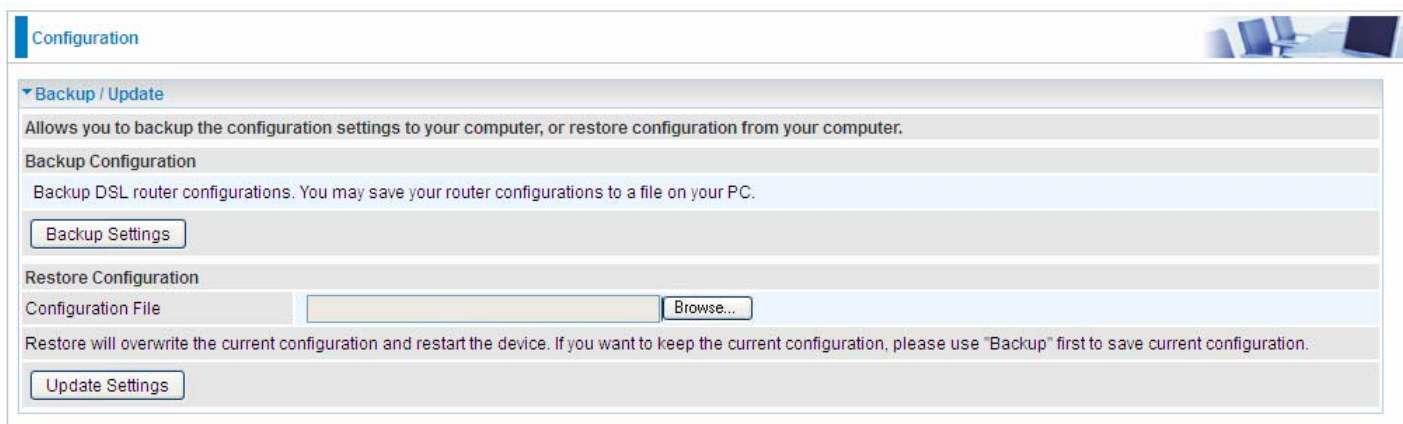
### Warning

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

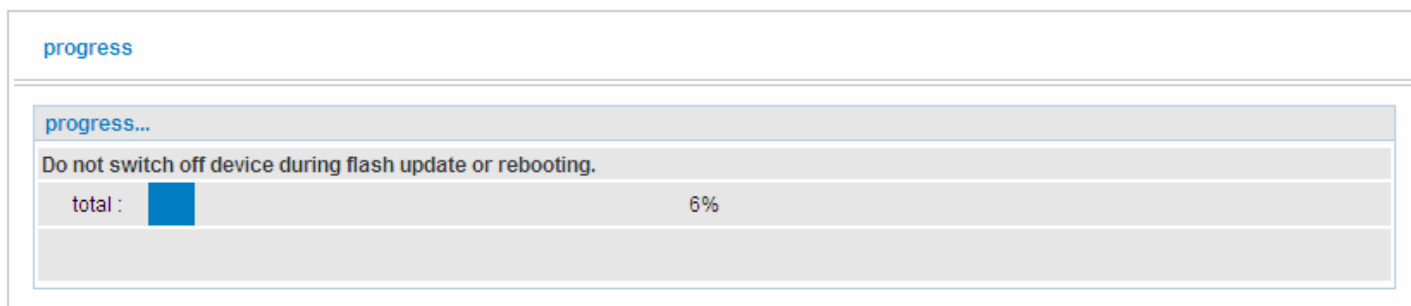
These functions allow you to save and backup your router's current settings to a file on your PC, or to restore from a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup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



The screenshot shows the 'Configuration' page with a sub-section titled 'Backup / Update'. It contains instructions for backing up and restoring settings, along with buttons for 'Backup Settings' and 'Update Settings'. A 'Restore Configuration' section includes a text input field for the configuration file and a 'Browse...' button. A warning message states: 'Restore will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.'

Click **Backup Settings**, a window appears, click save, then browse the location where you want to save the backup file.

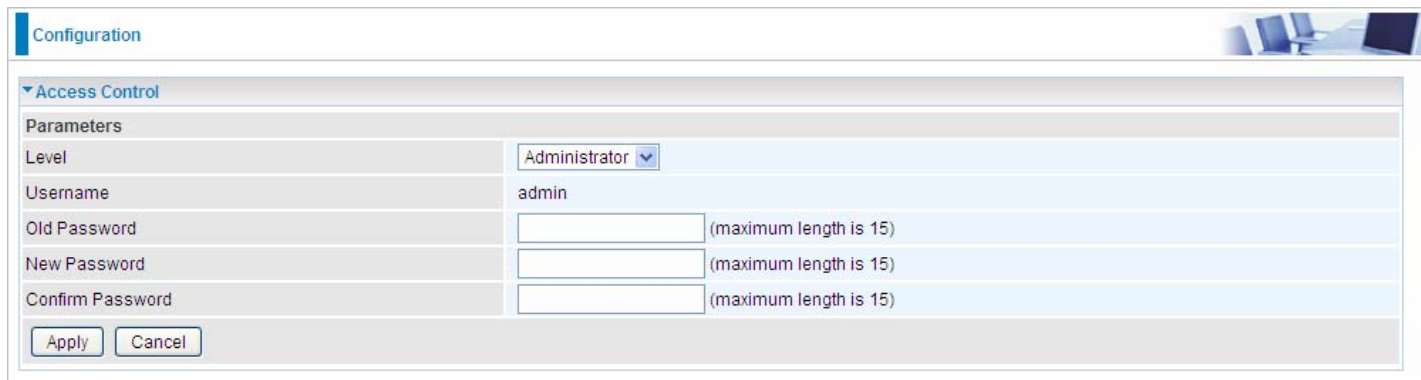
Click **Browse** and browse to the location where your backup file is saved, then click **Open**. Then in the above page, click **Update Settings**, the following process indicating screen will appear. Let it update to 100%, it will automatically turn to the Device Info page.



The screenshot shows a 'progress' screen with a warning: 'Do not switch off device during flash update or rebooting.' Below the warning is a progress bar labeled 'total :'. The progress bar is partially filled with blue, and the text '6%' is displayed to the right of the bar.

## 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 password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. 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 few items would be listed for common user, corresponding default username password are user and user respectively.

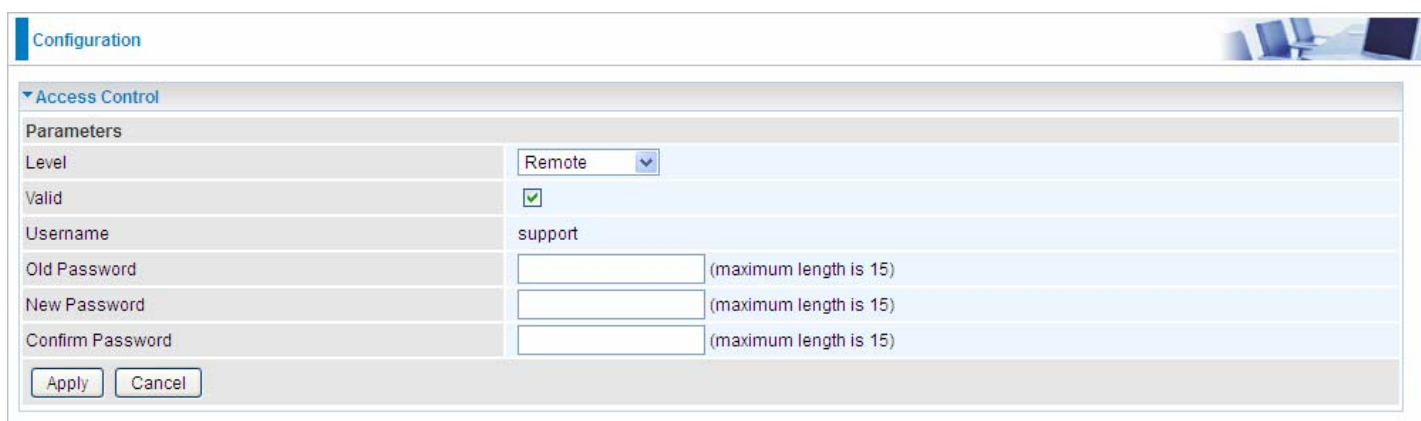
**Username:** The default username for each user level.

**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.

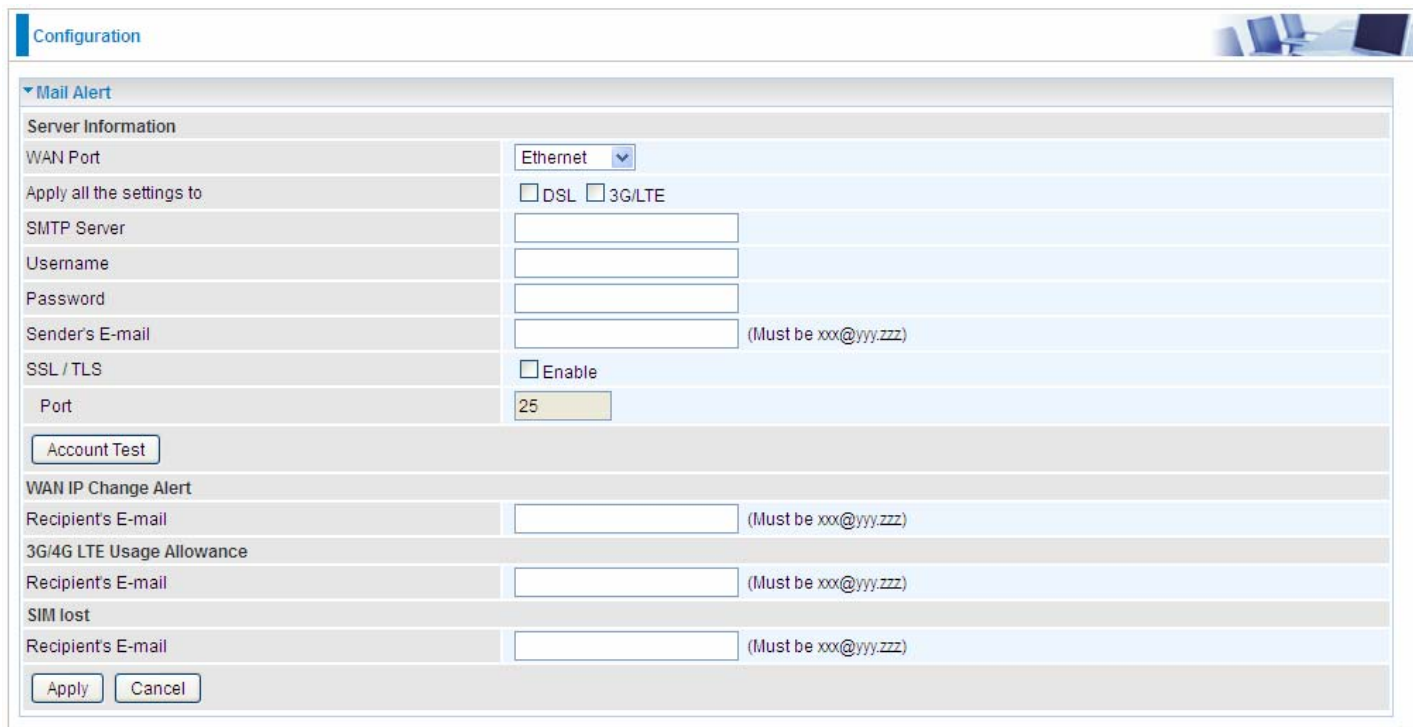


The screenshot shows the 'Configuration' page with the 'Access Control' section expanded. Under 'Parameters', the 'Level' is set to 'Remote'. The 'Valid' checkbox is checked. The 'Username' is 'support'. There are three password fields: 'Old Password', 'New Password', and 'Confirm Password', each with a note '(maximum length is 15)'. 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 page titled "Configuration" with a sub-section for "Mail Alert". The page is divided into several sections:

- Server Information:** Includes a dropdown for "WAN Port" (set to "Ethernet"), checkboxes for "Apply all the settings to" (with "DSL" and "3G/LTE" options), text input fields for "SMTP Server", "Username", and "Password", a text input for "Sender's E-mail" with a validation note "(Must be xxx@yyy.zzz)", a checkbox for "SSL / TLS" (set to "Enable"), and a text input for "Port" (set to "25"). There is an "Account Test" button below this section.
- WAN IP Change Alert:** A text input for "Recipient's E-mail" with a validation note "(Must be xxx@yyy.zzz)".
- 3G/4G LTE Usage Allowance:** A text input for "Recipient's E-mail" with a validation note "(Must be xxx@yyy.zzz)".
- SIM lost:** A text input for "Recipient's E-mail" with a validation note "(Must be xxx@yyy.zzz)".

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

**WAN Port:** Mail Alert feature can be applicable to every WAN mode: Ethernet, DSL and 3G/LTE. Select the port you want to use Mail Alert.

For example DSL, then when the WAN connection is in DSL mode and when there is any unexpected event, the alert message will be sent to your specified E-mail.

**Apply all settings to:** check whether you want to have a copy of the settings to apply to other WAN port, suppose the above Main port is DSL, then if you enable this function, then Ethernet port will have the same configuration.

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

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

**Password:** Enter the password of your email account.

**Sender's Email:** Enter your email address.

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

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

**Account Test:** Press this button to test the connectivity and feasibility to your sender's e-mail.

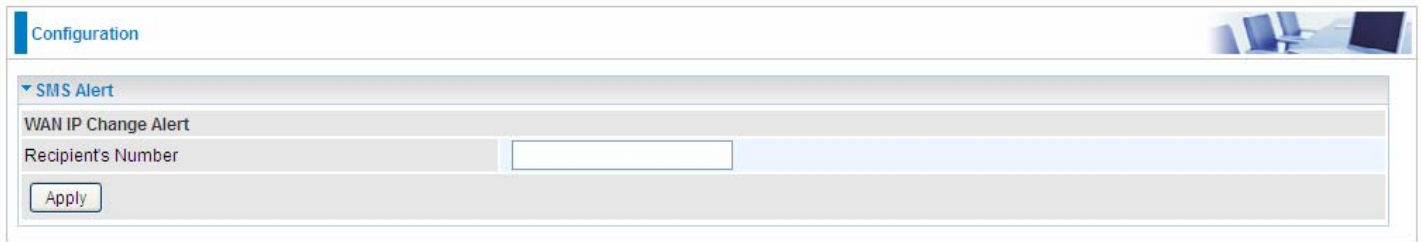
**Recipient's Email (WAN IP Change Alert):** Enter the email address that will receive the alert message once a WAN IP change has been detected.

**Recipient's Email (3G/4G LTE Usage Allowance):** Enter the email address that will receive the alert message once the 3G over Usage Allowance occurs.

**Recipient's Email (SIM lost):** Enter the email address that will receive the alert message once the SIM card loss has been detected.

## SMS Alert

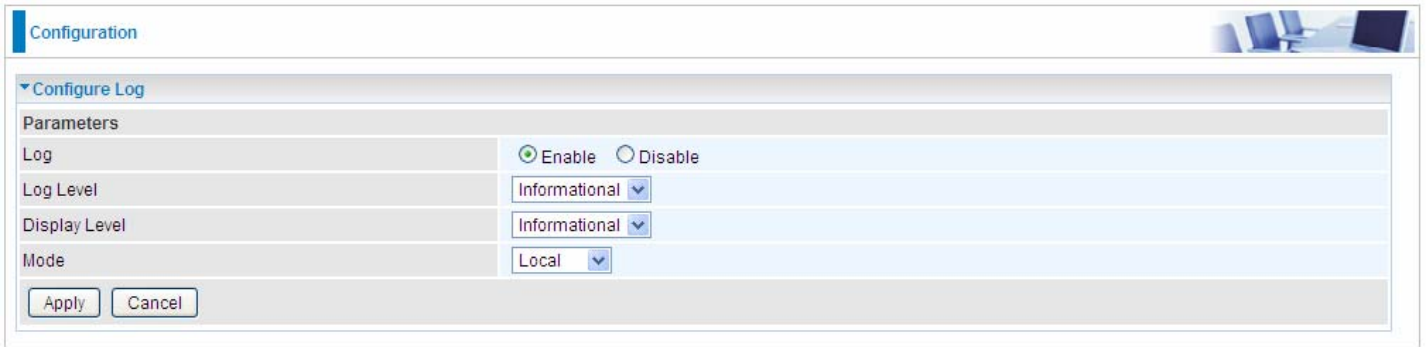
SMS, Short Message Service, is to inform clients the information clients subscribe. The BiPAC 8700NEXL R2 offers SMS alert sending clients alert messages when a WAN IP change is detected.



The screenshot shows a web-based configuration interface. At the top left, there is a 'Configuration' tab. Below it, a section titled 'SMS Alert' is expanded. Under this section, there is a 'WAN IP Change Alert' heading. Below the heading is a label 'Recipient's Number' followed by an empty text input field. At the bottom left of this section is an 'Apply' button. In the top right corner of the configuration area, there is a small graphic of a laptop and a chair.

**Recipient's Number (WAN IP Change Alert):** Enter the Recipient's number that will receive the alert message once a WAN IP change has been detected.

## Configure Log



Configuration

Configure Log

Parameters

Log  Enable  Disable

Log Level Informational

Display Level Informational

Mode Local

Apply Cancel

**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.

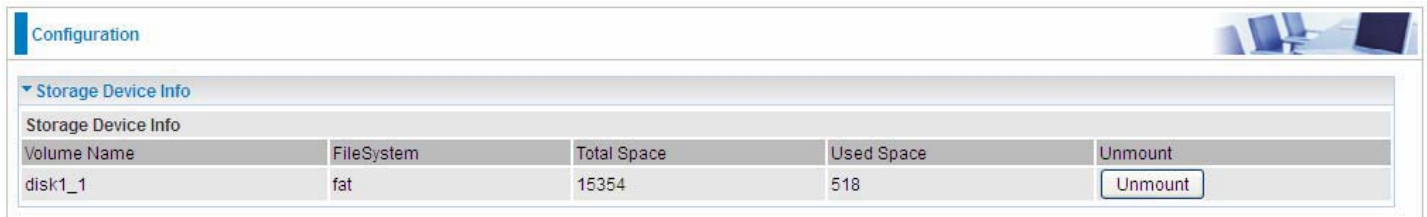
Click **Apply** to save your settings.

# 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 configuration interface with a 'Configuration' header and a 'Storage Device Info' section. The section contains a table with columns for Volume Name, FileSystem, Total Space, Used Space, and an Unmount button. The data row shows 'disk1\_1' with 'fat' file system, 15354 total space, and 518 used space.

Volume Name	FileSystem	Total Space	Used Space	Unmount
disk1_1	fat	15354	518	<input type="button" value="Unmount"/>

**Volume Name:** Display the storage volume name

**FileSystem:** Display the storage device's file system format, well-known is FAT.

**Total Space:** Display the total space of the storage, with unit MB.

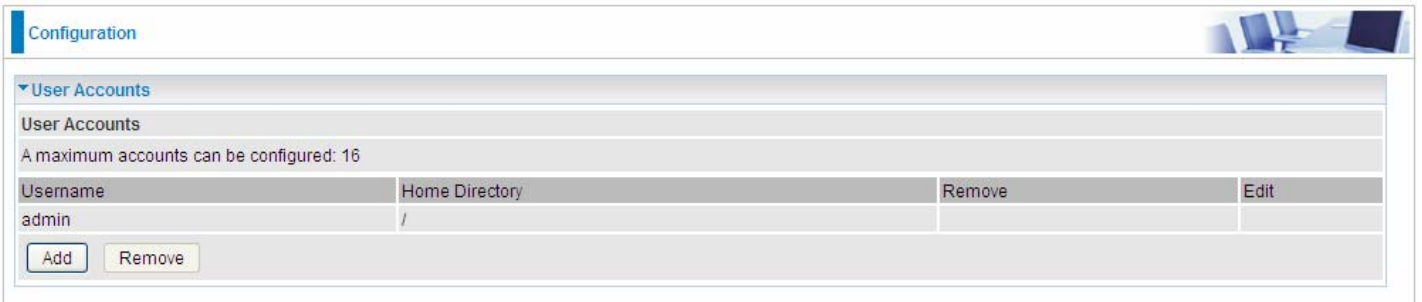
**Used Space:** Display the remaining space of each partition, unit MB.

**Unmount:** Click **Unmount** button if you want to uninstall the USB device. Please **Note** that first click **Unmount** before you uninstall your USB storage.

## User Account

Users here can add user accounts for access to the storage, in this way users can access the network sharing storage with the specified account, and again protect their own data.

Default user admin.



Configuration

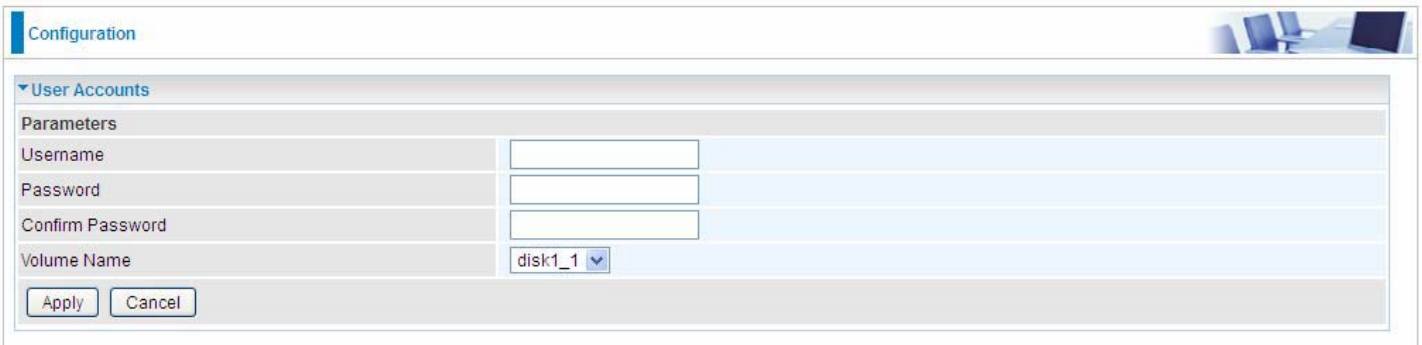
▼ User Accounts

User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		

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



Configuration

▼ User Accounts

Parameters

Username

Password

Confirm Password

Volume Name

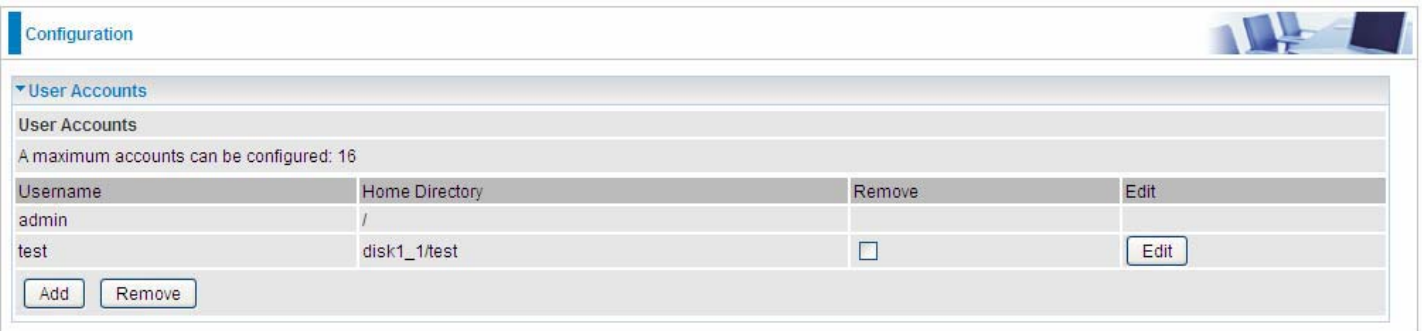
**Username:** user-defined name, but simpler and more convenient to remember would be favorable.

**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 disk1\_1.



Configuration

▼ User Accounts

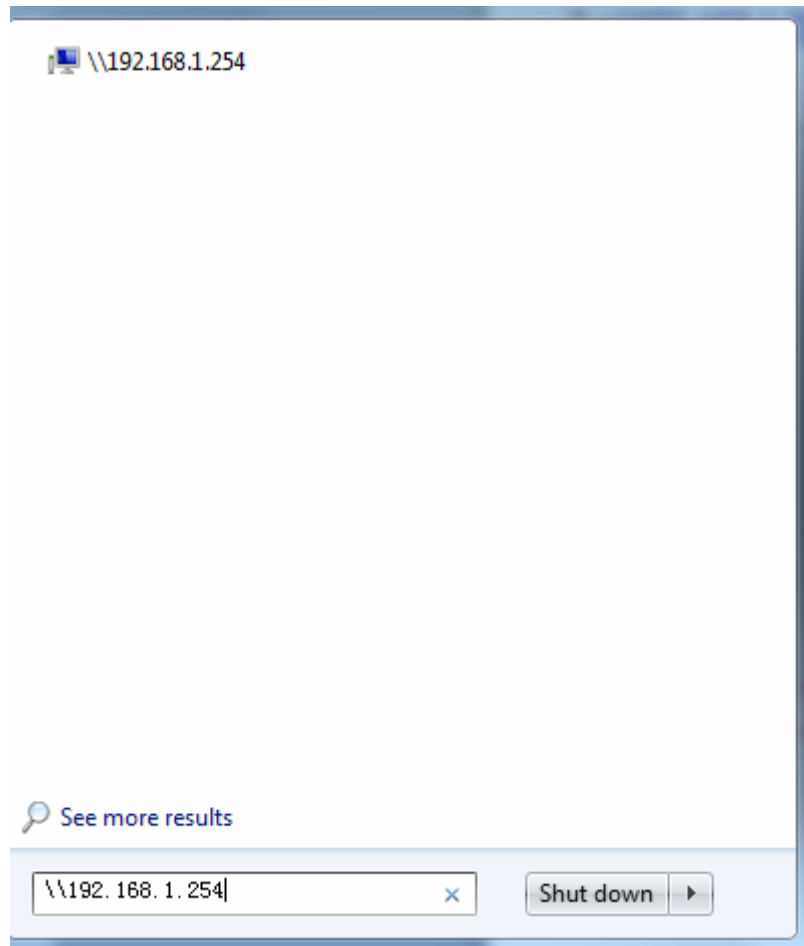
User Accounts

A maximum accounts can be configured: 16

Username	Home Directory	Remove	Edit
admin	/		
test	disk1_1/test	<input type="checkbox"/>	<input type="button" value="Edit"/>

## Accessing mechanism of Storage:

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



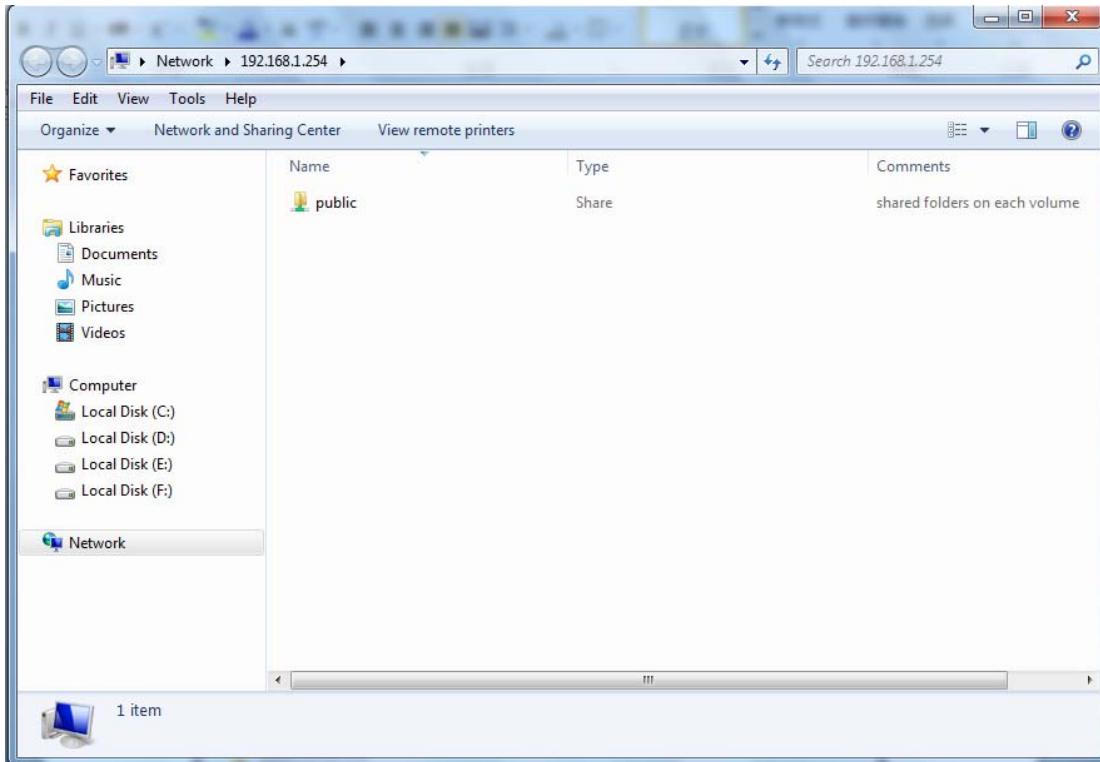


When accessing the network storage, you can see a folder named “**public**”, users should have the account to enter, and the account can be set at the User Accounts section.

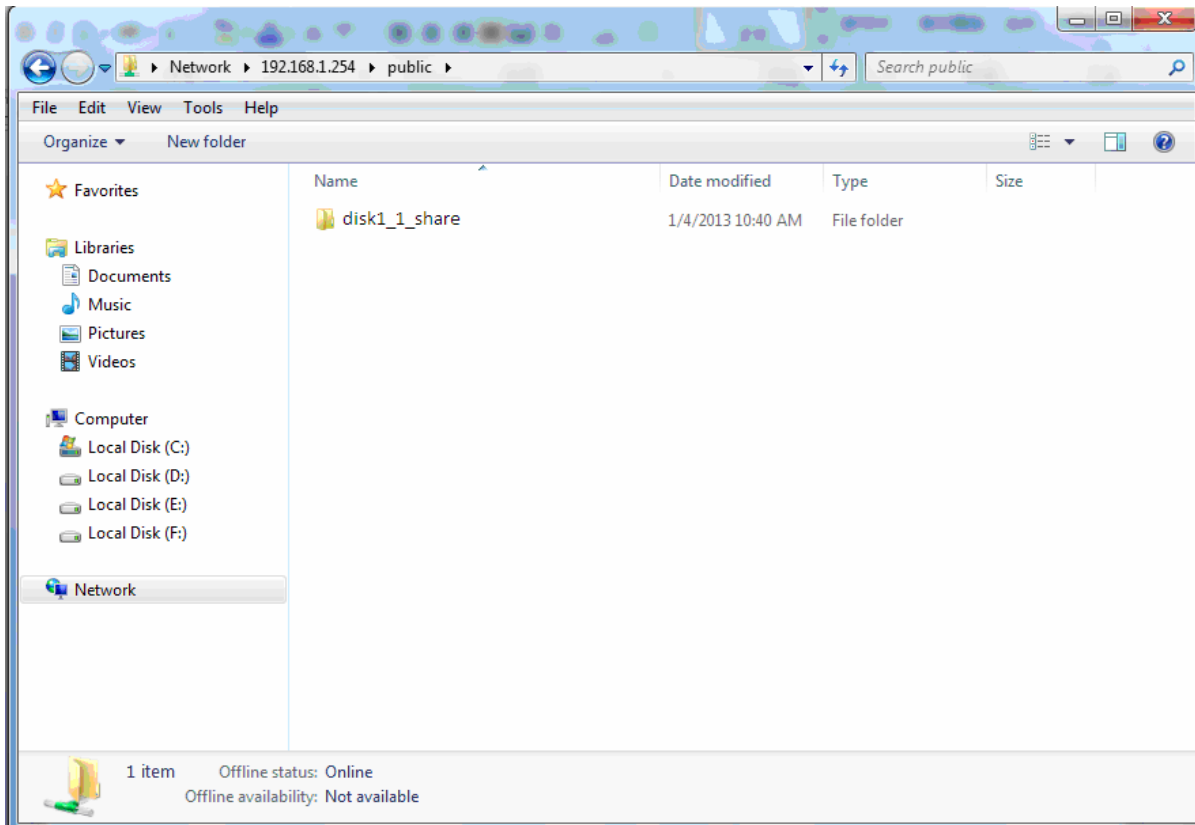
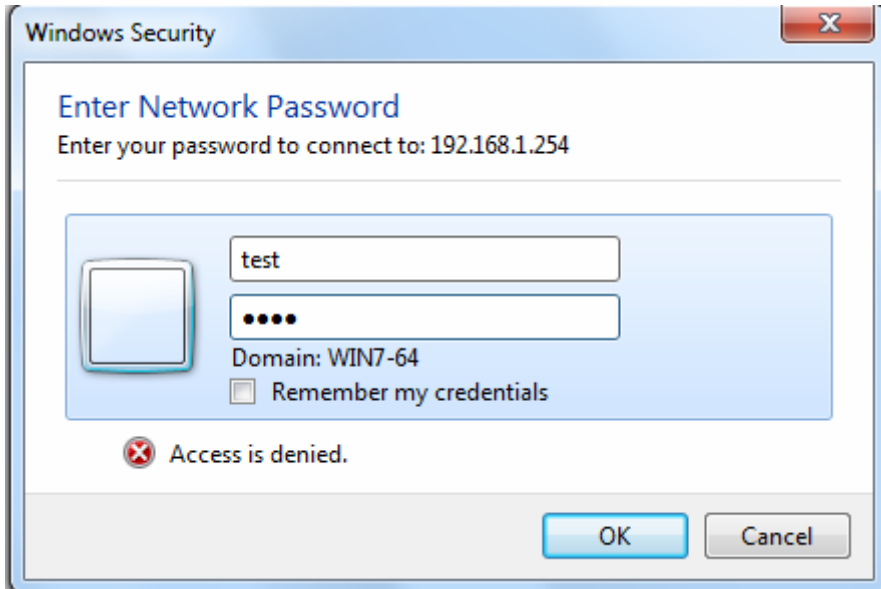
When first logged on to the network folder, you will see the “**public**” folder.

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

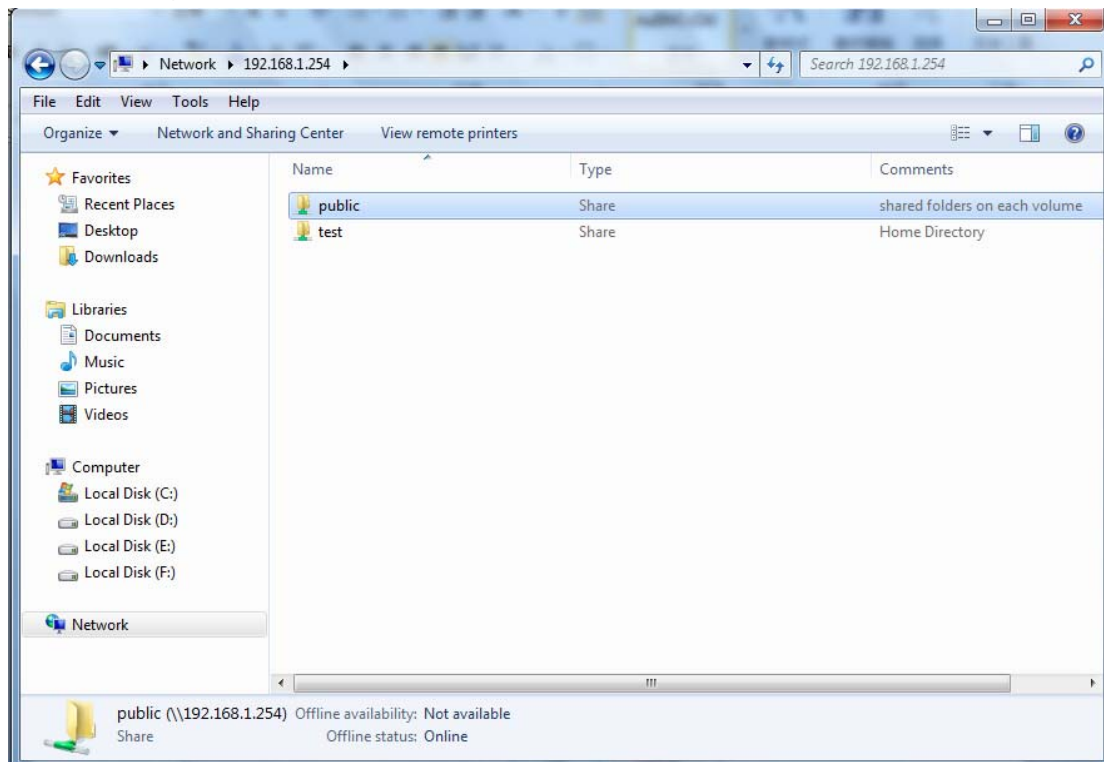
When user register a USB account and log successfully, a private folder (the same name as the user account registered) exclusive for each user is established. Go on to see the details.



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.



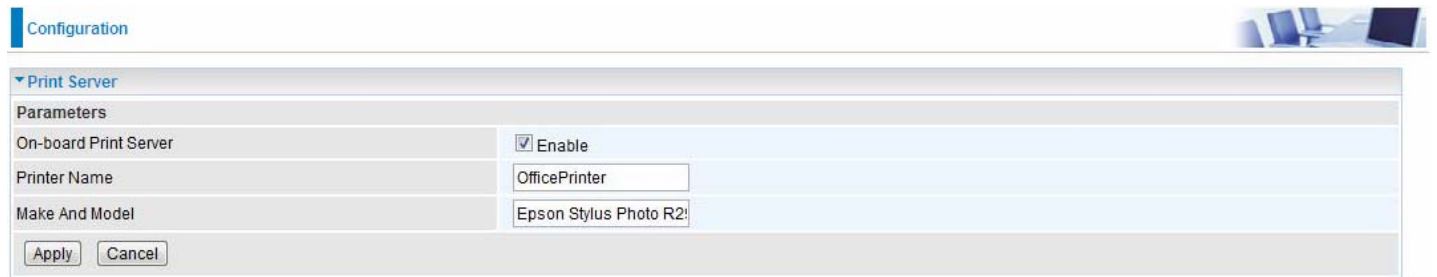
## Print Server

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 8700NEXL R2. This allows you to print from any location on your network.

**Note:** Only USB printers are supported

Setup of the printer is a 3 step process

1. Connect the printer to the 8700NEXL R2's USB port
2. Enable the print server on the 8700NEXL R2
3. Install the printer drivers on the PC you want to print from



Configuration

Print Server

Parameters

On-board Print Server	<input checked="" type="checkbox"/> Enable
Printer Name	OfficePrinter
Make And Model	Epson Stylus Photo R2!

Apply Cancel

**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*

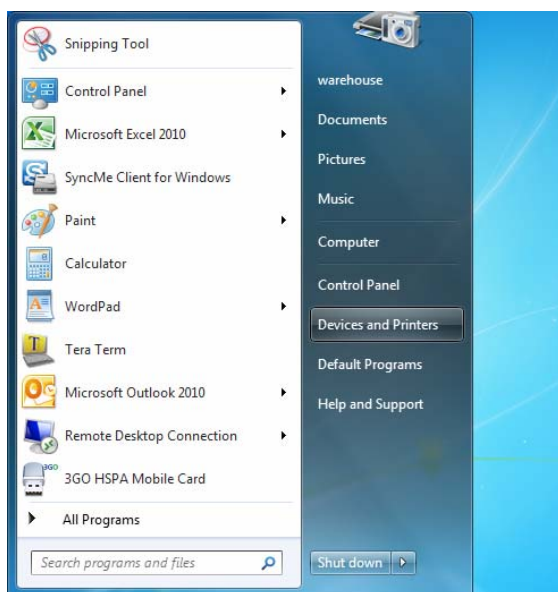
### Note:

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)

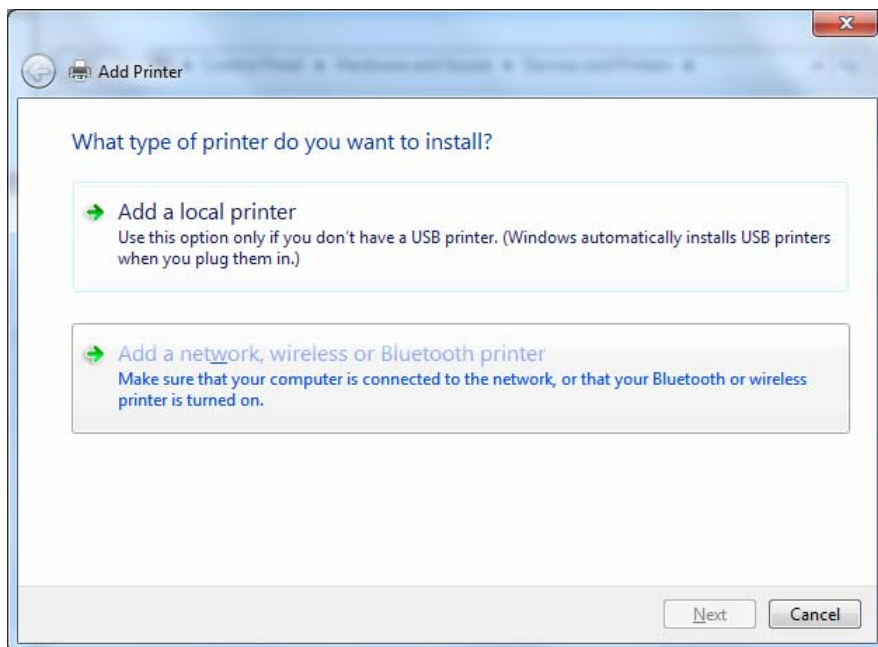
**Step 1:** Click **Start** and select "Devices and Printers"



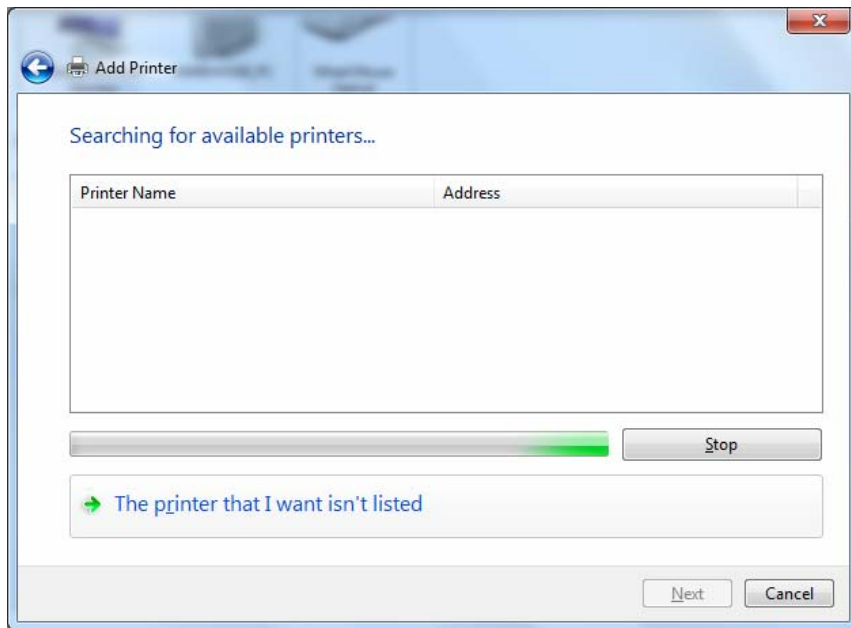
**Step 2:** Click "Add a Printer".



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



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

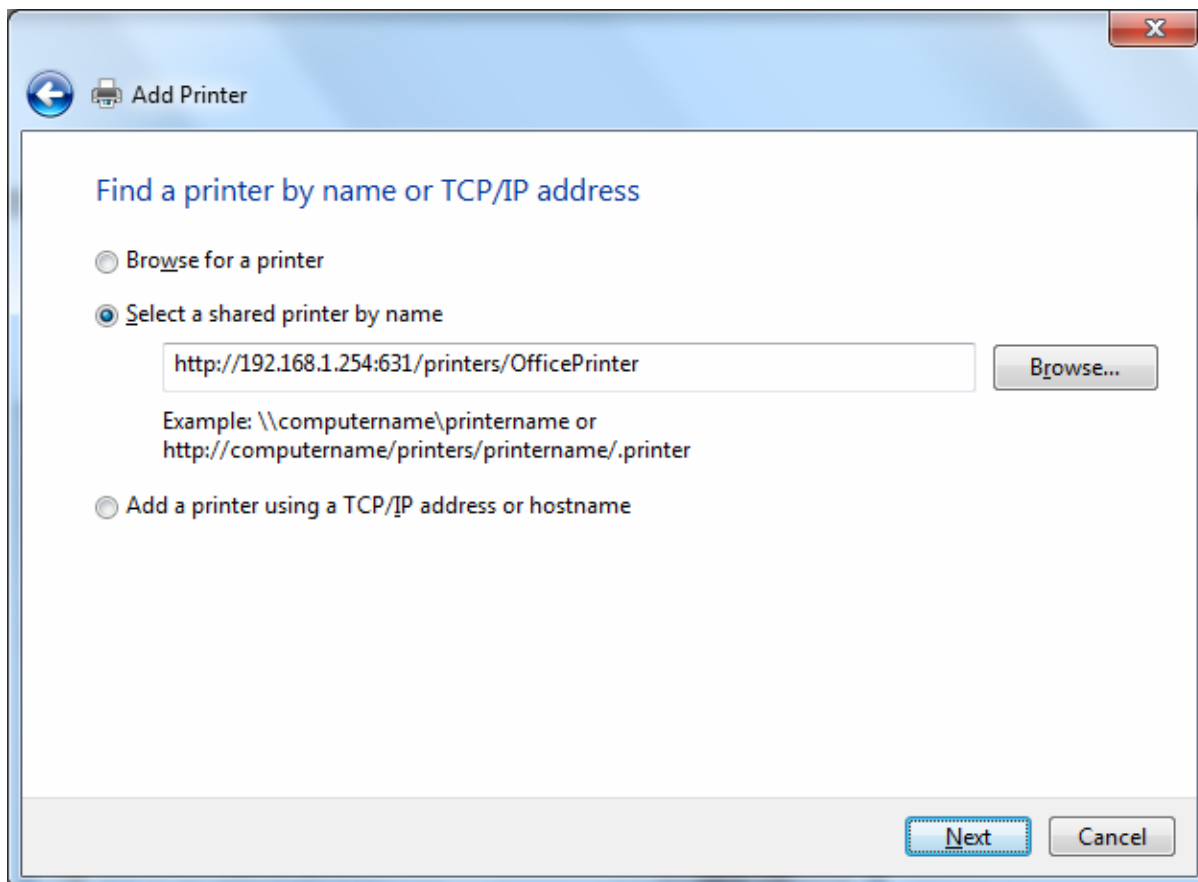


**Step 5:** Select “Select a shared printer by name”

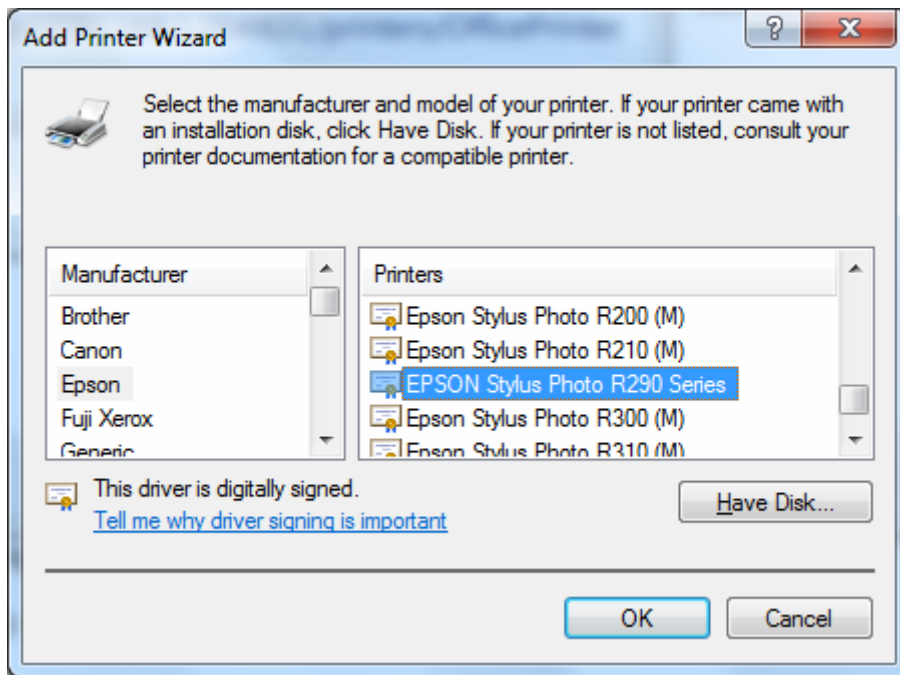
Enter `http://8700NEXL R2- LAN-IP:631/printers/printer-name` or. Make sure printer’s name is the same as what you set in the 8700NEXLR2 earlier

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

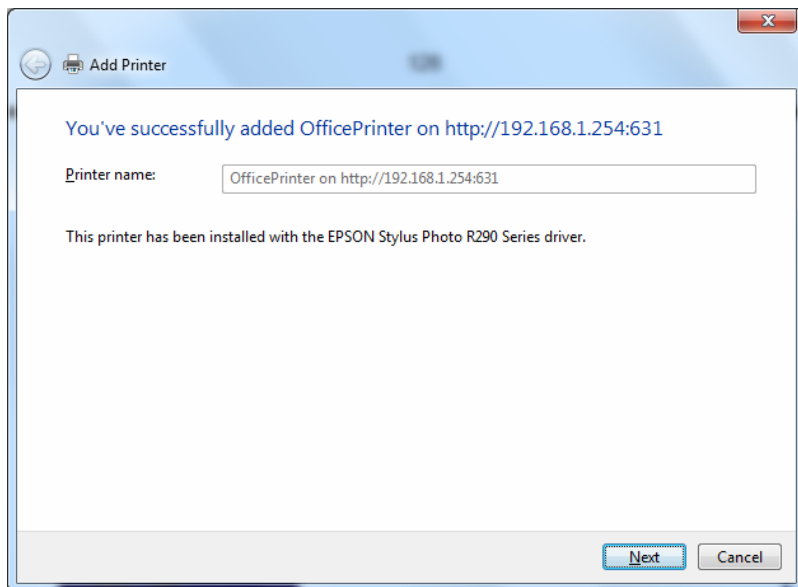
OfficePrinter is the Printer Name we setup earlier



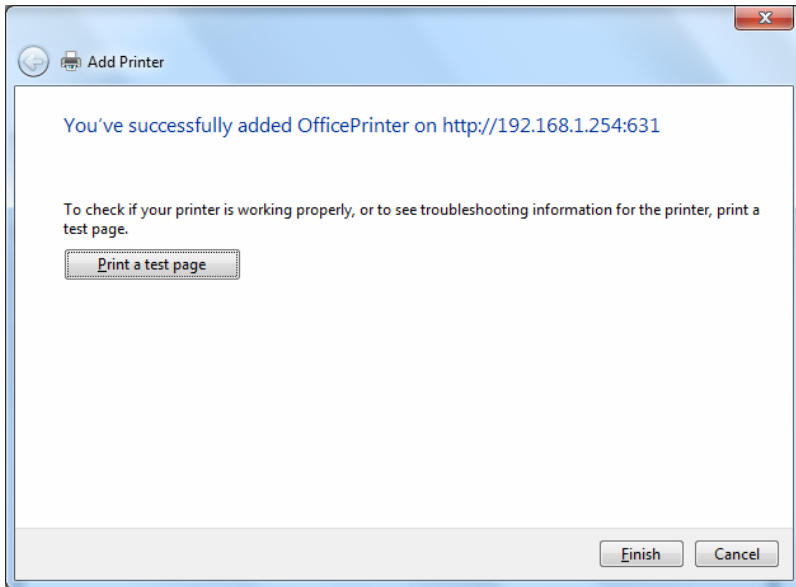
**Step 6:** Click “Next” to add the printer driver. If your printer is not listed and your printer came with an installation disk, click “Have Disk” find it and install the driver.



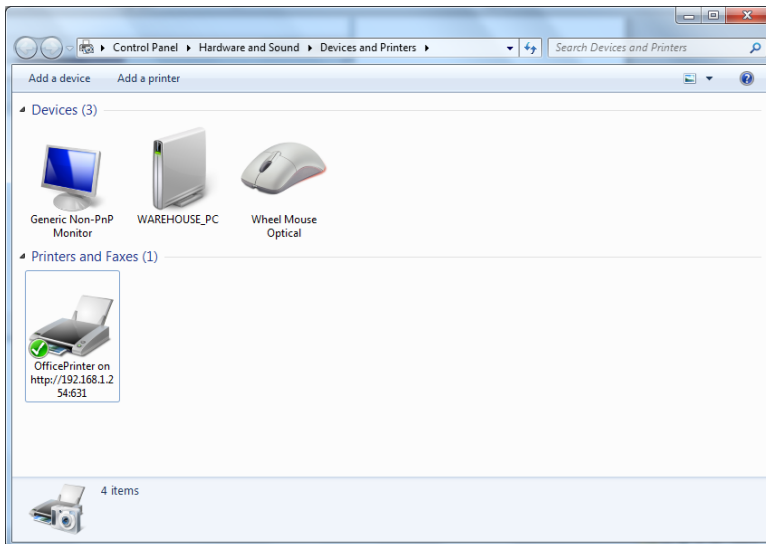
**Step 7:** Click “Next”



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



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





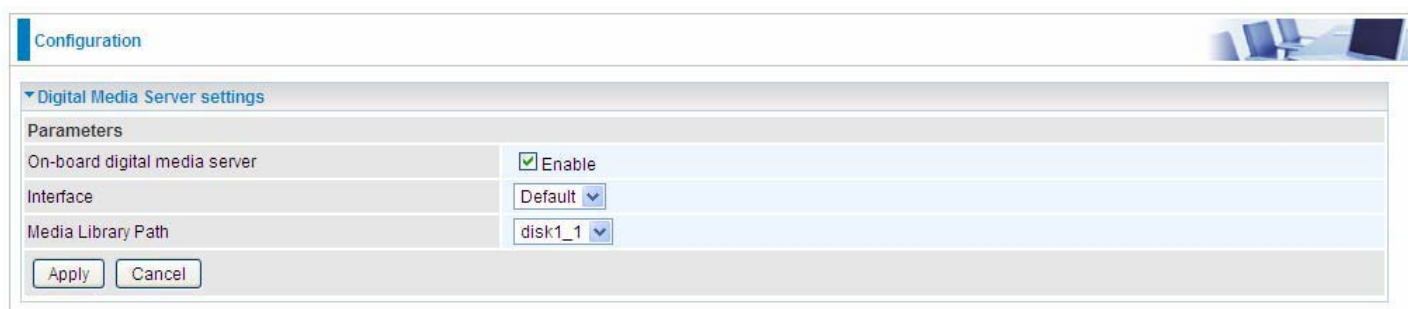
## DLNA

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, 8700NEXL R2 can serve as a DLNA server.



The screenshot shows a web-based configuration interface. At the top, there is a 'Configuration' header. Below it, a section titled 'Digital Media Server settings' is expanded. Under this section, there is a 'Parameters' table with the following settings:

Parameters	
On-board digital media server	<input checked="" type="checkbox"/> Enable
Interface	Default
Media Library Path	disk1_1

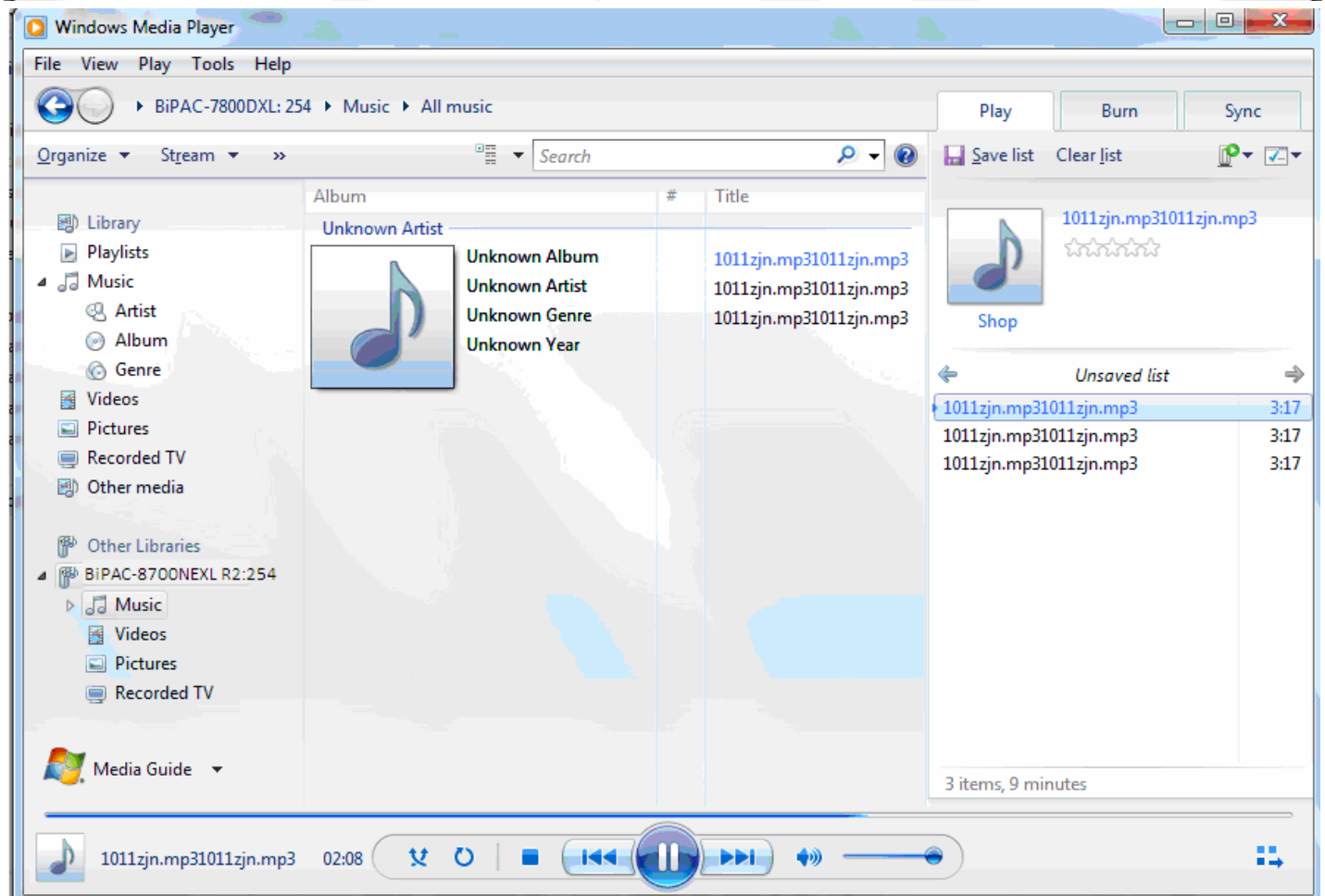
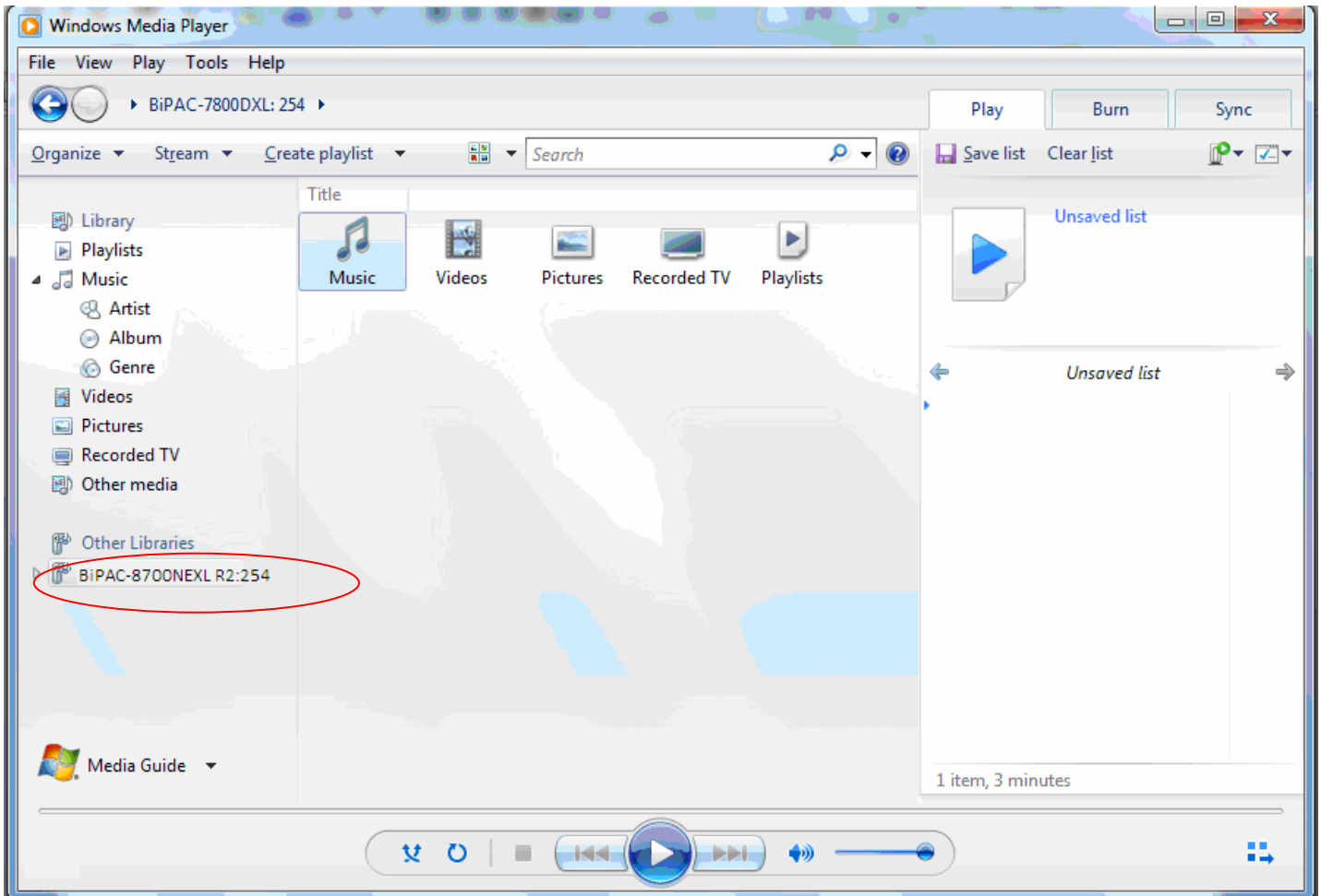
At the bottom of the settings area, there are two buttons: 'Apply' and 'Cancel'.

**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.

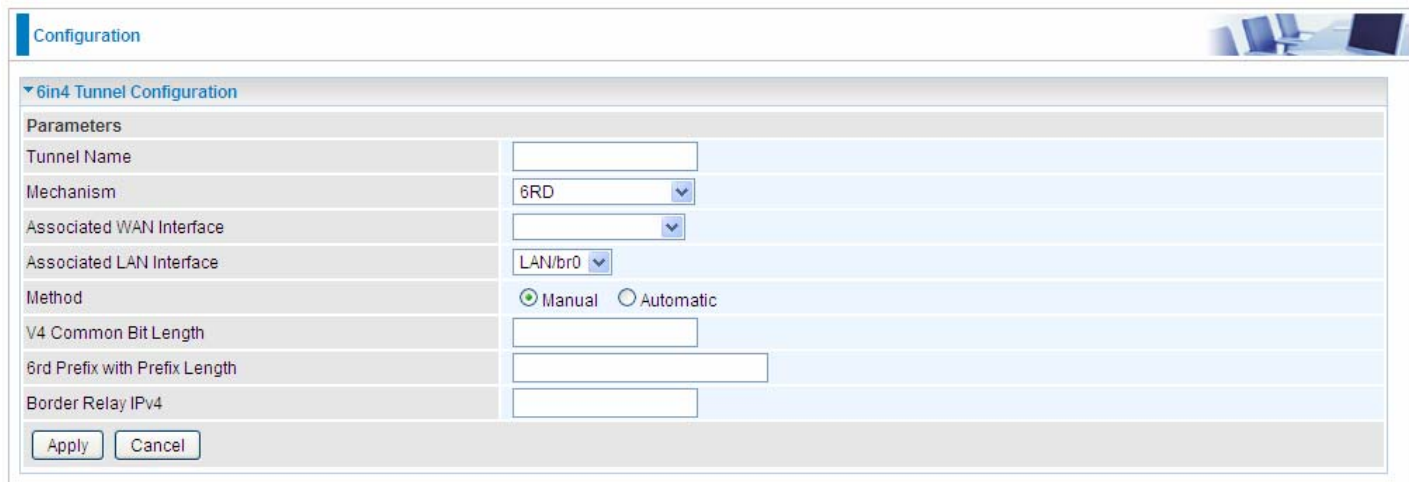
## 6RD:

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.



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



**Tunnel Name:** User-defined name.

**Mechanism:** Here only 6RD.

**Associated WAN Interface:** The applied WAN interface with the set tunnel, thus when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

**Associated LAN Interface:** Set the linked LAN interface with the tunnel.

**Method:** 6rd operation mechanism: manually configured or automatically configured. If manually, please fill out the following 6rd parameters.

**V4 Common Bit Length:** Specify the length of IPv4 address carried in IPv6 prefix, for example, 0 means to carry all the 32 bits of IPv4 address while 8 carries 24 bits of the IPv4 address.

**6rd Prefix with Prefix Length:** Enter the 6rd prefix and prefix length you uniquely designate to 6rd by the ISP( The 6rd prefix and prefix length are to replace the standard 6to4 prefix 2002::/16 by an IPv6 prefix that belongs to the ISP-assigned.)

**Border Relay IPv4 Address:** The IPv4 address of the border relay. The relay is used to unwrap capsulated IPv4 packets into IPv6 packets and send them to the IPv6 network.

## IPv4inIPv6

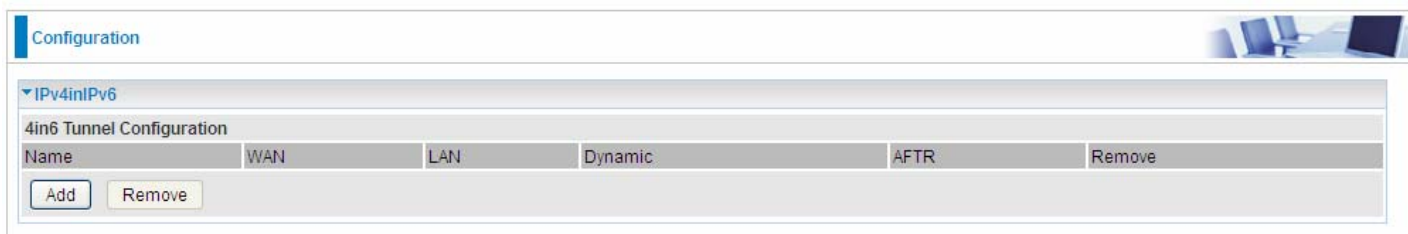
4in6 refers to tunneling of IPv4 in IPv6. It is an inherent internet interoperation mechanism allowing IPv4 to be used in an IPv6 only network.

4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. 4in6 tunnels are usually manually configured but they can be automated using protocols such as TSP to allow easy connection to a tunnel broker.

### DS – Lite

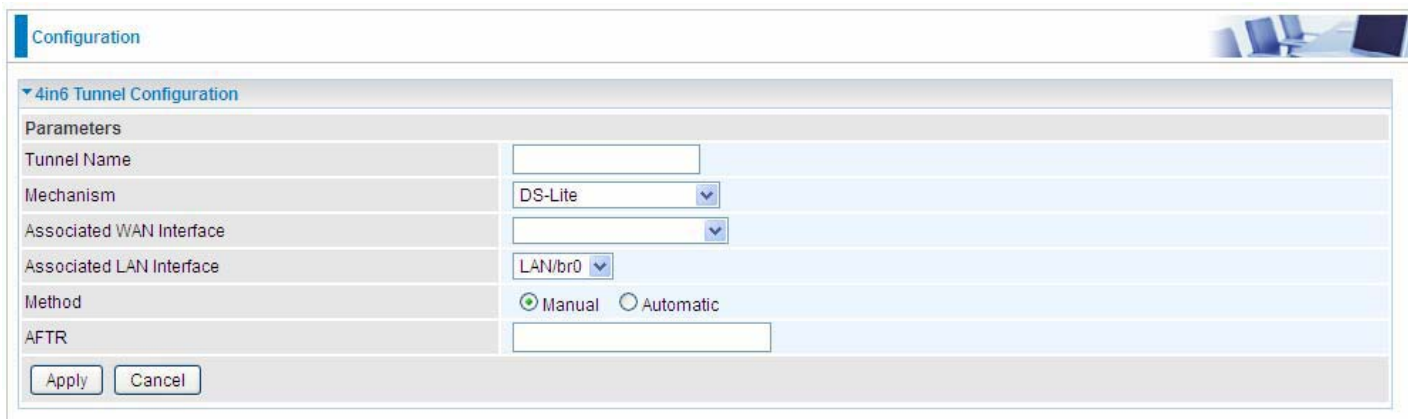
DS –Lite, or Dual-Stack Lite, is designed to let an ISP omit the deployment of any IPv4 address to the customer's CPE. Instead, only global IPv6 addresses are provided (Regular Dual-Stack Lite deploys global addresses for both IPv4 and IPv6).

The CPE distributes private IPv4 addresses for the LAN clients, the same as a NAT device. The subnet information is chosen by the customer, identically to the NAT model. However, instead of performing the NAT itself, the CPE encapsulates the IPv4 packet inside an IPv6 packet.



The screenshot shows a web interface for configuring IPv4inIPv6 tunnels. At the top, there is a 'Configuration' header. Below it, a section titled 'IPv4inIPv6' contains a table for '4in6 Tunnel Configuration'. The table has columns for Name, WAN, LAN, Dynamic, AFTR, and Remove. There is one entry with Name 'WAN', LAN 'LAN', Dynamic 'Dynamic', and AFTR 'AFTR'. 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 options:

- 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.
- Method:** Radio buttons for 'Manual' (selected) and 'Automatic'.
- AFTR:** A text input field.

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

**Tunnel Name:** User-defined tunnel name.

**Mechanism:** It is the 4in6 tunnel operation technology. Please select DS-Lite.

**Associated WAN Interface:** The applied WAN interface with the set tunnel, and when there are packets from/to the WAN interface, the tunnel would be used to transport the packets.

**Associated LAN Interface:** Specify the linked LAN interface with the tunnel.

**Method:** Manually to specify the AFTP (Address Family Transition Router) address or Automatic.

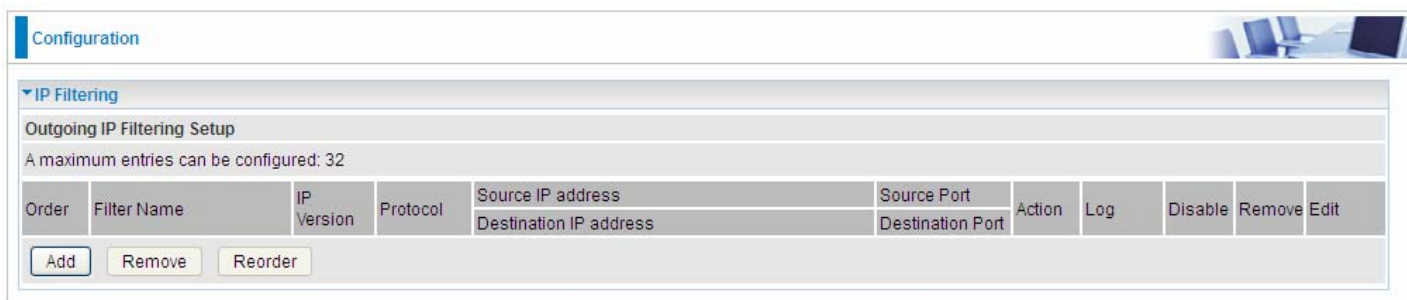
**AFTR:** Specify the address of AFTP (Address Family Transition Router) from your ISP.

# Security

## IP Filtering Outgoing

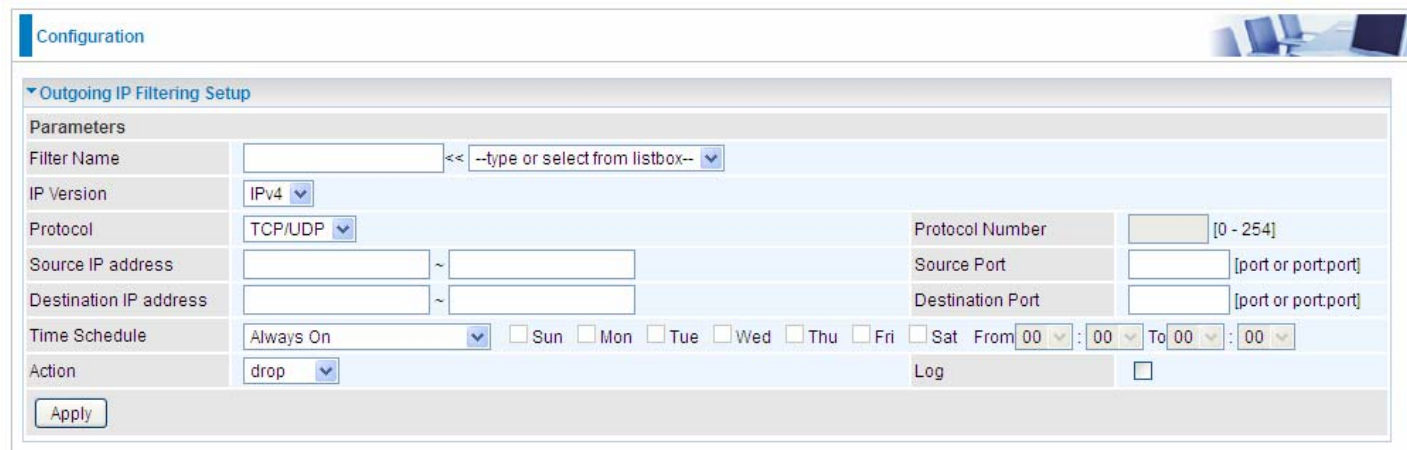
IP filtering enables you to configure your router to block specified internal/external users (**IP address**) from Internet access, or you can disable specific service requests (**Port number**) to /from Internet. The relationship among all filters is “**or**” operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.

**Note:** The maximum number of entries: 32.



The screenshot shows the 'Configuration' page with the 'IP Filtering' section expanded to 'Outgoing IP Filtering Setup'. A note states 'A maximum entries can be configured: 32'. Below this is a table with columns: Order, Filter Name, IP Version, Protocol, Source IP address, Destination IP address, Source Port, Destination Port, Action, Log, Disable, Remove, and Edit. At the bottom of the table are buttons for 'Add', 'Remove', and 'Reorder'.

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



The screenshot shows the 'Outgoing IP Filtering Setup' configuration page. It includes fields for: Filter Name (with a dropdown), IP Version (IPv4), Protocol (TCP/UDP), Protocol Number (0-254), Source IP address, Destination IP address, Source Port, Destination Port, Time Schedule (Always On, with checkboxes for days of the week and a time range), Action (drop), and Log (checkbox). An 'Apply' button is at the bottom.

**Filter Name:** A user-defined rule name. User can select simply from the list box for the application for quick setup.

**IP Version:** Select the IP Version, IPv4 or IPv6.

**Protocol:** Set the traffic type (TCP/UDP, TCP, UDP, ICMP, RAW, Any) 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.

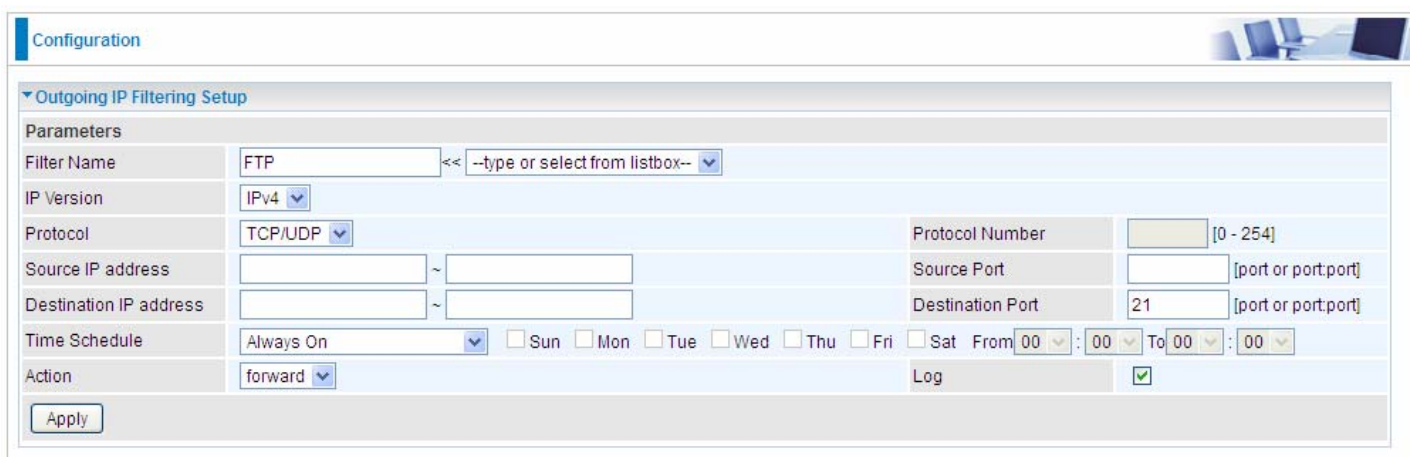
65535.

**Time Schedule:** Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon  in list table indicating the rule is inactive. See [Time Schedule](#).

**Action:** Select to **drop** or **forward** the packets fit the outgoing filtering rule.

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

**Example:** For example, if there is an outgoing rule set as follows, then the 21 application between source IP and destination IP will be blocked. Or exactly in the rule below, all traffic trying to access FTP will be blocked.



Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name: FTP << --type or select from listbox--

IP Version: IPv4

Protocol: TCP/UDP Protocol Number: [0 - 254]

Source IP address: ~

Source Port: [port or port:port]

Destination IP address: ~

Destination Port: 21 [port or port:port]

Time Schedule: Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

Action: forward Log:

Apply

." data-bbox="52 506 939 662"/>

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

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

Add Remove Reorder

(The rule is active; disable field shows the status of the rule, active or inactive)

Add another Outgoing IP Filtering rule, users will find the “arrow” icon to change the IP outgoing filter rule working orders.

; and Filter Name: HTTP, IP Version: 4, Protocol: TCP, Source IP address: Any, Destination IP address: Any, Source Port: Any, Destination Port: 80, Action: drop, Log: Disable, Disable: . The 'Order' column has arrows indicating the rule order." data-bbox="52 736 939 916"/>

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

Order	Filter Name	IP Version	Protocol	Source IP address	Destination IP address	Source Port	Destination Port	Action	Log	Disable	Remove	Edit
↓	FTP	4	TCP	Any	Any	Any	21	forward	Disable	<input type="checkbox"/>		Edit
↑	HTTP	4	TCP	Any	Any	Any	80	drop	Disable	<input type="checkbox"/>		Edit

Add Remove Reorder

## How to disable set rule.

Configuration

Outgoing IP Filtering Setup

Parameters

Filter Name	FTP	<< --type or select from listbox--
IP Version	IPv4	
Protocol	TCP	Protocol Number [0 - 254]
Source IP address		Source Port [port or port:port]
Destination IP address		Destination Port 21 [port or port:port]
Time Schedule	Disable	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat From 00 : 00 To 00 : 00
Action	forward	Log <input checked="" type="checkbox"/>

Apply

Configuration

IP Filtering

Outgoing IP Filtering Setup

A maximum entries can be configured: 32

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

Add Remove Reorder

(Rule inactive)



## IP Filtering Incoming

Incoming IP Filtering is set by default to **block** all incoming traffic, but user can set rules to **forward** the specific incoming traffic.

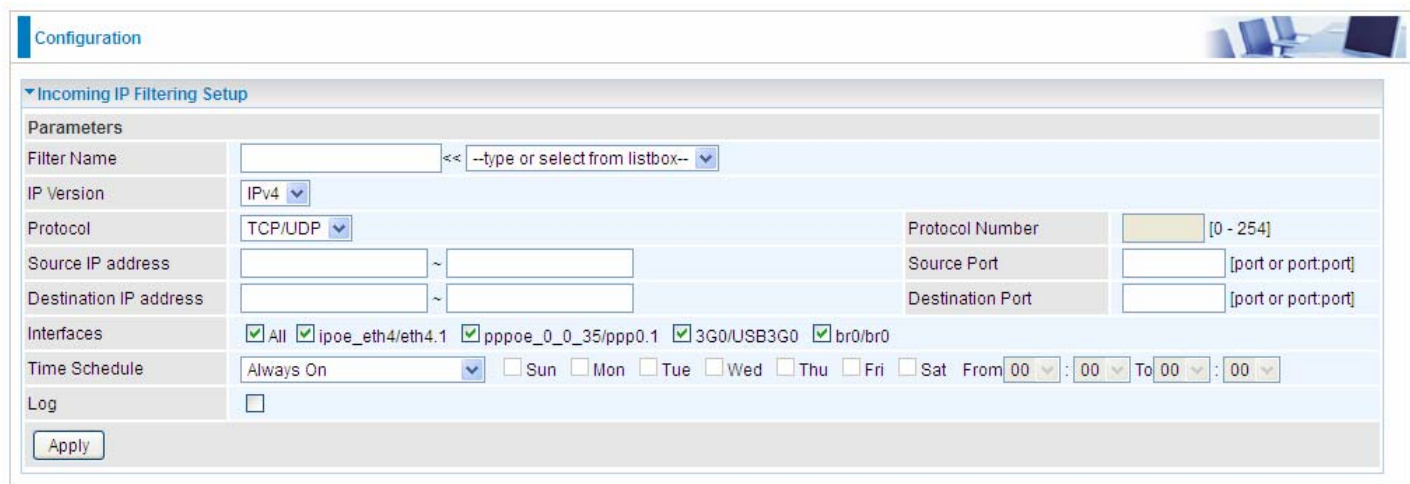
### Note:

1. The maximum number of entries: 32.
2. When LAN side firewall or firewall in WAN interface(s) is enabled, user can move here to add allowing rules to pass through the firewall.



The screenshot shows the 'Configuration' page for IP Filtering. Under 'Incoming IP Filtering Setup', it states 'A maximum entries can be configured: 32'. Below this is a table with columns: Filter Name, Interfaces, IP Version, Protocol, Source IP address, Destination IP address, Source Port, Destination Port, Log, Disable, Remove, and Edit. There are 'Add' and 'Remove' buttons below the table.

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



The screenshot shows the 'Incoming IP Filtering Setup' configuration page. It includes fields for Filter Name, IP Version (IPv4), Protocol (TCP/UDP), Source IP address, Destination IP address, Source Port, Destination Port, Interfaces (All, ipoe\_eth4/eth4.1, pppoe\_0\_0\_35/ppp0.1, 3G0/USB3G0, br0/lbr0), Time Schedule (Always On), and Log. There is an 'Apply' button at the bottom.

**Filter Name:** A user-defined rule name. User can select simply from the list box for the application for quick setup.

**IP Version:** Select the IP Version, IPv4 or IPv6.

**Protocol:** Set the traffic type (TCP/UDP, TCP, UDP, ICMP, RAW, Any ) that the rule applies to.


**Source IP address:** This is the Address-Filter used to allow or block traffic to/from particular IP address(es) featured in the IP range.. If you leave empty, it means any IP address.

**Source Port [port or port:port]:** The port or port range defines traffic from the port (specific application) or port in the set port range blocked to go through the router. Default is set port from range 1 – 65535.

**Destination IP address:** Traffic from LAN with the particular traffic destination address specified in the IP range is to be blocked from going through the router, similarly set as the Source IP address above.

**Destination Port [port or port : port]:** Traffic with the particular set destination port or port in the set port range is to be blocked from going through the router. Default is set port from port range: 1 – 65535

**Interfaces:** Check if the filter rule applies to all interfaces. User can base on need select interfaces to make the rule take effect with those interfaces.

**Time Schedule:** Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”  ” in the list table indicating the rule is inactive. See [Time Schedule](#).

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

## MAC Filtering

MAC Filtering is only effective on ATM PVCs configured in Bridged mode.

**FORWARDED** means that all MAC layer frames will be **forwarded** except those matching with any of the specified rules in the following table.

**BLOCKED** means that all MAC layer frames will be **blocked** except those matching with any of the specified rules in the following table.

Configuration

MAC Filtering

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface

Interface	Policy	Change
atm0.1	FORWARD	<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 LAN<=>WAN

WAN Interface br\_eth0/eth0.2

Apply

**Protocol type:** Select from the drop-down menu the protocol that applies to this rule.

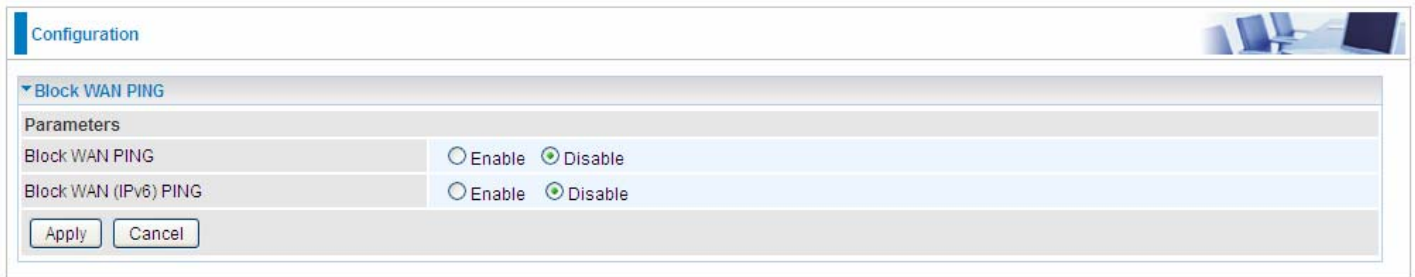
**Destination /Source MAC Address:** Enter the destination/source address.

**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.



The screenshot shows a configuration interface for a router. At the top left, there is a blue header with the word "Configuration". Below this, there is a section titled "Block WAN PING" with a dropdown arrow. Underneath, there is a "Parameters" section. It contains two rows of configuration options:

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

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

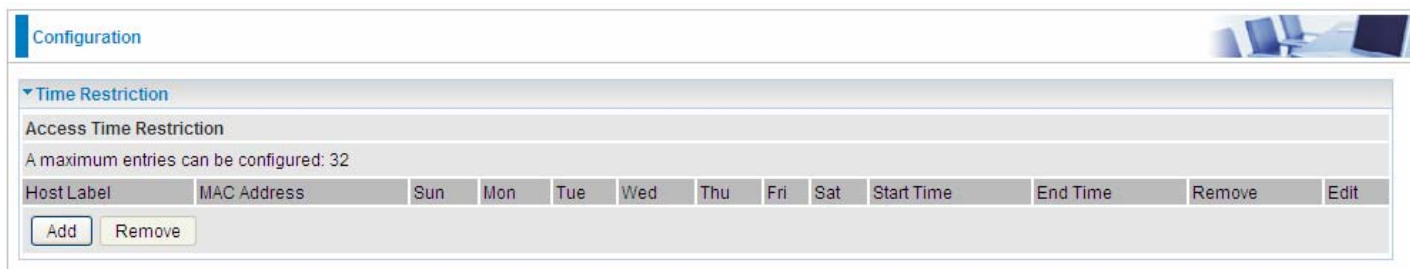
## Time Restriction

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. Please click Add button to add the device(s) to be subject to Time Restriction rules (forward or drop connection to internet). Devices Not added will not comply with the rules and access internet and router willingly.

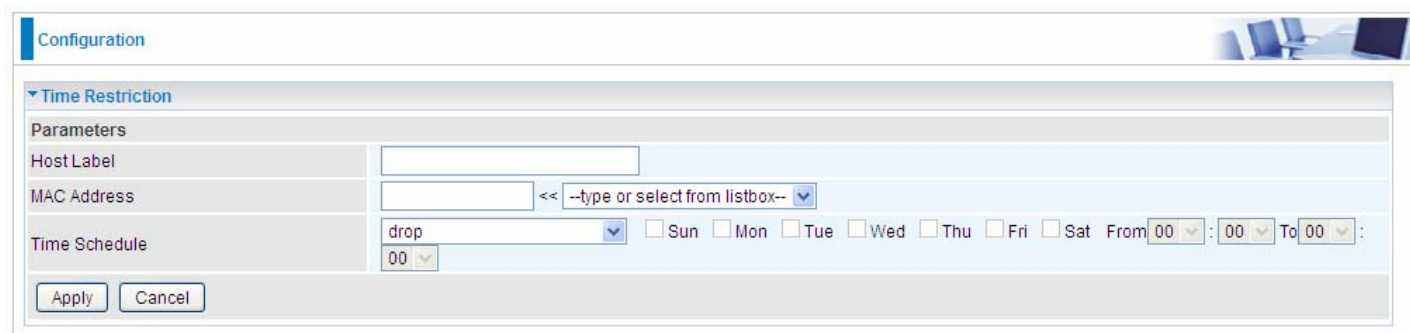
To find out the MAC address of a window based PC, go to command window, and type "ipconfig/all".

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



The screenshot shows the 'Configuration' page for 'Time Restriction'. It features a table with the following columns: Host Label, MAC Address, Sun, Mon, Tue, Wed, Thu, Fri, Sat, Start Time, End Time, Remove, and Edit. Below the table are 'Add' and 'Remove' buttons. A note above the table 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' and 'MAC Address'. The 'Time Schedule' section has a dropdown menu set to 'drop', checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat), and time selection fields for 'From' and 'To' times, both set to '00:00'. 'Apply' and 'Cancel' buttons are at the bottom.

**Host Label:** User-defined name.

**MAC Address:** Enter the MAC address(es) you want to allow or block to access the router and LAN. The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx. For convenience, user can select from the list box.

**Time Schedule:** Configure to control the PC from accessing router and internet.

- ① **Drop:** To drop the MAC entries always; in other words, the MACs are blocked access to router and internet always.
- ① **Forward:** To forward the MAC entries always; in other words, the MACs are granted access to the router and internet always.
- ① **Check or select from listbox:** To set the time duration during which the MACs are blocked from access the router and internet. "**select from listbox**" means that you can select the already set timeslot in "**Time Schedule**" section during which the MACs are blocked from access the router and internet.

Click **Apply** to confirm your settings. The following prompt window will appear to remind you of the attention.

An example:

The screenshot shows a configuration page titled "Configuration" with a sub-section "Time Restriction". Under "Access Time Restriction", it states "A maximum entries can be configured: 32". Below this is a table with columns for Host Label, MAC Address, and days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat), along with Start Time, End Time, and actions (Remove, Edit). Two entries are shown: "test" with MAC 18:a9:05:38:04:03 and "forward" restriction, and "child-use" with MAC 18:a9:05:04:12:23 and a restriction from 00:00 to 23:59 on Mon-Fri. Red circles highlight the "Remove" checkboxes for both entries and the "Remove" button at the bottom left.

Host Label	MAC Address	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Remove	Edit	
test	18:a9:05:38:04:03	forward										<input type="checkbox"/>	Edit
child-use	18:a9:05:04:12:23		x	x	x	x	x		00:00	23:59	<input type="checkbox"/>	Edit	

Buttons: 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. The “test” can access the internet always.

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

## URL Filter

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

### Note:

- 1) URL Filter rules apply to both IPv4 and IPv6 sources.
- 2) But in **Except IP Address** part, user can click [Detail](#) to set the exception IP address(es) for IPv4 and IPv6 respectively.

The screenshot shows a configuration window titled "Configuration" with a "URL Filter" section. The "Parameters" area includes:

- 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 00:00 To 00:00 (pickers)

Buttons for "Apply" and "Cancel" are located at the bottom left.

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

**Domains Filtering:** This function checks the whole URL address but not the IP address against your list of domains to block or allow. If it is matched, the URL request will either be sent (Trusted) or dropped (Forbidden).

**Restrict URL Features:** Click Block Java Applet to filter web access with Java Applet components. Click Block ActiveX to filter web access with ActiveX components. Click Block Cookie to filter web access with Cookie components. Click Block Proxy to filter web proxy access.

**Exception IP Address:** You can input a list of IP addresses as the exception list for URL filtering. These IPs will not be covered by the URL rules.

**Time Schedule:** Select or set exactly when the rule works. When set to “Always On”, the rule will work all time; and also you can set the precise time when the rule works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled. See [Time Schedule](#).

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

## Keywords Filtering

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

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



Configuration

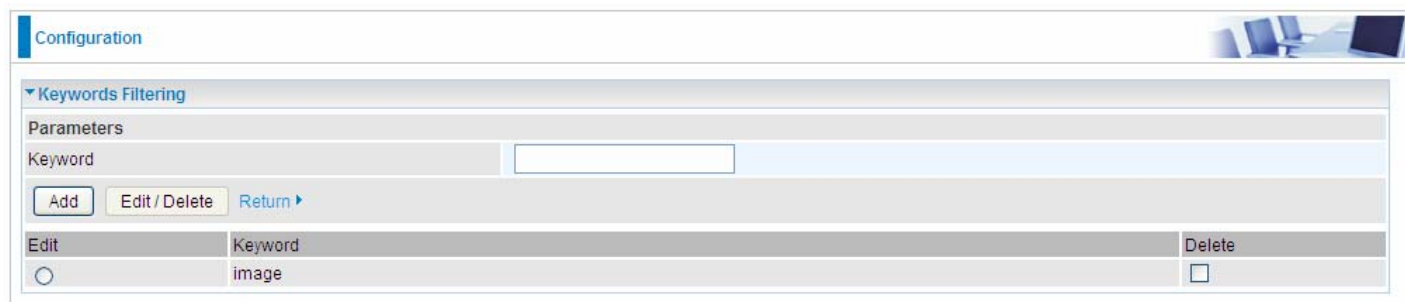
▼ Keywords Filtering

Parameters

Keyword

[Return ▶](#)

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



Configuration

▼ Keywords Filtering

Parameters

Keyword

[Return ▶](#)


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.

## Domains Filtering

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

Click [Detail ▶](#) to add Domains.



Configuration

▼ Domains Filtering

Parameters

Domains Filtering  Type

[Return ▶](#)

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

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

- ① **Forbidden Domain:** The domain is forbidden access.
- ① **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.

### Except 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 configuring URL filtering. At the top, there is a 'Configuration' tab. Below it, a section titled 'Except IP Address' is expanded. Under the 'Parameters' heading, there are two rows: 'IP Version' with a dropdown menu set to 'IPv4', and 'Internal IP Address' with two empty text input boxes separated by a tilde (~). At the bottom of this section, there are three buttons: 'Add', 'Edit / Delete', and 'Return ▶'.

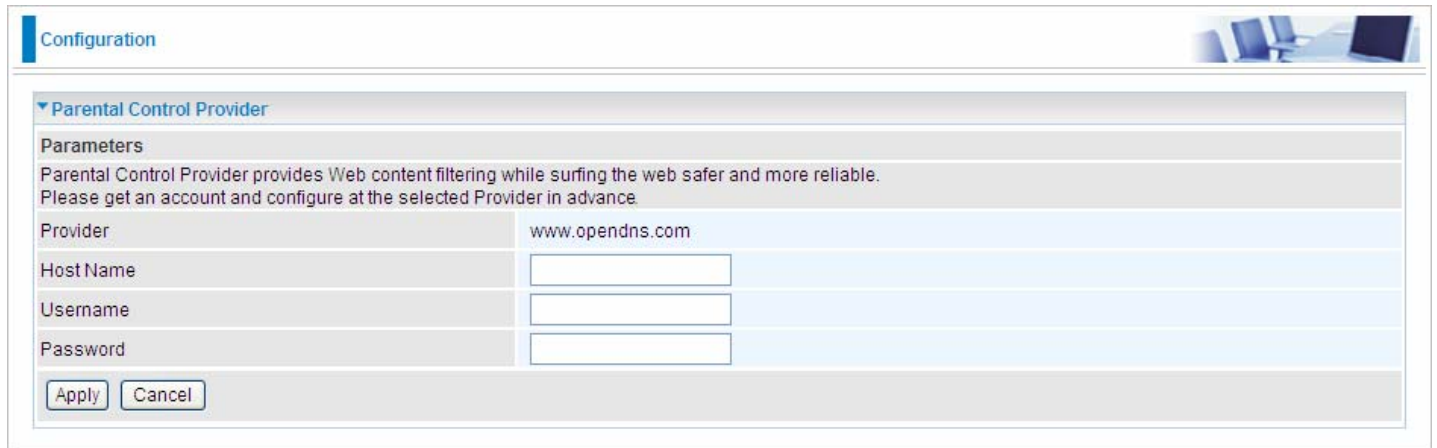
Enter the except IP address. Click **Add** to save your changes. The IP address will be entered into the **Except List**, and excluded from the URL filtering rules in effect. For specific process, please refer to **Keywords Filtering**.

For example, users can set IPv4 client 192.168.1.103 in your network as a exception address that is not limited to the rules set in URL filter ( or IPv4 clients (a range) ). And also an IPv6 client (2000:1211:1002:6ba4:d160:5adb:9009:87ae) or IPv6 clients(a range ) can be the exceptions from the URL rules.

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

## Parental Control Provider

Parental Control Provider provides Web content filtering offering safer and more reliable web surfing for users. Please get an account and configure at the selected Provider “[www.opendns.com](http://www.opendns.com)” in advance. To use parental control (DNS), user needs to configure to use parental control (DNS provided by parental control provider) to access internet at WAN configuration or DNS page(See [DNS](#)).



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Parental Control Provider". Under "Parameters", there is a descriptive text: "Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance." Below this, there are four input fields: "Provider" (pre-filled with "www.opendns.com"), "Host Name", "Username", and "Password". At the bottom left, there are "Apply" and "Cancel" buttons.

Parameters	
Parental Control Provider provides Web content filtering while surfing the web safer and more reliable. Please get an account and configure at the selected Provider in advance.	
Provider	www.opendns.com
Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

**Host Name, Username and Password:** Enter your registered domain name and your username and password at the provider website [www.opendns.com](http://www.opendns.com).

# QoS - Quality of Service

## Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet) to WAN (Internet). This feature allows you to control the quality and speed of throughput for each application when the system is running with full upstream load.

**Note:** VDSL/ADSL line speed is based on the VDSL/ADSL sync rate. But there is no QoS on 3G/4G LTE as the 3G/4G LTE line speed is various and can not be known exactly.

Configuration

QoS Classification Setup

EWAN Line Speed

Upstream / Downstream: 0 / 0 kbps [0 : Disable]

Apply

Maximum rules can be configured: 32

Class Name	IP Version	Direction	Internal IP Address	Internal Port	Protocol	External IP Address	External Port	DSCP Mark	Rate Type	Disabled	Remove	Edit
------------	------------	-----------	---------------------	---------------	----------	---------------------	---------------	-----------	-----------	----------	--------	------

Add Remove

## EWAN Line Speed

**Upstream / Downstream:** Specify the upstream and downstream rate of the EWAN interface. Click **Apply** to save the EWAN rate settings.

Click **Add** to enter QoS rules.

Configuration

Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

IP Version: IPv4

Application: << --type or select from listbox-- >>

Direction: LAN to WAN Protocol: Any DSCP Marking: Disable

Rate Type: Prioritization Ratio: % Priority: Normal

Internal IP Address: ~ Internal Port: ~

External IP Address: ~ External Port: ~

Time Schedule: Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00:00 To 00:00

Apply

**IP Version:** Select either IPv4 or IPv6 base on need.

**Application:** Assign a name that identifies the new QoS application rule. Select from the list box for quick setup.

**Direction:** Shows the direction mode of the QoS application.

- 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 used. If you choose *Prioritization* for the rule, you parameter *Priority* would be available, you can set the priority for this rule.
- ① **Set DSCP Marking:** When select *Set DSCP Marking*, the packets matching the rule will be forwarded according to the pre-set DSCP marking.

**Ratio:** The rate percent of each application/policy compared to total traffic on the interface with limited rate type. For example, we want to only allow 20% of the total data for the LAN-to-WAN direction to be used for FTP server. Then we can specify here with data ratio = 20. If you have ADSL LINE with 256K/bps.rate, the estimated data rate, in kbps, for this rule is  $20\% * 256 * 0.9 = 46\text{kbps}$ . (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.

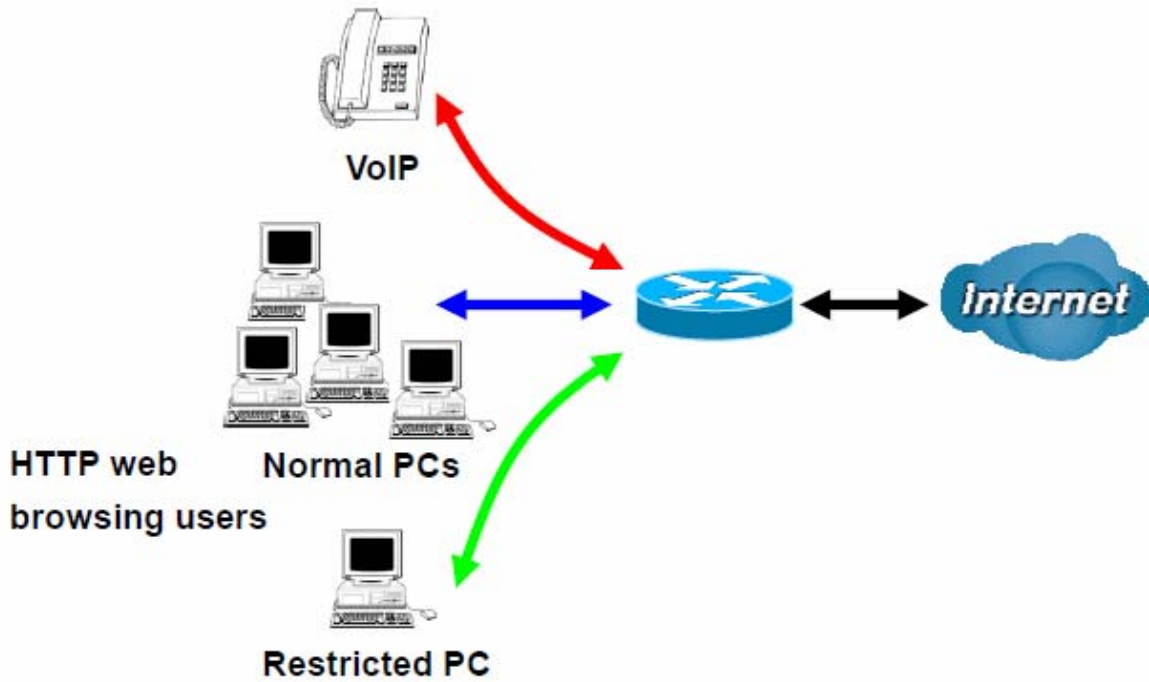
**External IP Address:** The IP address on remote / WAN side.

**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 - 19:00 from Monday to Friday. Or you can select the already set timeslot in “**Time Schedule**” during which the rule works. And when set to “Disable”, the rule is disabled or inactive and there will be an icon”

 ” indicating the rule is inactive. See [Time Schedule](#).

**Examples:** Common usage



1. Give outgoing VoIP traffic more priority.

The default queue priority is normal, so if you have VoIP users in your local network, you can set a higher priority to the outgoing VoIP traffic.

Configuration

Quality of Service

Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 100% Downstream (WAN to LAN) : 100%

IP Version	IPv4				
Application	Voip << --type or select from listbox--				
Direction	LAN to WAN	Protocol	Any	DSCP Marking	EF(101110)
Rate Type	Prioritization	Ratio	%	Priority	High
Internal IP Address		Internal Port			
External IP Address		External Port			
Time Schedule	timeslot1	<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

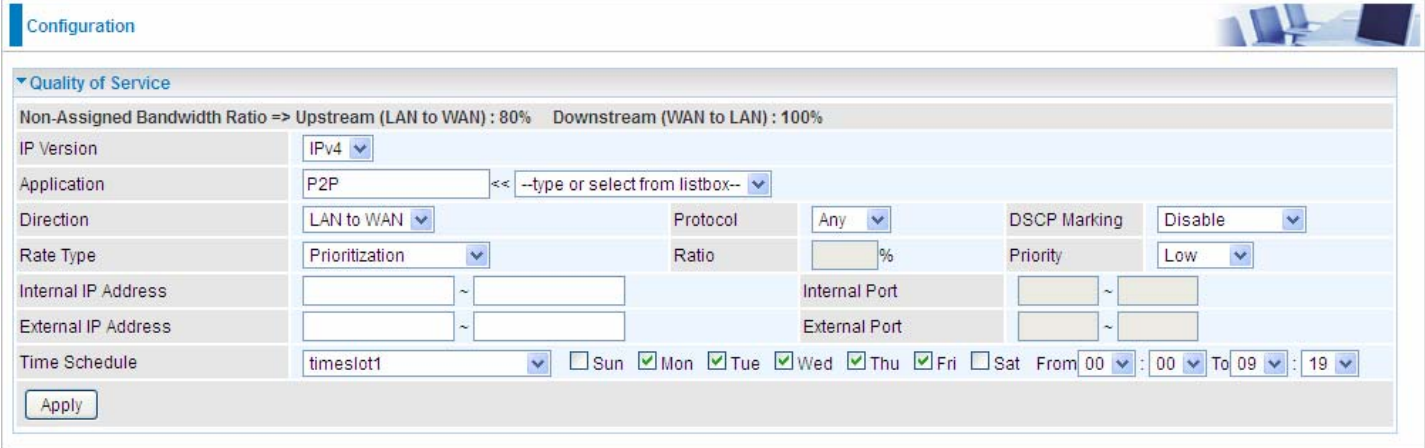
Quality of Service

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	DSCP Marking	Disable
Rate Type	Limited (Maximum)	Ratio	20 %	Priority	Normal
Internal IP Address		Internal Port			
External IP Address		External Port	80 ~ 80		
Time Schedule	timeslot1	<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.



The screenshot shows a network configuration page titled "Configuration" with a sub-section for "Quality of Service". At the top, it displays "Non-Assigned Bandwidth Ratio => Upstream (LAN to WAN) : 80% Downstream (WAN to LAN) : 100%". The configuration fields are as follows:

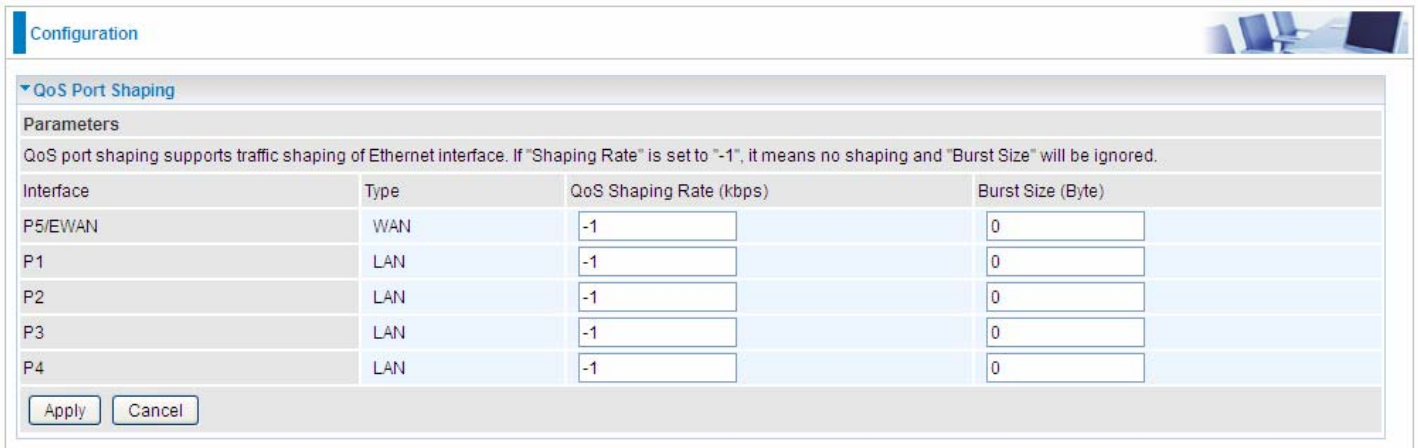
IP Version	IPv4				
Application	P2P << --type or select from listbox-- >>				
Direction	LAN to WAN	Protocol	Any	DSCP Marking	Disable
Rate Type	Prioritization	Ratio	%	Priority	Low
Internal IP Address	~	Internal Port	~		
External IP Address	~	External Port	~		
Time Schedule	timeslot1	<input type="checkbox"/> 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		

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

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

## QoS Port Shaping

QoS port shaping supports traffic shaping of Ethernet interfaces. It forcefully maximizes the throughput of the Ethernet interface. When “Shaping Rate” is set to “-1”, no shaping will be in place and the “Burst Size” is to be ignored.



Configuration

QoS Port Shaping

Parameters

QoS port shaping supports traffic shaping of Ethernet interface. If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	QoS Shaping Rate (kbps)	Burst Size (Byte)
P5/EWAN	WAN	-1	0
P1	LAN	-1	0
P2	LAN	-1	0
P3	LAN	-1	0
P4	LAN	-1	0

Apply Cancel

**Interface:** P1-P5. P5 used as EWAN also covered.

**Type:** All LAN when P4 is LAN port; P4 used as EWAN, type WAN and all others LAN.

**QoS Shaping Rate (Kbps):** Set the forcefully maximum rate.

**Burst Size(Bytes):** Set the forcefully Burst Size.

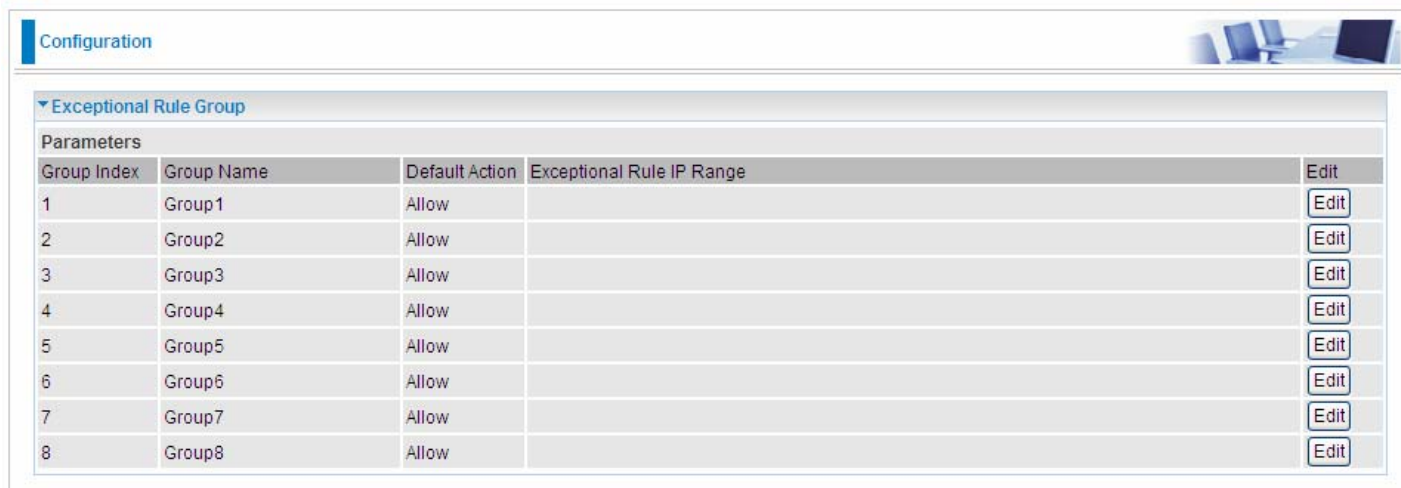


# NAT

NAT (Network Address Translation) feature translates a private IP to a public IP, allowing multiple users to access the Internet through a single IP account, sharing the single IP address. It is a natural firewall for the private network.

## Exceptional Rule Group

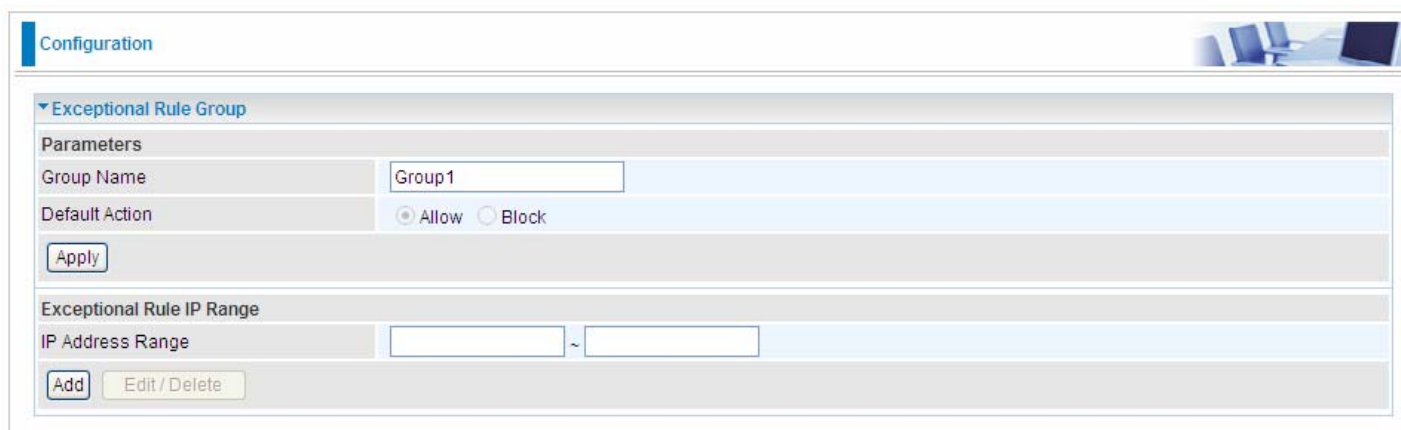
Exceptional Rule is dedicated to giving or blocking NAT/DMZ access to some specific IP or IPs(range). Users are allowed to set 8 different exceptional rule groups at most. In each group, user can add specific IP or IP range.



The screenshot shows a web interface for configuring Exceptional Rule Groups. It features a table with 8 rows, each representing a group. The columns are Group Index, Group Name, Default Action, Exceptional Rule IP Range, and Edit. Each row has an 'Edit' button next to it.

Group Index	Group Name	Default Action	Exceptional Rule IP Range	Edit
1	Group1	Allow		Edit
2	Group2	Allow		Edit
3	Group3	Allow		Edit
4	Group4	Allow		Edit
5	Group5	Allow		Edit
6	Group6	Allow		Edit
7	Group7	Allow		Edit
8	Group8	Allow		Edit

Press **Edit** to set the exceptional IP (IP Range).



The screenshot shows the configuration form for an Exceptional Rule Group. It includes fields for Group Name (set to 'Group1'), Default Action (radio buttons for 'Allow' and 'Block'), and Exceptional Rule IP Range (two input boxes separated by a tilde '~'). There are 'Apply', 'Add', and 'Edit / Delete' buttons.

**Default Action:** Please first set the range to make “**Default Action**” setting available. Select “Allow” to grant access to the listed IP or IPs to Virtual Server and DMZ Host.

While choose “Block” to ban the listed IP or IPs to access the Virtual Server and DMZ Host.

**Apply:** Press **Apply** button to apply the change.

## Exceptional Rule Range

**IP Address Range:** Specify the IP address range; IPv4 address range can be supported.

Click **Add** to add the IP Range.

For instance, if user wants block IP range of 172.16.1.102-172.16.1.106 from accessing your set virtual server and DMZ host, you can add this IP range and valid it.

Configuration

▼ Exceptional Rule Group

Parameters

Group Name:

Default Action:  Allow  Block

Exceptional Rule IP Range

IP Address Range:  ~

Edit	Action	IP Address Range	Delete
<input type="radio"/>	Block	172.16.1.102 ~ 172.16.1.106	<input type="checkbox"/>

## 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.

Configuration

▼ Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
<input type="button" value="Add"/> <input type="button" value="Remove"/>										

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

The following configuration page will appear to let you configure.

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

**WAN IP:** To specify the exact WAN IP address. It can be flexible while there are multiple WAN IPs on one interface. If the WAN IP field is empty, 8700NEXL R2 uses the current WAN IP of this interface.

**Server Name:** Select the server name from the drop-down menu.

**Custom Service:** It is a kind of service to let users customize the service they want. Enter the user-defined service name here. It is a parameter only available when users select **Custom Service** in the above parameter.

**Server IP Address:** Enter your server IP Address here. User can select from the list box for quick setup.


### External Port

- 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.

**Time Schedule:** Select or set exactly when the Virtual Server works. When set to "Always On", the Virtual Server will work all time; and also you can set the precise time when Virtual Server works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the Virtual Server works. And when set to "Disable", the rule is disabled and there will be an icon  in the list table indicating the rule is disabled. See [Time Schedule](#).

**Exceptional Rule Group:** Select the exceptional group listed. It is to grant or block Virtual Server

access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block Virtual Server access to this IP range, you can select Group1.

## ● Set up

1. Select a Server Name from the drop-down menu, then the port will automatically appear, modify some as you like, or you can just leave it as default. Remember to enter your server IP Address.

Virtual Servers

Parameters

Interface: pppoe\_0\_8\_35/ppp0.1 WAN IP:

Server Name: Custom Service

Custom Service:

Server IP Address:  << --type or select from listbox-- >>

Time Schedule: Always On  Sun  Mon  Tue  Wed  Thu  Fri  Sat From 00 : 00 To 00 : 00

Exceptional Rule Group: None

External Port		Protocol	Protocol Number	Internal Port	
Start	End			Start	End
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>

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	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1	<input type="checkbox"/>	<input type="checkbox"/>	Edit

Add Remove

Configuration

Virtual Servers

Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	✓	<input type="checkbox"/>	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit

Add Remove

(✓ Means the rule is inactive)

### Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, then press **Remove**, it will be OK.

Configuration

Virtual Servers

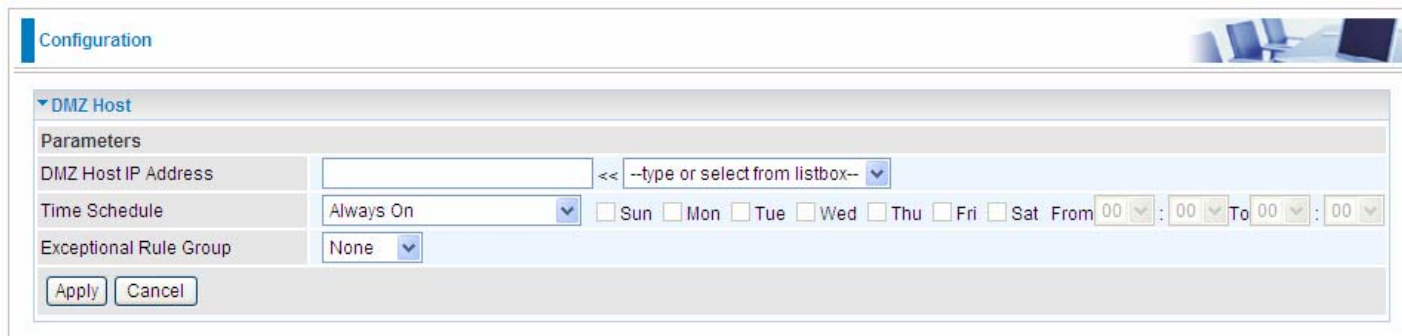
Virtual Servers Setup

Server Name	External Port		Protocol	Internal Port		Server IP Address	WAN Interface	Disabled	Remove	Edit
	Start	End		Start	End					
Age of Empires	47624	47624	TCP	47624	47624	192.168.1.103	ppp0.1	✓	<input type="checkbox"/>	Edit
Age of Empires	6073	6073	TCP	6073	6073	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	TCP	2300	2400	192.168.1.103	ppp0.1		<input type="checkbox"/>	Edit
Age of Empires	2300	2400	UDP	2300	2400	192.168.1.103	ppp0.1		<input checked="" type="checkbox"/>	Edit

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.



**DMZ Host IP Address:** Enter the IP Address of a host you want it to be a DMZ host. Select from the list box to quick set the DMZ.

**Time Schedule:** Select or set exactly when the DMZ works. When set to “Always On”, the DMZ will work all time; and also you can set the precise time when DMZ works, like 01:00 - 19:00 from Monday to Friday. Or you can select the already set timeslot in **Time Schedule** during which the DMZ works. And when set to “Disable”, the rule is disabled. See [Time Schedule](#).

**Exceptional Rule Group:** Select the exceptional group listed. It is to grant or block DMZ access to a group of IPs. For example, as we set previously group 1 blocking access to 172.16.1.102-172.16.1.106. If here you want to block DMZ Access to this IP range, you can select Group1.



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.

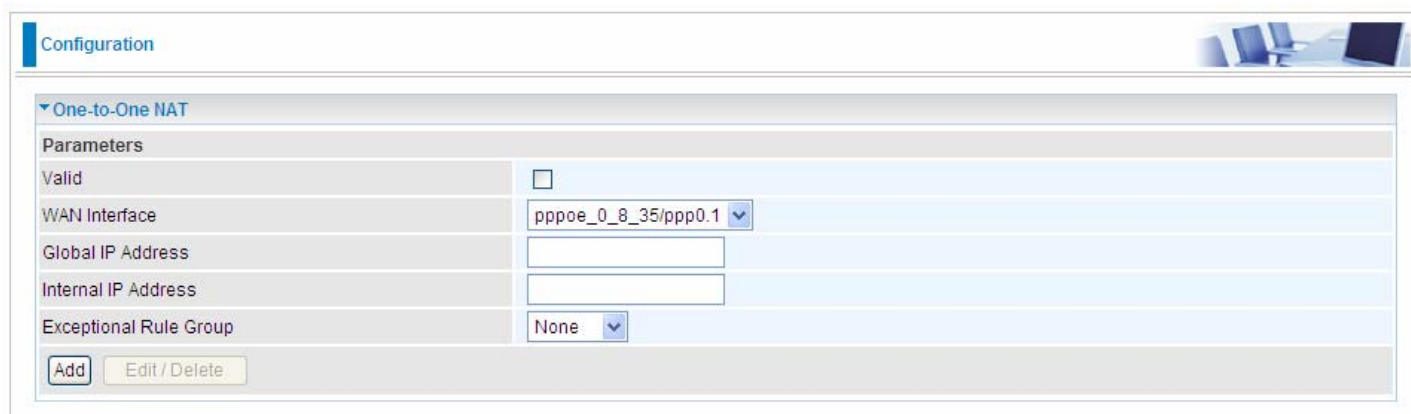


**Attention**

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 configuration window titled "Configuration" with a sub-section for "One-to-One NAT". Under the "Parameters" section, there are five fields: "Valid" (checkbox), "WAN Interface" (dropdown menu showing "pppoe\_0\_8\_35/ppp0.1"), "Global IP Address" (text input), "Internal IP Address" (text input), and "Exceptional Rule Group" (dropdown menu showing "None"). At the bottom of the configuration area, there are two buttons: "Add" and "Edit / Delete".

**Valid:** Check whether to valid the one-to-one NAT mapping rule.

**WAN Interface:** Select one based WAN interface to configure the one-to-one NAT.

**Global IP address:** The Global IP mapped to an internal device. It can be left empty, and under this circumstance, it can be reached through the WAN IP of interface set in the field above.

**Internal Address:** The IP address of an internal device in the LAN.

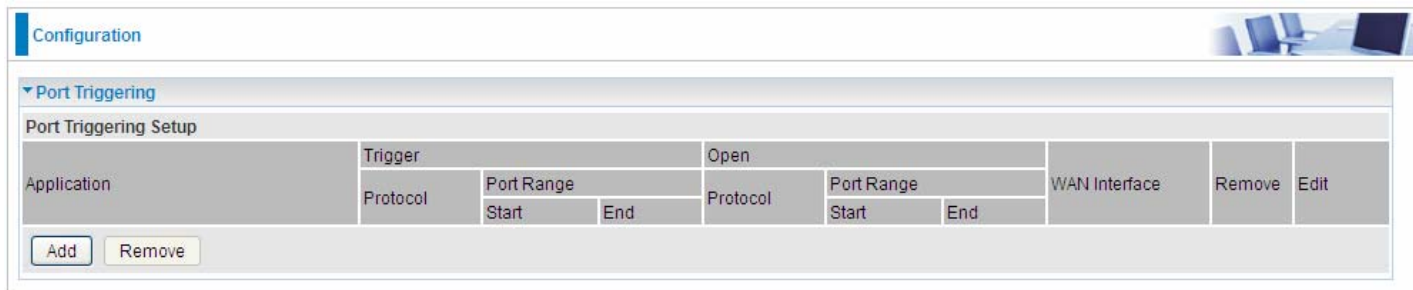
**Exceptional Rule Group:** Select the exceptional group listed. It is to give or block access to a group of IPs to the server after One-to-One NAT. For example, a server with 192.168.1.3 is mapped to 123.1.1.2 by One-to-One NAT, then the exceptional group can be designated to have or have not access to 123.1.1.2.

**For example,** you have an ADSL connection of pppoe\_0\_8\_35/ppp0.1 interface with three fixed global IP, and you then can assign the other two global IPs to two internal devices respectively.

If you have a WEB server (IP address: 192.168.1.3) and a FTP server (IP address: 192.168.1.4) in local network, owning a public IP address range of 123.1.1.2 to 123.1.1.4 assigned by ISP. 123.1.1.2 is used as WAN IP address of the router, 123.1.1.3 is used for WEB server and 123.1.1.4 is used for FTP server. With One-to-One NAT, the servers with private IP addresses can be accessed at the corresponding valid public IP addresses

## Port Triggering

Port triggering is a way to automate port forwarding with outbound traffic on predetermined ports ('triggering ports'), incoming ports are dynamically forwarded to the initiating host, while the outbound ports are in use. Port triggering triggers can open an incoming port when a client on the local network makes an outgoing connection on a predetermined port or a range of ports.



Configuration

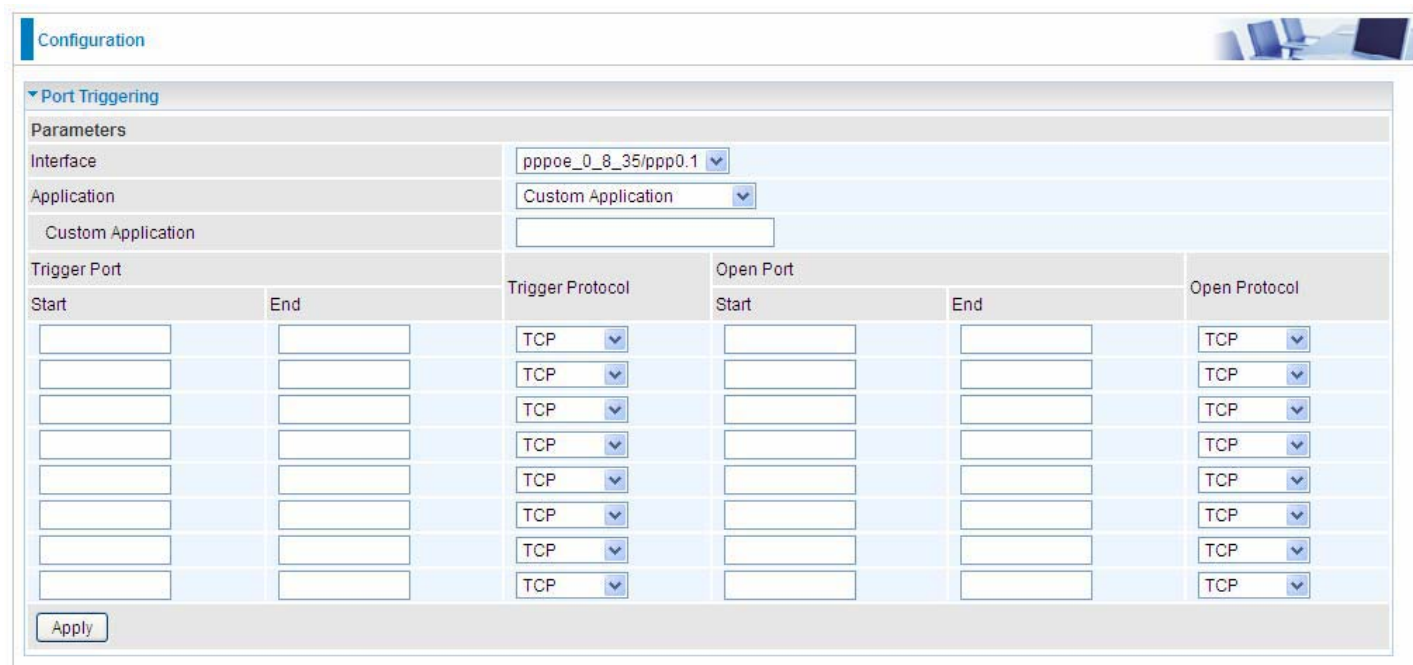
Port Triggering

Port Triggering Setup

Application	Trigger		Open			WAN Interface	Remove	Edit
	Protocol	Port Range	Protocol	Port Range	Port Range			
	Start	End	Start	End	End			

Add Remove

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



Configuration

Port Triggering

Parameters

Interface: pppoe\_0\_8\_35/ppp0.1

Application: Custom Application

Custom Application: [Text Field]

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

Add

**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.


Trigger Port		Trigger Protocol	Open Port		Open Protocol
Start	End		Start	End	
4099	4099	TCP	5191	5191	TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

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

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

## Remove

If you don't need a specified Server, you can remove it. Check the check box beside the item you want to remove, and then press **Remove**.

Configuration 

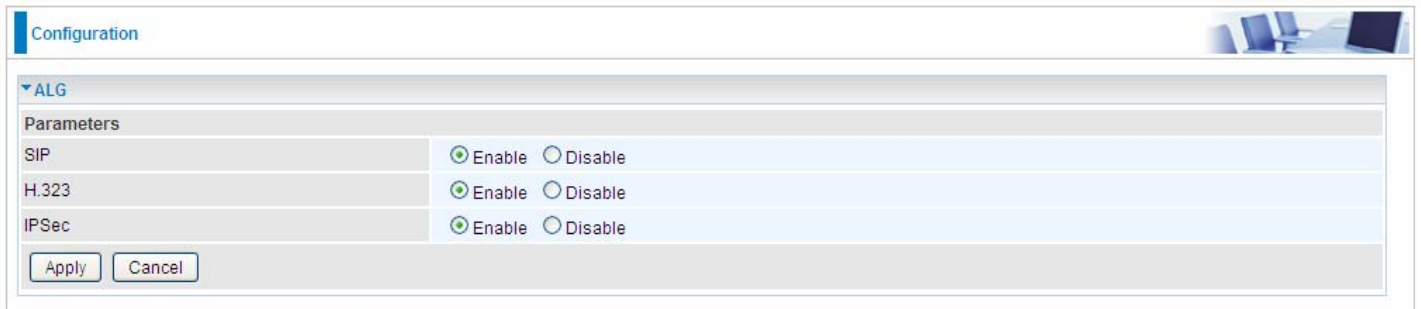
▼ Port Triggering

Port Triggering Setup

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

## ALG

The ALG Controls enable or disable protocols over application layer.



The screenshot shows a configuration window titled "Configuration" with a sub-section for "ALG". Under "Parameters", there are three rows, each with a protocol name and two radio buttons: "Enable" (selected) and "Disable".

Protocol	Enable	Disable
SIP	<input checked="" type="radio"/>	<input type="radio"/>
H.323	<input checked="" type="radio"/>	<input type="radio"/>
IPsec	<input checked="" type="radio"/>	<input type="radio"/>

At the bottom of the configuration window, there are two buttons: "Apply" and "Cancel".

**SIP:** Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP when SIP phone includes NAT-Traversal algorithm.

**H.323:** Enable to secure the voice communication using H.323 protocol when one or both terminals are behind a NAT.

**IPsec:** Enable IPsec ALG to allow one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

# Wake On LAN

Wake on LAN (WOL, sometimes WoL) is an Ethernet computer networking standard that allows a computer to be turned on or woken up remotely by a network message.

**Configuration**

**Wake On LAN**

Parameters

Host Label:

MAC Address:  << --select-- >> (type or select from listbox)

Wake by Schedule:  Enable [Schedule](#)

**Host Label:** Enter identification for the host.

**Select:** Select MAC address of the computer that you want to wake up or turn on remotely.

**Wake by Schedule:** Enable to wake up your set device at some specific time. For instance, user can set to get some device woken up at 8:00 every weekday. Click [Schedule](#) to enter time schedule configuring page to set the exact timeline.

**Configuration**

**Wake up Time Schedule**

Parameters

Name:

Day in a week:  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time: 00 : 00

Edit	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Delete
<input type="radio"/>	11		x	x	x	x	x		09:00	<input type="checkbox"/>

**Add:** After selecting, click Add then you can submit the Wake-up action.

**Edit/Delete:** Click to edit or delete the selected MAC address.

**Ready:**

“**Yes**” indicating the remote computer is ready for your waking up.

“**No**” indicating the machine is not ready for your waking up.

**Delete:** Delete the selected MAC address.

**Configuration**

**Wake On LAN**

Parameters

Host Label:

MAC Address:  << --select-- >> (type or select from listbox)

Wake by Schedule:  Enable [Schedule](#)

Edit	Action	Host Label	MAC Address	Ready	Delete
<input type="radio"/>	Schedule	billion-17bc8f1	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](#), [Certificate](#), [Multicast](#), [Management](#), and [Diagnostics](#).

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

# 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	eth4.1 USB3G0

Preferred WAN Interface As The System Default IPv6 Gateway

Selected WAN Interface: pppoe\_0\_8\_35/ppp0.1

Apply Cancel

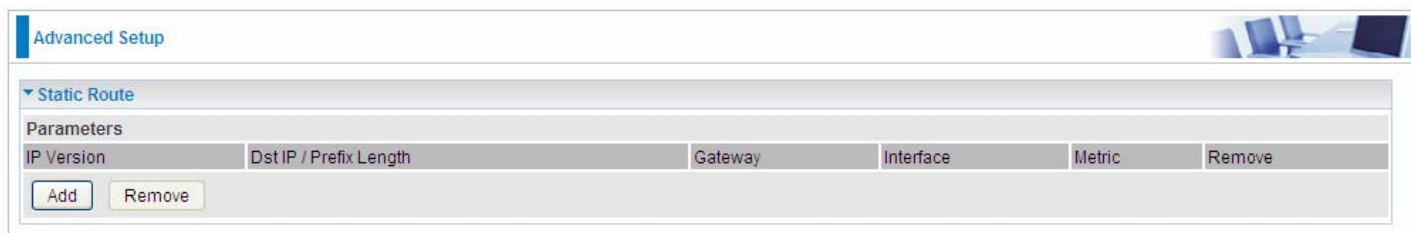
**WAN port:** Select the port this gateway applies to.

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.

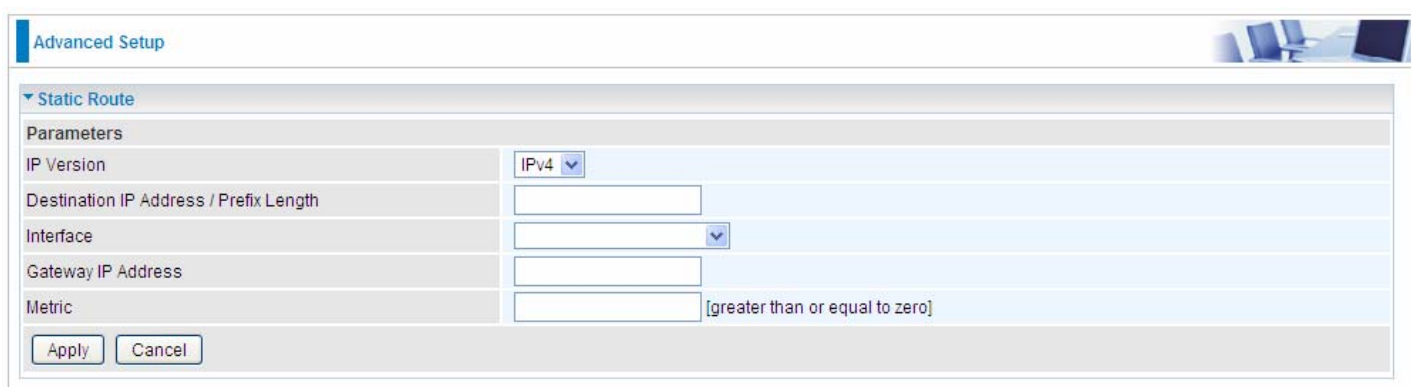
## Static Route

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.



The screenshot shows the 'Advanced Setup' interface with a 'Static Route' section. Below the section title is a table with the following columns: 'IP Version', 'Dst IP / Prefix Length', 'Gateway', 'Interface', 'Metric', and 'Remove'. Below the table are two buttons: 'Add' and 'Remove'.

Above is the static route listing table, click **Add** to create static routing.



The screenshot shows the 'Advanced Setup' interface with a 'Static Route' configuration form. The form has the following fields: 'IP Version' (dropdown menu set to 'IPv4'), 'Destination IP Address / Prefix Length' (text input), 'Interface' (dropdown menu), 'Gateway IP Address' (text input), and 'Metric' (text input with a note '[greater than or equal to zero]'). At the bottom are two buttons: 'Apply' and 'Cancel'.

**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"/>

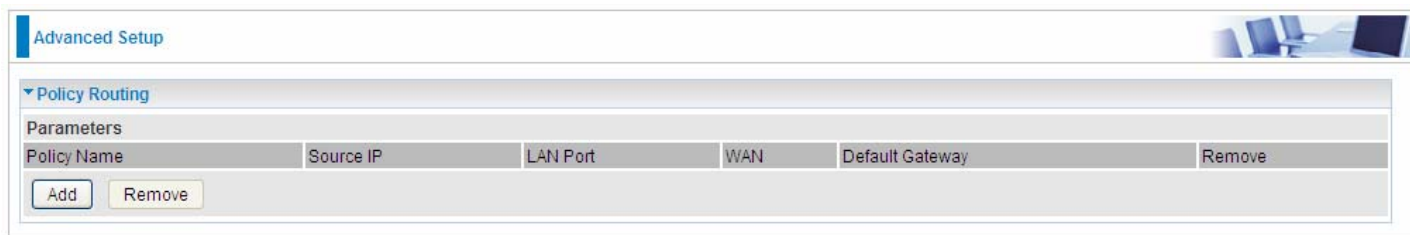
Add Remove



## 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.

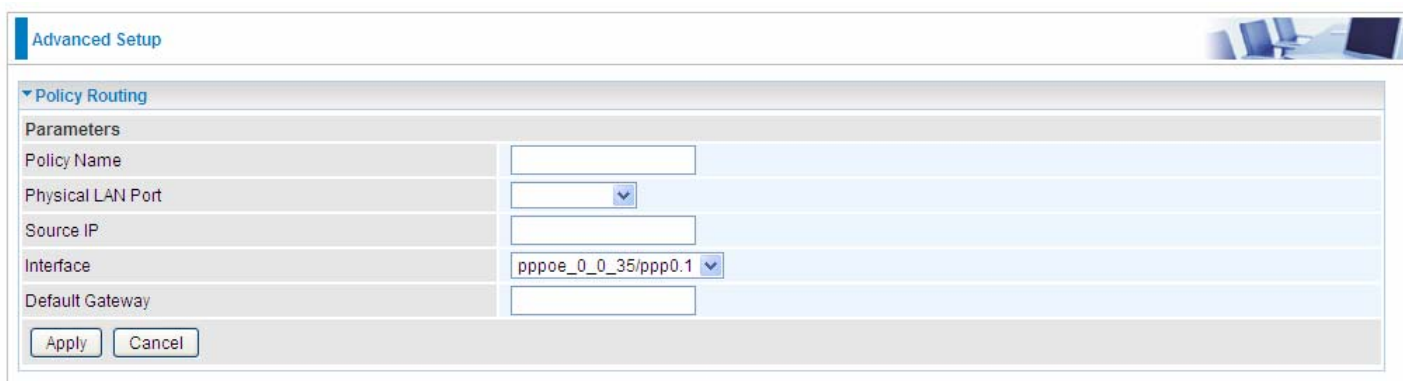
The following is the policy Routing listing table.



The screenshot shows the 'Advanced Setup' interface with the 'Policy Routing' section expanded. Below the section header is a 'Parameters' table with the following columns: Policy Name, Source IP, LAN Port, WAN, Default Gateway, and Remove. Below the table are two buttons: 'Add' and 'Remove'.

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

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



The screenshot shows the 'Advanced Setup' interface with the 'Policy Routing' section expanded. The configuration form contains the following fields: Policy Name (text input), Physical LAN Port (dropdown menu), Source IP (text input), Interface (dropdown menu with 'pppoe\_0\_0\_35/ppp0.1' selected), and Default Gateway (text input). At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

**Policy Name:** User-defined name.

**Physical LAN Port:** Select the LAN port.

**Source IP:** Enter the Host Source IP.

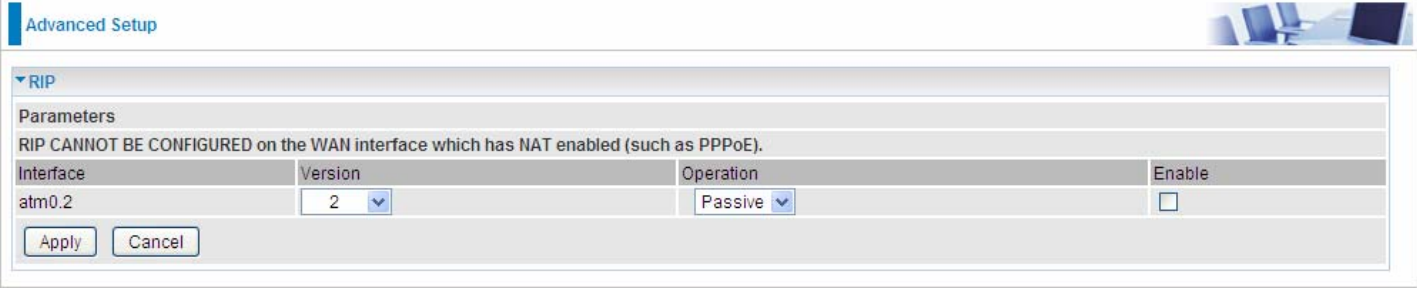
**Interface:** Select the WAN interface which you want the Source IP to access outside through.

**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.



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, RIP-1, RIP-2 and both.

**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

**Parameters**  
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses OR IP addresses provided by Parental Control Provider for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the 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	Available WAN Interfaces
ppp0.1 USB3G0	

Use the following Static DNS IP address

Primary DNS server:   
Secondary DNS server:

Use the IP Addresses provided by Parental Control Provider

Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

Obtain IPv6 DNS info from a WAN interface

WAN Interface selected:

Use the following Static IPv6 DNS address

Primary IPv6 DNS server:   
Secondary IPv6 DNS server:

### ➤ IPv4

#### Three ways to set an IPv4 DNS server

- ① **Select DNS server from available WAN interfaces:** Select a desirable WAN interface as the IPv4 DNS server.
- ① **User the following Static DNS IP address:** To specify DNS server manually by entering your primary and secondary DNS server addresses.
- ① **Use the IP address provided by Parental Control Provider:** If user registers and gets an DNS account in the parental control provider website, expecting to enjoy a more reliable and safer internet surfing environment, please select this option (need to configure at [Parental Control Provider](#)).

### ➤ IPv6:

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

#### Obtain IPv6 DNS info from a WAN interface

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

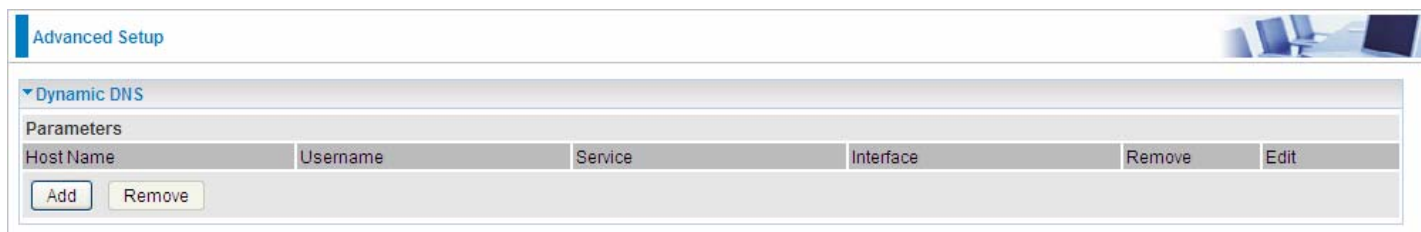
#### Use the following Static IPv6 DNS address

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

## Dynamic DNS

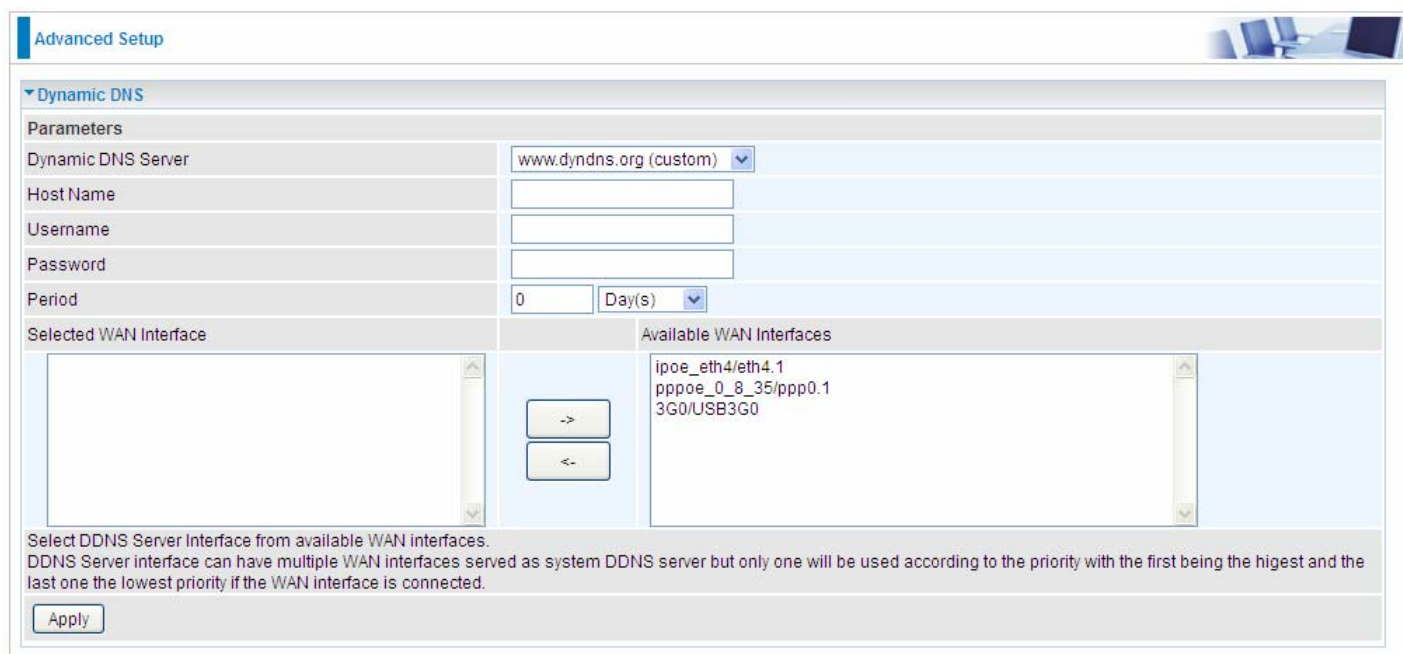
The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your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

Here users can register different WAN interfaces with different DNS(es).



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

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



Dynamic DNS Server:

Host Name:

Username:

Password:

Period:  Day(s)

Selected WAN Interface:

Available WAN Interfaces:

- ipoe\_eth4/eth4.1
- pppoe\_0\_8\_35/ppp0.1
- 3G0/USB3G0

Select DDNS Server interface from available WAN interfaces.  
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

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

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

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

**Period:** Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

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

## User can register different DDNS to different interfaces.

Examples: **Note** first users have to go to the Dynamic DNS registration service provider to register an account.

User **test** register two Dynamic Domain Names in DDNS provider <http://www.dyndns.org/>.

1. pppoe\_0\_8\_35 with DDNS: [www.hometest.com](http://www.hometest.com) using username/password test/test

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server:

Host Name:

Username:

Password:

Period:  Day(s)

Selected WAN Interface:

Available WAN Interfaces:

->

<-

Select DDNS Server Interface from available WAN interfaces.  
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Advanced Setup

Dynamic DNS

Parameters

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

2. ipoe\_eth4 with DDNS: [www.hometest1.com](http://www.hometest1.com) using username/password test/test.

Advanced Setup

Dynamic DNS

Parameters

Dynamic DNS Server	www.dyndns.org (custom)
Host Name	www.hometest1.com
Username	test
Password	••••
Period	25 Day(s)

Selected WAN Interface: ipoe\_eth4/eth4.1

Available WAN Interfaces: pppoe\_0\_8\_35/ppp0.1, 3G0/USB3G0

Select DDNS Server Interface from available WAN interfaces.  
DDNS Server interface can have multiple WAN interfaces served as system DDNS server but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected.

Apply

Advanced Setup

Dynamic DNS

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	eth4.1	<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.



The screenshot shows a web interface for configuring DNS Proxy. The page title is "Advanced Setup". Under the "DNS Proxy" section, there are three main fields: "DNS Proxy" with radio buttons for "Enable" (selected) and "Disable"; "Host name of the Broadband Router" with a text input field containing "home.gateway"; and "Domain name of the LAN network" with a text input field containing "home.gateway". At the bottom of the configuration area are "Apply" and "Cancel" buttons.

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

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

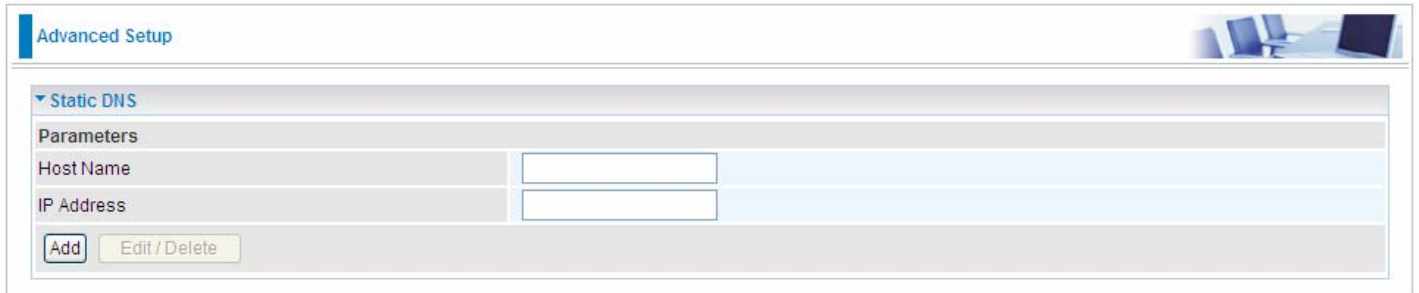
**Domain name of the LAN network:** Enter the domain name of the LAN network. home.gateway.



## Static DNS

Static DNS is a concept relative to Dynamic DNS; in static DNS system, the IP mapped is static without change.

You can map the specific IP to a user-friendly domain name. In LAN, you can map a PC to a domain name for convenient access. Or you can set some well-known Internet IP mapping item so your router will response quickly for your DNS query instead of querying from the ISP's DNS server.



The screenshot shows a web interface for 'Advanced Setup'. Under the 'Static DNS' section, there is a 'Parameters' table with two rows: 'Host Name' and 'IP Address', each with an empty text input field. Below the table are two buttons: 'Add' and 'Edit/Delete'.

Parameters	
Host Name	<input type="text"/>
IP Address	<input type="text"/>

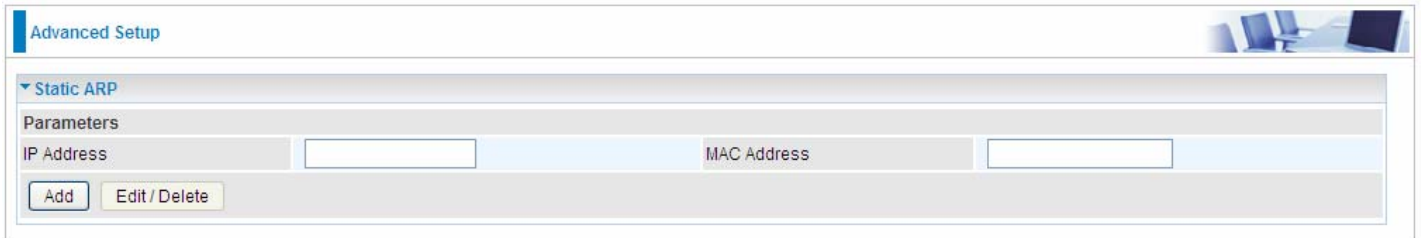
**Host Name:** Type the domain name (host name) for the specific IP .

**IP Address:** Type the IP address bound to the set host name above.

Click **Add** to save your settings.

## Static ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol that allows the resolution of network layer addresses into the link layer addresses. And “Static ARP” here allows user to map manually the layer-3 MAC (Media Access Control) address to the layer-2 IP address of the device.



The screenshot shows a web-based configuration interface for Static ARP. At the top, there is a tab labeled "Advanced Setup" and a small image of a computer workstation. Below this, a section titled "Static ARP" is expanded. Underneath, a "Parameters" section contains two input fields: "IP Address" and "MAC Address". Below the input 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.

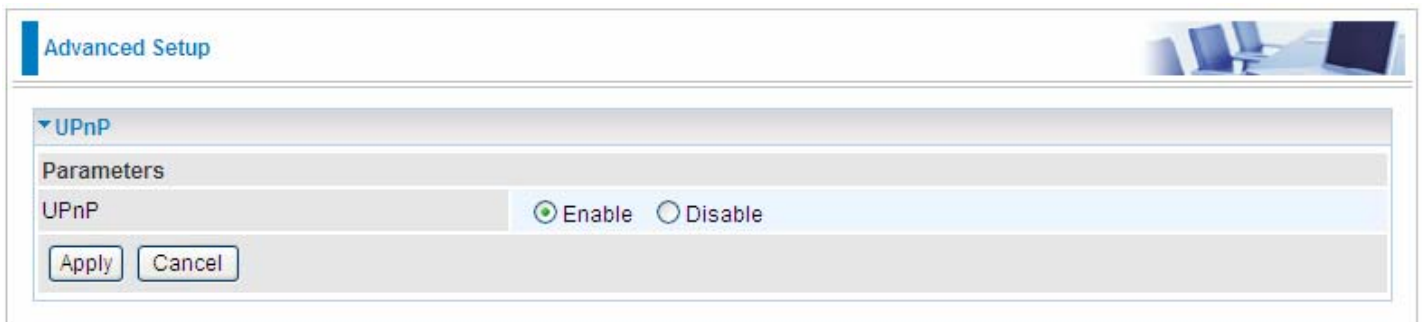
**MAC Address:** Enter the MAC address that corresponds to the IP address of the device.

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:

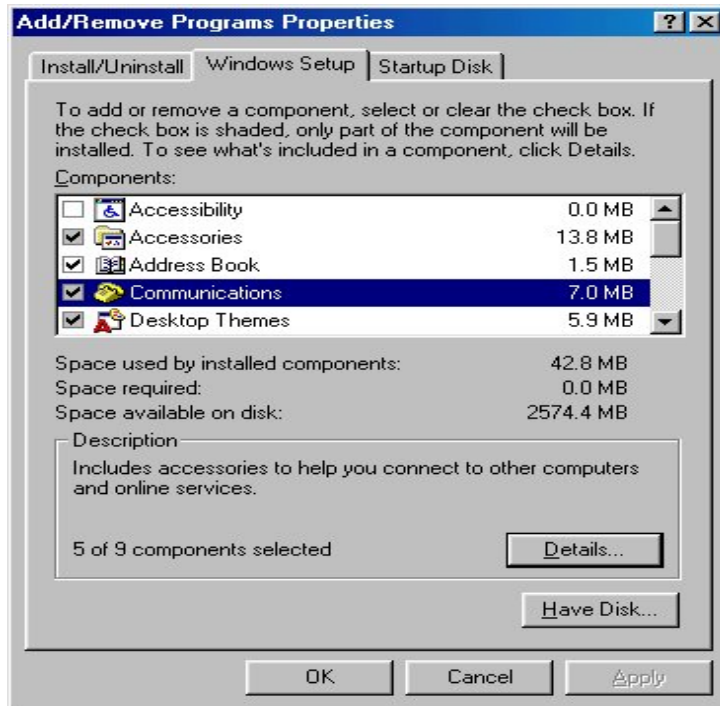
- ① **Enable:** Check to enable the router's UPnP functionality.
- ① **Disable:** Check to disable the router's UPnP functionality.

## Installing UPnP in Windows Example

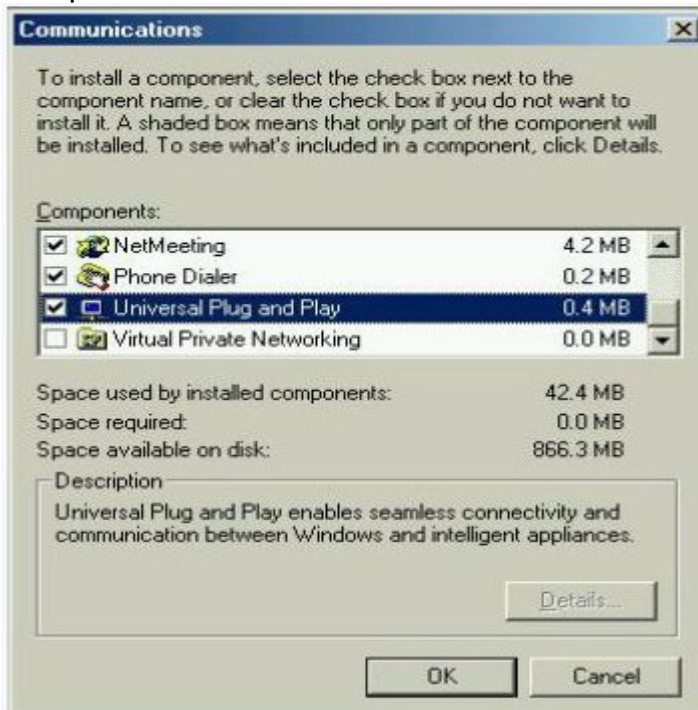
Follow the steps below to install the UPnP in Windows Me.

**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.

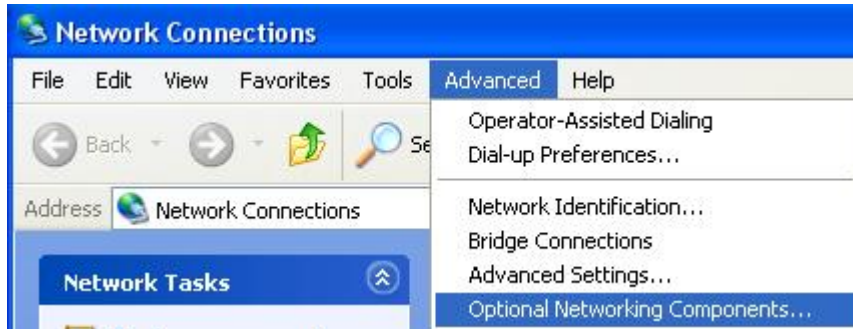
**Step 5:** Restart the computer when prompted.

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

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

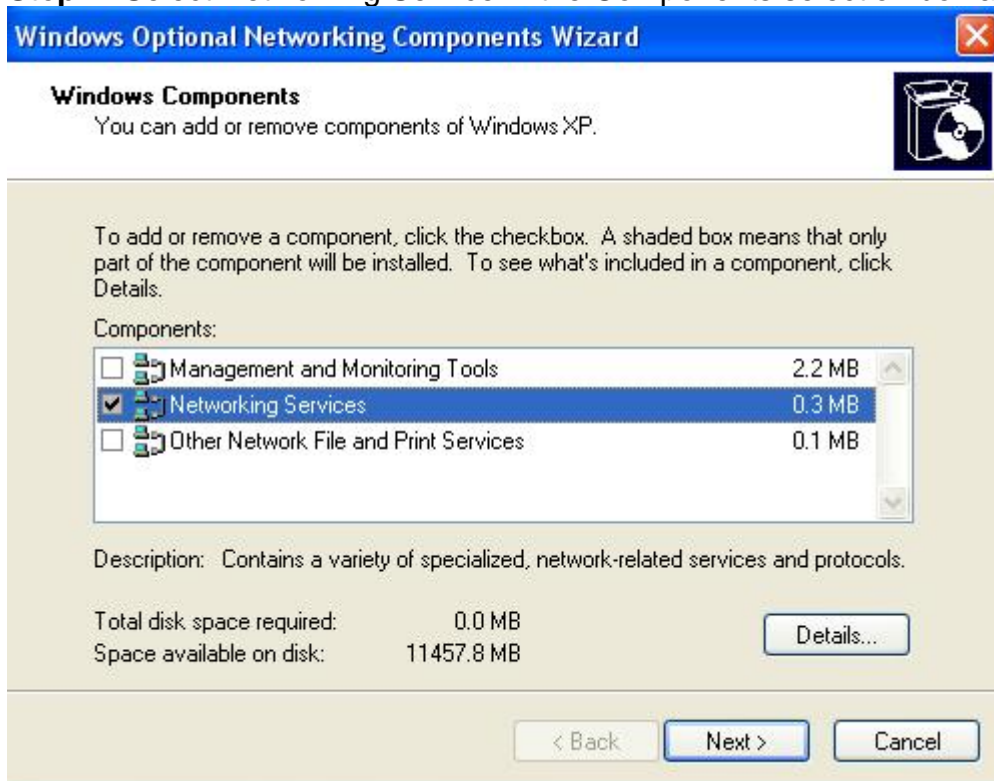
**Step 2:** Double-click Network Connections.

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



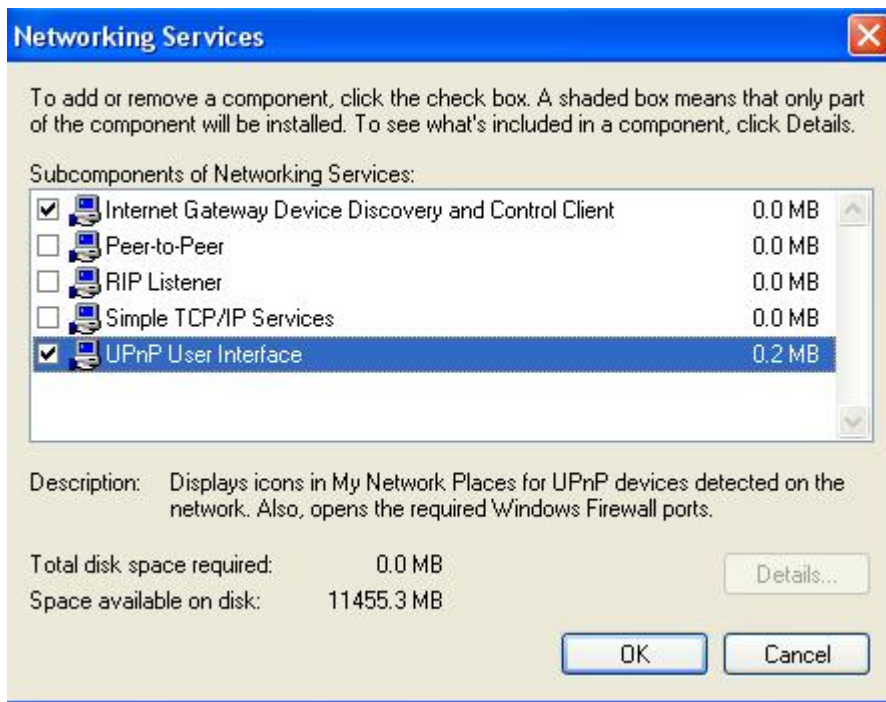
The Windows Optional Networking Components Wizard window displays.

**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.

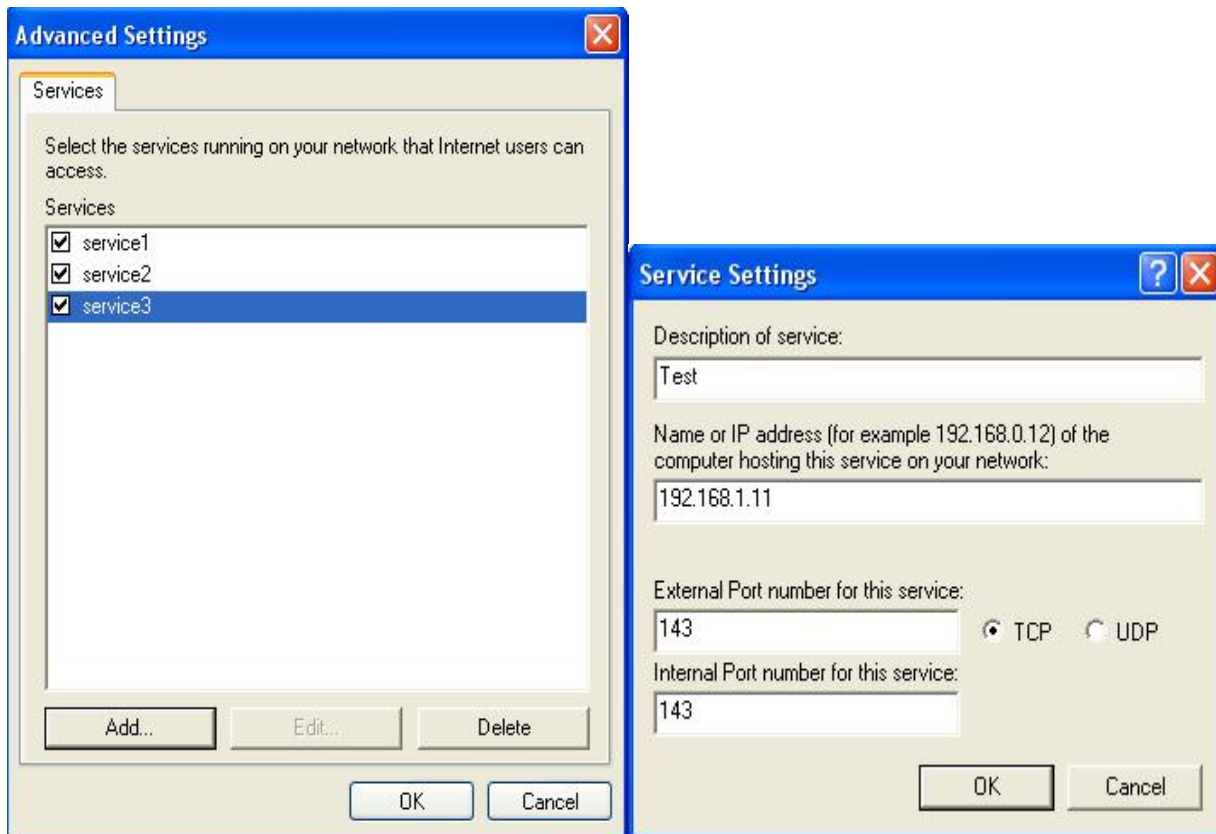
**Step 2:** Right-click the icon and select Properties.



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

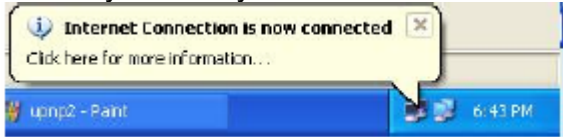


**Step 4:** You may edit or delete the port mappings or click Add to manually add port mappings.

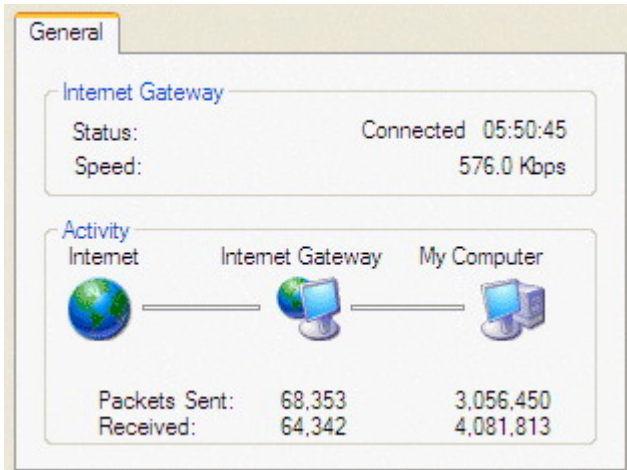


**Step 5:** Select Show icon in notification area when connected option and click OK. An icon displays

in the system tray



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

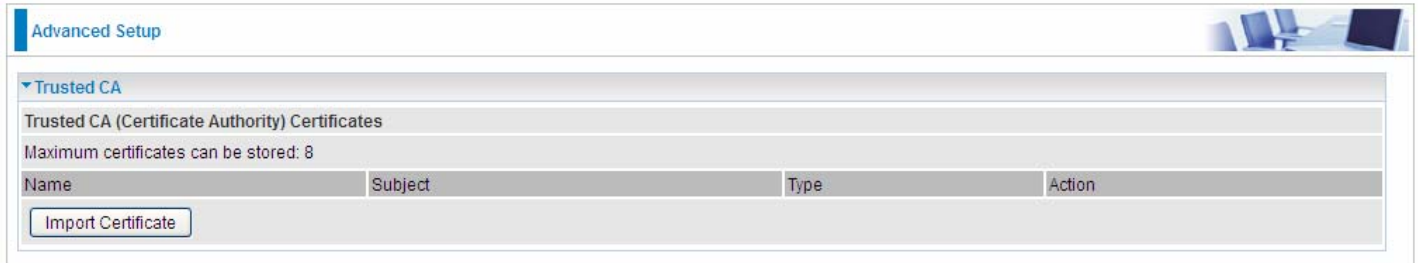




# Certificate

This feature is used for TR069 ACS Server authentication of the device using certificate, if necessary. If the imported certificate does not match the authorized certificate of the ACS Server, the device will have no access to the server.

## Trusted CA



**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	<input type="text"/>
------	----------------------

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-----  
MIICjDCCAfWgAwIBAgIEOUSLuTANBgkqhkiG9w0BAQUFADAmMQswCQYDVQQ  
GEwJD  
TjEXMBUGA1UEChMOQ0ZDQSBQb2xpY3kgQ0EwHhcNMDAwNjEyMDc0OTUyWhc  
NMjAw  
NjEyMDQzNzA2WjApMQswCQYDVQQGEwJDTjEaMBGGA1UEChMRQ0ZDQSBPcGV  
yYXRp  
b24gQ0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANesUKqN1sWtSpN  
ZuTJD  
rSwXGjaexPnBie5zNJc70SPQYgVhn3Qv9+vIuU2jYFzF8qiDYPQBv7hFjI/  
Uu9be  
pUJBenxvYRgTImUfJ0PEy+SsRUpcDAPxTWNp4Efv8QEnM0JGEHAOtLHDY73  
/se+H  
jB7Wh9HhzCTF5QqZRL3o2ILXAgMBAAGjgcMwgcAwSAYDVROfBEEwPzA9oDu  
gOaQ3  
MDUxCzAJBgNVBAYTAKNOMRcwFQYDVQQKEw5DRkNBIFBvbG1jeSBBDQITENMA  
GA1UE  
AxMEQ1JMMTALBgNVHQ8EBAMCAQYwHwYDVROjBBgwFoAUL5Jufe7tBb/wveS  
FaAqX  
k1NC0tAwHQYDVROBBYEFMMnxjZoyCdlJIEvkdLJjMC5RrpMAwGA1UdEwQ
```

Apply

Click Apply to confirm your settings.

Advanced Setup 

▼ Trusted CA

Trusted CA (Certificate Authority) Certificates

Maximum certificates can be stored: 8

Name	Subject	Type	Action
acscert	C=CN/O=CFCA Operation CA	ca	<a href="#">View</a> <a href="#">Remove</a>

[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	
<b>Multicast</b>	
Multicast Precedence	Disable [lower value, higher priority]
<b>IGMP</b>	
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
<b>MLD</b>	
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
[Apply] [Cancel]	

## IGMP

**Multicast Precedence:** It is for multicast QoS. With lower multicast precedence, IGMP packets will be put into higher-priority queue. Default is set to disable.

**Default Version:** Enter the supported IGMP version, 1-3, default is IGMP v3.

**Query Interval:** Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

**Query Response Interval:** Enter the response interval time (sec).

**Last Member Query Interval:** Enter the interval time (sec) the multicast router query the specified

group after it has received leave message.

**Robustness Value:** Enter the router robustness parameter, 2-7, the greater the robustness value, the more robust the Querier is.

**Maximum Multicast Groups:** Enter the Maximum Multicast Groups.

**Maximum Multicast Data Sources( for IGMP v3):** Enter the Maximum Multicast Data Sources,1-24.

**Maximum Multicast Group Members:** Enter the Maximum Multicast Group Members.

**Fast leave:** Check to determine whether to support fast leave. If this value is enabled, IGMP proxy removes the membership of a group member immediately without sending an IGMP membership query on downstream. This is very helpful if user wants fast channel (group change) changing in cases like IPTV environment.

## 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.

# Management

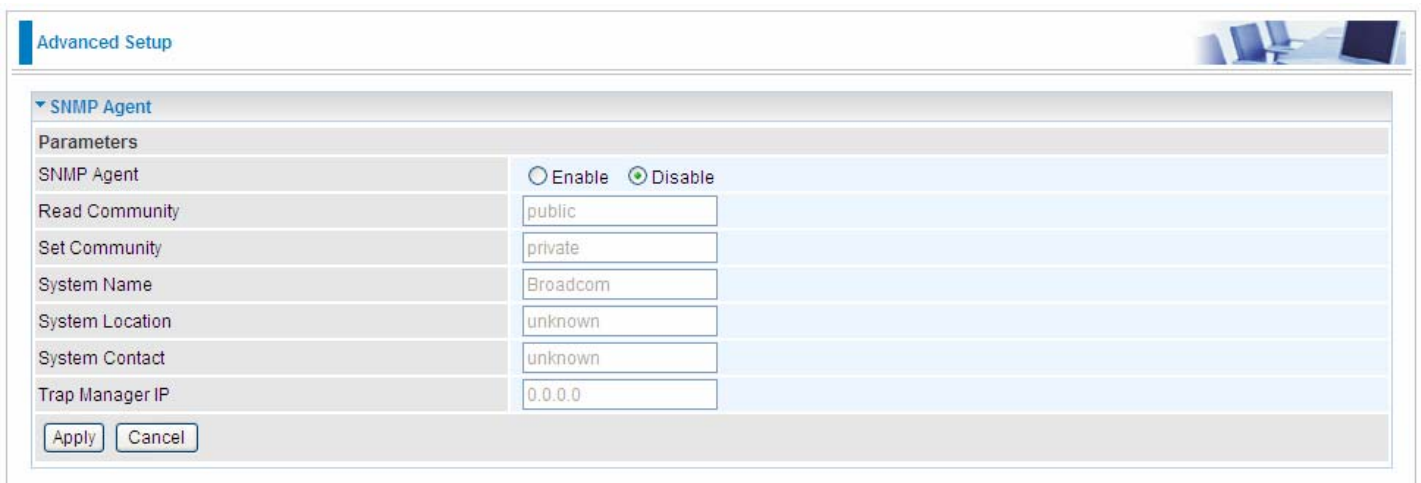
## SNMP Agent

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 the 'Advanced Setup' page for the SNMP Agent configuration. The page has a blue header with the text 'Advanced Setup' and a small image of a server rack on the right. Below the header, there is a section titled 'SNMP Agent' with a dropdown arrow. Underneath, there is a 'Parameters' section with a table of configuration options. The 'SNMP Agent' option is set to 'Disable'. Other options include 'Read Community' (public), 'Set Community' (private), 'System Name' (Broadcom), 'System Location' (unknown), 'System Contact' (unknown), and 'Trap Manager IP' (0.0.0.0). At the bottom of the configuration area, there are 'Apply' and 'Cancel' buttons.

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"/>

**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.

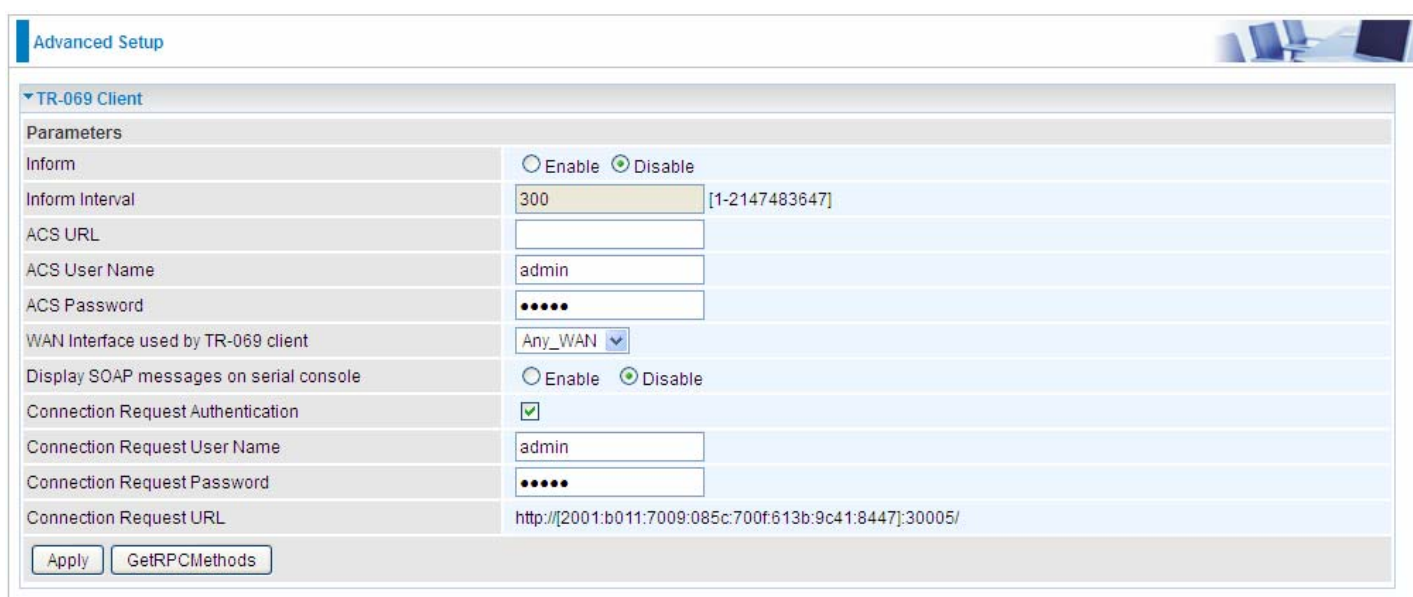
**System Contact:** user-defined contact message.

**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 the 'Advanced Setup' page for the 'TR-069 Client'. The configuration parameters are as follows:

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://[2001:b011:7009:085c:700f:613b:9c41:8447]:30005/

Buttons: 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.

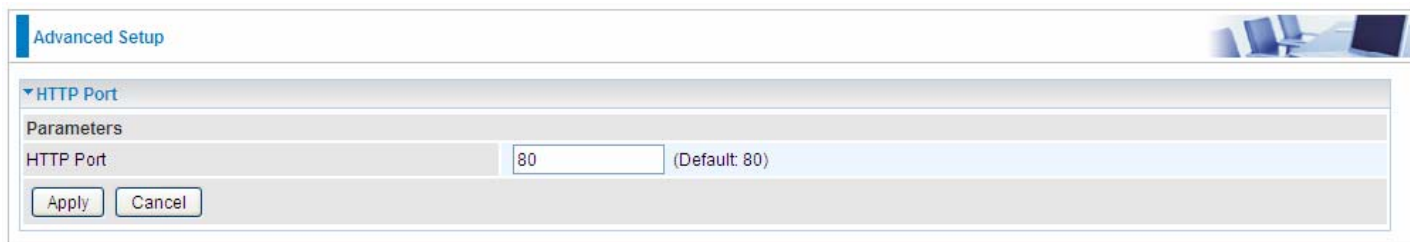
**GetRPCMethods:** Supported by both CPE and ACS, display the supported RFC listing methods.

Click **Apply** to apply your settings.



## HTTP Port

The device equips user to change the embedded web server accessing port. Default is 80.



Advanced Setup

HTTP Port

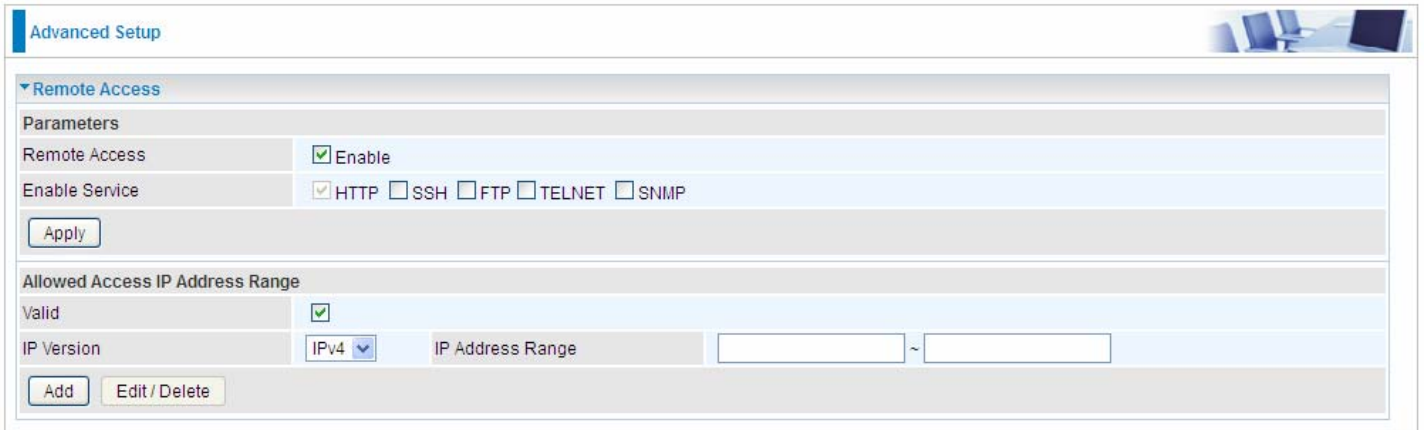
Parameters

HTTP Port  (Default: 80)

Apply Cancel

## Remote Access

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



**Remote Access:** Select “Enable” to allow management access from remote side (mostly from internet). If disabled, no remote access is allowed for any IPs even if you set allowed access IP address. So, please note that enabling remote access is an essential step before granting remote access to IPs.

**Enable Service:** Select to determine which service(s) is (are) allowed for remote access when remote access is enabled. By default (on condition that remote access is enabled), the web service (HTTP) is allowed for remote access.

Click **Apply** button to submit your settings.

"**Allowed Access IP Address Range**" was used to restrict which IP address could login to access system web GUI.

**Valid:** Enable/Disable Allowed Access IP Address Range

**IP Address Range:** Specify the IP address Range, IPv4 and IPv6 address range can be supported, users can set IPv4 and IPv6 address range individually.

Click **Add** to add an IP Range to allow remote access.

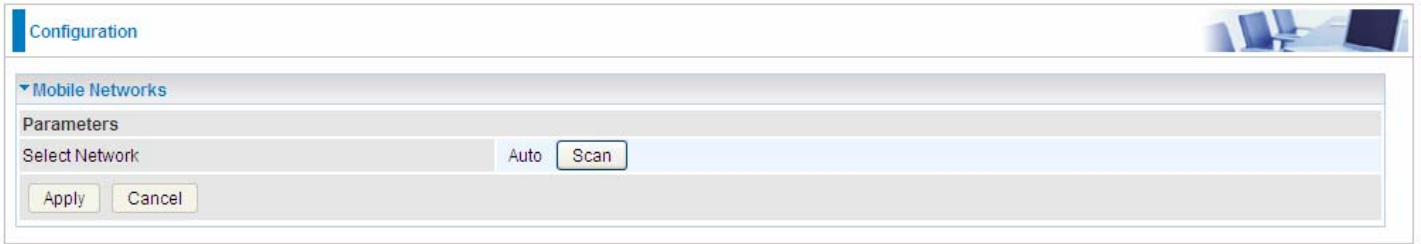
**Note: 1.** If user wants to grant remote access to IPs, first enable **Remote Access**.

**2. Remote Access enabled:**

- 1) Enable **Valid** for the specific IP(s) in the IP range to allow the specific IP(s) to remote access the router.
- 2) Disable **Valid** for all specific IP(s) in the IP range to allow any IP(s) to remote access the router.
- 3) No listing of IP range is to allow any IP(s) to remote access the router.

## Mobile Networks

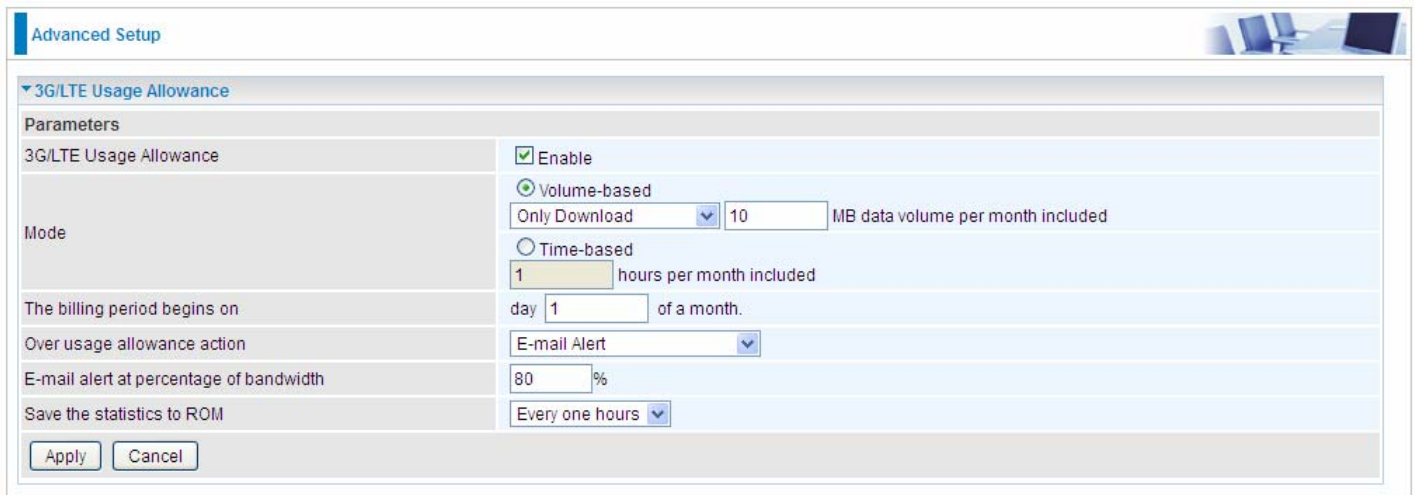
User can press **Scan** to discover available 3G/4G LTE mobile network.



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Mobile Networks". Under "Parameters", there is a "Select Network" field with a dropdown menu currently showing "Auto". To the right of the dropdown are two buttons: "Scan" and "Apply". Below the "Select Network" field are two buttons: "Apply" and "Cancel".

## 3G/4G LTE Usage Allowance

3G/4G LTE usage allowance is designated for users to monitor and control the 3G flow usage. 8700NEXL R2's 3G/4G LTE usage allowance offers exact control settings for each SIM card.



The screenshot shows a web-based configuration interface for "3G/LTE Usage Allowance". The interface is titled "Advanced Setup" and includes a "3G/LTE Usage Allowance" section. The "Parameters" table is as follows:

Parameters	
3G/LTE Usage Allowance	<input checked="" type="checkbox"/> Enable
Mode	<input checked="" type="radio"/> Volume-based
	Only Download <input type="text" value="10"/> MB data volume per month included
	<input type="radio"/> Time-based
	<input type="text" value="1"/> hours per month included
The billing period begins on	day <input type="text" value="1"/> of a month.
Over usage allowance action	E-mail Alert
E-mail alert at percentage of bandwidth	<input type="text" value="80"/> %
Save the statistics to ROM	Every one hours

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

**3G/4G LTE Usage Allowance:** Enable to monitor 3G/4G LTE usage.

**Mode:** include Volume-based and Time-based control.

- ① **Volume-based** include "only Download", "only Upload" and "Download and Upload" to limit the flow.
- ① **Time-based** control the flow by providing specific hours per month.

**The billing period begins on:** The beginning day of billing each month.

**Over usage allowance action:** What to do when the flow is over usage allowance, the available methods are "E-mail Alert", "Email Alert and Disconnect" and "Disconnect".

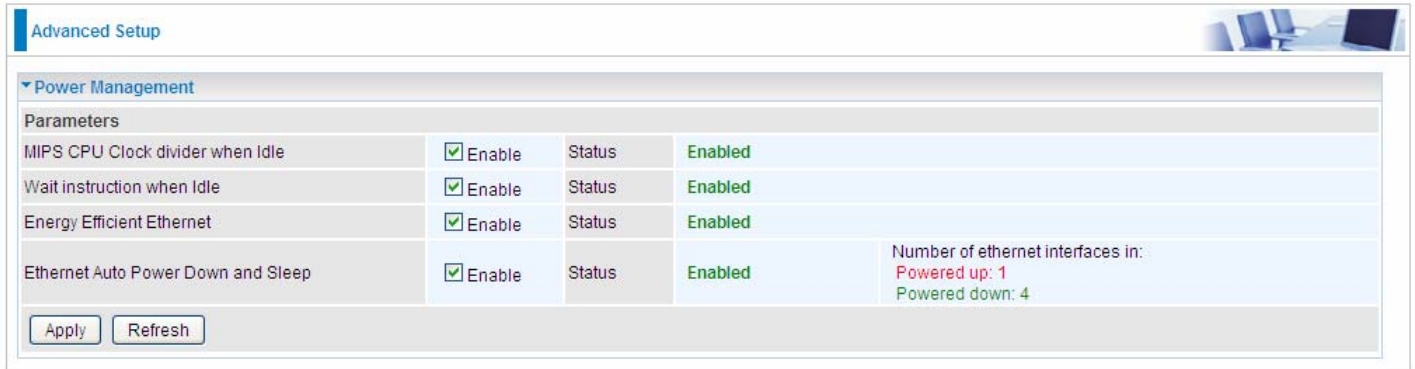
**E-mail alert at percentage of bandwidth:** When the used bandwidth exceeds the set proportion, the system will send email to alert.

**Save the statistics to ROM:** To save the statistics to ROM system.

## Power Management

Power management is a feature of some electrical appliances, especially computers that turn off the power or switch to a low-power state when inactive.

Five main parameters are listed for users to check to manage the performance of the router.



The screenshot shows the 'Advanced Setup' page of a router, specifically the 'Power Management' section. The page has a header 'Advanced Setup' and a sub-header 'Power Management'. Below the sub-header is a table of parameters. The table has four columns: Parameter Name, Action (Enable/Disable), Status, and a detailed status field. All parameters are currently set to 'Enabled'. At the bottom of the table, there are two buttons: 'Apply' and 'Refresh'. To the right of the 'Ethernet Auto Power Down and Sleep' row, there is a summary of ethernet interfaces: 'Number of ethernet interfaces in: Powered up: 1, Powered down: 4'.

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
Energy Efficient Ethernet	<input checked="" type="checkbox"/> Enable	Status	Enabled
Ethernet Auto Power Down and Sleep	<input checked="" type="checkbox"/> Enable	Status	Enabled

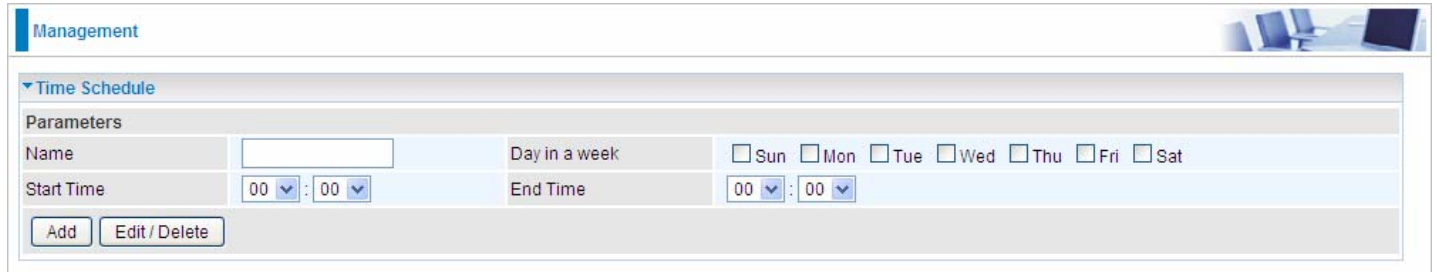
Number of ethernet interfaces in:  
Powered up: 1  
Powered down: 4

Apply Refresh

## Time Schedule

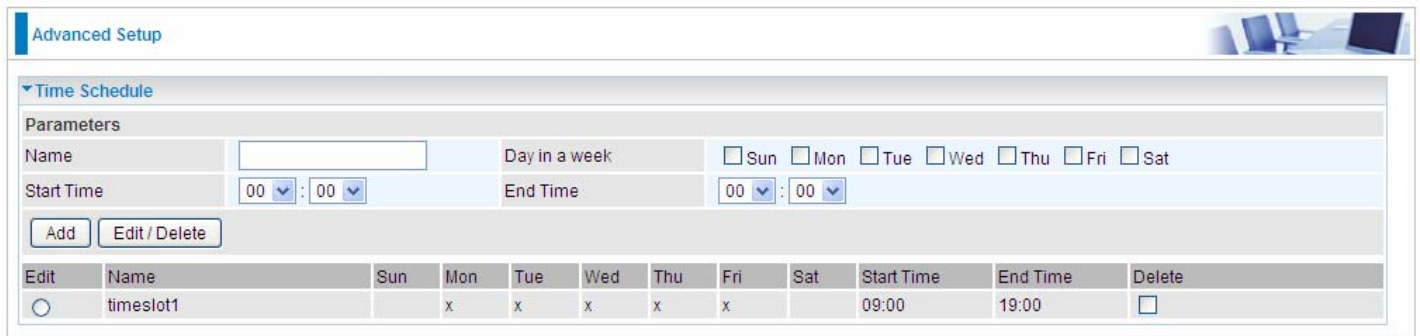
The Time Schedule supports up to **32** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

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 Time](#) for details. Your router time should synchronize with NTP server.



The screenshot shows the 'Management' page with a 'Time Schedule' section. It includes a 'Parameters' form with fields for Name, Day in a week (checkboxes for Sun-Sat), Start Time, and End Time. There are 'Add' and 'Edit / Delete' buttons.

For example, user can add a timeslot named "timeslot1" features a period of 9:00-19:00 on every weekday.

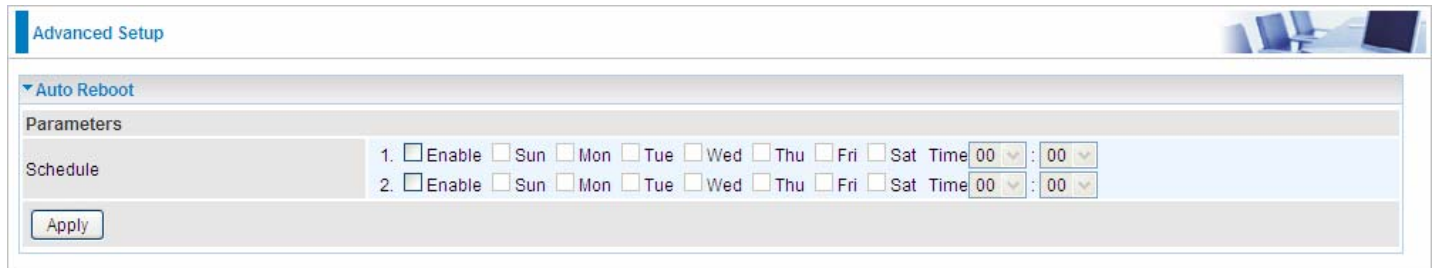


The screenshot shows the 'Advanced Setup' page with a 'Time Schedule' section. It includes a 'Parameters' form and a table of existing timeslots.

Edit	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	End Time	Delete
<input type="radio"/>	timeslot1		x	x	x	x	x		09:00	19:00	<input type="checkbox"/>

## Auto Reboot

Auto reboot offers flexible rebooting service (reboot with the current configuration) of router for users in line with scheduled timetable settings.



Advanced Setup

Auto Reboot

Parameters

Schedule

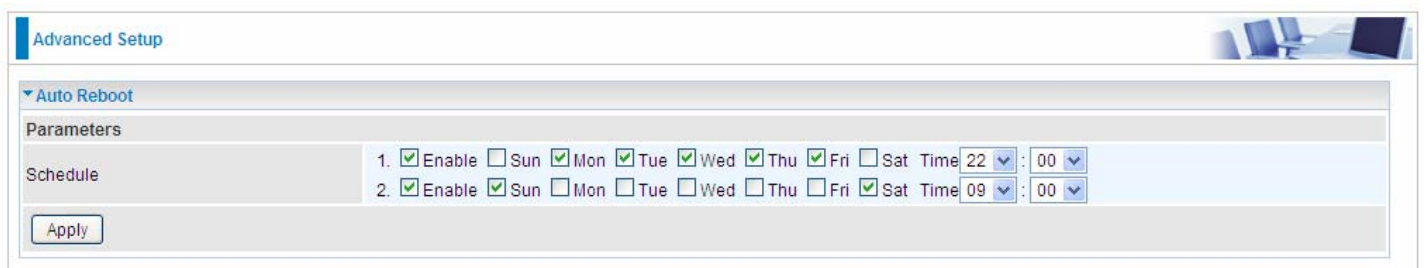
1.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 00 : 00

2.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 00 : 00

Apply

Enable to set the time schedule for rebooting.

For example, the router is scheduled to reboot at 22:00 every single weekday, and to reboot at 9:00 on Saturday and Sunday. You can set as follows:



Advanced Setup

Auto Reboot

Parameters

Schedule

1.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 22 : 00

2.  Enable  Sun  Mon  Tue  Wed  Thu  Fri  Sat Time 09 : 00

Apply

# Diagnostics

## Diagnostics Tools

BiPAC 8700NEXL R2 offers diagnostics tools including “Ping” and “Trace route test” tools to check for problems associated with network connections.

The screenshot shows the 'Advanced Setup' interface for diagnostics. It features two main sections: 'Ping Test' and 'Trace route Test'.  
The 'Ping Test' section includes:  
- 'Destination Host': A text input field.  
- 'Source Address': A radio button for 'Interface' (selected) and a radio button for 'IP Address' (unselected), followed by a text input field.  
- A 'Ping Test' button.  
The 'Trace route Test' section includes:  
- 'Destination Host': A text input field.  
- 'Source Address': A radio button for 'Interface' (selected) and a radio button for 'IP Address' (unselected), followed by a text input field.  
- 'Max TTL value': A text input field with '16' and a range indicator '[2-30]'.  
- 'Wait time': A text input field with '3' and a unit indicator 'seconds [2-999]'.  
- A 'Trace route Test' button.

**Ping Test:** to verify the connectivity between source and destination.

**Destination Host:** Enter the destination host (IP, domain name) to be checked for connectivity.

**Source Address:** Select or set the source address to test the connectivity from the source to the destination.

**Ping Test:** Press this button to proceed ping test.

**Trace route Test:** to trace the route to see how many hops (also see the exact hops) the packet of data has to take to get to the destination.

**Destination Host:** Set the destination host (IP, domain name) to be traced.

**Source Address:** Select or set the source address to trace the route from the source to the destination.

**Max TTL value:** Set the max Time to live (TTL) value.

**Wait time:** Set waiting time for each response in seconds.



## Example: Ping www.google.com

**Advanced Setup**

**▼ Diagnostics Tools**

**Ping Test**

Destination Host:

Source Address:  Interface   IP Address

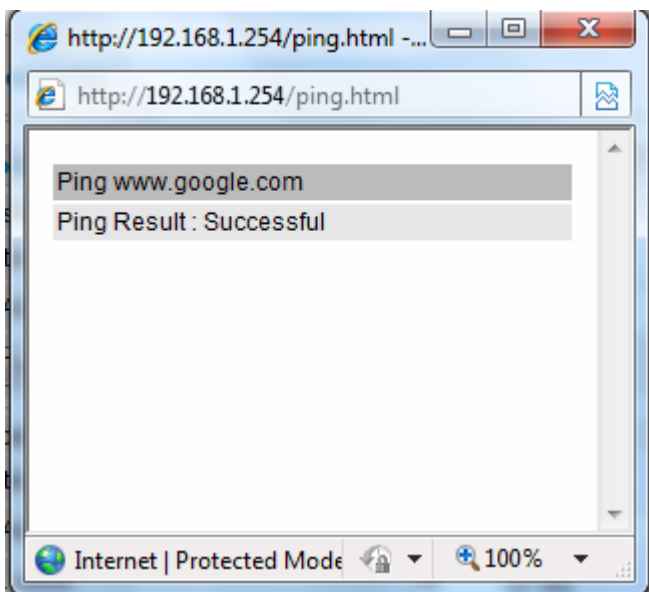
**Trace route Test**

Destination Host:

Source Address:  Interface   IP Address

Max TTL value:  [2-30]

Wait time:  seconds [2-999]



## Example: "trace" www.google.com

**Advanced Setup**

**▼ Diagnostics Tools**

**Ping Test**

Destination Host:

Source Address:  Interface   IP Address

**Trace route Test**

Destination Host:

Source Address:  Interface   IP Address

Max TTL value:  [2-30]

Wait time:  seconds [2-999]

http://192.168.1.254/tracert.html - Windows Intern...

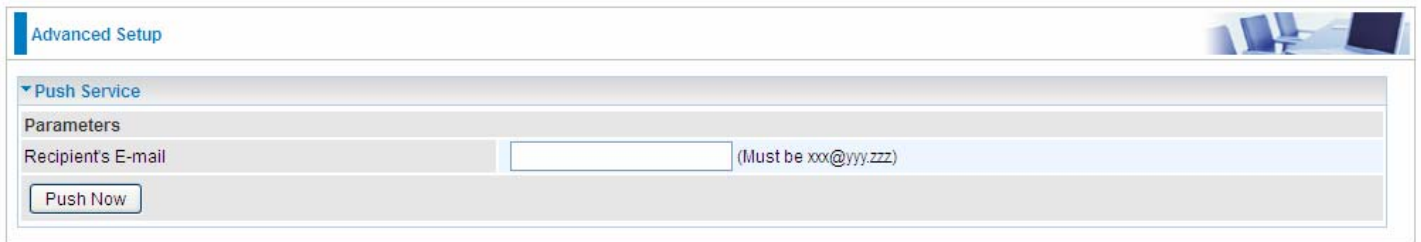
http://192.168.1.254/tracert.html

Trace www.google.com

No.	Route Address	Time
1	112.86.208.1	22.229 ms
2	221.6.9.93	20.352 ms
3	221.6.2.169	24.345 ms
4	219.158.24.41	52.837 ms
5	219.158.23.18	54.696 ms
6	219.158.19.190	54.904 ms
7	219.158.3.238	57.824 ms
8	72.14.215.130	58.851 ms
9	209.85.248.60	57.644 ms
10	209.85.250.122	81.242 ms
11	209.85.250.103	81.351 ms
12	*	**
13	173.194.72.147	79.753 ms

## Push Service

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



The screenshot shows a web interface for 'Advanced Setup'. Under the 'Push Service' section, there is a 'Parameters' area. It contains a text input field labeled 'Recipient's E-mail' with a placeholder '(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.

Click **Help** link that can lead you to the interpretation of the results and the possible, simply troubleshooting.

Advanced Setup 

▼ Test the connection to your local network --- pppoe\_0\_8\_35

Test LAN Connection ( P1 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P3 )	PASS	<a href="#">Help</a>
Test LAN Connection ( P4 )	FAIL	<a href="#">Help</a>
Test LAN Connection ( P2 )	FAIL	<a href="#">Help</a>
Test your Wireless Connection	PASS	<a href="#">Help</a>

▼ Test the connection to your DSL service provider

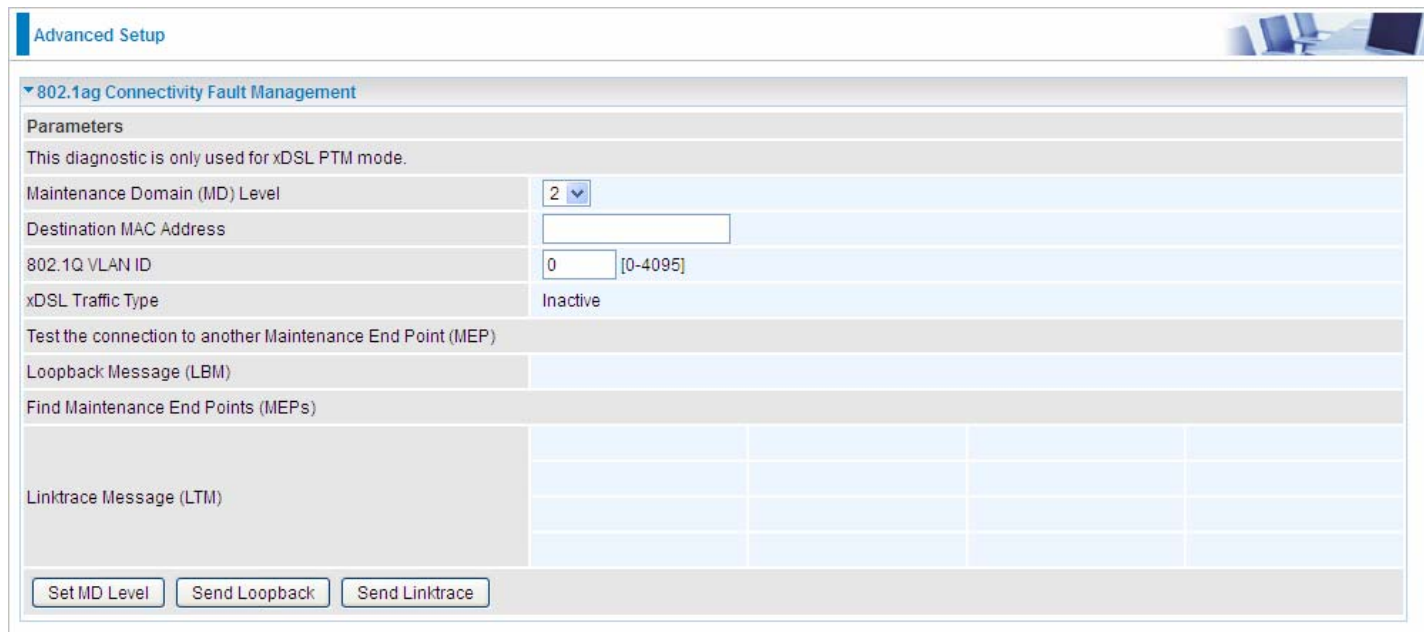
Test xDSL Synchronization	PASS	<a href="#">Help</a>
Test ATM OAM F5 segment ping	FAIL	<a href="#">Help</a>
Test ATM OAM F5 end-to-end ping	PASS	<a href="#">Help</a>

▼ 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	PASS	<a href="#">Help</a>

## 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 PTM connection; Push service



The screenshot shows the 'Advanced Setup' page for '802.1ag Connectivity Fault Management'. The page is titled 'Parameters' and includes a note: 'This diagnostic is only used for xDSL PTM mode.' The configuration fields are as follows:

Maintenance Domain (MD) Level	2
Destination MAC Address	
802.1Q VLAN ID	0 [0-4095]
xDSL Traffic Type	Inactive
Test the connection to another Maintenance End Point (MEP)	
Loopback Message (LBM)	
Find Maintenance End Points (MEPs)	
Linktrace Message (LTM)	

At the bottom of the configuration area, there are three buttons: 'Set MD Level', 'Send Loopback', and 'Send 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 Loop-back to successive MIPs can determine the location of a fault. Sending a high volume of Loop-back Messages can test bandwidth, reliability, or jitter of a service, which is similar to flood ping. A MEP can send a Loop-back to any MEP or MIP in the service. Unlike CCMs, Loop back messages are administratively initiated and stopped.

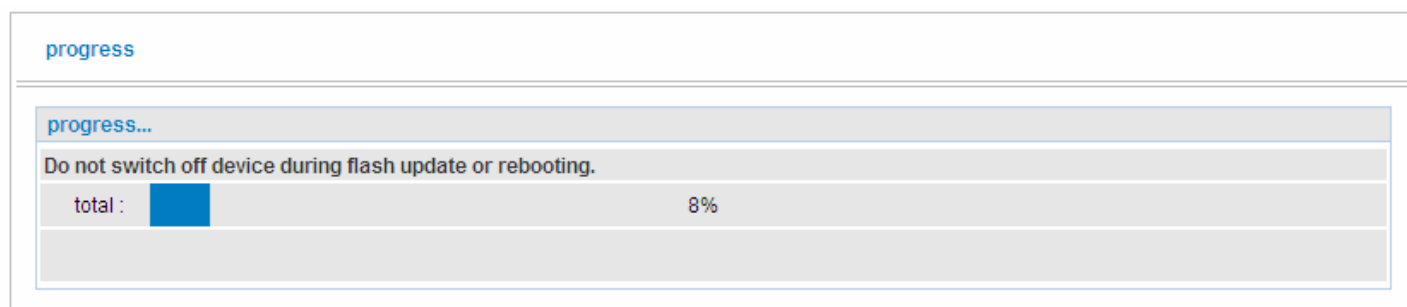
# Restart

This section lets you restart your router if necessary. Click  **Restart** in the low right corner of each configuration page.



The screenshot shows a configuration page with a 'Configuration' header. Below it is a 'Restart' section. The text reads: 'After restarting. Please wait for several seconds to let the system come up.' There are two radio button options: 'Factory Default Settings' and 'Current Settings'. The 'Current Settings' option is selected. A 'Restart' button is located at the bottom left of the section.

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.



The screenshot shows a progress page with a 'progress' header. The text reads: 'Do not switch off device during flash update or rebooting.' Below this is a progress bar labeled 'total :'. The progress bar is partially filled with blue, and the percentage '8%' is displayed to the right of the bar.

# 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 DSL 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 DSL 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
<b>Cannot PING any PC on LAN</b>	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 98, Windows NT, Windows 2000, Windows Me, Windows XP, Windows Vista, Windows 7 and Windows 8 are registered Trademarks of Microsoft Corporation.

## **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ♦ Reorient or relocate the receiving antenna.
- ♦ Increase the separation between the equipment and receiver.
- ♦ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- ♦ Consult the dealer or an experienced radio/TV technician for help.

## **FCC Caution:**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

## **Co-location statement**

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

## **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.