



# **BiPAC 8920AX(L)**

**Dual-lines VDSL2/ADSL2+  
Wireless-AC (VPN) 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
Wireless LAN .....	5
USB Application Server .....	6
Virtual Private Network (VPN) (8920AX only) .....	6
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.....	12
Chapter 3: Basic Installation .....	13
Connecting Your Router.....	14
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 .....	33
Configuration via Web Interface.....	33
Status .....	35
Summary .....	36
WAN .....	37
Statistics .....	38
LAN .....	38
WAN Service.....	39
xTM .....	39
xDSL.....	40
Bandwidth Usage .....	43
LAN .....	43
WAN Service.....	45
Route.....	47
ARP .....	48
DHCP .....	49
Log.....	50
System Log .....	50
Security Log.....	51

Quick Start.....	52
Quick Start.....	52
Configuration .....	57
LAN - Local Area Network .....	58
Ethernet .....	58
IPv6 Autoconfig.....	61
Interface Grouping.....	65
Wireless 5G(wl0) & 2.4G(Wl1) .....	68
Basic .....	69
Security .....	71
MAC Filter .....	83
Wireless Bridge .....	84
Advanced .....	86
Station Info.....	91
Schedule Control.....	92
WAN-Wide Area Network.....	93
WAN Service.....	93
DSL.....	93
Ethernet .....	104
Failover.....	111
DSL.....	112
Dual VDSL2 /ADSL2+ .....	114
SNR.....	115
System.....	116
Internet Time .....	116
Firmware Upgrade .....	117
Backup / Update .....	118
Access Control.....	119
Mail Alert .....	120
SMS Alert.....	121
Configure Log .....	122
USB.....	123
Storage Device Info .....	123
User Account.....	124
Print Server .....	129
DLNA .....	134
IP Tunnel .....	136
IPv6inIPv4.....	136
IPv4inIPv6.....	138
Security .....	139
IP Filtering Outgoing .....	139
IP Filtering Incoming .....	142
MAC Filtering .....	144
Blocking WAN PING .....	145
Time Restriction .....	146
URL Filter.....	148
Parental Control Provider .....	151
QoS - Quality of Service .....	152
Quality of Service .....	152
QoS Port Shaping .....	157
NAT.....	158
Exceptional Rule Group.....	158
Virtual Servers.....	159
DMZ Host .....	163

One-to-One NAT .....	164
Port Triggering .....	165
ALG .....	168
Wake On LAN .....	169
VPN (BiPAC 8920AX only) .....	170
IPSec .....	170
VPN Account .....	180
Exceptional Rule Group.....	181
PPTP .....	183
PPTP Server .....	183
PPTP Client .....	184
L2TP .....	195
L2TP Server .....	195
L2TP Client .....	197
GRE .....	211
Advanced Setup .....	212
Routing .....	213
Default Gateway .....	213
Static Route .....	214
Policy Routing .....	216
RIP .....	217
DNS.....	218
DNS.....	218
Dynamic DNS.....	220
DNS Proxy.....	223
Static DNS.....	224
Static ARP .....	225
UPnP.....	226
Certificate.....	232
Trusted CA.....	232
Multicast .....	235
Management.....	237
SNMP Agent .....	237
TR- 069 Client .....	238
HTTP Port .....	240
Remote Access .....	241
Power Management .....	242
Time Schedule .....	243
Auto Reboot .....	244
Diagnostics .....	245
Diagnostics Tools .....	245
Push Service .....	248
Diagnostics .....	249
Fault Management.....	250
Restart.....	251
Chapter 5: Troubleshooting .....	252
Appendix: Product Support & Contact .....	254

# Chapter 1: Introduction

## Introduction to your Router

The Billion BiPAC 8920AX(L) , a multi service VDSL2 Dual-lines (30a) Router over comparable single-port model. It features fibre-ready dual-WAN VDSL2 supports backward compatibility to ADSL2+ for a longer reach distance, an all-in-one advanced device including concurrent dual-band 802.11ac (5GHz) 1300Mbps and 802.11n (2.4GHz) 300Mbps, Gigabit Ethernet. As well as being IPv6-capable, the BiPAC 8920AX(L) VDSL2 router supports superfast 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. With an array of advanced features, the Billion BiPAC 8920AX(L) delivers a future-proof solution for VDSL2 connections, superfast FTTC and ultra-speed FTTH (Fibre-To-The-Home) network deployment and services.

### Flexible Deployment Options

The BiPAC 8920AX(L) provides users with flexible, scalable deployment options optimized to both reduce costs and provide the longest possible lifespan for the investment. The BiPAC8920AX(L) 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. Operators can now deploy one device to support current and future network migration.

### Maximum wireless performance

Featured with simultaneous dual-band technology, the BiPAC 8920AX(L) can run both 2.4GHz and 5GHz frequency bands at the same time, offering ultra-fast wireless speeds of up to 1600Mbps (1300+300 )and multiple SSIDs on both bands. The BiPAC 8920AX(L), by adopting this state-of-the-art technology, allows for multiple-demand applications, such as streaming HD videos and multiplayer gaming simultaneously. 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 8920AX(L) has five Gigabit LAN ports and port #5 can be configured as an Ethernet WAN port. This EWAN offers another broadband connectivity option for connecting to a cable, DSL, fibre modem. The BiPAC8920AX(L) again offers users convenience and optimal network performance with data rates reaching up to 1Gbps.

### IPv6 supported

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

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

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

### **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)
- Dual- WAN approach – VDSL2/ADSL2+, and Ethernet WAN for Broadband Connectivity
- 5-port Gigabit Ethernet switch
- 1-port (Port#5) Gigabit Ethernet WAN (EWAN) port for broadband connectivity.
- Compliant with IEEE 802.11a/b/g/n/ac standards
- Ultimate wireless speed 300+1300Mbps
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless security with WPA-PSK/WPA2-PSK
- Supports WDS repeater function
- Multiple wireless SSIDs with wireless guest access and client isolation
- Secured IPsec VPN with powerful DES/ 3DES/ AES (BiPAC 8920AX only)
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication (BiPAC 8920AX only)
- Pure L2TP and L2TP over IPsec (BiPAC 8920AX only)
- GRE tunnel (BiPAC 8920AX only)
- 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 and failback
- 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
  - ITU-T G.993.2 (VDSL2)
  - ITU-T G.998.4 (G.inp)
  - ITU-T G.993.5 (G.vector)
  - ITU-T G.992.5 (G.dmt.bis plus, Annex M )  
(ADSL2+ Annex M, available for BiPAC 8920AX(L)A model only)
  - ITU-T G.992.3 (G.dmt.bis, Annex M, ADSL2

Annex M, available for BiPAC 8920AX(L)A model only)

- Full-rate ANSI T1.413 Issue 2
- ITU-T G.992.1 (G.dmt)
- ITU-T G.992.2 (G.lite)
- ITU-T G.994.1 (G.hs)
- Supports VDSL2 band plan: 997 and 998
- ADSL/2/2+ fallback modes
- Supports VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a and 30a in single line mode
- Supports ATM and PTM modes

## **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)
- VLAN MUX support

## Wireless LAN

- Compliant with IEEE 802.11 a/ b/ g/ n/ac standards
- 2.4 GHz and 5GHz frequency range
- Up to 300+1300 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
- Wireless LAN Schedule control

## USB Application Server

- Storage/NAS: FTP server, Samba server, DLNA
- Printer Server

## Virtual Private Network (VPN) (8920AX only)

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

## Management

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

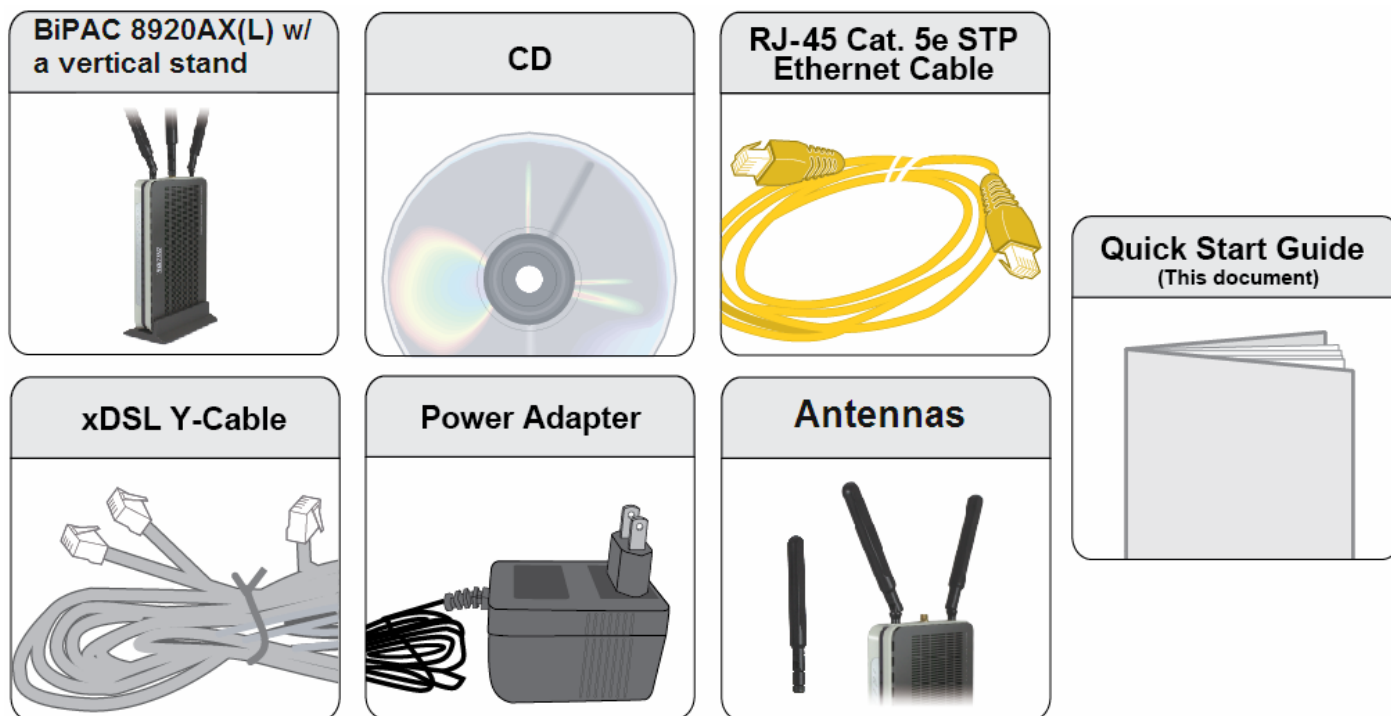
## Physical Interface

- WLAN: 3 external antennas
- DSL: VDSL port
- USB 2.0: 1-port USB 2.0 interface for storage service and printer server
- Ethernet: 5-port 10 / 100 / 1000Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: 1 Gigabit Ethernet port (port#5) connecting directly to Fiber/ xDSL/ Cable modem, also serving as a Ethernet port#5 when not in EWAN use
- Wireless on/off and WPS push button
- Power jack
- Power switch
- Factory default reset button

# Chapter 2: Installing the Router

## Package Contents

- BiPAC 8920AX(L) Dual-lines VDSL2/ADSL2+ Wireless-AC (VPN) Firewall Router
- Quick Start Guide
- CD containing the on-line manual
- Vertical Stand
- RJ-45 Cat. 5e STP Ethernet cable
- RJ-11 telephone cable
- Power adapter
- 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.

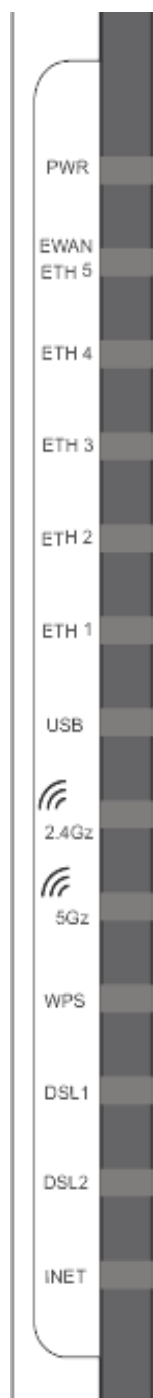


### Attention

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.

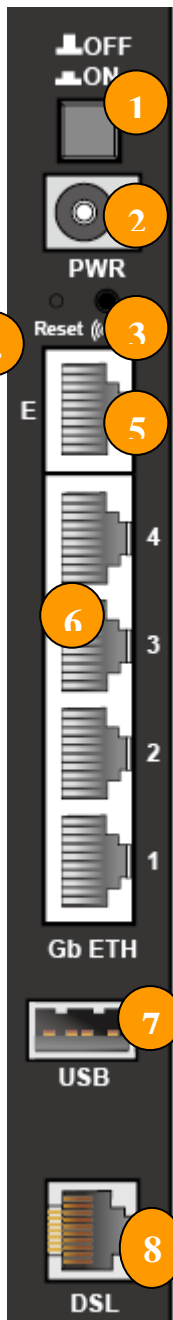
# Device Description

## The Front LEDs



LED	Status	Meaning
<b>Power</b>	Red	Boot failure or in emergency mode
	Green	System ready
<b>Gigabit Ethernet Port 5/EWAN</b>	Green	Connected to an Gigabit Ethernet device or to a broadband connection device.
	Orange	Connect to an 10/100Mbps Ethernet device
	Blinking	Data being transmitted / received
<b>Gigabit Ethernet Port 1-4</b>	Green	Successfully connected to a 1000Mbps LAN device
	Orange	Successfully connected to a 10/100Mbps LAN device
	Blinking	Data being transmitted / received
<b>USB</b>	Green	USB connection established
<b>Wireless</b>	Green	Wireless connection established
	Blinking	Data being transmitted / received
<b>WPS</b>	Green	Wireless device(s) being connected successfully via WPS mode
	Blinking	WPS configuration being in progress
	Off	WPS is off
<b>DSL 1 / 2</b>	Green	Successfully connected to an xDSL DSLAM (Line Synced)
	Green Blinking	DSL synchronizing or waiting for DSL synchronizing
	Off	DSL cable unplugged
<b>Internet</b>	Green	IP connected and traffic is passing through the device
	Blinking	Data being transmitted / received
	Red	BiPAC 8920AX(L) fails to obtain and IP.
	Off	BiPAC 8920AX(L) is either in bridged mode or WAN/DSL connection is not ready

# The Rear Ports



Port		Meaning
1	ON/OFF	Power ON / OFF switch.
2	PWR	Connect the supplied power adapter to this jack.
3	WPS /Wireless on/off button	By controlling the pressing time, users can achieve two different effects: <b>(1) WPS:</b> Press &hold the button for <b>less than 6 seconds</b> to trigger WPS function. <b>(2) Wireless ON/OFF button:</b> Press & hold the button for <b>more than 6 seconds</b> to On/Off the wireless.
4	Reset	Push and hold the reset button for five (5) seconds to restore to its factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
5	E (Gb EWAN)	Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable, for broadband connectivity. <b>Note: LAN 5 automatically becomes an EWAN port when EWAN internet interface is being selected in the GUI</b>
6	GB LAN Ethernet (1-5)	Connect PCs, Laptops or any other office/home LAN devices with the supplied RJ-45 Ethernet cable (Cat-5 or Cat-5e) to any of the five LAN ports. <b>Note: Port 5 is a LAN / WAN Configurable Port.</b>
7	USB	Connect with a hard driver for mobile connectivity.
8	DSL	Connect the device to an ADSL/VDSL telephone jack or splitter using a RJ-11 telephone cable / Y-Cable for xDSL Dual-lines

# 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 7 / 98 / NT / 2000 / XP / Me / Vista, etc. The product provides an easy and user-friendly interface for configuration.

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

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

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



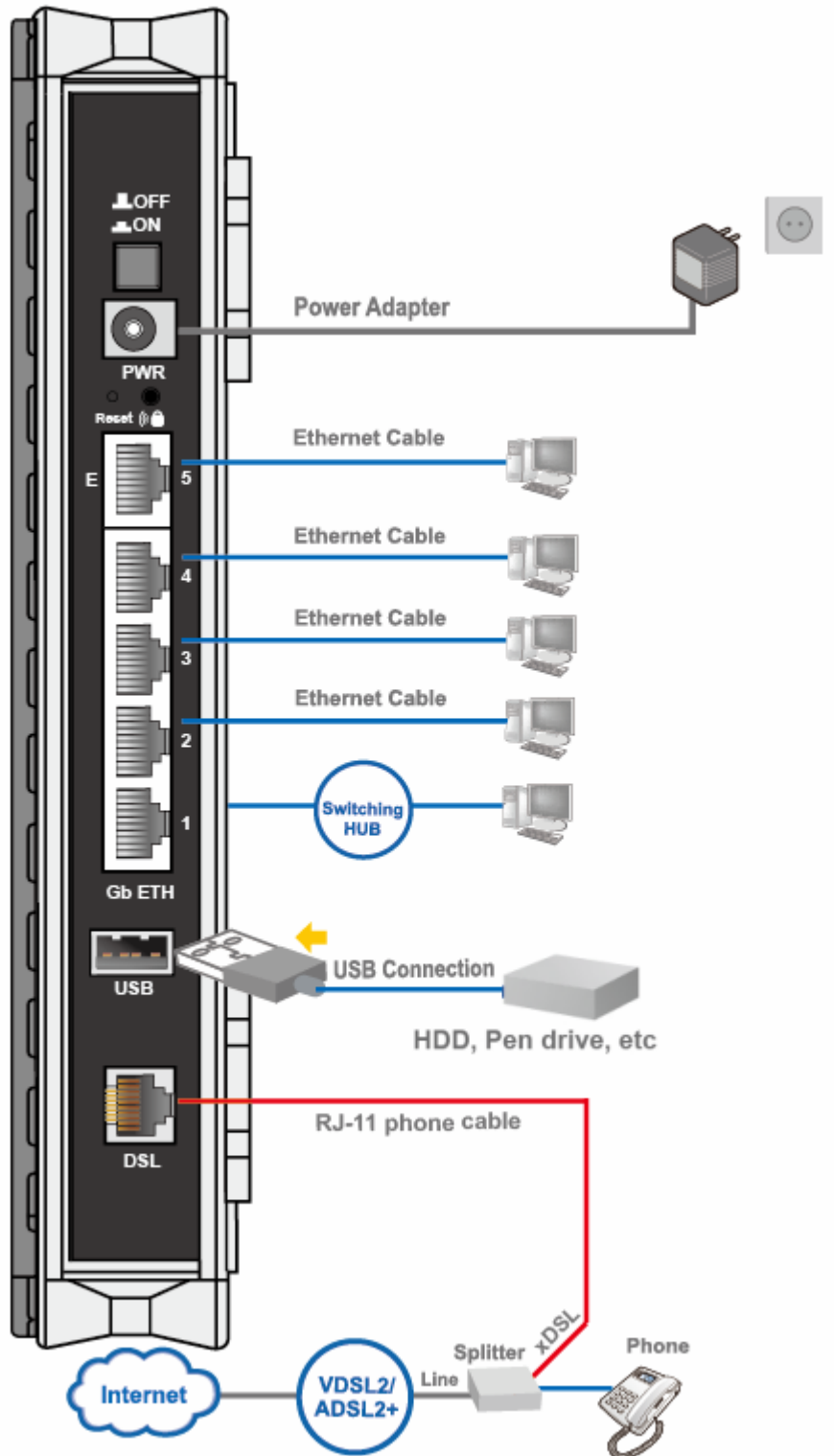
Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

# Connecting Your Router

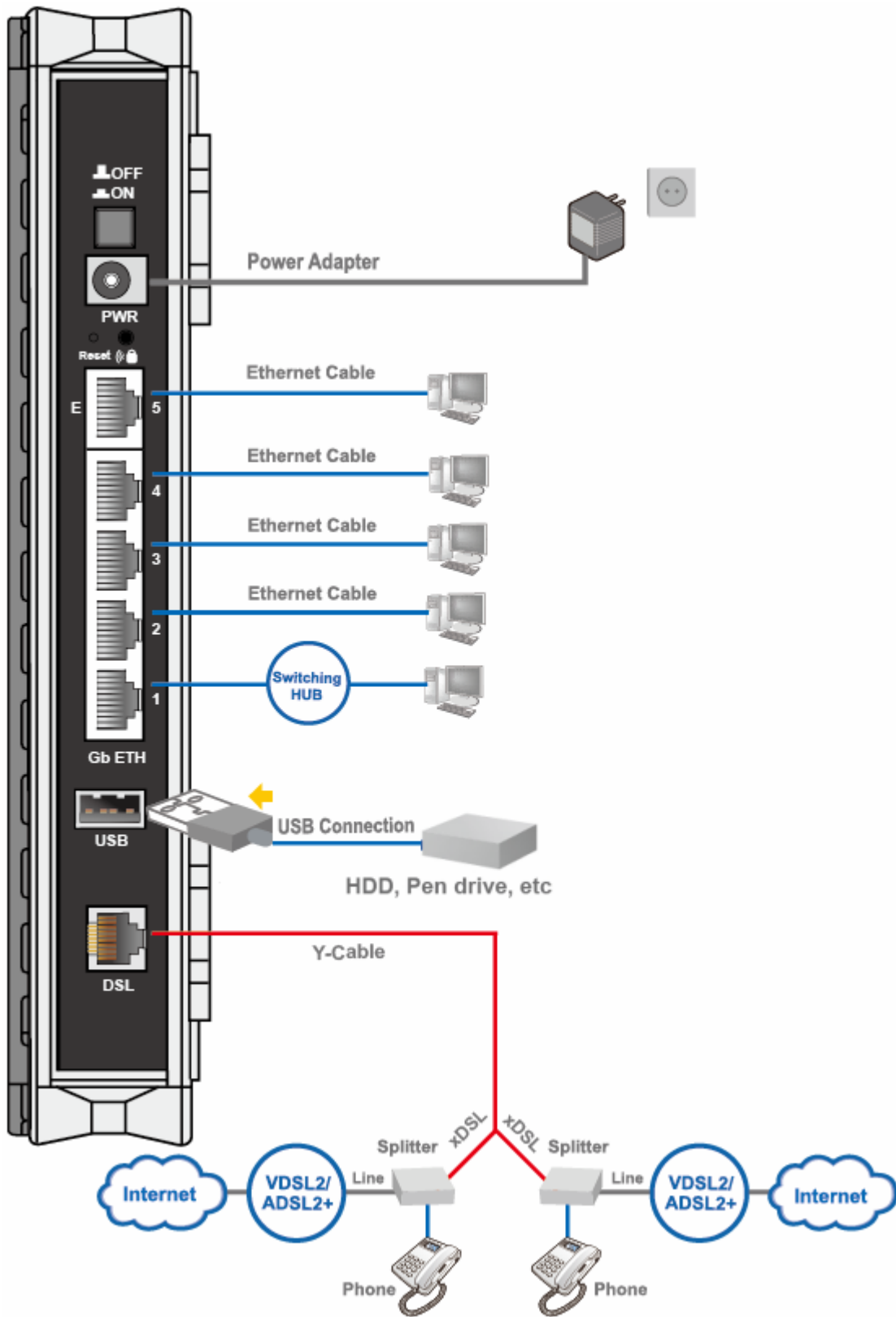
Users can connect the ADSL2+ router as the following.

DSL Router mode:

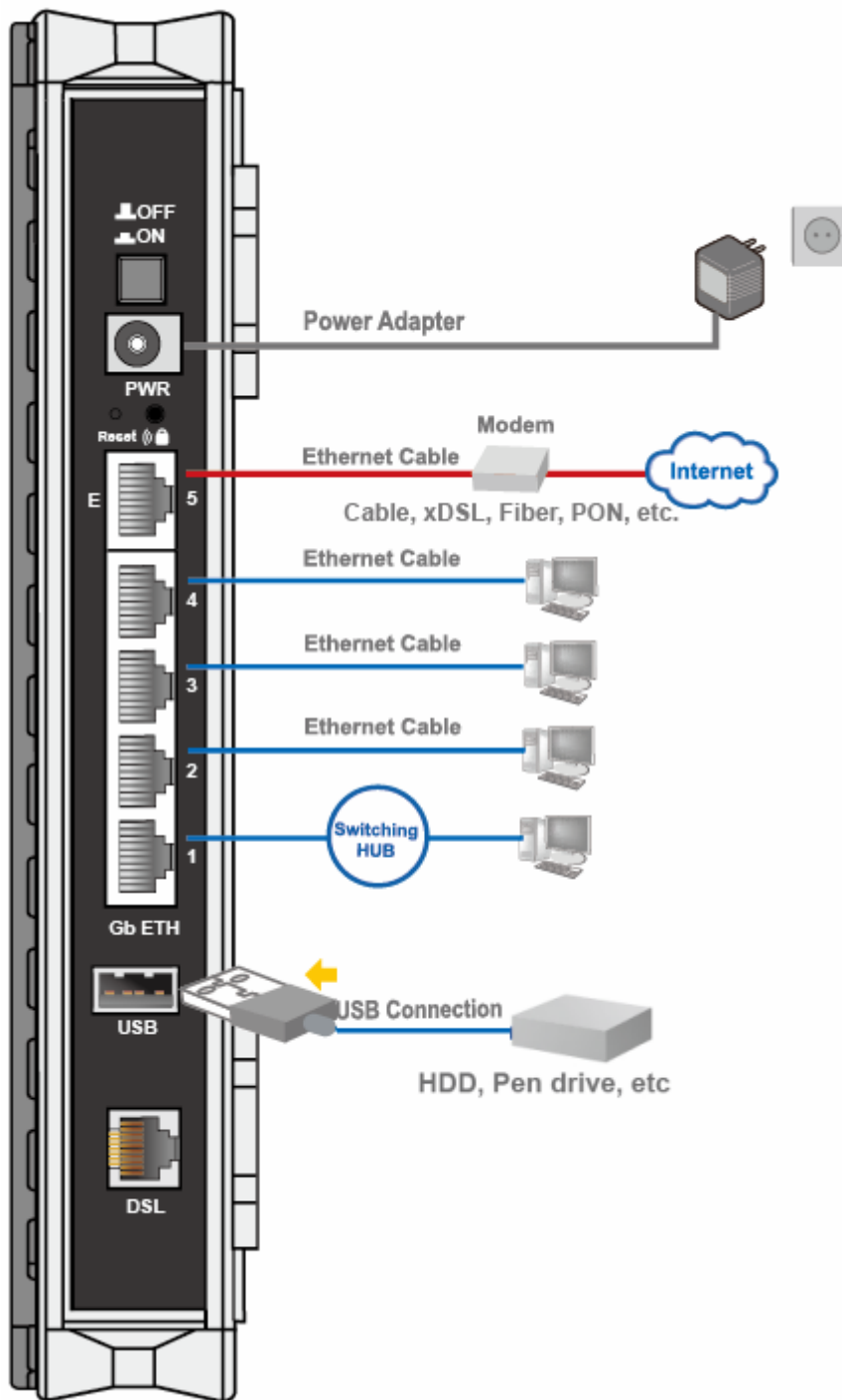
- **Single Pair**



- two-paired



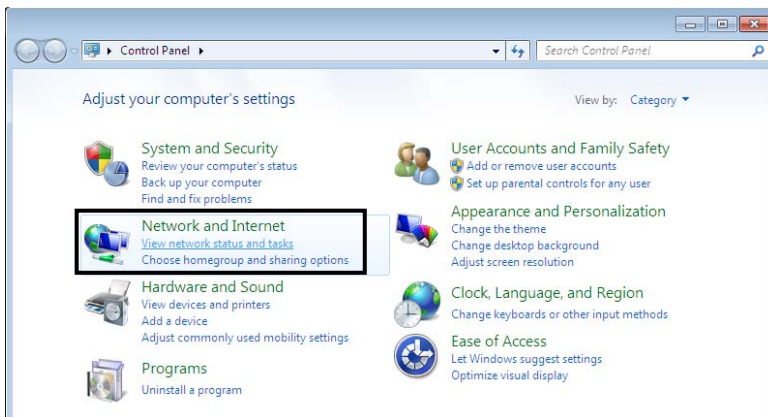
# Broadband Router mode:



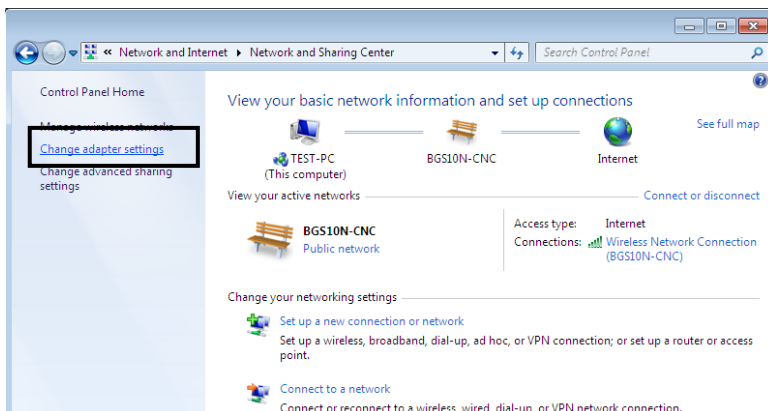
# Network Configuration

## Configuring a PC in Windows 7/ 8

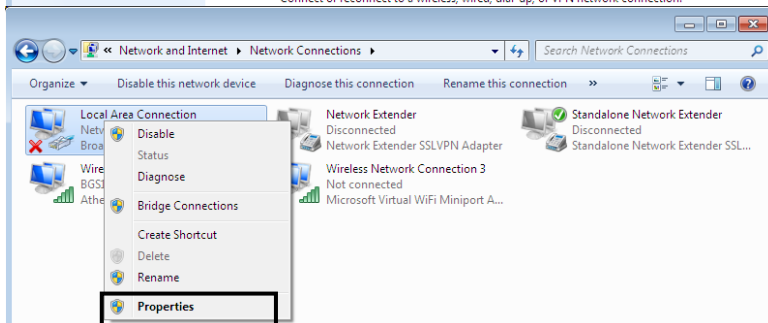
1. Go to **Start**. Click on **Control Panel**. Then click on **Network and Internet**.



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

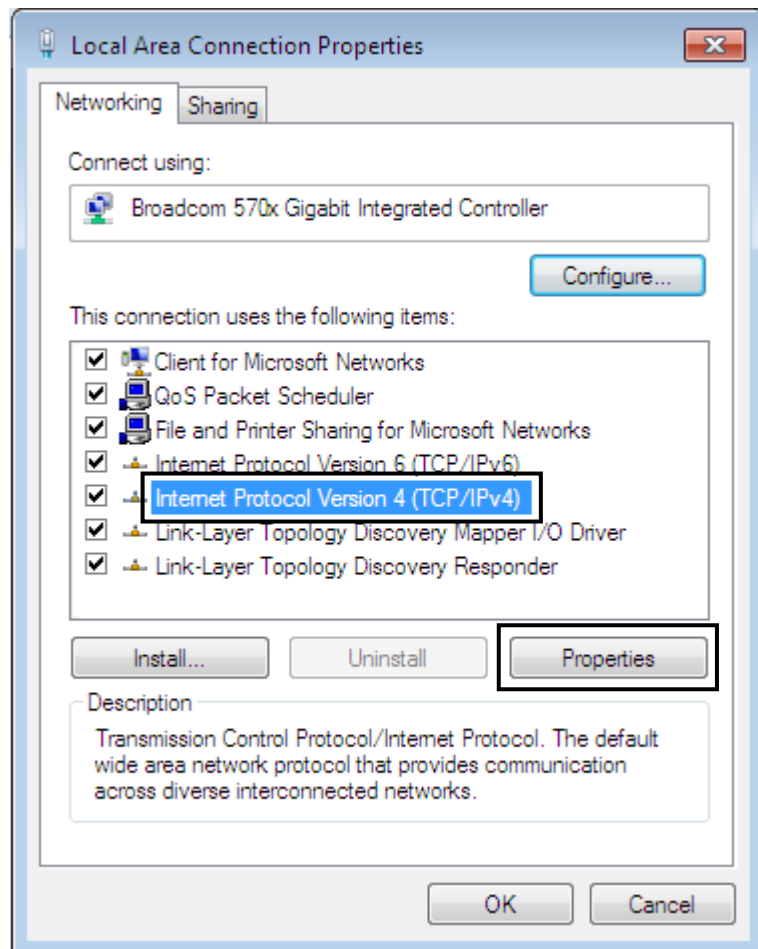


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

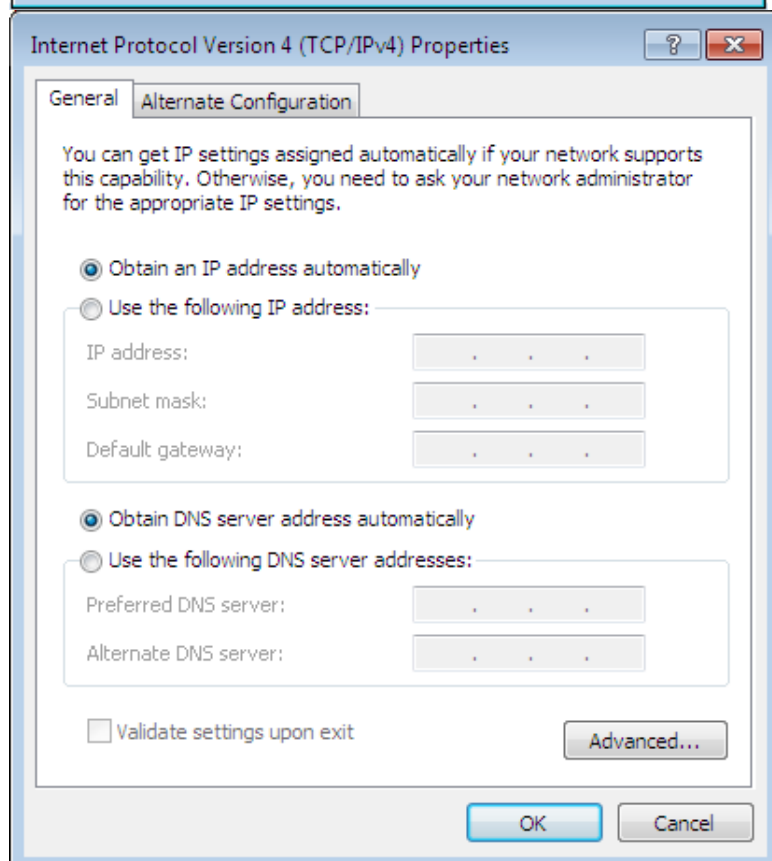


## IPv4:

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

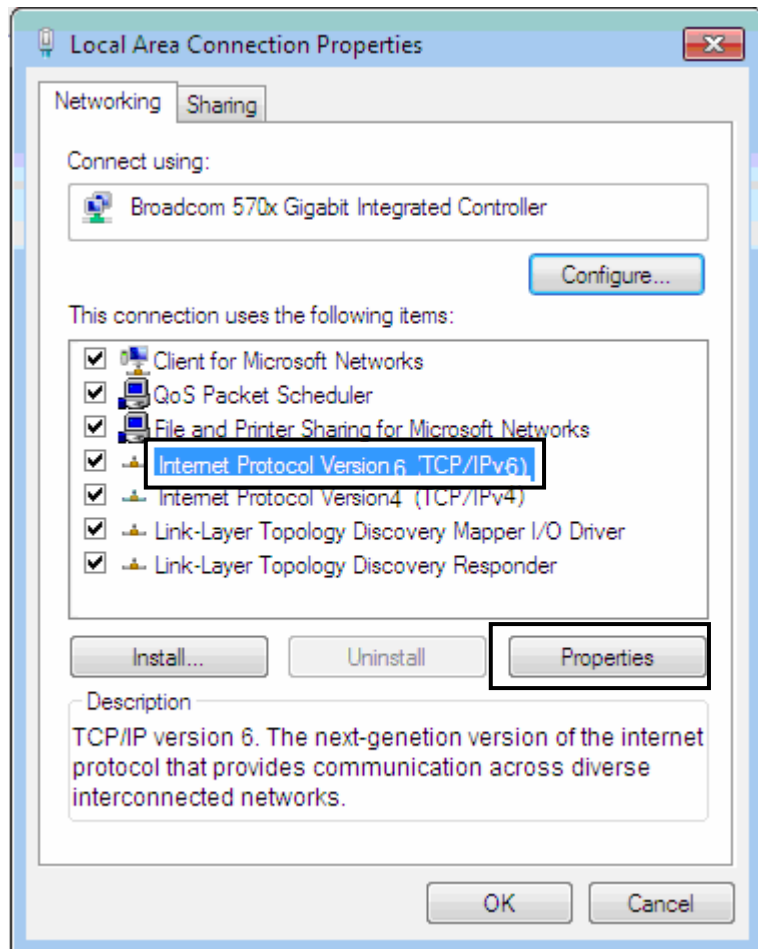


5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

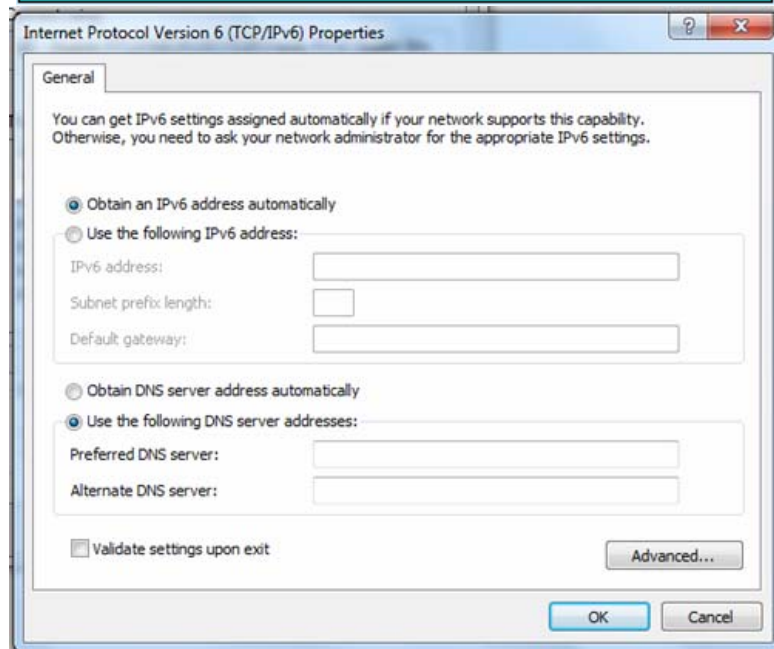


## IPv6:

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

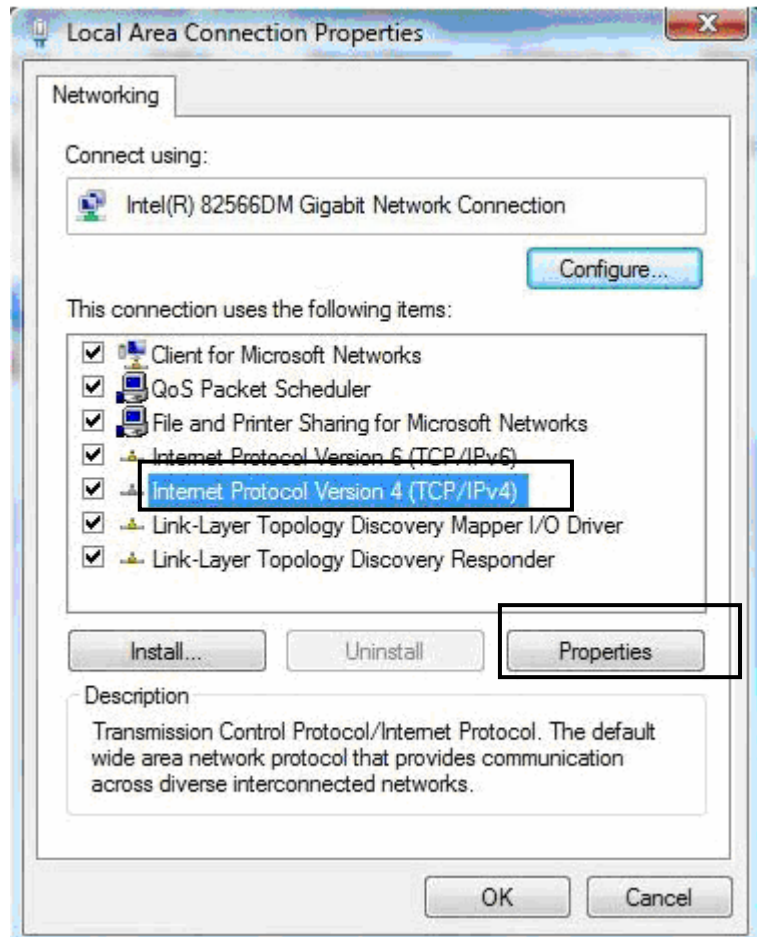
1. Go to **Start**. Click on **Network**.
2. Then click on **Network and Sharing Center** at the top bar.
3. When the **Network and Sharing Center** window pops up, select and click on **Manage network connections** on the left window pane.
4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



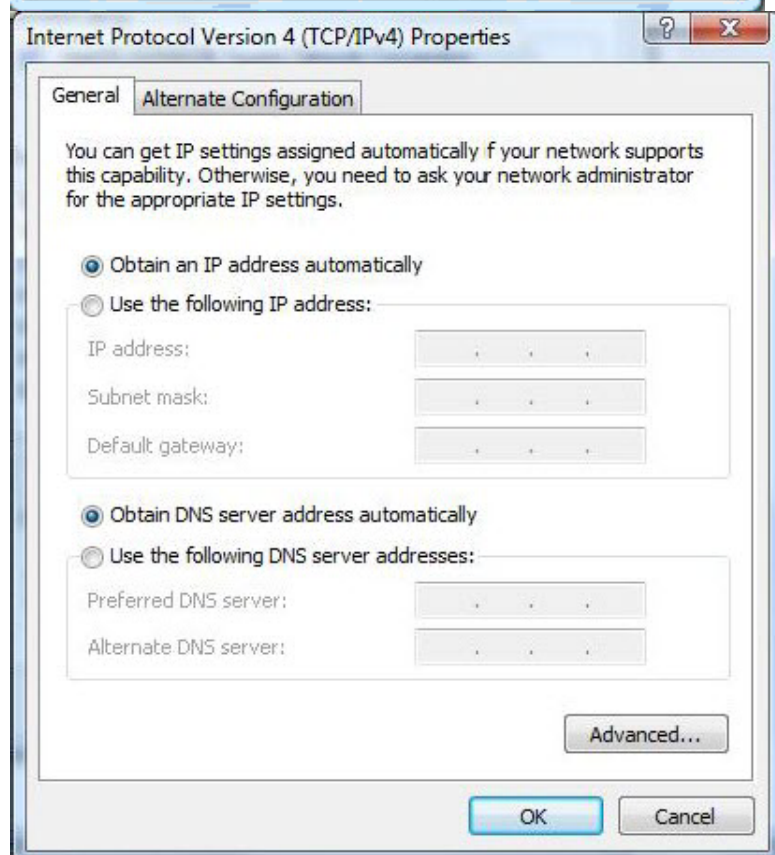


## IPv4:

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

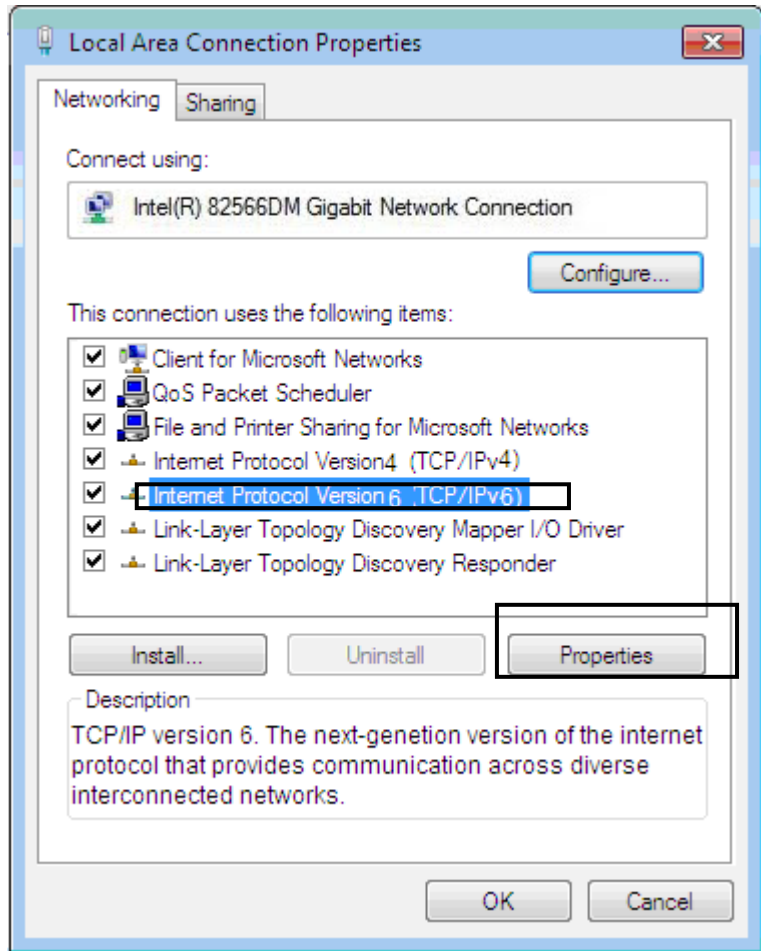


6. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
7. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



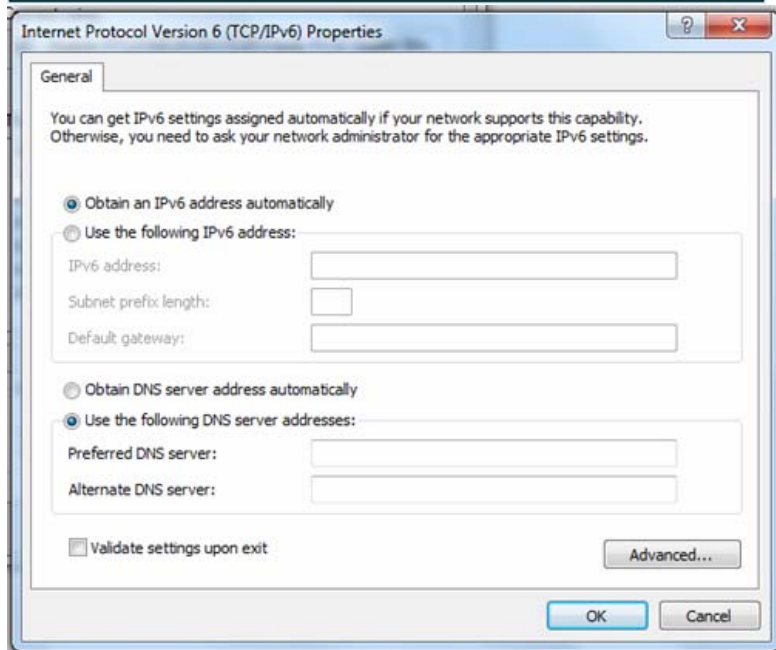
## IPv6:

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.

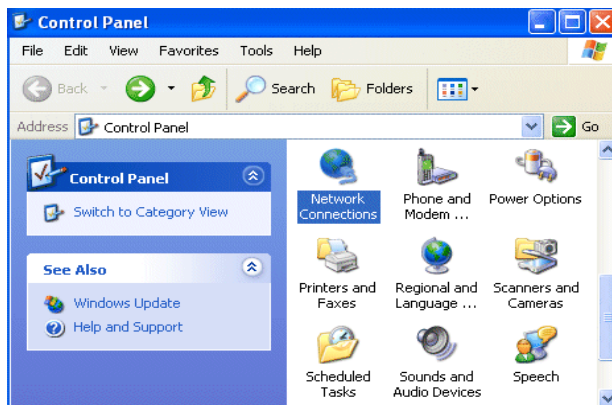
10. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



# Configuring a PC in Windows XP

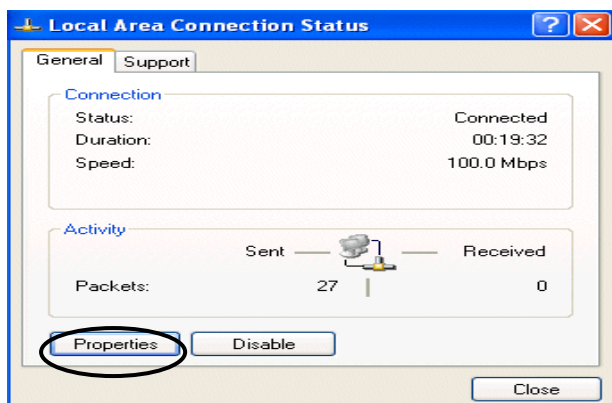
## IPv4:

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

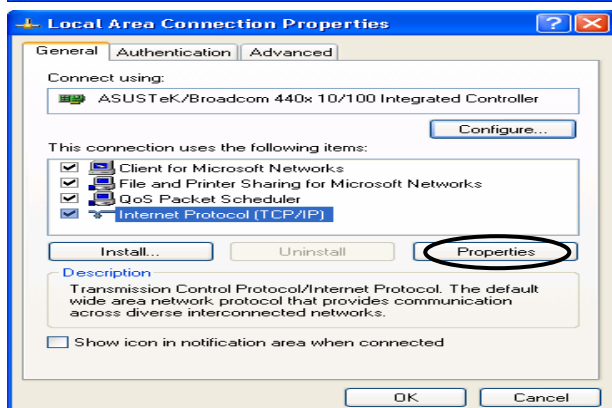


2. Double-click **Local Area Connection**.

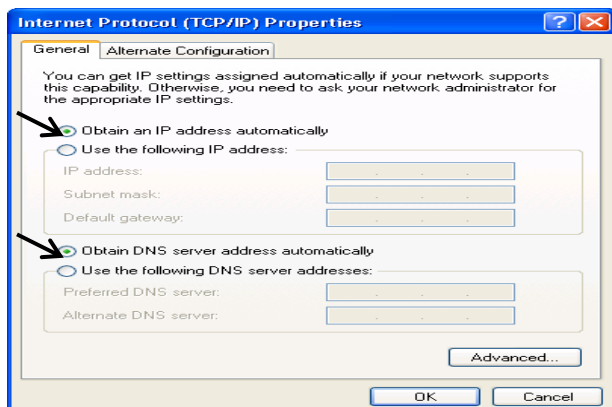
3. In the **Local Area Connection Status** window, click **Properties**.



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.



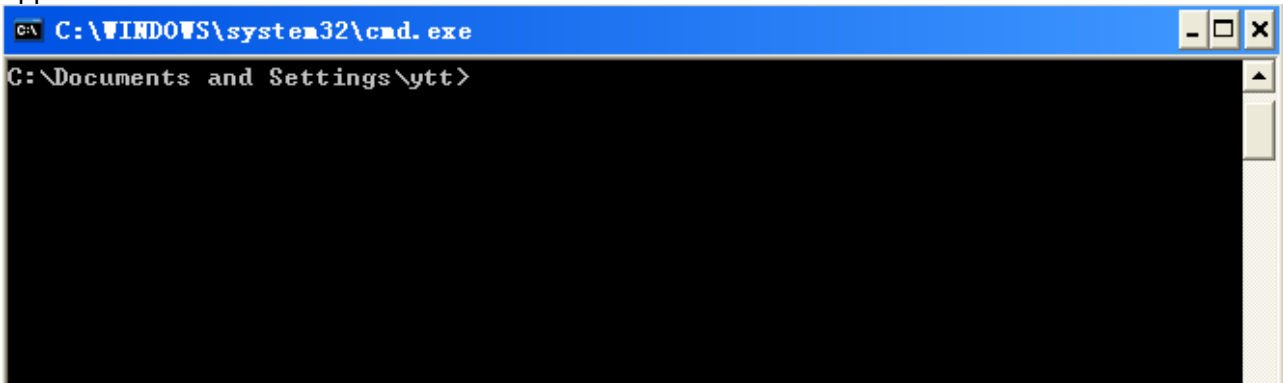
6. Click **OK** to finish the configuration.

## IPv6:

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

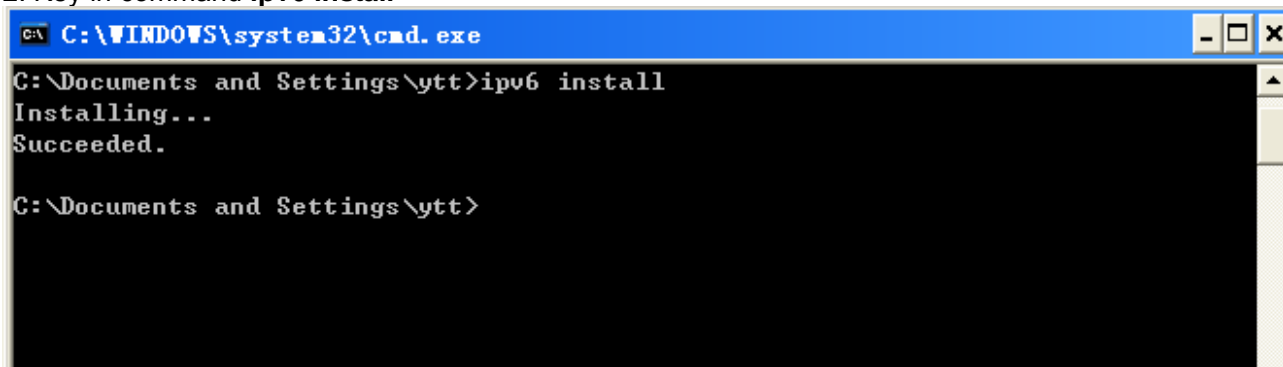
Act as shown below:

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.

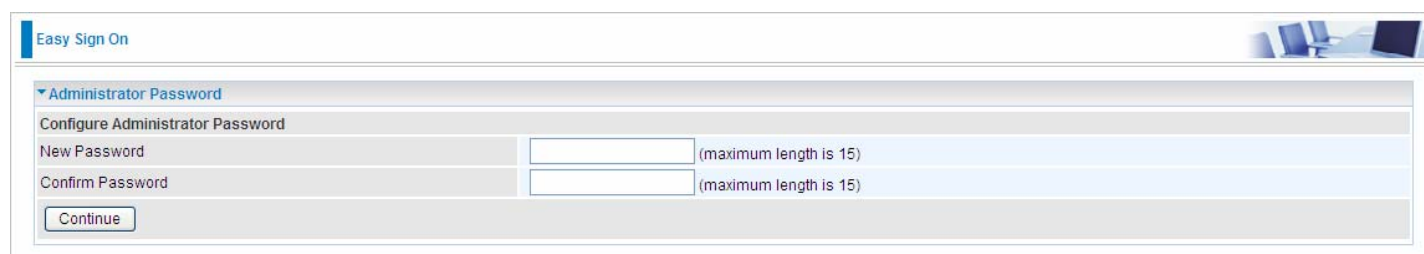
# Easy Sign On (EZSO)

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.



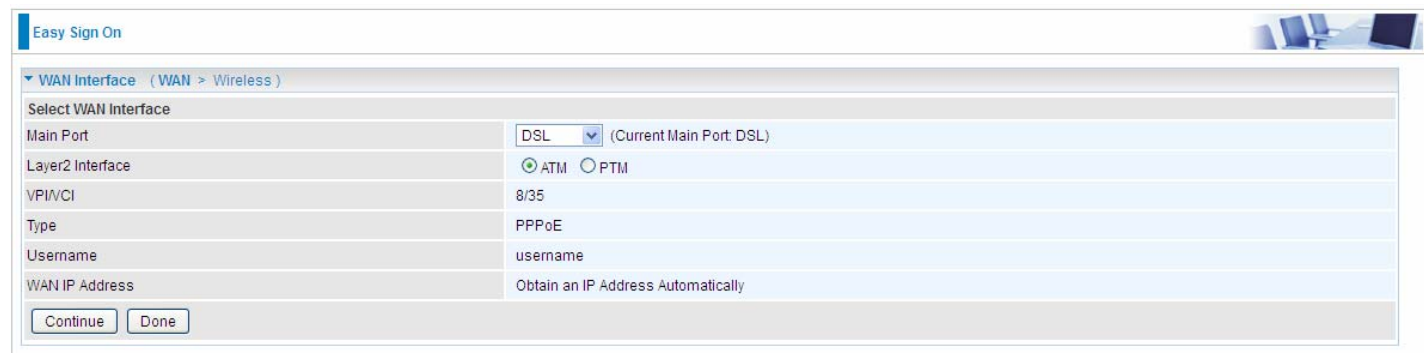
The screenshot shows the 'Easy Sign On' window with the 'Time Zone' section expanded. It contains a dropdown menu for 'Time zone offset' with the selected option '(GMT-00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. A 'Continue' button is located at the bottom left of the section.

**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.

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

1. 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)
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 DSL line doesn't synchronize, the page will pop up warning of the DSL connection failure.

Easy Sign On

WAN Interface (WAN > Wireless)

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

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

Easy Sign On

WAN Interface (WAN > Wireless)

Please wait while the device is configured.

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

Easy Sign On

WAN Interface (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless Done

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

Easy Sign On

WAN Interface

Stop EZSO

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

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 8920AX(L) supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key. (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

Easy Sign On

Wireless (WAN > Wireless)

Parameters

Band	5GHz (w10)
Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap-5g
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Easy Sign On

Wireless (WAN > Wireless)

Please wait while the device is configured.

## 6. Continue to set 2.4GHz wireless.

Easy Sign On

Wireless (WAN > Wireless)

Parameters

Band	2.4GHz (w11)
Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap-2.4g
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Easy Sign On

Wireless (WAN > Wireless)

Please wait while the device is configured.

## 7. Success in configuring the EZSO.

Easy Sign On

Process finished

Success.

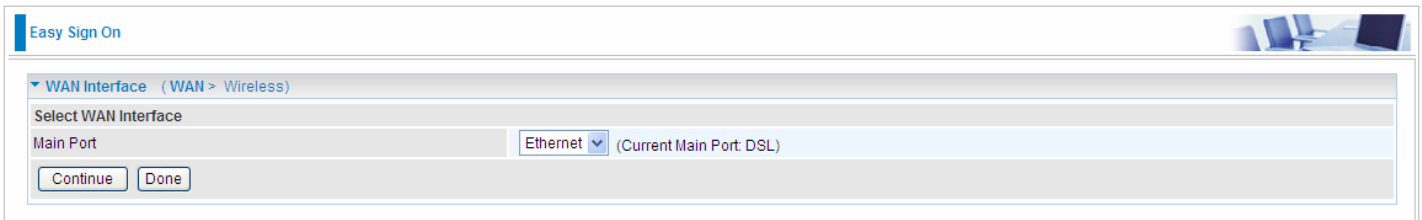
The Easy-Sign-On process is finished. Your device has been successfully configured.

You can now:

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

## Ethernet mode

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



Easy Sign On

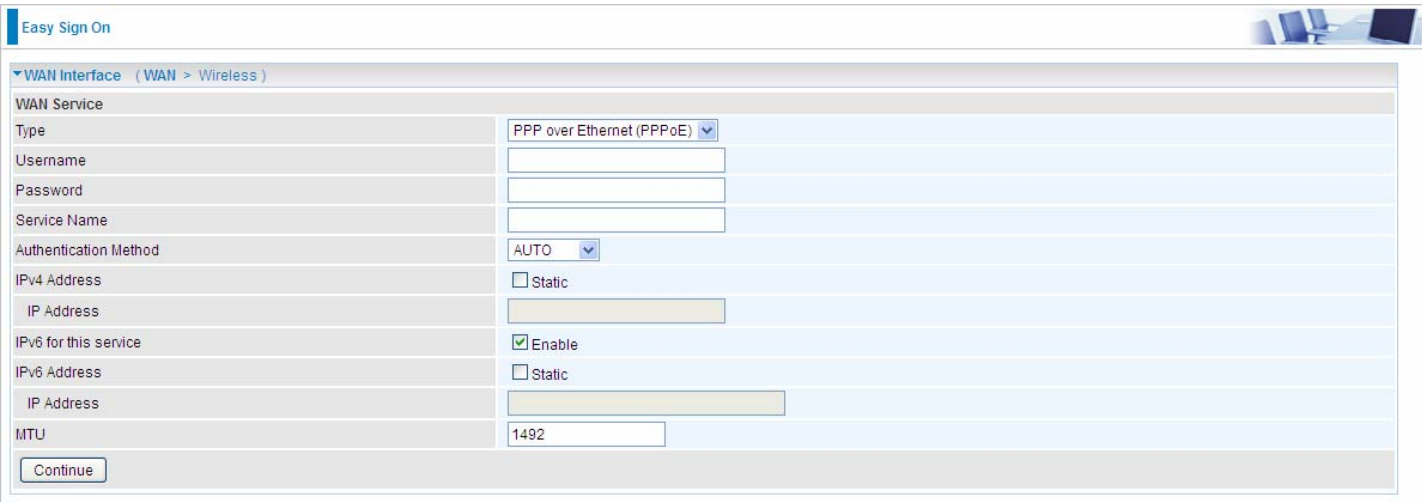
WAN Interface (WAN > Wireless)

Select WAN Interface

Main Port Ethernet (Current Main Port: DSL)

Continue Done

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 1492

Continue

3. Wait while the device is configured.

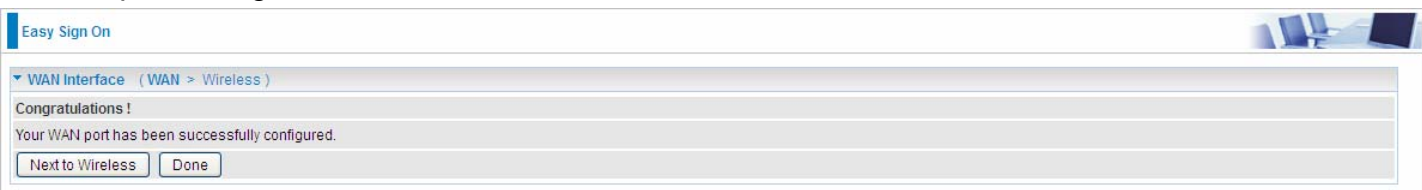


Easy Sign On

WAN Interface (WAN > Wireless)

Please wait while the device is configured.

4. WAN port configuration is success.



Easy Sign On

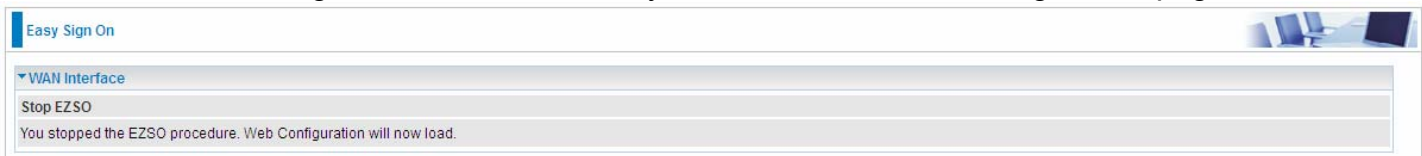
WAN Interface (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless Done

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



Easy Sign On

WAN Interface

Stop EZSO

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

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 8920AX(L) supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

Easy Sign On

Wireless (WAN > Wireless)

Parameters

Band	5GHz (wl0)
Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap-5g
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Easy Sign On

Wireless (WAN > Wireless)

Please wait while the device is configured.

6. Continue to set 2.4GHz wireless.

Easy Sign On

Wireless (WAN > Wireless)

Parameters

Band	2.4GHz (wl1)
Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap-2.4g
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Easy Sign On

Wireless (WAN > Wireless)

Please wait while the device is configured.

7. Success in configuring the EZSO.

Easy Sign On

Process finished

Success.


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

You can now:

1. Log onto the router management interface for more advanced settings on [192.168.1.254](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 VDSL2+ Router!**

Once you have logged on to your BiPAC 8920AX(L) Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Status** (Summary, WAN, Statistics, Bandwidth Usage, Route, ARP, DHCP, Log,)
- **Quick Start** (Quick Start)
- **Configuration** (LAN, Wireless 2.4G(wl0), Wireless 5G(wl1), WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)
- **VPN** (IPSec, VPN Account, Exceptional Rule Group, PPTP, L2TP, GRE)
- **Advanced Setup** (Routing, DNS, Static ARP, UPnP, Certificate, Multicast, Management, Diagnostics)

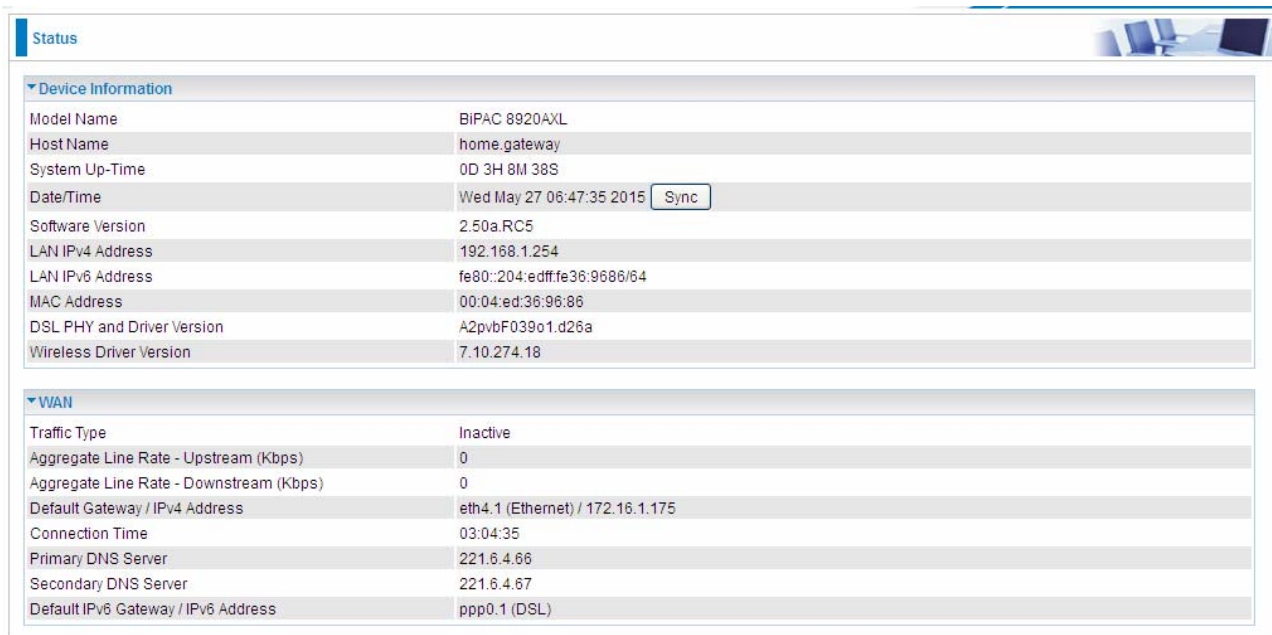
# Status

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](#), [Route](#), [ARP](#), [DHCP](#), and [Log](#) subsections are included.

▼ Status
▪ Summary
▪ WAN
▶ Statistics
▶ Bandwidth Usage
▪ 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 the 'Status' page of a router. It is divided into two main sections: 'Device Information' and 'WAN'. The 'Device Information' section lists various system details, and the 'WAN' section shows network connection status and settings.

Device Information	
Model Name	BIPAC 8920AXL
Host Name	home.gateway
System Up-Time	0D 3H 8M 38S
Date/Time	Wed May 27 06:47:35 2015 <input type="button" value="Sync"/>
Software Version	2.50a.RC5
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	fe80::204:edff:fe36:9686/64
MAC Address	00:04:ed:36:96:86
DSL PHY and Driver Version	A2pvbF039o1.d26a
Wireless Driver Version	7.10.274.18

WAN	
Traffic Type	Inactive
Aggregate Line Rate - Upstream (Kbps)	0
Aggregate Line Rate - Downstream (Kbps)	0
Default Gateway / IPv4 Address	eth4.1 (Ethernet) / 172.16.1.175
Connection Time	03:04:35
Primary DNS Server	221.6.4.66
Secondary DNS Server	221.6.4.67
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL)

## Device Information

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

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

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

**Date/Time:** Displays the current exact date and time. 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.

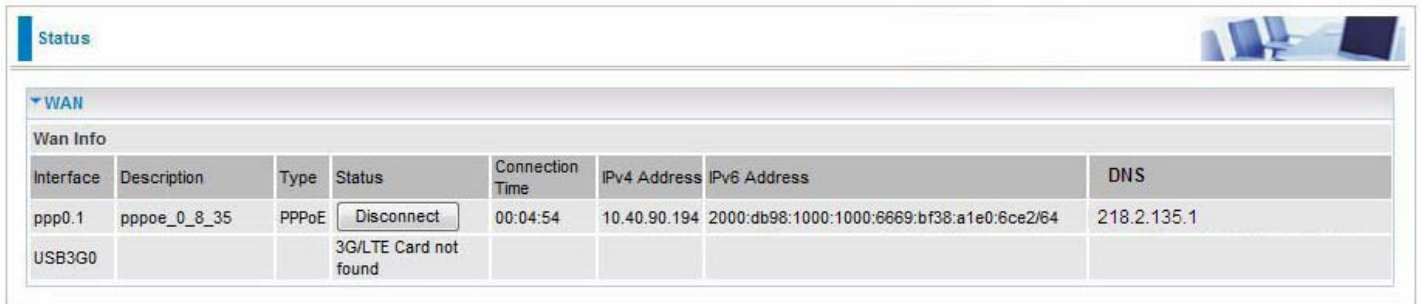
**Secondary DNS Server:** Displays IPV4 address of Secondary DNS Server.

**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	<input type="button" value="Disconnect"/>	00:04:54	10.40.90.194	2000:db98:1000:1000:8669:bf38:a1e0:6ce2/64	218.2.135.1
USB3G0			3G/LTE Card not found				

**Interface:** The WAN connection interface.

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

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

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

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

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

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

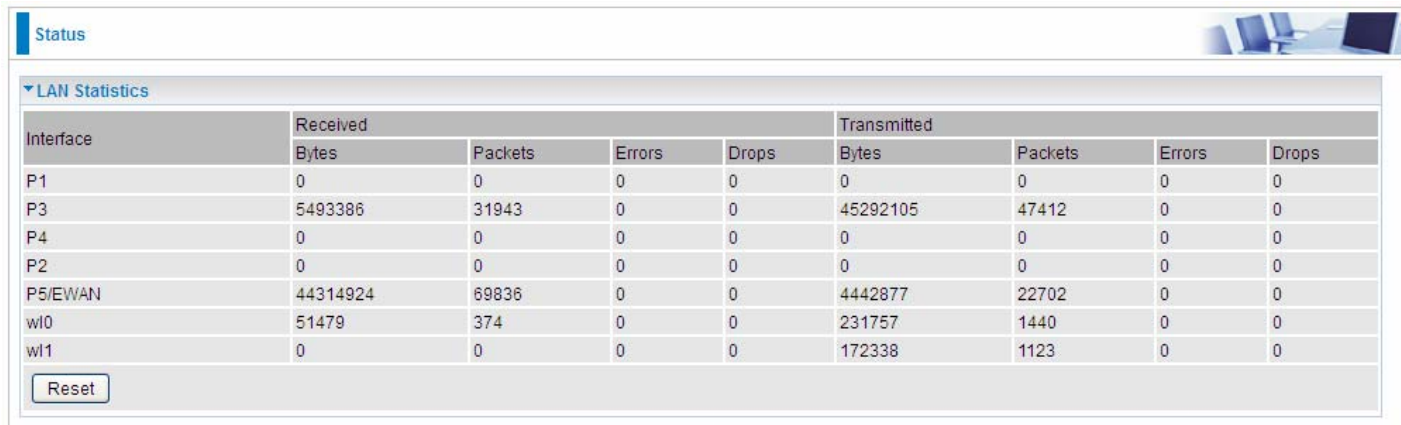
**DNS:** The DNS address the device obtained.

# Statistics

## LAN

The table shows the statistics of LAN.

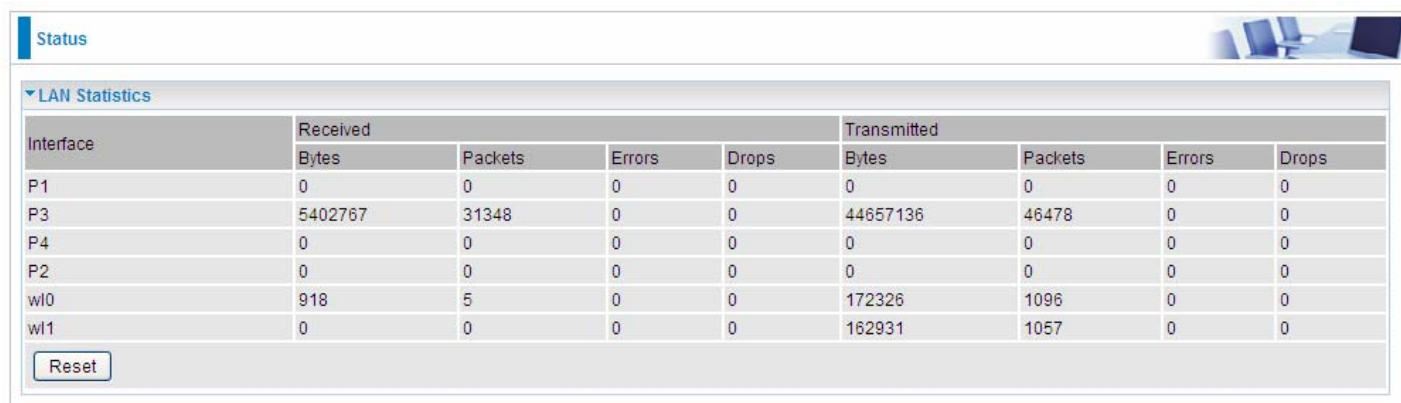
**Note:** P5 can be configured as EWAN, and when the device is in EWAN profile, there is no P5/EWAN interface as P5 is working as a WAN port.



The screenshot shows a web interface with a 'Status' tab and a 'LAN Statistics' section. The table below displays the statistics for various LAN interfaces. A 'Reset' button is located at the bottom left of the table.

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P1	0	0	0	0	0	0	0	0
P3	5493386	31943	0	0	45292105	47412	0	0
P4	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0
P5/EWAN	44314924	69836	0	0	4442877	22702	0	0
wl0	51479	374	0	0	231757	1440	0	0
wl1	0	0	0	0	172338	1123	0	0

(DSL)



The screenshot shows a web interface with a 'Status' tab and a 'LAN Statistics' section. The table below displays the statistics for various LAN interfaces. A 'Reset' button is located at the bottom left of the table.

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
P1	0	0	0	0	0	0	0	0
P3	5402767	31348	0	0	44657136	46478	0	0
P4	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0
wl0	918	5	0	0	172326	1096	0	0
wl1	0	0	0	0	162931	1057	0	0

(EWAN)

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

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

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

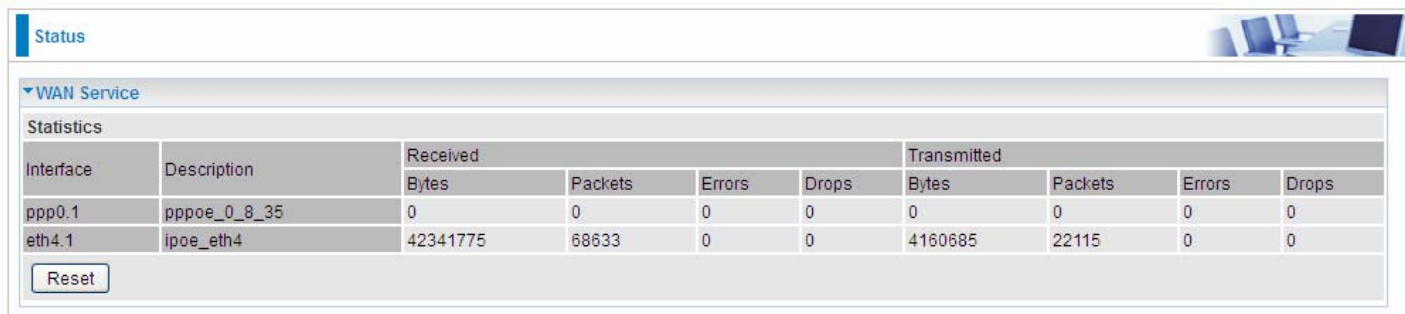
**Errors:** Display the statistics of errors arising in Receiving or Transmitting data.

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

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

## WAN Service

The table shows the statistics of WAN.



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', 'Description', 'Received' (Bytes, Packets, Errors, Drops), and 'Transmitted' (Bytes, Packets, Errors, Drops). There are two rows of data: one for 'ppp0.1' and one for 'eth4.1'. A 'Reset' button is located below the table.

Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
ppp0.1	pppoe_0_8_35	0	0	0	0	0	0	0	0
eth4.1	ipoe_eth4	42341775	68633	0	0	4160685	22115	0	0

**Interface:** Display the connection interface.

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

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

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

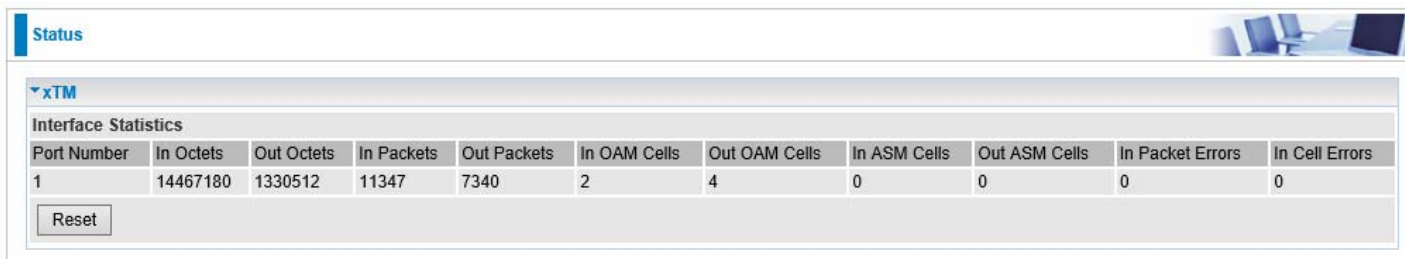
**Errors:** Display the statistics of errors arising in Receiving or Transmitting data.

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

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

## xTM

The Statistics-xTM screen displays all the xTM statistics



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'. There is one row of data for 'Port Number' 1. 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

Bonding Line Selection	line 0 ▼	
Mode	ADSL_2plus	
Traffic Type	ATM	
Status	Up	
Link Power State	L0	

	Downstream	Upstream
Line Coding (Trellis)	On	On
SNR Margin (dB)	7.2	7.2
Attenuation (dB)	0.0	1.3
Output Power (dBm)	7.2	9.3
Attainable Rate (Kbps)	28388	1335
Rate (Kbps)	27447	1299

MSGc (# of bytes in overhead channel message)	51	27
B (# of bytes in Mux Data Frame)	244	81
M (# of Mux Data Frames in FEC Data Frame)	1	1
T (Mux Data Frames over sync bytes)	4	1
R (# of check bytes in FEC Data Frame)	0	0
S (ratio of FEC over PMD Data Frame length)	0.2853	1.9939
L (# of bits in PMD Data Frame)	6869	329
D (interleaver depth)	1	1
Delay (msec)	0.7	0.49
INP (DMT symbol)	0.0	0.0
Super Frames	0	0
Super Frame Errors	0	0
RS Words	0	3255787
RS Correctable Errors	0	0
RS Uncorrectable Errors	0	0
HEC Errors	0	0
OCD Errors	0	0
LCD Errors	0	0
Total Cells	246668876	11669357
Data Cells	174531	18211
Bit Errors	0	0
Total ES	0	0
Total SES	0	0
Total UAS	25	25

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**ADSL BER Test -- Start**

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

Tested Time (sec)

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

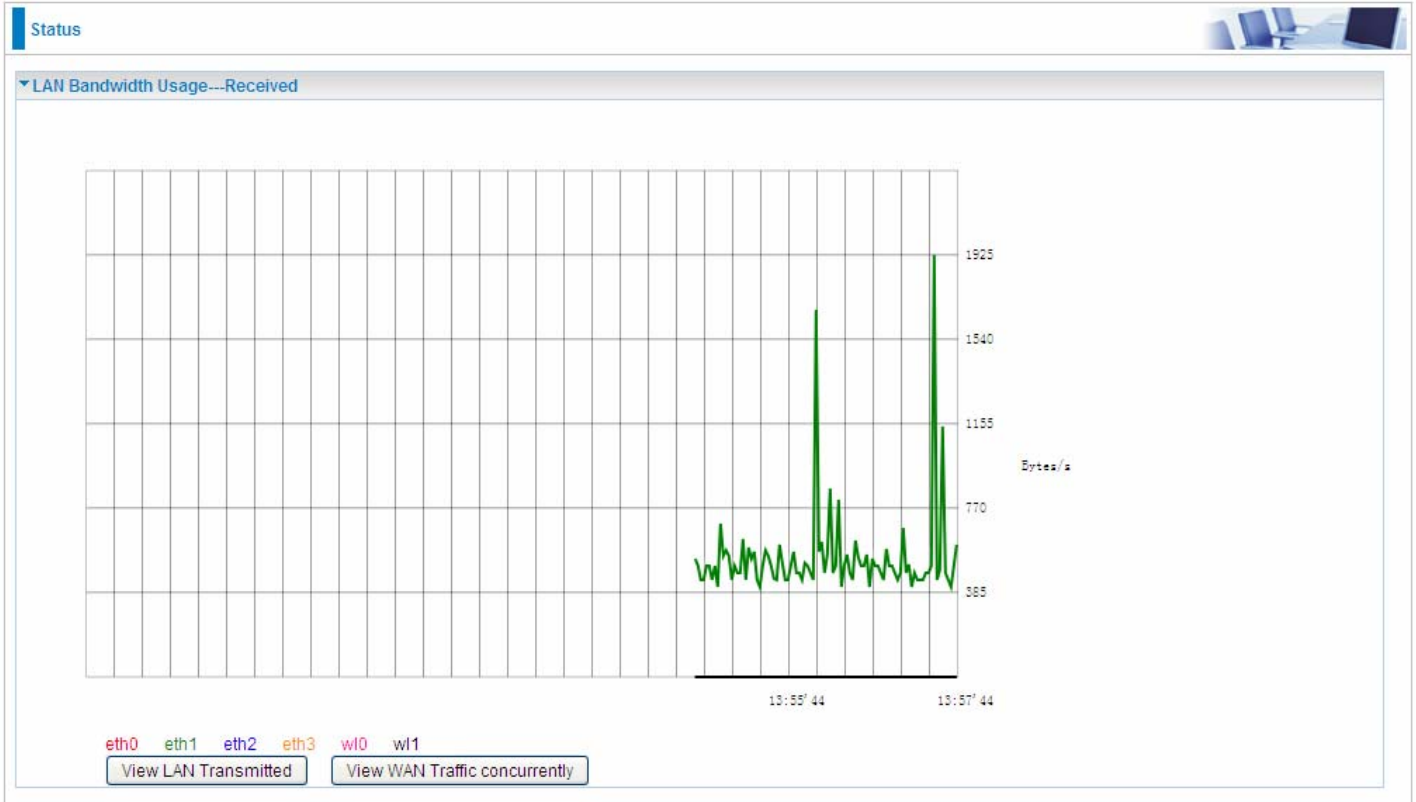
**Reset:** Click this button to reset the statistics.

# 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

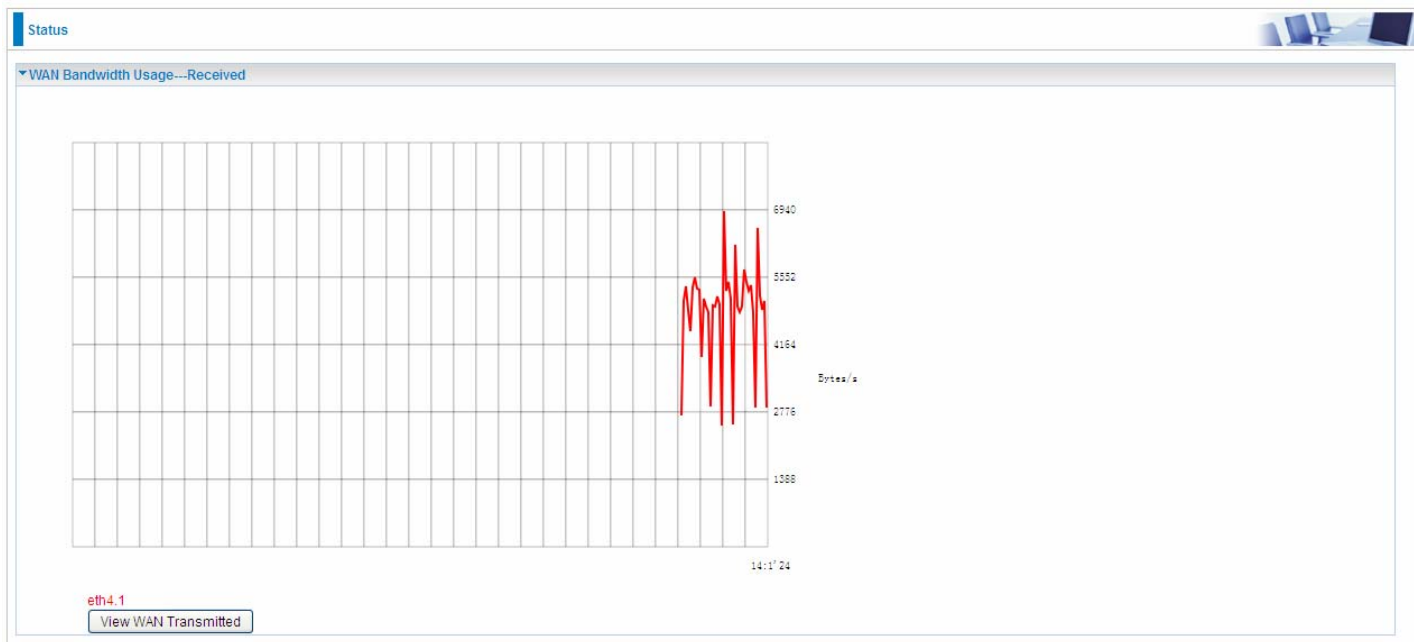
**Note:** P5 can be configured as EWAN, and when the device is in EWAN profile, there is no P5/EWAN interface as P5 is working as a WAN port.



(EWAN)

Press **View LAN Transmitted** button to change the diagram to the statistics from a Received Bytes of view. (**Note:** eth1 means Ethernet port #1, and the traffic information of the port #1 is identified with green, the same color with eth1 in the diagram; other ports all take the same mechanism.)

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





## WAN Service




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

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



# Route

Status 

▼ Route

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

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

**Destination:** The IP address of destination network.

**Gateway:** The IP address of the gateway this route uses.

**Subnet Mask:** The destination subnet mask.

**Flag:** Show the status of the route.

- ① **U:** Show the route is activated or enabled.
- ① **H (host):** destination is host not the subnet.
- ① **G:** Show that the outside gateway is needed to forward packets in this route.
- ① **R:** Show that the route is reinstated from dynamic routing.
- ① **D:** Show that the route is dynamically installed by daemon or redirecting.
- ① **M:** Show the route is modified from routing daemon or redirect.

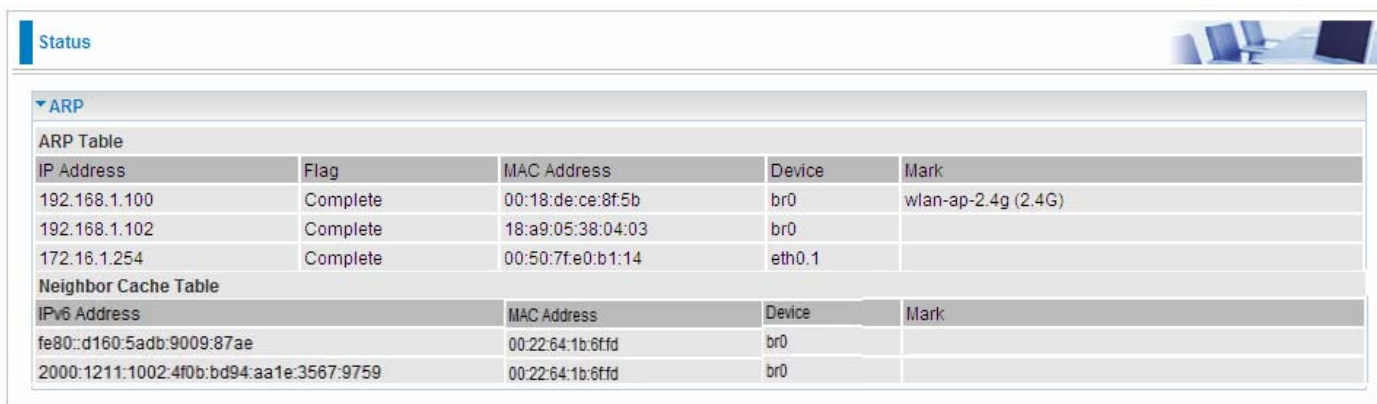
**Metric:** Display the number of hops counted as the Metric of the route.

**Service:** Display the service that this route uses.

**Interface:** Display the existing interface this route uses.

# ARP

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



The screenshot shows a network management 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.

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

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

## ARP table

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

**Flag:** Shows the current status of the ARP entries.

- ① Complete: the route resolving is processing well.
- ① M(Marked as permanent entry): the route is permanent.
- ① P (publish entry): publish this route item.

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

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

**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.



The screenshot shows a web-based interface with a 'Status' tab selected. Underneath, there is a 'DHCP' section with a 'Leased Table' table. The table has five columns: Host Name, MAC Address, IP Address, Expires In, and Mark. Two rows of data are visible.

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.

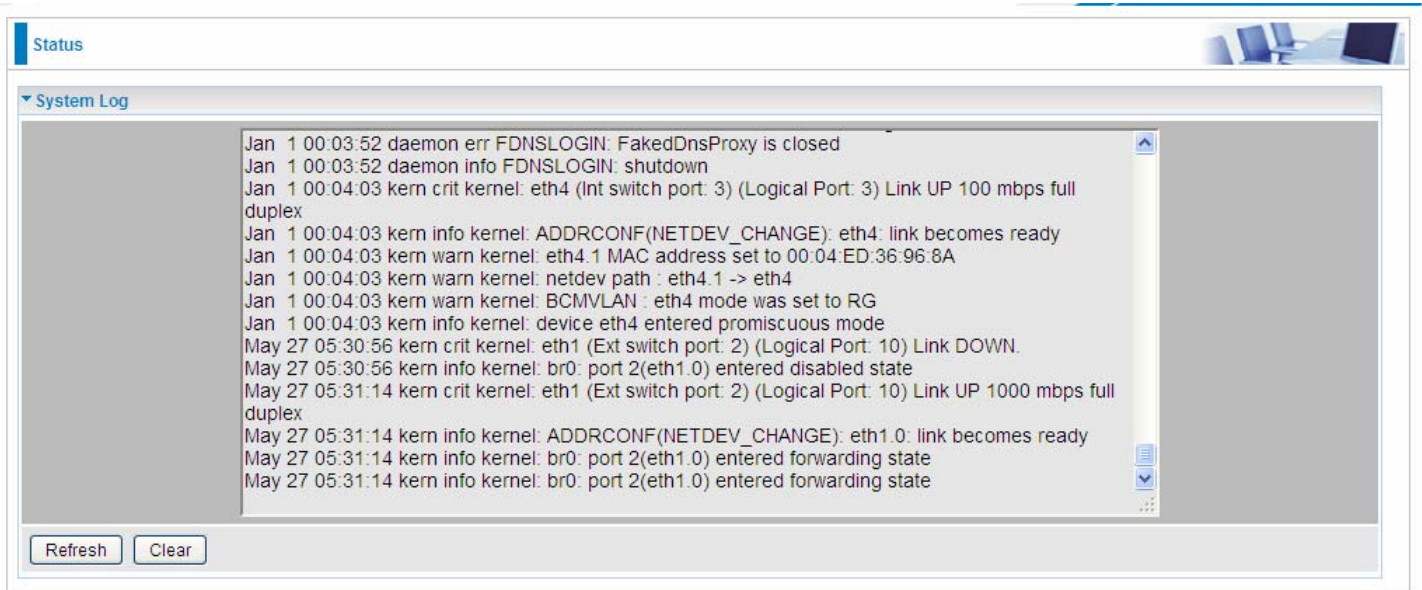
**Expires in:** Show the remaining time after registration.

**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. The entries include timestamps, severity levels, and messages related to network interface changes and daemon status. At the bottom of the log list, there are two buttons: 'Refresh' and 'Clear'.

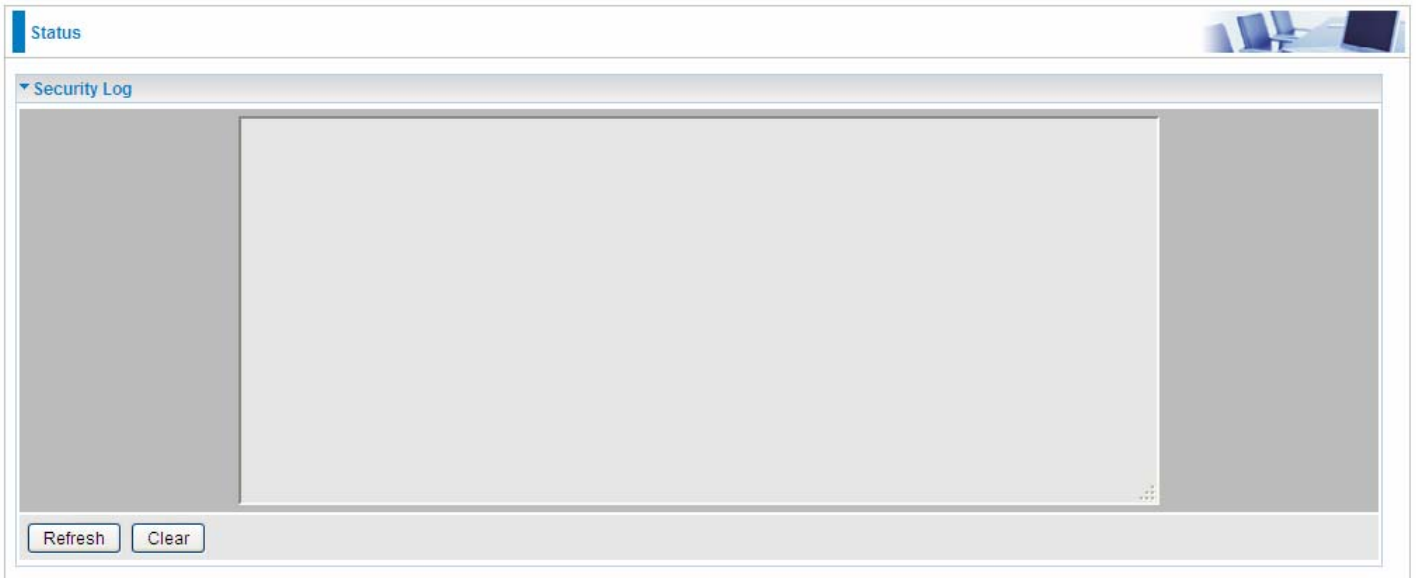
```
Jan 1 00:03:52 daemon err FDNSLOGIN: FakedDnsProxy is closed
Jan 1 00:03:52 daemon info FDNSLOGIN: shutdown
Jan 1 00:04:03 kern crit kernel: eth4 (Int switch port: 3) (Logical Port: 3) Link UP 100 mbps full duplex
Jan 1 00:04:03 kern info kernel: ADDRCONF(NETDEV_CHANGE): eth4: link becomes ready
Jan 1 00:04:03 kern warn kernel: eth4.1 MAC address set to 00:04:ED:36:96:8A
Jan 1 00:04:03 kern warn kernel: netdev path : eth4.1 -> eth4
Jan 1 00:04:03 kern warn kernel: BCMVLAN : eth4 mode was set to RG
Jan 1 00:04:03 kern info kernel: device eth4 entered promiscuous mode
May 27 05:30:56 kern crit kernel: eth1 (Ext switch port: 2) (Logical Port: 10) Link DOWN.
May 27 05:30:56 kern info kernel: br0: port 2(eth1.0) entered disabled state
May 27 05:31:14 kern crit kernel: eth1 (Ext switch port: 2) (Logical Port: 10) Link UP 1000 mbps full duplex
May 27 05:31:14 kern info kernel: ADDRCONF(NETDEV_CHANGE): eth1.0: link becomes ready
May 27 05:31:14 kern info kernel: br0: port 2(eth1.0) entered forwarding state
May 27 05:31:14 kern info kernel: br0: port 2(eth1.0) entered forwarding state
```

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

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

## Security Log

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



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

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

# Quick Start

## Quick Start

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

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

Here take ADSL for example.

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	8/35
Type	PPPoE
Username	username
WAN IP Address	Obtain an IP Address Automatically
<input type="button" value="Continue"/>	

Select DSL, press **Continue** to go on to next step. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.

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

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

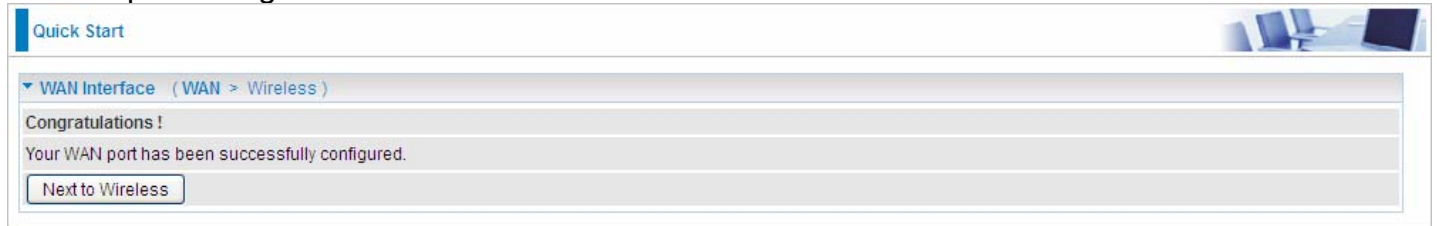
WAN Interface (WAN > Wireless)	
DSL Line Is Not Ready. Please Check your DSL Line and wait for a while.	



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



### 4. WAN port configuration is successful.



5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. The 8920AX(L) supports dual-band wireless, here you can set to activate wireless on which band or both and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).



### 6. Continue to set 2.4GHz wireless.



### 7. Success.



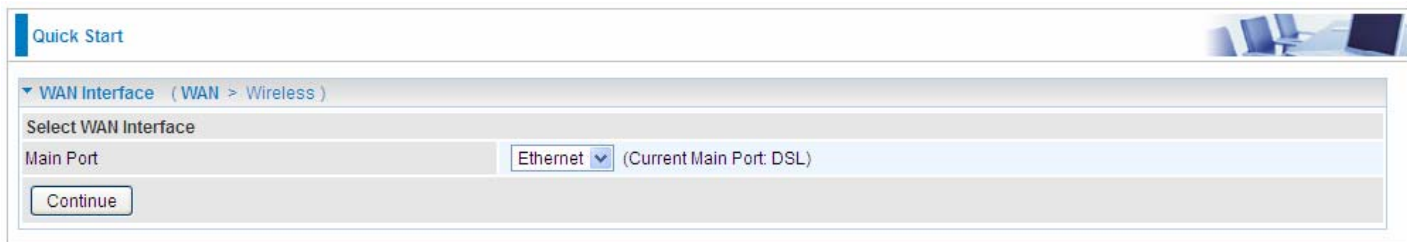
▼ Process finished

Success.

Go back to **Status > Summary** for more information.

## Ethernet mode

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



Quick Start

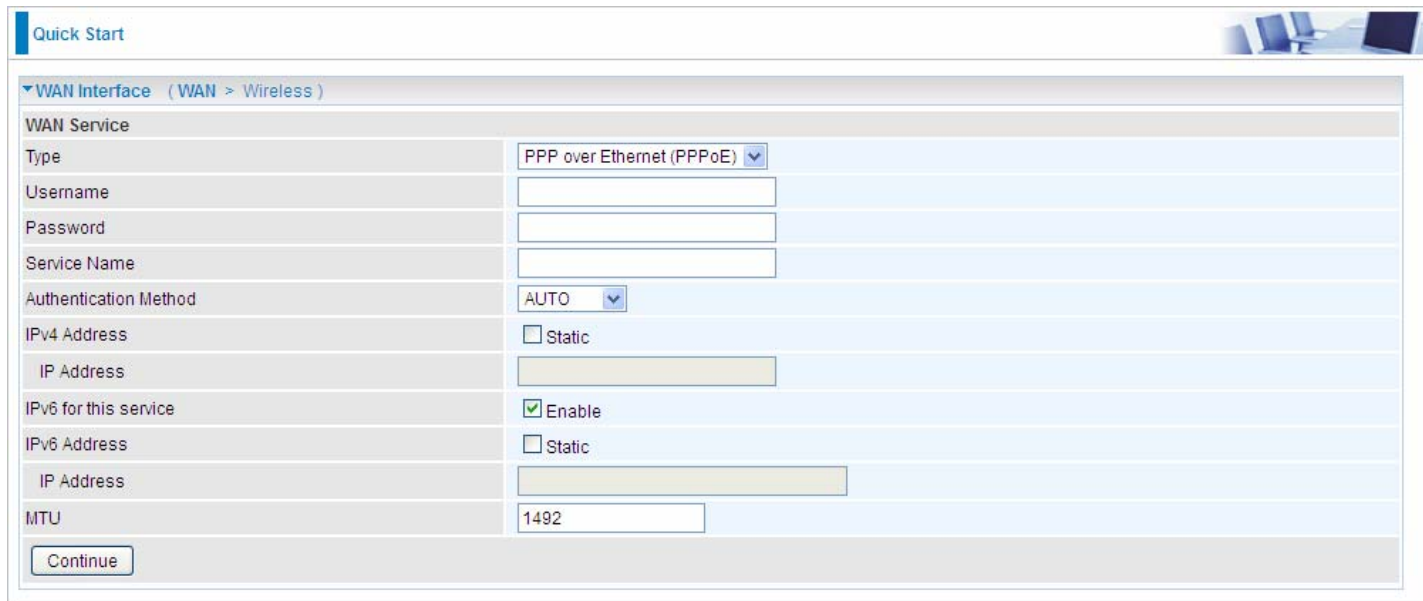
WAN Interface (WAN > Wireless)

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 input]

Password: [text input]

Service Name: [text input]

Authentication Method: AUTO

IPv4 Address:  Static

IP Address: [text input]

IPv6 for this service:  Enable

IPv6 Address:  Static

IP Address: [text input]

MTU: 1492

Continue

3. Wait while the device is configured.

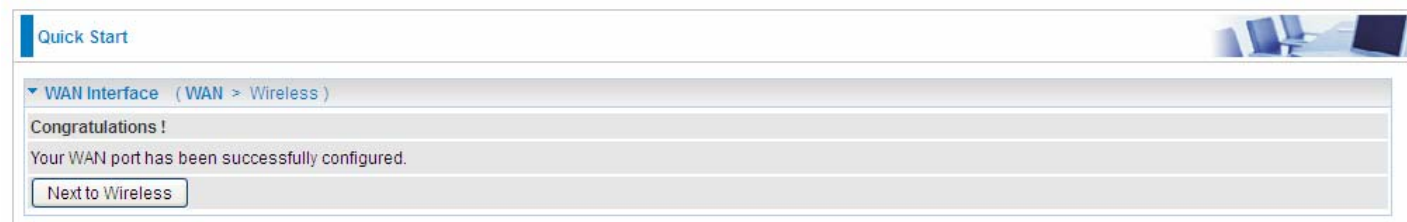


Quick Start

WAN Interface (WAN > Wireless)

Please wait while the device is configured.

4. WAN port configuration is successful.



Quick Start

WAN Interface (WAN > Wireless)

Congratulations!

Your WAN port has been successfully configured.

Next to Wireless

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

Quick Start

Wireless ( WAN > Wireless )

Parameters	
Band	5GHz (wl0)
Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap-5g
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Continue

Quick Start

Wireless ( WAN > Wireless )

Please wait while the device is configured.

6. Continue to set 2.4GHz wireless.

Quick Start

Wireless ( WAN > Wireless )

Parameters	
Band	2.4GHz (wl1)
Wireless	<input checked="" type="checkbox"/> Enable
SSID	wlan-ap-2.4g
WPA2 Pre-Shared Key	<input type="text"/> <a href="#">Click here to display</a>

Continue

Quick Start

Wireless ( WAN > Wireless )

Please wait while the device is configured.

7. Success.

Quick Start

Process finished

Success.

Go back to **Status > Summary** for more information

# Configuration

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

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

▶ Status
• Quick Start
▼ Configuration
▶ LAN
▶ Wireless 2.4G (wl0)
▶ Wireless 5G (wl1)
▶ 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 network configuration page titled "Configuration" with a sub-section for "LAN". The "Parameters" section includes:

- Group Name: Default (dropdown)
- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0
- IGMP Snooping:  Enable
- IGMP Snooping Mode:  Standard Mode  Blocking Mode
- IGMP LAN to LAN Multicast:  Enable (LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)
- LAN side firewall:  Enable

The "DHCP Server" section includes:

- DHCP Server: Enable (dropdown)
- Start IP Address: 192.168.1.100
- End IP Address: 192.168.1.199
- Leased Time (hour): 24
- Option 66:  Enable
- Use Router's setting as DNS Server:
- Primary DNS server: (empty text box)
- Secondary DNS server: (empty text box)

The "Static IP Lease List" section is a table with columns: Host Label, MAC Address, IP Address, Remove, and Edit. An "Add" button is located below the table.

The "IP Alias" section includes:

- IP Alias:  Enable
- IP Address: (empty text box)
- Subnet Mask: (empty text box)

At the bottom, there are "Apply" and "Cancel" buttons.

## Parameters

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

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

**Subnet Mask:** the default Subnet mask on the router.

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

When enabled, you will see two modes:

- ① **Standard Mode:** In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.
- ① **Blocking Mode:** In blocking mode, the multicast data will be blocked when there are no client subscribes to a multicast group, it won't flood to the bridge ports.

**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.

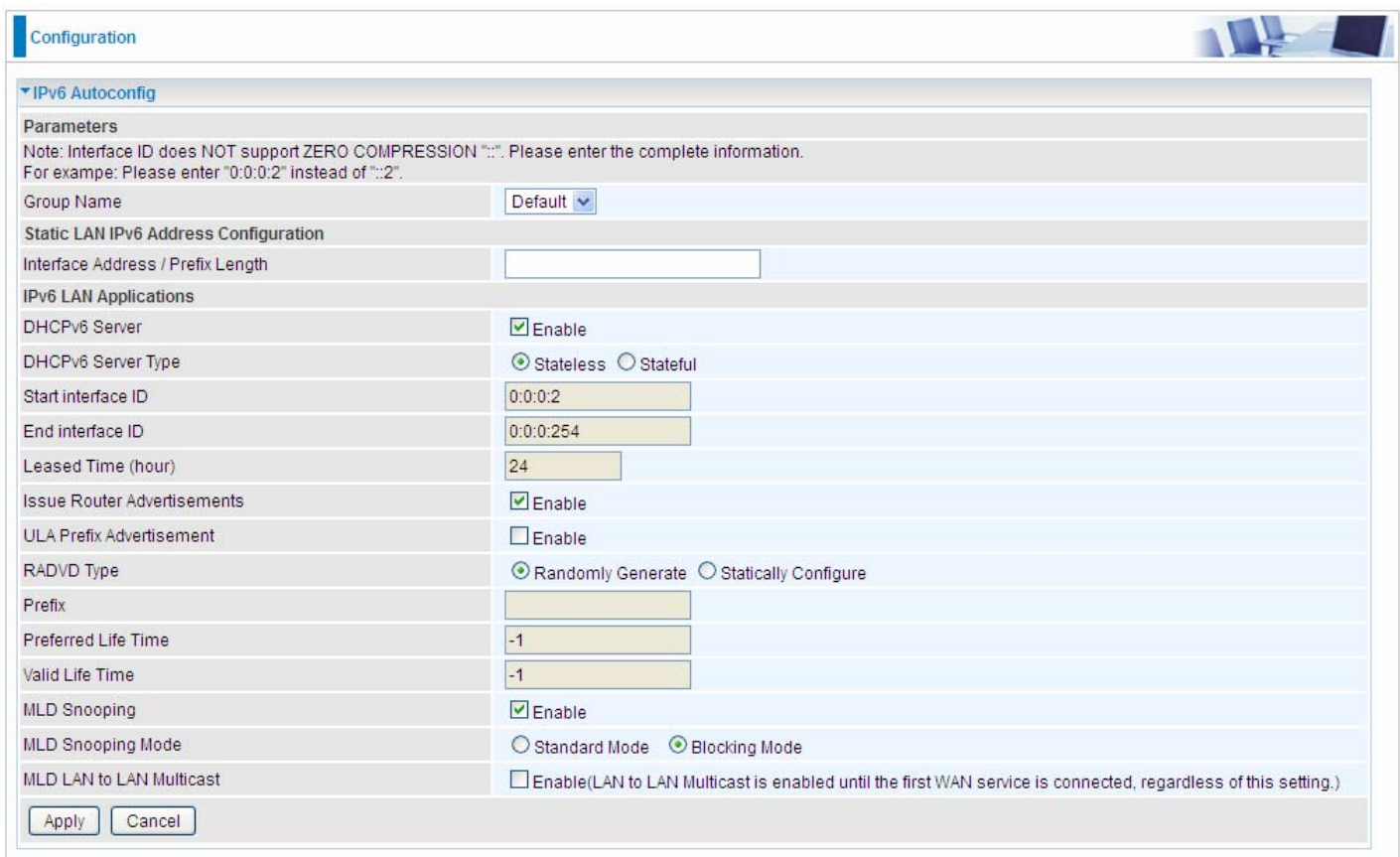


## IPv6 Autoconfig

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: "DHCPv6 Server" (checked), "DHCPv6 Server Type" (radio buttons for Stateless and Stateful), "Start interface ID" (0:0:0:2), "End interface ID" (0:0:0:254), "Leased Time (hour)" (24), "Issue Router Advertisements" (checked), "ULA Prefix Advertisement" (unchecked), "RADVD Type" (radio buttons for Randomly Generate and Statically Configure), "Prefix" (empty), "Preferred Life Time" (-1), "Valid Life Time" (-1), "MLD Snooping" (checked), "MLD Snooping Mode" (radio buttons for Standard Mode and Blocking Mode), and "MLD LAN to LAN Multicast" (unchecked with a note). At the bottom 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

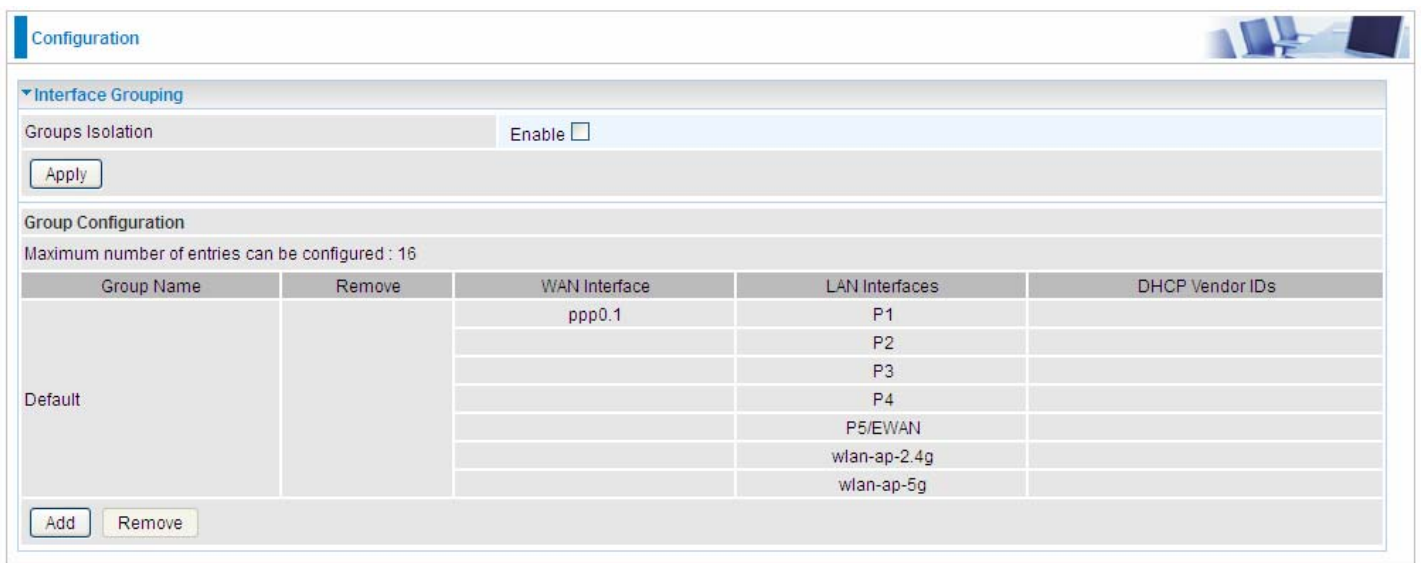
With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

## 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

Apply

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	
			P5/EWAN	
			wlan-ap-2.4g	
			wlan-ap-5g	

Add Remove

**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  
P5/EWAN  
wlan-ap-2.4g  
wlan-ap-5g

Automatically Add Clients With the following DHCP Vendor IDs

**Group Name:** Type a group name.

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

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

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

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

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

Configuration

Interface Grouping

Groups Isolation Enable

Apply

Group Configuration

Maximum number of entries can be configured : 16

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default	<input type="checkbox"/>		P1	
			P3	
			P4	
			P5/EWAN	
			wlan-ap-2.4g	
			wlan-ap-5g	
test	<input checked="" type="checkbox"/>	ppp0.1	P2	

Add Remove

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

Configuration

Interface Grouping

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	
			P5/EWAN	
			wlan-ap-2.4g	
			wlan-ap-5g	
test	<input checked="" type="checkbox"/>	ppp0.1	P2	

Add Remove

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

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

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

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

## Wireless 5G(wl0) & 2.4G(Wl1)

BiPAC 8920AX(L) is a simultaneous dual-band (2.4G and 5G) wireless router support 11b/g/n/a/ac wireless standards. It allows multiple wireless users in 2.4G and 5G radio bands to surf the Internet, checking e-mail, watching video, listening to music over the Internet concurrently.

You can choose the optimum radio band wireless connection base on your environment.

▶ Status
• Quick Start
▼ Configuration
▶ LAN
▼ Wireless 5G (wl0)
• Basic
• Security
• MAC Filter
• Wireless Bridge
• Advanced
• Station Info
• Schedule Control
▶ Wireless 2.4G (wl1)
▶ WAN
▶ System
▶ USB
▶ IP Tunnel
▶ Security
▶ Quality of Service
▶ NAT
• Wake On LAN
▶ Advanced Setup



## Basic

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

Configuration

▼ Basic

Parameters

Wireless	<input checked="" type="checkbox"/> Enable
Hide SSID	<input type="checkbox"/> Enable
Clients Isolation	<input type="checkbox"/> Enable
Disable WMM Advertise	<input type="checkbox"/> Enable
Wireless Multicast Forwarding (WMF)	<input type="checkbox"/> Enable
SSID	wlan-ap-5g
BSSID	00:04:ED:36:96:87
Country	UNITED STATES
Country RegRev	0
Max Clients	16 [1-16]

Wireless - Guest/Virtual Access Points

SSID	Hidden	Clients Isolation	Disable WMM Advertise	WMF	Max Clients	BSSID	Enable
w10_Guest1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A	<input type="checkbox"/>
w10_Guest2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A	<input type="checkbox"/>
w10_Guest3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16	N/A	<input type="checkbox"/>

Apply Cancel

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

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

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

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

Check to disable or enable this function.

**Wireless multicast Forwarding (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-5g** to a unique ID name to the AP already built-in to the router's wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

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

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

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

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

**Guest/virtual Access Points:** A "Virtual Access Point" is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple "Virtual APs", each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID

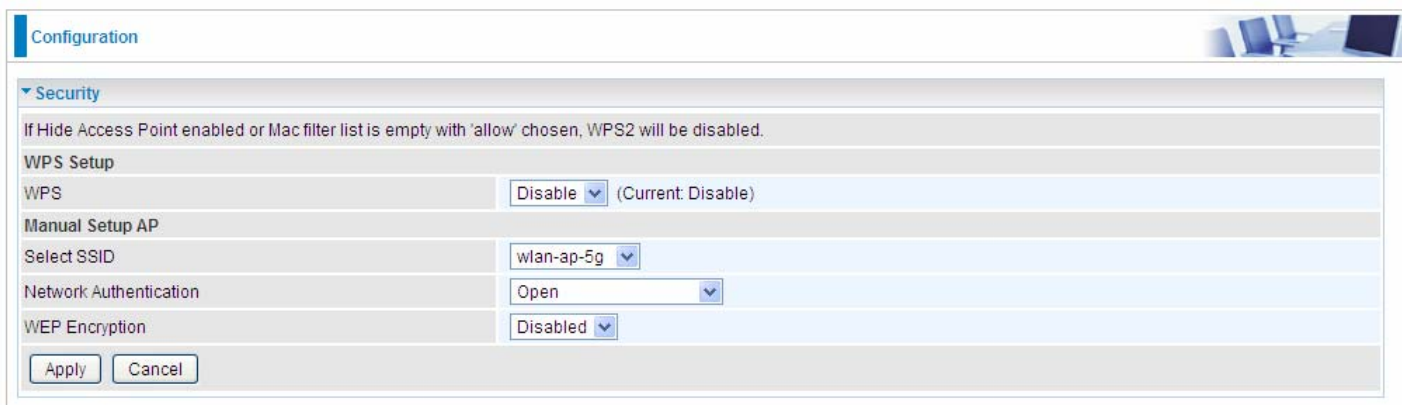
but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing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

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

Click **Apply** to apply your settings.

## Security

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



Configuration

**Security**

If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled.

**WPS Setup**

WPS: Disable (Current: Disable)

**Manual Setup AP**

Select SSID: wlan-ap-5g

Network Authentication: Open

WEP Encryption: Disabled

Apply Cancel

### Note:

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

## Manual Setup AP

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

### Network Authentication

#### ① Open

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

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

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

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

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

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

## ① Shared

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

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

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

## ① 802.1x

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

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

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

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

**RADIUS Key:** Enter the password of RADIUS authentication server.

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

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

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

## ① WPA

Network Authentication	<input type="text" value="WPA"/>
WPA Group Rekey Interval	<input type="text" value="3600"/> [0-2147483647]
RADIUS Server IP Address	<input type="text" value="0.0.0.0"/>
RADIUS Port	<input type="text" value="1812"/>
RADIUS Key	<input type="text"/>
WPA/WAPI Encryption	<input type="text" value="TKIP+AES"/>
WEP Encryption	<input type="text" value="Disabled"/>

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

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

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

**RADIUS Key:** Enter the password of RADIUS authentication server.

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

## ① WPA-PSK / WPA2-PSK

Network Authentication	<input type="text" value="WPA-PSK"/>
WPA/WAPI passphrase	<input type="text" value="••••••••"/> <a href="#">Click here to display</a>
WPA Group Rekey Interval	<input type="text" value="3600"/> [0-2147483647]
WPA/WAPI Encryption	<input type="text" value="TKIP+AES"/>
WEP Encryption	<input type="text" value="Disabled"/>

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

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

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

## ① WPA2

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

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

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

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

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

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

**RADIUS Key:** Enter the password of RADIUS authentication server.

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

## ① Mixed WPA2/WPA

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

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

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

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

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

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

**RADIUS Key:** Enter the password of RADIUS authentication server.

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

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

### ① Mixed WPA2/WPA-PSk

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

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

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

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

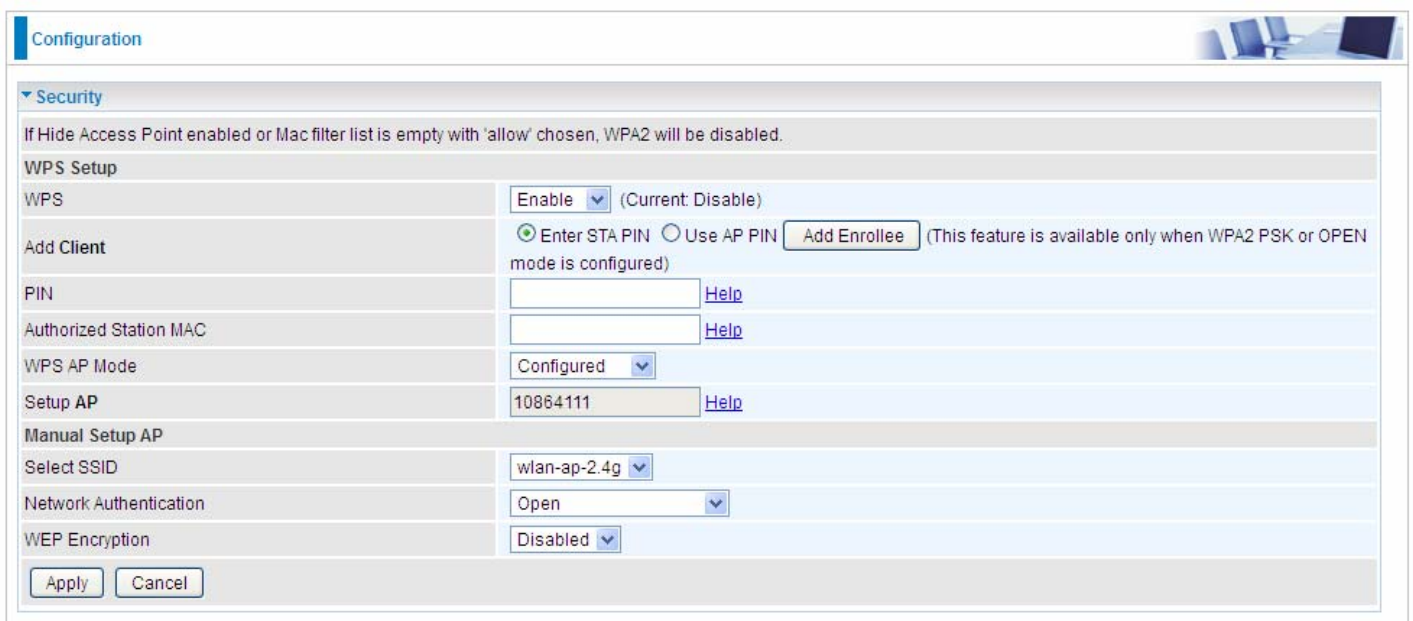
## WPS Setup

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

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

### Note:

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



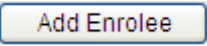
The screenshot shows a web-based configuration interface for WPS. At the top, there is a 'Configuration' tab and a small image of a laptop. Below the tab is a 'Security' section with a warning: 'If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.' The 'WPS Setup' section includes a 'WPS' dropdown set to 'Enable' (Current: Disable), an 'Add Client' section with radio buttons for 'Enter STA PIN' (selected) and 'Use AP PIN', and an 'Add Enrollee' button. Below these are input fields for 'PIN', 'Authorized Station MAC', and 'Setup AP' (10864111), each with a 'Help' link. The 'WPS AP Mode' dropdown is set to 'Configured'. The 'Manual Setup AP' section includes 'Select SSID' (wlan-ap-2.4g), 'Network Authentication' (Open), and 'WEP Encryption' (Disabled). At the bottom are 'Apply' and 'Cancel' buttons.

Configuration	
Security	
If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled.	
WPS Setup	
WPS	Enable (Current: Disable)
Add Client	<input checked="" type="radio"/> Enter STA PIN <input type="radio"/> Use AP PIN <input type="button" value="Add Enrollee"/> (This feature is available only when WPA2 PSK or OPEN mode is configured)
PIN	<input type="text"/> <a href="#">Help</a>
Authorized Station MAC	<input type="text"/> <a href="#">Help</a>
WPS AP Mode	Configured
Setup AP	10864111 <a href="#">Help</a>
Manual Setup AP	
Select SSID	wlan-ap-2.4g
Network Authentication	Open
WEP Encryption	Disabled
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	



## Configure AP as Registrar

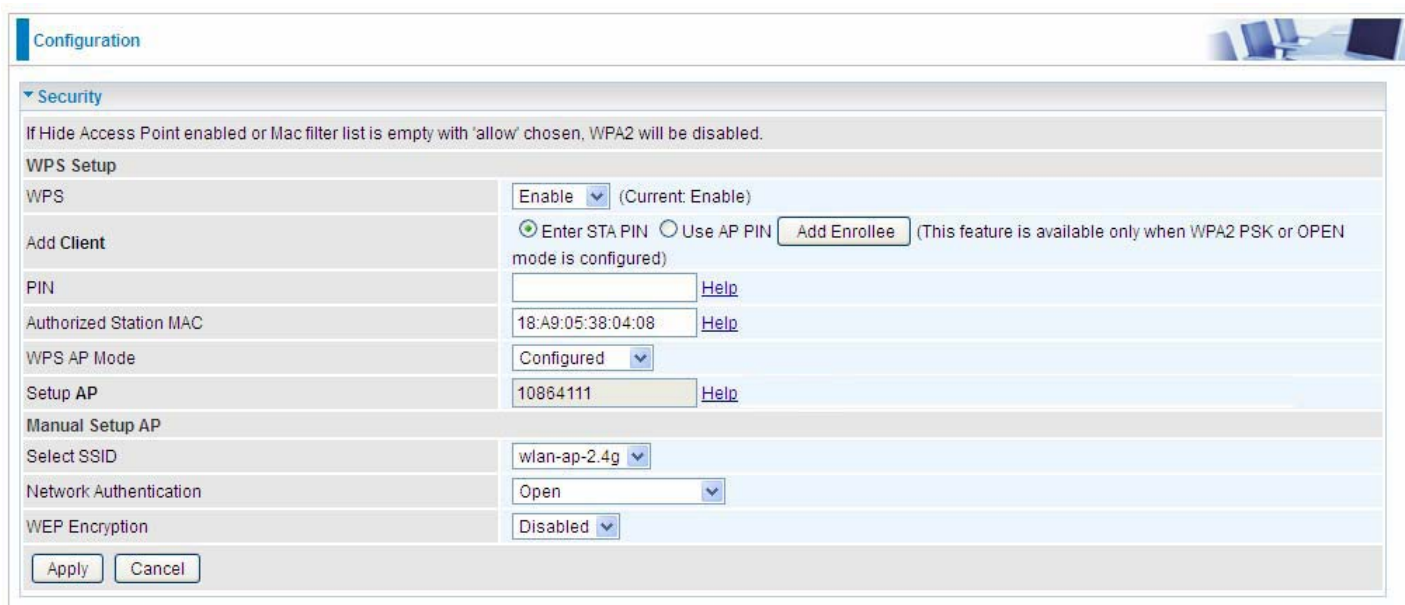
### ● Add Enrollee with PIN method

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



The screenshot shows the 'Configuration' page for an Access Point, specifically the 'Security' section. Under 'WPS Setup', the 'WPS' dropdown is set to 'Enable' (Current: Disable). The 'Add Client' section has two radio buttons: 'Enter STA PIN' (selected) and 'Use AP PIN'. An 'Add Enrollee' button is visible next to the 'Use AP PIN' option. The 'PIN' field contains the value '16837546'. The 'Authorized Station MAC' field is empty. The 'WPS AP Mode' is set to 'Configured'. The 'Setup AP' field contains '10864111'. The 'Manual Setup AP' section includes 'Select SSID' (wlan-ap-2.4g), 'Network Authentication' (Open), and 'WEP Encryption' (Disabled). 'Apply' and 'Cancel' buttons are at the bottom.

(Station PIN)



The screenshot shows the same 'Configuration' page, but with the 'Use AP PIN' radio button selected. The 'Add Enrollee' button is now highlighted. The 'PIN' field is empty. The 'Authorized Station MAC' field contains the value '18:A9:05:38:04:08'. 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-2.4g) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

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-01-00-02	1
	wlan-ap-2.4g	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
- Buttons:** PIN, PBC, 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, SNR0 >> n/a, GI >> n/a, MCS >> n/a, SNR1 >> n/a

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

The screenshot displays a network management interface with several sections:

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

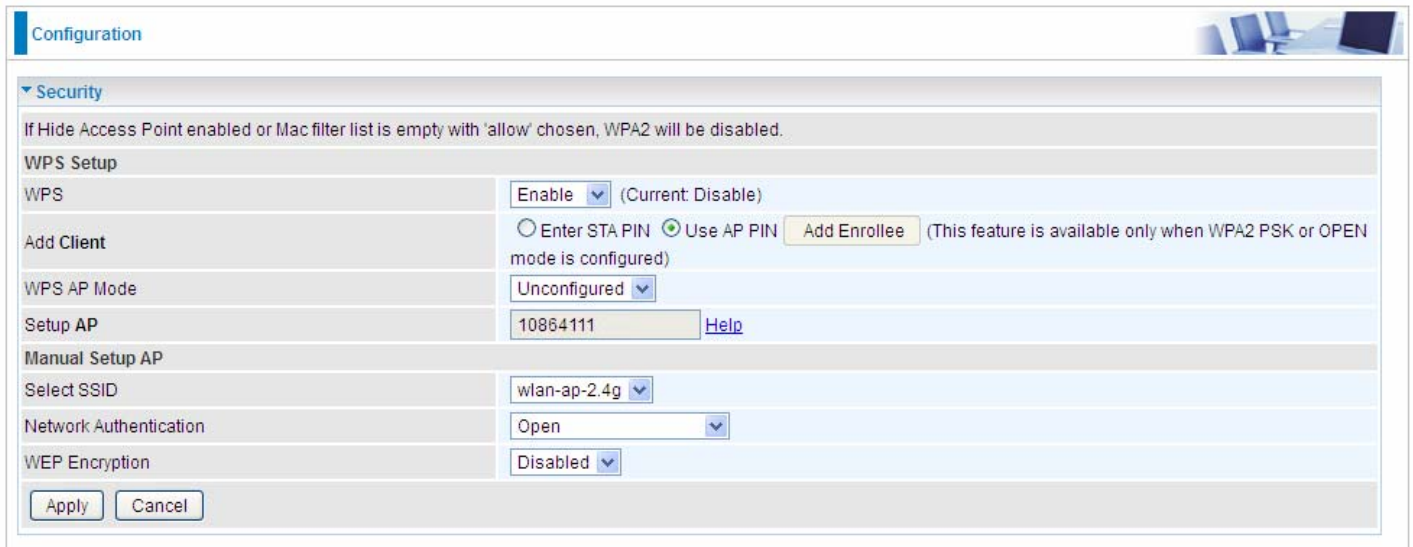
ID :	wlan-ap-2.4g	00-04-ED-01-00-01	1
ID :	wlan-ap	00-04-ED-38-F7-2E	1
- WPS Profile List:** wlan-ap
- WPS Configuration:**
  - WPS Associate IE
  - WPS Probe IE
  - Progress >> 100%
  - Message: PIN - Get WPS profile successfully.
- Right Panel:** Rescan, Information, Pin Code (16837546), Renew, Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
- Connection Status (Left):**
  - Status >> wlan-ap-2.4g <-> 00-04-ED-01-00-01
  - Extra Info >> Link is Up [TxPower:100%]
  - Channel >> 1 <-> 2412 MHz; central channel : 3
  - Authentication >> Open
  - Encryption >> NONE
  - Network Type >> Infrastructure
  - IP Address >> 192.168.1.1
  - Sub Mask >> 255.255.255.0
  - Default Gateway >> 192.168.1.254
- Connection Status (Right):**
  - Link Quality >> 100%
  - Signal Strength 1 >> 64%
  - Signal Strength 2 >> 34%
  - Noise Strength >> 26%
- Transmit/Receive Performance:**
  - Transmit: Link Speed >> 270.0 Mbps, Throughput >> 5.600 Kbps
  - Receive: Link Speed >> 54.0 Mbps, Throughput >> 81.608 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 a web-based configuration interface for an Access Point (AP). The page is titled "Configuration" and features a "Security" section. A warning message states: "If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPA2 will be disabled." The "WPS Setup" section includes the following fields:

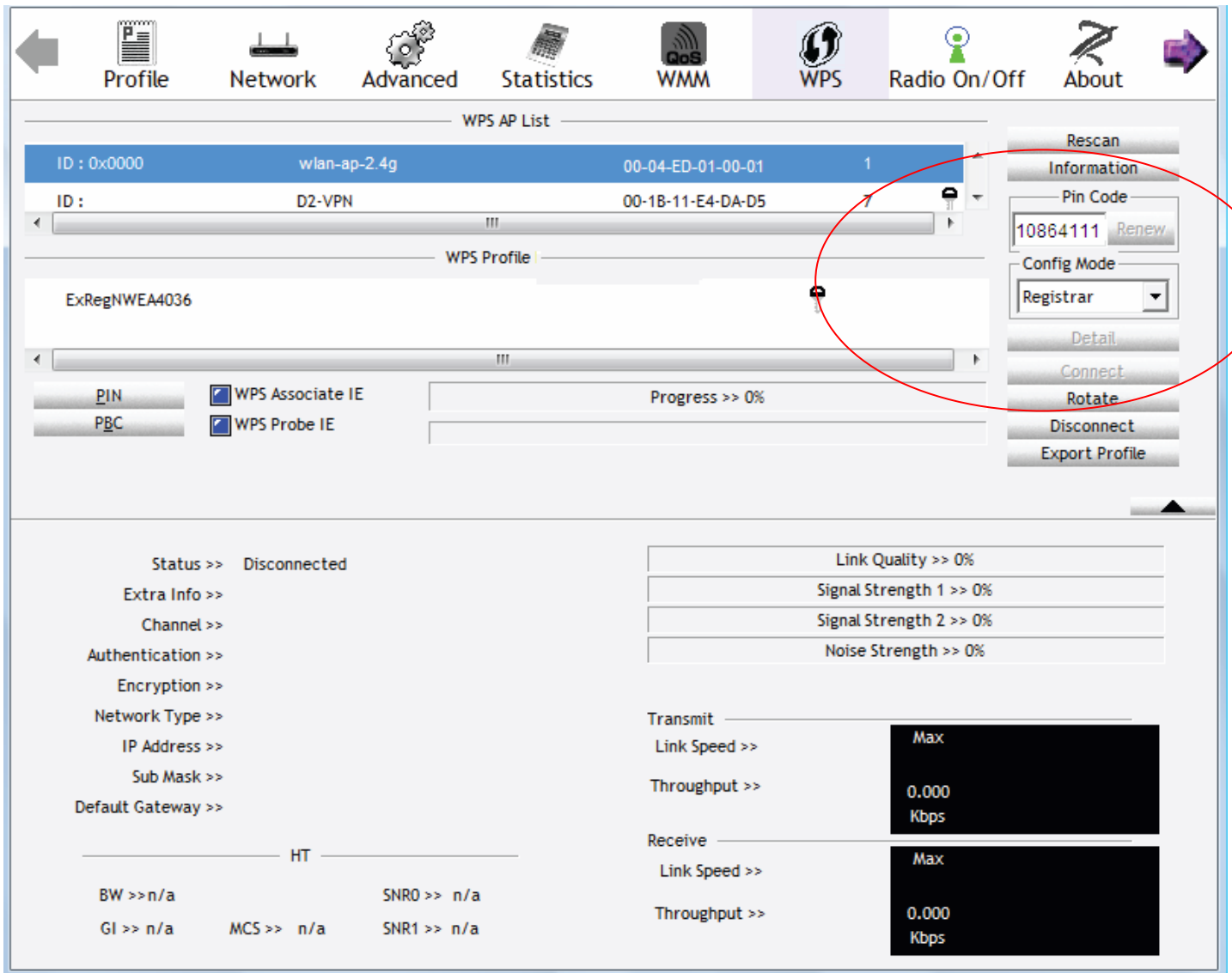
- WPS:** A dropdown menu set to "Enable" (Current: Disable).
- Add Client:** Radio buttons for "Enter STA PIN" (unselected) and "Use AP PIN" (selected). An "Add Enrollee" button is present. A note indicates: "(This feature is available only when WPA2 PSK or OPEN mode is configured)".
- WPS AP Mode:** A dropdown menu set to "Unconfigured".
- Setup AP:** A text input field containing "10864111" and a "Help" link.

The "Manual Setup AP" section includes:

- Select SSID:** A dropdown menu set to "wlan-ap-2.4g".
- Network Authentication:** A dropdown menu set to "Open".
- WEP Encryption:** A dropdown menu set to "Disabled".

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

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-2.4g) 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, navigation tabs include Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The WPS section is active, showing a 'WPS AP List' with two entries: 'wlan-ap-2.4g' (MAC: 00-04-ED-01-00-01) and 'wlan-ap' (MAC: 00-04-ED-38-F7-2E). Below this is the 'WPS Profile List' showing 'ExRegNWEA4036' with PIN 6229909. A progress bar indicates 'Progress >> 100%' and a message states 'PIN - Get WPS profile successfully.'. On the right, there are buttons for Rescan, Information, Pin Code (10864111), Config Mode (Registrar), Detail, Connect, Rotate, Disconnect, and Export Profile. The bottom section shows connection status for 'wlan-ap-2.4g' with a red circle around it, including details like 'Link is Up [TxPower:100%]', 'Channel >> 1 <-> 2412 MHz; central channel : 3', 'Authentication >> WPA2-PSK', 'Encryption >> AES', 'Network Type >> Infrastructure', 'IP Address >> 192.168.1.1', 'Sub Mask >> 255.255.255.0', and 'Default Gateway >> 192.168.1.254'. To the right of the status are signal strength indicators: 'Link Quality >> 100%', 'Signal Strength 1 >> 65%', 'Signal Strength 2 >> 39%', and 'Noise Strength >> 26%'. Below these are transmit and receive throughput graphs showing 'Link Speed >> 243.0 Mbps' and 'Throughput >> 0.000 Kbps' for transmit, and 'Link Speed >> 40.5 Mbps' and 'Throughput >> 98.612 Kbps' for receive.

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-5g

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.

MAC Filter

Parameters

MAC Address: 1 f0:de:f1:31:68:70 << --type or select from listbox--

2 Apply Cancel

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

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

MAC Filter

Parameters

Select SSID: wlan-ap-5g

MAC Restrict Mode \*:  Disable  Allow  Deny

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

MAC Address	Remove	Edit
F0:DE:F1:31:68:70	<input type="checkbox"/>	Edit

Add Remove

To delete entries , check the remove checkbox and press **Remove** to delete it.

To make changes, click **Edit** of a MAC address to reconfigure the MAC as needed.