BiPAC 7820NZ

3G/4G LTE Embedded with Dual-SIM Slots ADSL2+ Wireless-N VPN Firewall Router

User Manual

Version Released: 2.32d.dr1

Last revised date: June 30, 2014

Table of Contents

Chapter 1: Introduction *1*
Introduction to your Router 1
Features 3
ADSL Compliance 3
Network Protocols and Features 4
3G/4G LTE 4
Firewall 4
Quality of Service Control 5
ATM, PTM and PPP Protocols 5
IPTV Applications 5
Wireless LAN 5
USB Application Server 6
Virtual Private Network (VPN) 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 16
Configuring a PC in Windows 7/8 16
Configuring a PC in Windows Vista 19
Configuring a PC in Windows XP 22
Configuring a PC in Windows 2000 24
Configuring a PC in Windows 95/98/Me 25
Configuring a PC in Windows NT4.0 26
Factory Default Settings 27
Information from your ISP 29
Easy Sign On (EZSO) *30*
Chapter 4: Configuration *37*
Configuration via Web Interface 37
Status 39
Summary 40

WAN 41
Statistics 42
LAN 42
WAN Service 43
xTM 43
xDSL 44
Bandwidth Usage 47
LAN 47
WAN Service 49
3G/LTE Status 51
Route 52
ARP 53
DHCP 54
VPN 55
IPSec 55
PPTP 56
L2TP 57
OpenVPN 58
GRE 59
Log 60
System Log 60
Security Log 61
VRRP Status 62

Quick Start 63
Quick Start 63

Configuration 70
LAN - Local Area Network 71
Ethernet 71
IPv6 Autoconfig 74
Interface Grouping 78
VRRP 81
Wireless 82
Basic 83
Security 85
MAC Filter 97
Wireless Bridge 98
Advanced 100
Station Info 102
Schedule Control 103
WAN-Wide Area Network 104
WAN Service 104
Dual SIM 127
DSL 128
SNR 130
System 131
Internet Time 131
Firmware Upgrade 132
Backup / Update 133
Access Control 134
Mail Alert 135
SMS Alert 136
Configure Log 137

USB 138
Storage Device Info 138
User Account 139
Print Server 146
DLNA 151
IP Tunnel 153
IPv6inIPv4 153
IPv4inIPv6 155
Security 156
IP Filtering Outgoing 156
IP Filtering Incoming 159
MAC Filtering 161
Blocking WAN PING 162
Time Restriction 163
URL Filter 165
Parental Control Provider 168
QoS - Quality of Service 169
QoS Port Shaping 174
NAT 175
Exceptional Rule Group 175
Virtual Servers 177
DMZ Host 181
One-to-One NAT 182
Port Triggering 183
ALG 186
Wake On LAN 187

VPN 188
IPSec 188
VPN Account 198
Exceptional Rule Group 199
PPTP 201
PPTP Server 201
PPTP Client 202
L2TP 213
L2TP Server 213
L2TP Client 215
OpenVPN 229
OpenVPN Server 229
OpenVPN CA 231
OpenVPN Client 232
GRE 239

Advanced Setup 240
Routing 241
Default Gateway 241
Static Route 242
Policy Routing 244
RIP 245
DNS 246
DNS 246
Dynamic DNS 248
DNS Proxy 251
Static DNS 252

Static ARP 253
UPnP 254
Certificate 261
Trusted CA 261
Multicast 264
Management 266
SNMP Agent 266
TR- 069 Client 267
HTTP Port 269
Remote Access 270
Mobile Network 271
3G/LTE Usage Allowance 272
Power Management 273
Time Schedule 274
Auto Reboot 275
Diagnostics 276
Diagnostics Tools 276
Push Service 279
Diagnostics 280
Fault Management 281
Restart 282
Chapter 5: Troubleshooting 283
Appendix: Product Support & Contact 285

Chapter 1: Introduction

Introduction to your Router

The BiPAC 7820NZ, triple-WAN 3G/LTE/ADSL2+ firewall router is integrated with the 802.11n Wireless Access Point and 4-port switch. It is a cutting-edge networking product for SOHO and office users. Uniquely, the router allows users to directly insert 3G/4G LTE SIM card into its built-in SIM slots instead of requiring external USB modems. This design will avoid compatibility issues of many different 3G/LTE USB modems. With the increasing popularity of the 3G/4G LTE standard, communication via the BiPAC 7820NZ is becoming more convenient and widely available - enabling users to use a 3G/4G LTE, UMTS, EDGE, GPRS, or GSM Internet connection, making downstream rates of up to 100Mbps possible. Users can watch movies, download music or access e-mail wherever a 3G/4G LTE connection is available.

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

The BiPAC 7820NZ router allows you to insert 3G/4G LTE SIM card to its built-in SIM slots, enabling you to use a 3G/4G LTE Internet connection, which makes downstream rates of up to 100Mbps[*3] possible. With the increasing popularity of the 3G/4G LTE standard, communication via the BiPAC 7820NZ is becoming more convenient and widely available - allowing you to watch movies, download music on the road, or access e-mail no matter where you are. You can even share your Internet connection with others, no matter if you're in a meeting, or speeding across the country on a train. The auto fail-over feature ensures optimum connectivity and minimum interruption by quickly and smoothly connecting to a 3G/4G LTE network in the event that you ADSL/Fibre/Cable line fails. The BiPAC 7820NZ will then automatically reconnect to the ADSL/Fibre/Cable connection when it is restored, reducing connection costs. These features are perfect for office situations when a constant and smooth WAN connection is critical.

Optimal wireless performance

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

Secure VPN Connections

The BiPAC 7820NZ supports all currently popular secure VPNs, including embedded IPSec VPN, PPTP, L2TP, OpenVPN, GRE, which satisfies different users' needs, allowing users to establish encrypted private connections over the Internet with your optimum VPN options. You can access your corporate Intranet and transmit sensitive data between branch offices and remote sites anytime; even when you are out of office, thus enhancing productivity.

Smooth, Responsive Net Connection

Quality of Service (QoS) gives user full control over outgoing data traffic. Priority can be assigned by the router to ensure that important transmissions like gaming packets, or IPTV/streaming content passes through the router at lightning speed, even when there is heavy Internet traffic. The speed of different types of outgoing data passing through the router is also controlled to ensure that users do not saturate bandwidth with their browsing activities.

IPv6 supported

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

The BiPAC 7820NZ fully supports IPv6 (Internet Protocol Version 6), launched as the current IPv4 range is filling up, and IPv6 is gradually becoming the indispensable addressing system for savvy cloud computing users. Dual stack means the router is capable of running IPv4 and IPv6 in parallel during the transition period. With Billion IPv6 enabled devices, three major transition mechanisms such as Dual-Stack, Dual-Stack Lite, and 6RD (IPv6 rapid deployment) are supported to be adapted easily into service provider's IPv4/IPv6 network

Virtual AP

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

Web Based GUI

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

Firmware Upgradeable

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

Features

- IPv6 ready (IPv4/IPv6 dual stack)
- Triple-WAN ports for 3G/4G LTE, ADSL2+, Ethernet WAN (EWAN) for broadband connectivity
- 3G/4G LTE embedded with dual SIM card slots
- High-speed Internet Access via ADSL2 / 2+; Backward Compatible with ADSL
- Ethernet port #4 can be configured as a WAN interface for broadband connectivity
- Auto fail-over to ensure an always-on WAN connection
- IEEE 802.11 b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP) support
- Secured 16 IPSec VPN tunnels with powerful DES/ 3DES/ AES
- PPTP VPN with Pap/ Chap/ MS-CHAPv2 authentication
- Pure L2TP and L2TP over IPSec
- OpenVPN with CA authentication and extensive OpenSSL encryption
- GRE tunnel
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization and Bandwidth management
- Universal Plug and Play (UPnP) Compliance
- Supports IPTV Application*2
- USB port for print server, NAS(Samba), FTP server DLNA media server
- Ease of Use with Quick Installation Wizard (EZSO)

ADSL Compliance

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

Network Protocols and Features

- IPv4 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- IPv6 Stateless / Stateful Address Auto-configuration
- IPv6 Router Advertisement
- IPv6 over PPP
- DHCPv6
- IP Tunnel IPv6 in IPv4(6RD)
- IP Tunnel IPv4 in IPv6(DS-Lite)
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ
- 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
- SMTP client with SSL/TLS
- Supports port-based and tag-based Interface Grouping (VLAN)

3G/4G LTE *3

- LTE: peak downlink speed of up to 100Mbps and peak uplink speed of up to 50Mbps
  - Supports multi-band LTE: 2100MHz (B1), 1800MHz (B3), 2600MHz (B7), 900MHz (B8), 800MHz (B20).
  - Supports multi-band WCDMA: 2100MHz (B1), 1900MHz (B2), 850MHz (B5), 900MHz (B8)
- 3G/HSPA+: peak downlink speed of up to 14.4Mbps and peak uplink speed of up to 5.76Mbps
  - Supports dual-band WCDMA: 900MHz and 2100MHz or multi-band WCDMA: 850MHz, 1900MHz and 2100MHz
  - Supports Quad-band EDGE/GPRS/GSM: 850MHz, 900MHz, 1800MHz, 1900MHz
- Web-based GUI for configuration and management

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- Supports Web (http)/SSH/FTP/Telnet/SNMP
- Packet Filtering (v4/v6) - port, source IP address, destination IP 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, PTM and PPP Protocols

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

IPTV Applications*2

- IGMP Snooping and IGMP Proxy
- MLD Snooping and MLD Proxy
- Interface Grouping (VLAN)
- Quality of Service (QoS)
- Supports VLAN MUX

Wireless LAN

- Compliant with IEEE 802.11 b/ g/ n standards
- 2.4-2.484GHz radio band for wireless
- Up to 300 Mbps wireless operation rate
- 64 / 128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Supports WPS v2
- Wireless Security with WPA-PSK / WPA2-PSK support
- Multiple wireless SSIDs with wireless gust access and client isolation

- WDS repeater function support
- 802.1x radius authentication supported

USB Application Server

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

Virtual Private Network (VPN)

- 16 IPSec VPN tunnels
- IKE key management
- DES, 3DES and AES encryption for IPSec
- L2TP over IPSec
- Pap/ Chap/ MS-CHAPv2 authentication for PPTP
- IPSec pass-through
- OpenVPN with CA authentication and extensive OpenSSL encryption
- GRE tunnel

Management

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

Hardware Specifications

Physical Interface

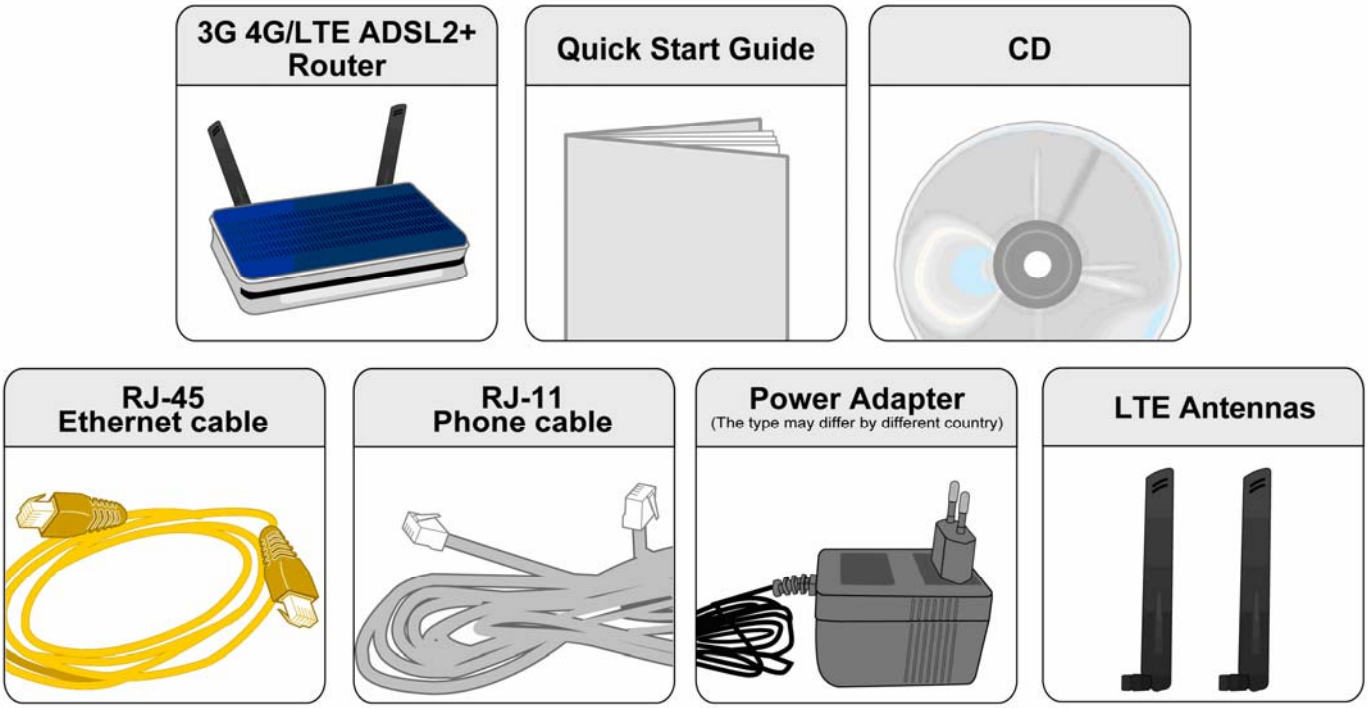
- WLAN: internal antennas
- 3G antenna: 3G antenna x 1 PCS[*3](only for 3G mode)
- 4G LTE antennas x 2 PCS[*3] (only for 4G LTE mode)
- DSL: ADSL port
- USB 2.0 port for storage service (Samba, FTP server), printer server
- Ethernet: 4-port 10 / 100Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: Ethernet port #4 can be configured as a WAN interface for Broadband connectivity.
- Dual SIM card slots
- Factory default reset button
- WPS push button
- Power jack
- Power switch

NOTE:	1. On request for Telco / ISP projects 2. IPTV application may require subscription to IPTV services from a Telco / ISP. 3. The 3G / 4G LTE data rate is dependent on your local service provider and your 3G / 4G LTE card. The 3G model comes with 1 antenna and 3G/4G LTE model comes with 2 antennas. 4. Specifications on this datasheet are subject to change without prior notice.

Chapter 2: Installing the Router

Package Contents

- 3G/4G LTE Embedded with Dual-SIM Slots ADSL2+ Wireless-N VPN Firewall Router
- Quick Start Guide
- CD containing the on-line manual
- RJ-45 Cat. 5e STP Ethernet cable
- RJ-11 ADSL/ telephone cable
- Power adapter
- 3G antenna: 3G antenna x 1 PCS (only for 3G mode)
- 4G LTE antennas x 2 PCS (only for 4G LTE mode)
- Splitter / Micro-filter (Optional)



(LTE mode)

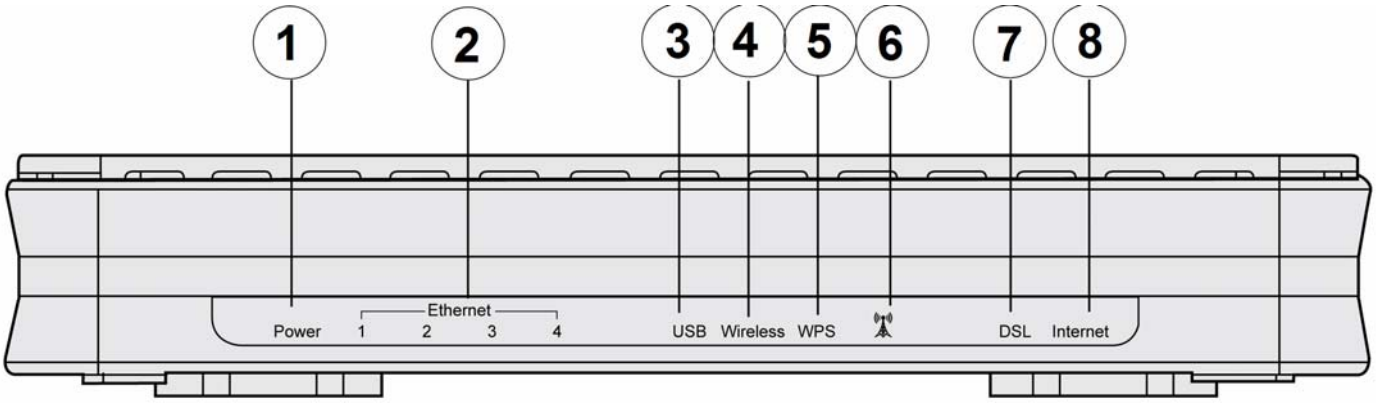
Important note for using this router

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 too hot, turn off the power immediately and have it repaired at a qualified service center. 4. Avoid using this product and all accessories outdoors.

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

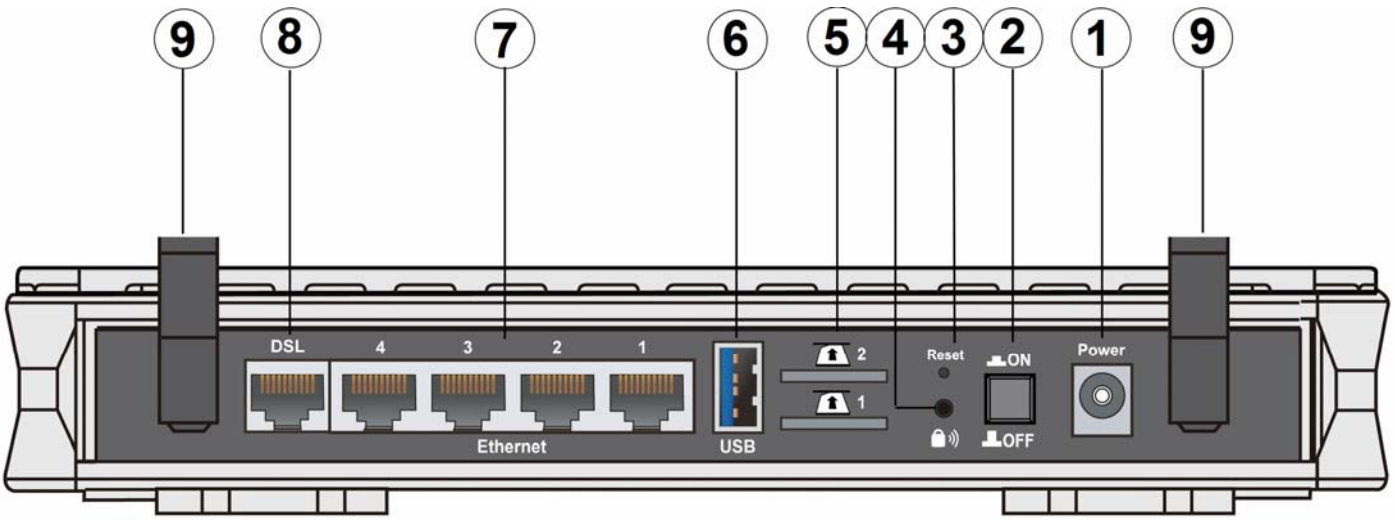
Device Description

The Front LEDs



LED		Status	Meaning
1	**Power**	Red	Boot failure or in emergency mode
		Green	System ready
2	**Ethernet Port 1-4 (EWAN)**	Green	Transmission speed hitting 10/100Mbps
		Blinking	Data being transmitted/received
3	**USB**	Green	Connected to the USB device (USB 2.0 Storage, Printer).
4	**Wireless**	Green	Wireless connection established
		Green blinking	Sending/receiving data
5	**WPS**	Green blinking	WPS configuration being in progress
		Off	WPS process completed or WPS is off
6	**3G/LTE**	Green	3G/LTE service(down) is up.
		Slow orange blinking	Weak 3G/LTE signal
		Quick orange blinking	Moderate 3G/LTE signal
		Solid orange	Strong 3G/LTE signal
7	**DSL**	Green Blinking	DSL synchronizing or waiting for DSL synchronizing
		Green	Successfully connected to an ADSL DSLAM (Line Sync).
		Off	DSL cable unplugged
8	**Internet**	Green	Having obtained an IP address successfully
		Off	Router in bridge mode or DSL connection not present.

The Rear Ports



Port		Meaning
1	**Power**	Connect the supplied power adapter to this jack.
2	**Power Switch**	Power ON / OFF switch.
3	**RESET**	After the device is powered on, press it **5 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot the password)
4	**WPS**	1 WPS button: Push WPS button to trigger Wi-Fi Protected Setup function. 2. Wireless on/off: When WPS is disabled, WPS button can act as wireless on/off button. Press WPS button more than 2 seconds to switch on/off the wireless connectivity,.
5	**SIM card slots**	BiPAC 7820NZ provides dual-SIM failover mobile connection with two embedded SIM slots. Please plug SIM card into the slot.
6	**USB**	Connect the USB device (USB 2.0 hard driver, Printer) to this port to server.
7	**Ethernet**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps. **Note:** Port #4 can be configured as a WAN Interface for Broadband connectivity.
8	**DSL**	Connect this port to the DSL network with the RJ-11 cable (telephone) provided.
8	**Antennas**	The detachable antennas. • 3G antenna: 3G antenna x 1 PCS (only for 3G mode) • 4G LTE antennas x 2 PCS (only for 4G LTE mode)

Cabling

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

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

Chapter 3: Basic Installation

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

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

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

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

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

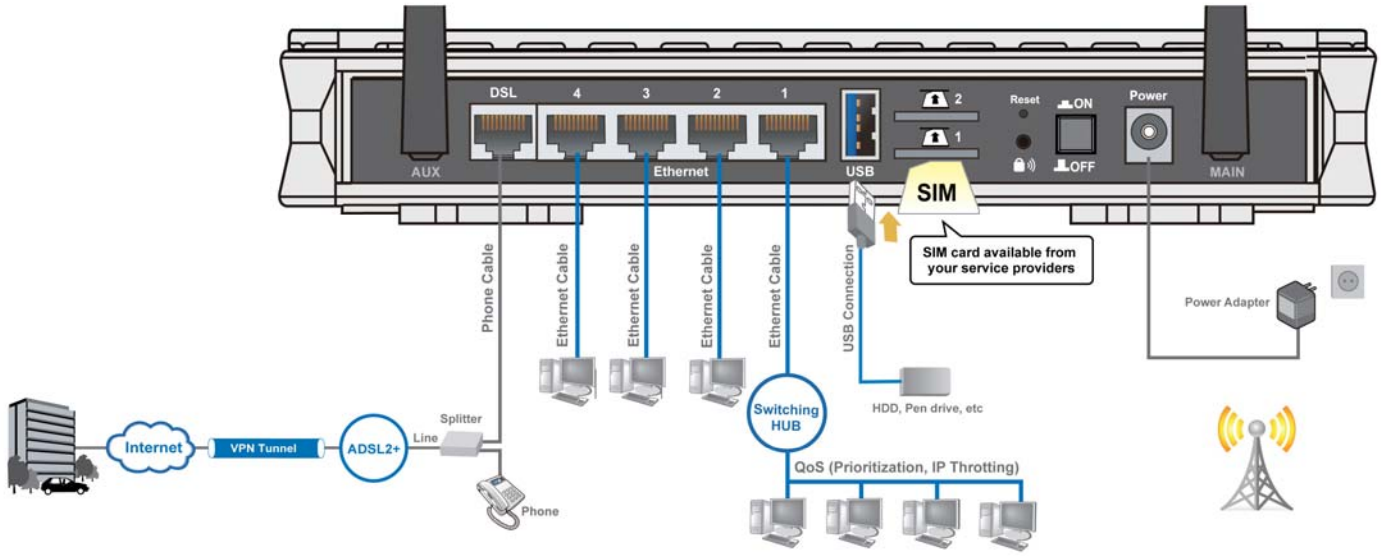
Connecting Your Router

Users can connect the Dual-SIM 3G/4G LTE ADSL2+ router as the following.

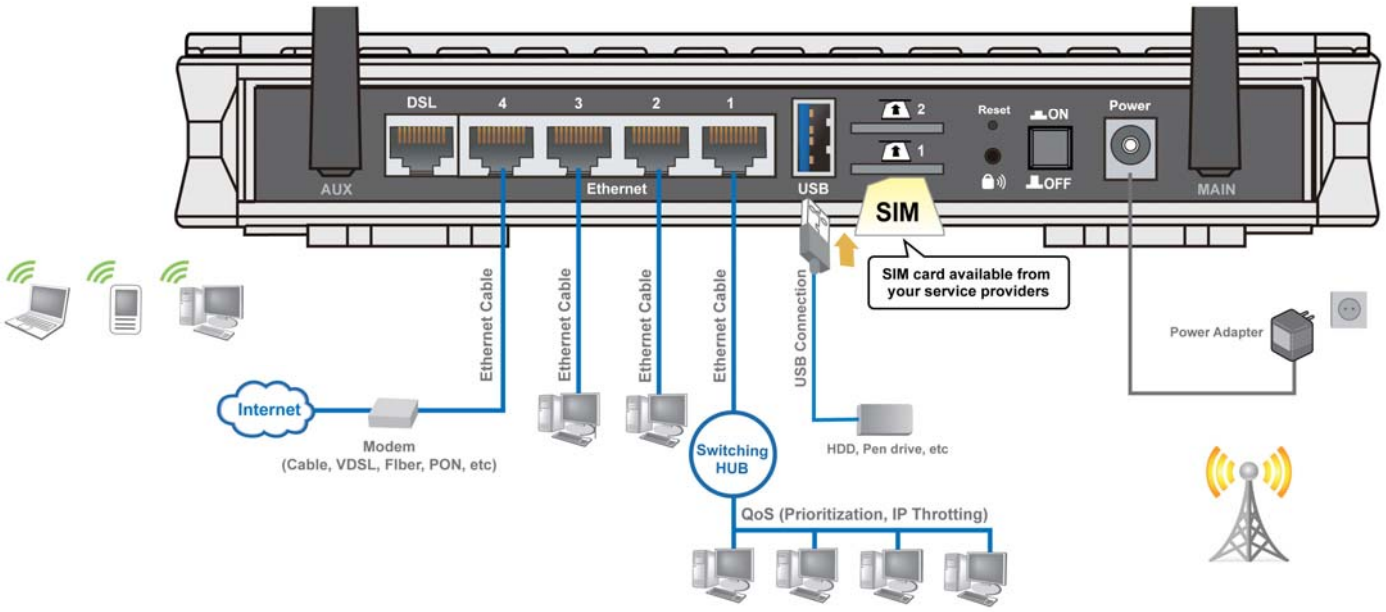
Note: BiPAC 7820NZ offers different mobile antennas distribution for 3G and 4G/LTE mode for an optimal performance. Here, we take the LTE mode for an example in the illustration.

- 3G antenna: 3G antenna x 1 PCS
- 4G LTE antennas x 2 PCS

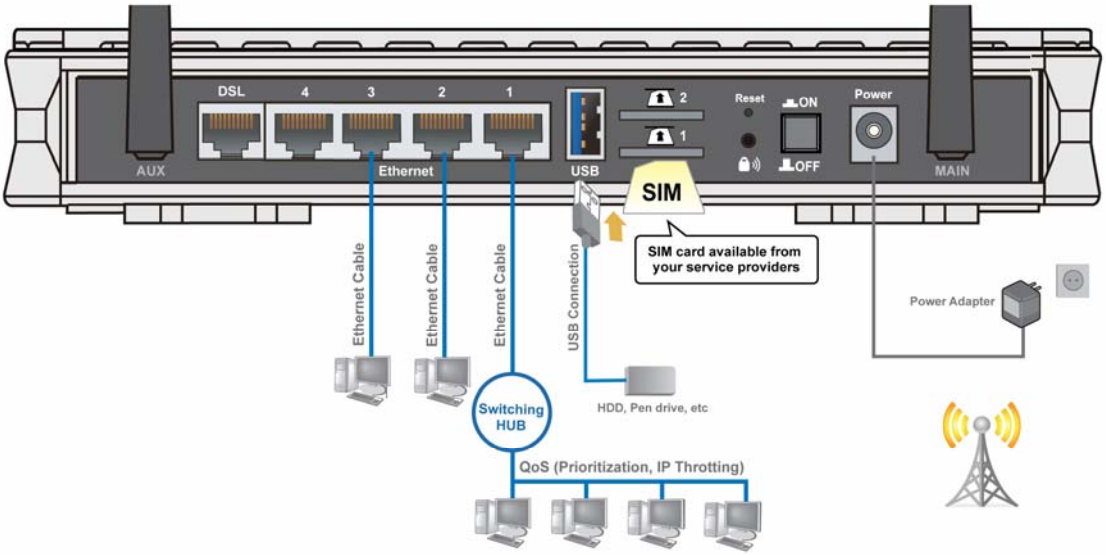
ADSL Router mode:



Broadband Router mode:



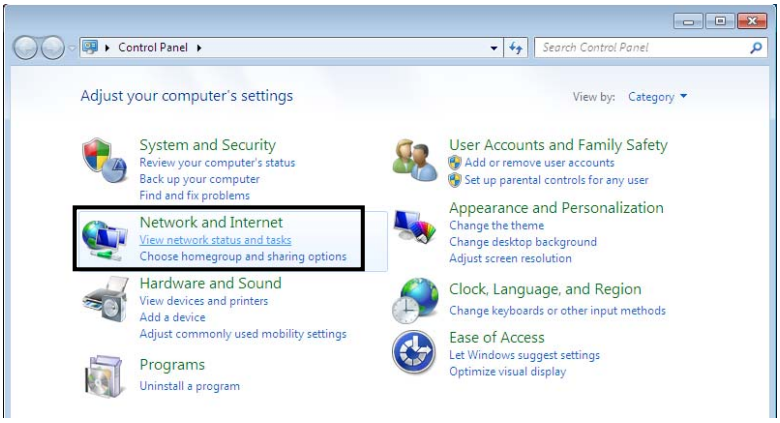
3G/LTE Router mode



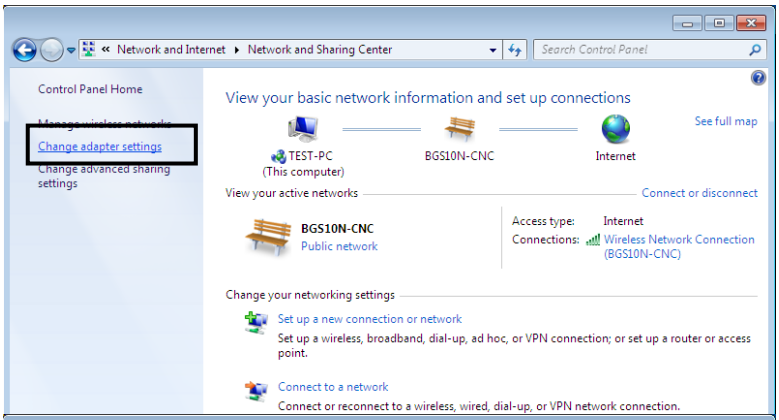
Network Configuration

Configuring a PC in Windows 7/8

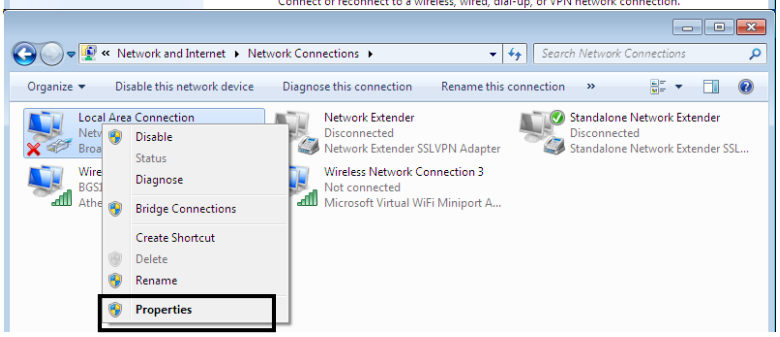
1. Go to **Start**. Click on **Control Panel**.
   Then click on **Network and Internet**.



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

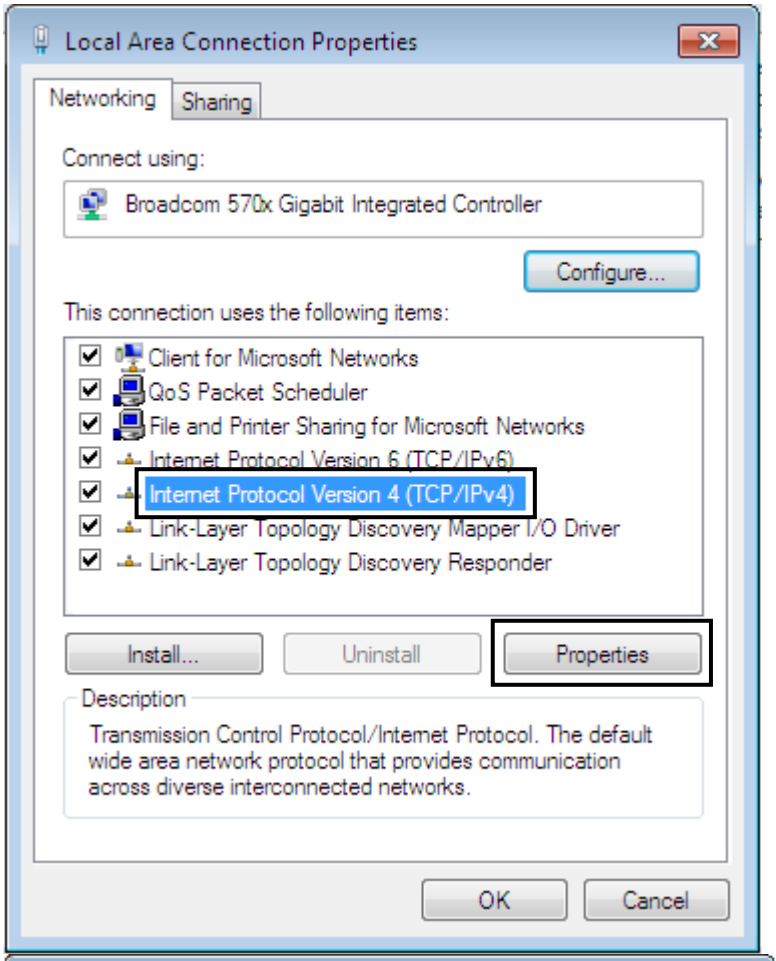


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.



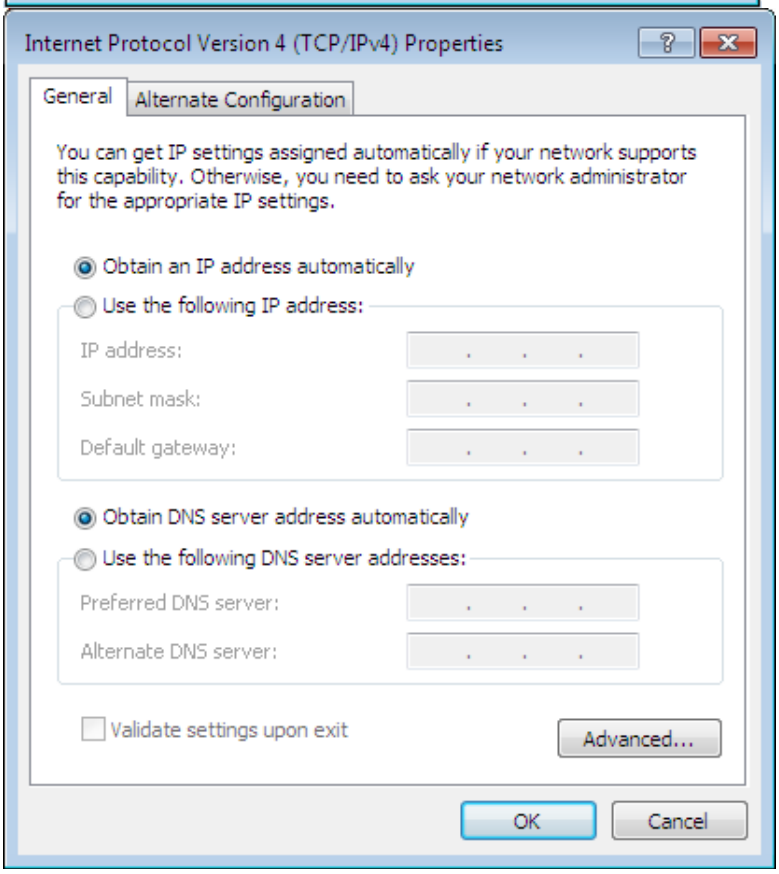
IPv4:

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



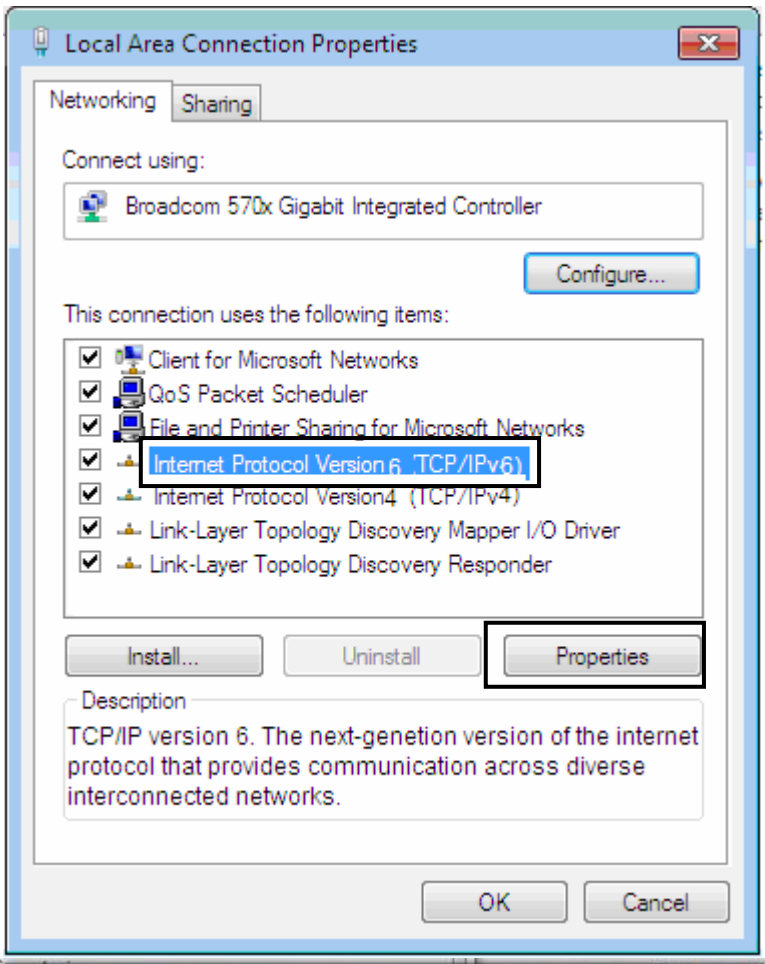
5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



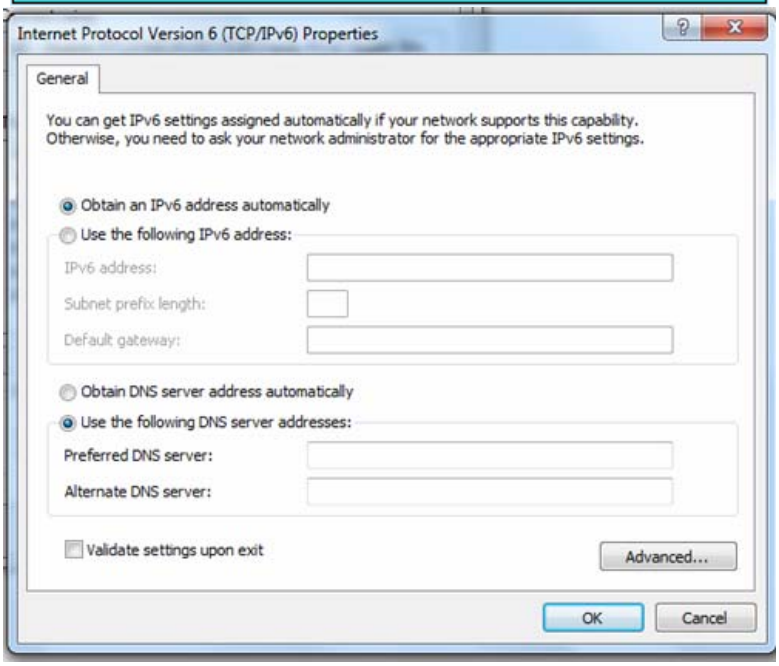
IPv6:

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



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

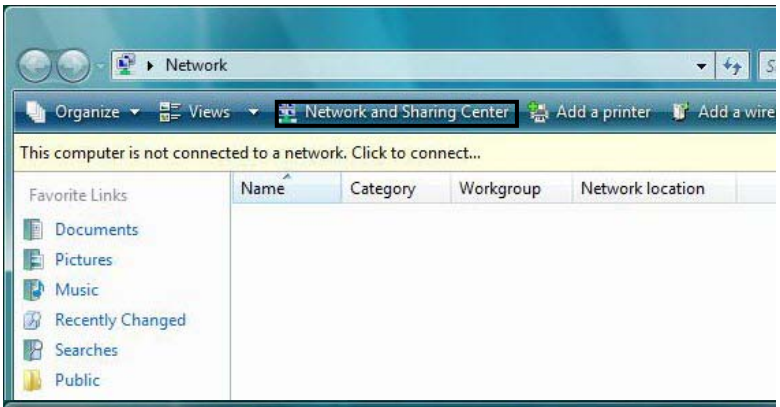
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



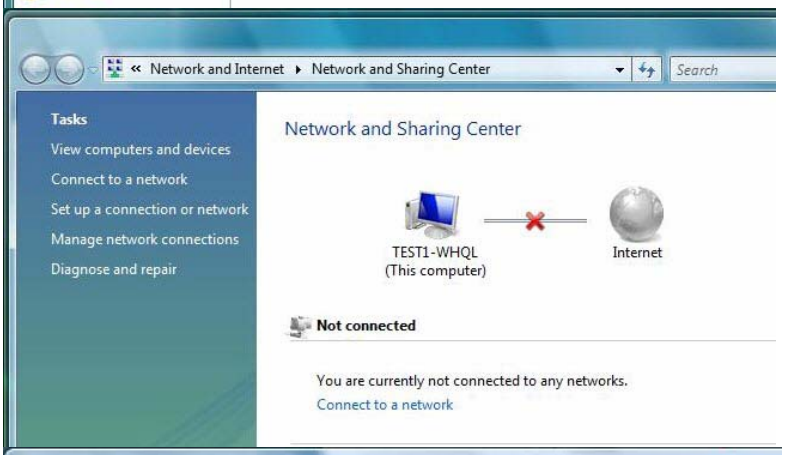
Configuring a PC in Windows Vista

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

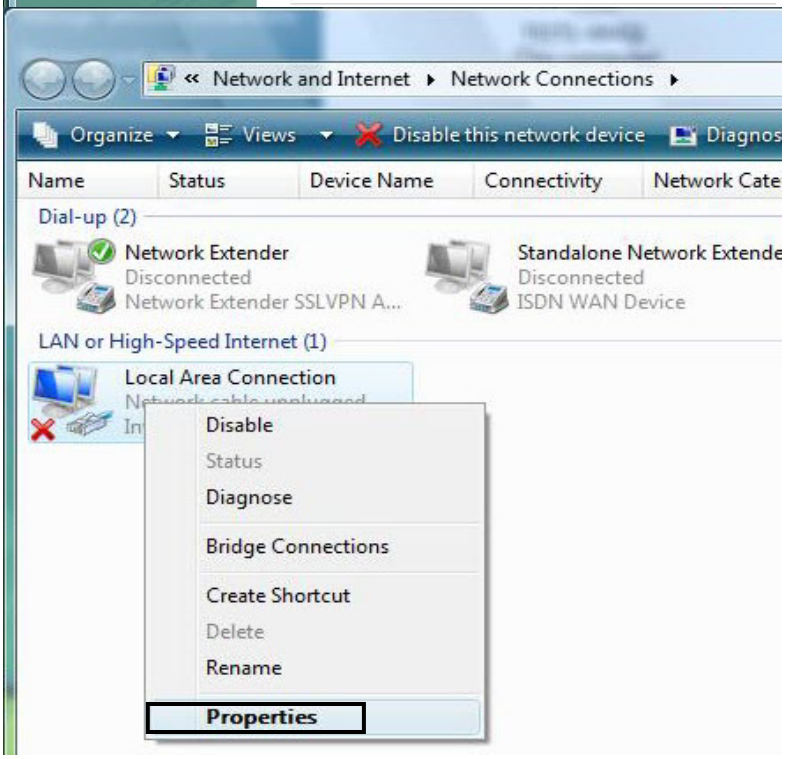
2. Then click on **Network and Sharing Center** at the top bar.



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

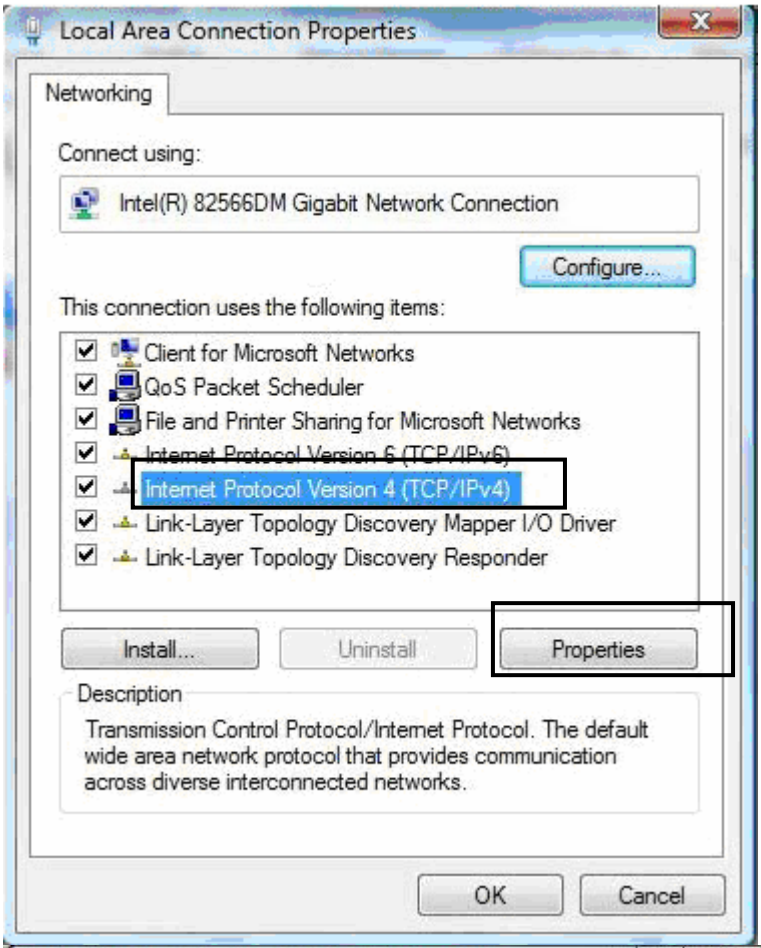


4. Select the **Local Area Connection**, and right click the icon to select **Properties**.



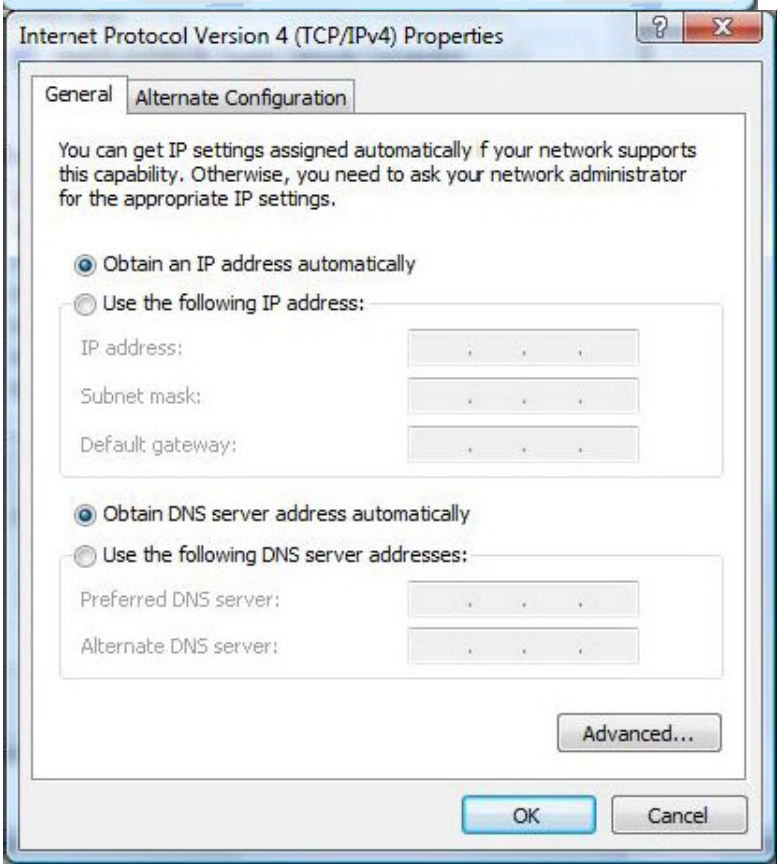
IPv4:

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



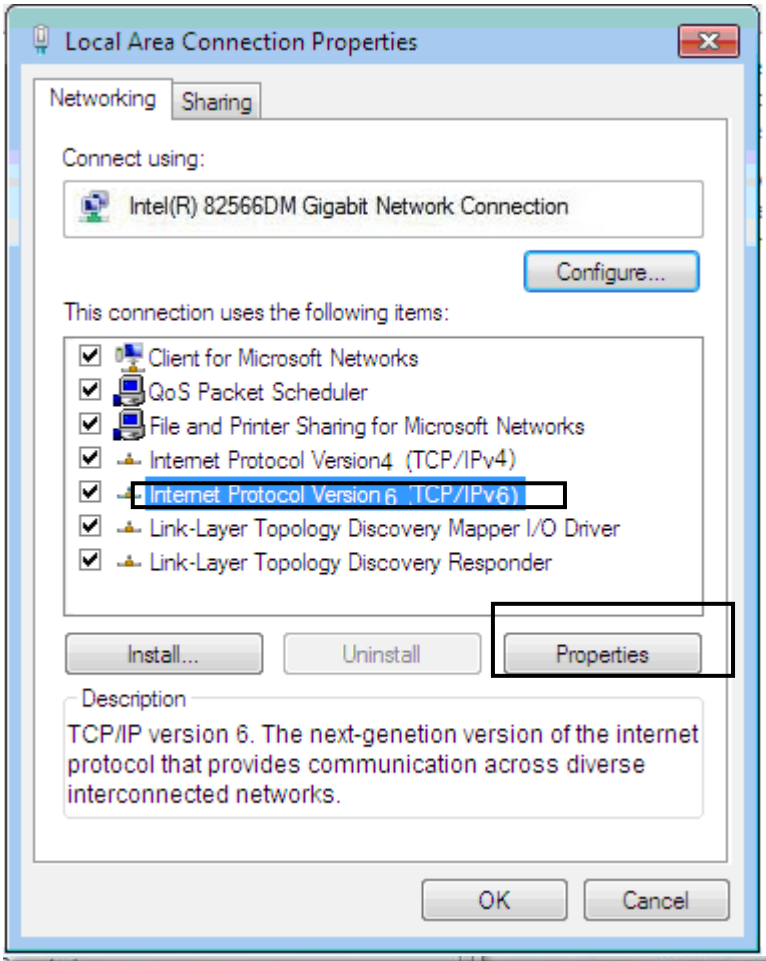
6. In the **TCP/IPv4 properties** window, select the Obtain an **IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.

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



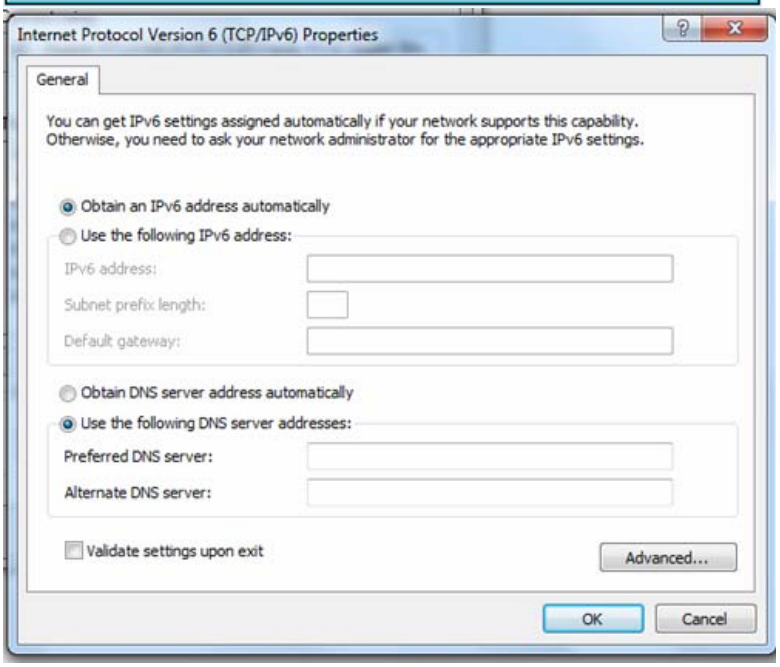
IPv6:

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



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

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

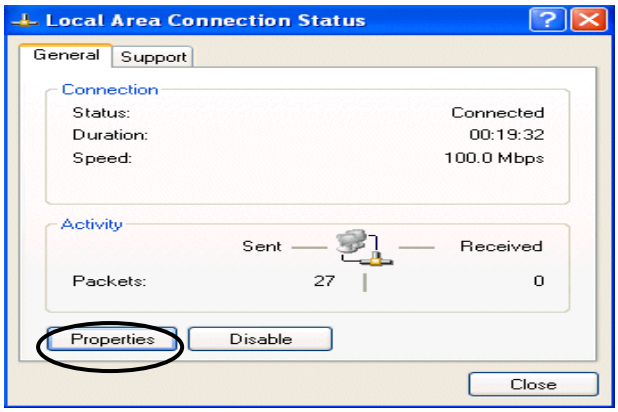


Configuring a PC in Windows XP

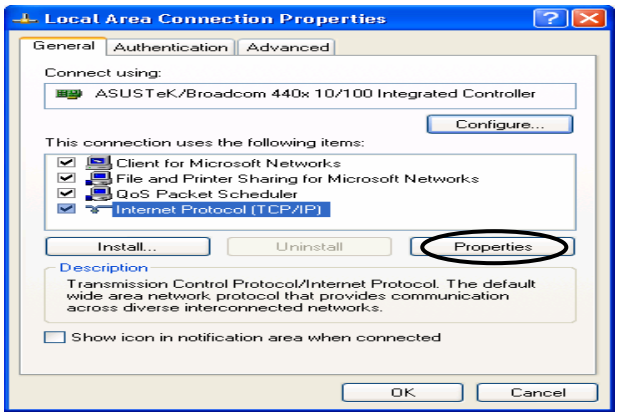
IPv4:

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

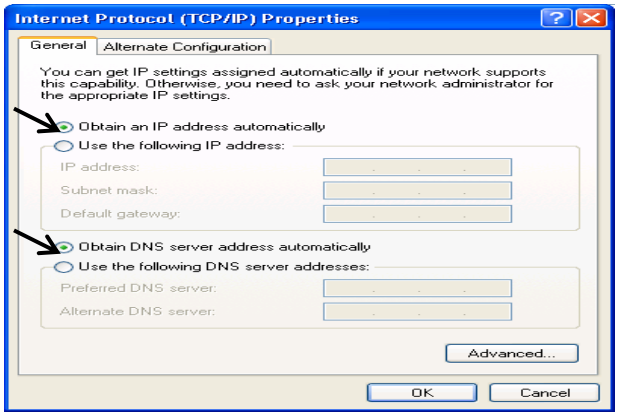
3. In the **Local Area Connection Status** window, click **Properties**.



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

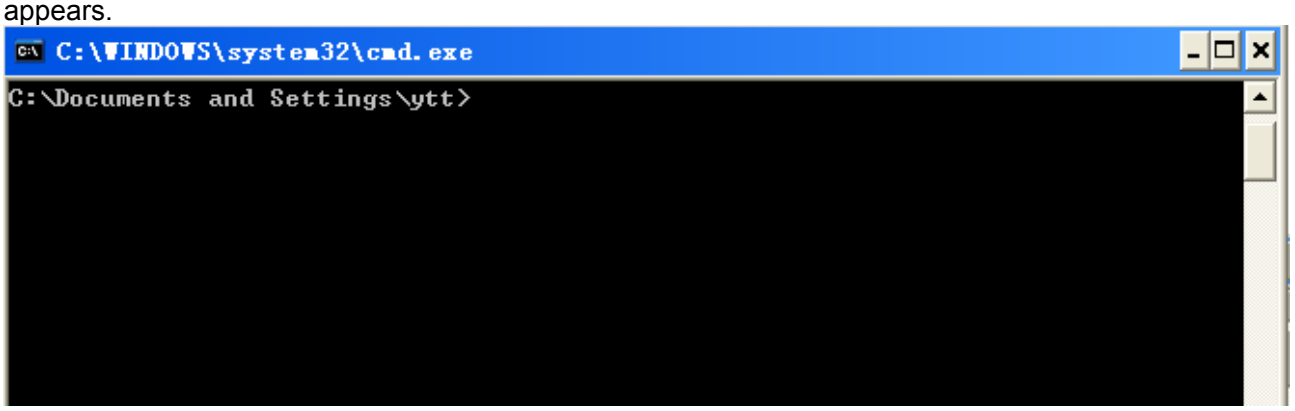


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

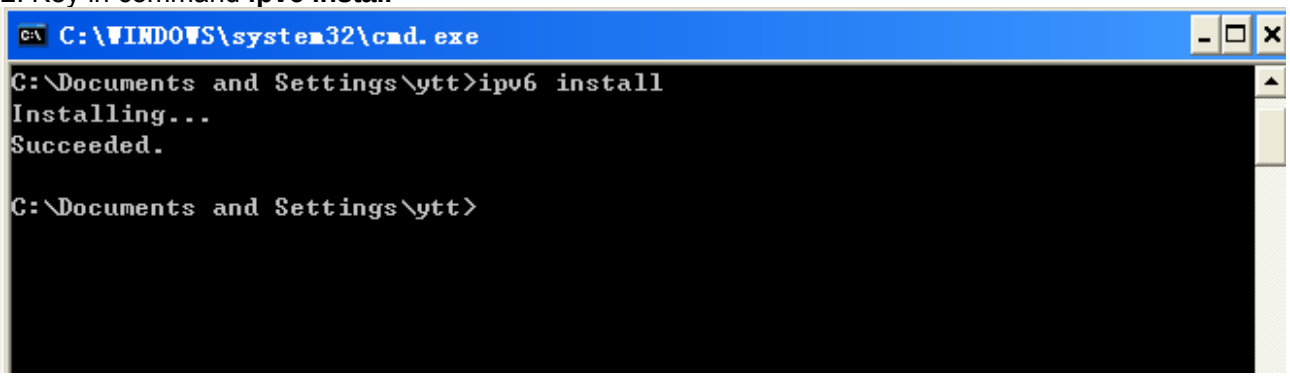


IPv6:

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



2. Key in command **ipv6 install**

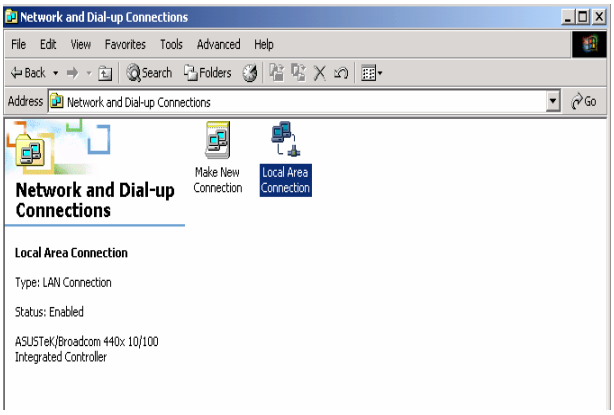


Configuration is OK now, you can test whether it works ok.

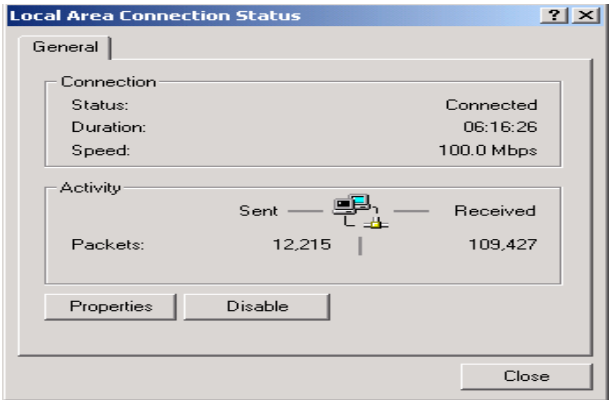
Configuring a PC in Windows 2000

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

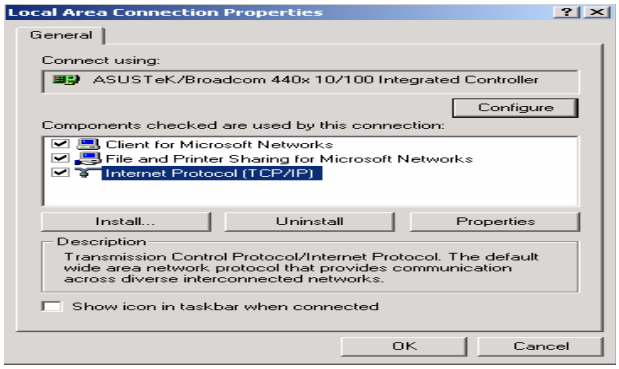
2. Double-click Local Area Connection.



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

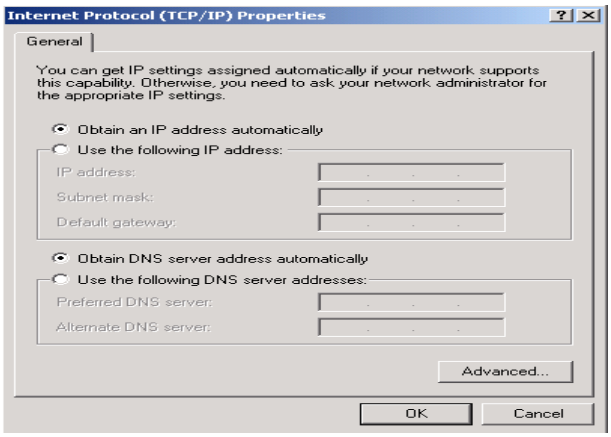


4. Select Internet Protocol (TCP/IP) and click Properties.



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

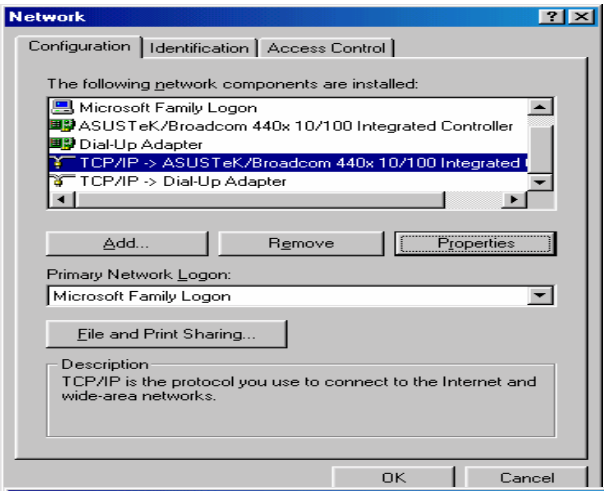
6. Click OK to finish the configuration.



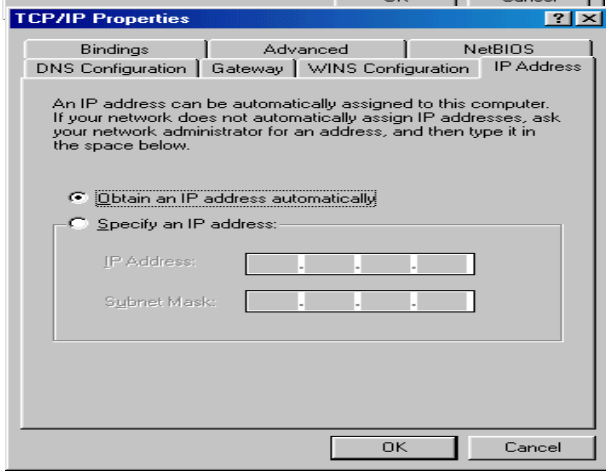
Configuring a PC in Windows 95/98/Me

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

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

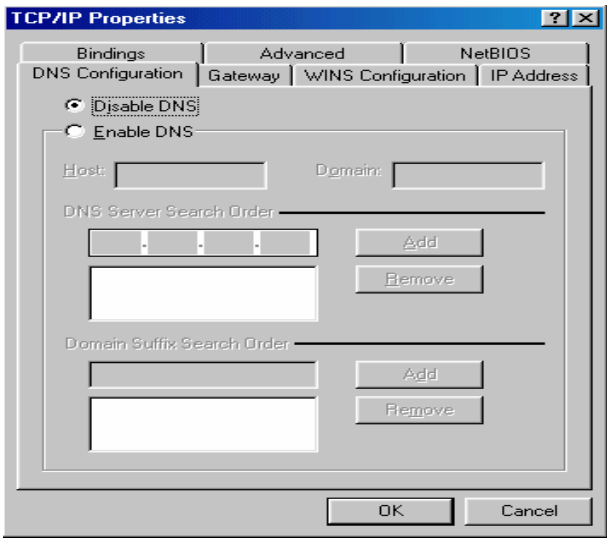


3. Select the Obtain an IP address automatically radio button.



4. Then select the DNS Configuration tab.

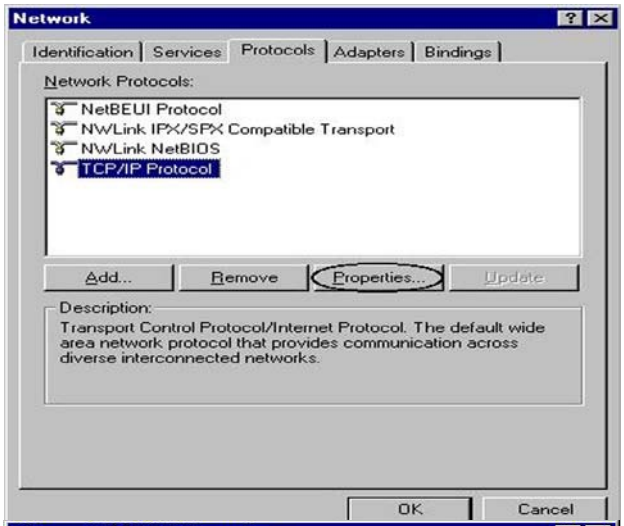
5. Select the Disable DNS radio button and click OK to finish the configuration.



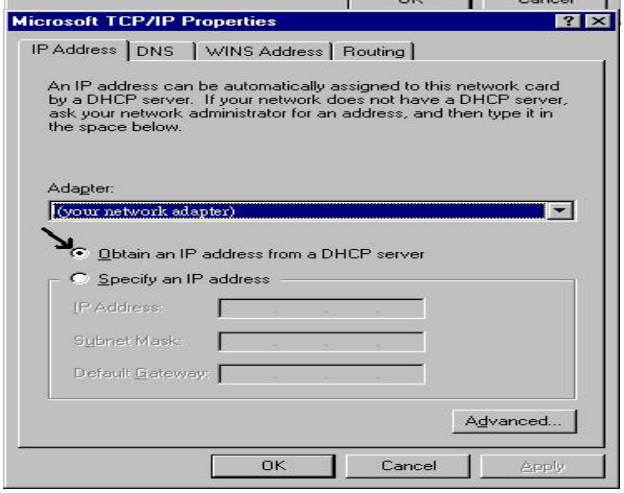
Configuring a PC in Windows NT4.0

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

2. Select TCP/IP Protocol and click Properties.



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



Factory Default Settings

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

Web Interface (Username and Password)

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

Administrator

- Username: admin
- Password: admin

Local

- Username: user
- Password: user

Remote

- Username: support
- Password: support

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

Device LAN IPv4 settings

- IPv4 Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

Device LAN IPv6 settings

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

DHCP server for IPv4

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

LAN and WAN Port Addresses

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

IPv4

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

IPv6

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

Information from your ISP

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

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

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

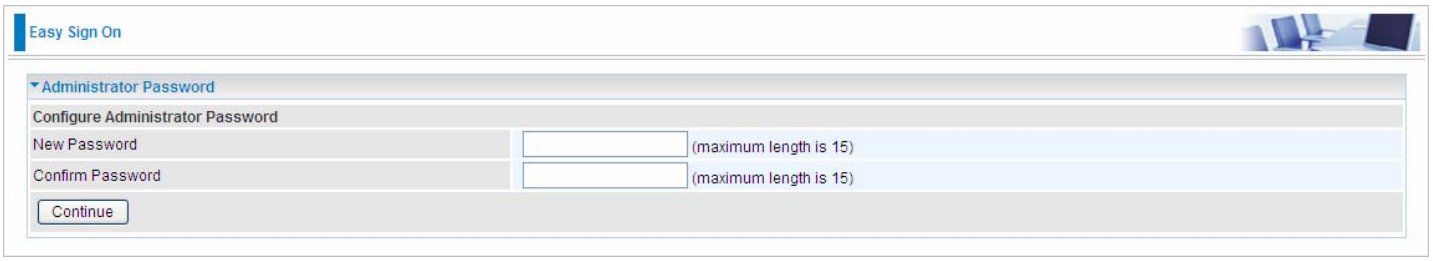
Easy Sign On (EZSO)

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

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

EZSO window pops up:

Step1: Set the administration password.

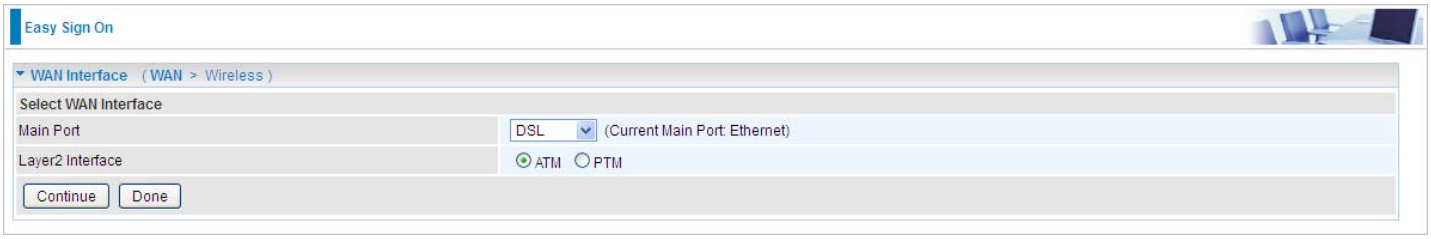


Step 2: Set the Time Zone.

Step 3: Configure the WAN interface.

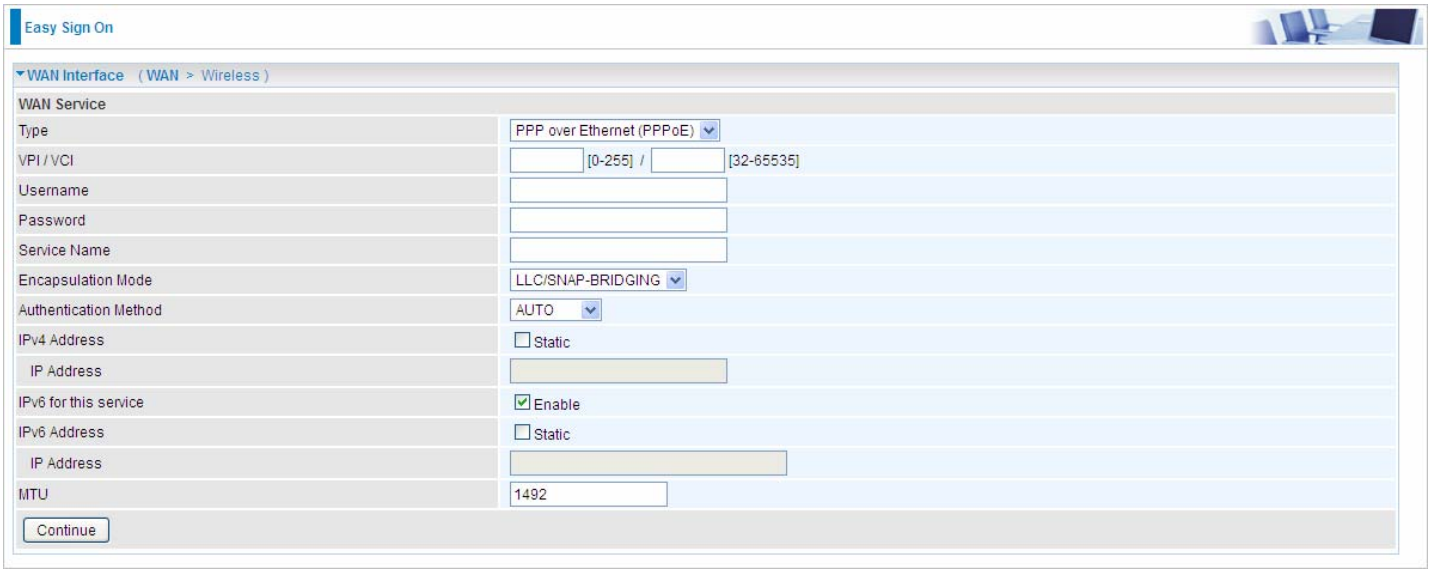
DSL mode

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

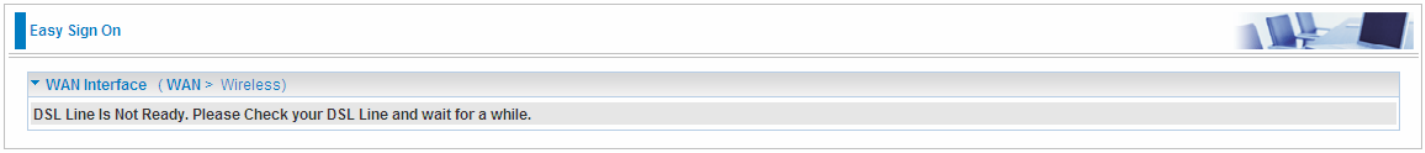


1. Select DSL, press **Continue** to go on to next step, press “Done” to quit the setting.

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

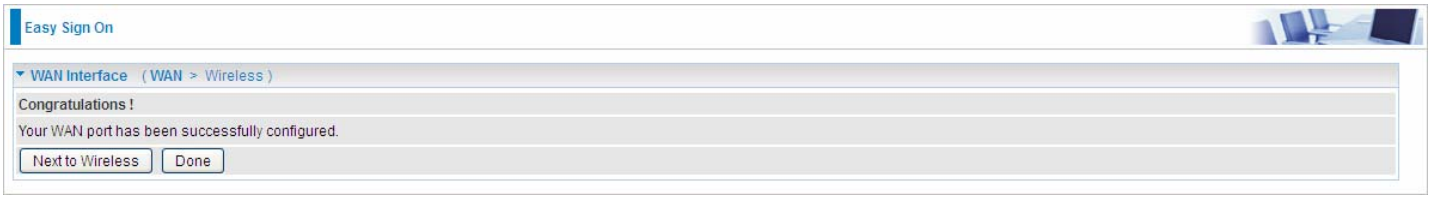


If the DLS line doesn't synchronize, the page will pop up warning of the DSL connection failure.



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

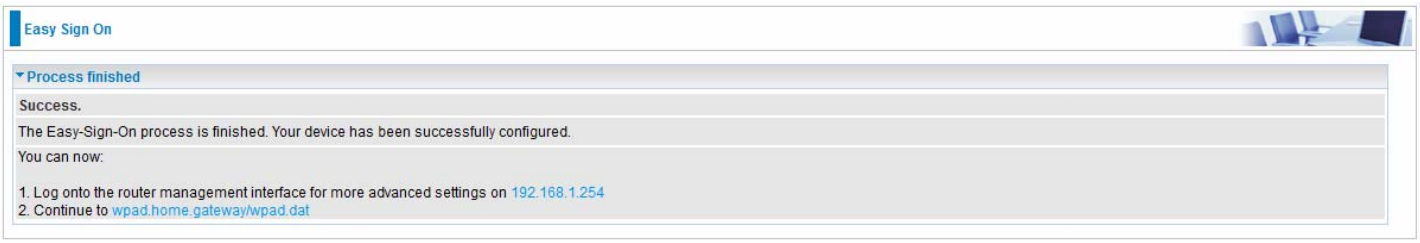
4. WAN port configuration is success and next to wireless, if you want skip wireless setting, click **Done**.



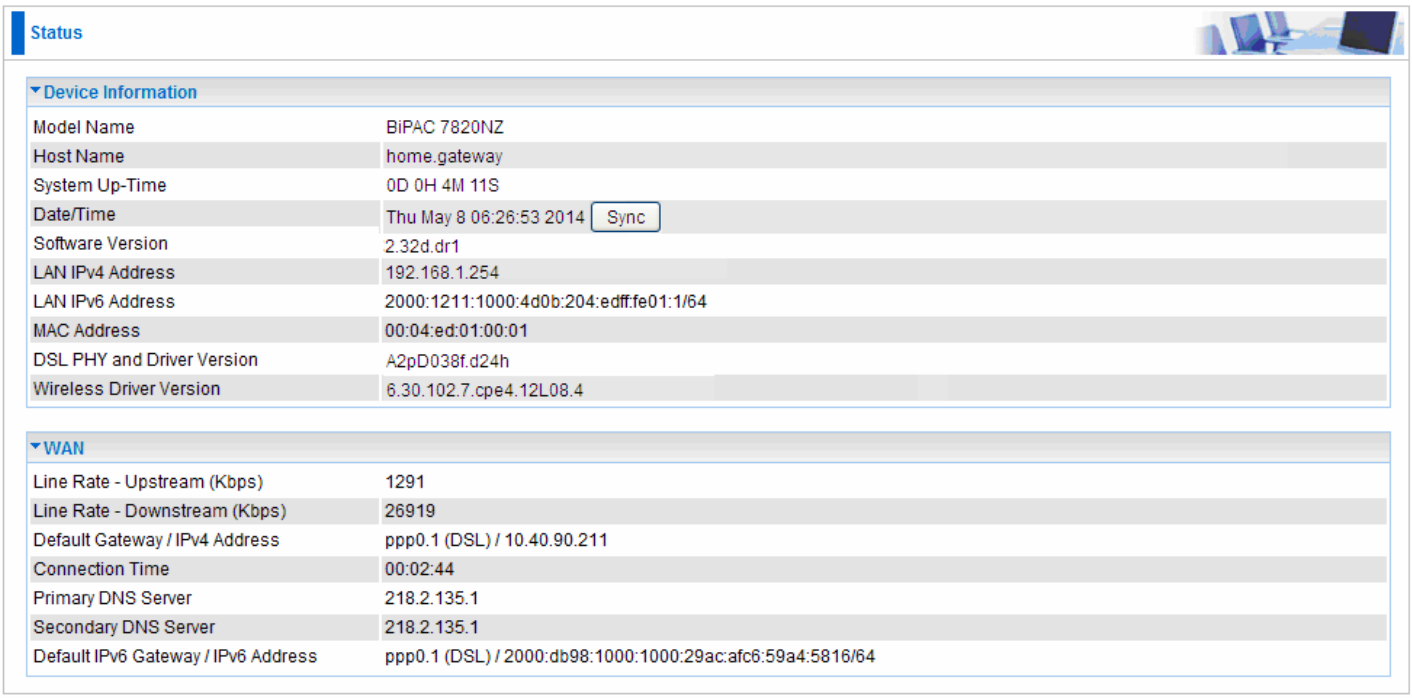
Click **Done**, web configuration will be loaded, you will enter the web configuration page.

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable the wireless and set the SSID and encryption Key. (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

6. Success in configuring the EZSO.

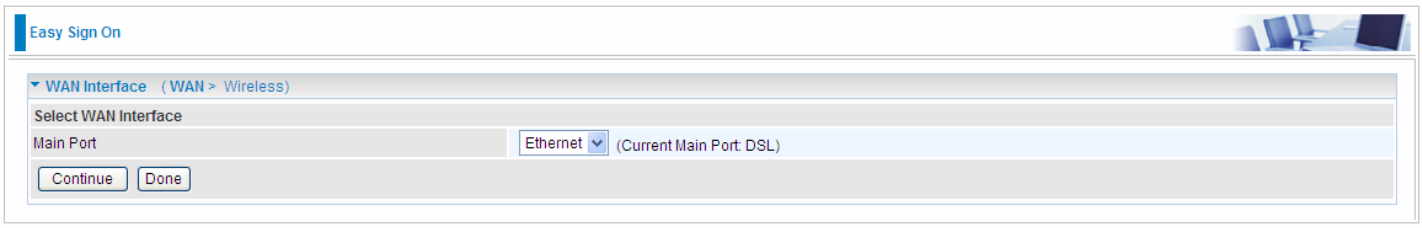


Click link ***192.168.1.254***, it will lead you to the following page.

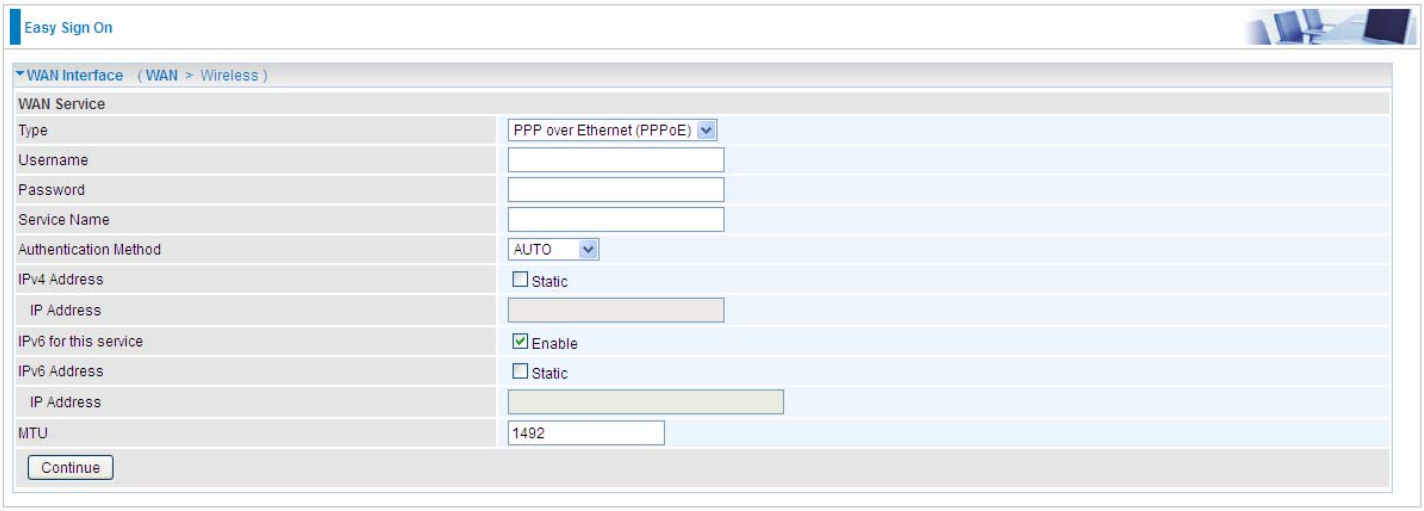


Ethernet mode

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

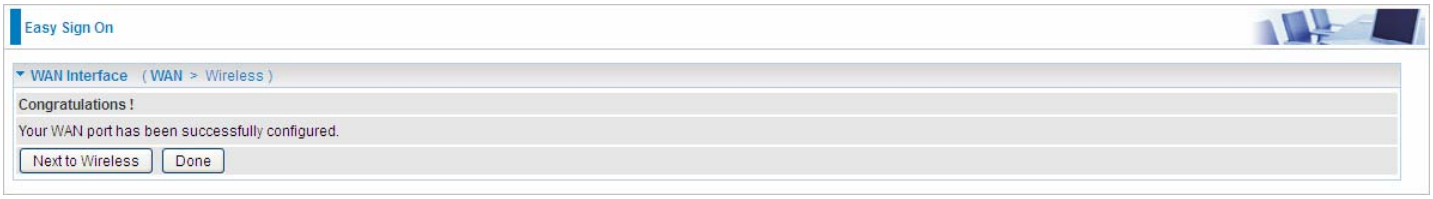


2. Enter the username, password from your ISP, for IP and DNS settings, also refer to your ISP. Here IPv6 service is enabled by default.



3. Wait while the device is configured.

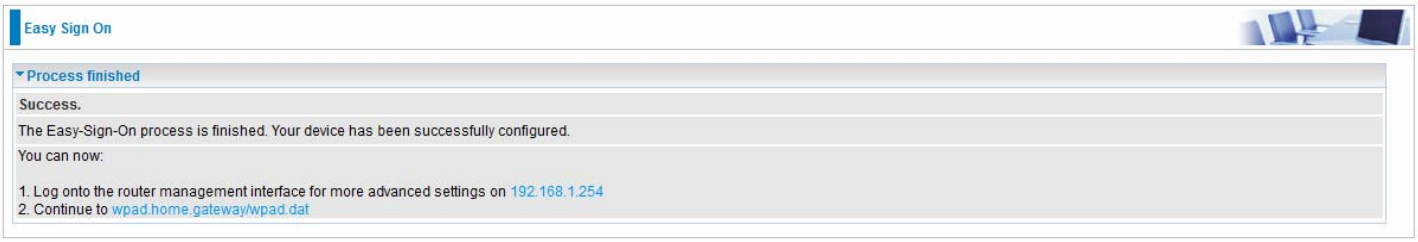
4. WAN port configuration is success.



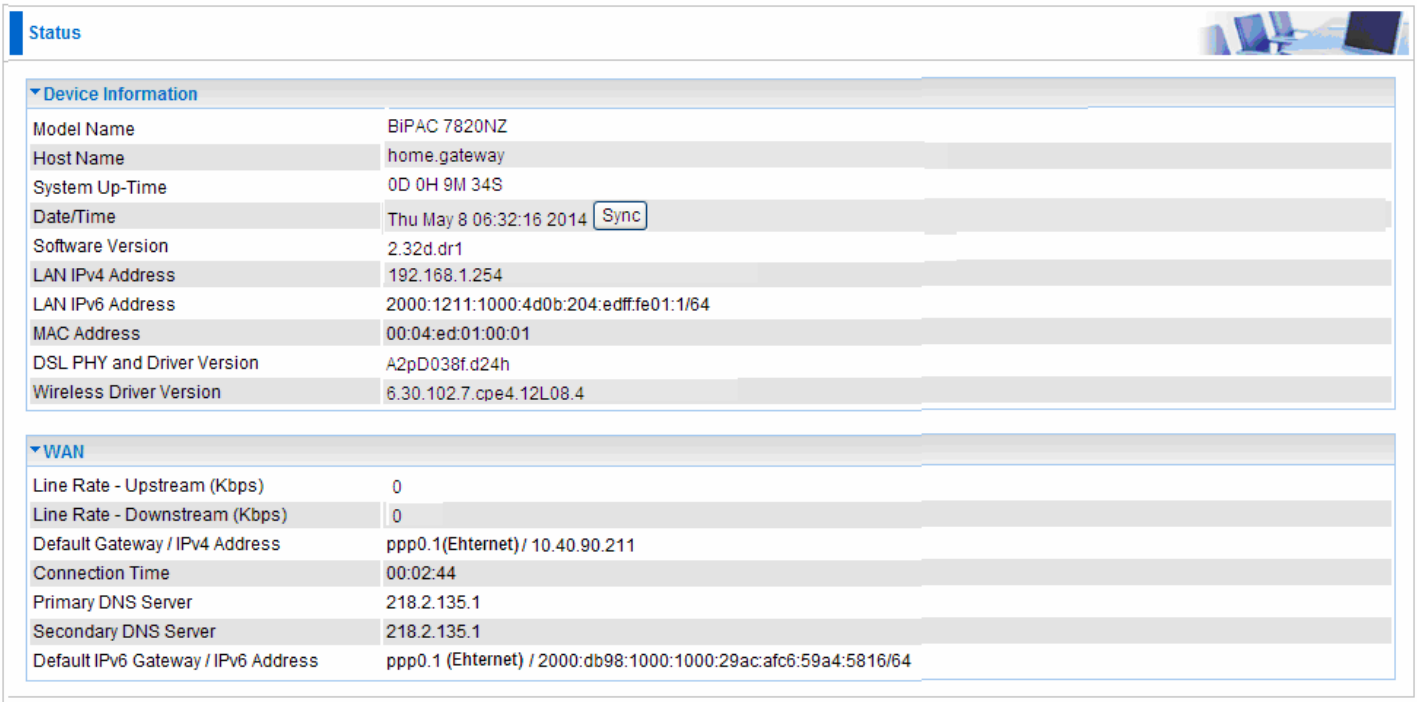
Click **Done**, web configuration will be loaded, you will enter the web configuration page.

5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

6. Success in configuring the EZSO.

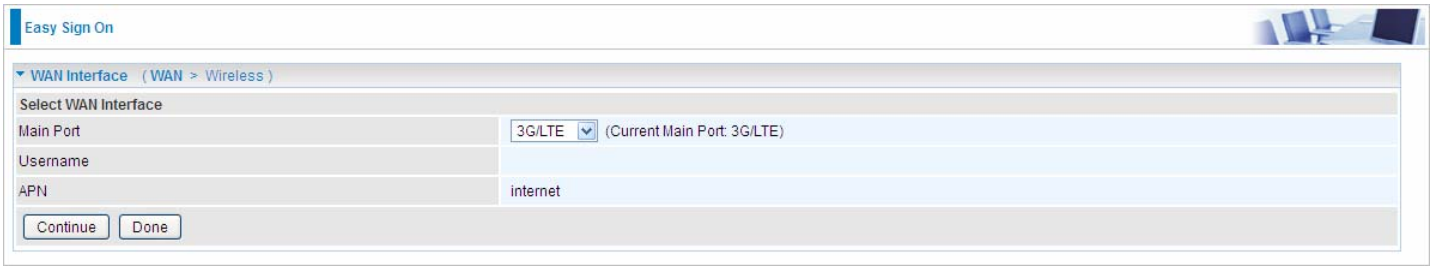


Click ***192.168.1.254***, it will lead you to the following page.



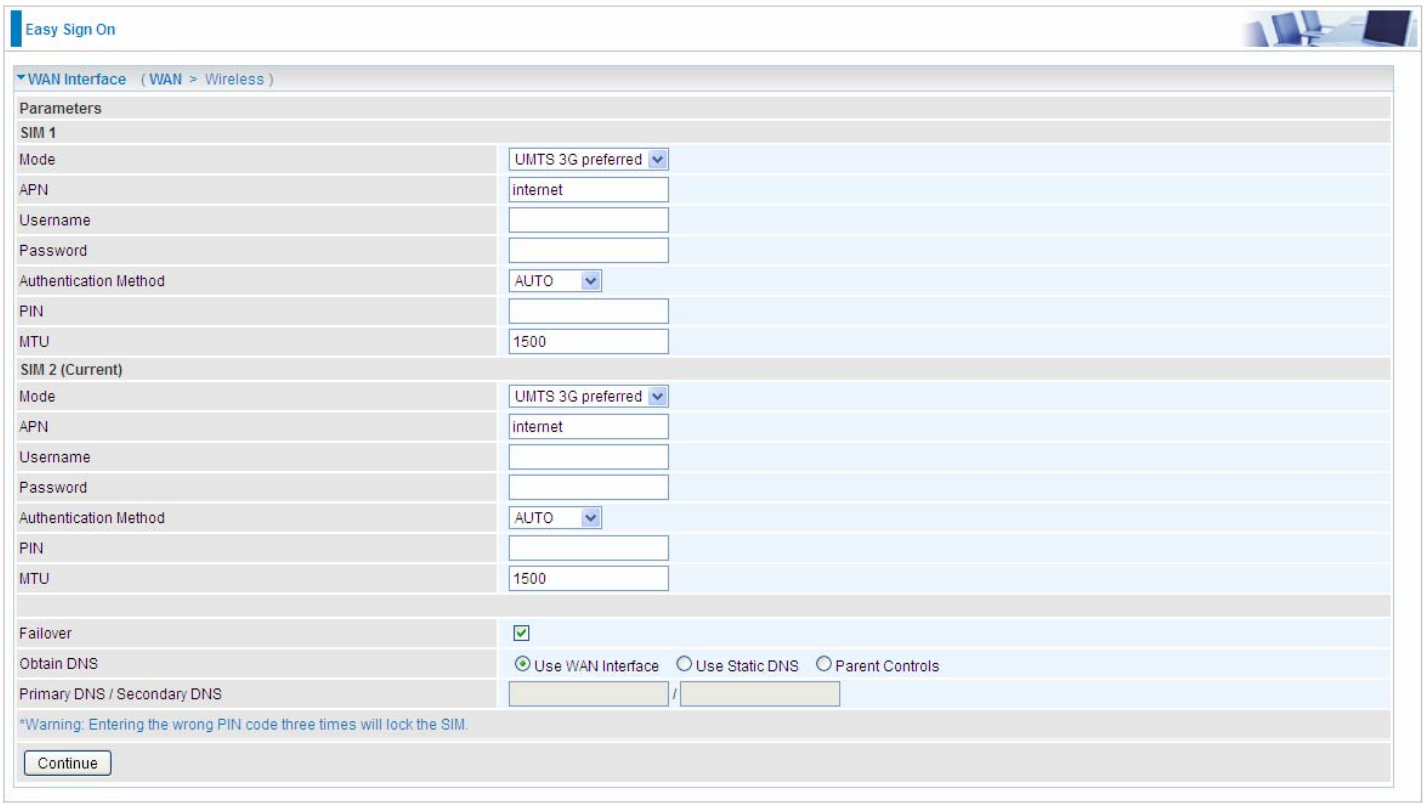
3G/LTE

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



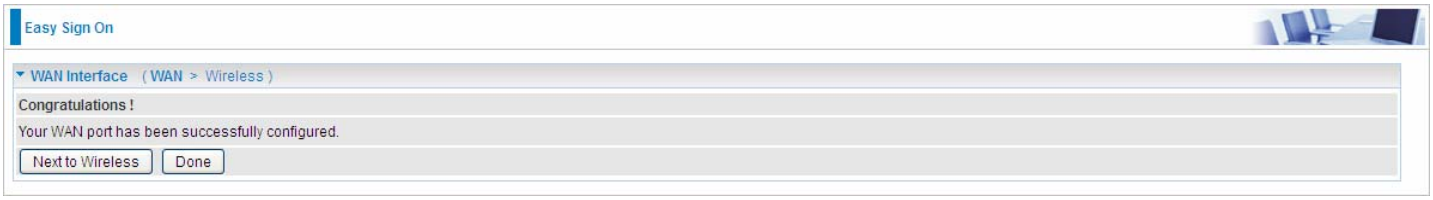
2. Select the 3G/LTE mode, and enter the APN, username, password from your ISP; and check with your ISP with the authentication method setting for each SIM (SIM1 and SIM2).

Note: Given that BiPAC 7820NZ supports dual -SIM mobile connectivity, please determine which SIM you are gonna use or both (3G/LTE failover), and set the exact required connecting information for each SIM (SIM1 and SIM2).

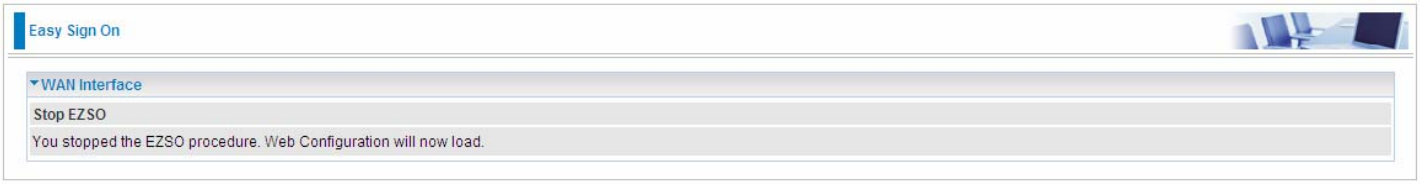


3. Wait while the device is configured.

4. WAN port configuration is success.



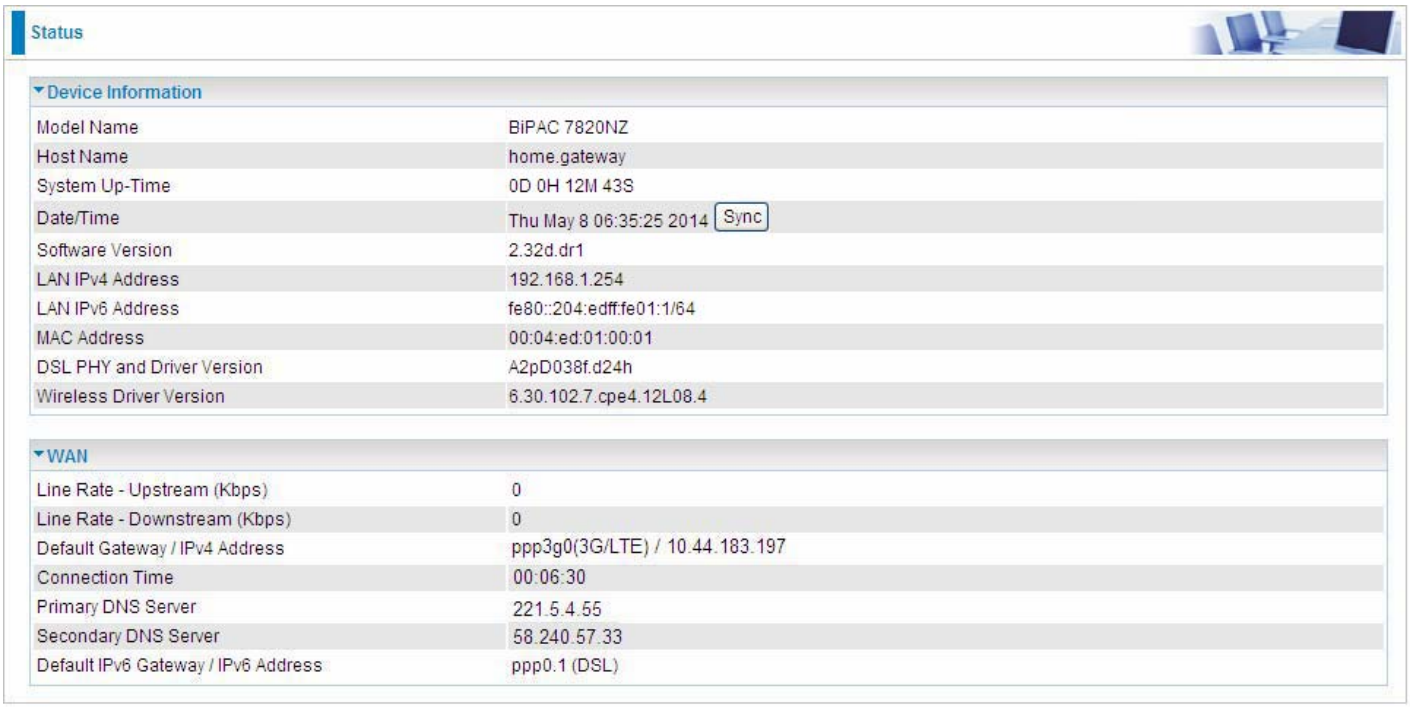
Click **Done**, web configuration will be loaded, you will enter the web configuration page.



5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

7. Success in configuring the EZSO.

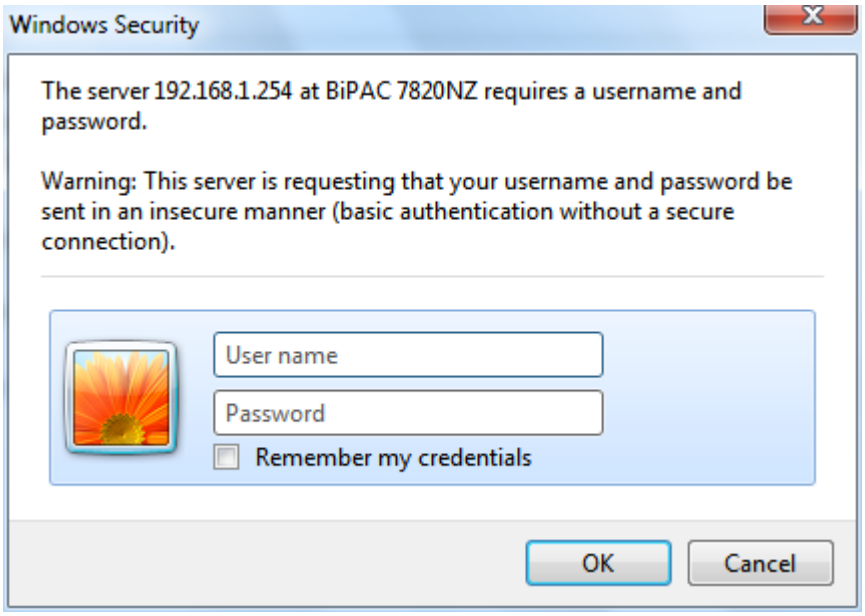
Click ***192.168.1.254***, it will lead you to the following page.



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.



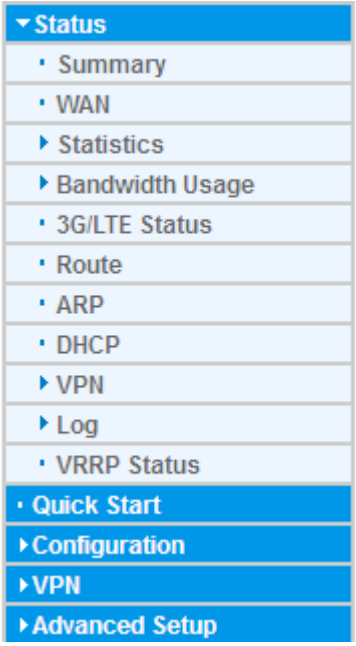
Congratulations! You are now successfully logged on to the Triple WAN ADSL2+ Firewall Router!

Once you have logged on to your BiPAC 7820NZ Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

- **Status** (Summary, WAN, Statistics, Bandwidth Usage, Route, 3G/LTE Status, Route, ARP, DHCP, VPN, Log, VRRP Status)
- **Quick Start** (Quick Start)
- **Configuration** (LAN, Wireless, WAN, System, USB, IP Tunnel, Security, Quality of Service, NAT, Wake On LAN)
- **VPN** (IPSec, VPN Account, Exceptional Rule Group, PPTP, L2TP, OpenVPN, GRE)
- **Advanced Setup** (Routing, DNS, Static ARP, UPnP, Certificate, Multicast, Management, Diagnostics)

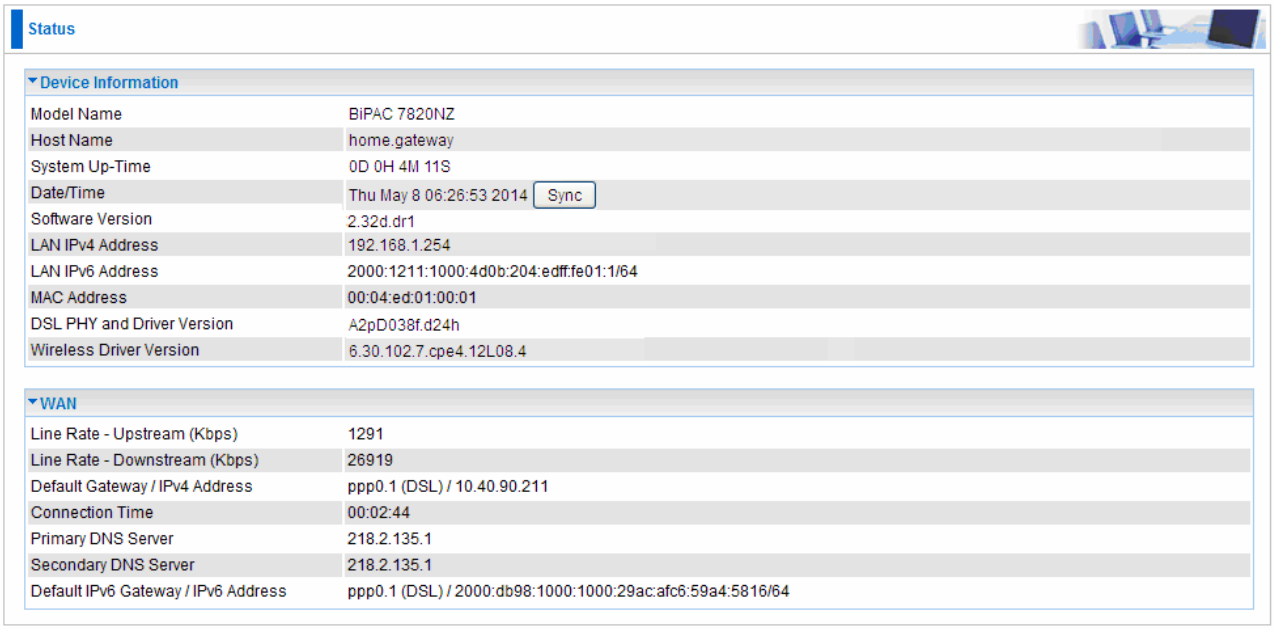
Status

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**, **3G/LTE Status**, **Route**, **ARP**, **DHCP**, **VPN**, **Log** and **VRRP Status** subsections are included.



Summary

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



Status

Device Information

Model Name	BiPAC 7820NZ
Host Name	home.gateway
System Up-Time	0D 0H 4M 11S
Date/Time	Thu May 8 06:26:53 2014 Sync
Software Version	2.32d.dr1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

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

Device Information

Model Name: Displays the model name.

Host Name: Displays the name of the router.

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

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

Software Version: Firmware version.

LAN IPv4 Address: Displays the LAN IPv4 address.

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

MAC Address: Displays the MAC address.

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

Wireless Driver Version: Displays wireless driver version.

WAN

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

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

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

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

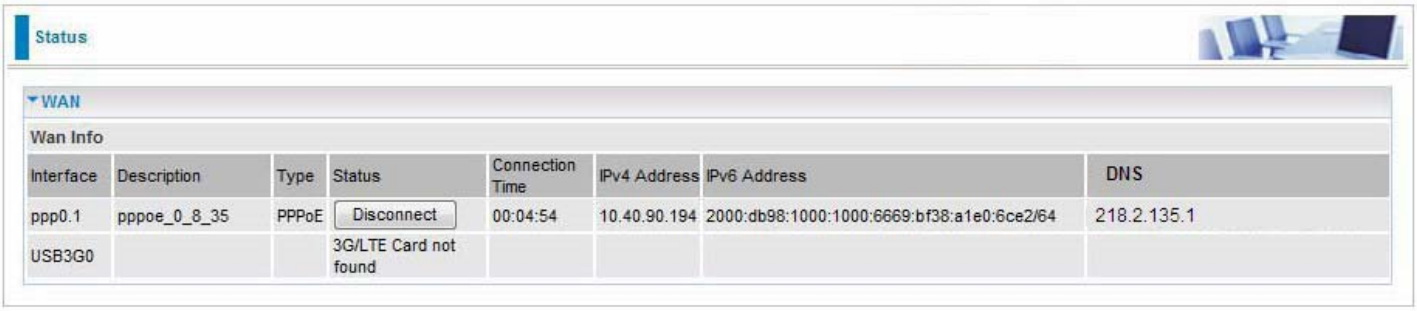
Primary DNS Server: Displays IPV4 address of Primary DNS Server.

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.



Status

WAN

Wan Info

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

Interface: The WAN connection interface.

Description: The description of this connection.

Type: The protocol used by this connection.

Status: To disconnect or connect the link.

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

IPv4 Address: The WAN IPv4 Address the device obtained.

IPv6 Address: The WAN IPv6 Address the device obtained.

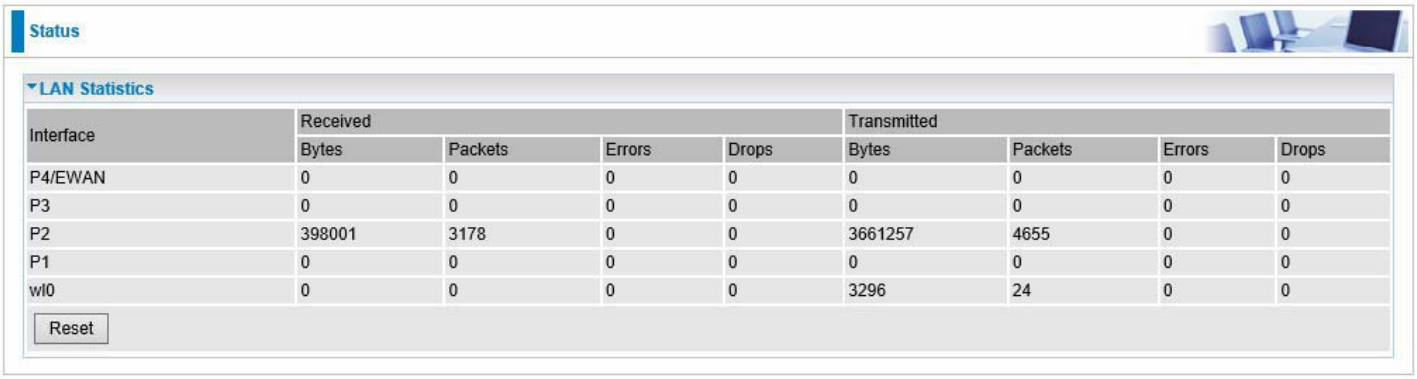
DNS: The DNS address the device obtained.

Statistics

LAN

The table shows the statistics of LAN.

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



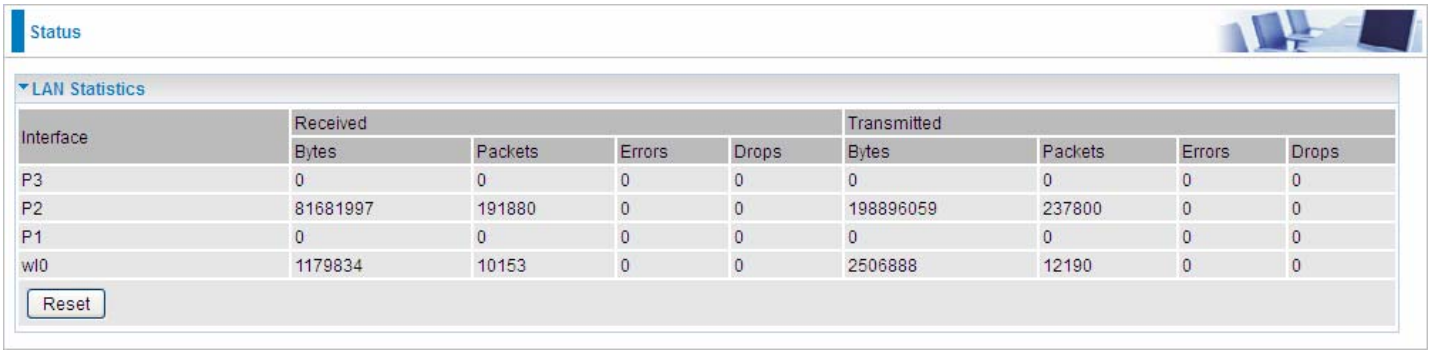
Status

LAN Statistics

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

Reset

(DSL)



Status

LAN Statistics

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

Reset

(EWAN)

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

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

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

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

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

Reset: Press this button to refresh the statistics.

WAN Service

The table shows the statistics of WAN.

Status

WAN Service

Statistics

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

Reset

Interface: Display the connection interface.

Description: the description for the connection.

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

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

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

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

Reset: Press this button to refresh the statistics.

xTM

The Statistics-xTM screen displays all the xTM statistics

Status

xTM

Interface Statistics

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

Reset

Port Number: Shows number of the port for xTM.

In Octets: Number of received octets over the interface.

Out Octets: Number of transmitted octets over the interface.

In Packets: Number of received packets over the interface.

Out Packets: Number of transmitted packets over the interface.

In OAM Cells: Number of OAM cells received.

Out OAM Cells: Number of OAM cells transmitted.

In ASM Cells: Number of ASM cells received.

Out ASM Cells: Number of ASM cells transmitted.

In Packet Errors: Number of received packets with errors.

In Cell Errors: Number of received cells with errors.

Reset: Click to reset the statistics.

xDSL

Status

xDSL

xDSL		
Mode	ADSL_2plus	
Traffic Type	ATM	
Status	Up	
Link Power State	L0	
	Downstream	Upstream
Line Coding (Trellis)	On	On
SNR Margin (dB)	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

xDSL BER Test Reset

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.

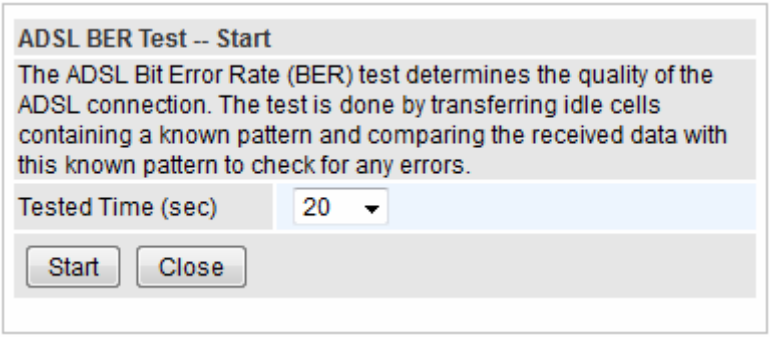
Bit Errors: Total number of bit errors.

Total ES: Total Number of Errored Seconds.

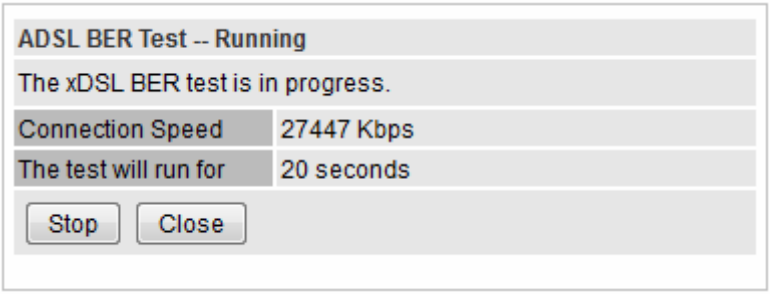
Total SES: Total Number of Severely Errored Seconds.

Total UAS: Total Number of Unavailable Seconds.

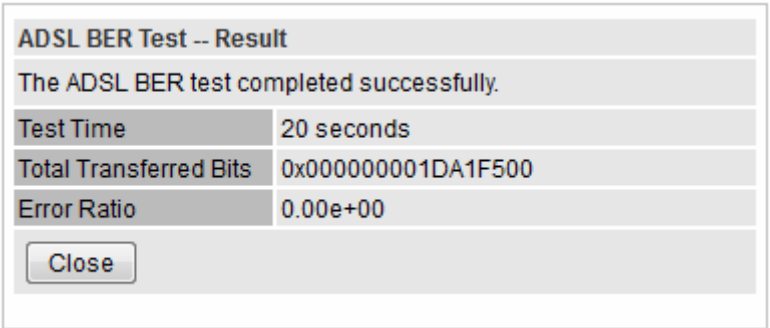
xDSL BER Test: Click this button to start a bit Error Rate Test. The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.



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



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



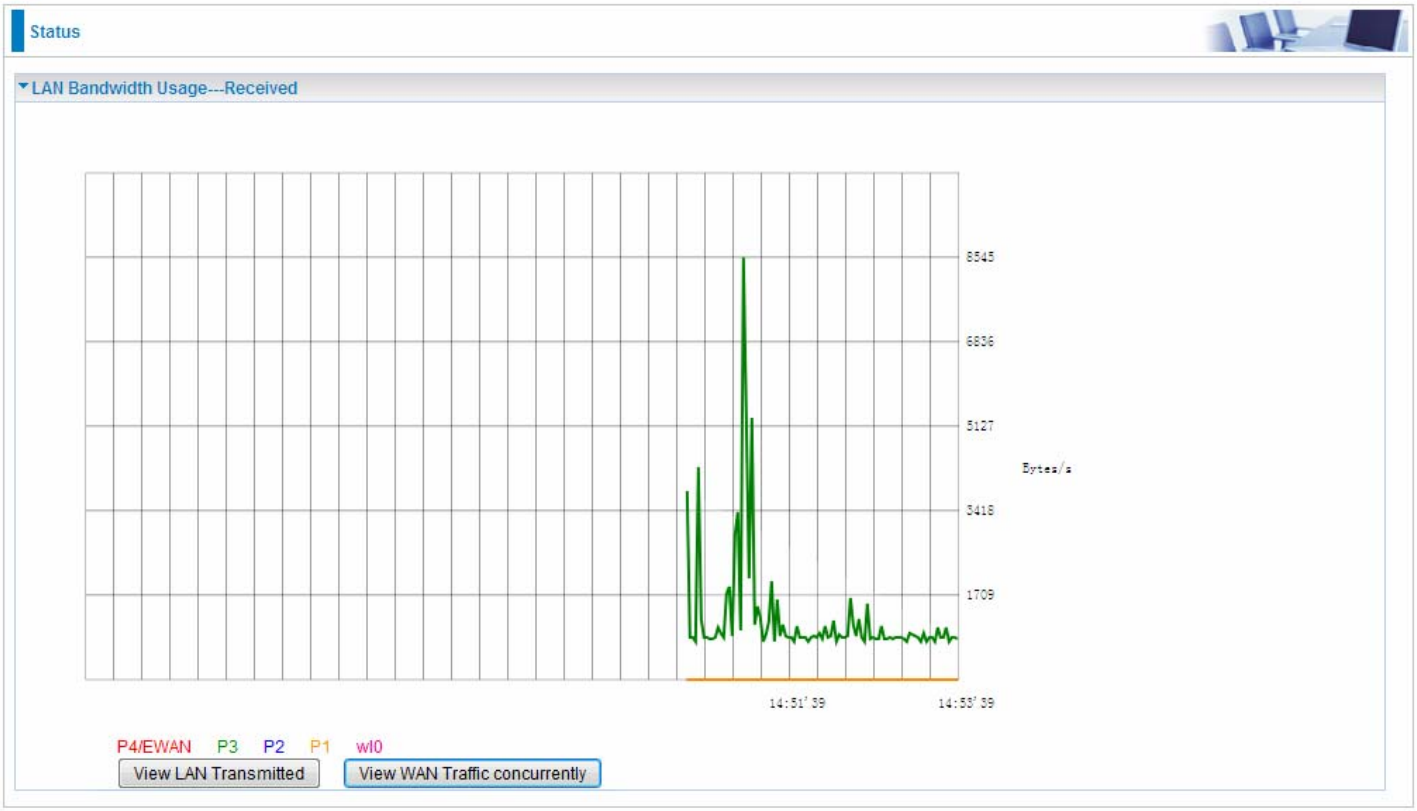
Reset: Click this button to reset the statistics.

Bandwidth Usage

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

LAN

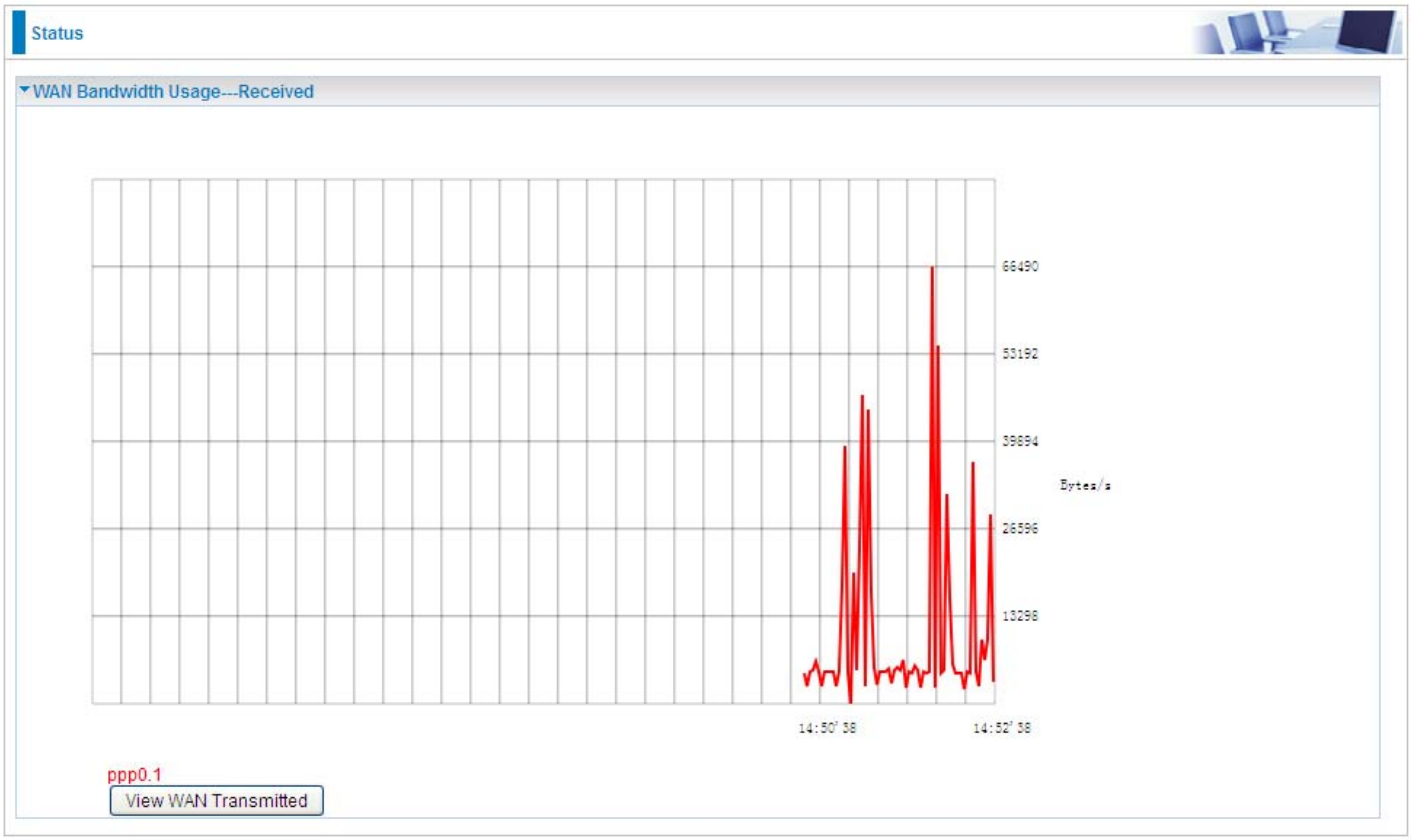
Note: P4 can be configured as EWAN, and when the device is in EWAN profile, there is no P4/EWAN interface as P4 is working as a WAN port.



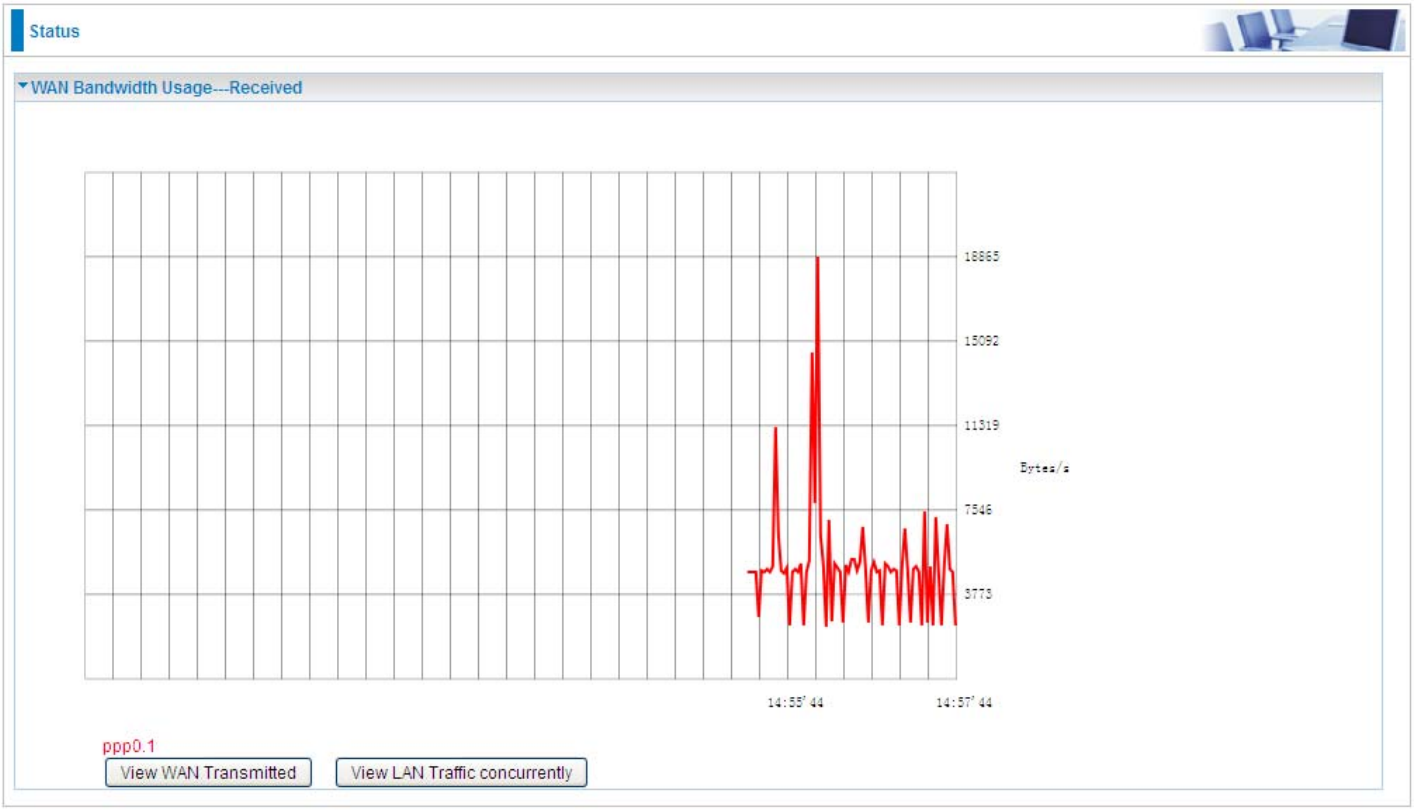
(DSL)

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

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

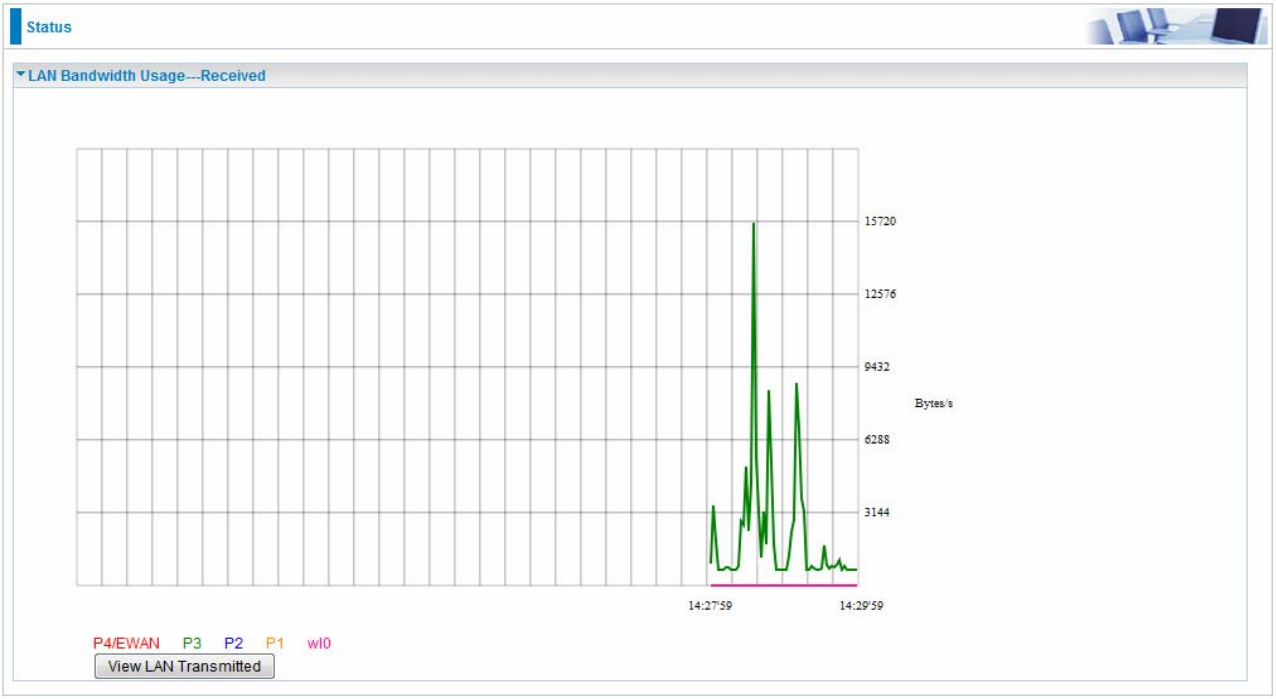


WAN Service



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

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



3G/LTE Status

Status

3G/LTE Status

Parameters	
Current SIM	SIM 1
Status	Up
Signal Strength	
Network Name	N/A
Network Mode	UMTS
Card Name	[redacted]
Card Firmware	[redacted]
Current TX Bytes / Packets	65.5K / 1K
Current RX Bytes / Packets	1.7M / 1.3K
Total TX Bytes / Packets	0.2M / 4.4K
Total RX Bytes / Packets	10.7M / 8K
Total Connection Time	00:14:55

Current SIM: The current SIM in use.

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

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

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

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

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

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

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

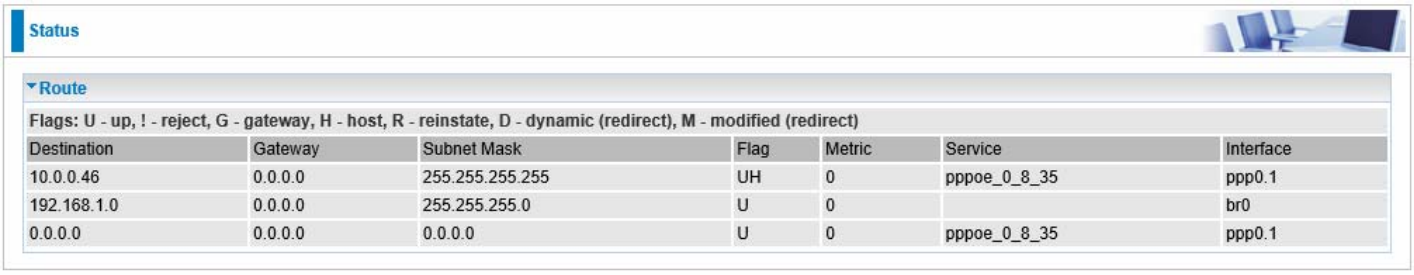
Current RX Bytes / Packets: The statistics of received Bytes / Packets, count for this call.

Total TX Bytes / Packets: The statistics of transmitted Bytes / Packets, count since 3G/LTE connection is ready.

Total RX Bytes / Packets: The statistics of received Bytes / Packets, count since 3G/LTE connection is ready.

Total Connection Time: The statistics of the connection time since 3G/LTE connection is ready.

Route



Status

Route

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

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

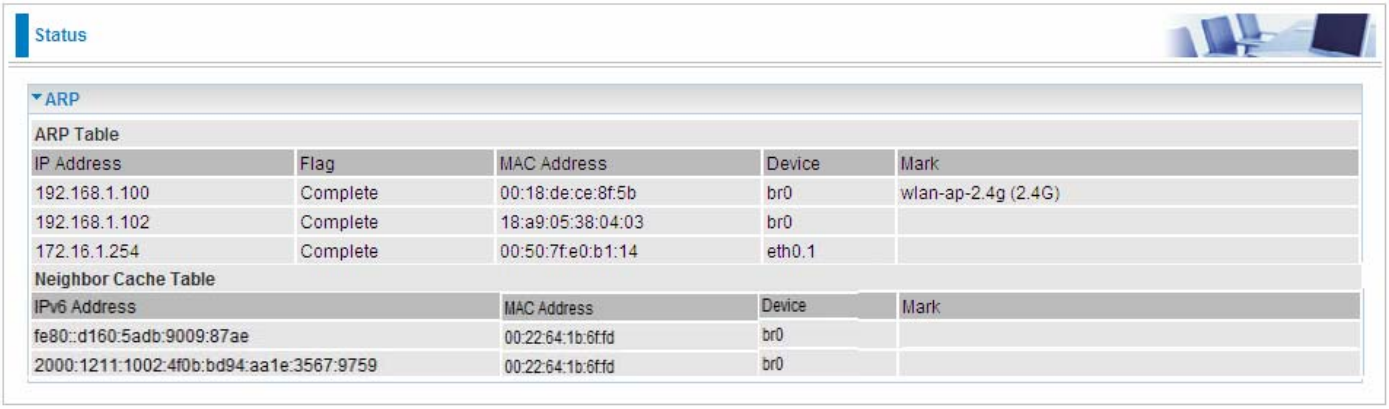
Destination: The IP address of destination network.
Gateway: The IP address of the gateway this route uses.
Subnet Mask: The destination subnet mask.
Flag: Show the status of the route.

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

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

ARP

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



ARP table

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

Flag: Shows the current status of the ARP entries.

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

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

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

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

Neighbor Cache Table

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

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

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

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

DHCP

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

Host Name	MAC Address	IP Address	Expires In	Mark
billion-17bc6f1	18:a9:05:38:04:03	192.168.1.100	18 hours, 47 minutes, 19 seconds	
ytt-PC	00:18:de:ce:8f:5b	192.168.1.101	23 hours, 59 minutes, 11 seconds	wlan-ap-2.4g

Host Name: The Host Name of DHCP client.

MAC Address: The MAC Address of DHCP client host.

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

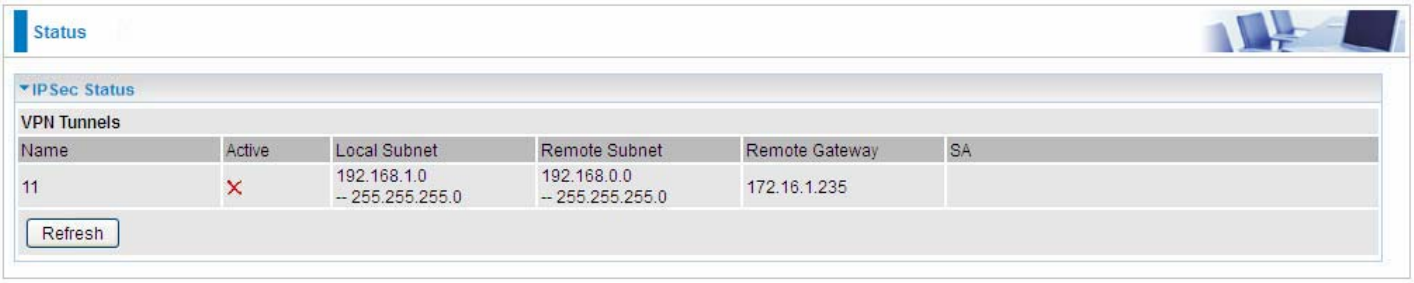
Expires in: The remaining time of the IP being available for this host.

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

VPN

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

IPSec



Name: The IPSec connection name.

Active: Display the connection status.

Local Subnet: Display the local network.

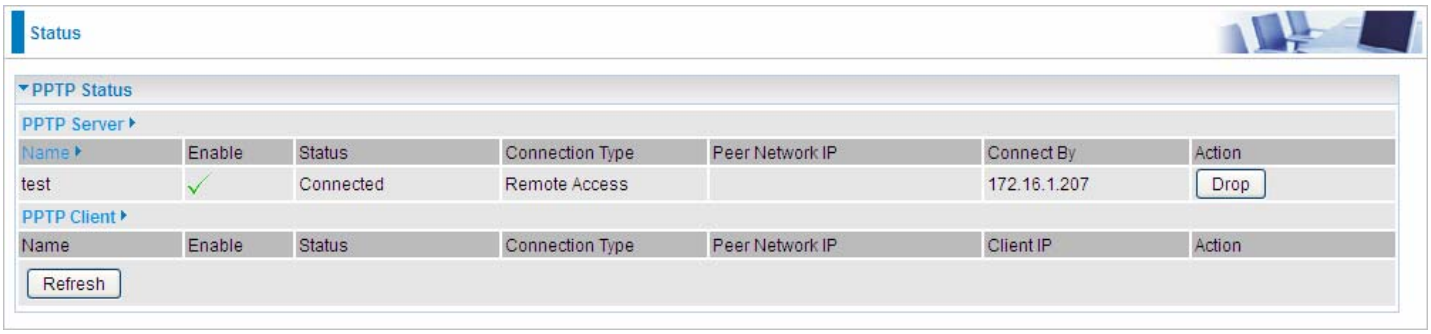
Remote Subnet: Display the remote network.

Remote Gateway: The remote gateway address.

SA: The Security Association for this IPSec entry.

Refresh: Click this button to refresh the tunnel status.

PPTP



PPTP Server

Name: The PPTP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

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

Connected By: Display the IP of remotely connected client.

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

PPTP Client

Name: The PPTP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

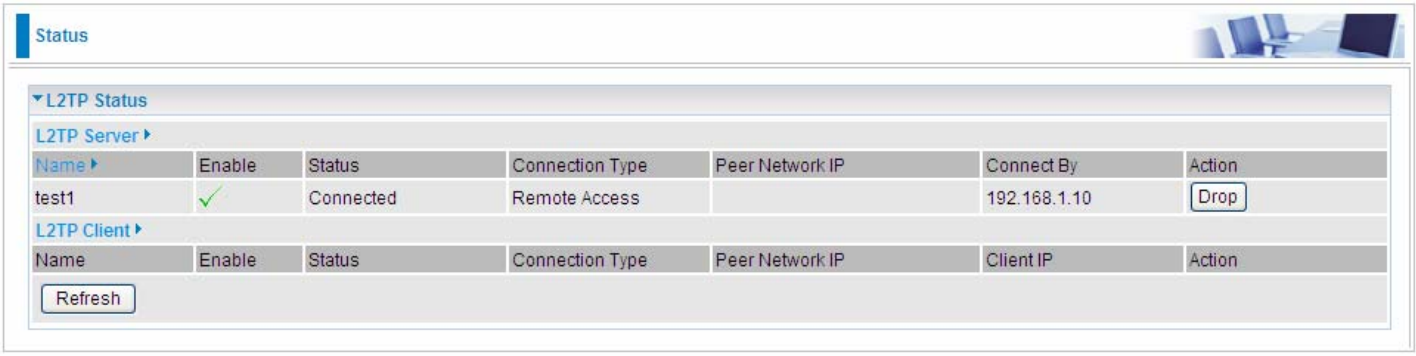
Peer Network IP: Display the remote (server side) network and subnet mask.

Client: Assigned IP by PPTP server.

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

Refresh: Click this button to refresh the connection status.

L2TP



L2TP Server

Name: The L2TP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

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

Connected By: Display the IP of remotely connected client.

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

L2TP Client

Name: The L2TP connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

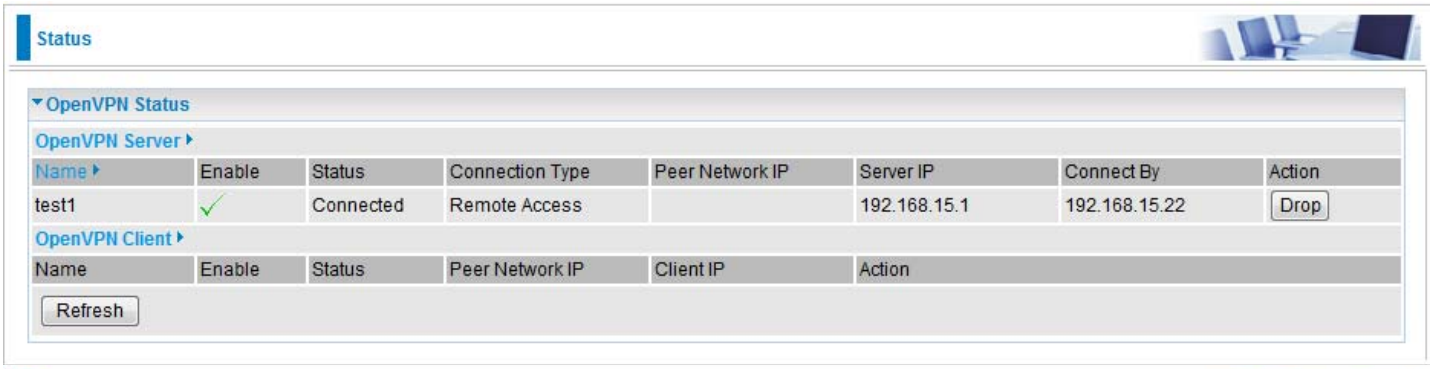
Peer Network IP: Display the network and subnet mask of server side.

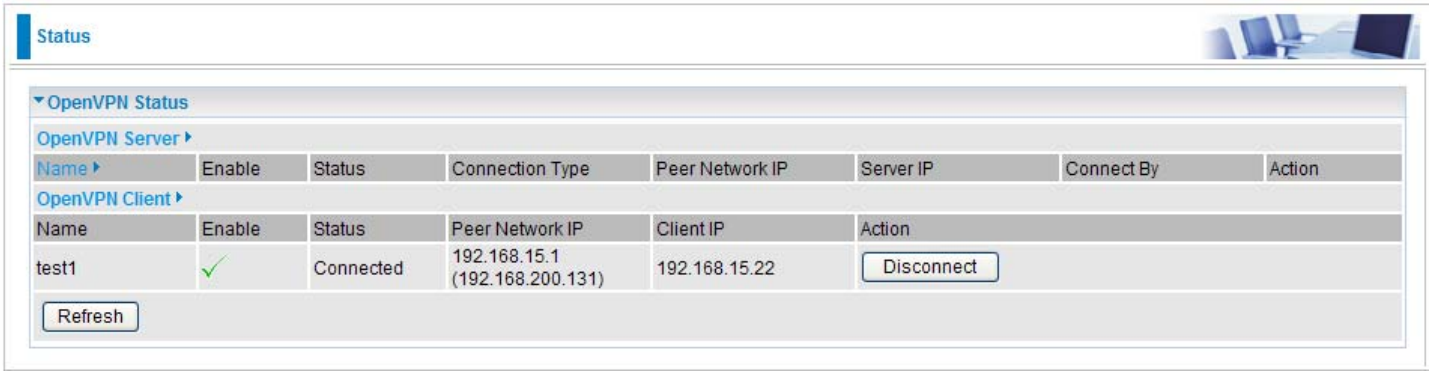
Client: Assigned IP by L2TP server.

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

Refresh: Click this button to refresh the connection status.

OpenVPN





OpenVPN Server

Name: The OpenVPN connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

Peer Network IP: Display the subnet address of client side in LAN to LAN mode.

Server IP: The tunnel virtual IP of server side assigned by server itself.

Connected By: The assigned tunnel virtual IP to remotely connected OpenVPN client.

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

OpenVPN Client

Name: The OpenVPN connection name.

Enable: Display the connection status with icon.

Status: The connection status.

Connection Type: Remote Access or LAN to LAN.

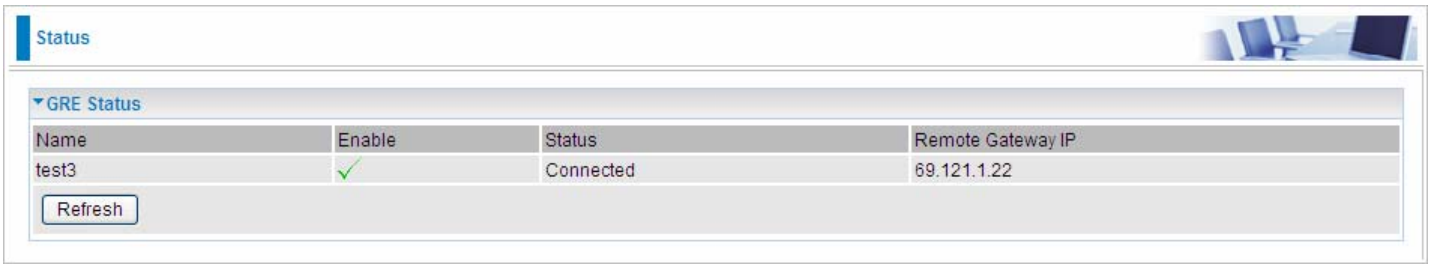
Peer Network IP: Display the tunnel virtual address (WAN address) of server side.

Client: Assigned tunnel virtual IP by OpenVPN server.

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

Refresh: Click this button to refresh the connection status.

GRE



Name: The GRE connection name.

Enable: Display the connection status with icons.

Status: The connection status, connected or disable.

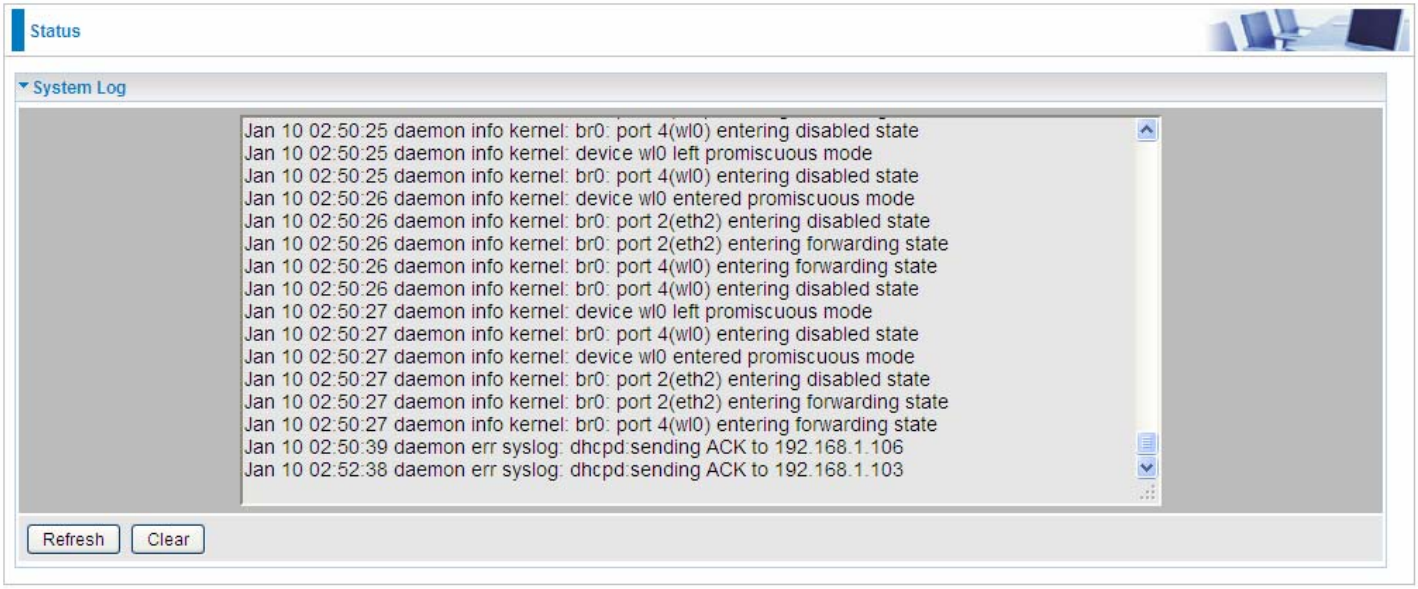
Remote Gateway: The IP of remote gateway.

Refresh: Click this button to refresh the connection status.

Log

System Log

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

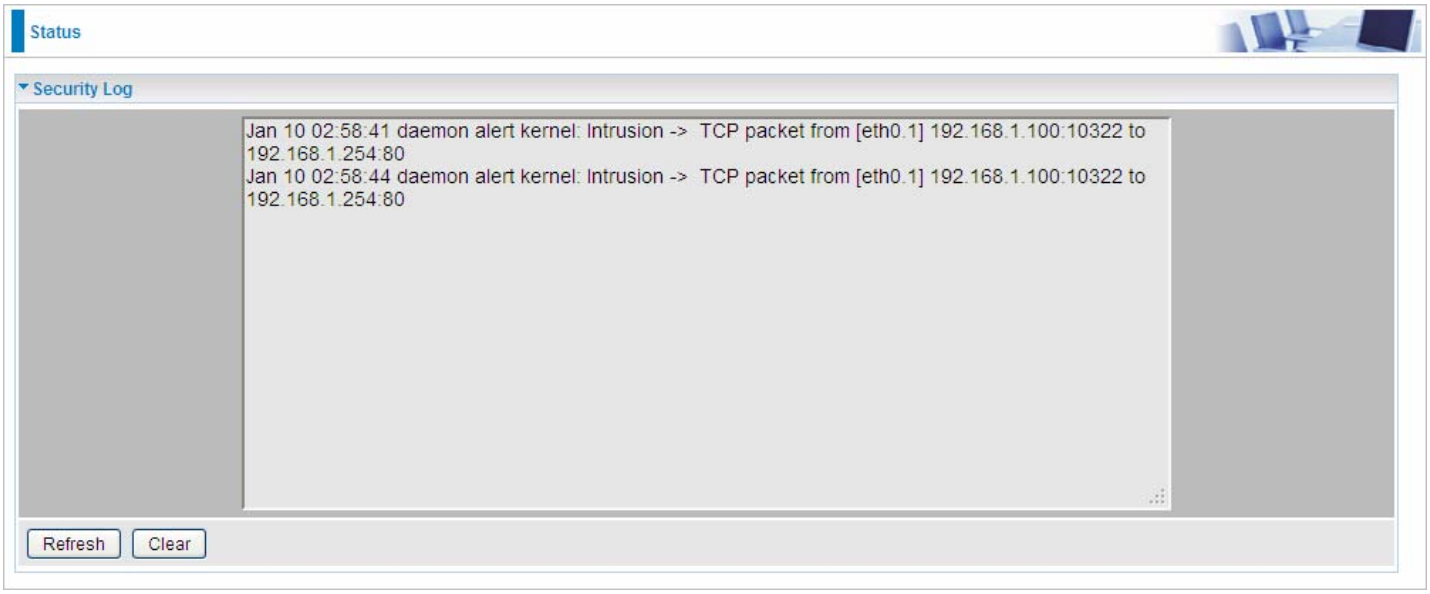


Refresh: Click to update the system log.

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.

VRRP Status

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

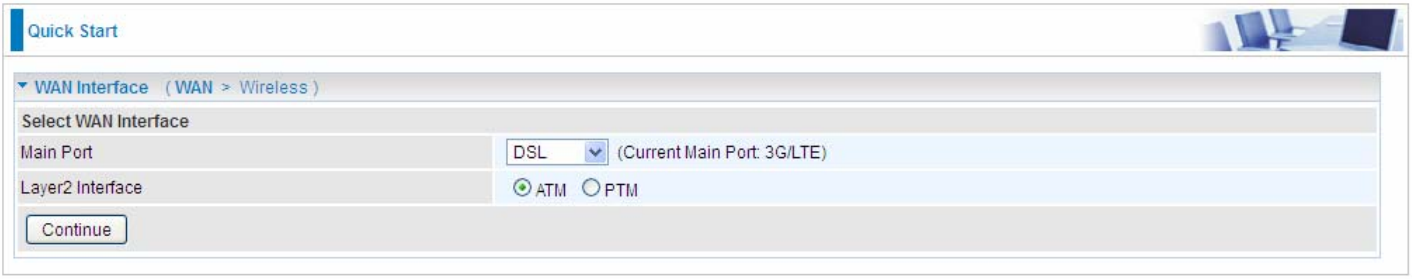
Current Master: Show the IP address of current master.

Quick Start

Quick Start

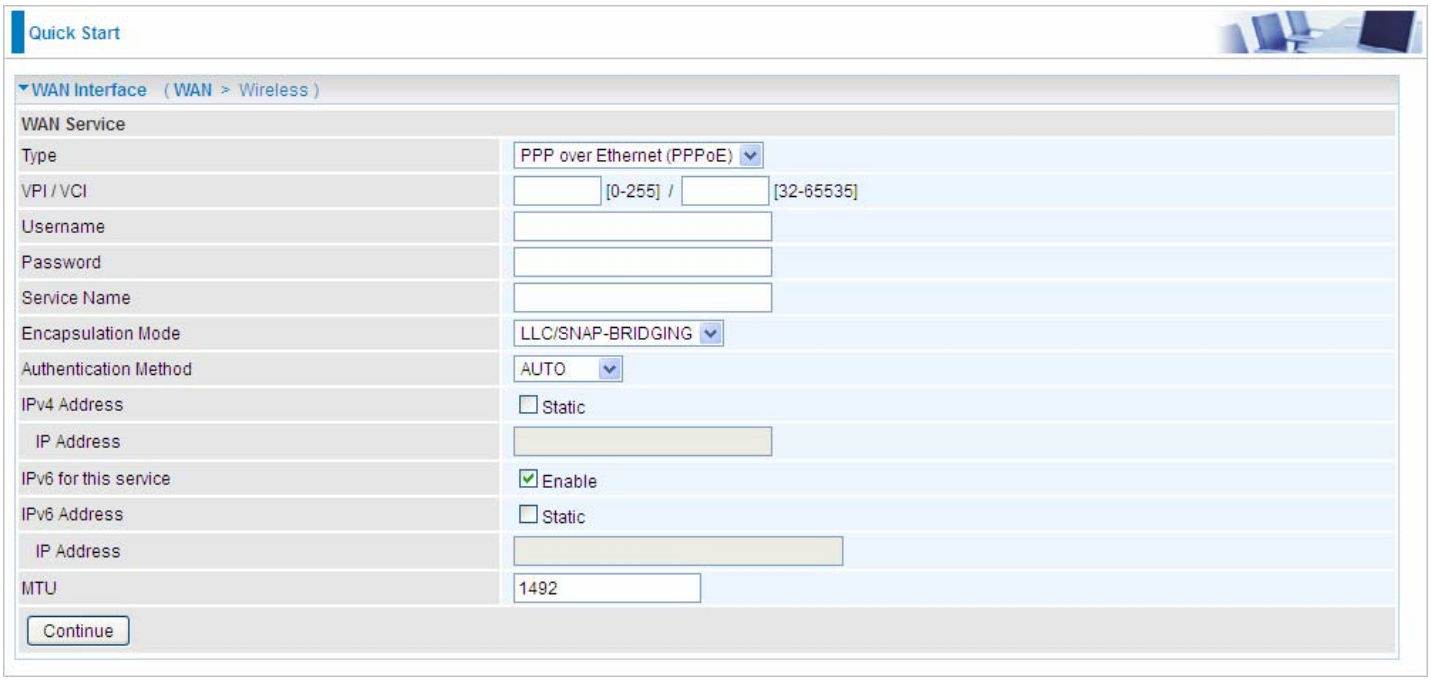
This part allows you to quickly configure and connect your router to internet.

DSL mode



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

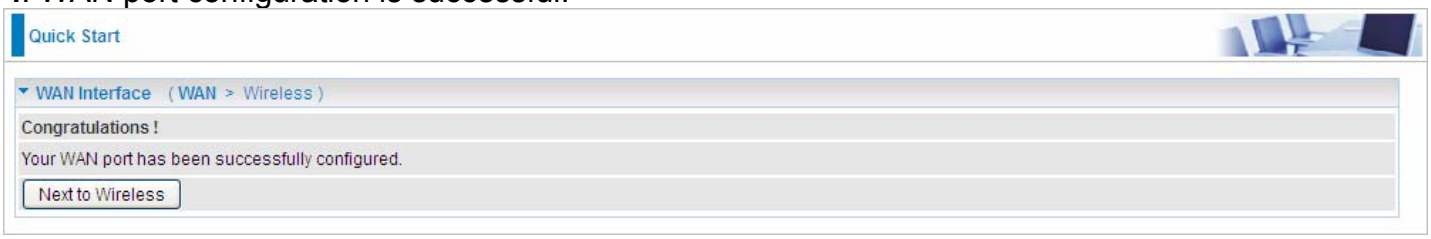
2. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.



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

3. Wait while the device is configured.

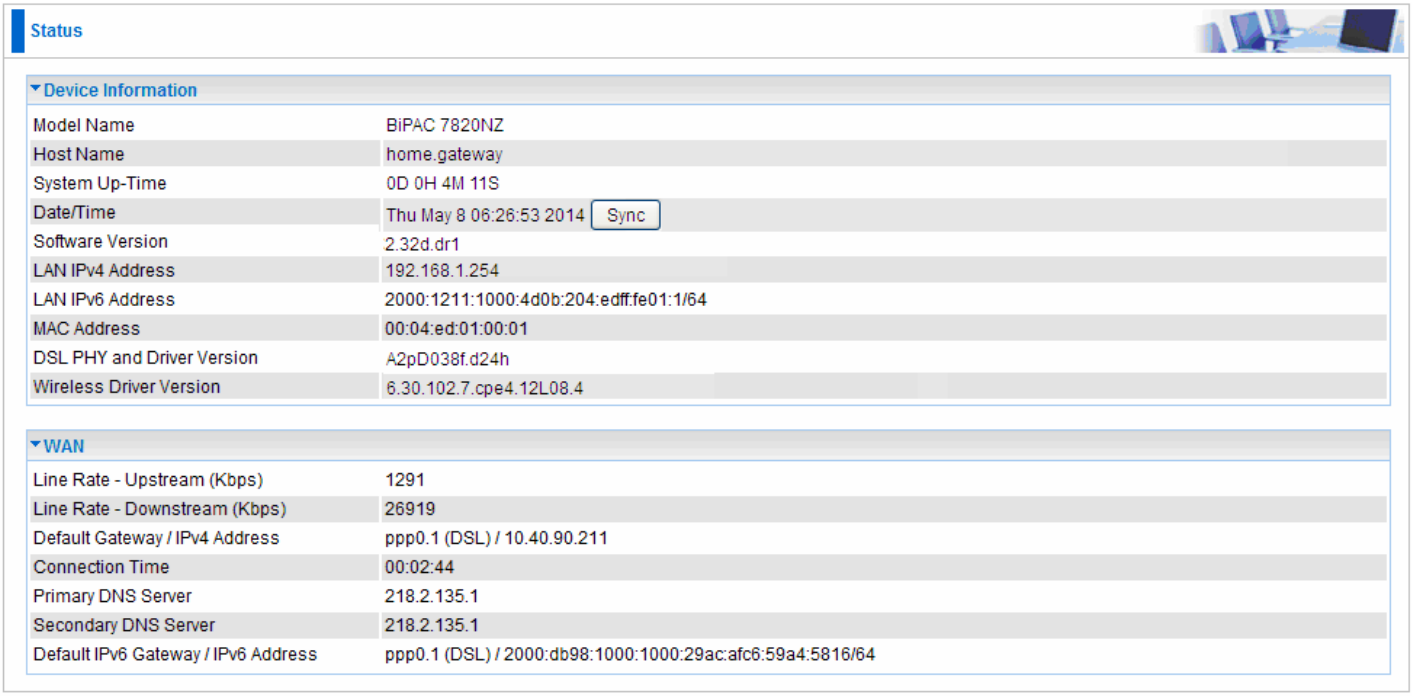
4. WAN port configuration is successful.



5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

6. Success.

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



Status

Device Information

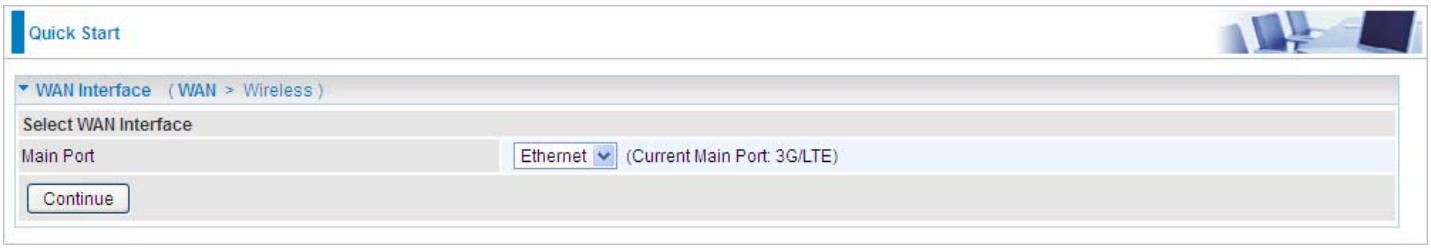
Model Name	BiPAC 7820NZ
Host Name	home.gateway
System Up-Time	0D 0H 4M 11S
Date/Time	Thu May 8 06:26:53 2014 Sync
Software Version	2.32d.dr1
LAN IPv4 Address	192.168.1.254
LAN IPv6 Address	2000:1211:1000:4d0b:204:edff:fe01:1/64
MAC Address	00:04:ed:01:00:01
DSL PHY and Driver Version	A2pD038f.d24h
Wireless Driver Version	6.30.102.7.cpe4.12L08.4

WAN

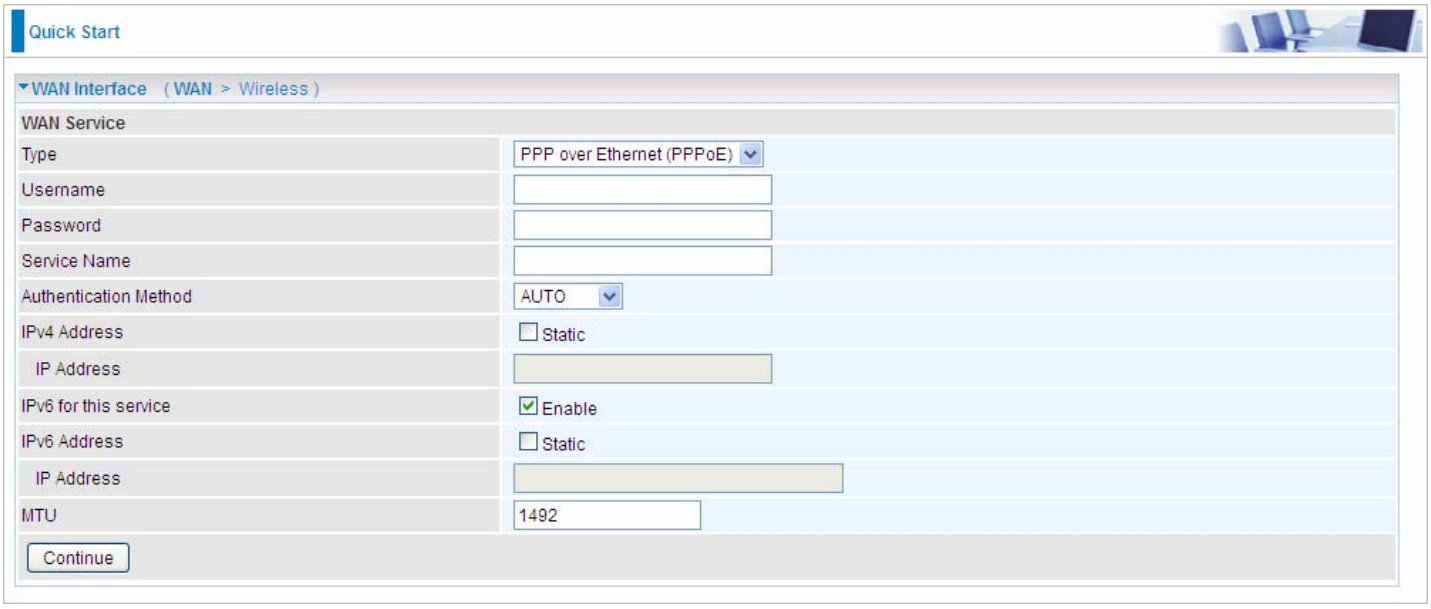
Line Rate - Upstream (Kbps)	1291
Line Rate - Downstream (Kbps)	26919
Default Gateway / IPv4 Address	ppp0.1 (DSL) / 10.40.90.211
Connection Time	00:02:44
Primary DNS Server	218.2.135.1
Secondary DNS Server	218.2.135.1
Default IPv6 Gateway / IPv6 Address	ppp0.1 (DSL) / 2000:db98:1000:1000:29ac:afc6:59a4:5816/64

Ethernet mode

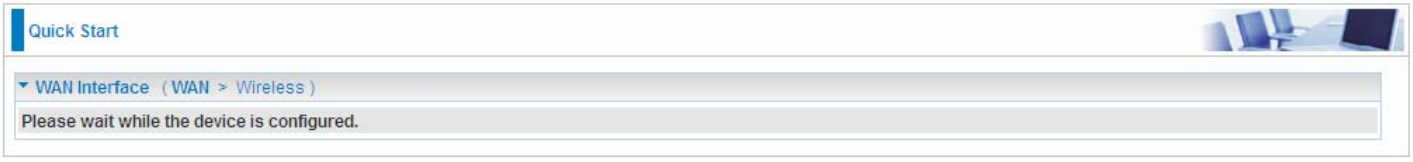
1. Select **Ethernet,** press **Continue** to go on to next step.



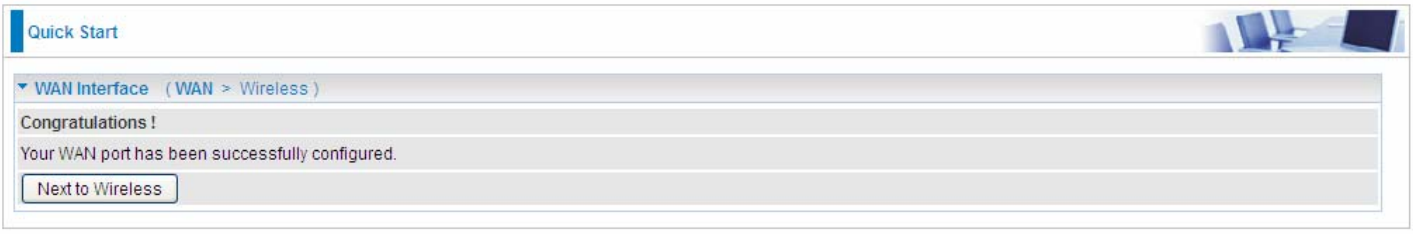
2. Enter the username, password from your ISP, for IP and DNS settings; also refer to your ISP. Here IPv6 service is enabled by default.



3. Wait while the device is configured.



4. WAN port configuration is successful.

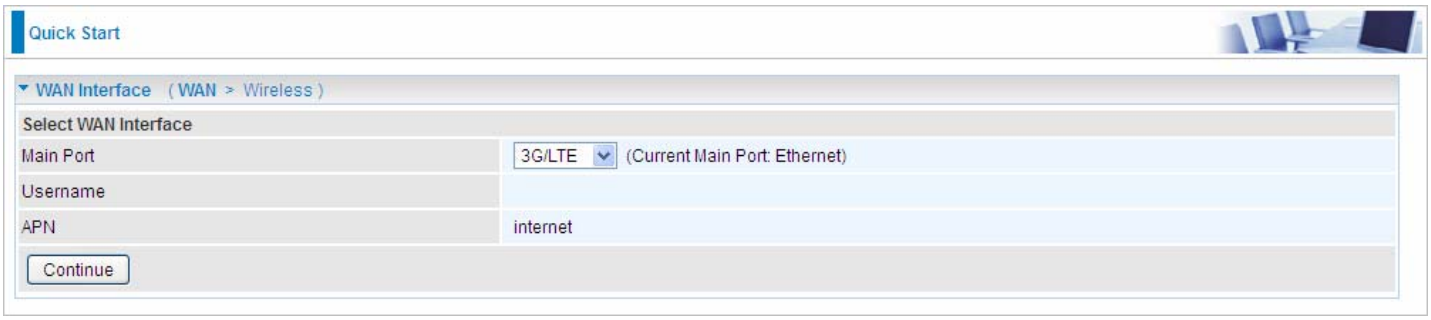


5. After the configuration is successful, click **Next to Wireless** button and you may proceed to configure the Wireless setting. Enable wireless and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

6. Success.

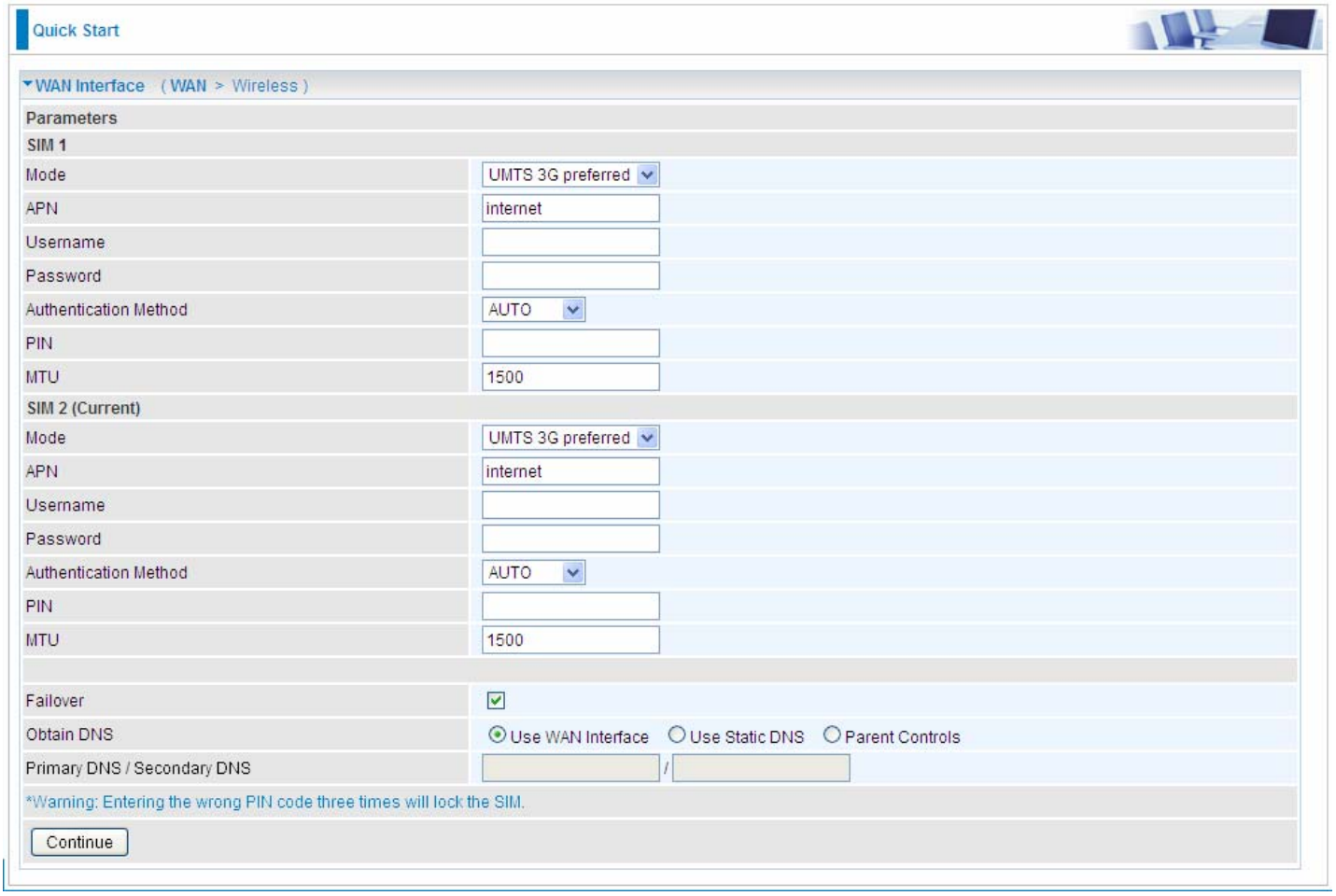
3G/LTE

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



2. Select the 3G/LTE mode, and enter the APN, username, password from your ISP; and check with your ISP with the authentication method setting for each SIM (SIM1 and SIM2).

Note: Given that BiPAC 7820NZ supports dual -SIM mobile connectivity, please determine which SIM you are gonna use or both (3G/LTE failover), and set the exact required connecting information for each SIM (SIM1 and SIM2).



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. Enable wireless and set the SSID and encryption Key (1. Leave it empty to disable the wireless security; 2. Fill in the Key, and the encryption mode will be WPA2-PSK/AES).

6. Success.

Configuration

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

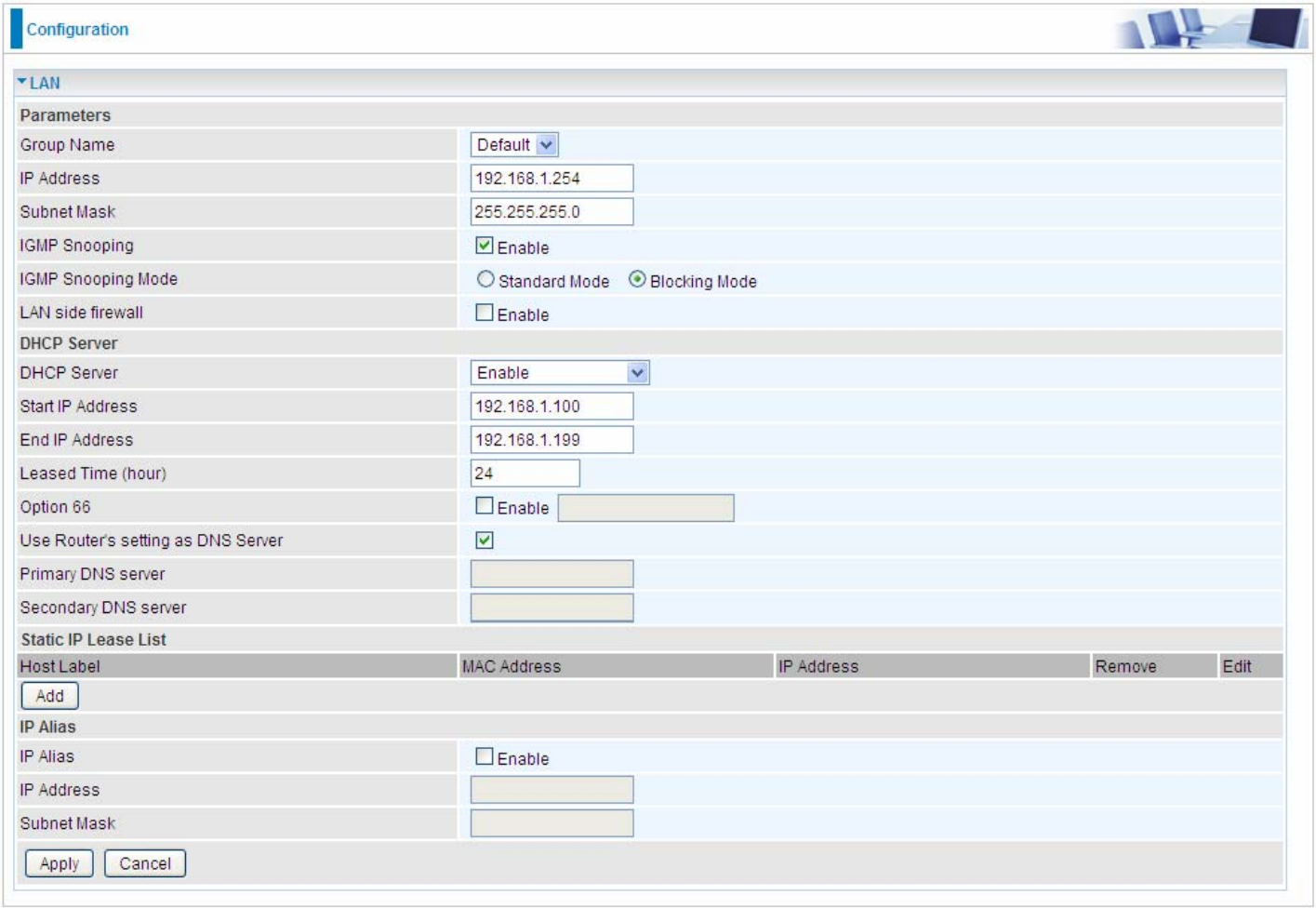
LAN, **Wireless**, **WAN**, **System**, **USB**, **IP Tunnel**, **Security**, **Quality of Service**, **NAT** and **Wake On LAN**.

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



Parameters

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

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

Subnet Mask: the default Subnet mask on the router.

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

When enabled, you will see two modes:

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

LAN side firewall: Enable to drop all traffic from the specified LAN group interface. After activating it,

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

DHCP Server

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

ⓘ Disable

DHCP Server	
DHCP Server	Disable

Disable the DHCP Server function.

ⓘ Enable

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

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

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

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

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

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

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

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

ⓘ DHCP Server Relay

DHCP Server	
DHCP Server	DHCP Server Relay
DHCP Server IP Address	

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

Static IP List

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

Static IP Lease List

Host Label	MAC Address	IP Address	Remove	Edit

Add

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

Configuration

Static IP

Parameters

Host Label	
MAC Address	
IP Address	

Apply Cancel

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

Static IP Lease List

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

IP Alias

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

IP Alias

IP Alias	☐ Enable
IP Address	
Subnet Mask	

Apply Cancel

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.

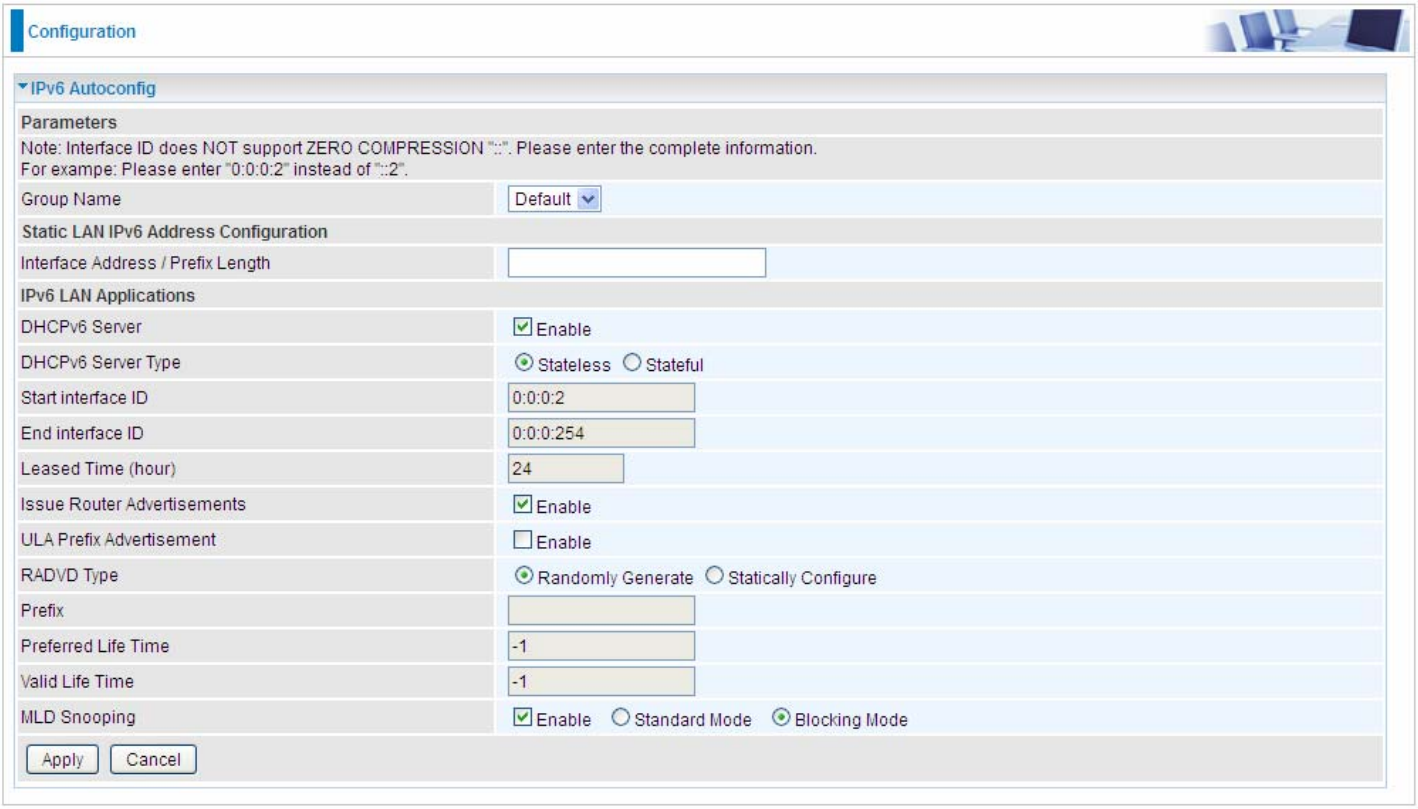
Click **Apply** to apply your settings.

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.



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

Static LAN IPv6 Address Configuration

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

IPv6 LAN application

DHCPv6 Server: Check whether to enable DHCPv6 server.

DHCPv6 Server Type: Select Stateless or Stateful. When DHCPv6 is enabled, this parameter is

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

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

End interface ID: Enter the end interface ID.

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

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

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

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

RADVD Type: The way that ULA prefix is generated.

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

Prefix: Set the prefix manually.

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

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

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

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

Stateless and Stateful IPv6 address Configuration

Stateless: Two methods can be carried.

ⓘ With DHCPv6 disabled, but Issue Router Advertisement Enabled

DHCPv6 Server	☐ Enable
Issue Router Advertisements	☑ Enable

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

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled

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

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

Stateful: two methods can be adopted.

ⓘ With only DHCPv6 enabled

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

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

ⓘ With both DHCPv6 and Issue Router Advertisement Enabled

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

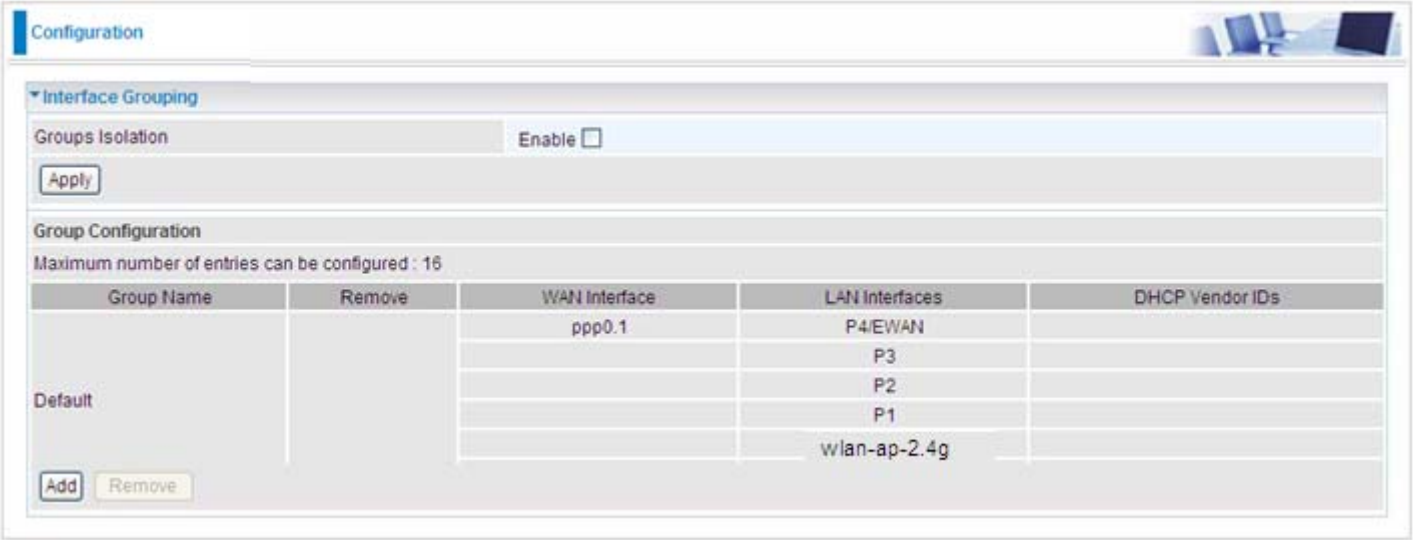
With this method, the PCs' addresses are configured the same like above, and the address information in RA packets will be neglected.

Interface Grouping

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

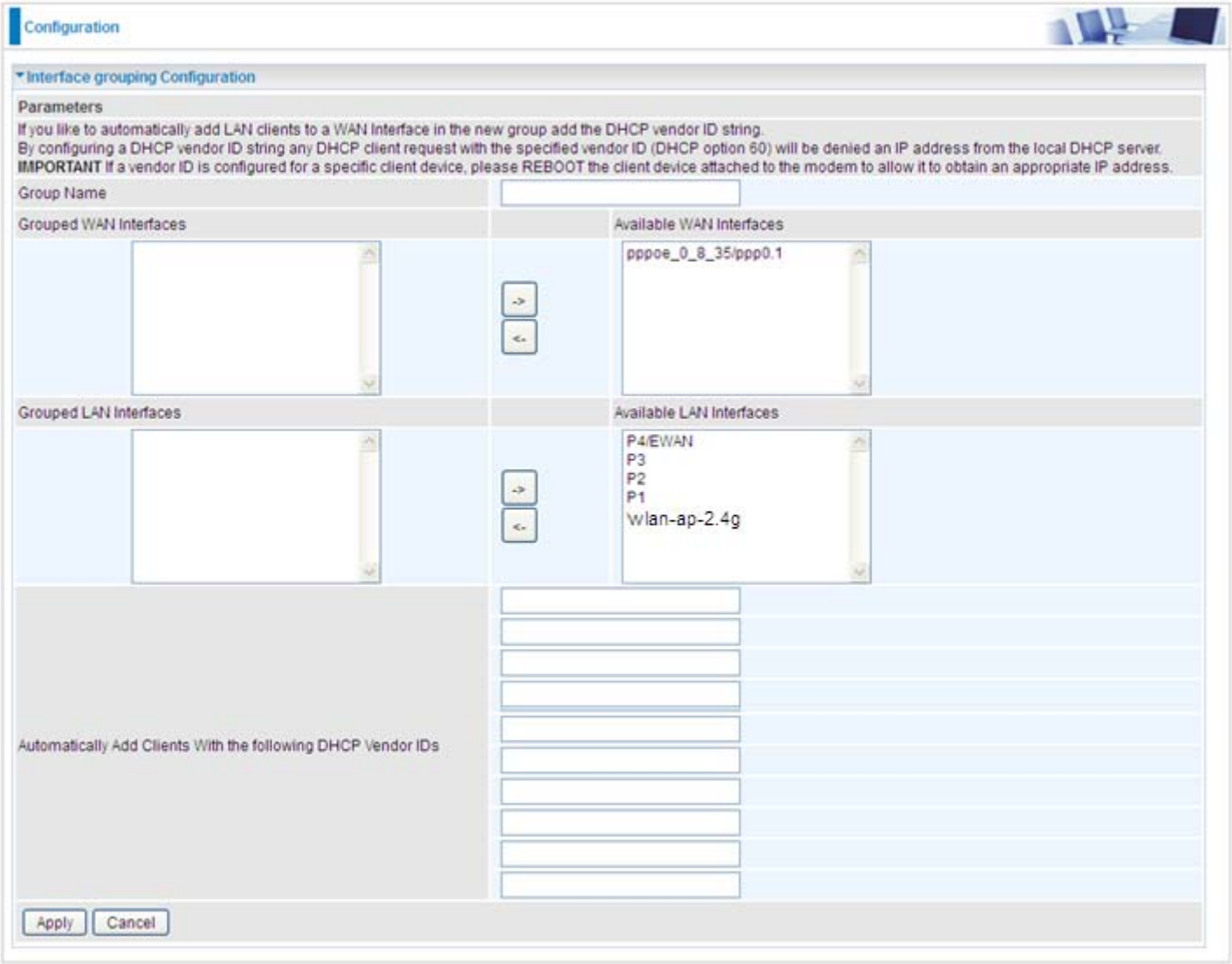
Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button.

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



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

Click **Add** to add groups.



Group Name: Type a group name.

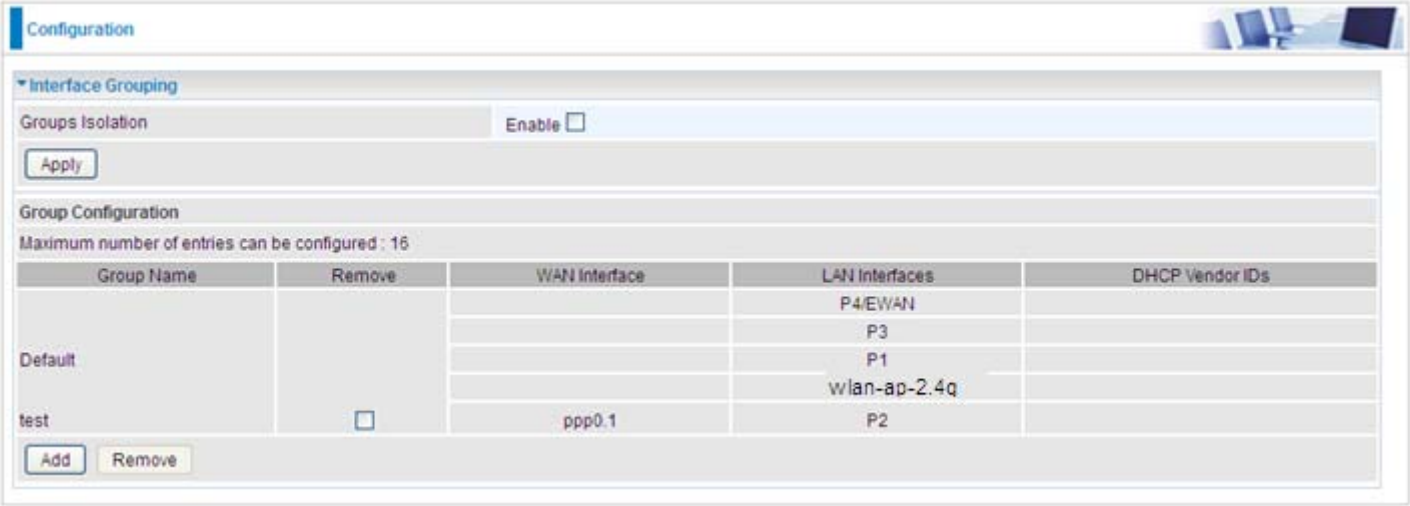
Grouped WAN Interfaces: Select from the box the WAN interface you want to applied in the group.

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

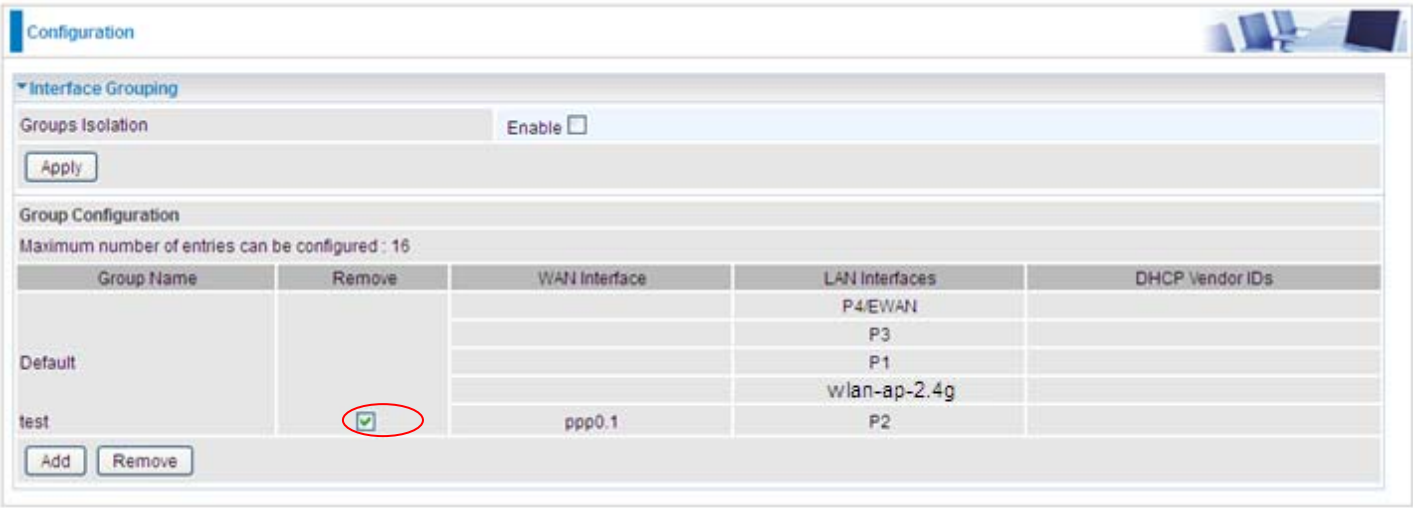
Automatically Add Clients with following DHCP Vendor IDs: Enter the DHCP Vendor IDs for which you want the Clients automatically added into the group. DHCP vendor ID (DHCP 60) is an Authentication for DHCP Messages.

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**.



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



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

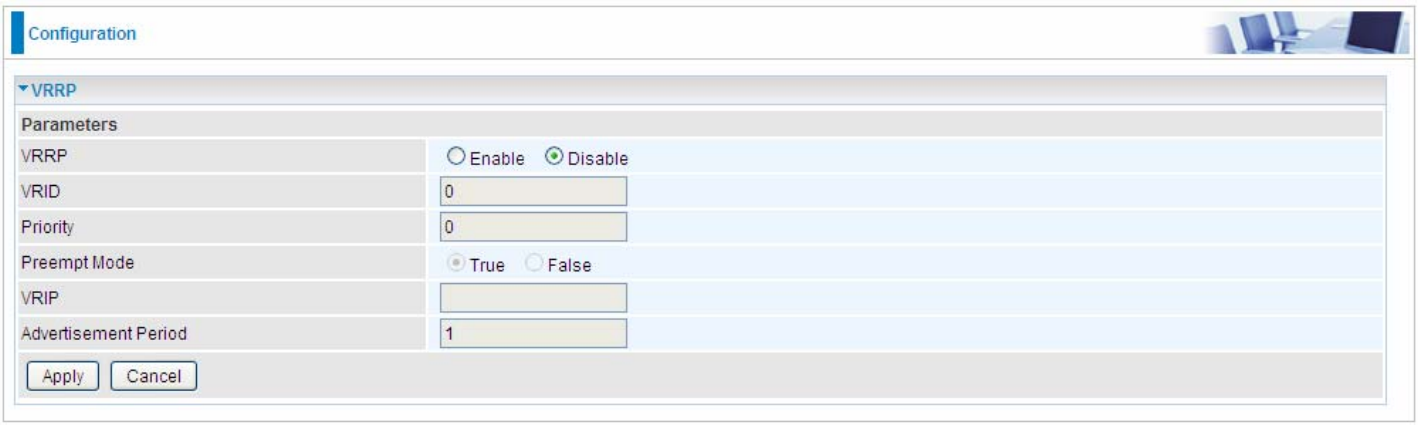
By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

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

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

VRRP

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



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

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

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

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

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

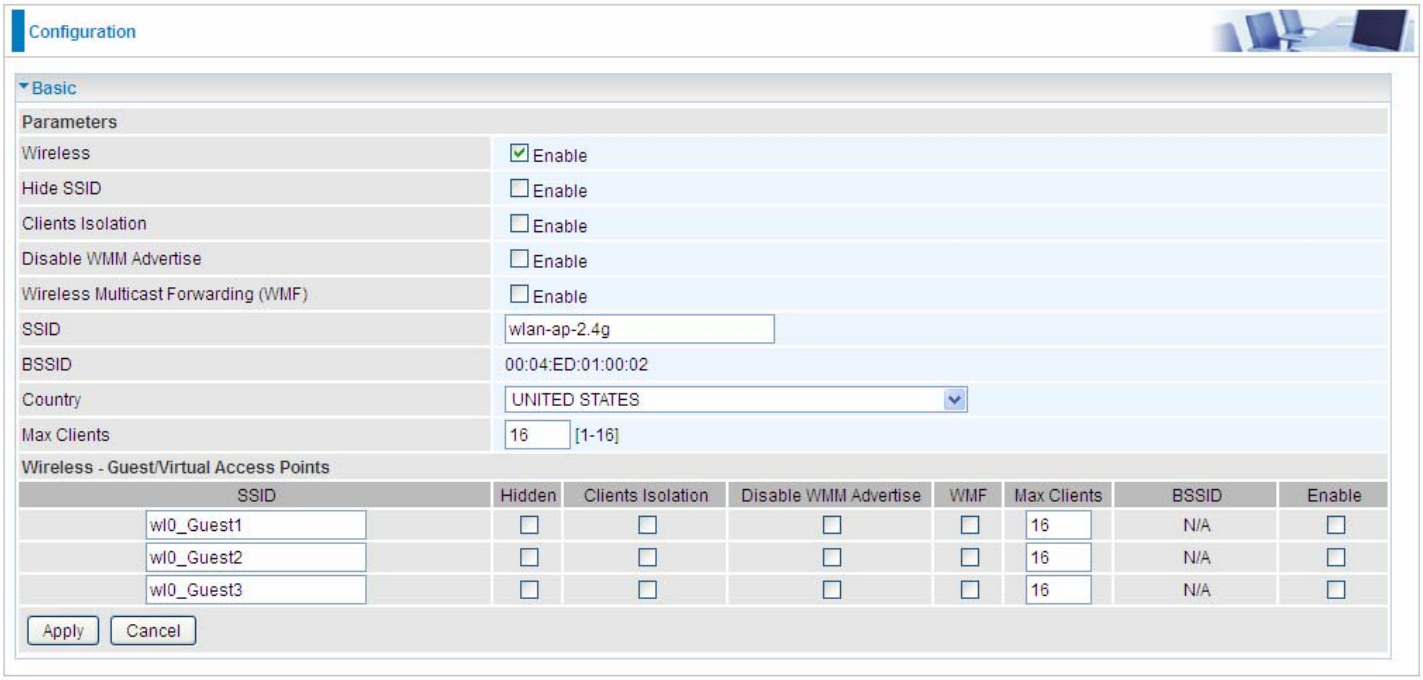
Advertisement period: Indicates the time interval in seconds between advertisements. The default value is 1 second.

Wireless

This section provides you ways to configure wireless access. The BiPAC 7820NZ supports wireless on the 2.4GHz for users. This part has sub-items as **Basic**, **Security**, **MAC Filter**, **Wireless Bridge**, **Advanced** and **Station Info** here.

Basic

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



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

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

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

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

Check to disable or enable this function.

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

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

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

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

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

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

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

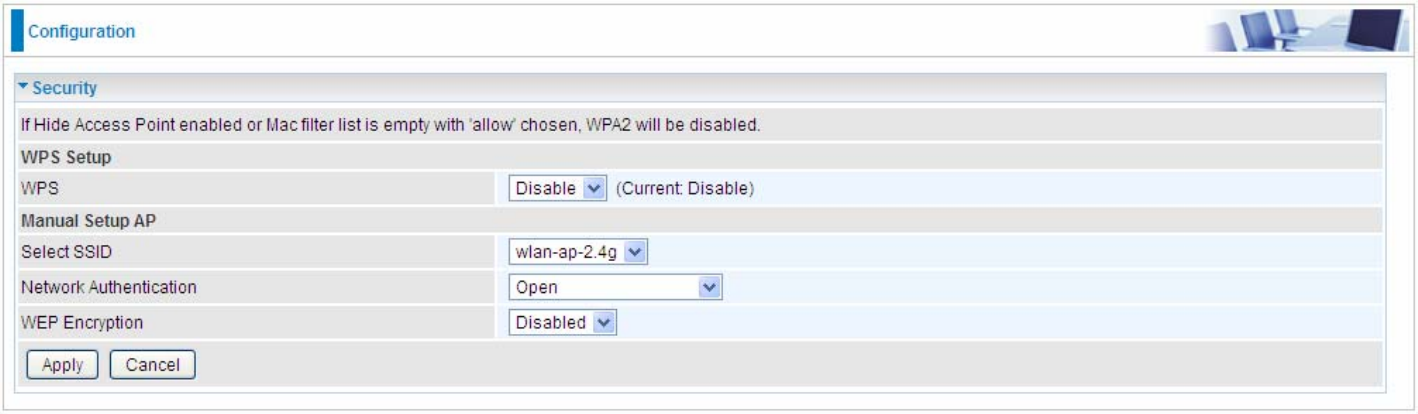
simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

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

Click **Apply** to apply your settings.

Security

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



Note:

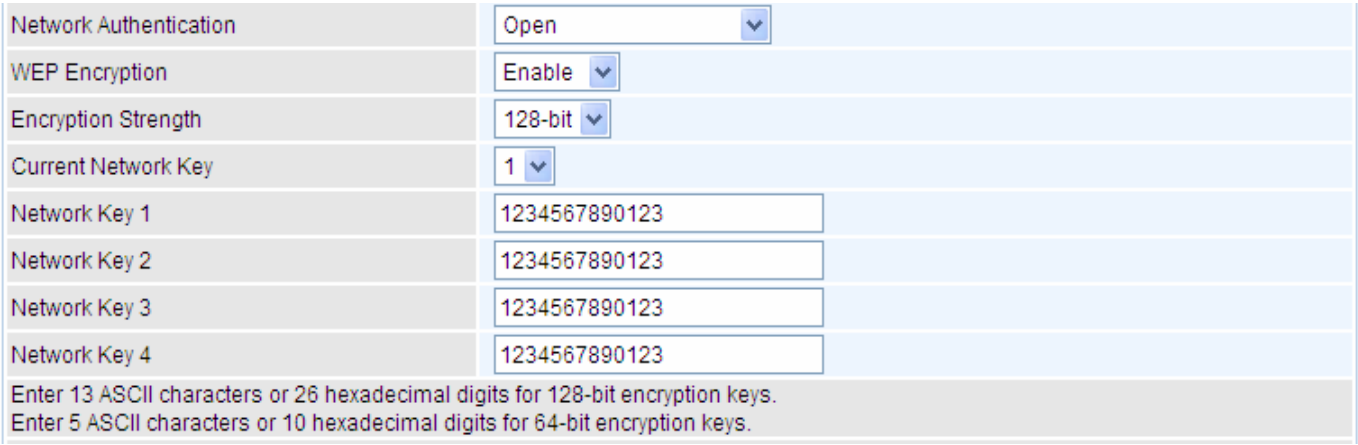
The WPS feature will also be unavailable when the security setting is not WPA2 or OPEN. So, if you manually set the wireless security setting, you should give notice to it, but you can find prompt indicating configuration.

Manual Setup AP

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

Network Authentication

ⓘ **Open**



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

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

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

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

ⓘ Shared

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

Network Authentication	Shared
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.	

ⓘ 802.1x

Network Authentication	802.1X
RADIUS Server IP Address	0.0.0.0
RADIUS Port	1812
RADIUS Key	
WEP Encryption	Enable
Encryption Strength	128-bit
Current Network Key	2
Network Key 1	1234567890123
Network Key 2	1234567890123
Network Key 3	1234567890123
Network Key 4	1234567890123
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.	

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

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

RADIUS Key: Enter the password of RADIUS authentication server.

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

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

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

ⓘ WPA

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

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

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

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

RADIUS Key: Enter the password of RADIUS authentication server.

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

ⓘ WPA-PSK / WPA2-PSK

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

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

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

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

ⓘ WPA2

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

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

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

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

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

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

RADIUS Key: Enter the password of RADIUS authentication server.

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

ⓘ Mixed WPA2/WPA

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

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

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

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

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

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

RADIUS Key: Enter the password of RADIUS authentication server.

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

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

ⓘ Mixed WPA2/WPA-PSk

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

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

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

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

WPS Setup

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

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

Note:

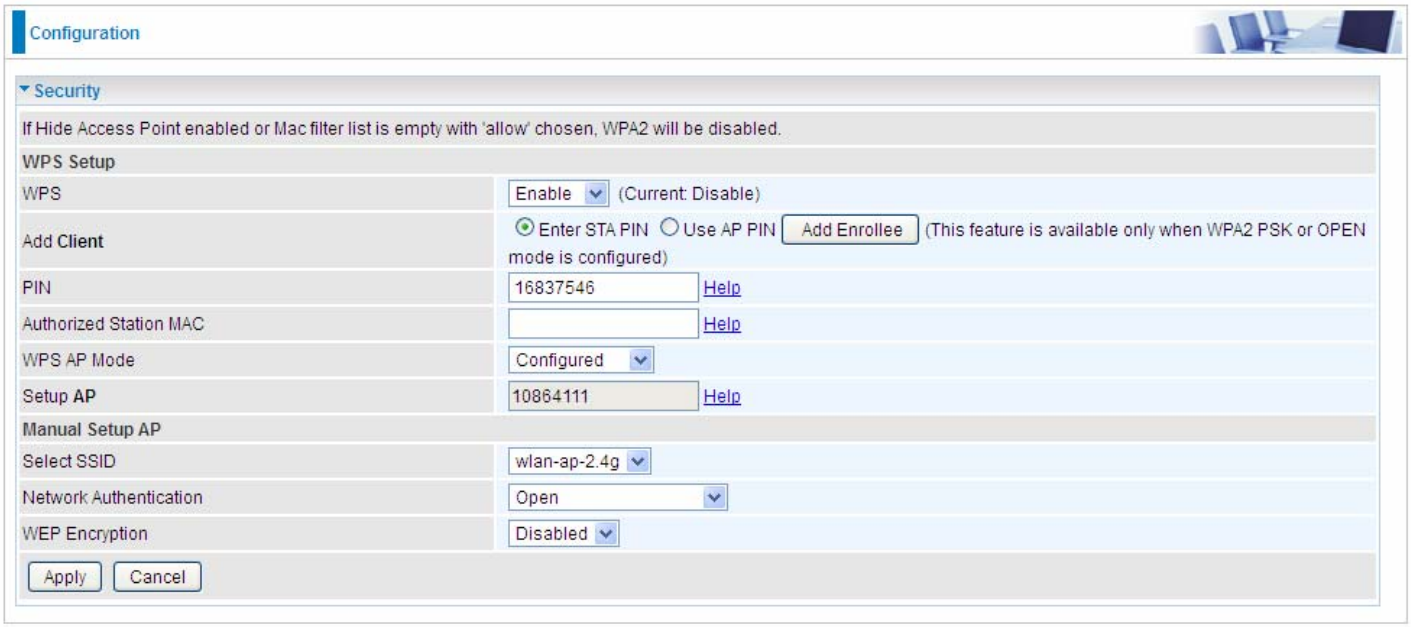
1) WPS feature is only available when in WPA2 or OPEN mode in security settings.

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

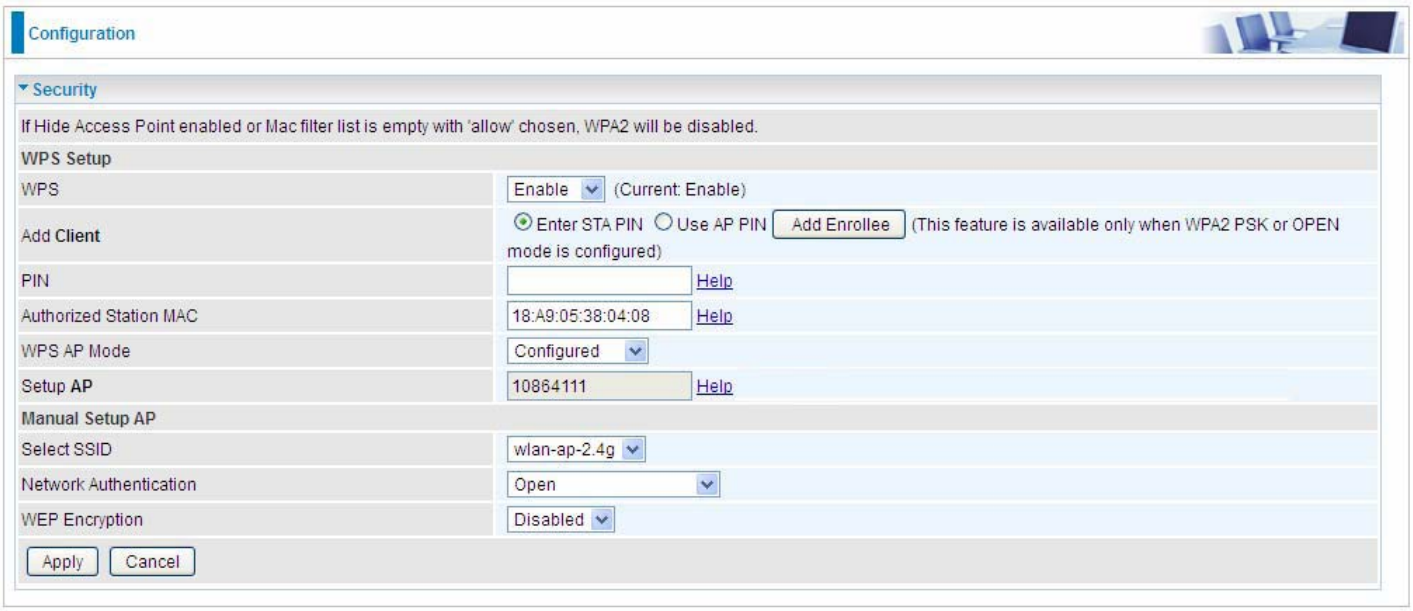
Configure AP as Registrar

Add Enrollee with PIN method

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



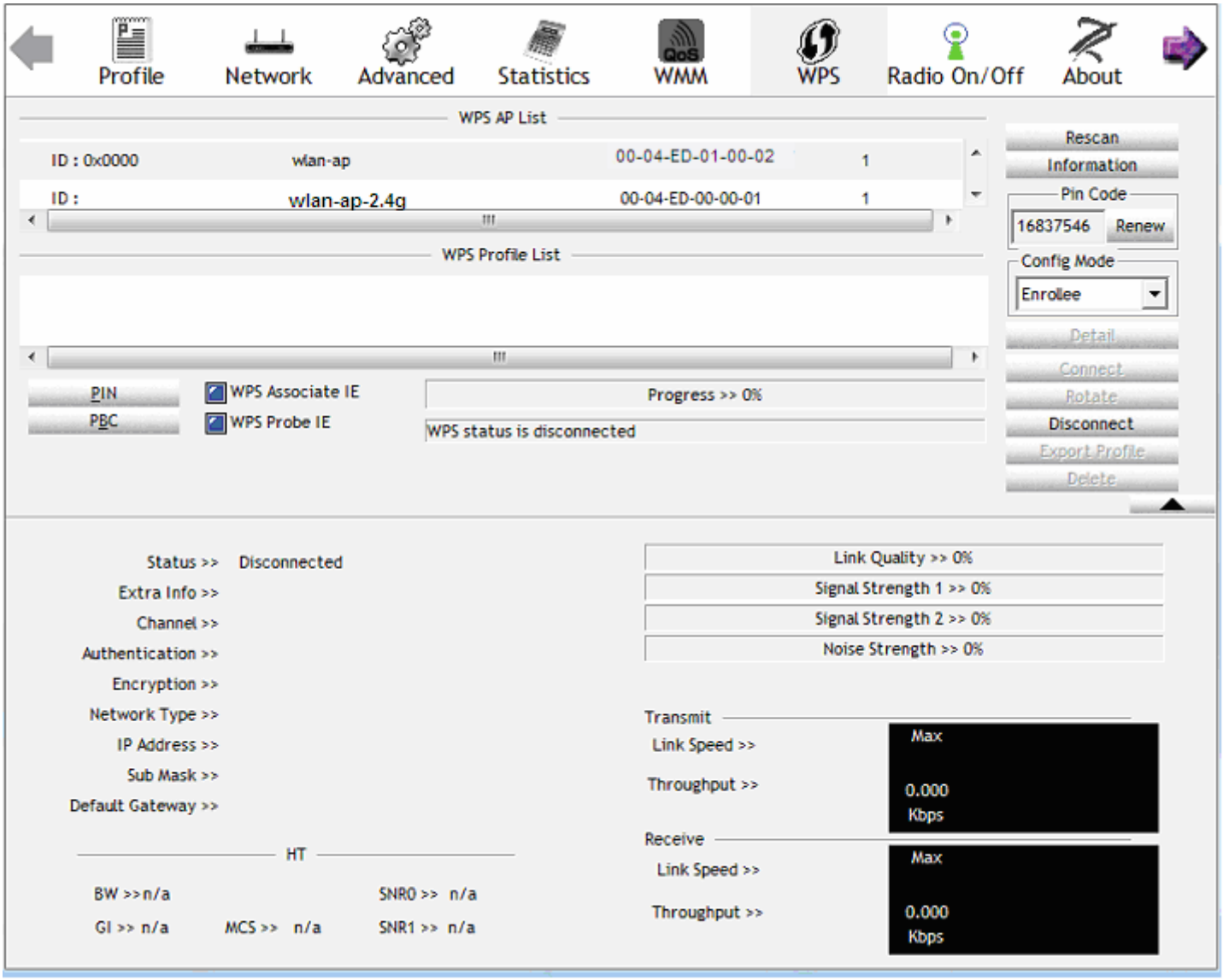
(Station PIN)



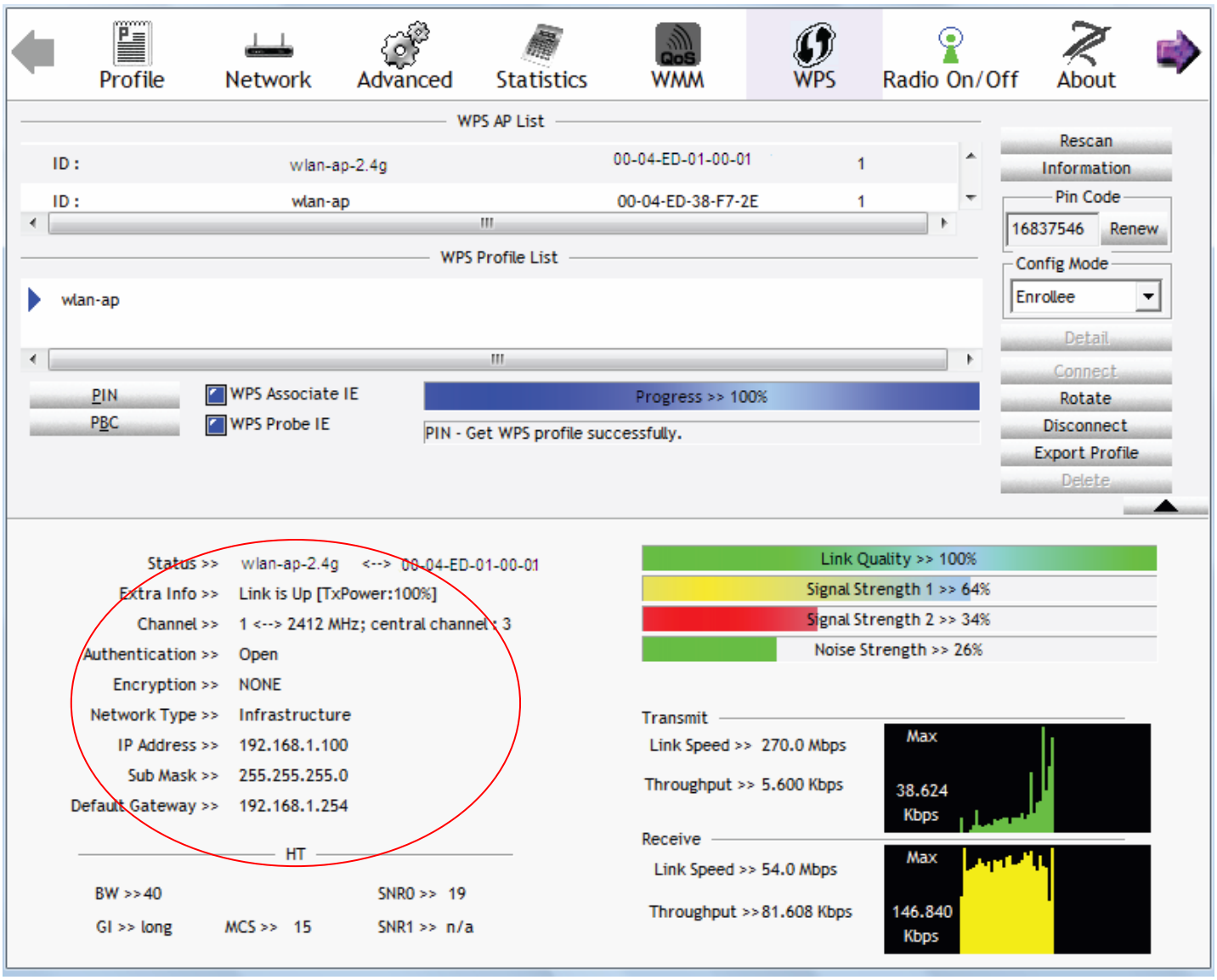
(Station MAC)

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

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



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

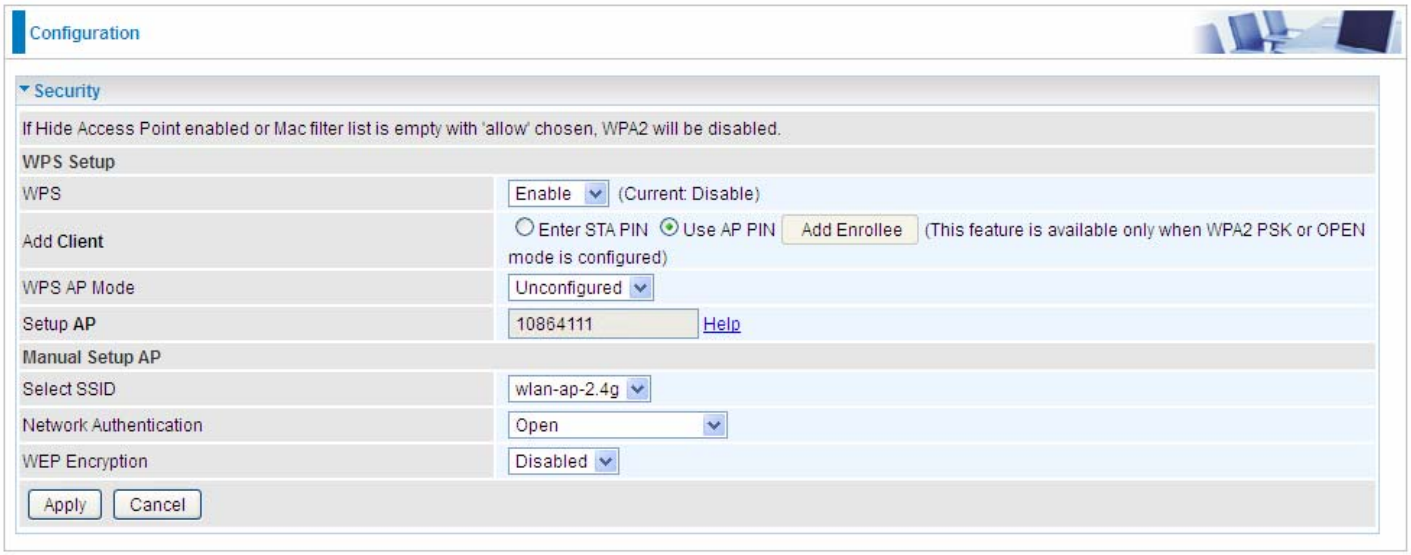
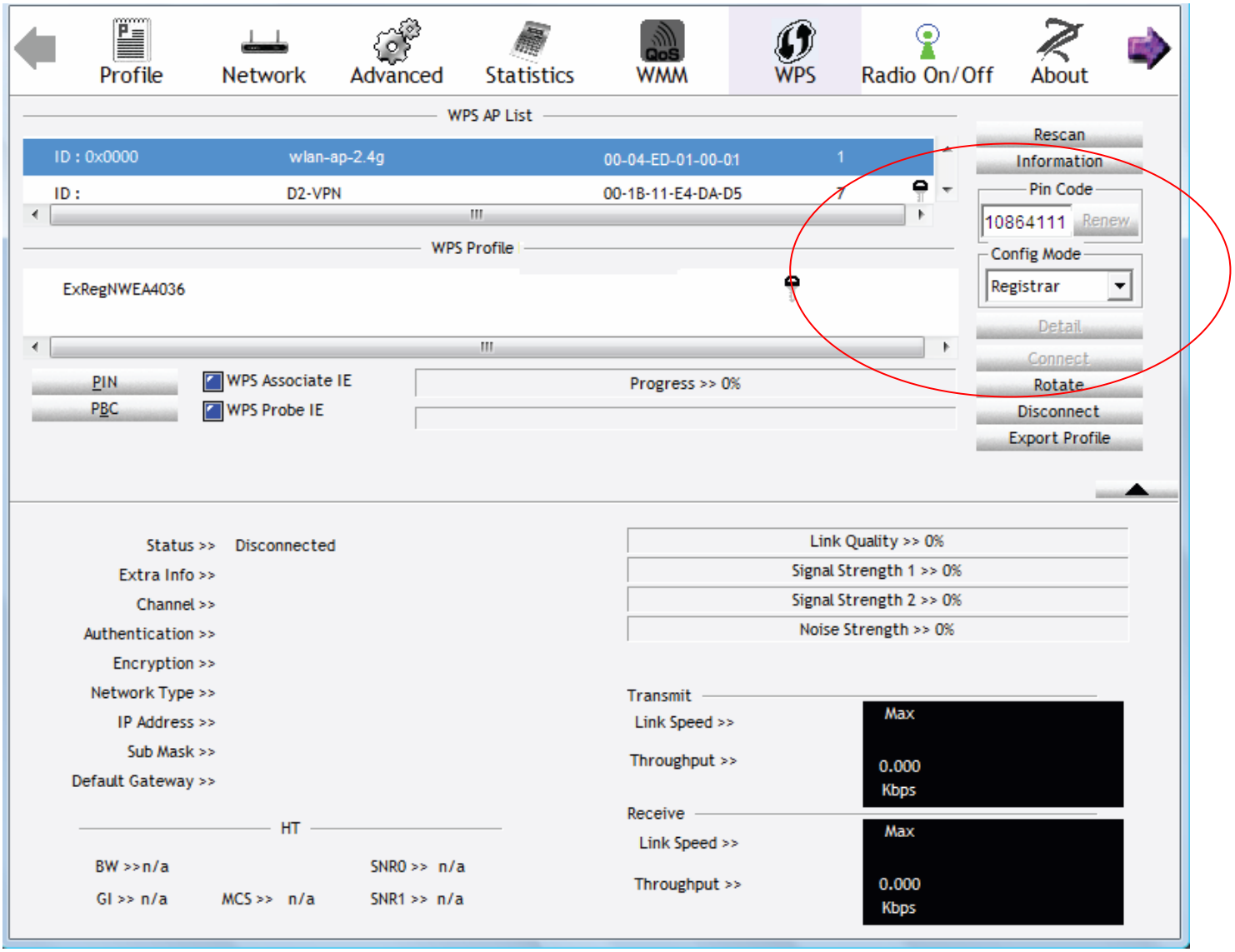


You can check the message in the red ellipse with the security parameters you set, here we all use the default.

Configure AP as Enrollee

Add Registrar with PIN Method

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



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.