BiPAC 9300(V)NX

GPON (VoIP) Wireless-N Gateway

User Manual

Firmware Version 1.04f

Last Revised on Feb 2010

Table of Contents

Chapter 1: Product 1
Introduction to your Router 1
Mini IP-PBX for VoIP calls 1
OMCI remote management 1
Optimal Wireless Speed and Coverage 2
Features 3
GPON Compliance 3
Network Protocols and Features 3
Firewall 4
Quality of Service Control 4
IPTV Applications 4
Wireless LAN 4
VoIP 4
Management 5
Hardware Specifications 6
Physical Interface 6
Physical Specifications 6
Operating Environment 6
Chapter 2: Installing the Router 7
Package Contents 7
Device Description 9
BiPAC 9300VN(X) 9
Front Panel LED 9
Rear Ports 10
BiPAC 9300N(X) 11
Front Panel LED 11
Rear Ports 12
Cabling 14
Chapter 3: Basic Network Installation 15
Applications of the device 16

Hardware Installation 17
Power Connection 17
GPON Connection 17
LAN Connection 18
Network Configuration 19
Configuring PC in Windows Vista 19
Configuring PC in Windows XP 21
Configuring PC in Windows 2000 22
Configuring PC in Windows 95/98/Me 23
Configuring PC in Windows NT4.0 24
Factory Default Settings 25
Easy Internet Access Configuration 26
Configuring with your Web Browser 26
Chapter 4: Configuration 27
Quick Start 28
Basic Configuration Mode 30
Status 30
WAN 32
PPPoE 32
DHCP Client 33
Static IP 34
Pure Bridge 35
WLAN 36
Quick VoIP (Only for 9300VN(X)) 38
Advanced Configuration Mode 40
Status 40
GPON Status 42
ARP Table 43
DHCP Table 44
System Log 45
Firewall Log 46
VoIP CDR Log (Only for 9300VN(X)) 47

SIP Accounts Status (ITSP) (Only for 9300VN(X)) 48
SIP Extensions Status (Only for 9300VN(X)) 49
VoIP Call Status (Only for 9300VN(X)) 50
UPnP Portmap 51
Configuration 52
LAN - Local Area Network 53
WAN - Wide Area Network 72
System 77
Firewall 84
QoS - Quality of Service 93
Virtual Server 98
Time Schedule 102
Advanced 103
Advanced VoIP (Only for 9300VN(X)) 117
Extensions 118
SIP Accounts (ITSP) 120
Mini IP-PBX 123
Save Configuration to Flash 129
Restart 130
Logout 131
Chapter 5: Troubleshooting 132
Appendix: Product Support & Contact 134

Chapter 1: Product

Introduction to your Router

Thank you for purchasing BiPAC 9300(V)NX Wireless-N Gateway Router. Your new router is a next-generation Gigabit Passive Optical Network (GPON) integrated access device (IAD). It uses BroadLight's BL2348 embedded System-on-Chip solution and is fitted with a 4-port Gigabit Ethernet Switch and Wi-Fi 802.11n access point.

BiPAC 9300(V)NX is a cost-effective solution for point-to-multipoint; fiber-to-the-premises network architecture in which passive optical splitters are used to allow a single optical fiber to serve multiple premises. Compliant with the ITU-T G.984 GPON standards, the device supports maximum downstream rates up to 2.5Gbps and upstream rates up to 1.25Gbps. With this technology, users can enjoy high-speed GPON services and bandwidth-consuming multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever before.

BiPAC 9300(V)NX also has two RJ-11 FXS ports for connecting to regular telephones, allowing users to make economical VoIP calls.

BiPAC 9300(V)NX supports the ONT Management and Control Interface (OMCI), which ensures that Billion's GPON ONT router is easy to configure, activate and manage remotely from a Optical Line Terminal (OLT). By reducing call-outs, deployment and support costs of the ONT device are greatly reduced.

Mini IP-PBX for VoIP calls

BiPAC 9300VNX Series is compliant with SIP standard (RFC3261) and supports SIP registrar. The unique feature of the gateway is that it can be used as a mini IP-PBX that supports up to 20 user accounts for SIP extensions and 2 SIP accounts for making economical VoIP calls provided by Internet Telephony Service Providers (ITSP). This router series integrates two FXS ports allowing users to make or receive phone calls over the Internet simply by connecting the device to their existing telephone set. This state-of-the-art feature is ideal for SOHO users, delivering free communication between branch offices and client sites. Making VoIP calls is just as easy as dialing an extension number!

OMCI remote management

In order to meet the ITU-T G.984.4 requirements for OMCI (ONT Management Control Interface), and defined compatibility and message transfer between OLT and ONT, and Management Information Base (MIB) physical device management, BiPAC 9300VNX Series uses OpenCon's OMCI management. This tool is field-proven and interoperable with other GPON Systems with OMCI capabilities for both OLT and ONT equipment. OpenCon's OMCI management has been thoroughly tested to consistently meet ITU-T G.984.4 and is approved by the Full Service Access Network (FSAN) Group.

Optimal Wireless Speed and Coverage

With an integrated 802.11n Wireless Access Point, the router delivers up to 6 times the speed and 3 times the wireless coverage of an 802.11b / g network device. It supports a link rate up to 300Mbps and is also compatible with 802.11b/g equipment. The Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) and Wired Equivalent Privacy (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 the user's network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function expands the wireless network without needing any external wires or cables.

Features

- ITU-T G.984 GPON compliant
- Supports bandwidth maximum downstream rates up to 2.5Gbps and upstream rates up to 1.25Gbps
- Supports transmission distance up to 20km
- Dual-wavelength: Tx at 1310nm and Rx at 1490nm
- Supports OMCI (ONT Management and Control Interface) remote management
- Voice over IP compliant with SIP standards
- Two FXS ports for connecting to regular telephones
- Supports FAX Transmission: T.38 fax relay, G.711 pass-through
- Supports mini-IP PBX Features
- Draft 802.11n wireless and delivers up to 300Mbps link rate
- 802.11n Wireless AP with WPA-PSK/WPA2-PSK Supported
- Supports Wi-Fi WMM prioritization
- SOHO Firewall Security with DoS Prevention and SPI
- Quality of Service for traffic prioritization and bandwidth management
- Supports IPTV Applications
- Easy Sign-On (EZSO)
- Ideal for Home, SOHO and Office users

GPON Compliance

- GPON Compliance
- Compliant with ITU-T G.984 GPON standards
- G.984.1 General characteristics
- G.984.2 Physical Media Dependent (PMD) layer specifications
- G.984.3 Transmission convergence layer specifications
- G.984.4 Management and control interface

Network Protocols and Features

- NAT, static routing and RIP-1 / 2
- Universal Plug and Play (UPnP) compliant
- Dynamic Domain Name System (DDNS)

- Virtual Server and DMZ
- SNTP, DNS relay and IGMP proxy

Firewall

- Stateful Packet Inspection (SPI)
- DoS attack prevention including IP Spoofing, Land Attack, Smurf Attack, Ping of Death, TCP SYN Flooding, etc.
- Packet Filtering - port, source IP address, destination IP address, MAC address
- URL Content Filtering - string or domain name detection in URL string

Quality of Service Control

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

IPTV Applications

IPTV application may require subscription to IPTV services from a Telco / ISP.

- IGMP proxy and snooping for video service
- Virtual LAN (VLAN)
- Quality of Service (QoS)

Wireless LAN

- Compliant with IEEE 802.11n draft 2.0, 802.11g and 802.11b standards
- 2.4GHz - 2.484GHz frequency range
- Up to 300Mbps wireless operation rate
- Wi-Fi Protected Setup (WPS) for easy setup
- 64- / 128-bit WEP supported for encryption
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support

VoIP

- Two RJ-11 FXS ports for connecting to regular telephones
- Supports two SIP accounts for connecting to Internet Telephony Service Provider (ITSP)
- Supports SIP extensions
- Supports G.711 A/μ law, and G.729 Audio CODEC standards

• Supports FAX Transmission: T.38 fax relay, G.711 pass-through

• Supports Telephony Features: silence suppression, Voice Activity Detection (VAD), Comfort Noise Generation (CNG), G.168 echo cancellation, packet loss concealment

• Supports mini-IP PBX Features: Call Waiting, Call Transfer, Call Hold, Call Forward, Speed Dial, Direct Inward Dialing (DID), Do Not Disturb (DND), Caller ID, Call Detail Record, Call blocking (future release), 3-way conference (future release), Meeting Room (future release)

• Adaptive jitter buffer support

• DTMF: In-band/out-of-band (RFC2833) / SIP INFO

Management

• Quick Installation Wizard and Auto-scan for GPON settings

• Web-based GUI for remote and local management

• Firmware upgrades and configuration data upload and download via web-based GUI

• Embedded Telnet server for remote and local management

• SNMP v3, MIB-I and MIB-II support

• Supports DHCP server / client / relay

• OMCI supports remote management

• TR-069

Hardware Specifications

Physical Interface

- WLAN: detachable antenna
- WAN: SC/APC GPON port
- Telephone: 2-port FXS
- LAN: 4-port Gigabit auto-crossover (MDI/MDI-X) Switch
- USB 2.0 host port (BiPAC 9300VNX only)
- Factory default reset button
- WPS button
- Power jack
- Power switch

Physical Specifications

- Dimensions: 9.04” x 6.10” x 1.69” (229.5 x 155 x 43mm)
- Power Requirements: Input: 15V DC, 1.6A

Operating Environment

Operating temperature: 0 – 40°C

Storage temperature: -20 – 70°C

Humidity: 20 – 95% non-condensing

Chapter 2: Installing the Router

Package Contents

BiPAC 9300(V)NX GPON (VoIP) Wireless-N Gateway Router

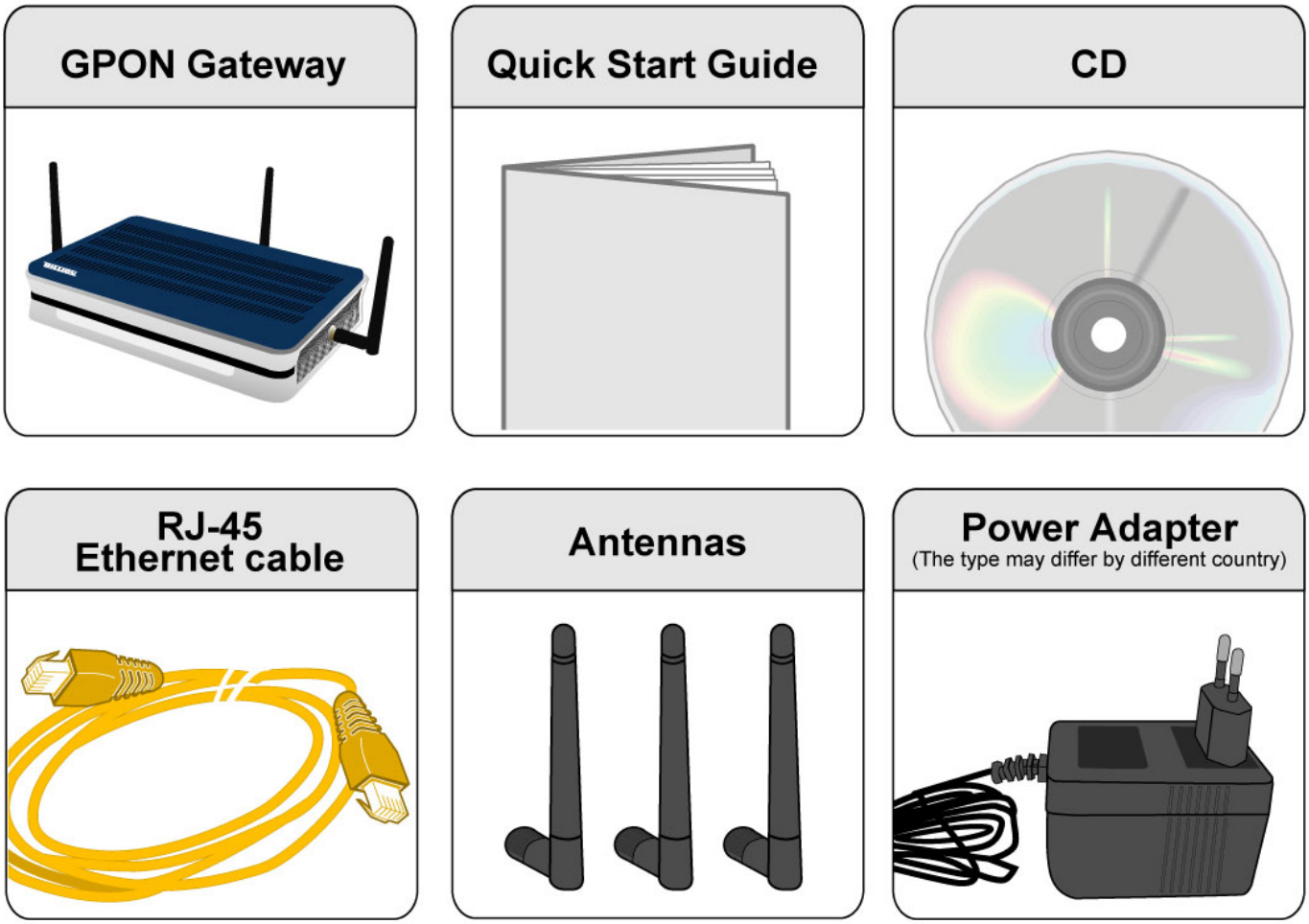
CD containing the online manual

Ethernet (RJ-45) cable

Three 2dBi detachable antennas

Power adapter

Quick Start Guide



Important note for using this router

Warning

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

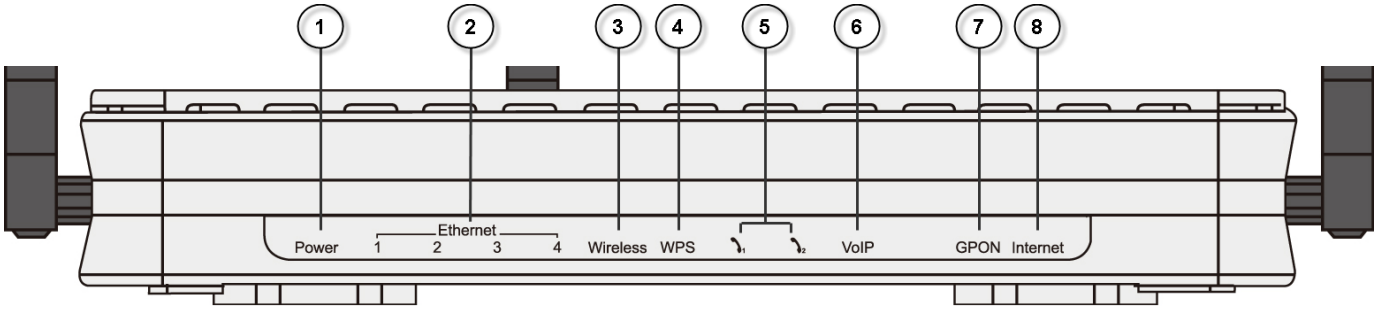
Attention

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

Device Description

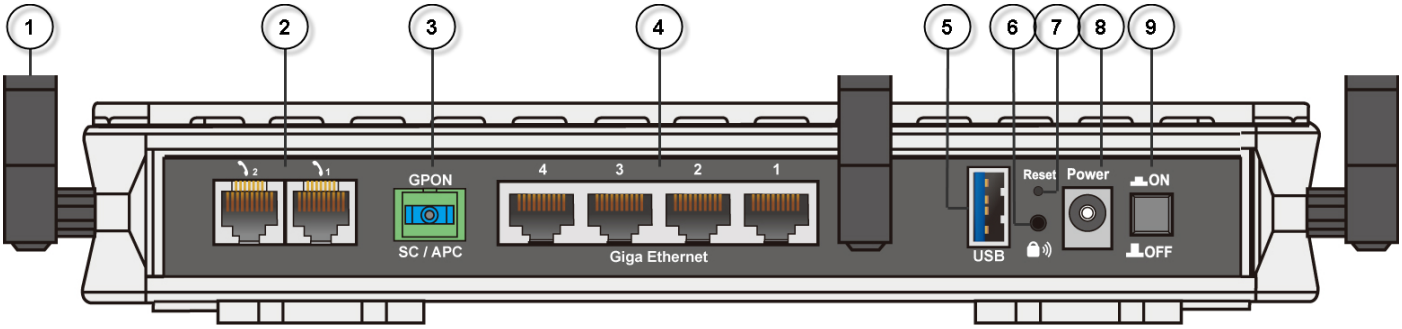
BiPAC 9300VN(X)

Front Panel LED



LED		Meaning
1	**Power**	Lit red when the device is booting. Lit green when the system is ready. Blinking when the device is rebooting or firmware is upgrading.
2	**Ethernet Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an office/ home network of 1Gbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an office/ home network of 10/100Mbps. Blinking when data is transmitted/ received.
3	**Wireless**	Lit green when a wireless connection is established. Blinking when data is transmitted/received.
4	**WPS**	Blinking when WPS is in progress. Lit up brightly and then lit off within 5 seconds when WPS ends.
5	**Phone** (RJ-11 connector)	Lit green when phone is off hook.
6	**VoIP** (RJ-11 connector)	After SIP registration is OK, the LED will lit green whenever the phone is off hook.
7	**GPON**	Lit green when GPON is operational. Lit off when fiber is disconnected or GPON is not operational.
8	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when the device is in bridge mode or when WAN connection is absent.

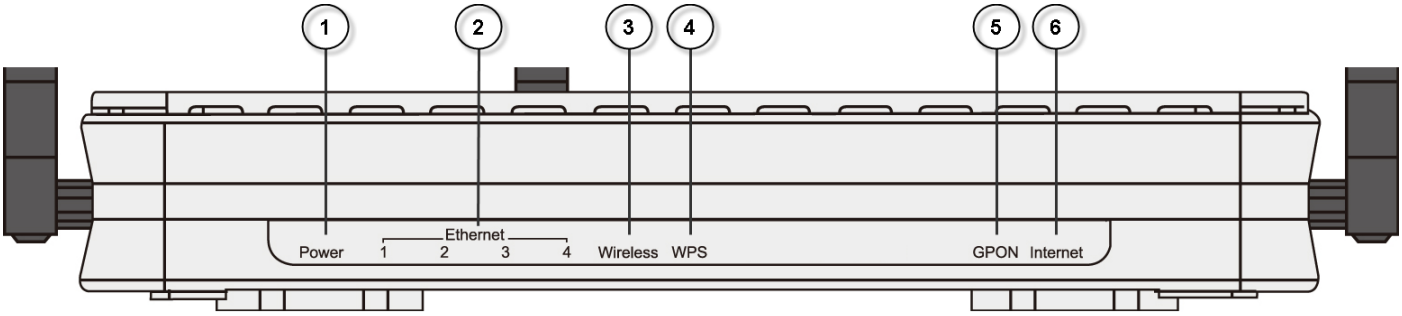
Rear Ports



Port		Meaning
1	**Antenna**	Connect the detachable antenna to this port.
2	**Phone** **1X- 2X** (RJ-11 connector)	Connect this port to an analog phone set with RJ-11 cable.
3	**GPON** **SC / APC** (SC/APC connector)	Connect the SMF fiber cable to the GPON SC/APC port.
4	**Giga Ethernet** **1X - 4X** (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5e or smaller) to one of the LAN ports when connecting to a PC or an office/home network of 10/100Mbps. Connect a UTP Ethernet cable (Cat-5e or larger) to one of the LAN ports when connecting to a PC or an office/home network of 1Gbps.
5	**USB**	Connect the USB cable to this port (BiPAC 9300VNX only).
6	**WPS**	Push this button to trigger Wi-Fi Protected Setup function.
7	**Reset**	Press this button for 6 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
8	**Power**	Connect it with the supplied power adapter.
9	**Power Switch**	Power ON/OFF switch.

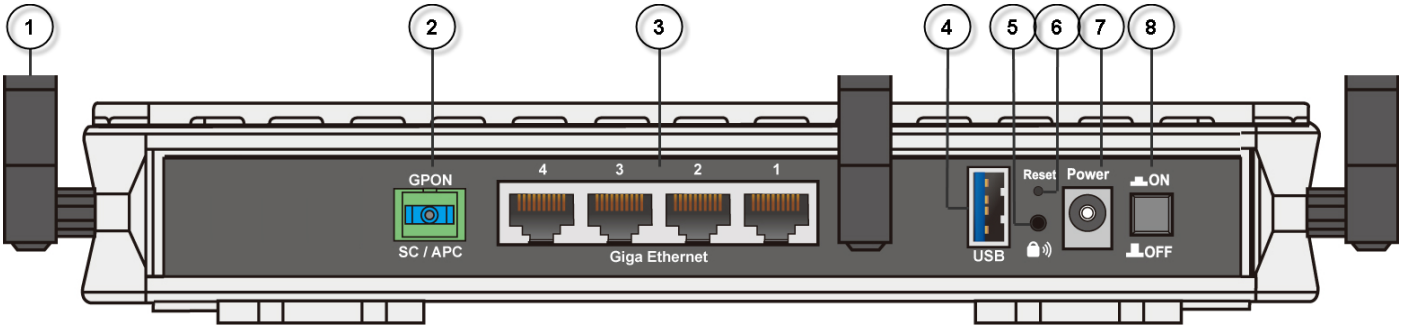
BiPAC 9300N(X)

Front Panel LED



LED		Meaning
1	**Power**	Lit red when the device is booting. Lit green when the system is ready. Blinking when the device is rebooting or firmware is upgrading.
2	**Ethernet Port** **1X — 4X** (RJ-45 connector)	Lit green when one of the LAN ports is connected to an office/ home network of 1Gbps. Blinking when data is transmitted/ received. Lit orange when one of the LAN ports is connected to an office/ home network of 10/100Mbps. Blinking when data is transmitted/ received.
3	**Wireless**	Lit green when a wireless connection is established. Blinking when data is transmitted/received.
4	**WPS**	Blinking when WPS is in progress. Lit up brightly and then lit off within 5 seconds when WPS ends.
5	**GPON**	Lit green when GPON is operational. Lit off when fiber is disconnected or GPON is not operational.
6	**Internet**	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully. Lit off when the device is in bridge mode or when WAN connection is absent.

Rear Ports



Port		Meaning
1	**Antenna**	Connect the detachable antenna to this port.
2	**GPON** **SC / APC** (SC/APC connector)	Connect the SMF fiber cable to the GPON SC/APC port.
3	**Giga Ethernet** **1X - 4X** (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5e or smaller) to one of the LAN ports when connecting to a PC or an office/home network of 10/100Mbps. Connect a UTP Ethernet cable (Cat-5e or larger) to one of the LAN ports when connecting to a PC or an office/home network of 1Gbps.
4	**USB**	Connect the USB cable to this port (BiPAC 9300NX only).
5	**WPS**	Push this button to trigger Wi-Fi Protected Setup function.
6	**Reset**	Press this button for 6 seconds at least to reset device to restore the device to factory default settings. ***Note: Be sure that the device is being turned on when press Reset button.*** (If you cannot login to the router or forget your Username/ Password, press this button for more than 6 seconds).
7	**Power**	Connect it with the supplied power adapter.
8	**Power Switch**	Power ON/OFF switch.

Recovery Operation

1. Recovery procedures for non-working routers (e.g. after a failed firmware upgrade flash):

The system will check the firmware of this device automatically while turning on the modem. Once the firmware is not integrated, the system enters the recovery state. The modem emergency-reflash web interface will then be accessible via http://192.168.1.254 where you can upload a firmware image to restore the modem to a functional state. Please note that the modem will only respond via its web interface at this address, and will not respond to ping requests from your PC or to telnet connections.

2. Recovery procedures for a lost web interface password:

After turning the router on, please press the Reset Button on the back of the modem, and hold the button until all the lights on the modem begin to flash and then it will reboot itself to restore the factory default settings. The login username and password will then be reset to admin. You can then access its GUI via its default IP address at http://192.168.1.254/.

NOTE:

Before the router is turned on to initiate its recovery process, please configure the IP address of the PC to 192.168.1.1 and then proceed with the following steps:
1. Turn off the router.
2. Turn on the router (the IP of the router will reset to an Emergency IP address, like 192.168.1.254).

Cabling

One of the most common causes of problem is bad cabling or GPON 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 GPON line LEDs are lit. If they are not, verify if you are using the proper cables.

Fiber cable is very fragile, please be careful not to snap the cable when you use it. In order to avoid dust entering, please put a lid on the head-end of the fiber cable when not in use. If you still have problem, please contact your ISP and tell them the serial number of this device (can be found on the Status page).

Chapter 3: Basic Network 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 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.

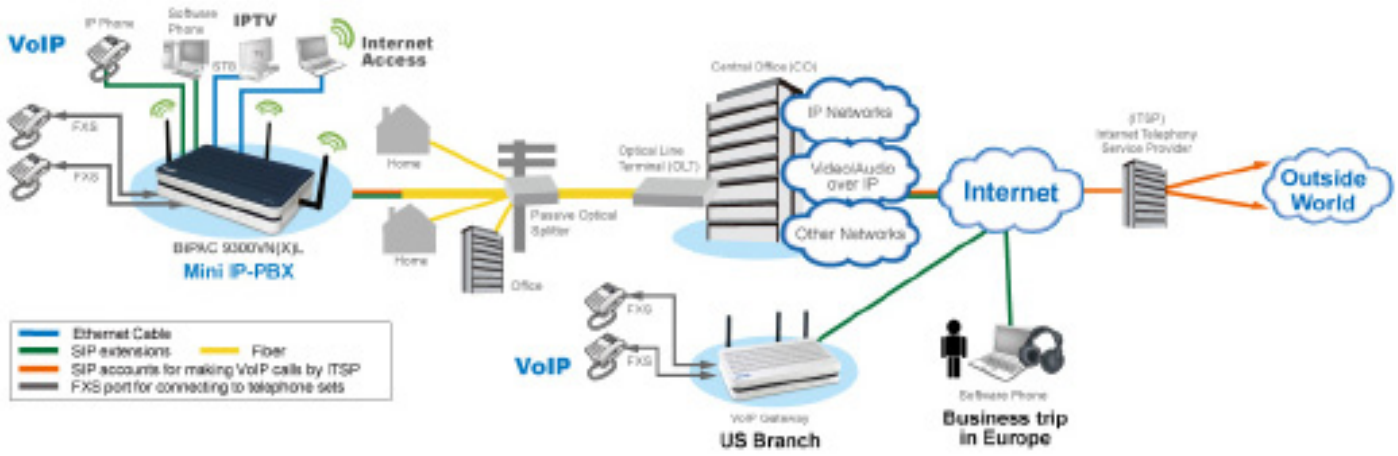
There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server 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.

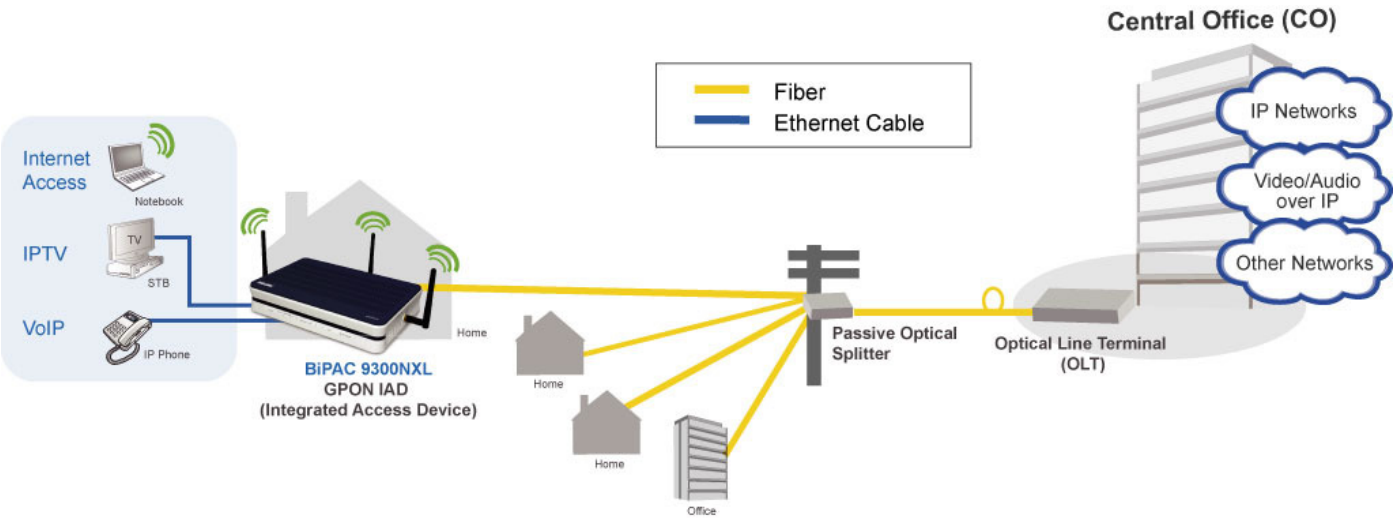
NOTE: Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

Applications of the device

BiPAC 9300VN(X)



BiPAC 9300N(X)

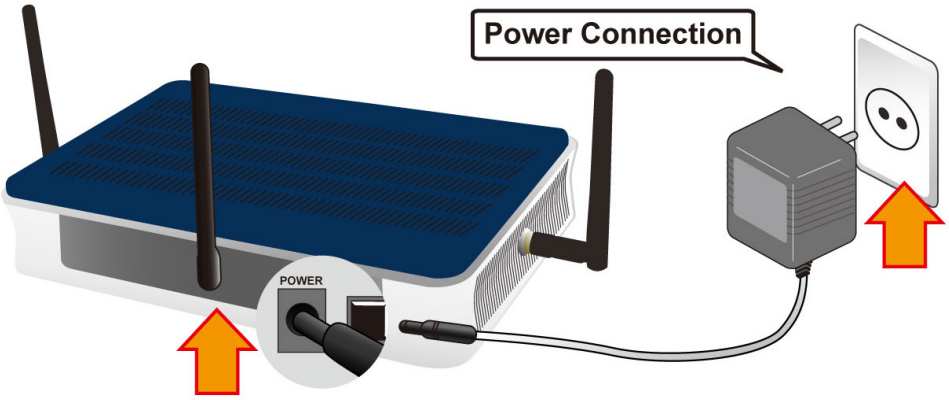


Hardware Installation

It is easy to connect BiPAC 9300(V)NX simply by performing the following instructions:

Power Connection

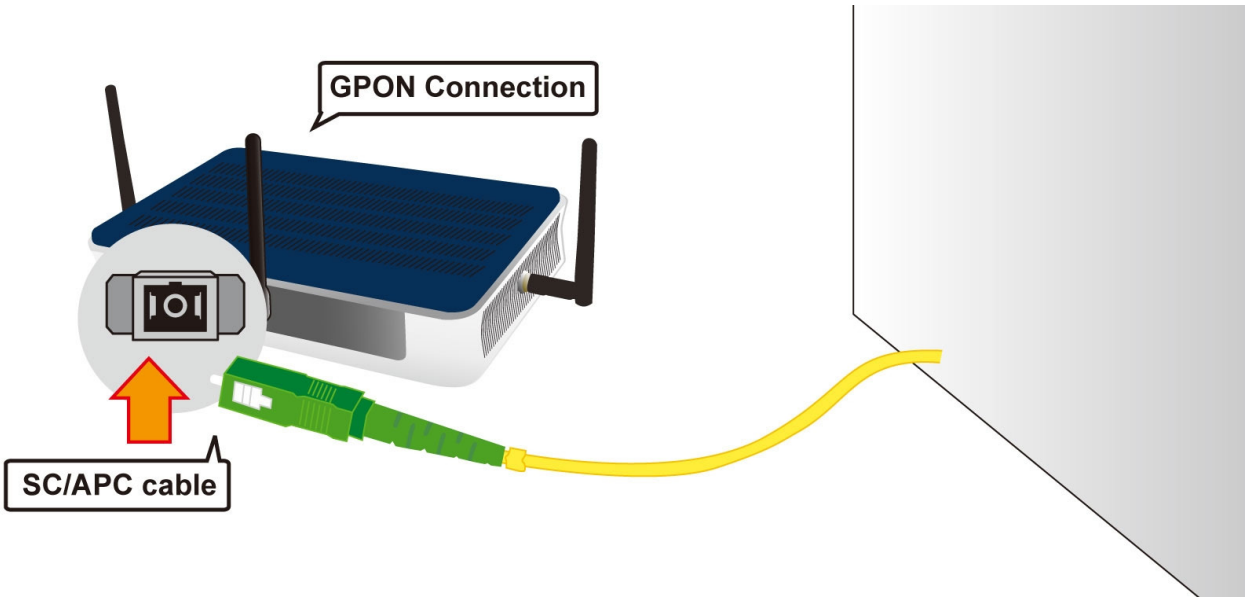
Plug one side of the supplied power adapter into the wall jack and connect the other side to the gateway.



Note: The plug type may vary from country to country.

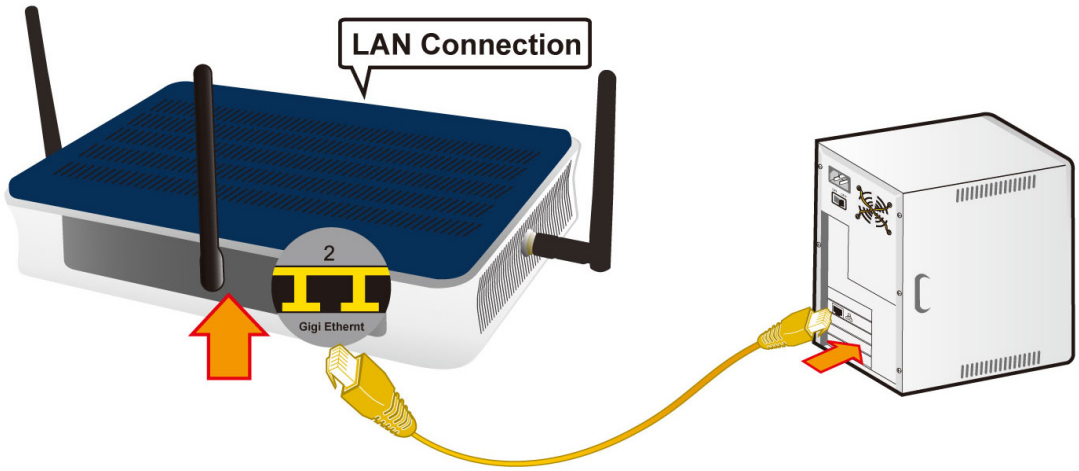
GPON Connection

Connect the supplied SC/APC cable to the gateway's GPON port.



LAN Connection

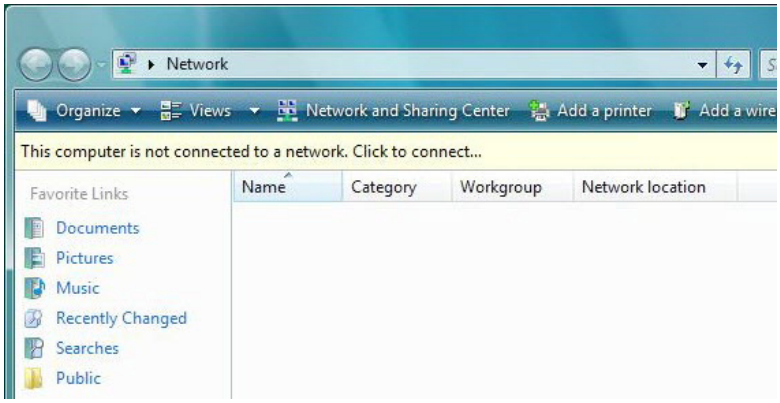
Connect one side of the supplied RJ-45 Ethernet cable to one of the Giga Ethernet ports, and the other side to other Ethernet interface.



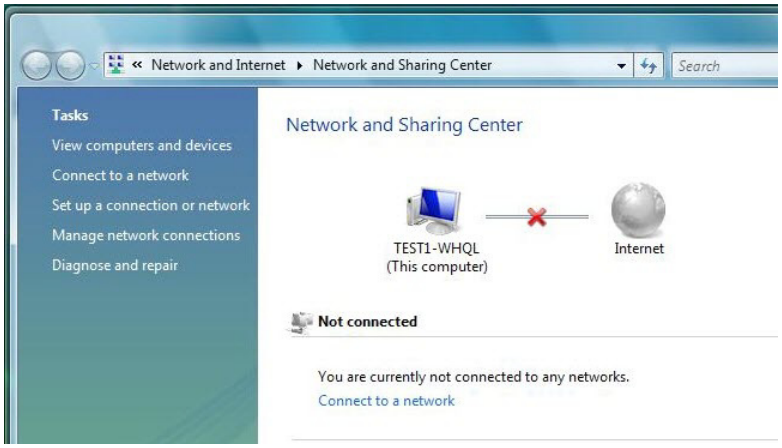
Network Configuration

Configuring PC in Windows Vista

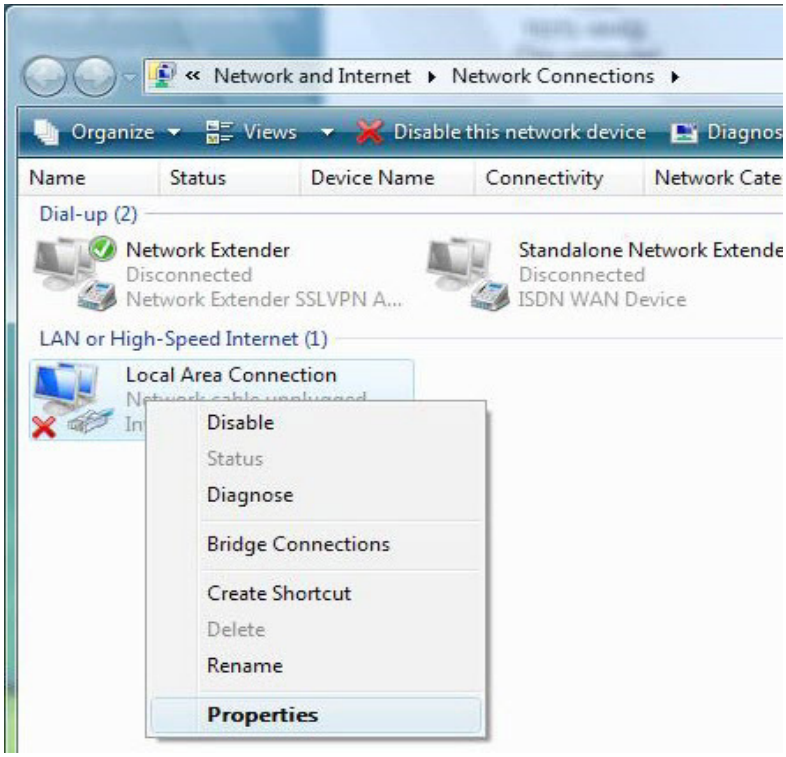
1. Go to Start. Click on Network.
2. Then click on Network and Sharing Center at the top bar.



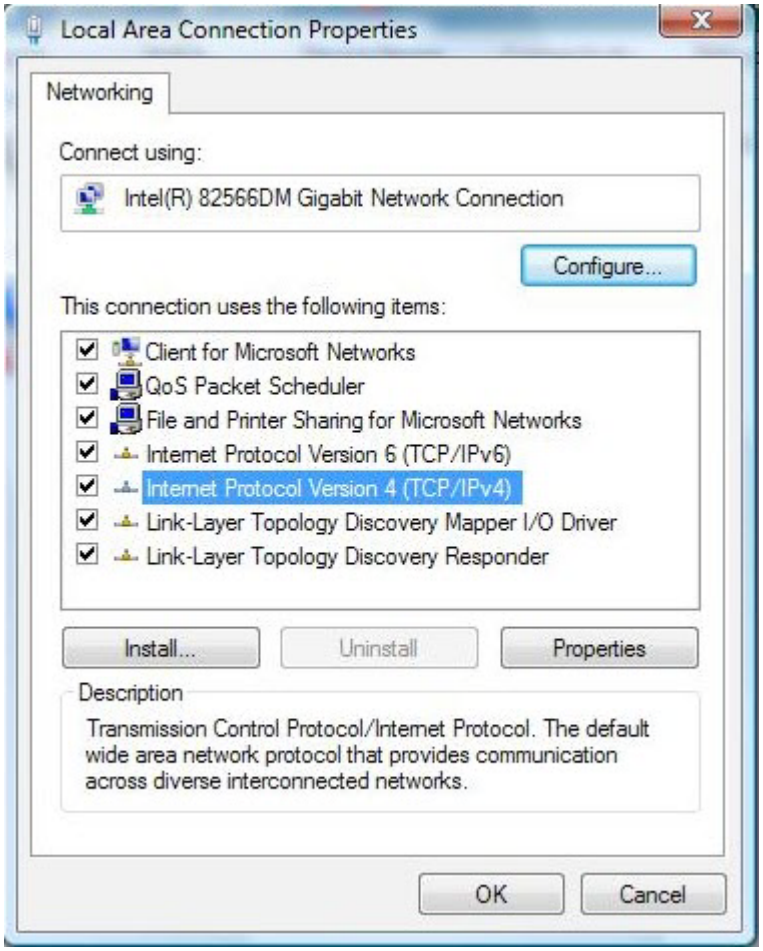
3. When the Network and Sharing Center window pops up, select and click on Manage network connections on the left window column.



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

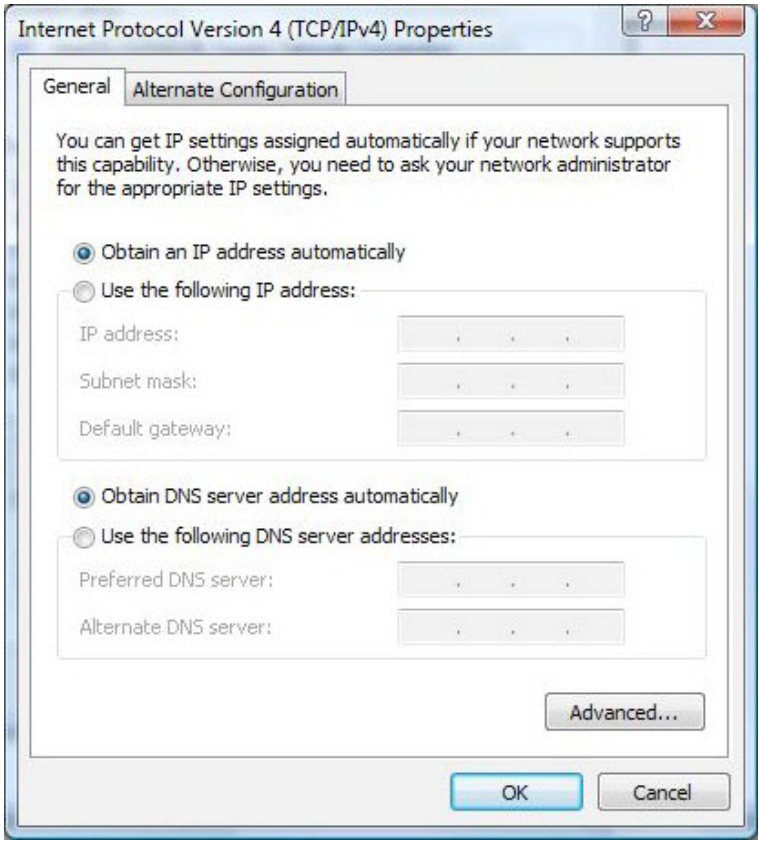


5. Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



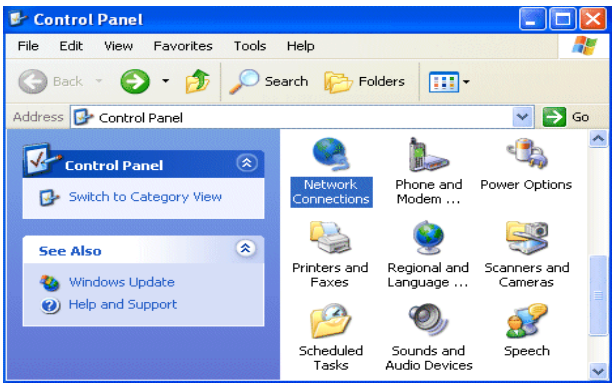
6. In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting.

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

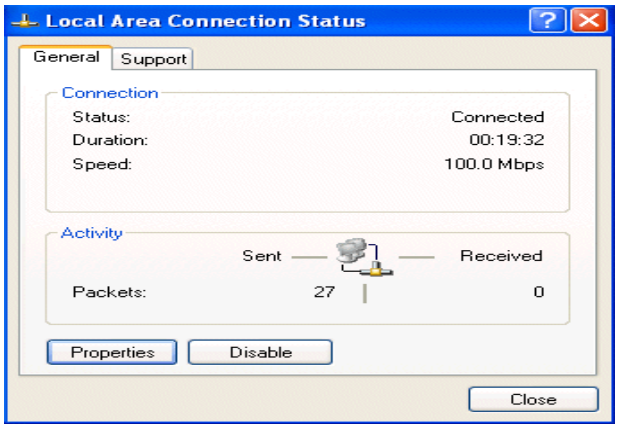


Configuring PC in Windows XP

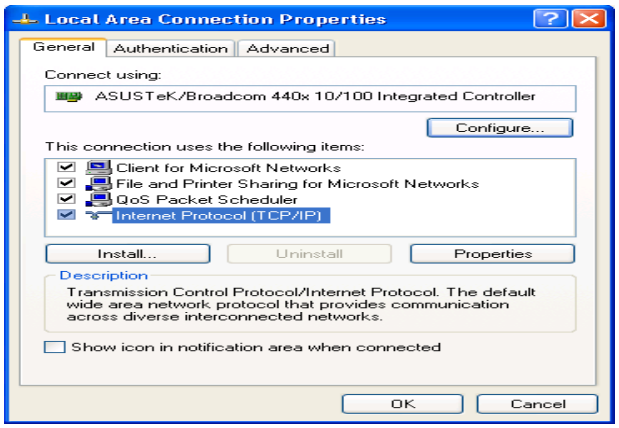
1. Go to Start > Control Panel (in Classic View). In the Control Panel, double-click on Network Connections
2. Double-click Local Area Connection.



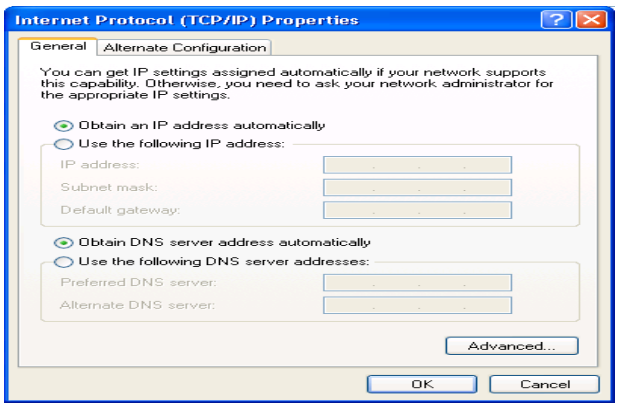
3. In the Local Area Connection Status window, click Properties.



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

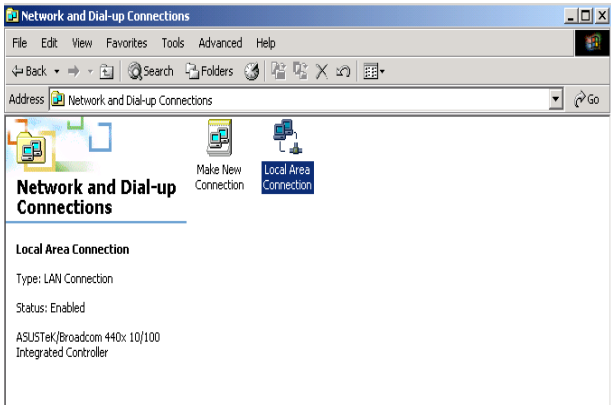


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

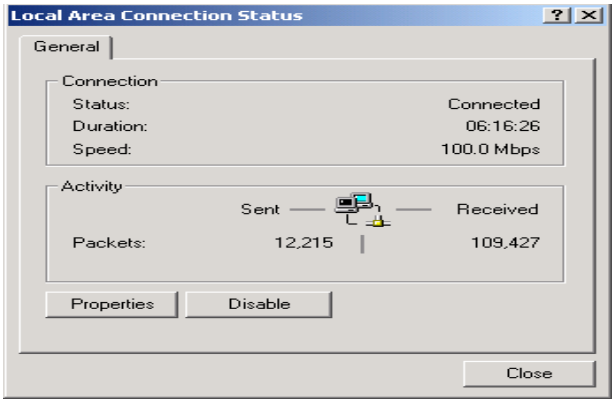


Configuring PC in Windows 2000

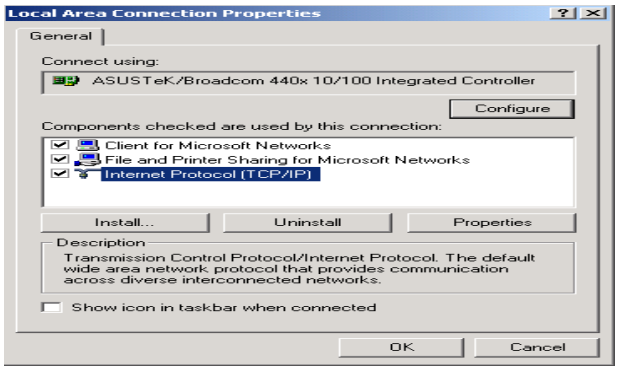
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



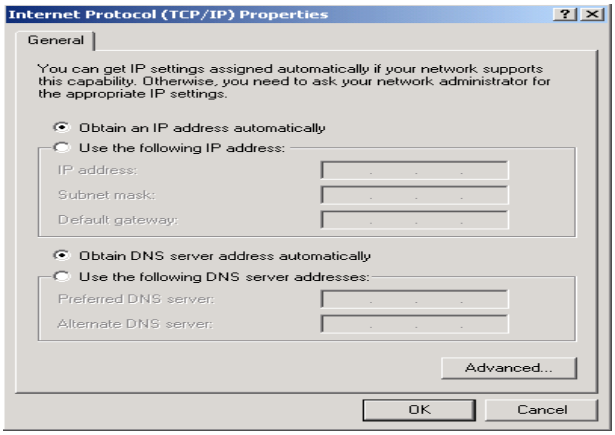
3. In the Local Area Connection Status window click Properties.



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

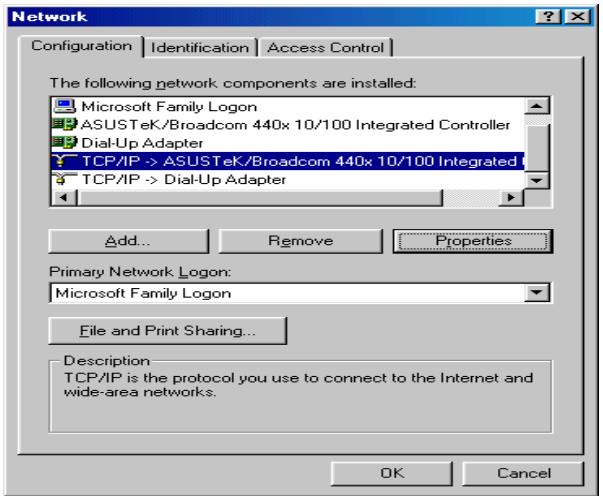


5. Select the Obtain an IP address automatically and the Obtain DNS server address automatically radio buttons.
6. Click OK to finish the configuration.

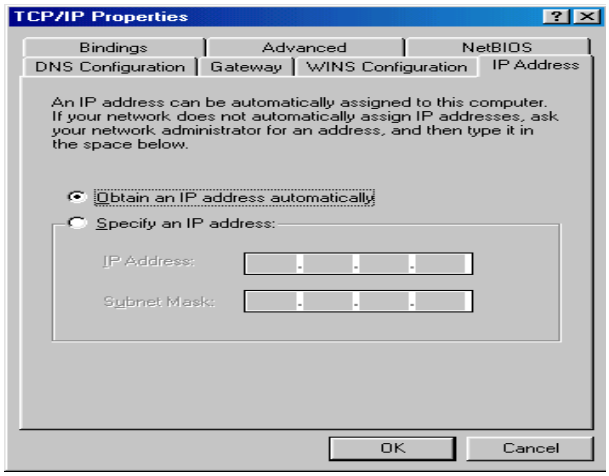


Configuring PC in Windows 95/98/Me

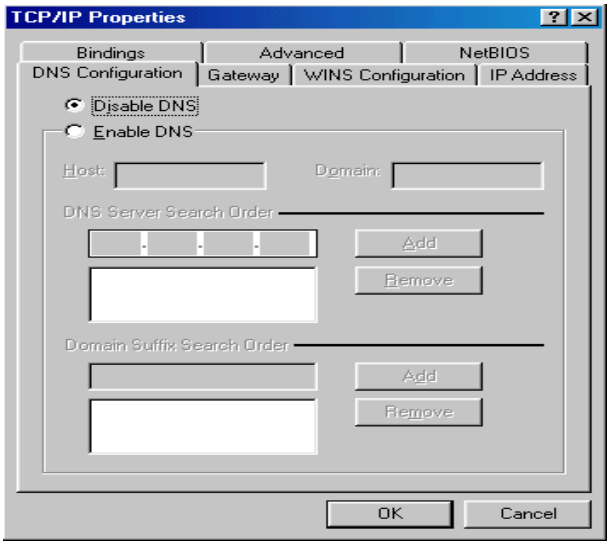
1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Configuration tab.
2. Select TCP/IP > NE2000 Compatible, or the name of your Network Interface Card (NIC) in your PC.



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

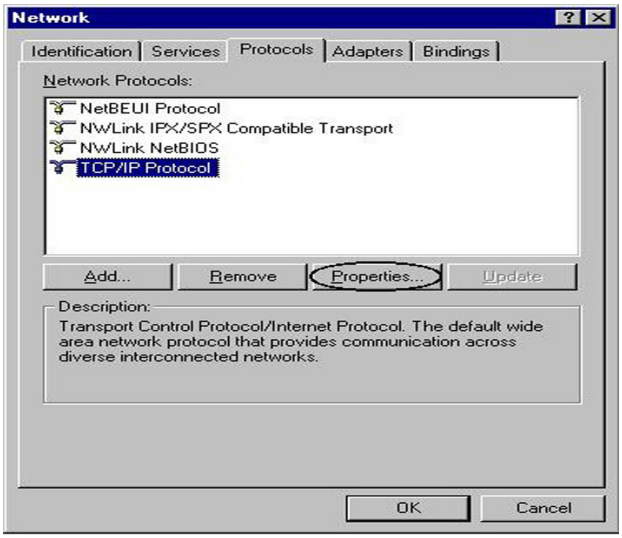


4. Then select the DNS Configuration tab.
5. Select the Disable DNS radio button and click OK to finish the configuration.

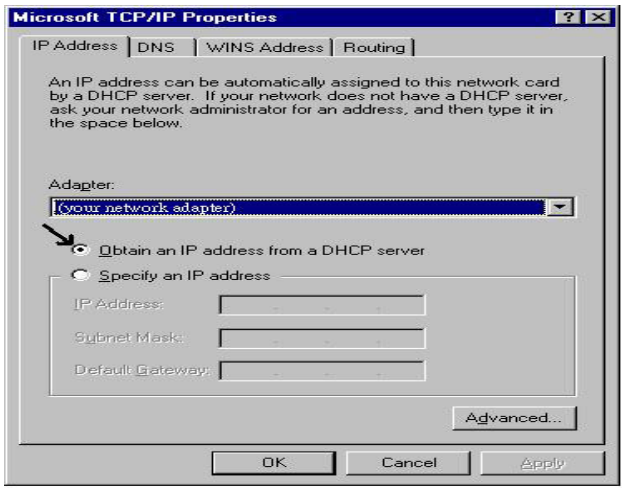


Configuring PC in Windows NT4.0

1. Go to Start > Settings > Control Panel. In the Control Panel, double-click on Network and choose the Protocols tab.
2. Select TCP/IP Protocol and click Properties.



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



Factory Default Settings

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

Web Interface (Username and Password)

- Username: admin
- Password: admin

The default username and password are “**admin**” and “**admin**” respectively.

Attention

If you have forgotten your username or password for the router, you can restore your device to its default setting by pressing the Reset button for more than 1 second.

Device LAN IP settings

- IP Address: 192.168.1.254
- Subnet Mask: 255.255.255.0

ISP setting in WAN site

- PPPoE

DHCP server

- 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 tale.

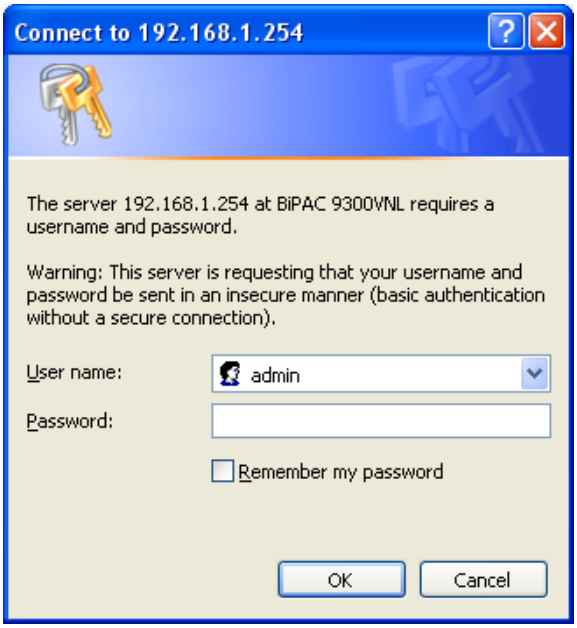
LAN Port		WAN Port
IP address	192.168.1.254	The PPPoE function is enabled to automatically get the WAN port configuration from the ISP. However, you have to set the username and password first.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

Easy Internet Access Configuration

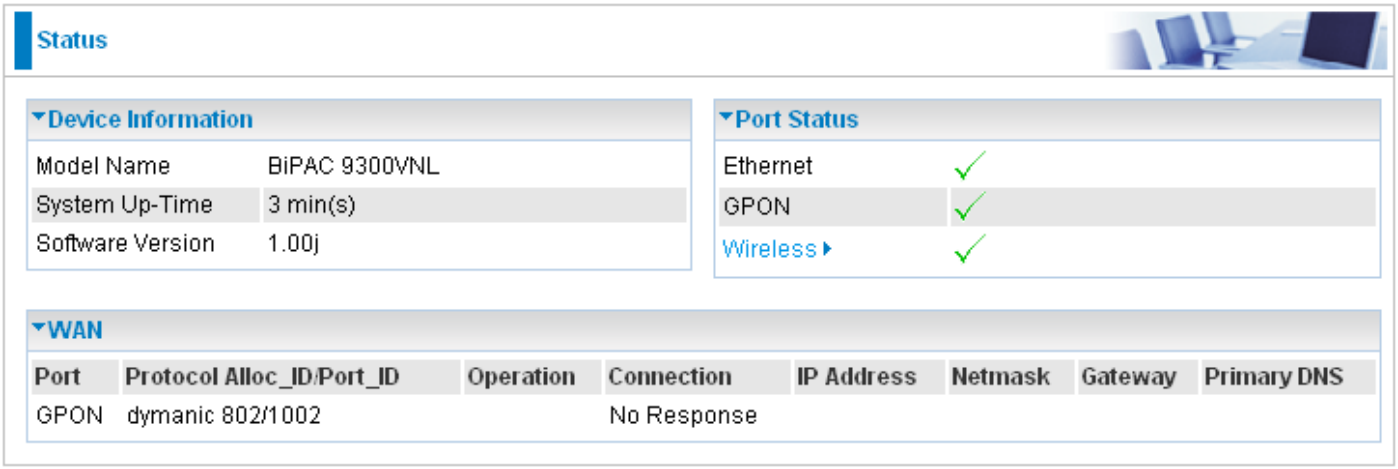
To easily configure this device for internet access, you must have IE 5.0 / Netscape 4.5 or above installed on your computer. There is basically one way to configure your router before you are able to connect to the internet: **Web Interface**. Configuration of this method will be discussed in detail in the following section.

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click “Go”, a user name and password window prompt will appear. The default username and password are “admin” and “admin” respectively.



Congratulations! You are now successfully logon to the Gateway Router!



If the authentication succeeds, the homepage Status will appear on the screen.

Chapter 4: Configuration

Once you have logged on to your router GUI via your web browser, you can begin to configure the router according to your needs. On the configuration homepage, the left navigation pane provides the links to different setup pages.

Sections embedded within the Basic Configuration mode:

Advanced (Press to switch to Advanced Configuration mode)

Status

Quick Start

WAN

WLAN

Quick VoIP (Only for 9300VN(X))

Sections embedded within the Advanced Configuration mode:

Basic (Press to switch to Basic Configuration mode)

Status (GPON Status / ARP table / DHCP table / System Log / Firewall Log / VoIP CDR Log / SIP Accounts (ITSP) / SIP Extensions / VoIP Call Status / UPnP portmap)

Quick Start

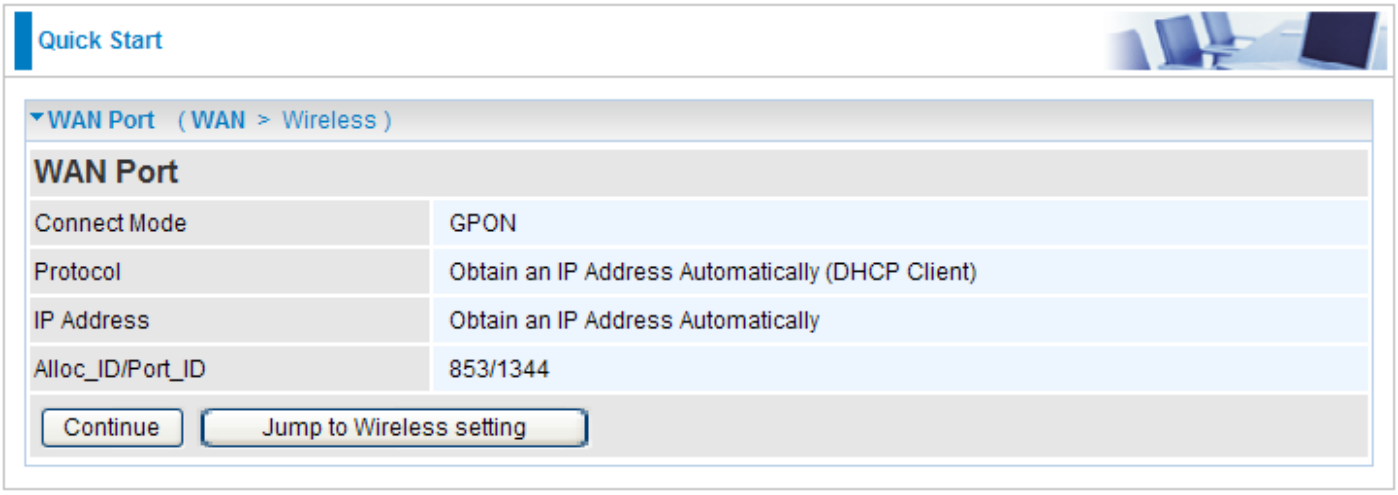
Configuration (LAN / WAN / System / Firewall / QoS / Virtual Server / Time Schedule / Advanced)

Advanced VoIP (Extensions / SIP Accounts (ITSP) / Mini IP-PBX) (Only for 9300VN(X))

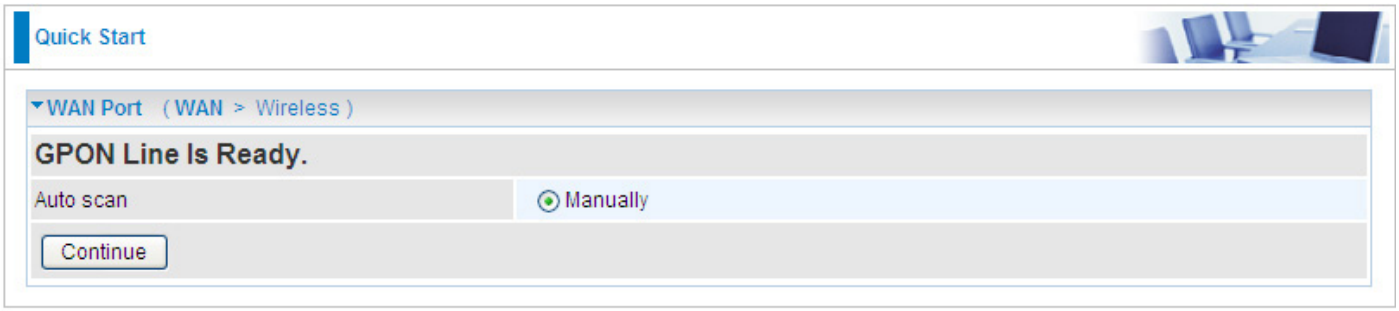
Each of these setup pages will be discussed in detail in sections that follow ahead.

Quick Start

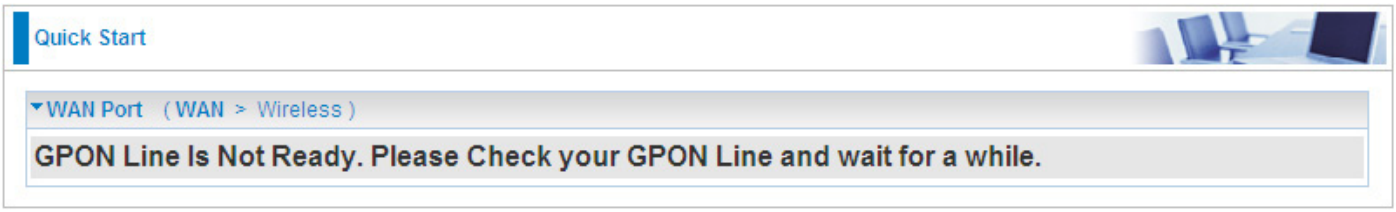
Whether on the Basic or Advanced Configuration Mode, click Quick Start link to WAN Port setup pages.



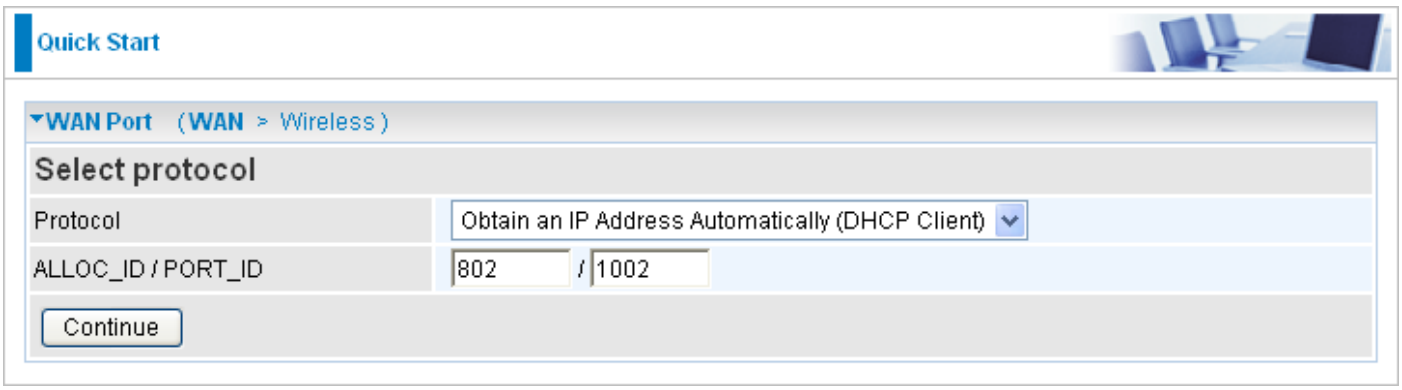
1. Select the appropriate connect mode from the drop down menu. Then press Continue to go to the next configuration page.
2. Press Continue to auto scan for the presence of GPON line.



Note: If the GPON line is not ready, a page will display as below and your new configuration can not be saved.



3. Configure the WAN, then click Continue. The device will then configure itself. There are several types of WAN protocol in this version. The detail of these protocols will be discussded in the next sections.



Quick Start

WAN Port (WAN > Wireless)

Please wait while the device is configured.

4. After your WAN is configured, press Next to Wireless button to proceed with your wireless configuration.

Quick Start

WAN Port (WAN > Wireless)

Congratulations !

Your WAN port has been successfully configured.

Next to Wireless

Note: If the WAN line is not ready, a page will display as below and your new configuration can not be saved.

Quick Start

WAN Port

Fail!!

WAN port setting is not successful, you can do this procedure again.

5. To activate wireless function, click on the enable radio button and then fill in its ESSID, select its channel ID and security mode. When it is done, click Continue to apply the setting. The system will save your configuration and update your new setting.

Quick Start

Wireless (WAN > Wireless)

Set Wireless configuration.

WLAN Service	Enable Disable
ESSID	wlan-ap
Channel ID	Channel 1 (2.412 GHz)
Security Mode	Disable

Continue

Quick Start

Save confguration

Saving configuration to FLASH. Please wait for 10 seconds

Quick Start

Process finished

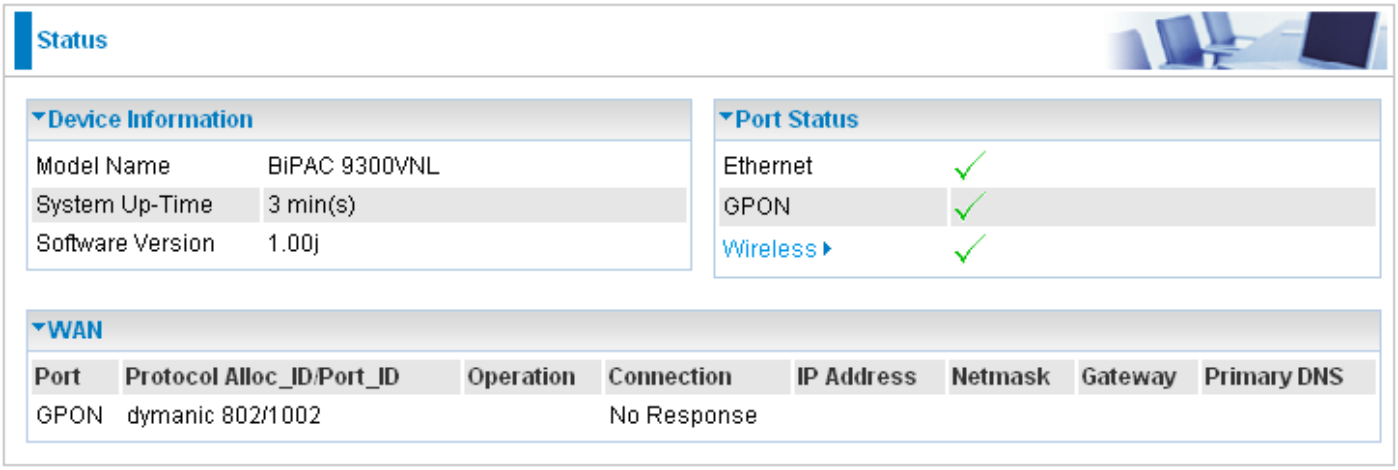
Success.

The Quick Start process is finished. Your device has been successfully configured.

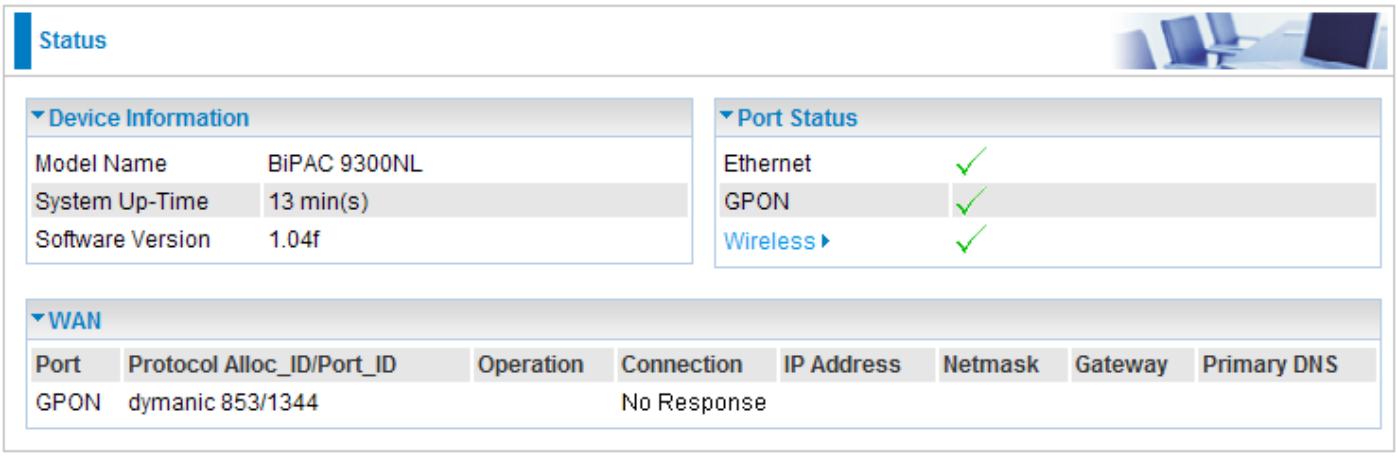
Basic Configuration Mode

Status

9300VN(X)



9300N(X)



Device Information

Model Name: Provide a name for the router for identification purposes.

System Up-Time: Record system up-time.

Software Version: Firmware version.

Port Status

Port Status: User can look up to see if they are connected to Ethernet, GPON and Wireless.

If ✕ is shown in GPON, the GPON port has not successfully connected or detected the optical signal.

If ✓ is shown in GPON, the GPON port has correctly connected.

If ⊘ is shown in GPON, the GPON connection has not been activated by OLT.

WAN

Port: Name of the WAN connection.

Protocol Alloc_ID/Port_ID: Allocation Identifier and GEM Port Identifier.

Operation: Current status in WAN interface.

Connection: Current connection status.

IP Address: WAN port IP address.

Netmask: WAN port IP subnet mask.

Gateway: IP address of the default gateway.

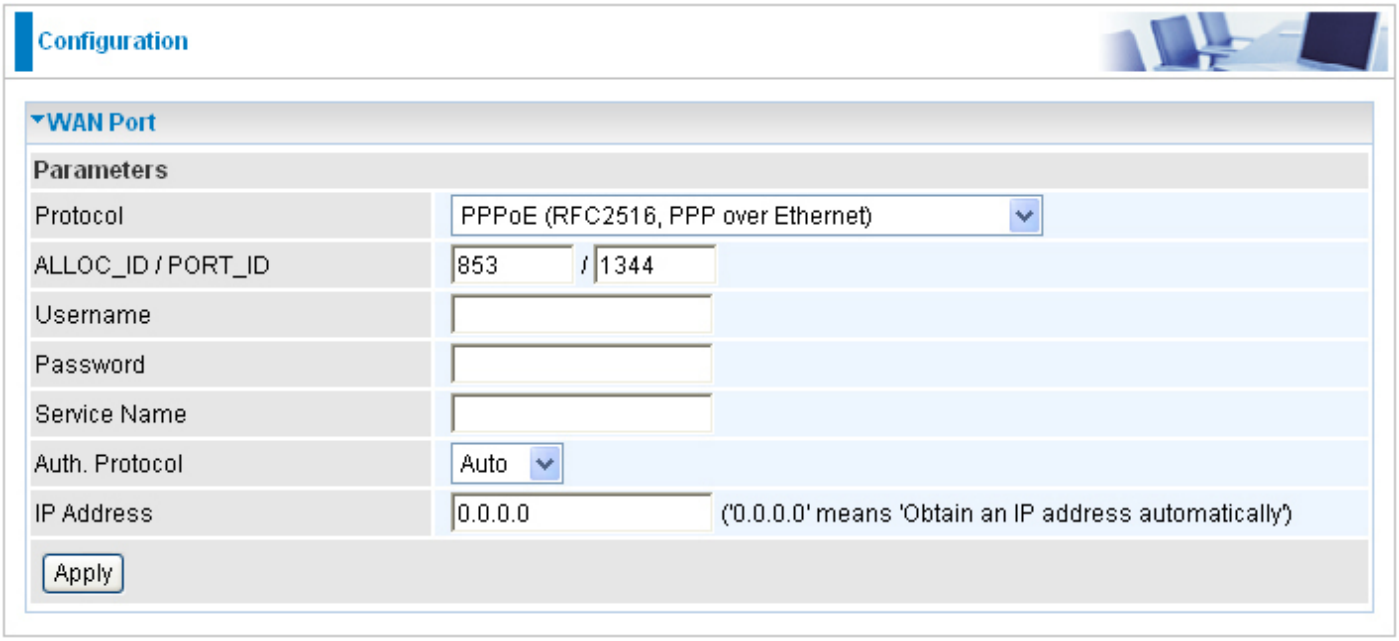
Primary DNS: IP address of the primary DNS server.

WAN

For WAN connect mode there are 4 types of connection protocols: **PPPoE**, **Obtain an IP Address Automatically (DHCP Client)**, **Static IP** and **Pure Bridge**.

PPPoE

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



Protocol: Select the protocol you will use in the device.

ALLOC_ID/PORT_ID: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is the format of username “username@ispname” instead of “username”.

Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is 15 alphanumeric characters.

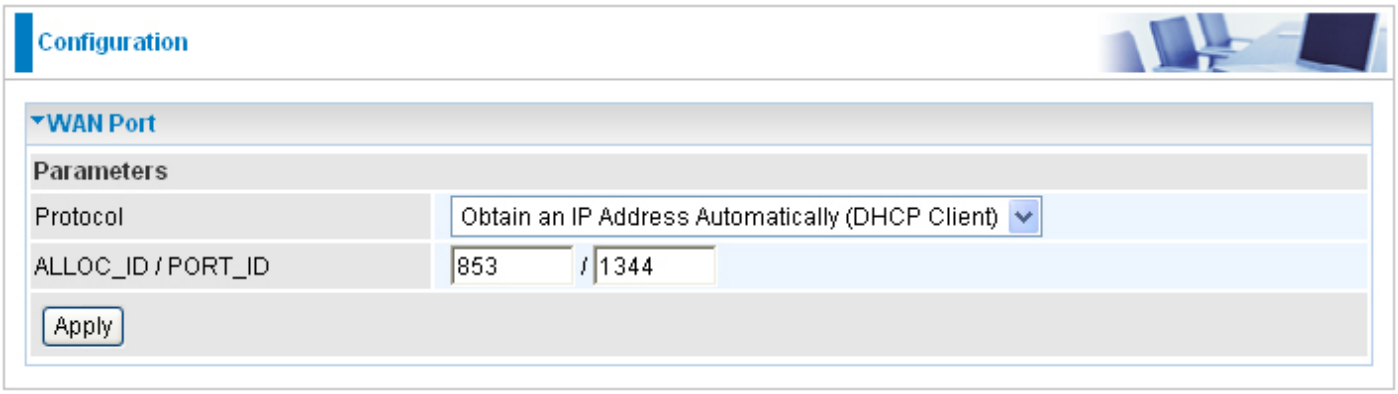
Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

IP Address: Your WAN IP address. Leave the IP address as 0.0.0.0 to enable the device to automatically obtain an IP address from your ISP.

Click Apply to confirm the settings.

DHCP Client

By configuring DHCP settings, the device is able to obtain IP settings automatically from the ISP.



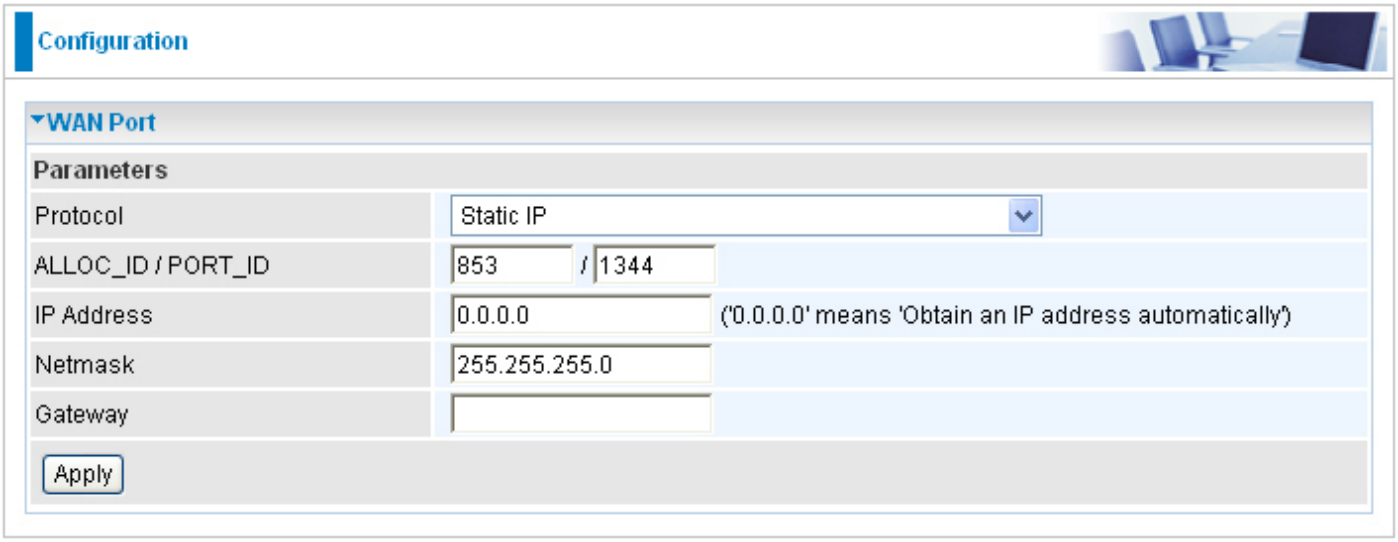
Protocol: Select the protocol you will use in the device.

ALLOC_ID/PORT_ID: Enter the information provided by your ISP.

Click Apply to confirm the settings.

Static IP

A Static WAN connection will be configured according to the IP properties defined by your ISP.



Protocol: Select the protocol you will use in the device.

ALLOC_ID/PORT_ID: Enter the information provided by your ISP.

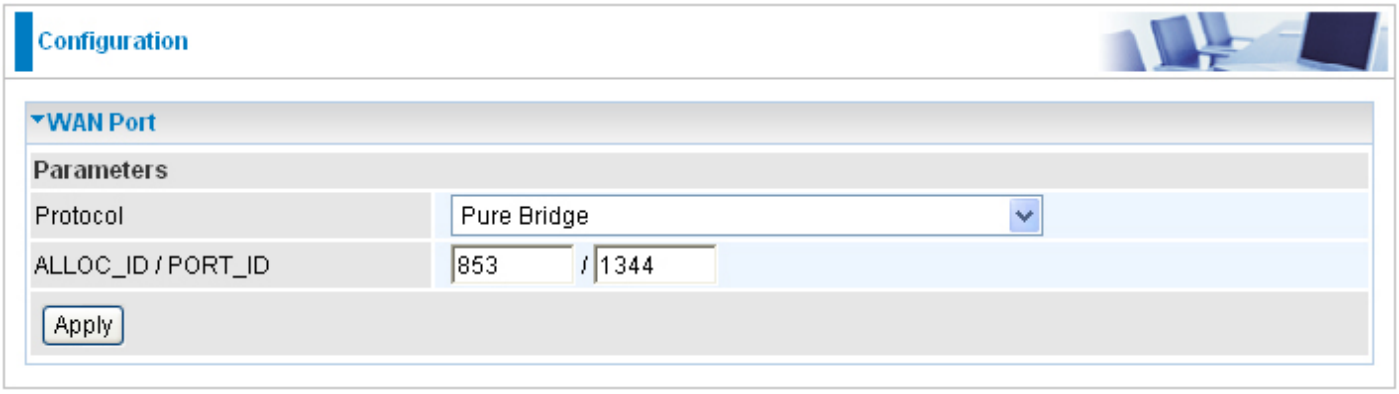
IP Address: Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Netmask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128. Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway (if given).

Click Apply to confirm the settings.

Pure Bridge

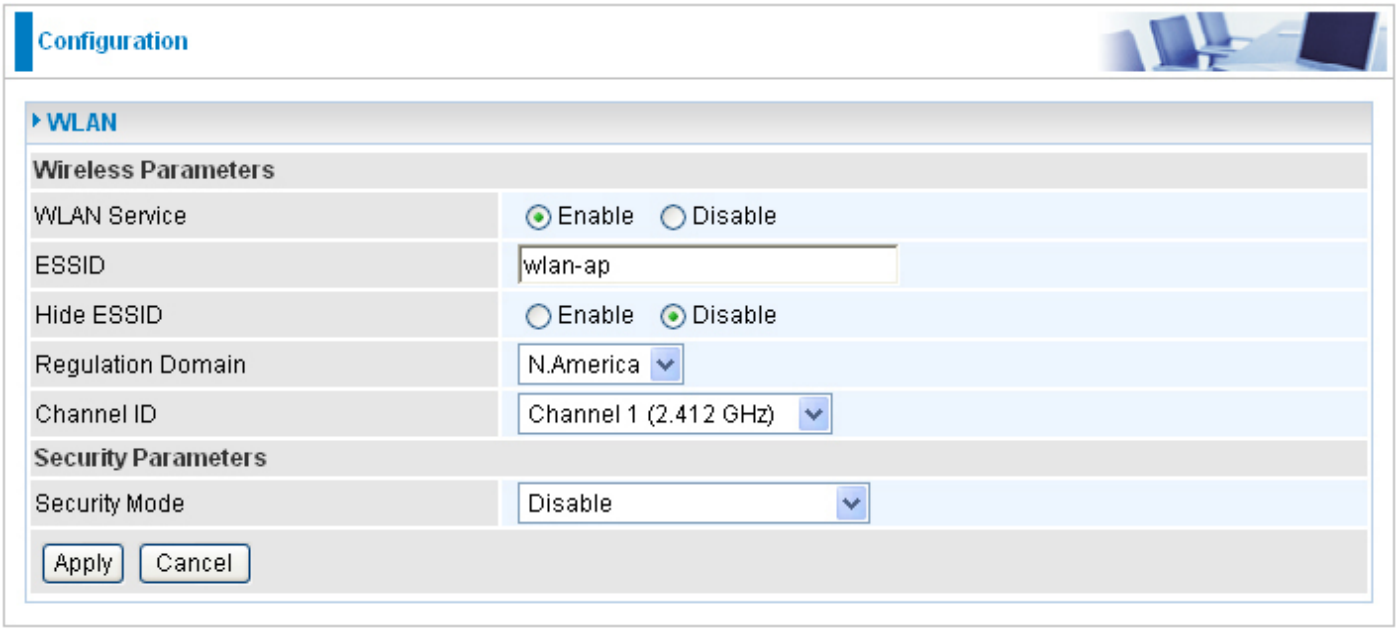


Protocol: Select the protocol you will use in the device.

ALLOC_ID/PORT_ID: Enter the information provided by your ISP.

Click Apply to confirm the settings.

WLAN



Wireless Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

ESSID: The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change the default wlan-ap to a unique ID name that is already built into the router wireless interface. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

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

Hide ESSID: It is used to broadcast its ESSID on the network so that when a wireless client searches for a network, the router can be discovered and recognized. Default setting is **Disable.**

> **Enable:** When enabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.
>
> **Disable:** When disabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection ID channel that you would like to use.

Note: Wireless performance may degrade if the selected ID channel is already being occupied by other AP(s).

Security Parameters

Security Mode: You can disable or enable the function with WPA or WEP to protect the wireless network. The default mode of wireless security is Disable.

Security Mode

WPA / WPA2 / WPA/WPA2 Pre-Shared Key

Security Parameters	
Security Mode	WPA/WPA2 Pre-Shared Key
WPA Shared Key	
Group Key Renewal	3600 seconds

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

WEP

Security Parameters	
Security Mode	WEP
WEP Authentication	Open System
Default Used WEP Key	1 2 3 4
Passphrase (Generate Key)	WEP64 WEP128
Key 1	Hex
Key 2	Hex
Key 3	Hex
Key 4	Hex

WEP 64 - Hex: 10 Hex codes, (1~9, a~f, A~F). EX. 11aa22cc33.
WEP 64 - ASCII: 5 ASCII characters are required. Insert your WEP key manually. EX: 1a3eb.
WEP 128 - Hex: 26 Hex codes, (1~9, a~f, A~F). EX. 11aa22cc33dd44ee55efffe35f.
WEP 128 - ASCII: 13 ASCII characters are required. Insert your WEP key manually. EX: 1a3e?!dbd3ert.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System**, **Share key** and **Both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

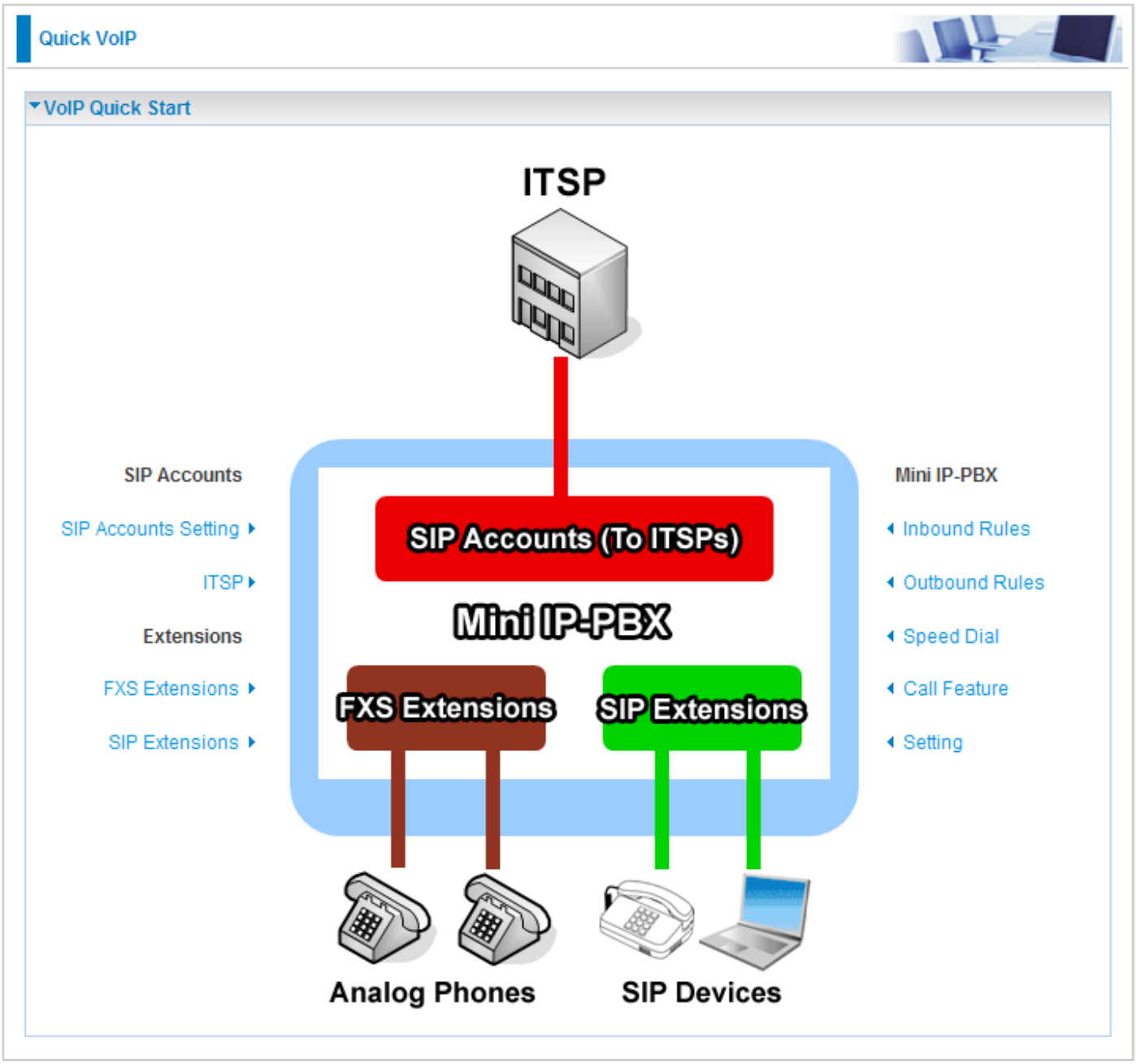
Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 or 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Quick VoIP (Only for 9300VN(X))

VoIP provides you the convenience & efficiency to make phone calls through your internet broadband. VoIP technology not only provides all the features and functions that PSTN (Public Switched Telephone Network) posseses, it also eables you to make international & long distance phone calls using IP at charging rate much lower than traditional phone. Thus, by using VoIP technology, you can save more money and embrace more functions.

BiPAC 9300VN(X) has a full support for SIP feature, it also has 2 fxs ports and a fxo port. User can apply for an SIP account from a phone company that offers internet phone service. You can then call your friends as you will use a traditional phone through the SIP account. In addition, the built in SIP proxy server feature also provides SIP phone terminal registration and connection within a company.

Quick VoIP provides a quick and simple way to configure the basic setting of your VoIP setting under the basic configuration mode.



SIP Accounts

SIP account is the SIP server that makes connection to the external VoIP service provider easy to establish. You can click **SIP Accounts Setting** and **ITSP** links to configure SIP accounts.

Extensions

The BiPAC router comes with 2 built in phone ports (FXS port) that enables the device to connect up to 2 phones. You can click **FXS Extensions** and **SIP Extensions** links to configure SIP Extensions.

Mini IP-PBX

Please click **Inbound Rules**, **Outbound Rules**, **Speed Dial**, **Call Feature** and **Setting** links to configure Mini IP-PBX parameters.

For VoIP configuration please refer to the **Advanced VoIP** section for detail description.

Advanced Configuration Mode

Status

9300VN(X)

Status

Device Information

Model Name	BiPAC 9300VNL
Host Name	home.gateway
System Up-Time	4 min(s)
Current Time	Thu Jan 1 00:04:10 1970
Software Version	1.00j
MAC Address	00:04:ed:11:22:aa
Serial Number	0000000000000002

Port Status

Ethernet	✓
GPON	✓
Wireless	✓

WAN

Port	Protocol Alloc_ID/Port_ID	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
GPON	dymanic 802/1002		No Response				

9300N(X)

Status

Device Information

Model Name	BiPAC 9300NL
Host Name	home.gateway
System Up-Time	14 min(s)
Current Time	Thu Jan 1 00:14:05 1970
Software Version	1.04f
MAC Address	00:50:c2:59:77:88
Serial Number	0000000000000088

Port Status

Ethernet	✓
GPON	✓
Wireless	✓

WAN

Port	Protocol Alloc_ID/Port_ID	Operation	Connection	IP Address	Netmask	Gateway	Primary DNS
GPON	dymanic 853/1344		No Response				

Device Information

Model Name: Displays the model name.

Host Name: Provide a name for the router for identification purposes. Host Name lets you change the router name.

System Up-Time: Records system up-time.

Current Time: Set the current time. See the Time Zone section for more information.

Software Version: Firmware version.

MAC Address: The LAN MAC address.

Serial Number: Displays the serial number of this router.

Port Status

Port Status: User can look up to see if they are connected to Ethernet, GPON and Wireless.

If ✕ is shown in GPON, the GPON port has not successfully connected or detected the optical signal.

If ✓ is shown in GPON, the GPON port has correctly connected.

If ⊘ is shown in GPON, the GPON connection has not been activated by OLT.

WAN

Port: Name of the WAN connection.

Protocol Alloc_ID/Port_ID: Allocation Identifier and GEM Port Identifier.

Operation: The current status in WAN interface.

Connection: The current connection status.

IP Address: WAN port IP address.

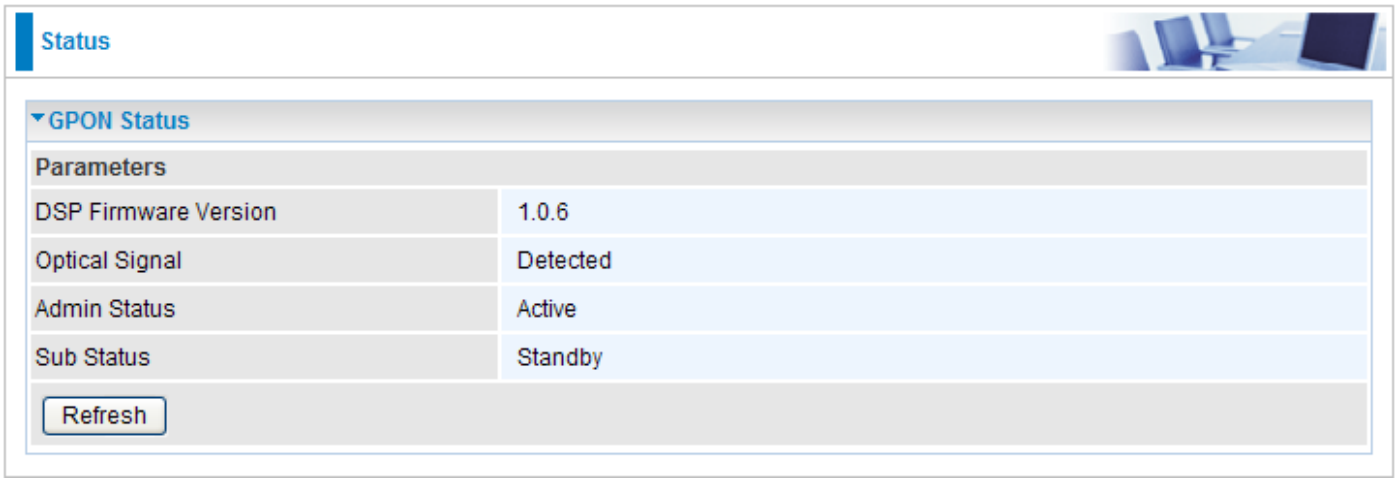
Netmask: WAN port IP subnet mask.

Gateway: The IP address of the default gateway.

Primary DNS: The IP address of the primary DNS server.

GPON Status

This section displays the overall status of GPON, such as DSP firmware version, Optical Signal, Admin Status and Sub Status.



DSP Firmware Version: DSP code version

Optical Signal: Current signal status

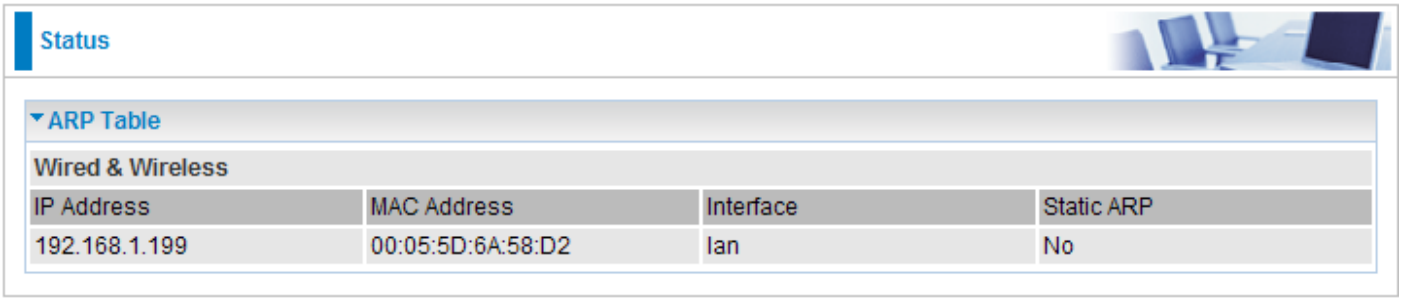
Admin Status: Current admin status

Sub Status: Show the state of GPON operation.

Note: Admin Status shows "Active" and Sub Status shows "Standby" when the router is ready. Admin Status shows "Active" and Sub Status shows "Operational" when the GPON connection is operated.

ARP Table

This section displays the router ARP (Address Resolution Protocol) Table which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way of determining the MAC address of the network interface of your PCs that use the Firewall – MAC Address Filter function. See the Firewall section of this manual for more information on this feature.



IP Address: Shows a list of IP addresses of devices on your LAN (Local Area Network).

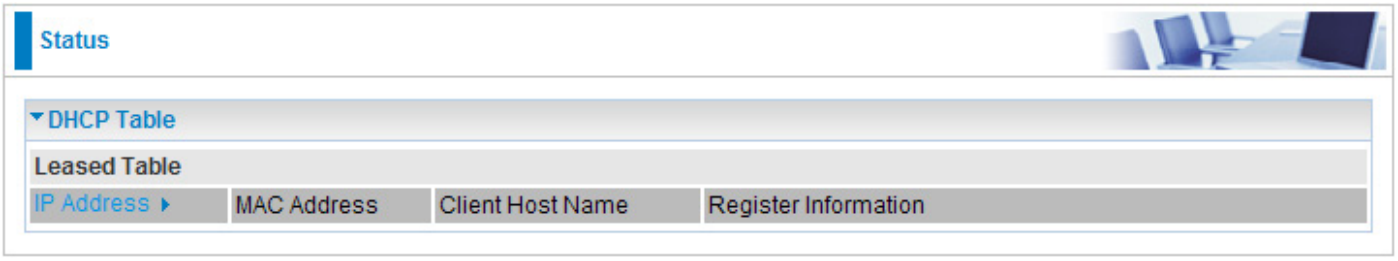
MAC Address: Shows the MAC (Media Access Control) addresses of each device on your LAN.

Interface: Shows the interface for the ARP item.

Static ARP: Shows the state of the static ARP item.

DHCP Table

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



IP Address: The current corresponding DHCP-assigned dynamic IP address of the device.

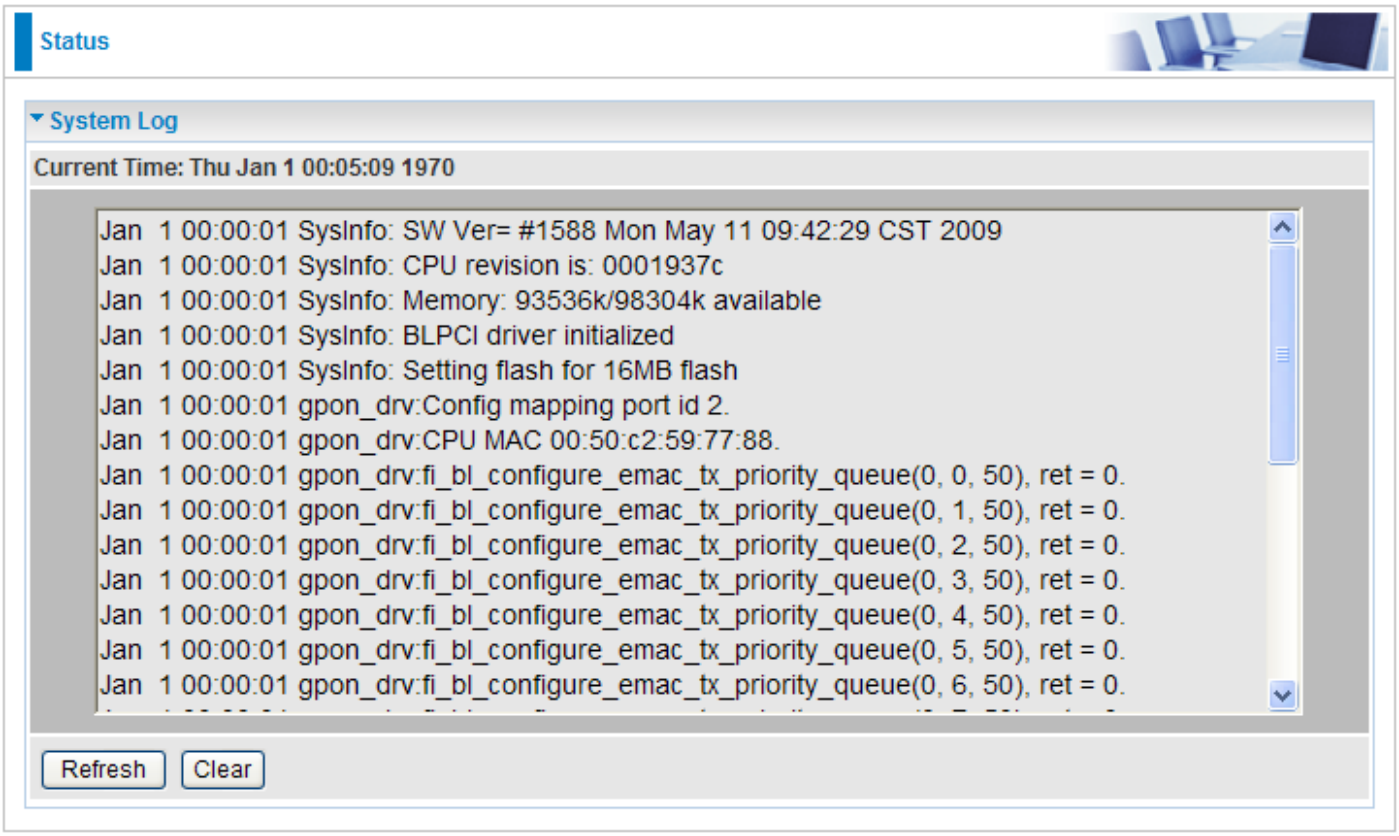
MAC Address: The MAC Address of internal dhcp client host.

Client Host Name: The Host Name of the internal dhcp client.

Register Information: Register time information.

System Log

Display system logs accumulated up to the present time. You can trace its historical information with this function.



Refresh: Click to update the system log.

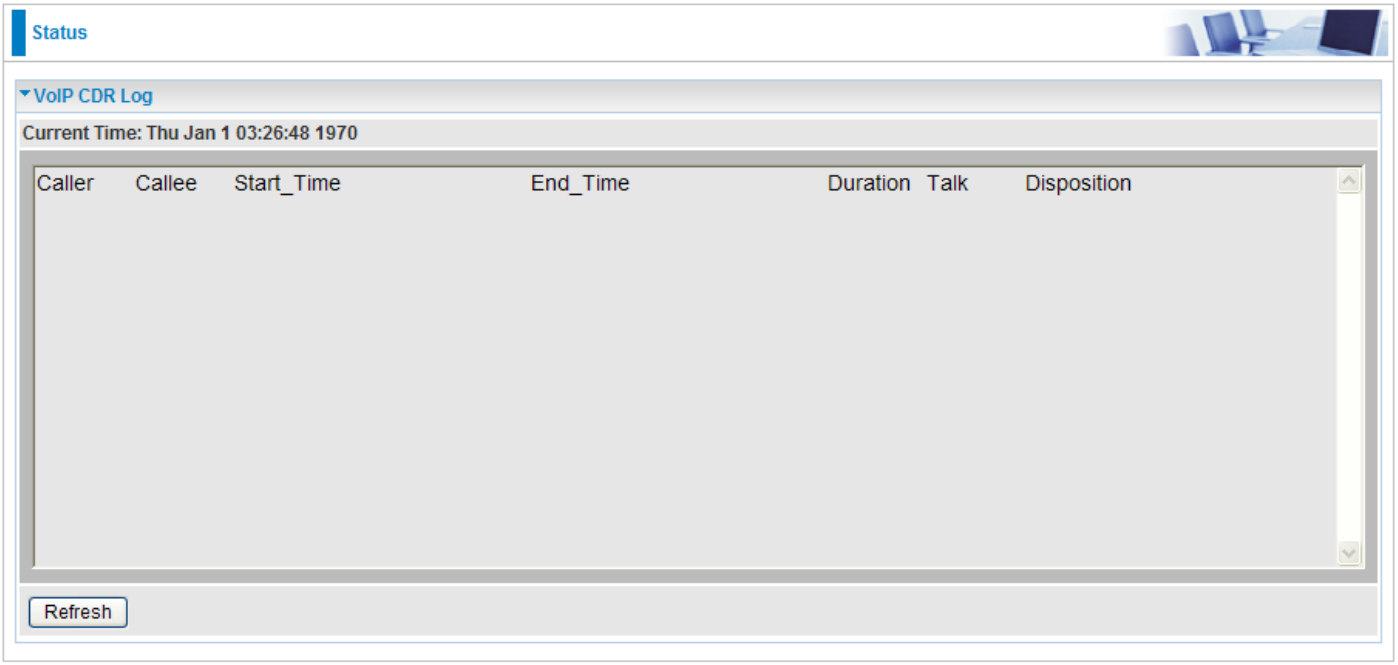
Clear: Click to clear the current log from the screen.

Firewall Log

Firewall Log displays the log information of any unexpected events that occurs to your firewall settings. This page displays the router Firewall Log entries which have been recorded when you have enabled Intrusion Detection or Block WAN PING in the Configuration – Firewall section of the interface. Please see the Firewall section of this manual for more details on how to enable Firewall event logging.

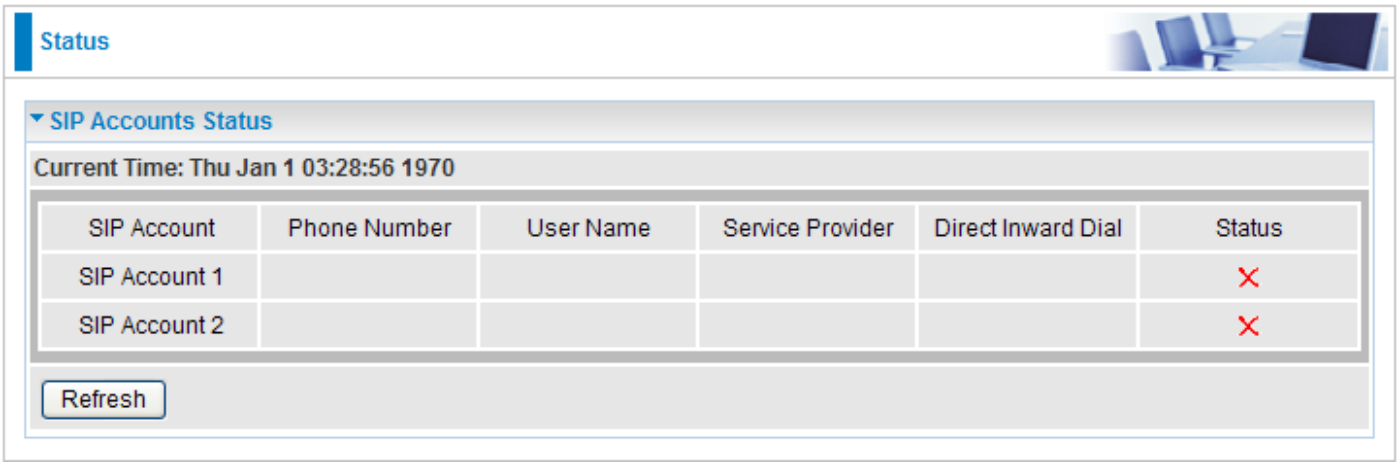
VoIP CDR Log (Only for 9300VN(X))

Display VoIP CDR logs accumulated up to the present time. You can see the associated information, including Caller, Callee, Start Time, End Time, Duration, Talk and Disposition, with this function.



SIP Accounts Status (ITSP) (Only for 9300VN(X))

This section lists the informaion of all the SIP accounts.



SIP Account: Display all the SIP accounts.

Phone Number: The phone number of the SIP account.

User Name: The registered user name of the SIP account.

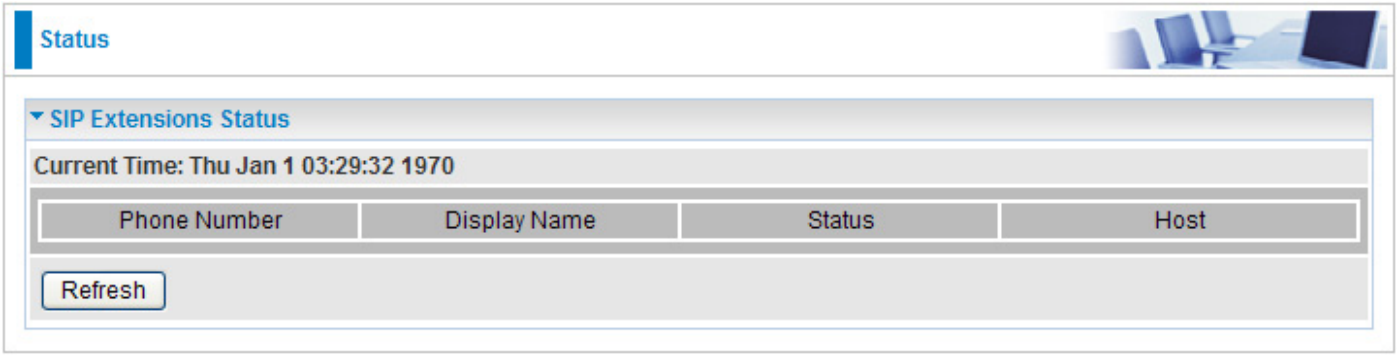
Service Provider: The VoIP service provider for the SIP account.

Direct Inward Dial: The direct inward dial of the SIP account.

Status: The connection state of the SIP account.

SIP Extensions Status (Only for 9300VN(X))

Displays the information of SIP extensions.



Phone Number: The phone number of the SIP extended connection.

Display Name: The name of this connection.

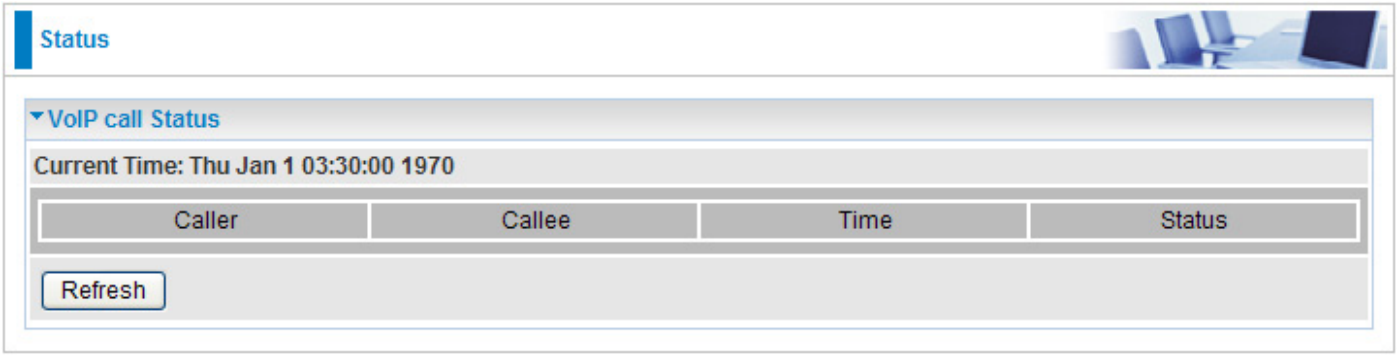
Status: The state of this connection.

Host: The host name of this connection.

VoIP Call Status (Only for 9300VN(X))

VoIP (Voice over Internet Protocol) is a technology for delivery of voice communications over IP networks such as the Internet. It involves in originating an Internet telephone call conversing the analog voice signal to digital format and compressing/translating the signal into Internet protocol packets for transmission over the Internet; the process is reversed at the receiving end.

This page displays the information of VoIP Call.



Caller: The terminal of the caller that initiates the call.

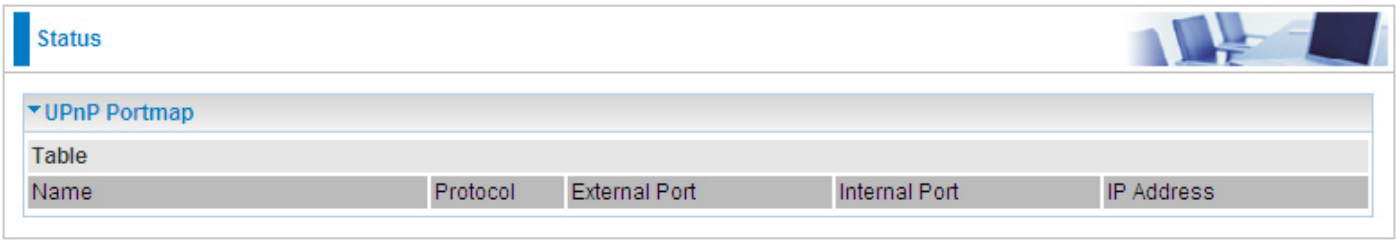
Callee: The terminal of the callee that is being called.

Time: The length of time for this VoIP call.

Status: The state of this VoIP call.

UPnP Portmap

This section lists all the established port-mapping using UPnP (Universal Plug and Play).



Name: The Host Name of the internal UPNP client.

Protocol: The connection protocol of the UPNP client.

External Port: The external port for this connection.

Internal Port: The internal port for this connection.

IP Address: IP of the internal UPNP client.

Configuration

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

LAN, **WAN**, **System**, **Firewall**, **QoS**, **Virtual Server**, **Time Schedule** and **Advanced**

The function of each configuration sub-item is described in the following sections.

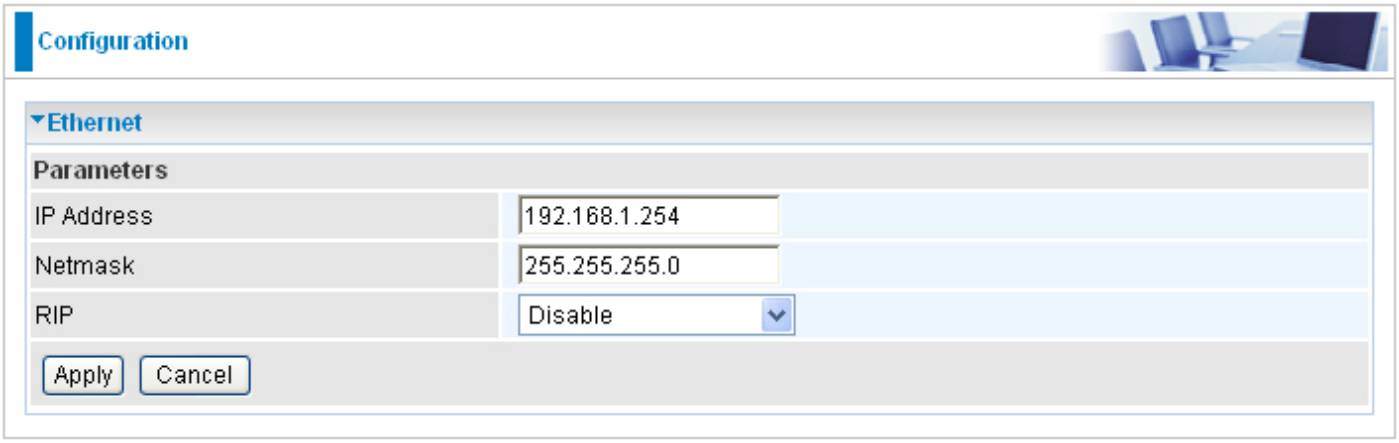
LAN - Local Area Network

A Local Area Network (LAN) is a shared communication system to which many computers are attached together and is limited to the immediate area, usually within the same building or storey of a building.

These are the items within the LAN section: **Ethernet**, **IP Alias**, **Wireless**, **Wireless Security**, **WPS** and **DHCP Server**.

Ethernet

The router supports more than one Ethernet IP addresses in the LAN that supports multiple internet access at the same time. Users usually only have one subnet in their LAN. The default IP address for the router is 192.168.1.254.



IP Address: The default IP address of this router.

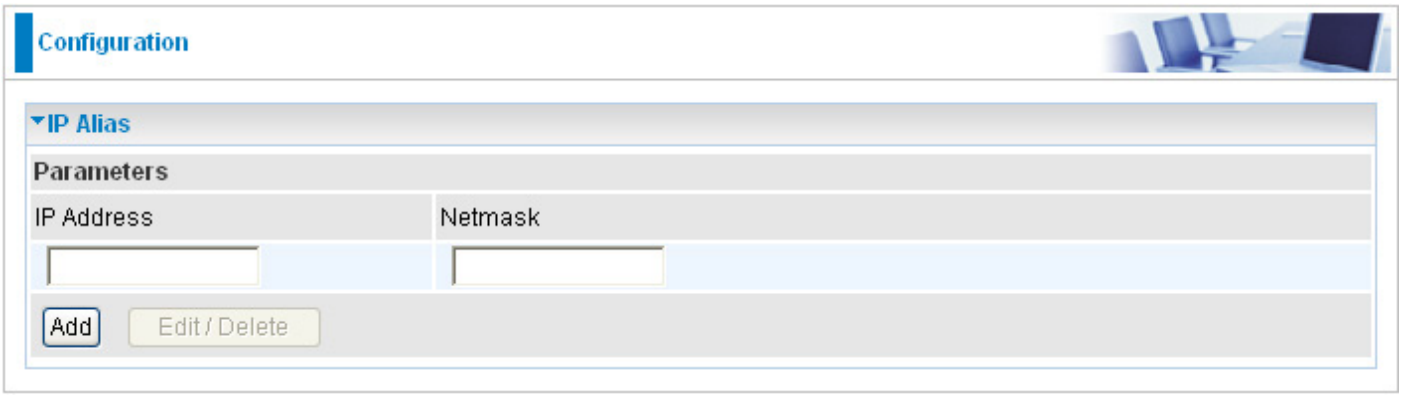
Netmask: The default subnet mask of this router.

RIP: RIP v1, RIP v2 Broacast, RIP v2 Multicast and RIP v1+v2 Broacast. Check to enable RIP function.

Click Apply to confirm the settings.

IP Alias

This function enables the creation of multiple virtual IP interfaces for this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.



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

Netmask: Specify a subnet mask for this virtual interface.

Click Add to confirm the settings.

Wireless

Configuration

Wireless

Parameters	
WLAN Service	Enable Disable
Mode	802.11g + n
ESSID	wlan-ap
Hide ESSID	Enable Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx PowerLevel	100 (0 ~ 100)
AP MAC Address	00:04:ED:11:22:AA
AP Firmware Version	RT2880 iNIC 1.1.8.0
WPS Service	Enable Disable
WPS State	Configured Unconfigured
WMM	Enable Disable
Wireless Distribution System (WDS)	
WDS Service	Enable Disable
Peer WDS MAC address	1. 2. 3. 4.

** WDS depends on the settings of main security encrption type. **

Apply Cancel Security settings

Parameters

WLAN Service: Default setting is set to Enable. If you do not have any wireless, select Disable.

Mode: The default setting is 802.11b+g+n (Mixed mode). If you do not know or do not have both 11g and 11b devices on your network, then keep the setting in mixed mode. From the drop-down menu, you can select 802.11g if you have only 11g card. If you have only 11b card, then select 802.11b. And if you have 11n card, select 802.11n.

ESSID: The ESSID is a unique name of a wireless access point (AP) used to distinguish one from another. For security purpose, change to a unique ID name which is already built into the router wireless interface. It is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the ESSID as the device in order to connect to your network.

Hide ESSID: This function enables the router to become invisible on the network. Thus, any clients using the wireless setting to search for available or specific router on the network will not be able to discover the router whose Hide ESSID function is set to enabled. The default setting is disabled.

> **Enable:** When enabled, you do not broadcast your ESSID. Therefore, no one will be able to locate the Access Point (AP) of your router.
>
> **Disable:** When disabled, you allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection ID channel that you would like to use.

Note: Wireless performance may degrade if the selected ID channel is already being occupied by other AP(s).

Channel width: Select either 20 MHz or 20/40 MHz for the channel bandwidth. The higher the bandwidth the better the performance will be.

TX PowerLevel: It is a function that enhances the wireless transmission signal strength. User may adjust this power level from minimum 0 up to maximum 100.

Note: The power level may be different in each accss network uer premise environment, so choose the most suitable level for your network.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

WPS Service: Select Enable if you would like to activate WPS service.

WPS State: You can set the WPS state as Configured or Unconfigured.

WMM: This feature is used to control the prioritization of traffic according to 4 Access categories: Voice, Video, Best Effort and Background. Default is set to disable.

Wireless Distribution System (WDS)

It is a wireless access point mode that enables wireless link and communication with other access points. It is easy to install simply by defining the peer's MAC address of the connected AP. WDS takes advantage of the cost saving and flexibility which no extra wireless client device is required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network. It can connect up to 4 wireless APs for extending cover range at the same time.

In addition, WDS also enhances its link connection security mode. Key encryption and channel must be the same for both access points.

WDS Service: The default setting is disabled. Check Enable radio button to activate this function.

Peer WDS MAC Address: It is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to acknowledge and communicate with each other.

1. **Peer WDS MAC Address:** It is the second associated AP's MAC Address.
2. **Peer WDS MAC Address:** It is the third associated AP's MAC Address.
3. **Peer WDS MAC Address:** It is the fourth associated AP's MAC Address.

Note: For MAC Address, semicolon (:) must be included.

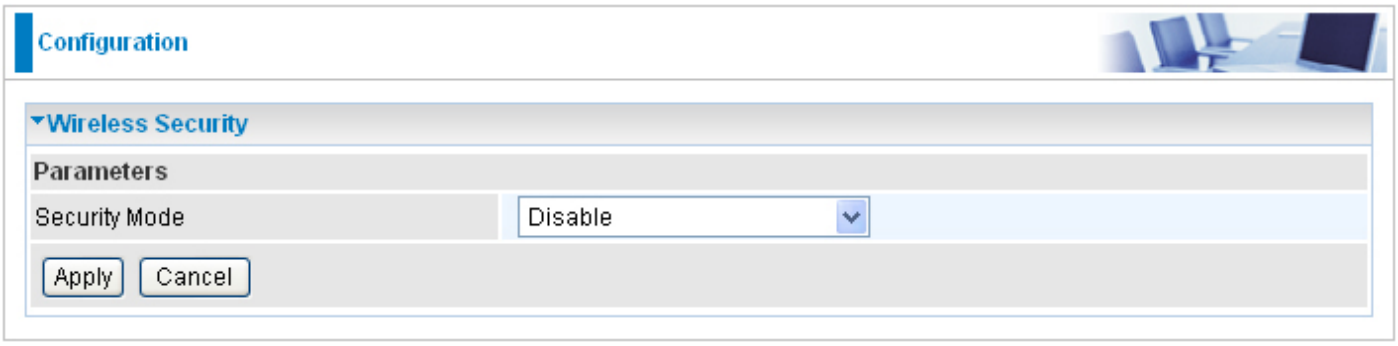
You can click Security settings link next to Cancel button to go to Wireless Security screen (see **Wireless Security** section).

Click Apply to confirm the settings.

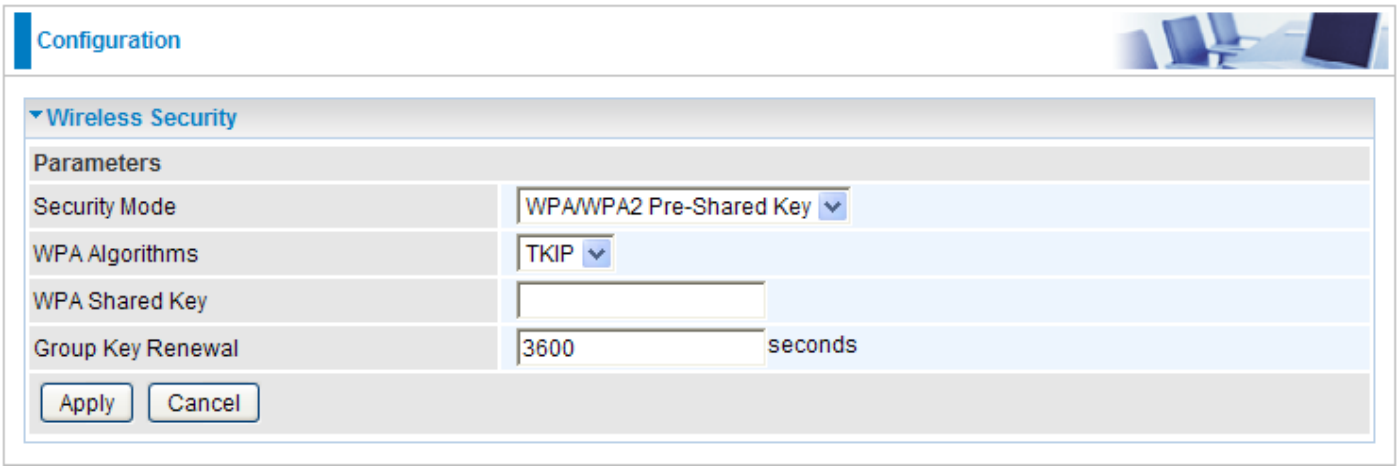
Wireless Security

You can disable or enable the wireless security function using WPA or WEP for wireless network protection.

The default mode of wireless security is disabled.



WPA / WPA2 / WPA/WPA2 Pre-Shared Key



Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

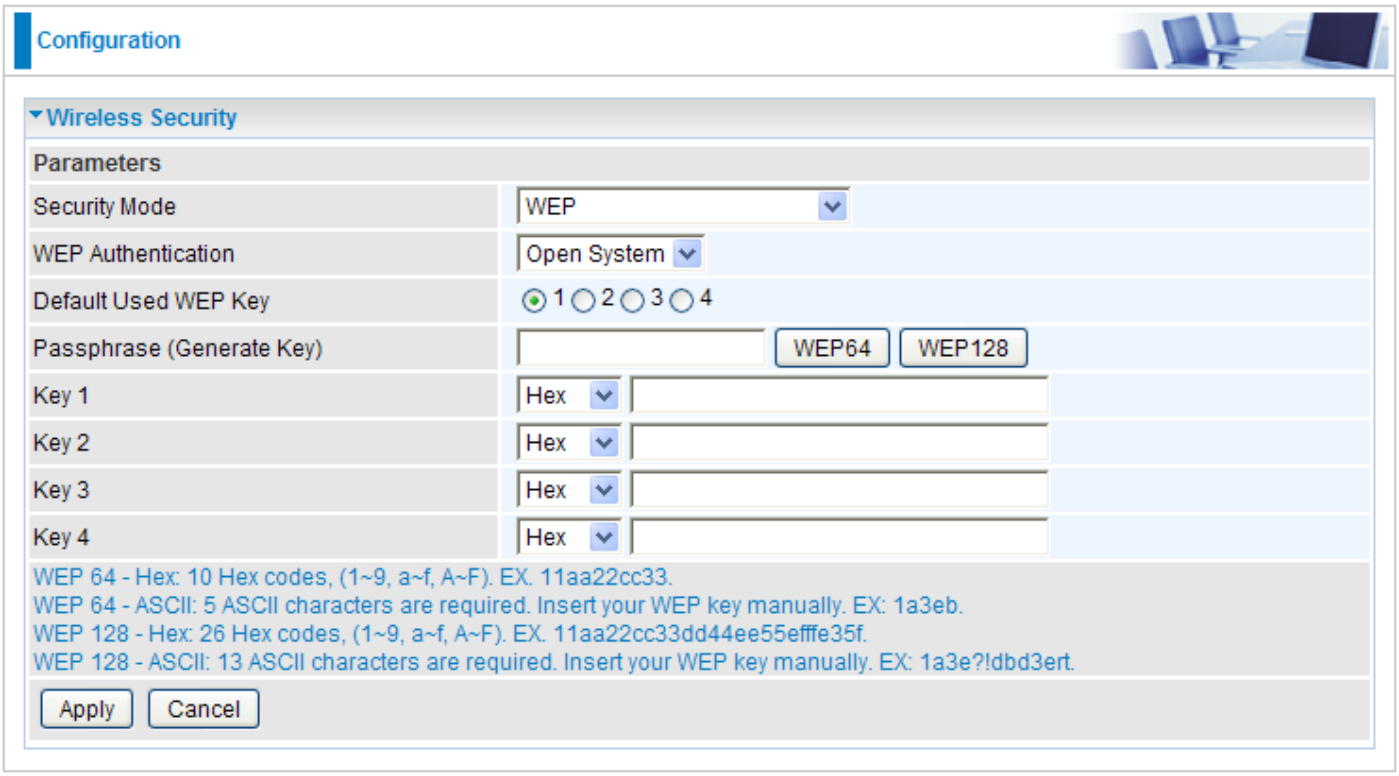
WPA Algorithms: There are 3 types of the WPA-PSK, WPA2-PSK & WPA/WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is 3600 seconds.

Click Apply to confirm the settings.

WEP



Security Mode: You can disable or enable with WPA or WEP for protecting wireless network.

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are three options to select from: **Open System**, **Share Key** or **Both**.

Default Used WEP Key: Select the encryption key ID; please refer to **Key (1~4)** below.

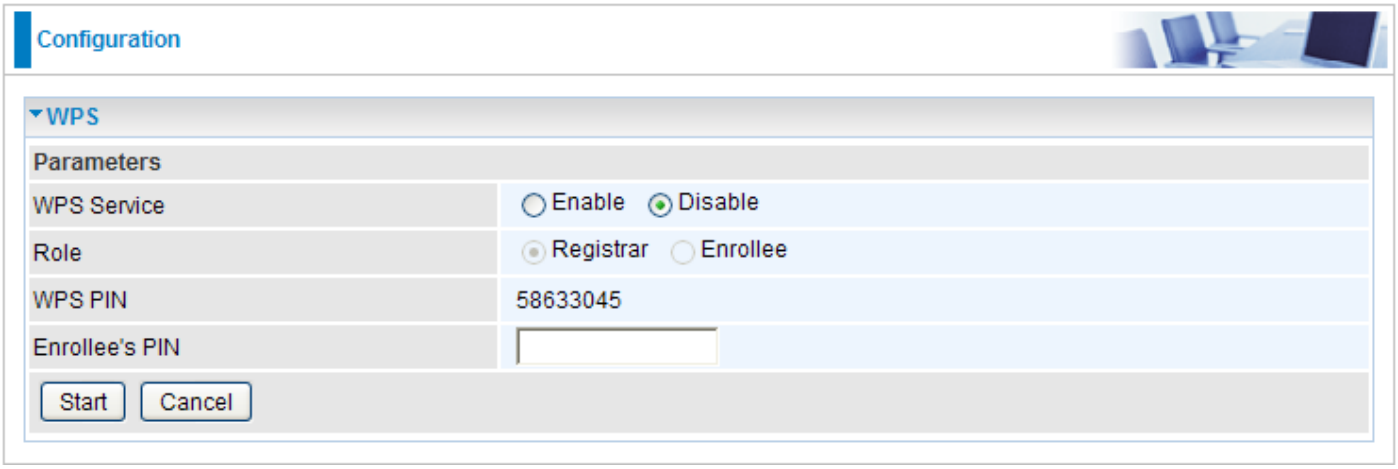
Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128.

Key (1~4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX or ASCII style, 5 and 13 ASCII codes are required for WEP64 and WEP128 or 10 and 26 HEX codes are required for WEP64 and WEP128 respectively.

Click Apply to confirm the settings.

WPS

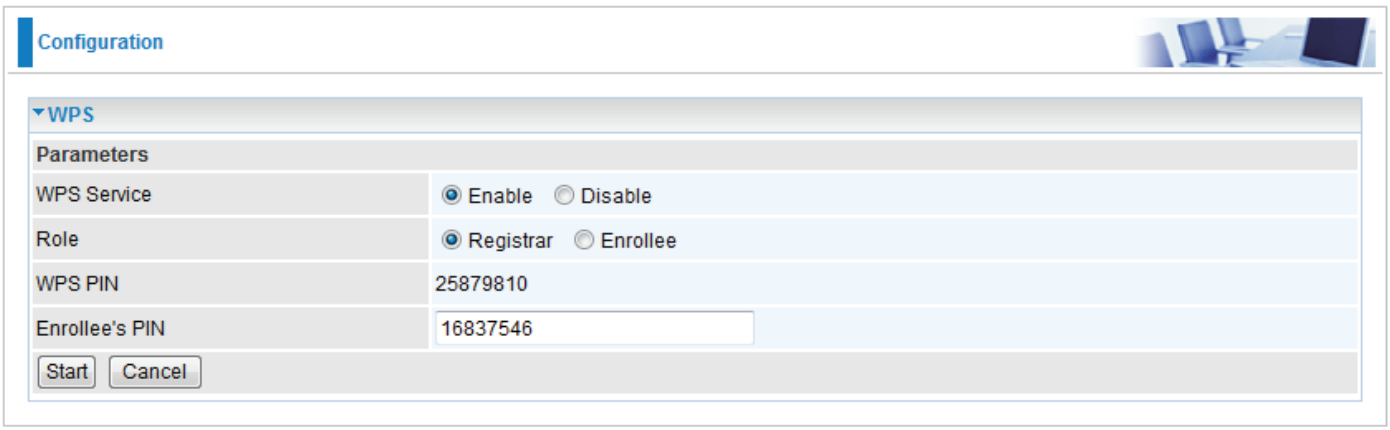
WPS (WiFi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi networks for a residential or an office setting. WPS supports two types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.



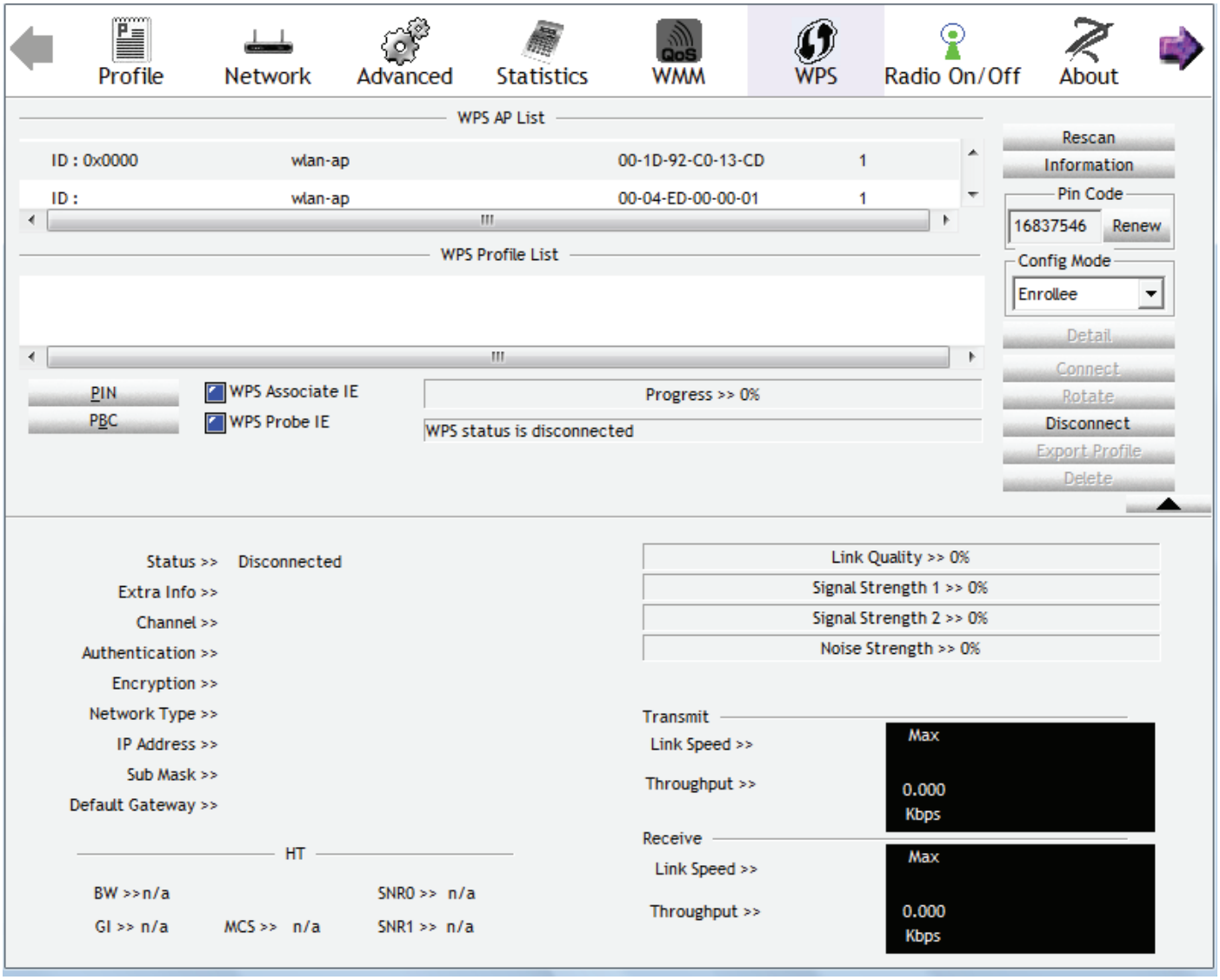
Wi-Fi Network Setup

PIN Method: Configure AP as Registrar

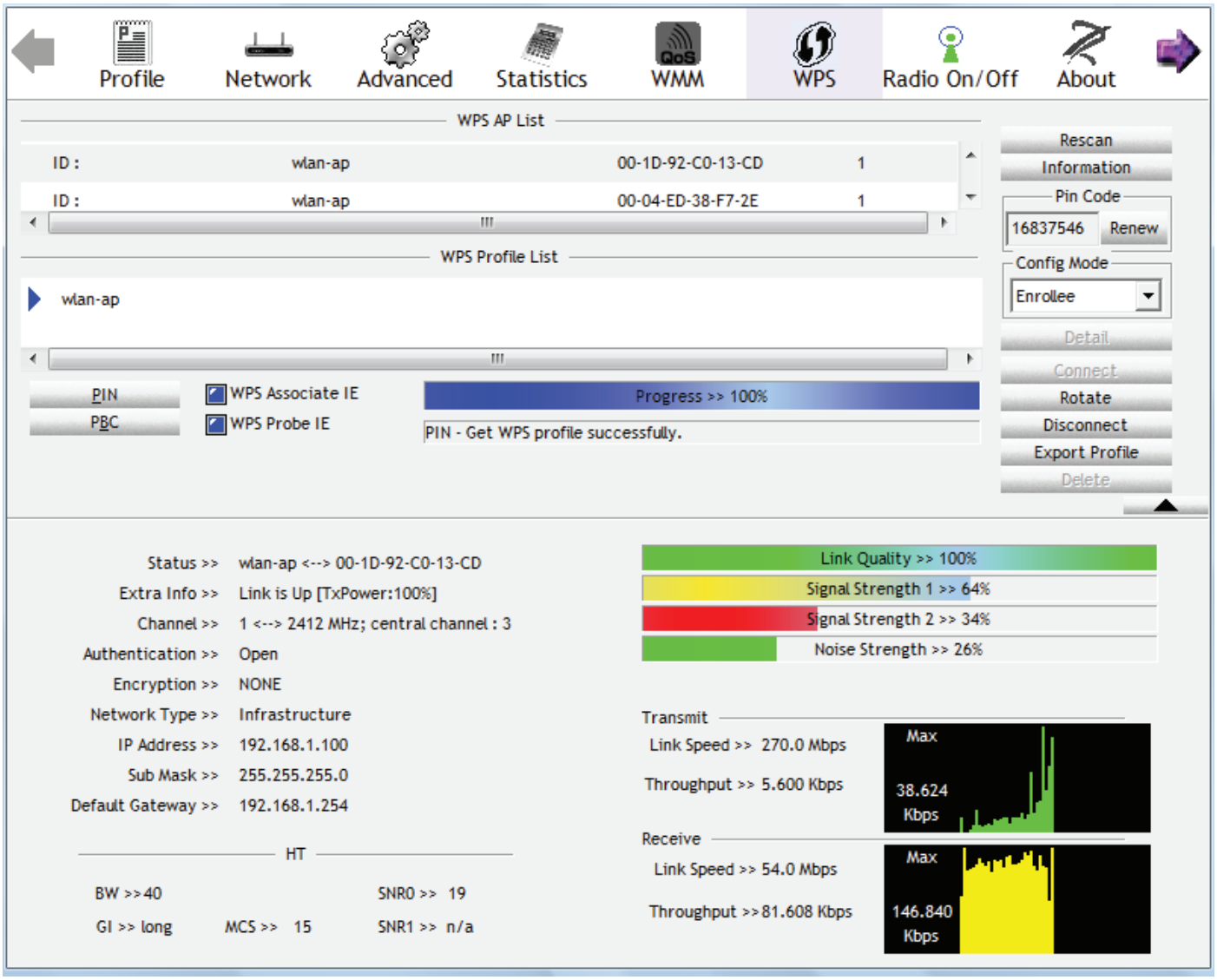
1. Jot down the client's Pin (eg. 16837546).



2. Enter the Enrollee's PIN number and then press Start.
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. wlan-ap) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.

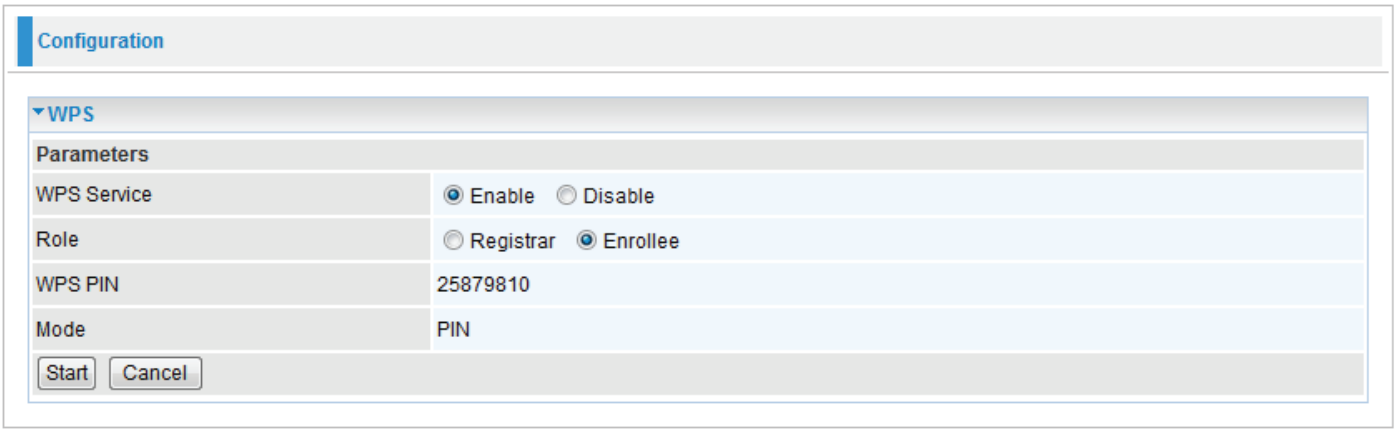


4. The client's SSID and security setting will now be configured to match the SSID and security setting of the registrar.

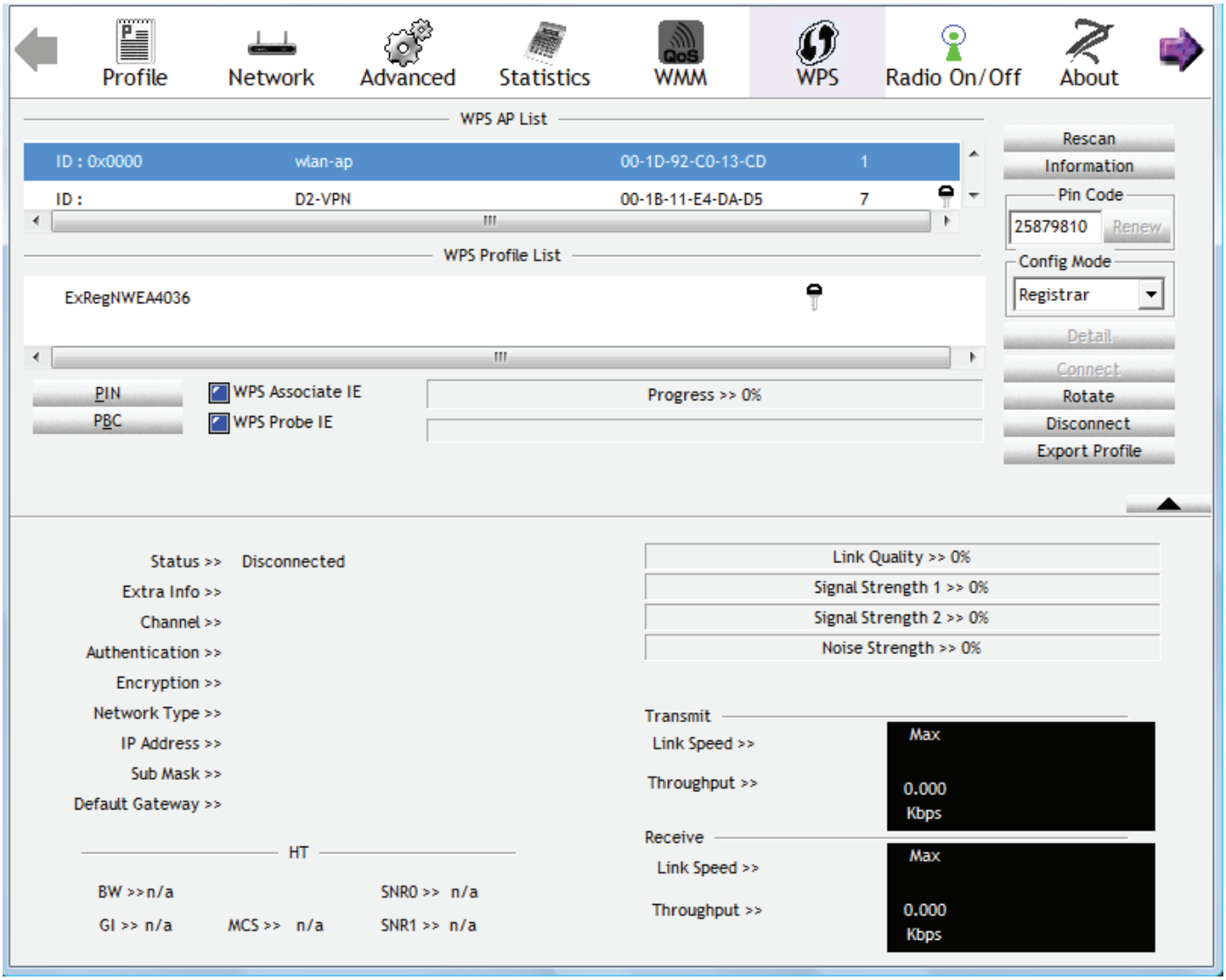


PIN Method: Configure AP as Enrollee

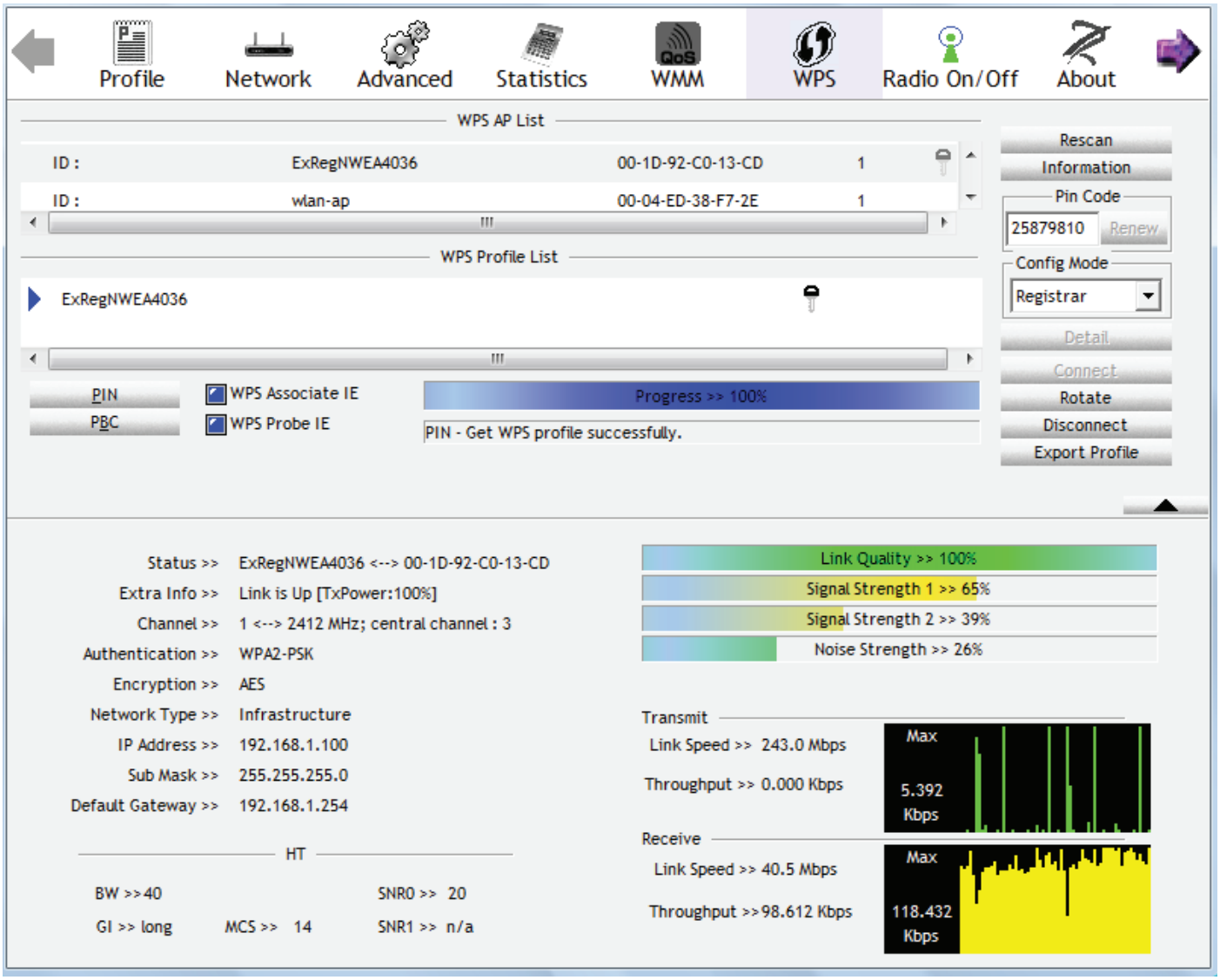
1. In the WPS configuration page, change the Role to Enrollee. Then press Start.
2. Jot down the WPS PIN (eg. 25879810).



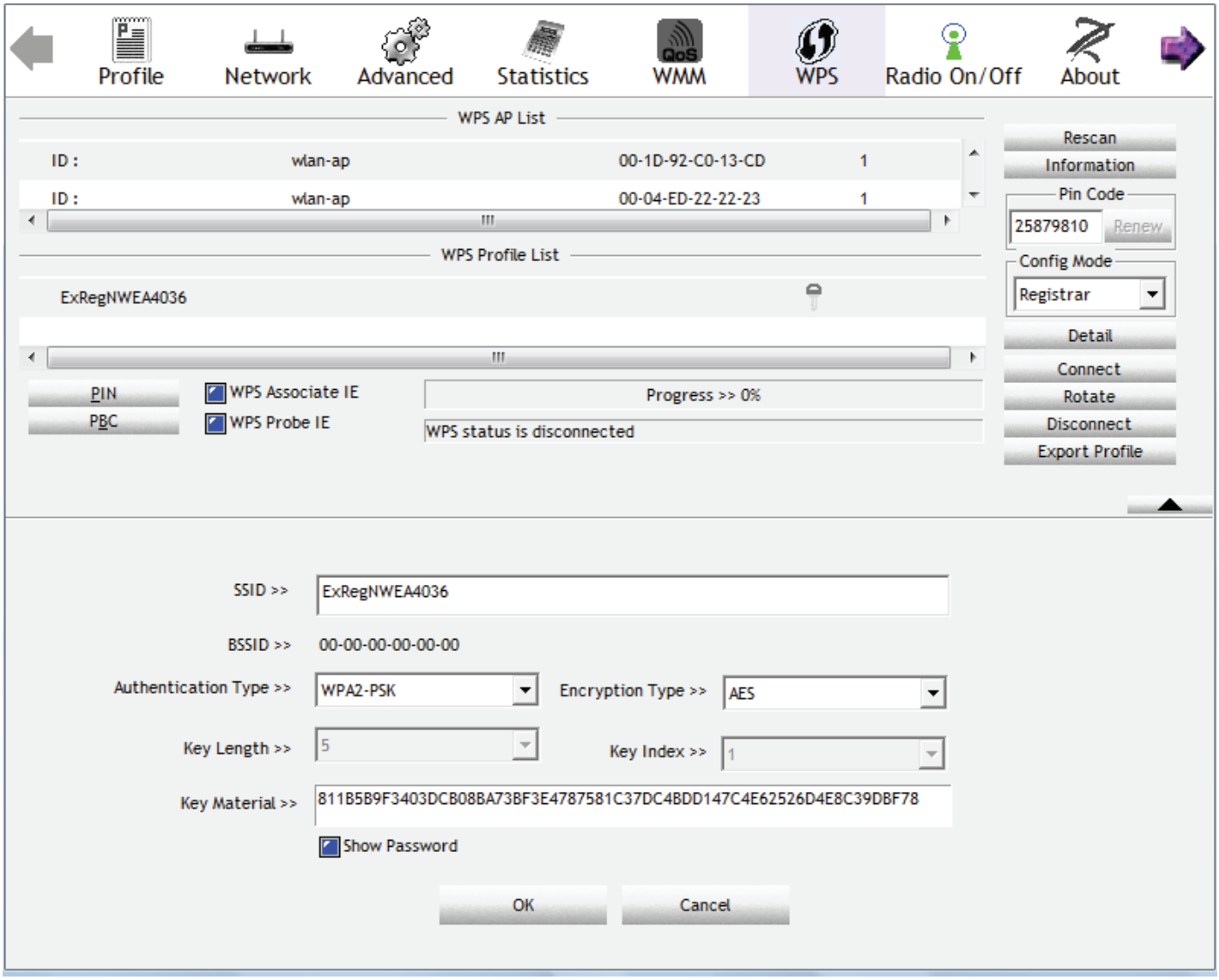
3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PIN button to run the scan.



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



5. Now to make sure that the setup is correctly done, cross check to see if the SSID and the security setting of the registrar setting match with the parameters found on both Wireless Configuration and Wireless Security Configuration page.



Wireless

Parameters	
WLAN Service	Enable Disable
Mode	802.11g + n
ESSID	ExRegNWEA4036
Hide ESSID	Enable Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	1.1.7.0
WPS Service	Enable Disable
WPS State	Configured Unconfigured
WMM	Enable Disable
Wireless Distribution System (WDS)	
WDS Service	Enable Disable
Peer WDS MAC address	1. 2. 3. 4.

Apply Cancel Security settings

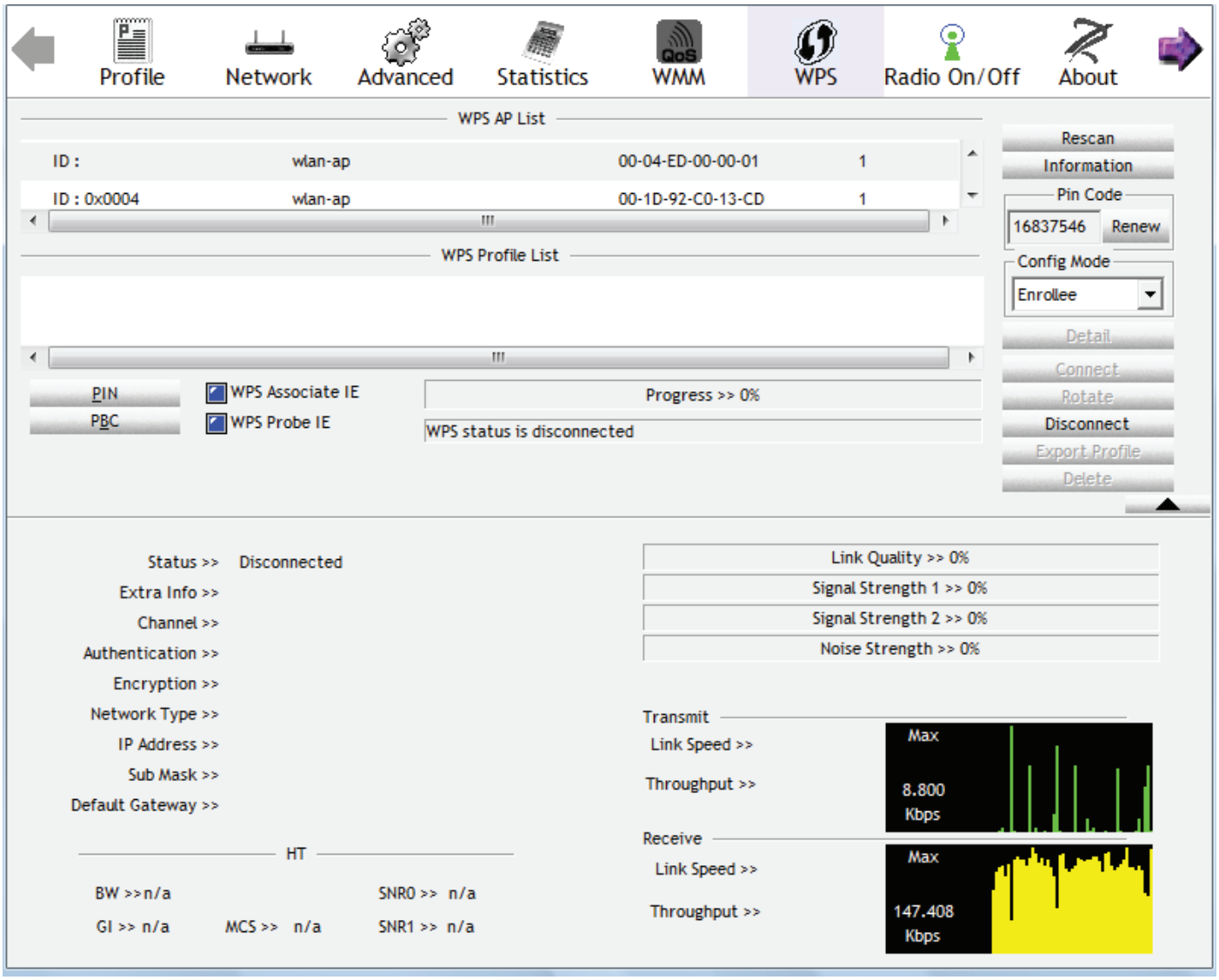
Wireless Security

Parameters	
Security Mode	WPA2 Pre-Shared Key
WPA Algorithms	AES
WPA Shared Key	811B5B9F3403DCB08I
Group Key Renewal	3600 seconds

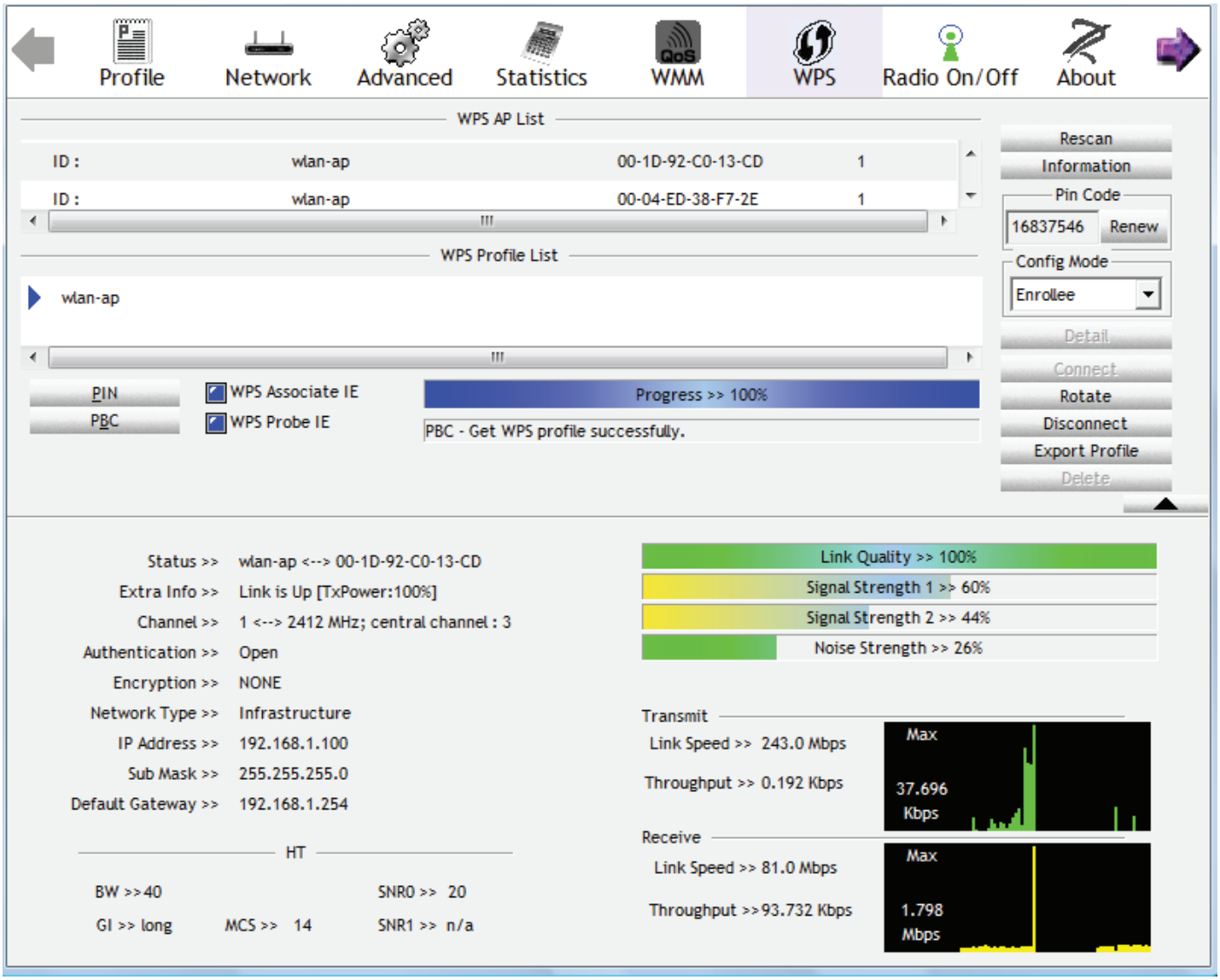
Apply Cancel

PBC Method:

1. Press the PBC button of the AP.
2. Launch the wireless client's WPS Utility (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. wlan-ap) from the WPS AP List section before pressing the PBC button to run the scan.

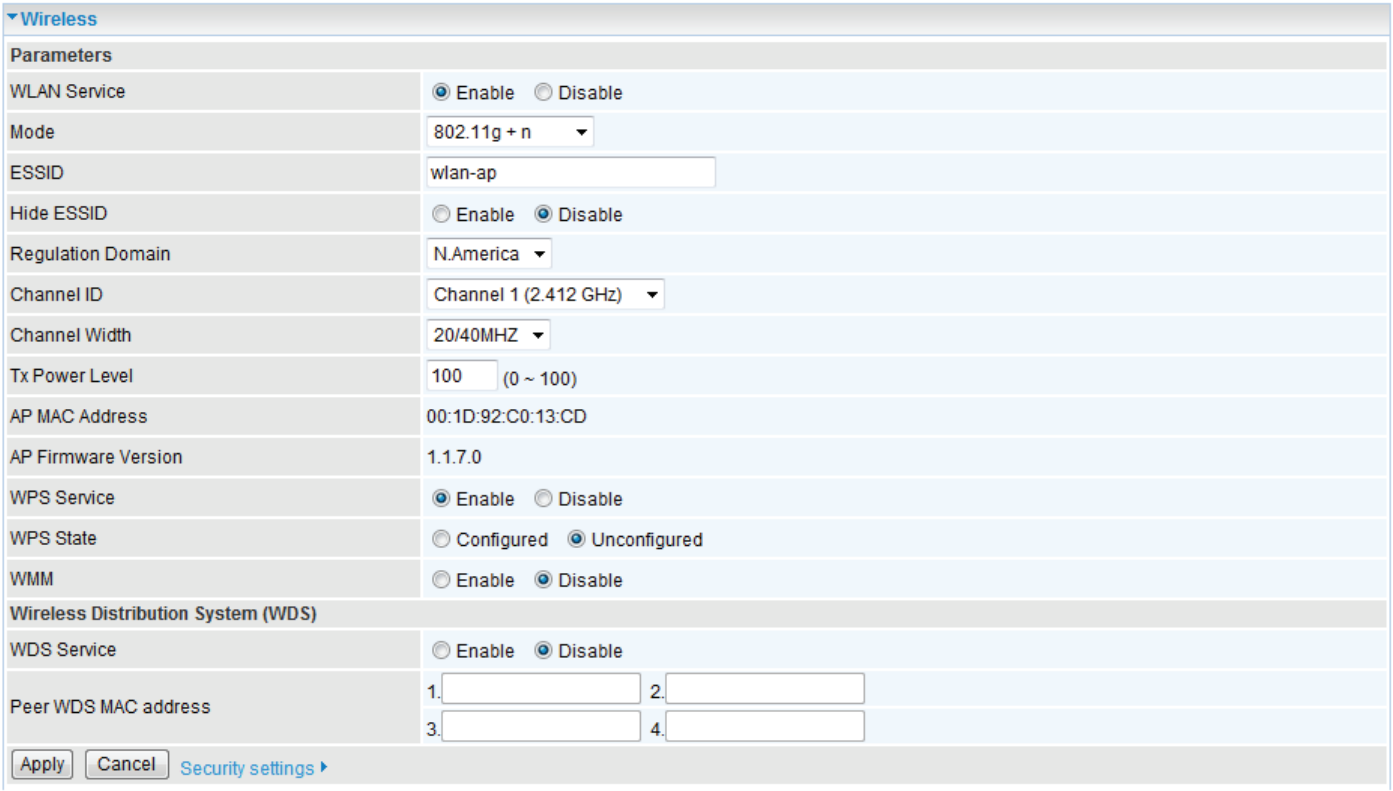


3. When the PBC button is pushed, a wireless communication will be established between your router and the PC. The client's SSID and security setting will now be configured to match the SSID and security setting of the router.



Wi-Fi Network Setup with Windows Vista WCN:

1. Jot down the AP PIN from the Web (eg. 25879810).
2. Access the Wireless configuration of the web GUI. Enable WPS service, set the WPS State to Unconfigured and then click Apply.

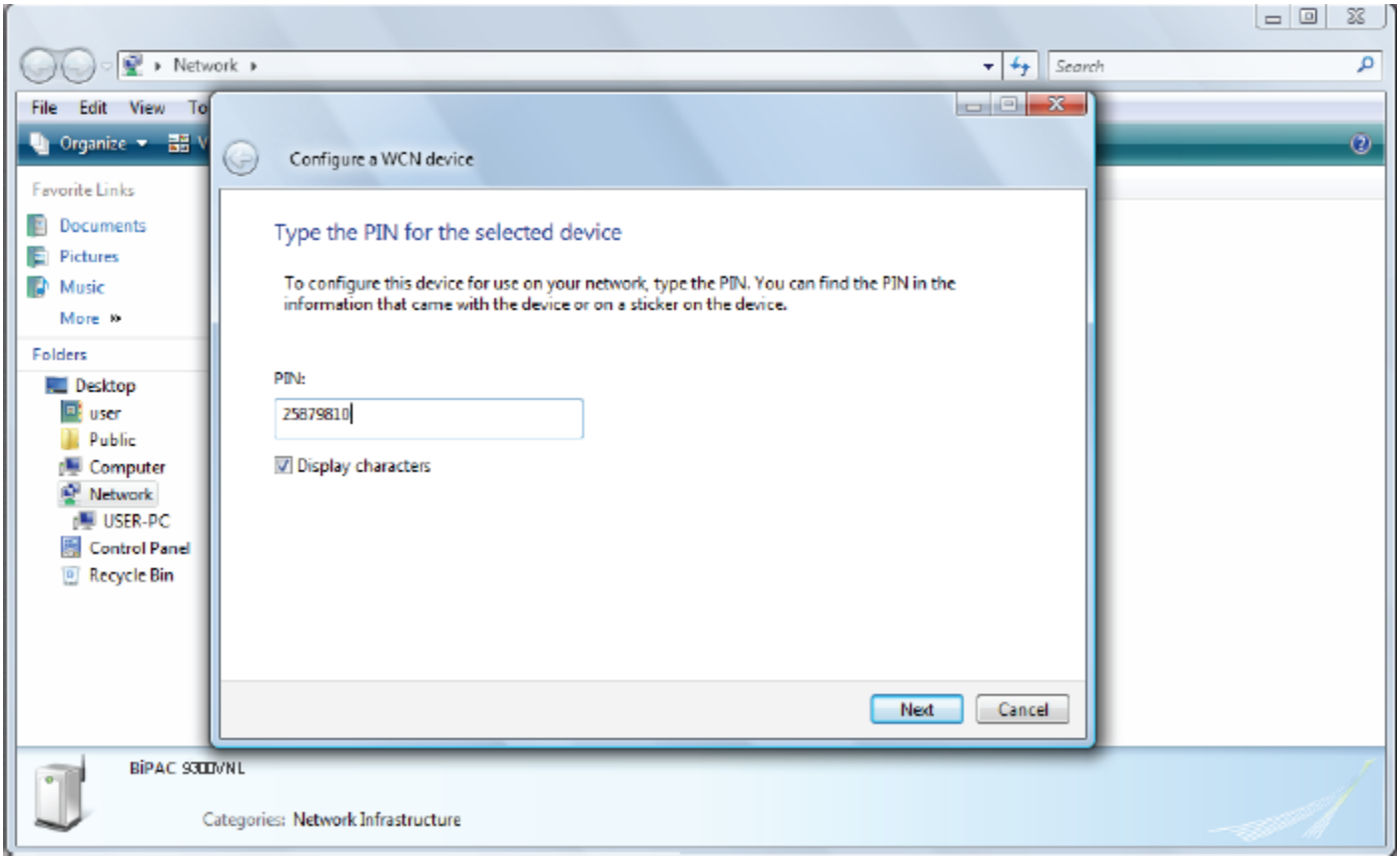


Wireless

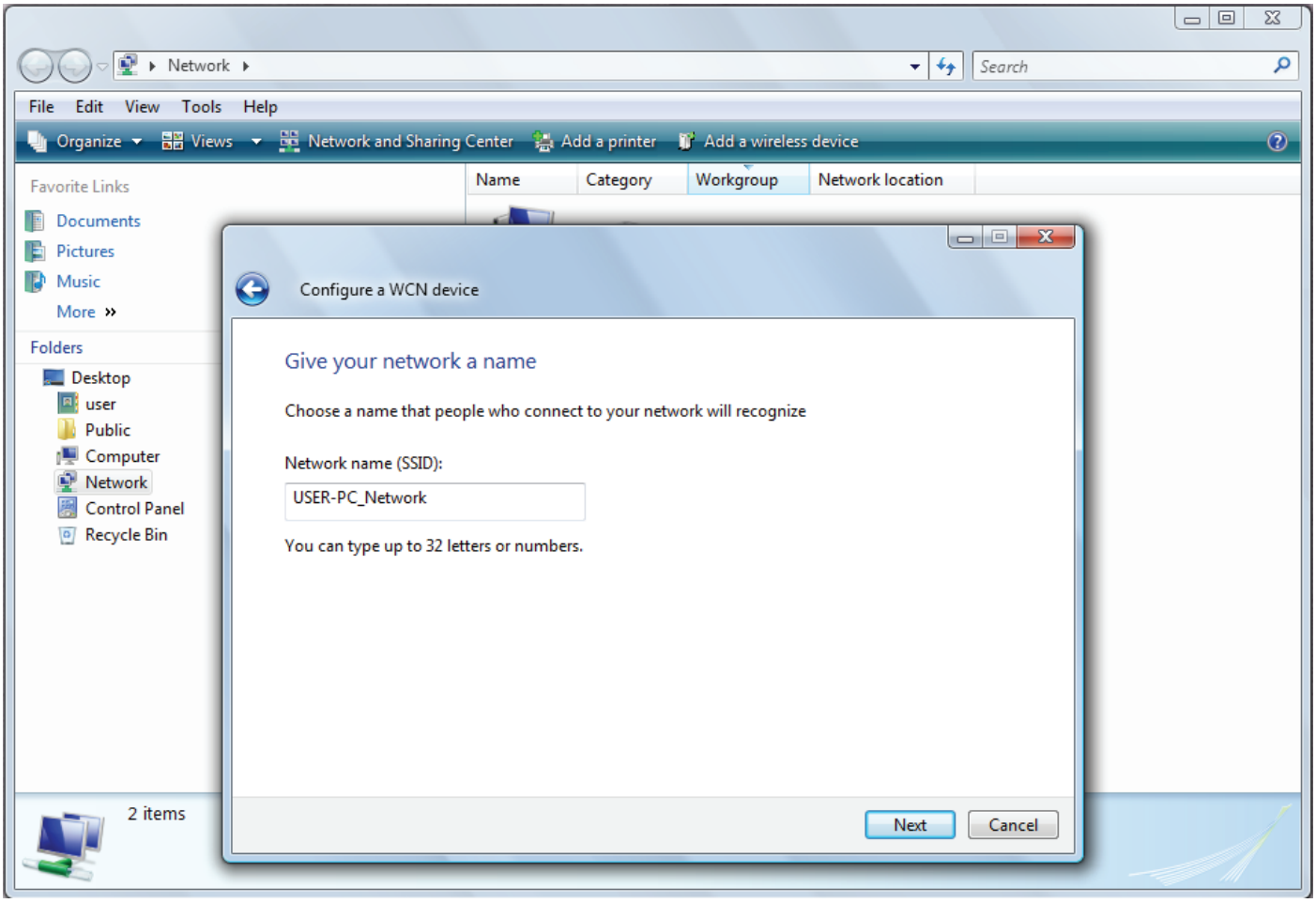
Parameters	
WLAN Service	Enable Disable
Mode	802.11g + n
ESSID	wlan-ap
Hide ESSID	Enable Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Channel Width	20/40MHZ
Tx Power Level	100 (0 ~ 100)
AP MAC Address	00:1D:92:C0:13:CD
AP Firmware Version	1.1.7.0
WPS Service	Enable Disable
WPS State	Configured Unconfigured
WMM	Enable Disable
Wireless Distribution System (WDS)	
WDS Service	Enable Disable
Peer WDS MAC address	1. 2. 3. 4.

Apply Cancel Security settings

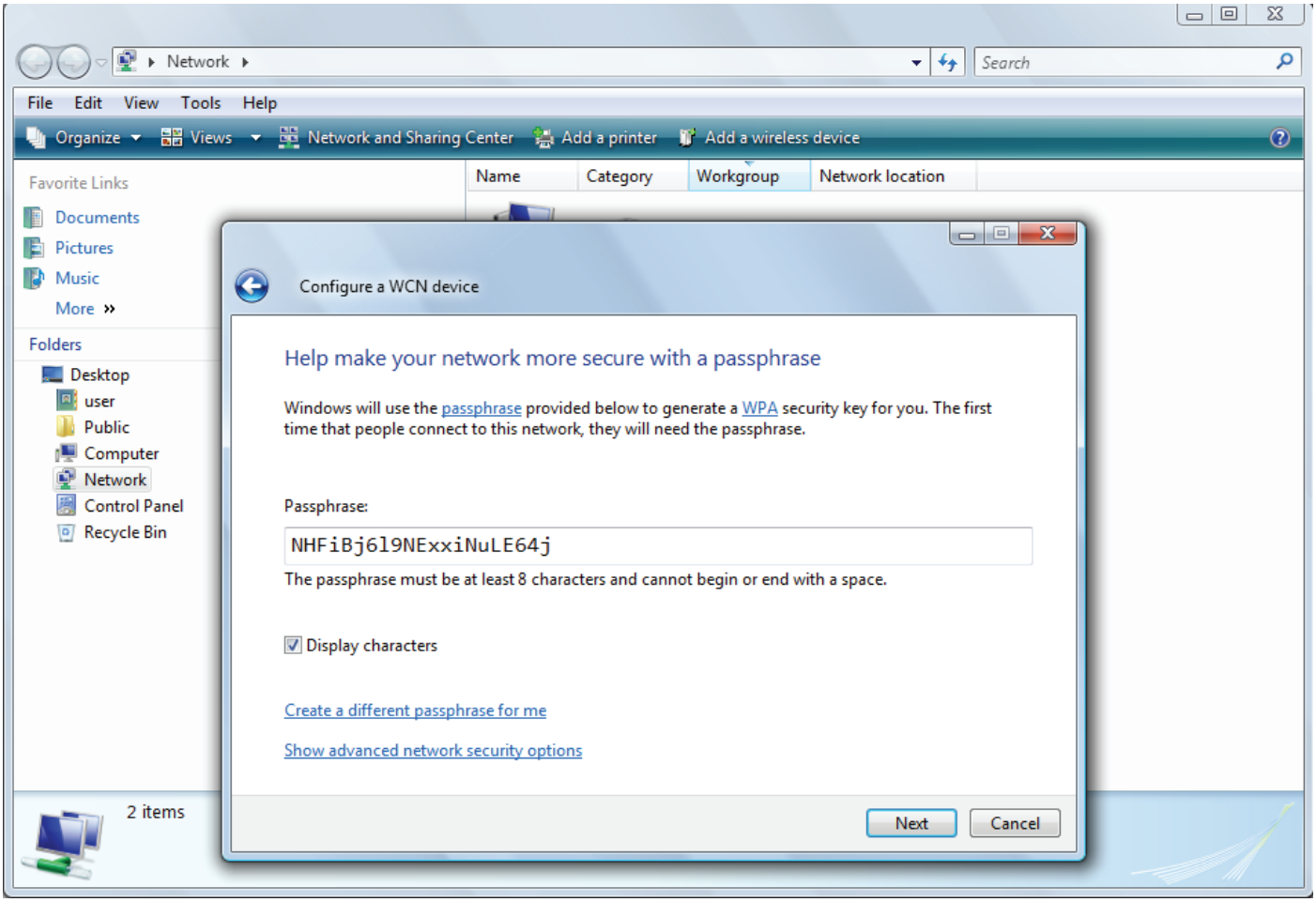
3. In your Vista operating system, access the Control Panel page, then select Network and Internet > View Network Computers and Devices. Double click on the BiPAC 9300VN(X)/9300N(X) icon and enter the AP PIN in the column provided then press Next.



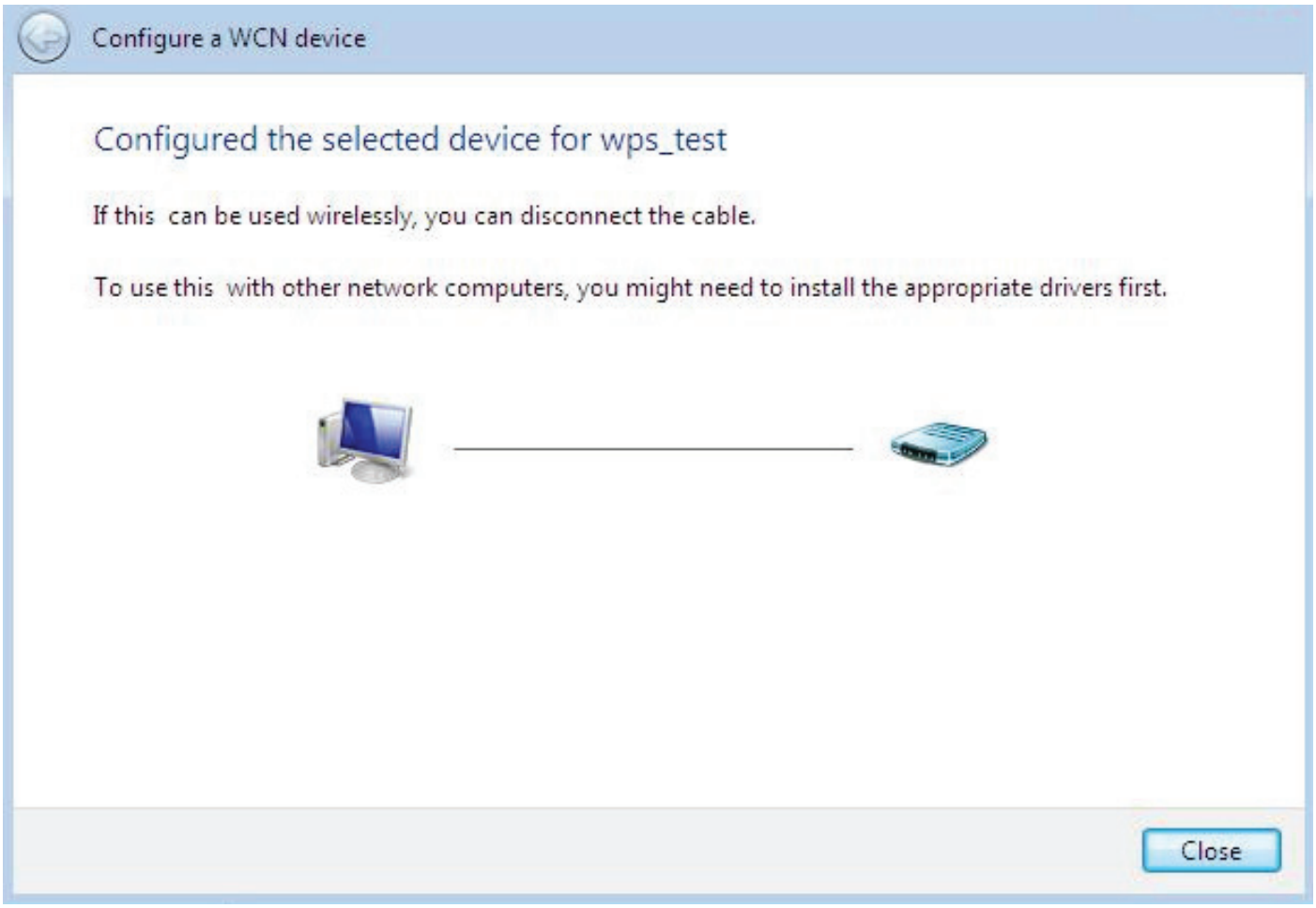
4. Enter the AP SSID then click Next.



5. Enter the passphrase then click Next.

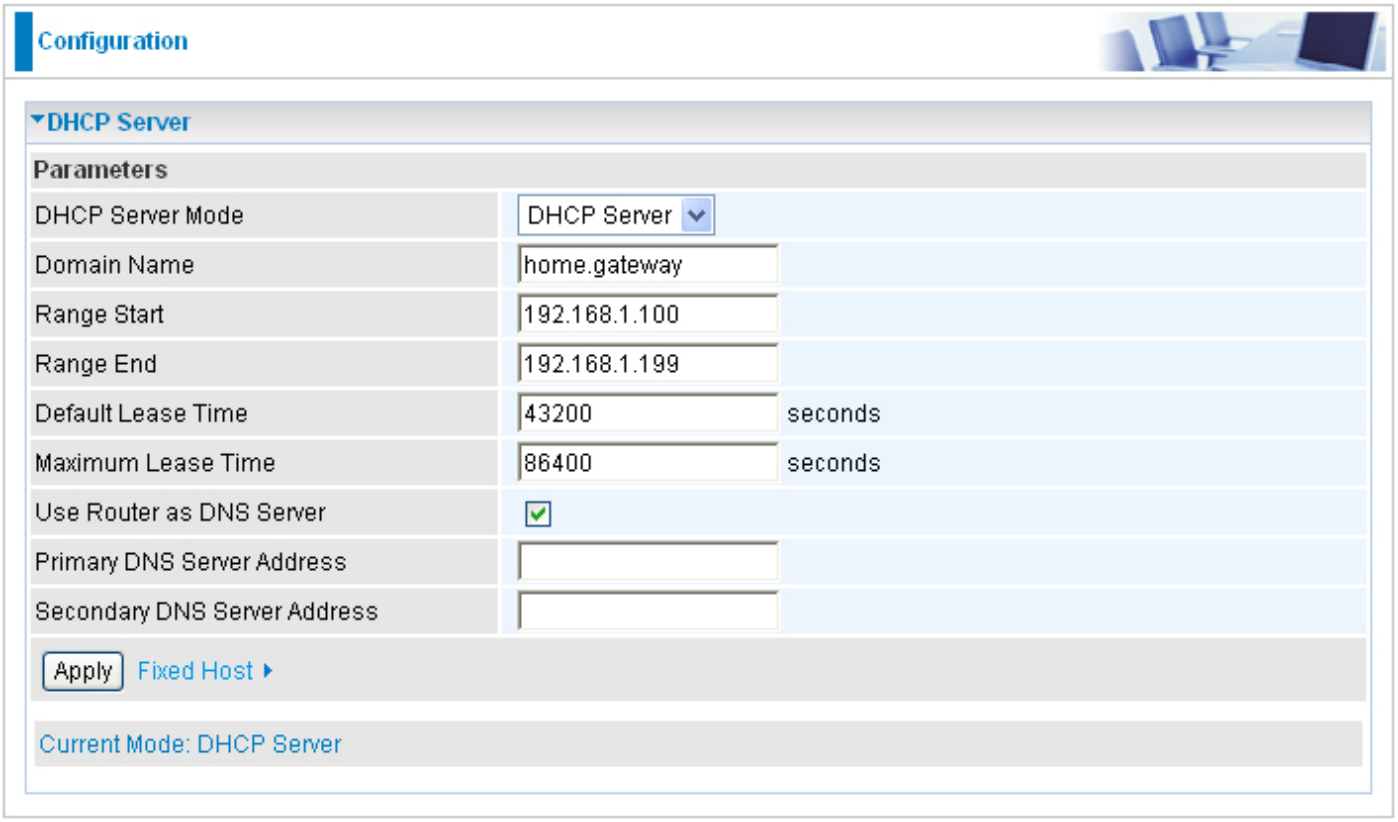


6. When you have come to this step, you will have comleted the Wi-Fi network setup using the built-in WCN feature in Windows Vista.



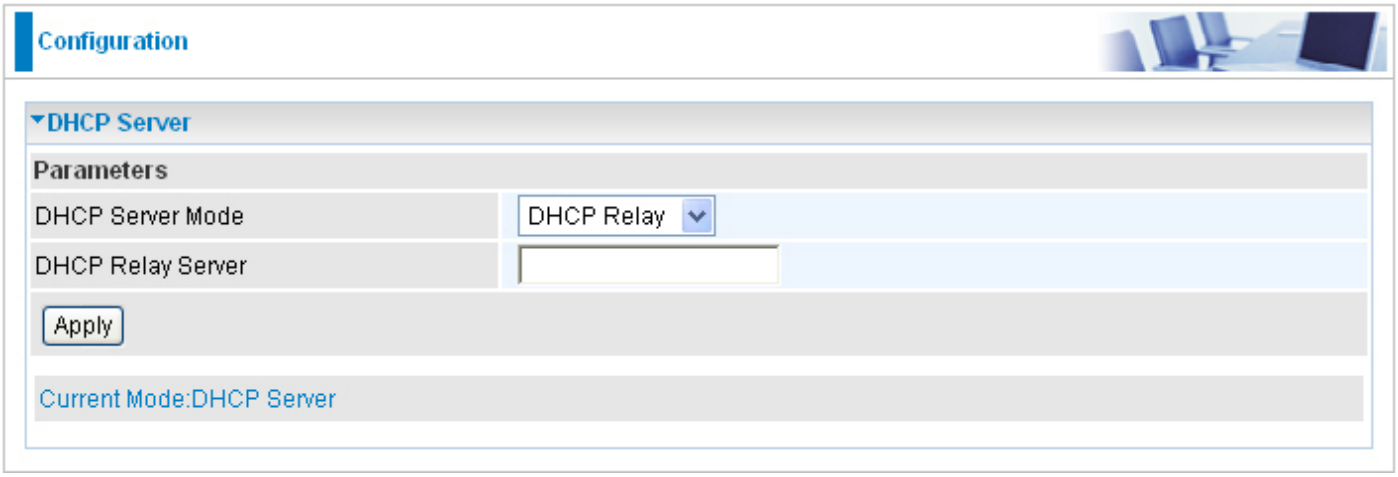
DHCP Server

DHCP allows networked devices to obtain information on the parameter of IP, Netmask, Gateway as well as DNS through the Ethernet Address of the device.



To configure the router's DHCP Server, select **DHCP Server** from the DHCP Server Mode drop-down menu. You can then configure parameters of the DHCP Server including the domain, IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. If you check "Use Router as a DNS Server", the GPON Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network). Click Apply to enable this function.

If you select **DHCP Relay** from the DHCP Server Mode drop-down menu, you must enter the IP address of the DHCP server that assigns an IP address to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP. Click Apply to enable this function.



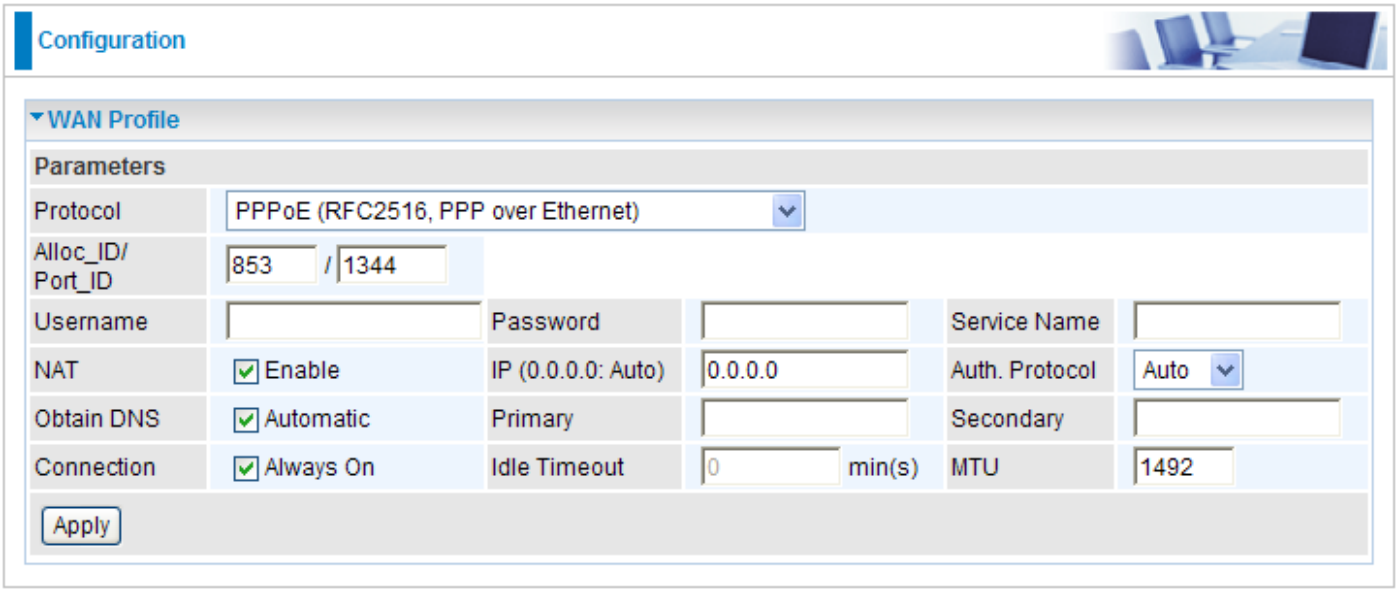
WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and the Internet.

WAN Profile

PPPoE Connection

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



Protocol: Select the protocol you will use in the device.

Alloc_ID/Port_ID: Enter the information provided by your ISP.

Username: Enter the username provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive). This is the format of username "username@ispname" instead of "username".

Password: Enter the password provided by your ISP. You can input up to 128 alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information. Maximum input is 15 alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

Auth. Protocol: Default is Auto. Your ISP should advise you on whether to use Chap or Pap.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Connection:

Always on: If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

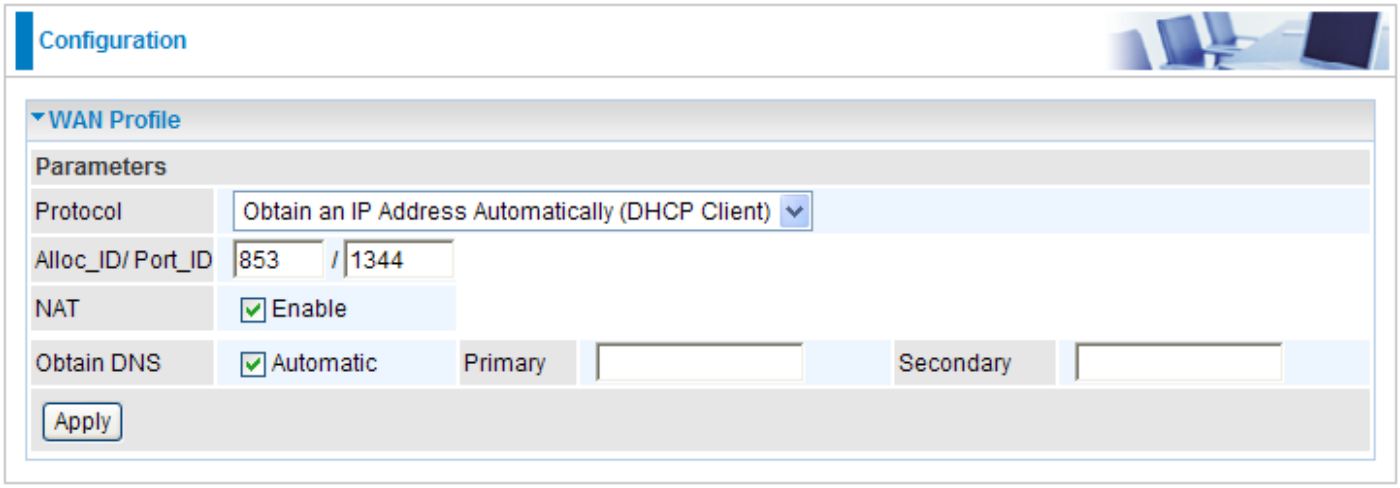
Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

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

Click Apply to confirm the settings.

Obtain an IP Address Automatically (DHCP Client)

By configuring DHCP settings, the device is able to obtain IP settings automatically from the ISP.



Protocol: Select the protocol you will use in the device.

Alloc_ID/Port_ID: Enter the information provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

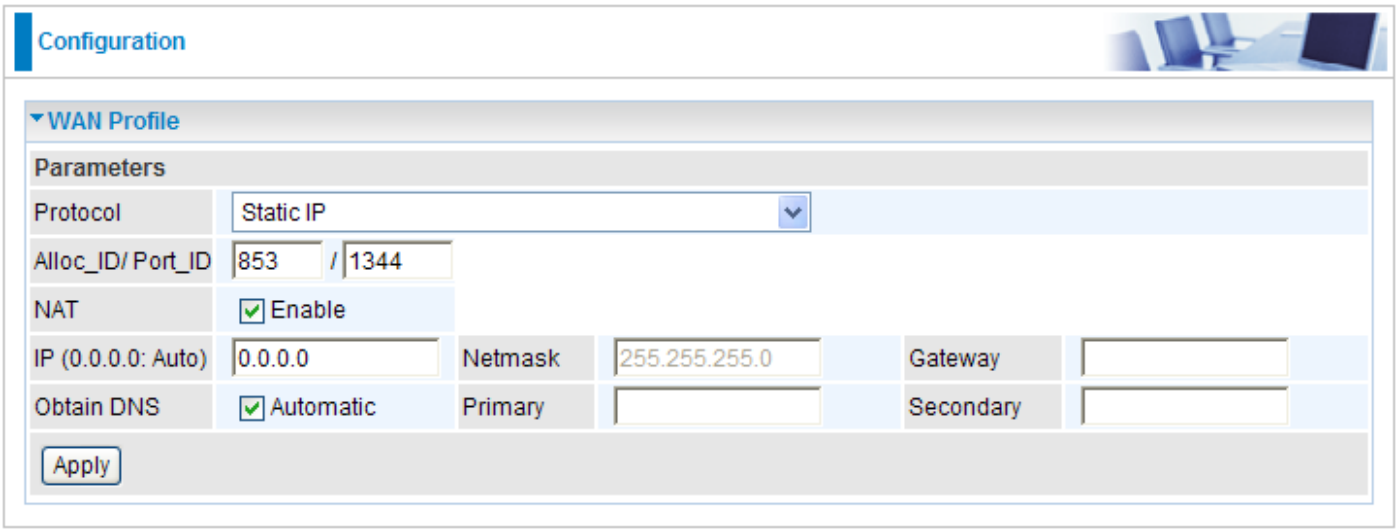
Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Click Apply to confirm the settings.

Static IP

A Static WAN connection will be configured according to the IP properties defined by your ISP.



Protocol: Select the protocol you will use in the device.

Alloc_ID/Port_ID: Enter the information provided by your ISP.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Specify an IP address allowed to logon and access the router's web server.

Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon the device and modify data.

Netmask: The default is 255.255.255.0. Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the IP address of the default gateway (if given).

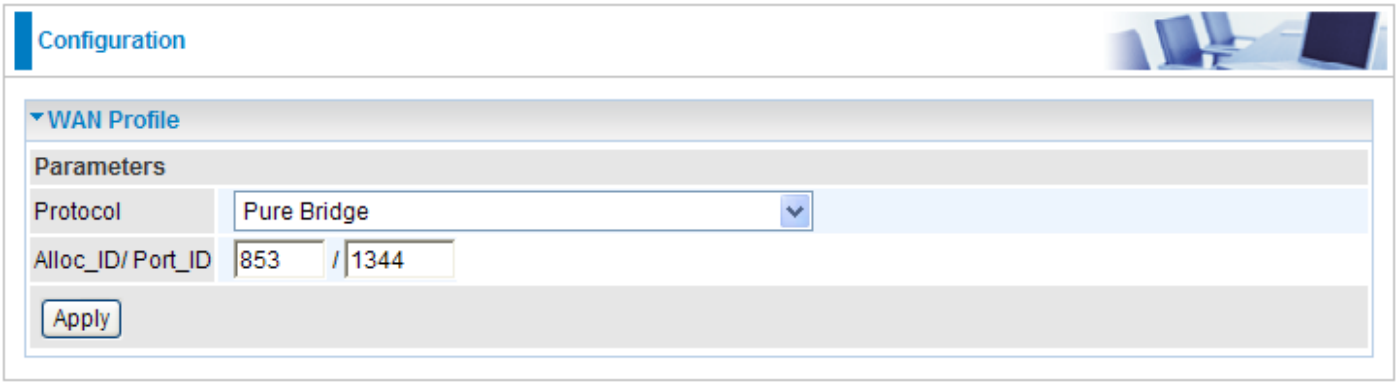
Obtain DNS: A Domain Name System (DNS) contains a mapping table for domain name and IP addresses. DNS helps to find the IP address for the specific domain name. Check the checkbox to obtain DNS automatically.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Click Apply to confirm the settings.

Pure Bridge



Protocol: Select the protocol you will use in the device.

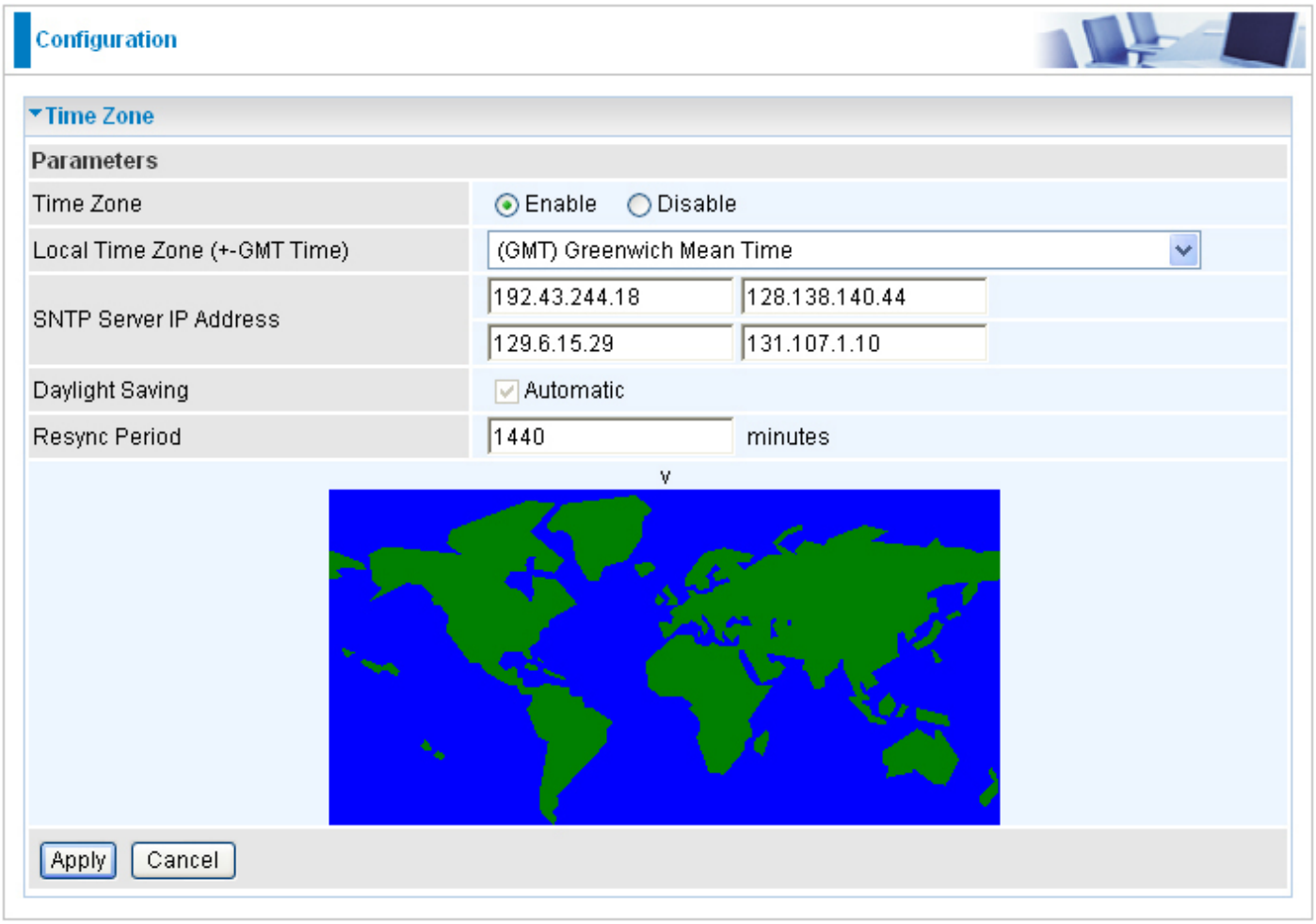
Alloc_ID/Port_ID: Enter the information provided by your ISP.

Click Apply to confirm the settings.

System

These are the items within the System section: **Time Zone**, **Firmware Upgrade**, **Backup/Restore**, **Restart**, **User Management** and **Mail Alert**.

Time Zone



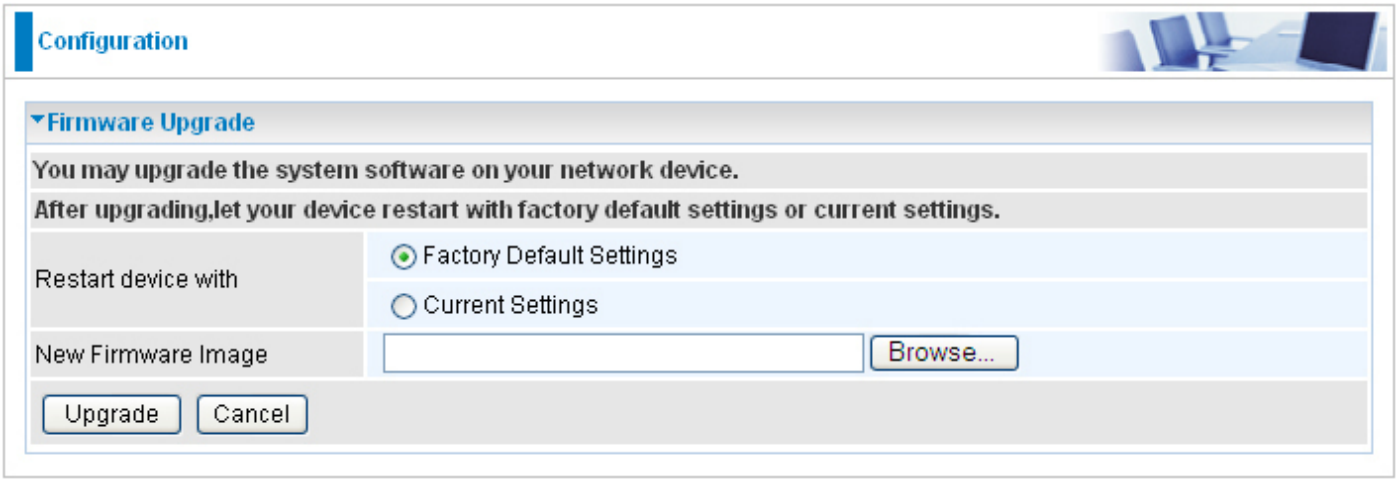
The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone from the drop down menu. To apply the selected local time zone, check Enable and click the Apply button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the drop-down list, simply enter its IP address in their appropriate blanks provided as shown above. Your ISP may also provide an SNTP server for you to use.

Daylight Saving is also known as Summer Time Period. Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check Enable box to set your local time.

Resync Period (in minutes) is the periodic interval the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days. The default value is set at 1440 minutes.

Firmware Upgrade

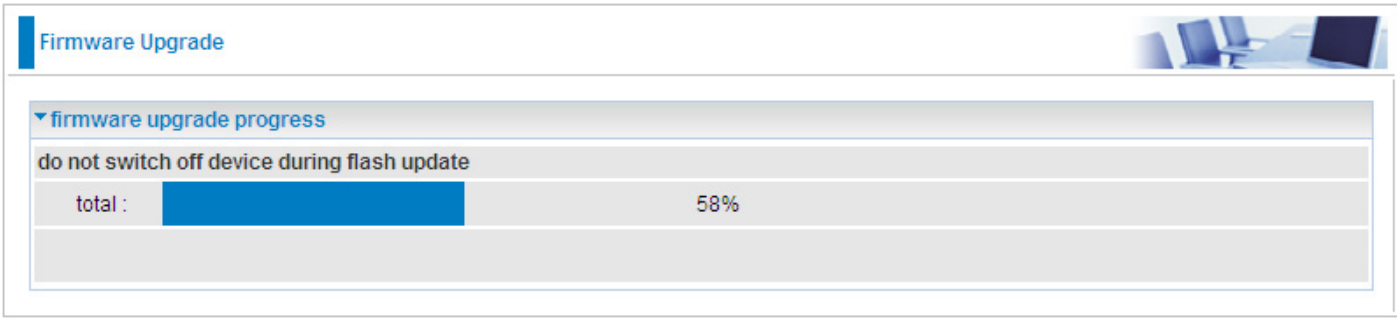
Your router's firmware is the software that enables it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software that runs in your router. Thus, by upgrading the newly improved version of the firmware allows you the advantage to use newly integrated features.

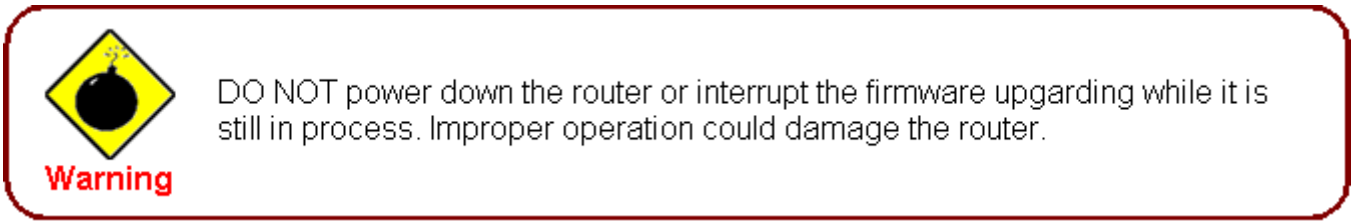


Factory Default Settings: If select this setting, the device will reboot to restore the parameters of all its applications to its default values.

Current Settings: If select this setting, the device will reboot and retain the customized settings of all applications.

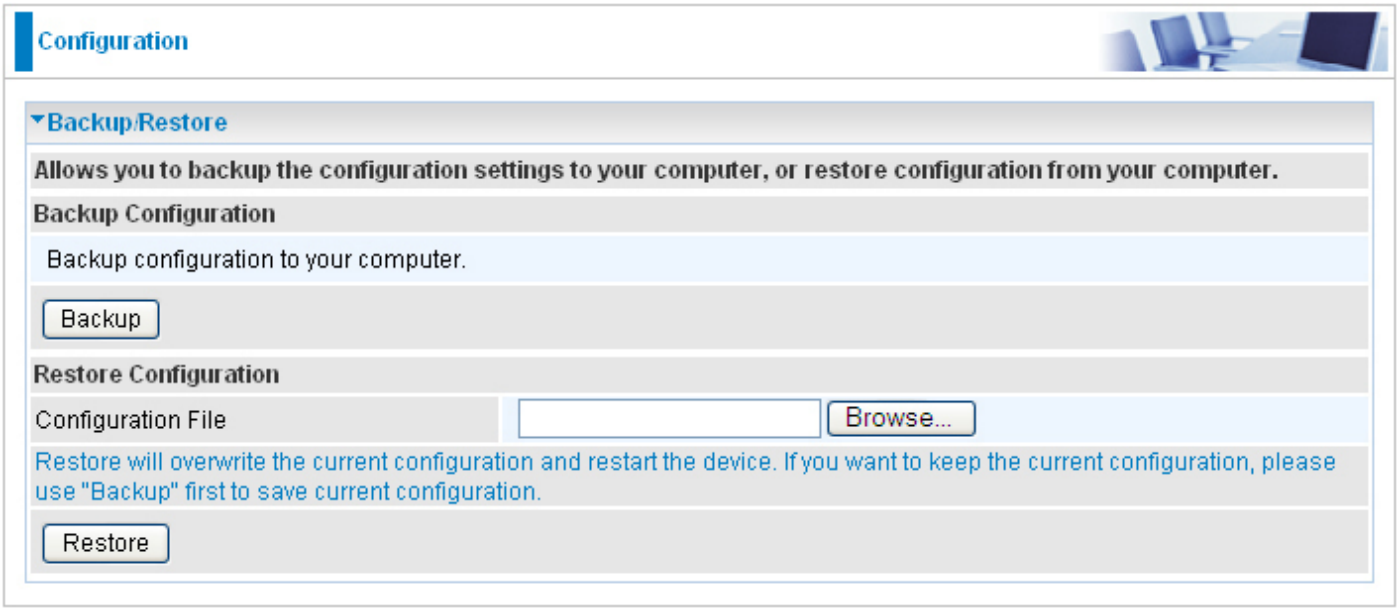
Click on Browse button to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware to your router.





Backup / Restore

These functions allow you to save a backup of the current configuration of your router to a defined location on your PC, or to restore a previously saved configuration. This is useful if you wish to experiment with different settings, knowing that you have a backup in hand in case any mistakes occur. It is advisable that you backup your router configuration before making any changes to your router configuration.



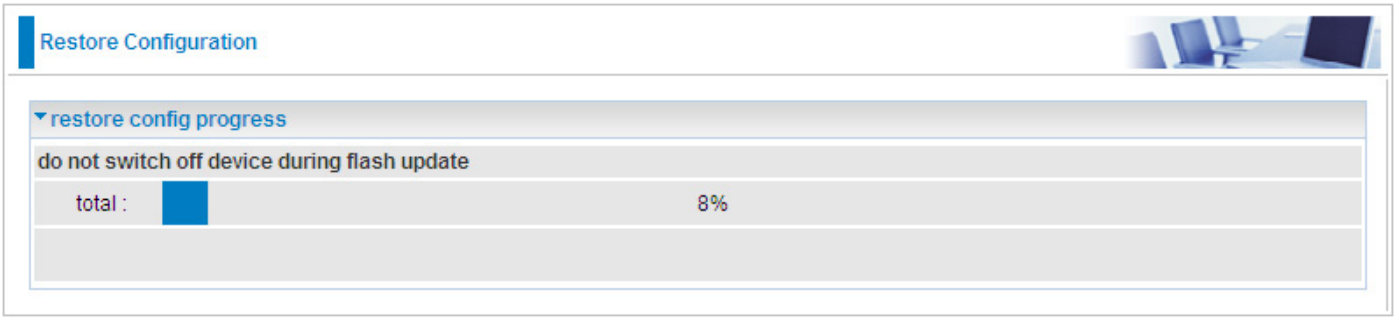
Backup Configuration

Press Backup to select where on your local PC you want to store your setting file. You may also change the name of the file if you wish to keep multiple backups.

Restore Configuration

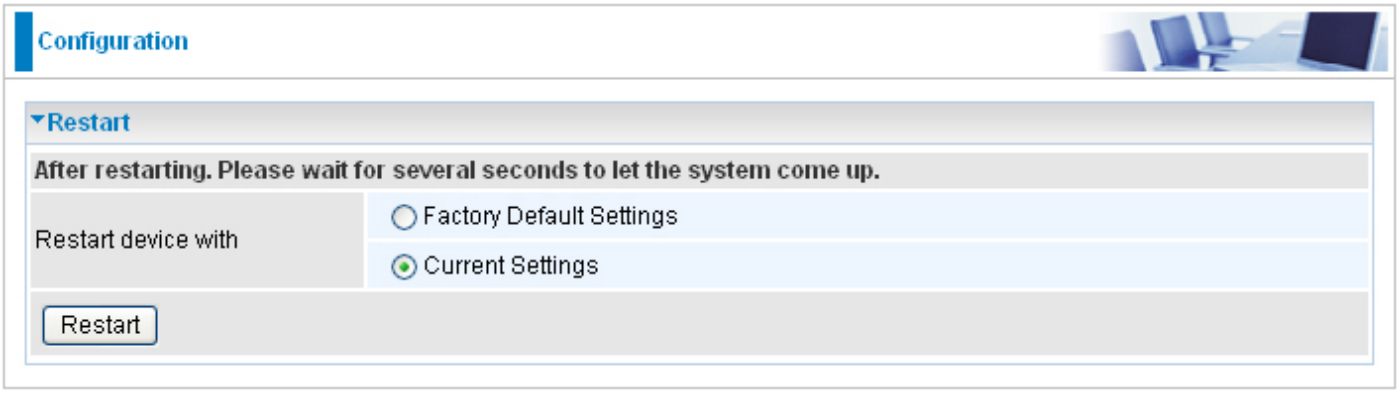
Press Browse to select a file from your PC to restore. You should only restore your router setting that has been generated by the Backup function which is created with the current version of the router firmware. Settings files saved to your PC should not be manually edited in any way.

Select the settings files you wish to use, and press Update Settings to load the setting into the router. Click Restore to begin restoring the configuration and wait for the router to restart before performing any actions.



Restart

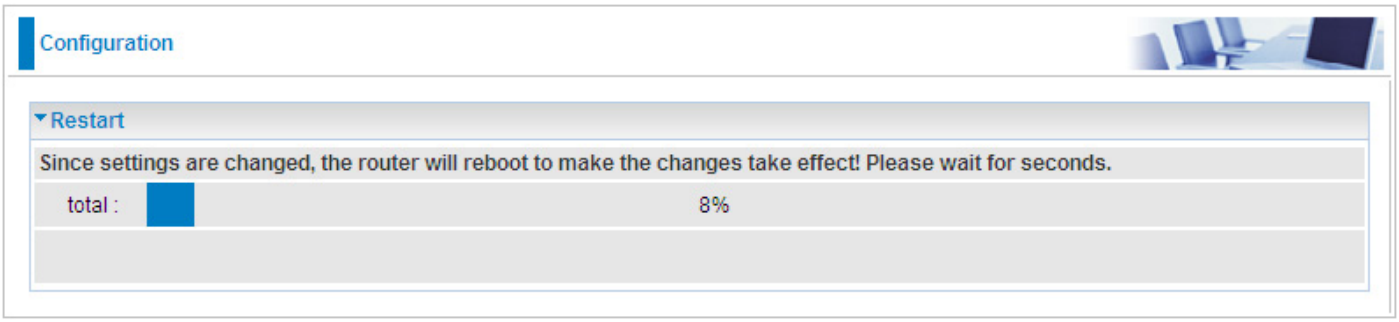
There are two options for you to choose from before restarting the your 9300(V)NX device. You can either choose to restart your device to restore it to the Factory Default Settings or to restart the device with your current settings applied. Restarting your device to Factory Default Setting will be useful especially after you have accidentally changed your settings that may result in undesirable outcome.



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings.

Click Restart with option Current Settings to reboot your router (and restore your last saved configuration).

After selecting the type of setting you want the device to restart with, click the Restart button to initiate the process. After restarting, please wait several minutes to let the selected setting applied to the system.

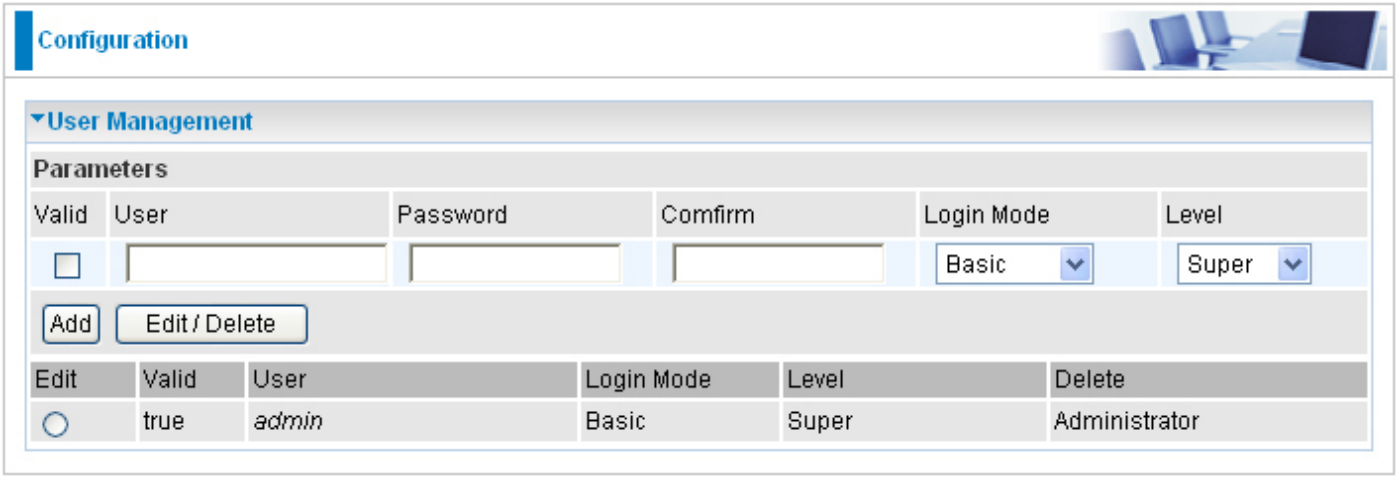


You may also reset your router to factory settings by holding the small Reset pinhole button more than 6 seconds on the back of your router.

User Management

In order to prevent unauthorized access to your router configuration interface, it requires all users to login with a username and password. Therefore only system administrator can access the system.

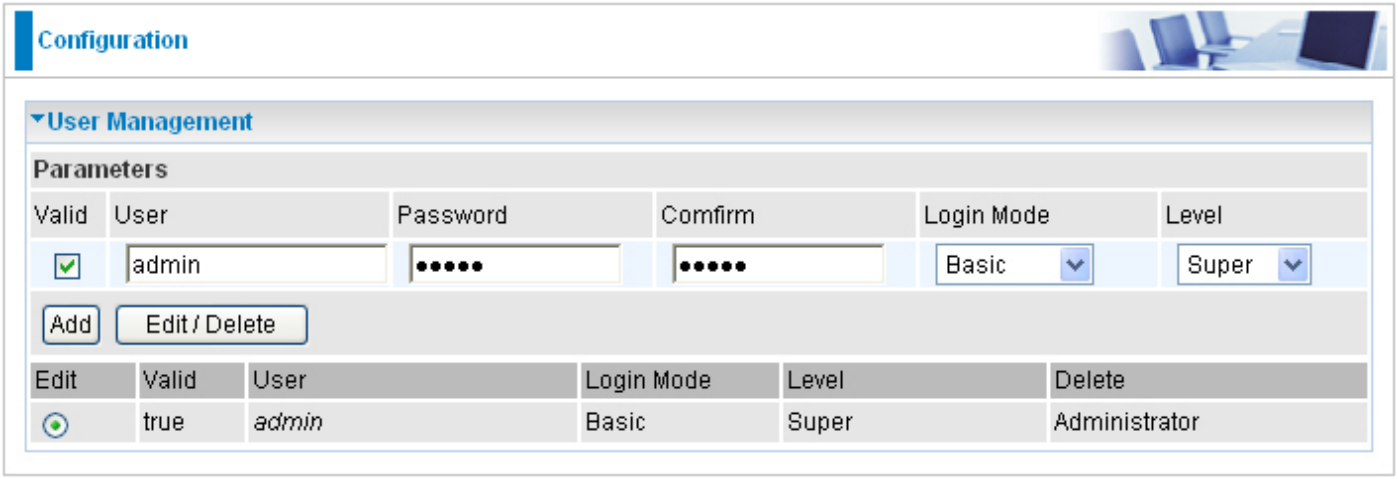
This feature allows you to set up multiple user accounts which contains a unique password of its own. In addition, you can also edit any existing user accounts or add new users to allow access to the device configuration interface.



Edit Account Information

You can change the informations of any account whether the account is active or valid.

1. To edit an account, click on the Edit radio button of the account you want to edit. Once selected, all information of that account will be displayed.
2. Delete the information to be edited and replace it with the new one.
3. When it is done, simply click on the Edit/ Delete button to save your changes.



Note: It is highly recommended that you change the password immediately to prevent security breach to your GUI.

Add an Account

1. Check the Valid checkbox, fill in all the information: User name, Comment (optional), Password, Confirm Password.
2. When it is done, click the Add button.

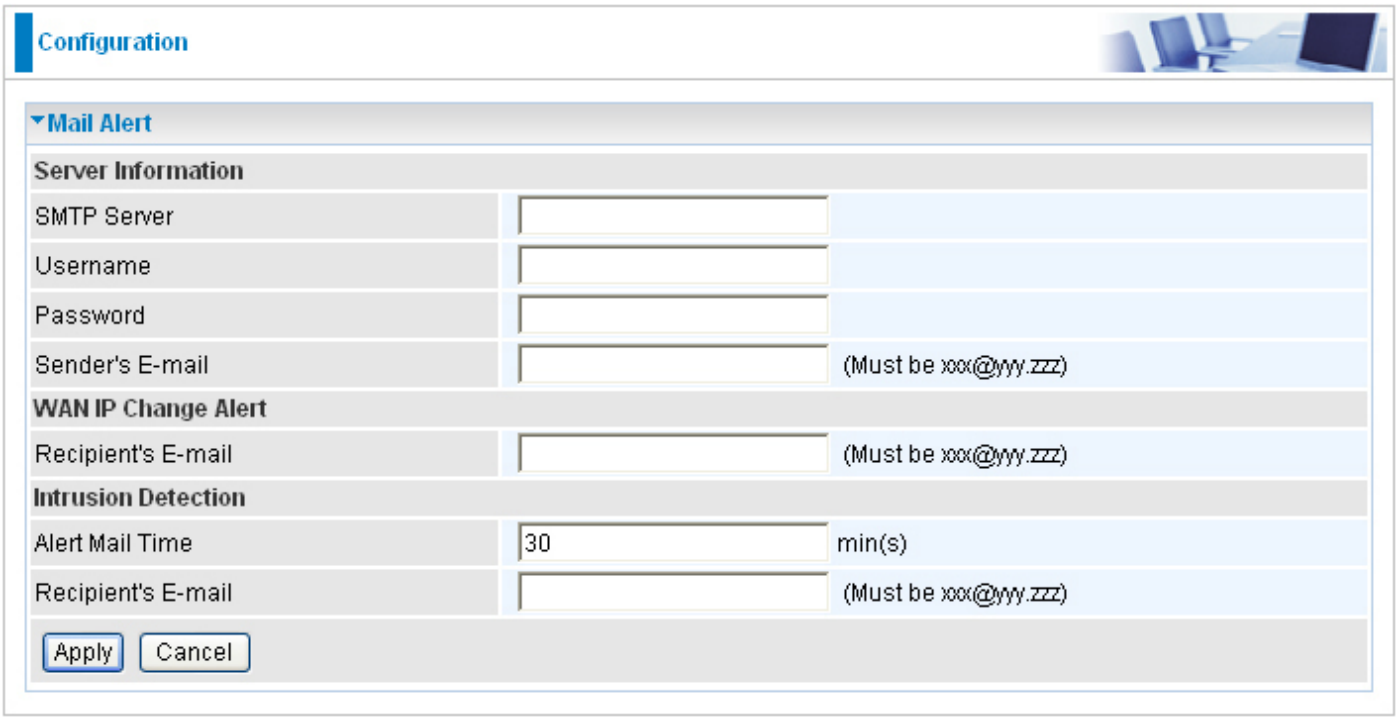
Delete a user account

1. Check the Delete checkbox of the account you want to delete.
2. Then click the Edit/Delete to confirm the deletion.

Note: You can delete any user account except for the default admin account. Thus there is no delete radio button available for this account.

Mail Alert

Mail Alert allows administrator to receive notifications from the router through email about important events that is occurring in real time. This allows administrator to be able to take immediate actions to counteract any possible hacking or to restore the router to its original status should any failover / failback ever occurs.



Server Information

SMTP Server: Enter the SMTP (mail) server address.

Username: Enter the username of your SMTP server.

Password: Enter the password associated with the username.

Sender's E-mail: Enter the email address you wish to send the mail alert email to.

WAN IP Change Alert

Recipient's E-mail: Enter the email address you wish to send the WAN IP Change email to.

Intrusion Detection

Alert Mail Time: Set the time for sending the Alert mail.

Recipient's E-mail: Enter the email address you wish to send the Intrusion Detection email to.

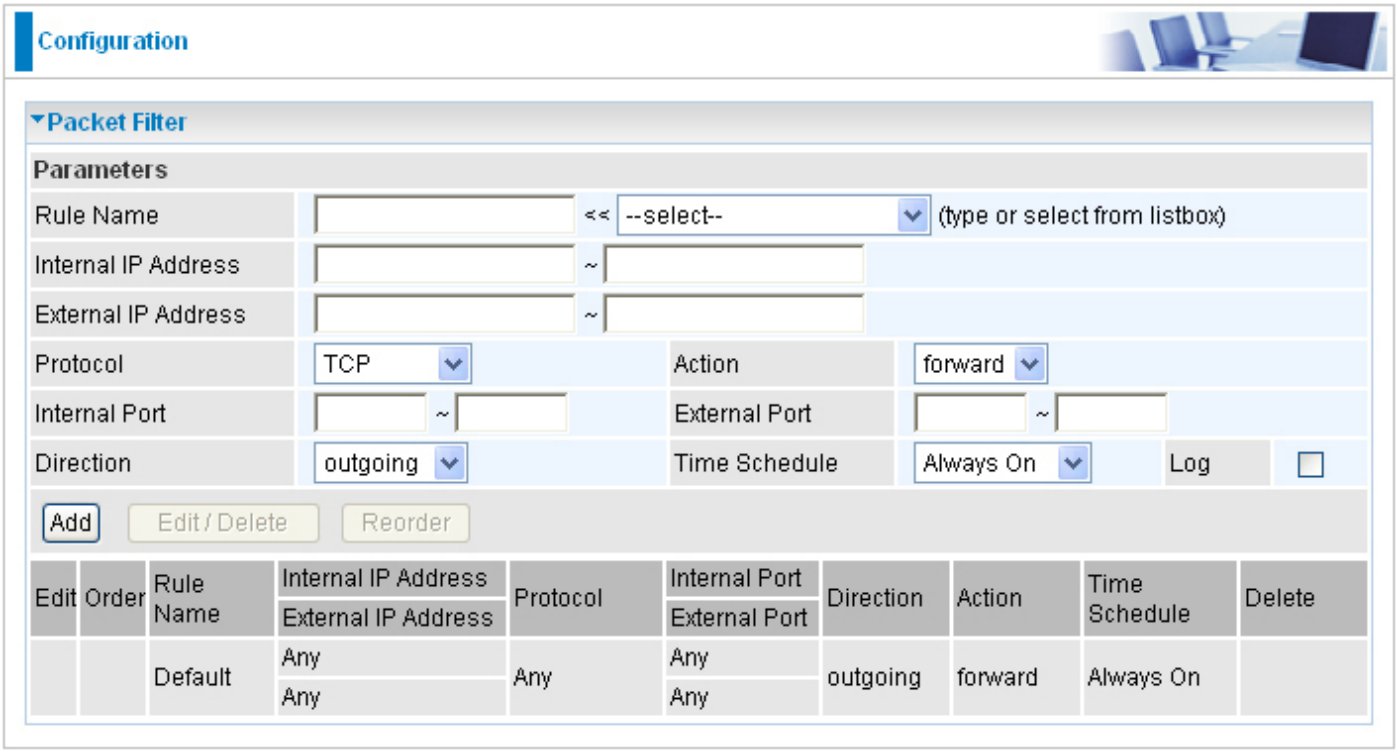
Click Apply to confirm the settings.

Firewall

Listed are the items under the Firewall section: **Packet Filter**, **MAC Filter**, **Intrusion Detection**, **Block WAN PING** and **URL Filter**.

Packet Filter

Packet filtering enables you to configure your router to block specific internal / external users (IP address) from Internet access, or disable specific service requests (Port number) to / from the Internet. This configuration program allows you to set up different filter rules for different users based on their IP addresses or their network Port number. The relationship among all filters is "or" operation, which means that the router checks these different filter rules one by one, starting from the first rule. As long as one of the rules is satisfied, the specified action will be taken.



Rule Name: User defined description for entry identification. The maximum name length is 20 characters, or choose an application that you want from the listbox.

Internal IP Address / External IP Address: This is the Address-Filter used to allow or block traffic to/rom particular IP address(es). Input the range you want to filter out. If you leave these four fields empty or enter 0.0.0.0, it means any IP address.

Protocol: Specify the packet type (TCP, UDP, ICMP, etc.) that the rule applies to. Select TCP if you wish to search for the connection-based application service on the remote server using the port number. Or select UDP if you want to search for the connectionless application service on the remote server using the port number.

Action: If a packet matches this filter rule, forward (allows the packets to pass) or drop (disallow the packets to pass) this packet.

Internal Port: This Port or Port Range defines the ports allowed to be used by the Remote/WAN to connect to the application. Default is set from range 0 ~ 65535. It is recommended that this option be configured by an advanced user.

External Port: This is the Port or Port Range that defines the application.

Direction: Determine whether the rule is for outgoing packets or for incoming packets.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Check the checking box if you wish to generate logs when the filer rule is applied to a packet.

Add: Click this button to add a new packet filter rule and the added rule will appear at the bottom table.

Edit: Tick Edit next to the item you wish to edit, and then change parameters as desired. Complete it by press “Edit/Delete”.

Delete: Tick Delete next to the item you wish to delete, and press “Edit/Delete” to remove this rule.

Order: Be aware that packet filtering parameters appear in priority order i.e. the first one takes precedence over all other rules. There is a sort function next to the Rule Name column, you can move the rule to higher or lower priority by clicking the Order arrow, and press “Reorder” to save the new priority.

Edit	Order	Rule Name	Internal IP Address / External IP Address	Protocol	Internal Port / External Port	Direction	Action	Time Schedule	Delete
○	↓	FTP	Any / Any	TCP	Any / 21~21	outgoing	forward	Always On	☐
○	↑	HTTP	Any / Any	TCP	Any / 80~80	outgoing	forward	Always On	☐
		Default	Any / Any	Any	Any / Any	outgoing	forward	Always On	

MAC Filter

A MAC (Media Access Control) address is the unique network hardware identifier for each PC on your network's interface (i.e. its Network Interface Card or Ethernet card). Using your router's MAC Address Filter function, you can configure the network to block specific machines from accessing your LAN.

There are no pre-defined MAC address filter rules, you can add the filter rules to meet your requirements.

The format of MAC address could be: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.

Filter Action

Action: Select an action for MAC Filter. Default is Block. You can check Disable this feature or Allow to activate the filter. Click Apply to confirm the change.

Server Information

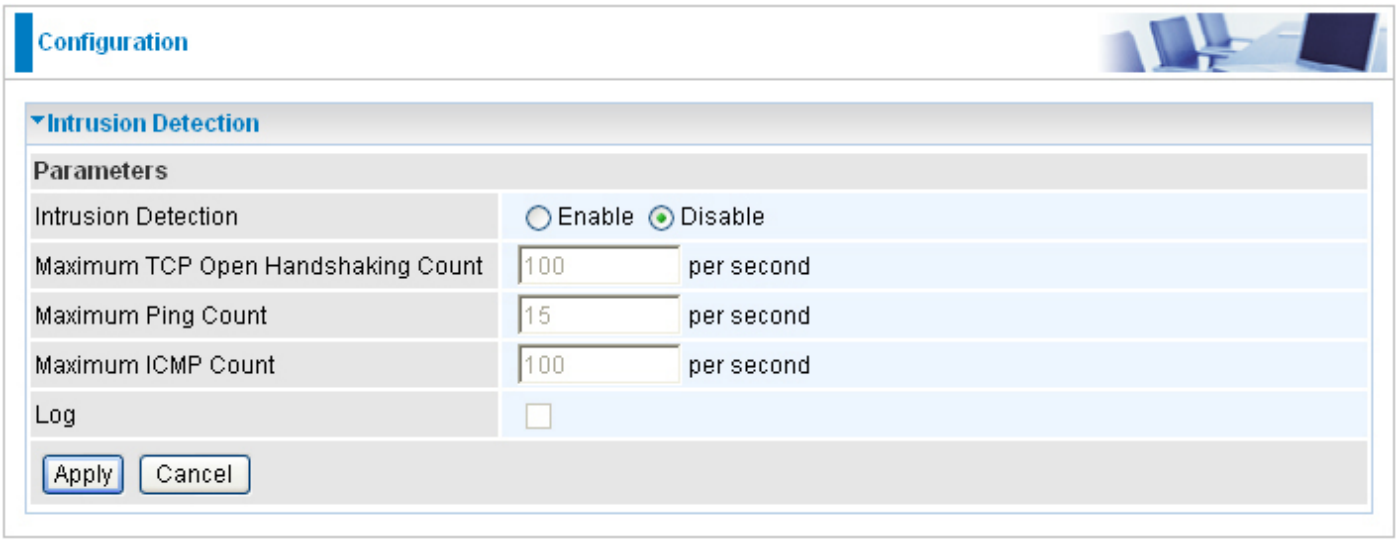
MAC Address: Enter the MAC addresses you wish to have the filter rule applies.

Time Schedule: It is a self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Click Add to apply the settings.

Intrusion Detection

The router Intrusion Detection System (IDS) is used to detect hacker's attack and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.



Intrusion Detection: Check Enable if you wish to detect intruders accessing your computer without permission.

Maximum TCP Open Handshaking Count: This is a threshold value to decide whether a SYN Flood attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Maximum Ping Count: This is a threshold value to decide whether an ICMP Echo Storm is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Maximum ICMP Count: This is a threshold to decide whether an ICMP flood is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

Log: Check Log if you wish to generate logs when the filer rule is applied to the Intrusion Detection.

Click Apply to confirm the settings.

Table: Hacker attack types recognized by the IDS

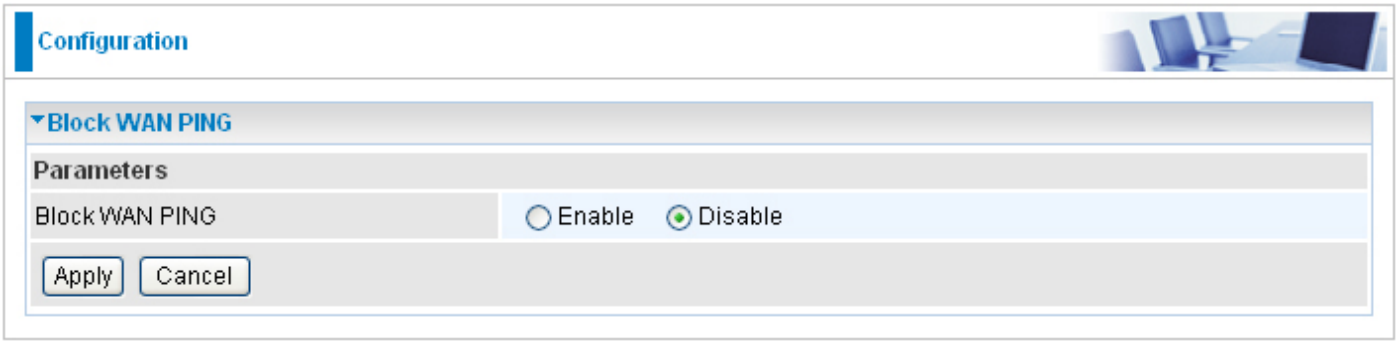
Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP
Src Port: Source Port
Dst Port: Destination Port
Dst IP: Destination IP

Block WAN PING

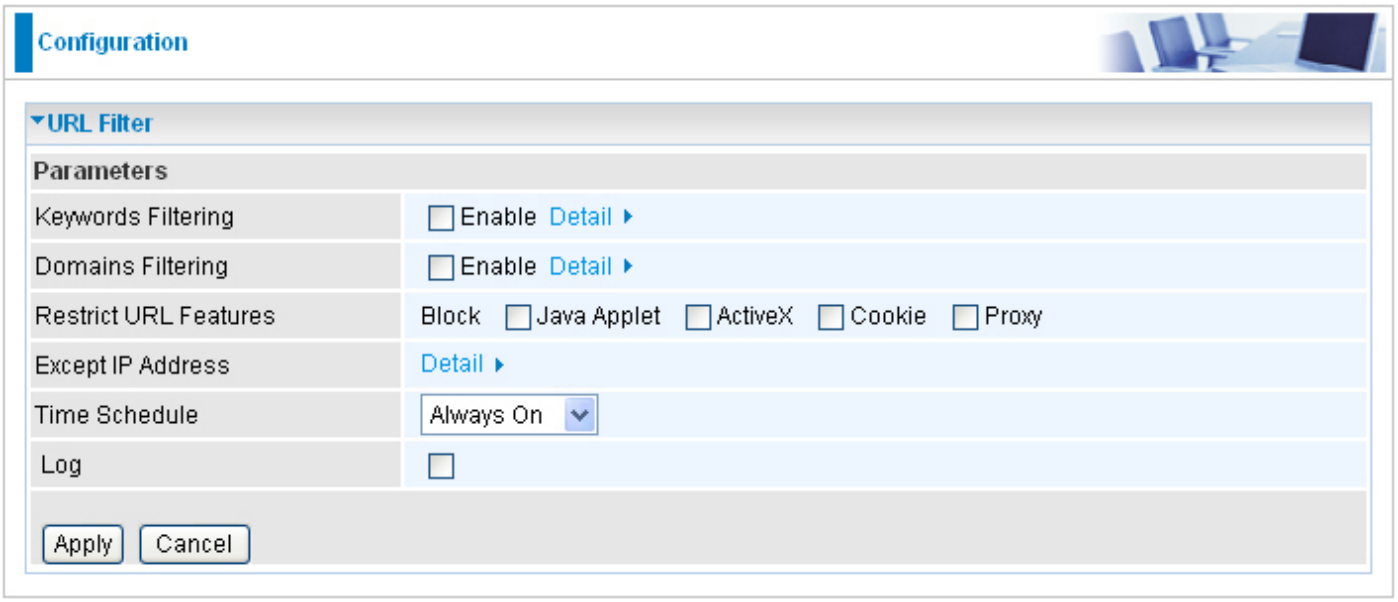
This feature is to be enabled when you want the public WAN IP address on your router not to respond to any ping command.

This feature is disabled by default. To activate the Block WAN PING feature, check the Enable box then click the Apply button.

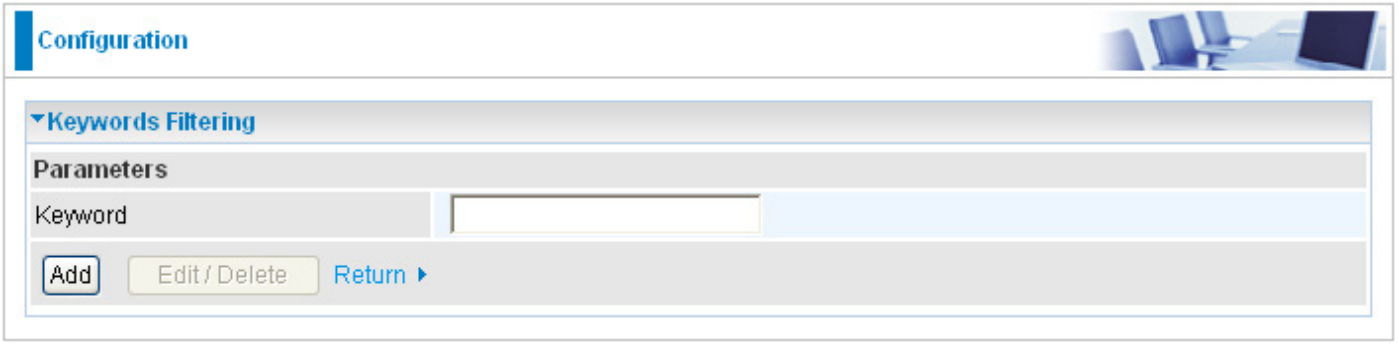


URL Filter

URL (Uniform Resource Locator) (e.g. an address in the form of http://www.abcde.com or http://www.example.com) filter rule allows you to prevent users on your network from accessing specific websites defined by their URL. There are no predefined URL filter rules, therefore you can add filter rules to meet your requirements.



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

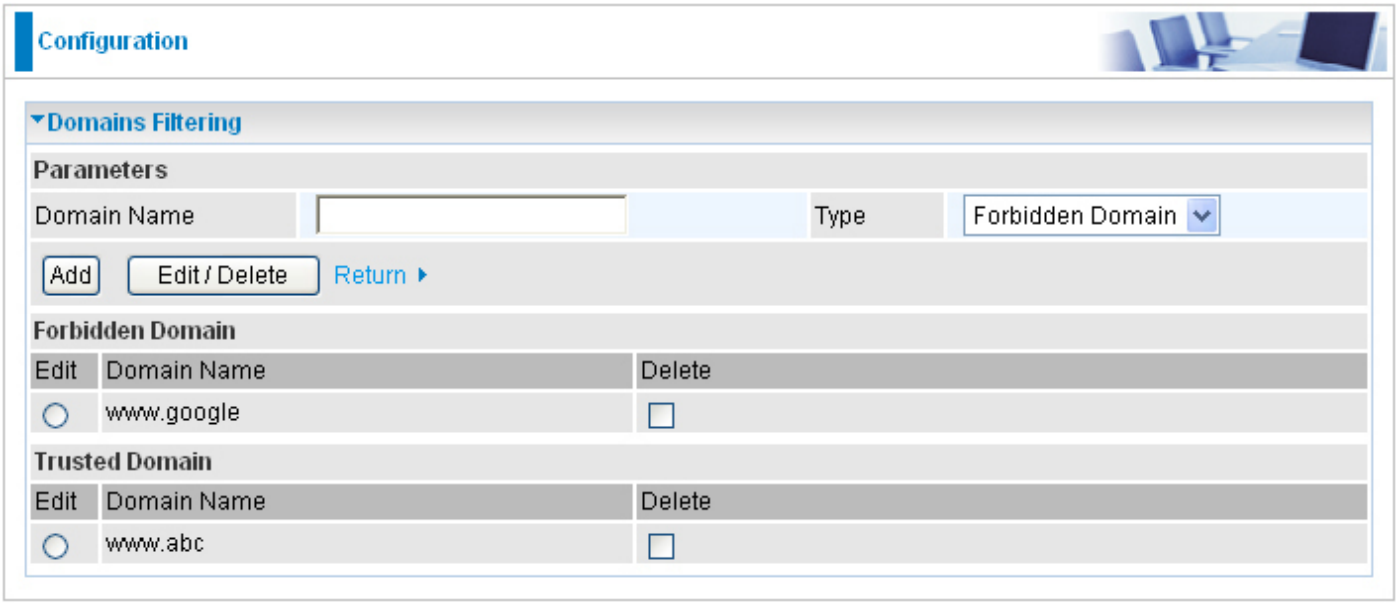


For example, if the URL is **http://www.abc.com/abcde.html**, it will be dropped as the keyword "abcde" occurs in the URL.

Domains Filtering: This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. Check the domain in the URL to determine if it is in the trusted list. If yes, the connection attempt is sent to the remote web server.
2. If not, check if it is listed in the forbidden list. If yes, then the connection attempt will be dropped.
3. If the packet does not match either of the above two items, it is sent to the remote web server.

4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to **www.google.com.au**, enter “**www.google**” or “**www.google.com**”.



Restrict URL Features: This function enhances the restriction to your URL rules.

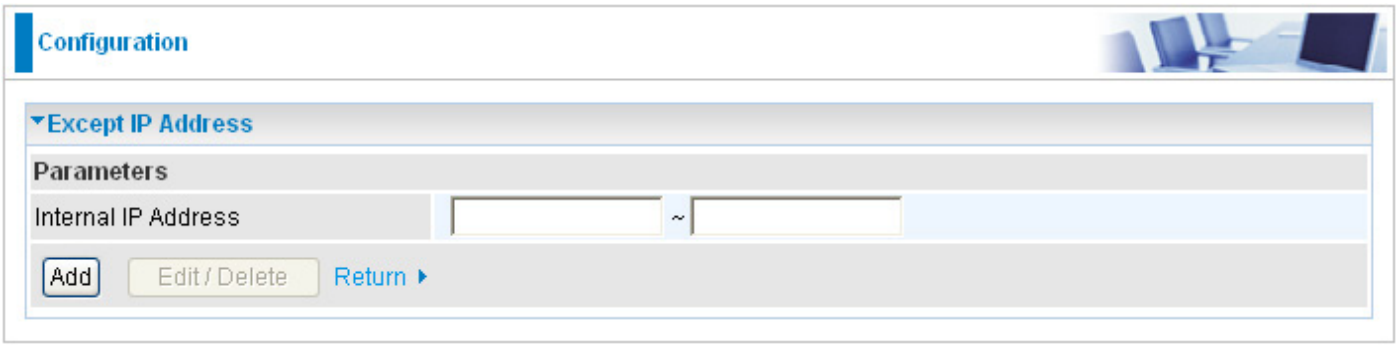
Block Java Applet: Blocks Web content which includes the Java Applet to prevent someone who wants to damage your system via the standard HTTP protocol.

Block ActiveX: Blocks ActiveX.

Block Cookies: Blocks Cookies.

Block Proxy: Blocks Proxy.

Except IP Address: The except IP address list.



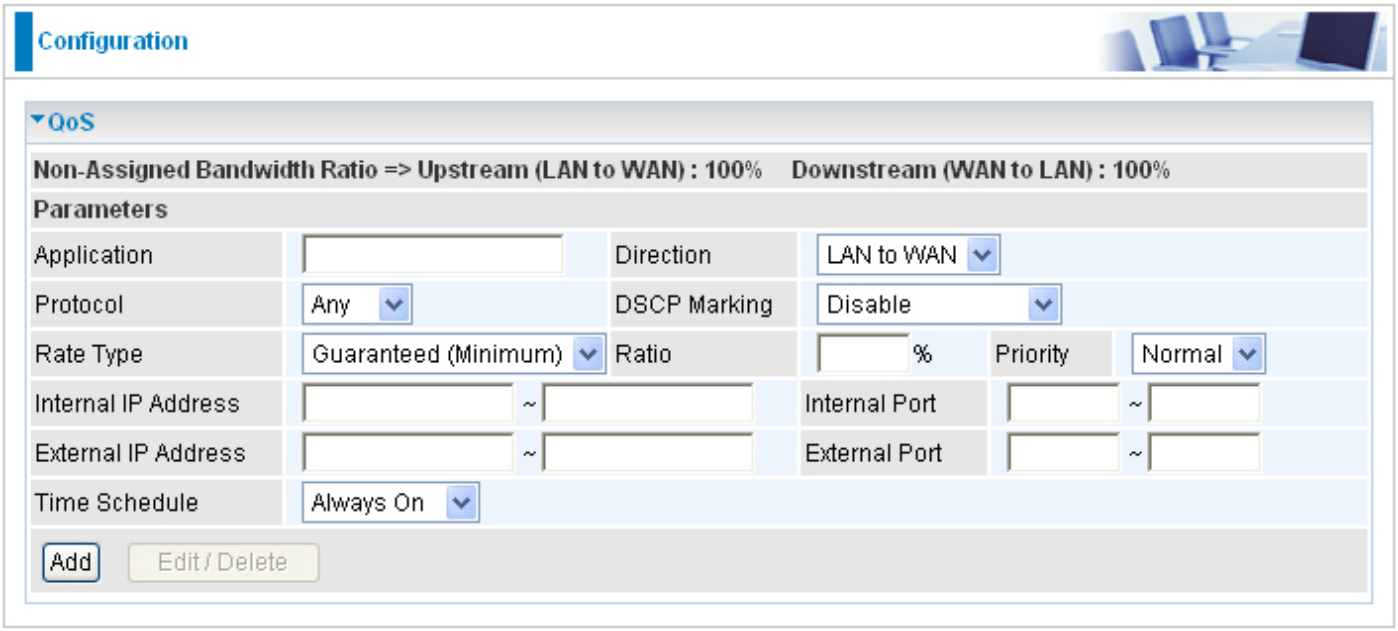
Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to Time Schedule section.

Log: Check this checking box if you wish to generate logs when the filer rule is applied to the URL Filter.

Click Apply to confirm the settings.

QoS - Quality of Service

QoS helps you to control the data upload traffic of each application from LAN (Ethernet and/ or Wireless) to WAN (Internet). It facilitates you the features to control the quality and speed of throughput for each application when the system is running with full upstream load.



After clicking the QoS item, you can Add/Edit/Delete a QoS policy. This page will show the brief information for policies you have added or edited. This page will also display the total available (Non-assigned) bandwidth, in percentage, can be assigned.

Application: Assign a name that identifies the new QoS application rule.

Direction: The traffic flow direction to be controlled by the QoS policy. There are two settings to be provided in the Router:

> **LAN to WAN:** Control the traffic flow from the local network to the outside world. For example, when you have a FTP server inside the local network and want to have a limited traffic rate controlled by the QoS policy, you need to add a policy with LAN to WAN direction setting.
>
> **WAN to LAN:** Control Traffic flow from the WAN to LAN. (The connection maybe either issued from LAN to WAN or WAN to LAN.)

Protocol: Select the supported protocol from the drop down list. For GRE protocol, there is no need to specify the IP addresses or Application ports in this page. For other protocols, at least one value shall be given.

> **Any:** No protocol type is specified.
>
> **TCP**
>
> **UDP**
>
> **ICMP**
>
> **GRE:** For PPTP VPN Connections.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value. See **DSCP Mapping Table**.

Note: Make sure that the router(s) in the network backbone are capable to execute and check the DSCP throughout the QoS network.

DSCP Mapping Table

DSCP Mapping Table	
(Wireless) GPON Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Rate Type: Two types are provided:

Limited (Maximum): Specify a limited data rate for this policy. It is the maximal rate for this policy. As above FTP server example shows, if you want to “throttle” the outgoing FTP speed to 20% of 100M and limit to it, please choose this type.

Guaranteed (Minimum): Specify a minimal data rate for this policy. For example, if you want to provide a guaranteed data rate for your outside customers to access your internal FTP server with, say at least, 20% of your total bandwidthm, please choose this type. Then, if the available bandwidth is not used, it will be given to this policy by following priority assignment.

Ratio: Assign the data ratio for this policy to be controlled. For examples, when we want to allow only 20% of the total data transfer rate for the LAN-to-WAN direction to be used for FTP server, we can specify here with data ratio = 20. If you have GPON LINE with 100M/bps.rate, the estimated data rate, in kbps, for this rule is 20%*100*0.9 = 20Mbps. (For 0.9 is an estimated factor for the effective data transfer rate for a GPON LINE from LAN to WAN. For WAN-to-LAN, it is 0.85 to 0.8).

Priority: The priority given to each policy/application. You may adjust this setting to fit your policy / application. For examples, you are allowed to specify two different QoS policies for different applications. Both applications need minimal or higher bandwidth, besides the assigned one, if there is any available/non-used one available, you can specify which application can have higher priority by acquiring the non-used bandwidth.

High

Normal: The default is set to normal.

Low

For the sample priority assignment for different policies, it is served in a First-In-First-Out way.

Internal IP Address: The IP address values for Local LAN machines you want to control. (For IP packets from LAN to WAN, it is the source IP address. For IP packages from WAN to LAN, it is the destination IP address.)

Internal Port: The Application port values for local LAN machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the source port value. For TCP/UDP packets from WAN to LAN, it is the destination port value.)

External IP Address: The IP address values for Remote WAN machines you want to control. (For IP packets from LAN to WAN, it is the destination IP address. For IP packages from WAN to LAN, it is the source IP address.)

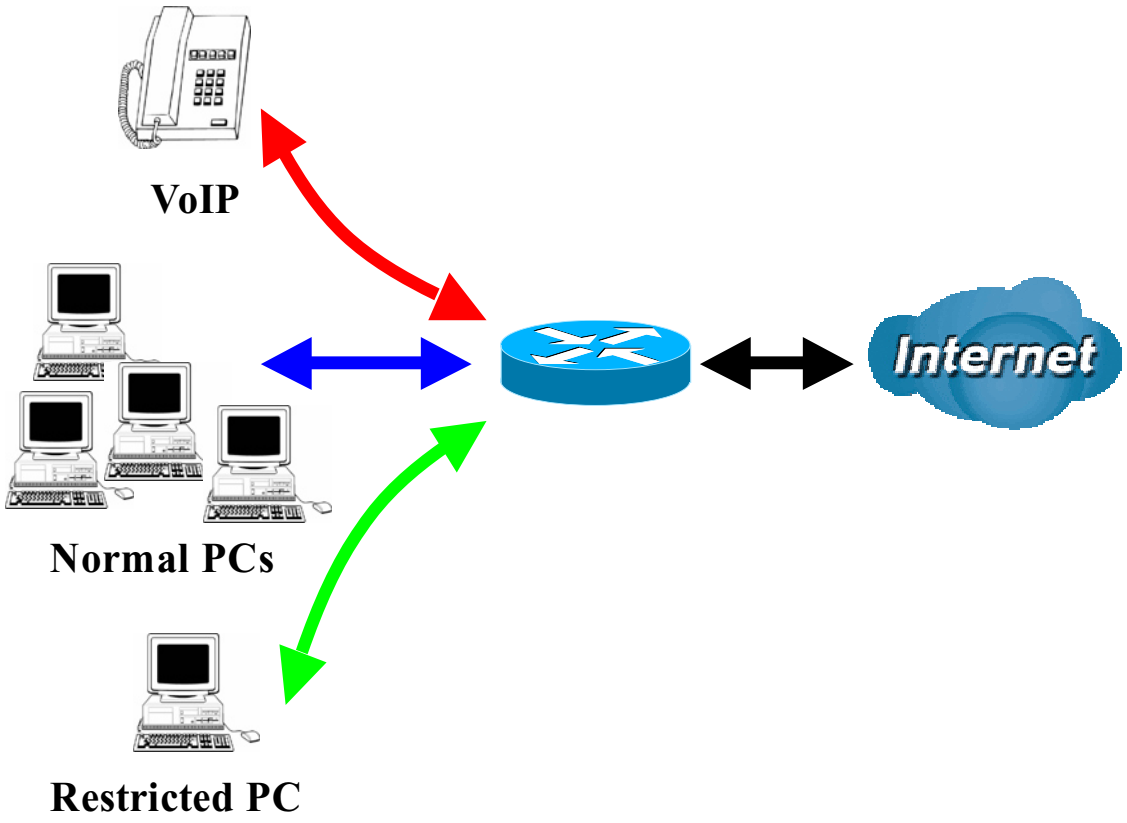
External Ports: The Application port values for remote machines you want to control. (For TCP/UDP packets from LAN to WAN, it is the destination port value. For TCP/UDP packets from WAN to LAN, it is the source port value.)

Time Schedule: Scheduling your prioritization policy.

Remember clicking Add to save your settings.

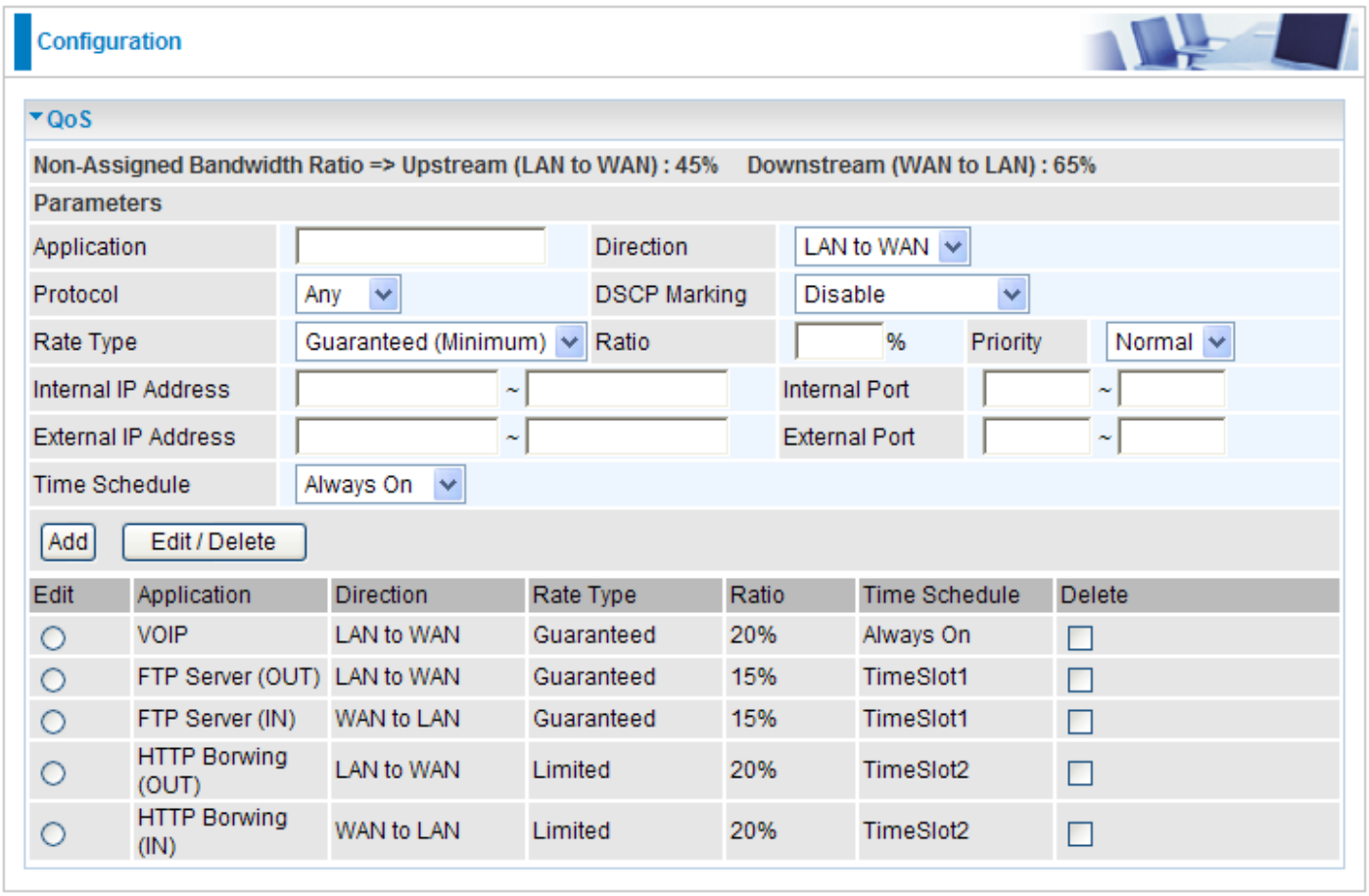
Example: QoS for your Network

Connection Diagram



Application	IP / Ports	Control Flow	Data Rate	Time Schedule
VoIP user	192.168.0.1	Outgoing	Minimal 20% with high priority for non-used bandwidth with DSCP marking Class 1 Gold Service.	Always
FTP Server	192.168.0.100	Incoming & Outgoing	Outgoing :minimal 30% data rate. Incoming :minimal 30% data rate. Both with low priority for non-used bandwidth.	Only during working hours 9:00 to 17:00 Monday to Friday
HTTP Web user	80	Incoming & Outgoing	Outgoing : limited 20% data rate. Incoming : limited 30% data rate.	Always

Example: QoS Setup



VoIP application

Voice is latency-sensitive application. Most VoIP devices are used SIP protocol and the port number will be assigned by SIP module automatically. Better to use fixed IP address for catching VoIP packets as high priority.

Virtual Server

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

In TCP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You also need to use port forwarding if you wish to host an online game server.

Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table below). The registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

Examples of well-known and registered port numbers are shown below, for further information, please see IANA’s website at: **http://www.iana.org/assignments/port-numbers**.

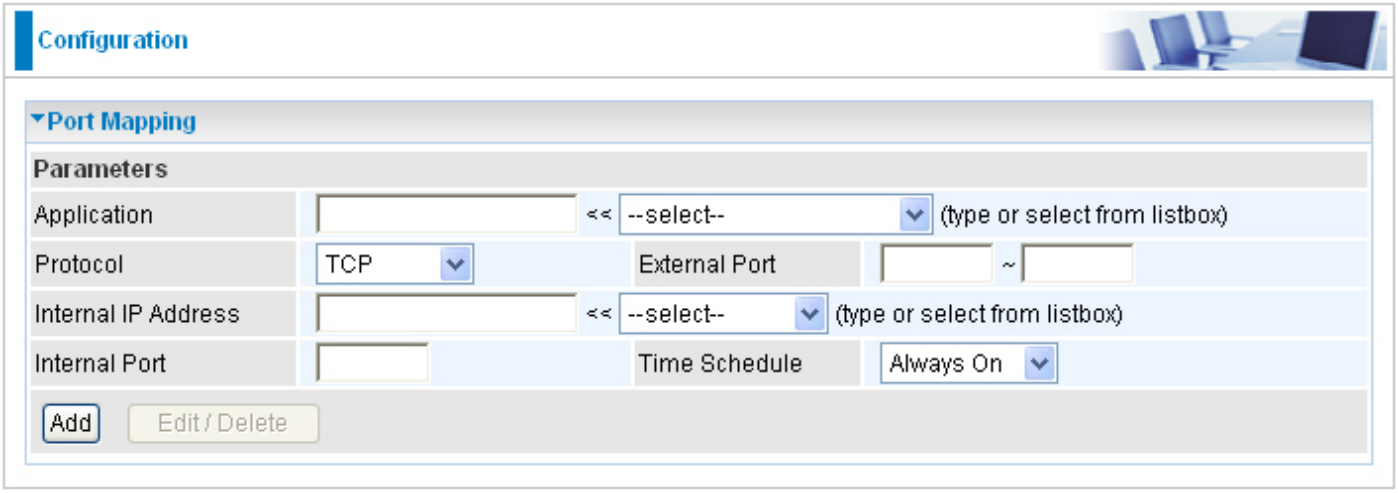
For help on determining which private port numbers are used by common applications on this list, please see the FAQs (Frequently Asked Questions) at **http://www.billion.com**.

Table: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	Real Audio

Port Mapping

Since NAT acts as a “natural” Internet firewall, your router protects your network from accessed by outside users, as all incoming connection attempts point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network. When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request the router for a specified port is received, it is forwarded to the corresponding internal server.



For example, if you set the port number 80 (Web/HTTP) to be mapped to the IP Address 192.168.1.2, then all incoming HTTP requests from outside users are forwarded to the local server (PC) with the IP address of 192.168.1.2. If the port is not listed as a predefined application, you need to add it manually.

Edit	Application	Protocol	External Port	Internal IP Address	Internal Port	Time Schedule	Delete
○	FTP	TCP	21~21	192.168.1.25	Any	Always On	☐
○	HTTP	TCP	80~80	192.168.1.2	Any	Always On	☐

In addition to specifying the port number used, you also need to specify the protocol used. The protocol is determined by a particular application. Most applications use TCP or UDP, however you may also specify other protocols using the drop-down Protocol menu. Setting the protocol to “all” causes all incoming connection attempts using all protocols on all port numbers to be forwarded to the specified IP address.

Application: Select the service you wish to configure.

Protocol: A protocol is automatically applied when an Application is selected from the listbox or you may select a protocol type which you want. The protocol used to be determined by a particular application. Most applications will use TCP or UDP.

External Port & Internal Port: Enter the public port number & range you wish to configure.

Internal IP Address: Enter the IP address of a specific internal server to which requests from the specified port is forwarded.

Time Schedule: Scheduling your prioritization policy.

Add: Click to add a new virtual server rule. Click again and the next figure appears.

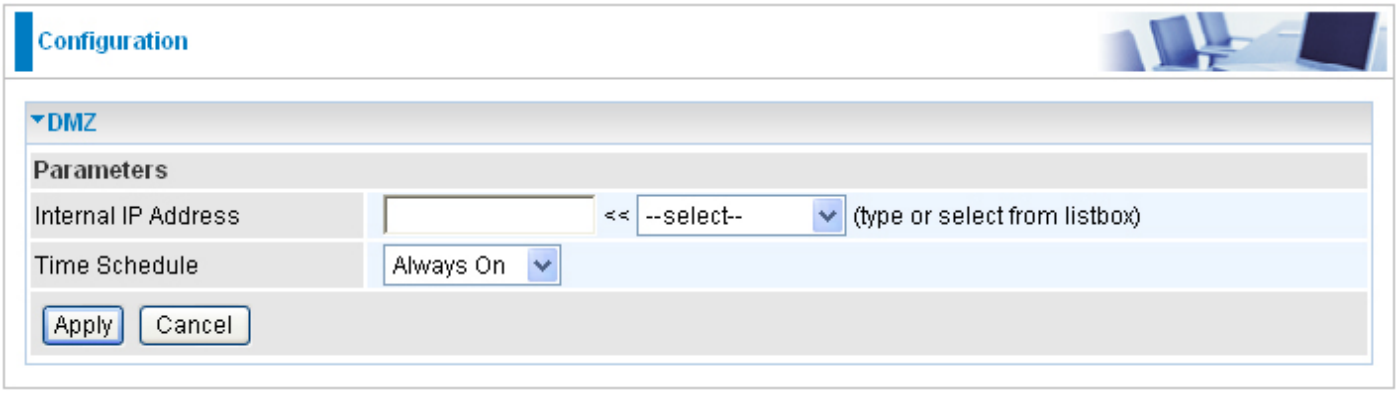
Edit: Check the Edit radio button to display the parameter of the selected application, then after changing the parameters click the Edit/Delete button to apply the changes.

Delete: To remove a port mapping application, check the Delete box of the selected application then click the Edit/Delete button.

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets that do not use a port number which is already used by any other Virtual Server entries will first be checked by the Firewall and NAT algorithms before it is passed to the DMZ host.

Cautious: This Local computer exposing to the Internet may face various security risks.



Time Schedule: Scheduling your prioritization policy.

Click Apply to confirm the settings.

Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server will hence become invalid. If the DHCP option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP addresses to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

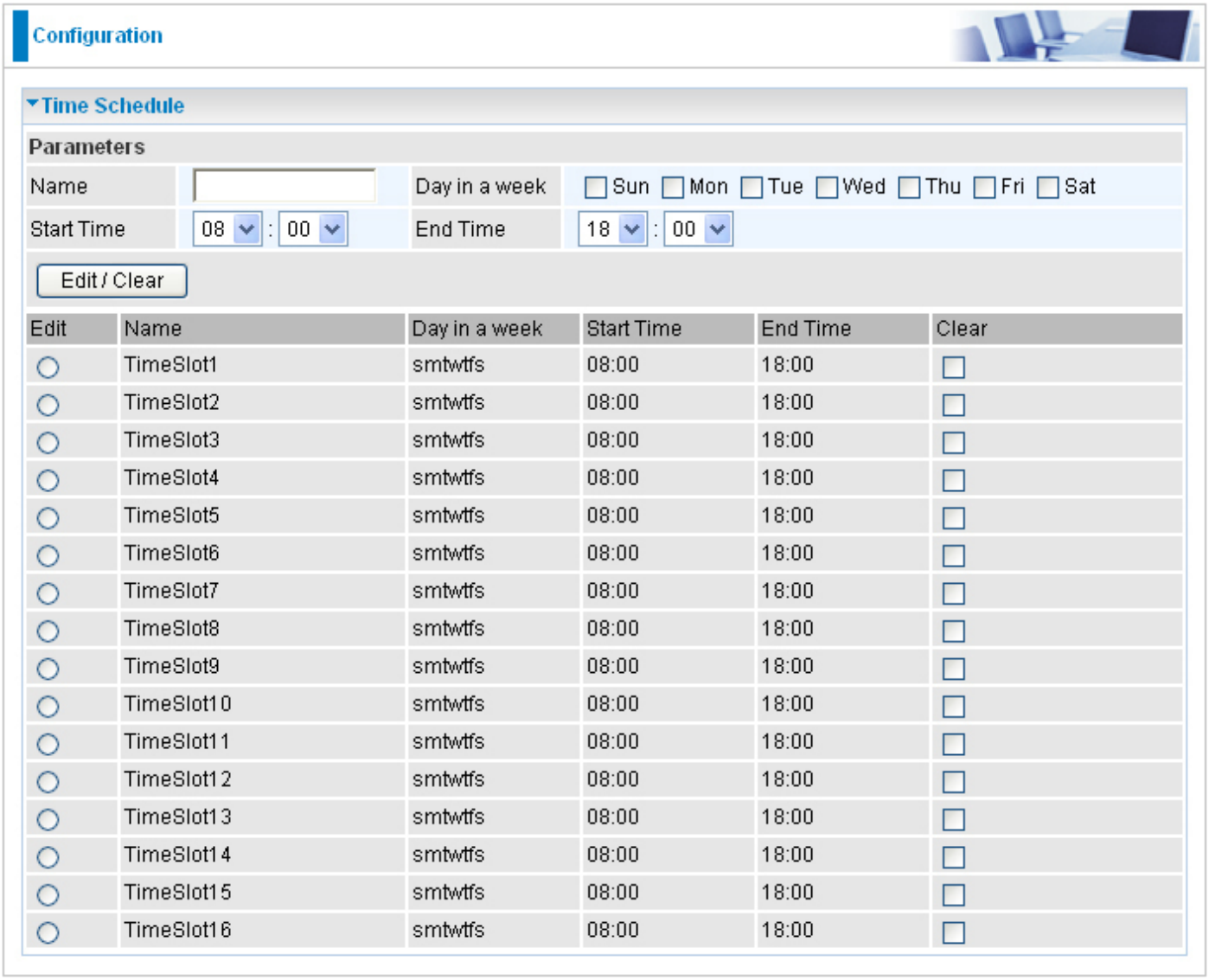
NOTE:

Since outside users are able to connect to the PCs on your network, port mapping utilization imposes security implications. You are therefore advised to use specific Virtual Server entries just for those ports that your applications require.

Time Schedule

The Time Schedule supports up to 16 time slots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to Time Zone for details. You router time should correspond with your local time. If the time is not set correctly, your Time Schedule will not function properly.



Name: A user-define description to identify this time portfolio.

Day in a week: The default is set from Sunday through Saturday. You may specify the days for the schedule to be applied.

Start Time: The default is set at 8:00 AM. You may specify the start time of the schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify the end time of the schedule.

Click the Edit/Clear button to save your changes.

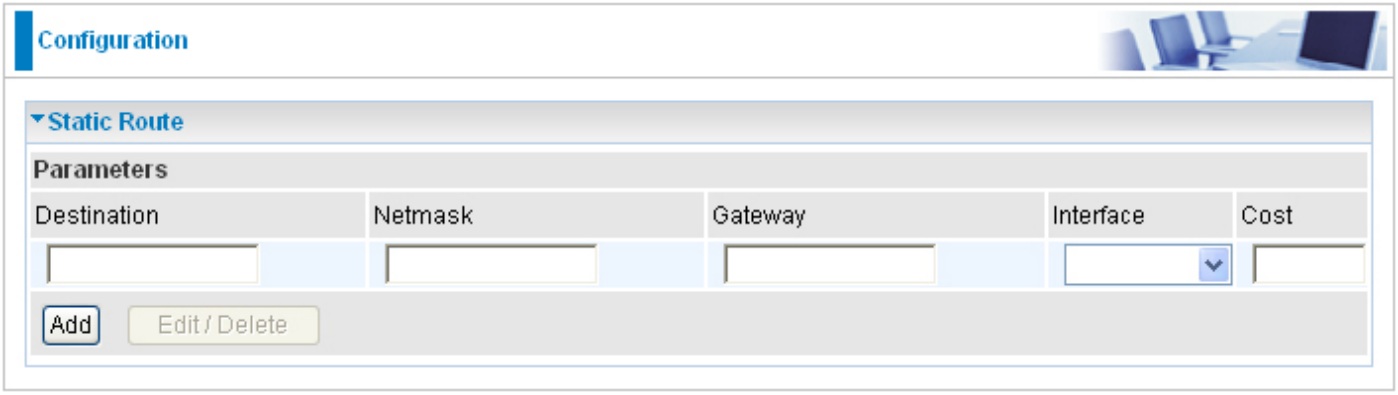
Advanced

Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the Advanced section: **Static Route**, **Static ARP**, **Dynamic DNS**, **VLAN**, **Device Management**, **IGMP** and **Remote Access**.

Static Route

With static route feature, you are equipped with the capability to control the routing of the all the traffic across your network. With each routing rule created, you can specifically assign the destination where the traffic will be routed to.



Destination: Enter the destination IP where the traffic is to be forwarded.

Netmask: Enter the netmask of the destination.

Gateway: Enter the gateway address for the traffic.

Interface: Select an appropriate interface for the new routing rule from the drop down menu.

Cost: This is the same meaning as Hop and represents the cost of transmission for routing purposes. The number needs not be precise, but it must between 0 and 65535; usually be left at 1.

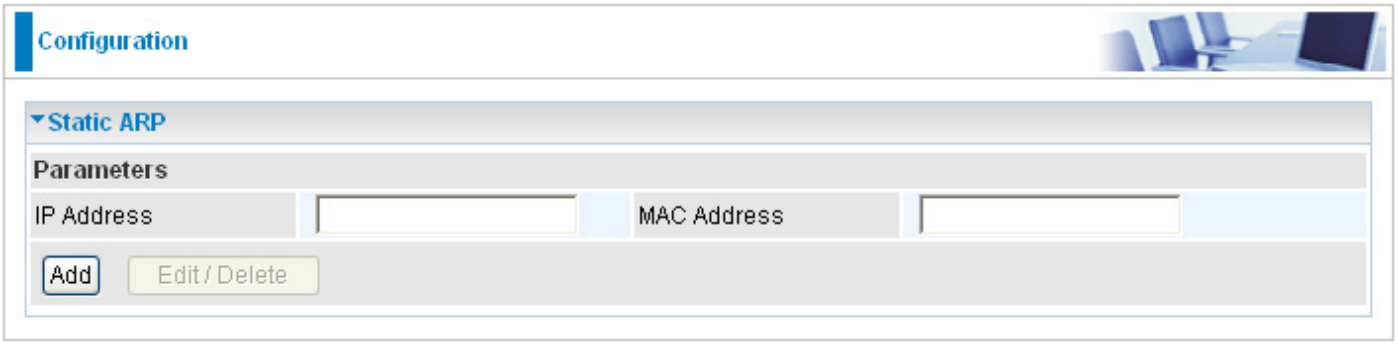
Click Add to confirm the settings.

Edit: Check the Edit radio button to display the parameter of the selected rule, then after changing the parameters click the “Edit/Delete” button to apply the changes.

Delete: To remove a static route entry, check the Delete box of the selected entry then click the “Edit/Delete” button.

Static ARP

This feature allows you to map the layer-2 MAC (Media Access Control) address that corresponds to the layer-3 IP address of the device.



IP Address: Enter the IP of the device that the corresponding MAC address will be mapped to.

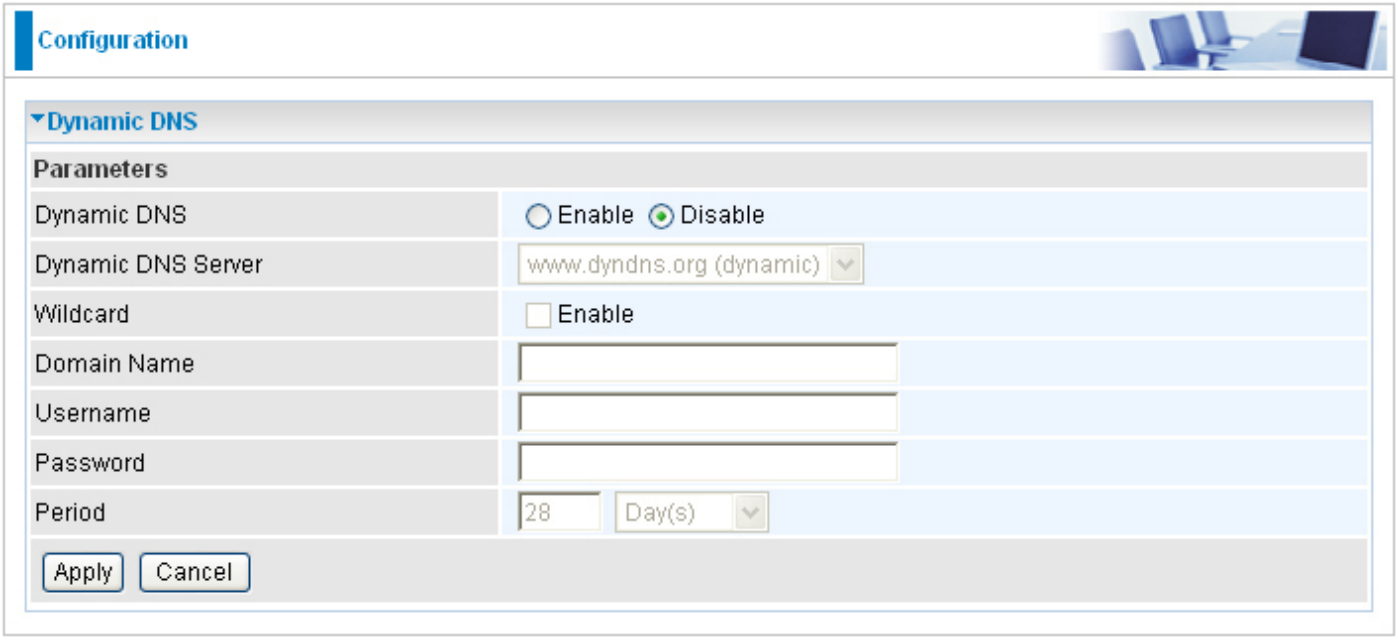
MAC Address: Enter the MAC address that corresponds to the IP address of the device.

Click Add to confirm the settings.

Dynamic DNS

The Dynamic DNS function lets you alias a dynamic IP address to a static hostname, so if your ISP does not assign you a static IP address you can still use a domain name. This is especially useful when hosting servers via your GPON connection, so that anyone wishing to connect to you may use your domain name, rather than the dynamic IP address which is assigned to you by ISP.

You need to first register and establish an account with the Dynamic DNS provider using their website, for example **http://www.dyndns.org/**.

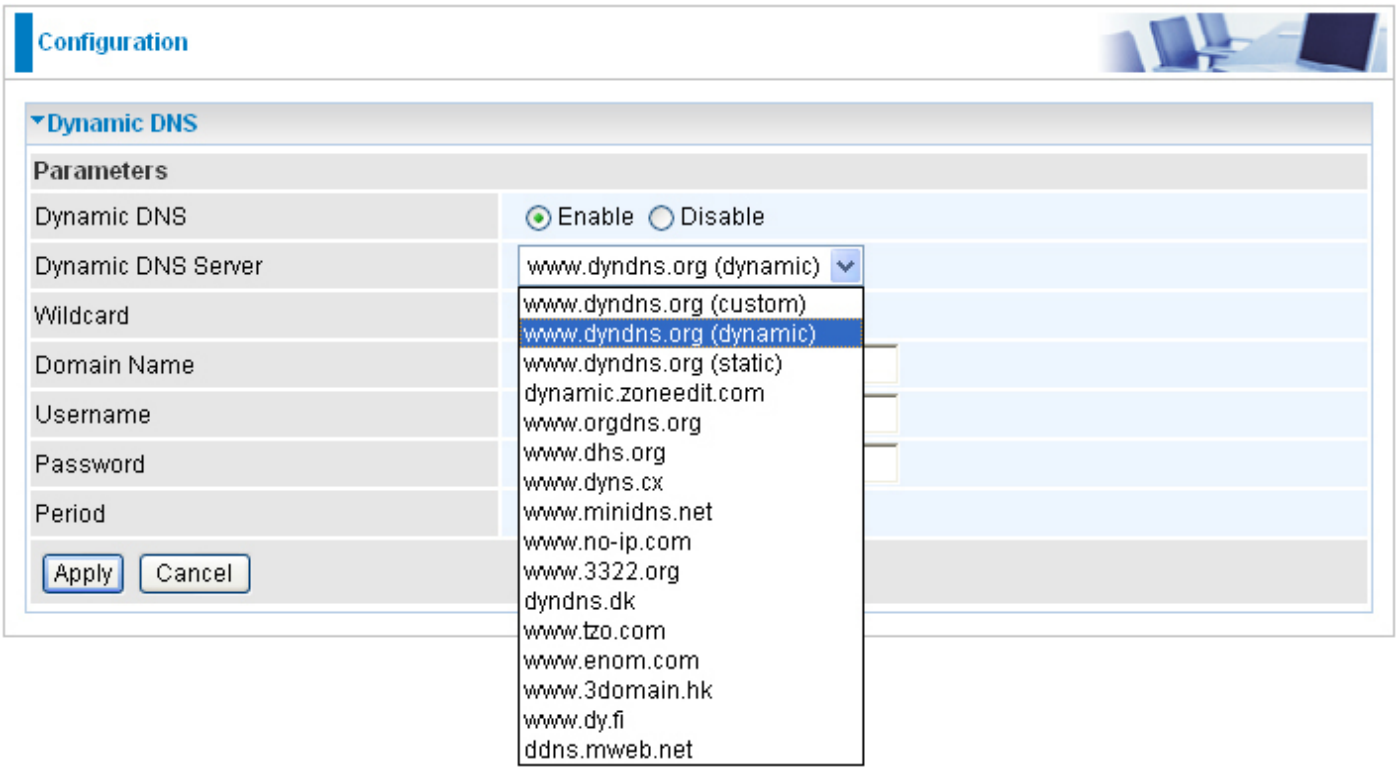


Dynamic DNS:

Disable: Check to disable the Dynamic DNS function.

Enable: Check to enable the Dynamic DNS function. The following fields will be activated and required.

Dynamic DNS Server: Select the DDNS service you have established an account with.



Wildcard: When enabled, you allow the system to lookup on domain names that do not exist to have MX records synthesized for them.

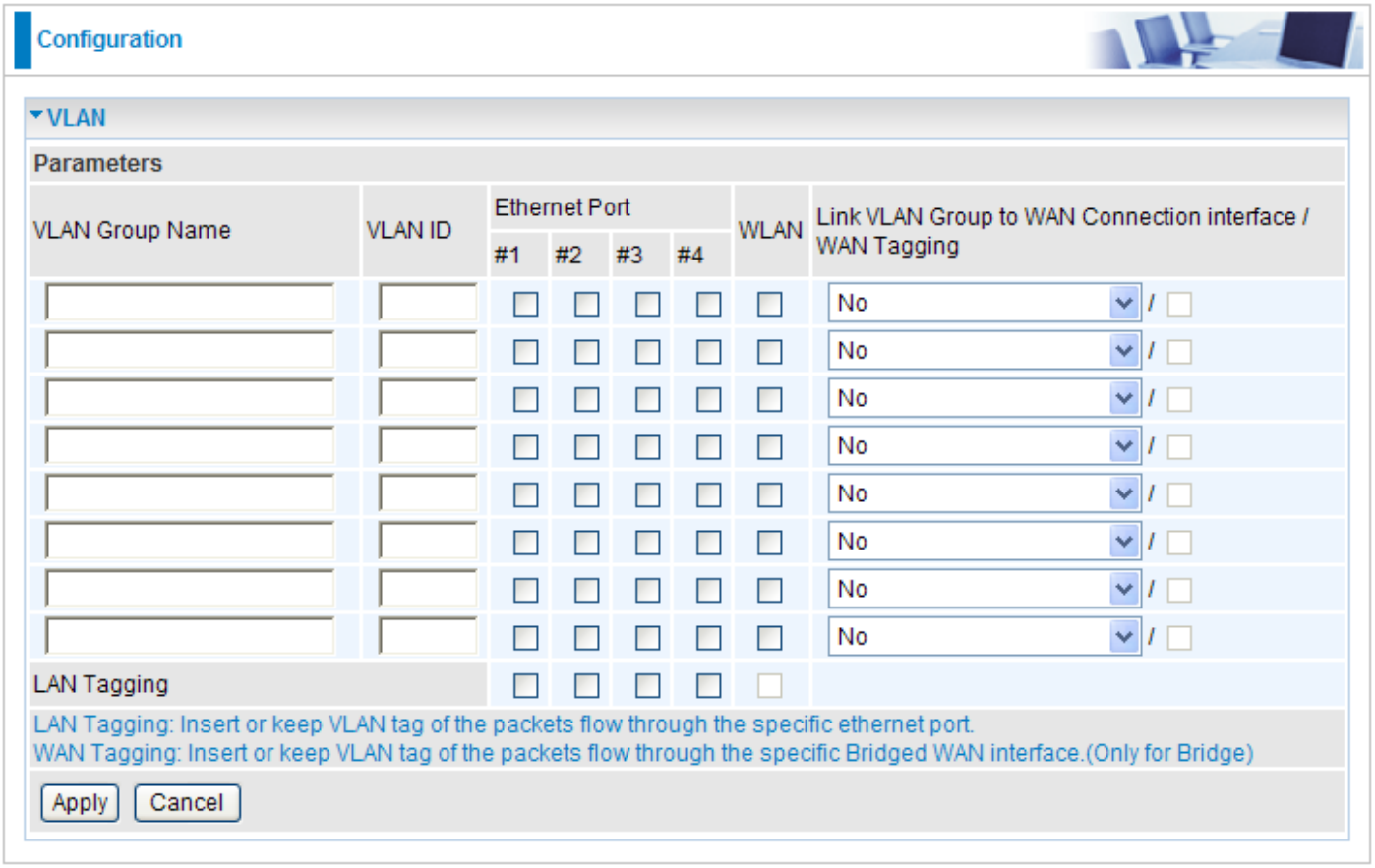
Domain Name, **Username** and **Password:** Enter your registered domain name and your username and password for this service.

Period: Enter the length of the period in the blank, you can set the period unit in day (d), hour (H) or minute (M). In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Click Apply to confirm the settings.

VLAN

VLAN (Virtual Local Area Network) is a group of devices on different physical LAN segments that can communicate with each other as if they were all on the same physical LAN segment.



VLAN Group Name: Please input VLAN name of this rule.

VLAN ID: Please input VLAN ID that will be used for Tagged member port(s).

Ethernet Port(s): Please check the interface that you would like to use in this VLAN ID group.

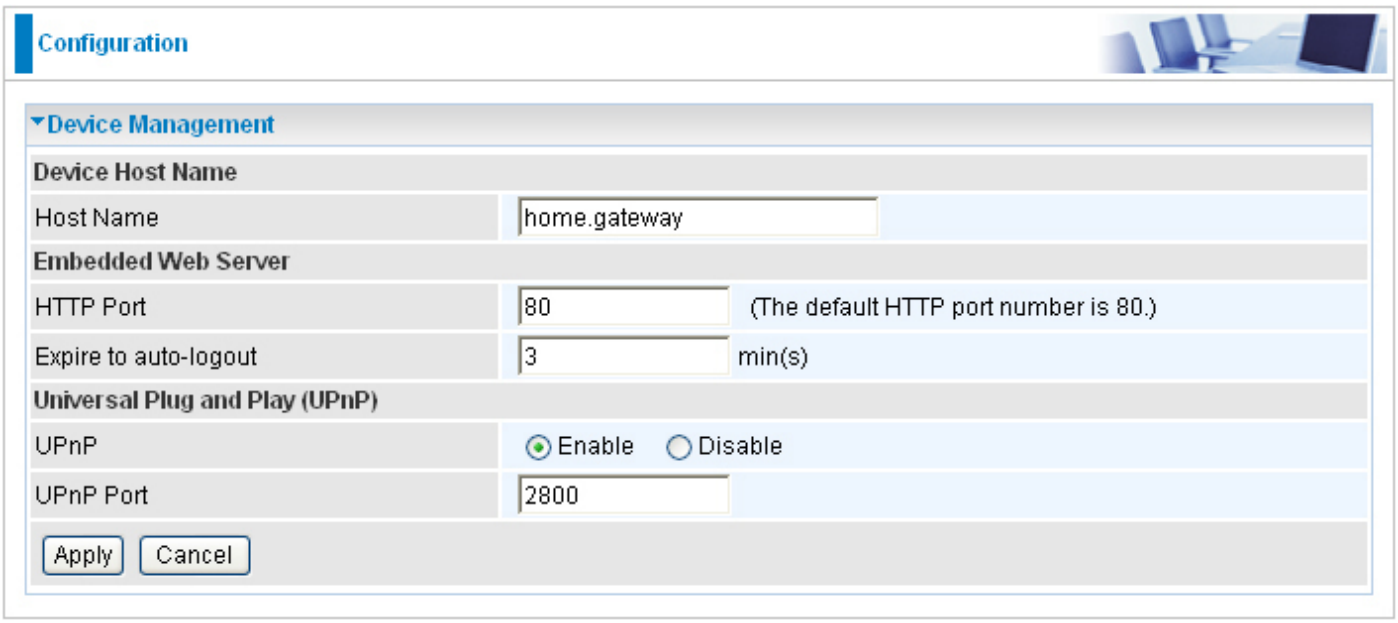
WLAN: Please check the interface that you would like to use in this VLAN ID group.

Link VLAN Group to WAN connection interface / WAN Tagging: Select the WAN interface from the drop-down menu to associate the VLAN Group with it.

Click Apply to confirm the settings.

Device Management

The Device Management advanced configuration settings allows you to control your router's security options and device monitoring features.



Device Host Name

Host Name: Assign it a name.

(The Host Name cannot be used with one word only. There are two words should be connected with a '.' at least.
Example:
Host Name: homegateway ==> Incorrect
Host Name: home.gateway or my.home.gateway ==> Correct)

Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Expire to auto-logout: Specify a time length for the system to auto-logout user from the configuration session.

Example: User A enters 100 for HTTP port number, specifies 192.168.1.55 for his/hser own IP address, and sets the logout time to 100 minutes. The router will allow User A to access only from the IP address 192.168.1.55 to logon to the Web GUI by typing: http://192.168.1.254:100 in their web browser. After 100 minutes, User A is logged out by the device automatically.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with the feature to control data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems. By letting the application control the required settings and removing the need for the user to control the advanced configuration of their device will make tasks such as port forwarding become easier.

Both user's Operating System and its relevant applications must support UPnP in addition to the router. Windows XP and Windows Me have a native built-in support for UPnP (when the component is installed). Windows 98 users may have to install the Internet Connection Sharing client from Windows XP in order to support UpnP feature. Windows 2000 does not support UPnP.

Disable: Check to inactive the router's UPnP functionality.

Enable: Check to active the router's UPnP functionality.

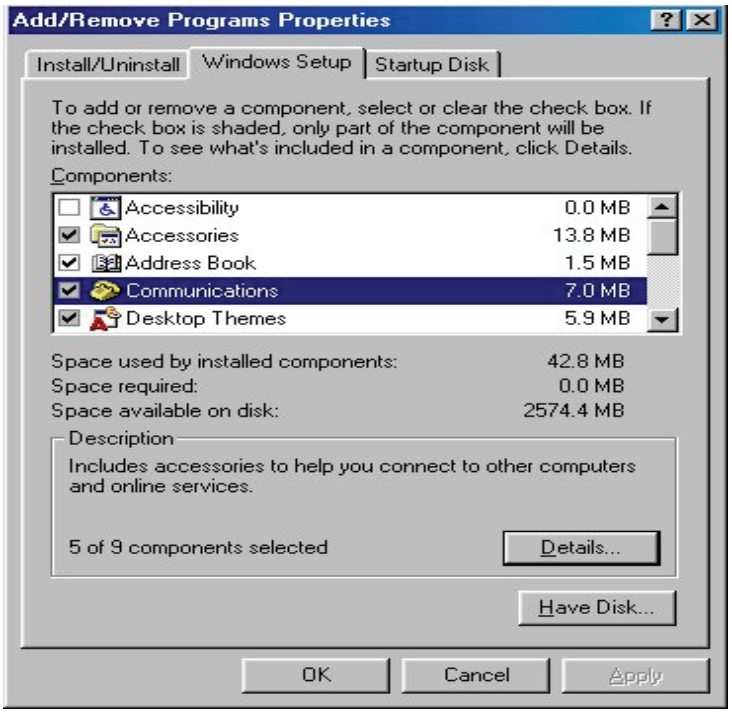
UPnP Port: Default setting is 2800. It is highly recommended for users to use this port value. If this value conflicts with other ports that have been used, you are allowed to change the port number.

Installing UPnP in Windows Example

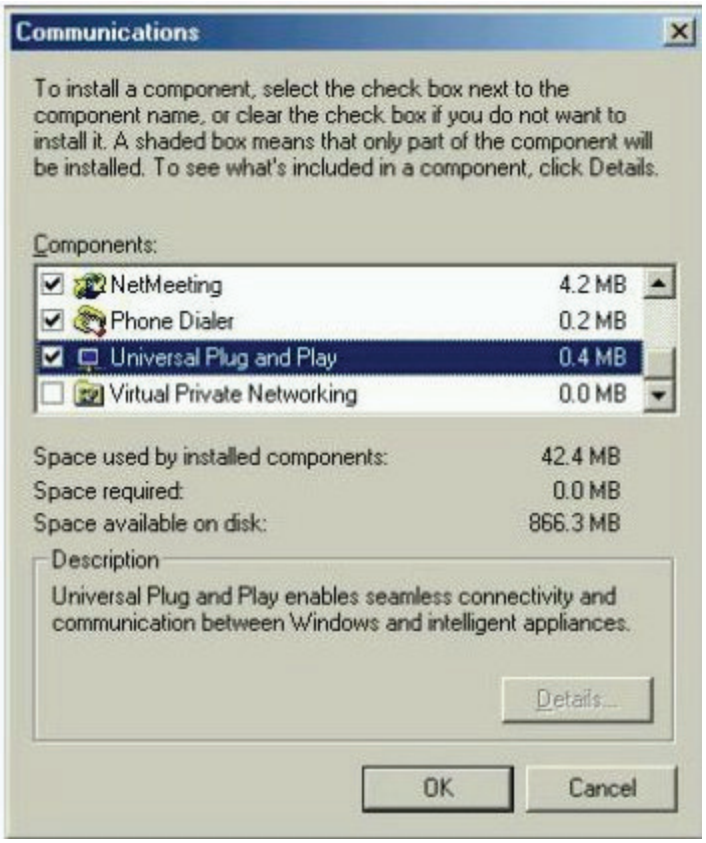
Follow the steps below to install the UPnP in Windows Me.

Step 1: Click Start and Control Panel. Double-click Add/Remove Programs.

Step 2: Click on the Windows Setup tab and select Communication in the Components selection box. Click Details.



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



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

Step 5: Restart the computer when prompted.

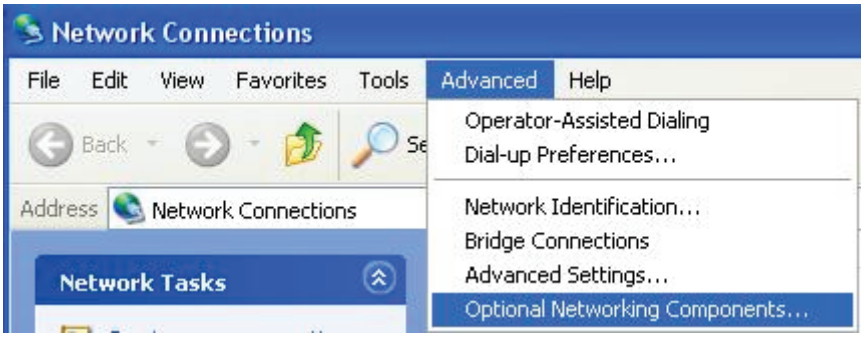
Follow the steps below to install the UPnP in Windows XP.

Step 1: Click Start and Control Panel.

Step 2: Double-click Network Connections.

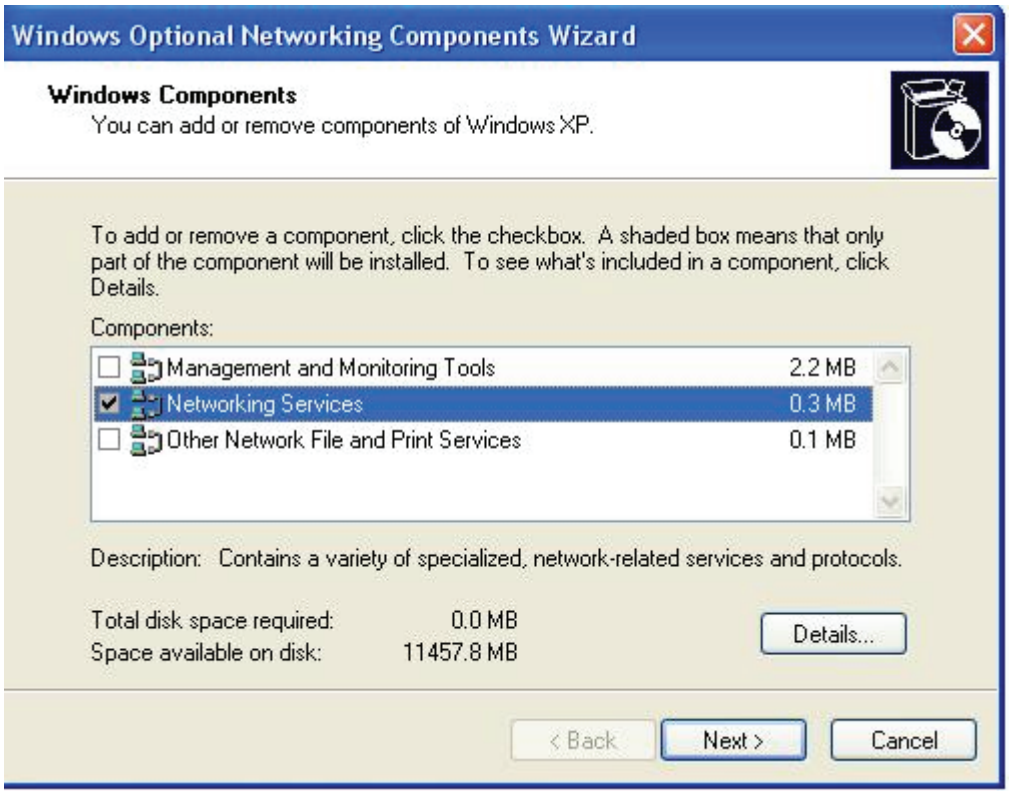
Step 3: In the Network Connections window, click Advanced in the main menu and select Optional Networking Components ….

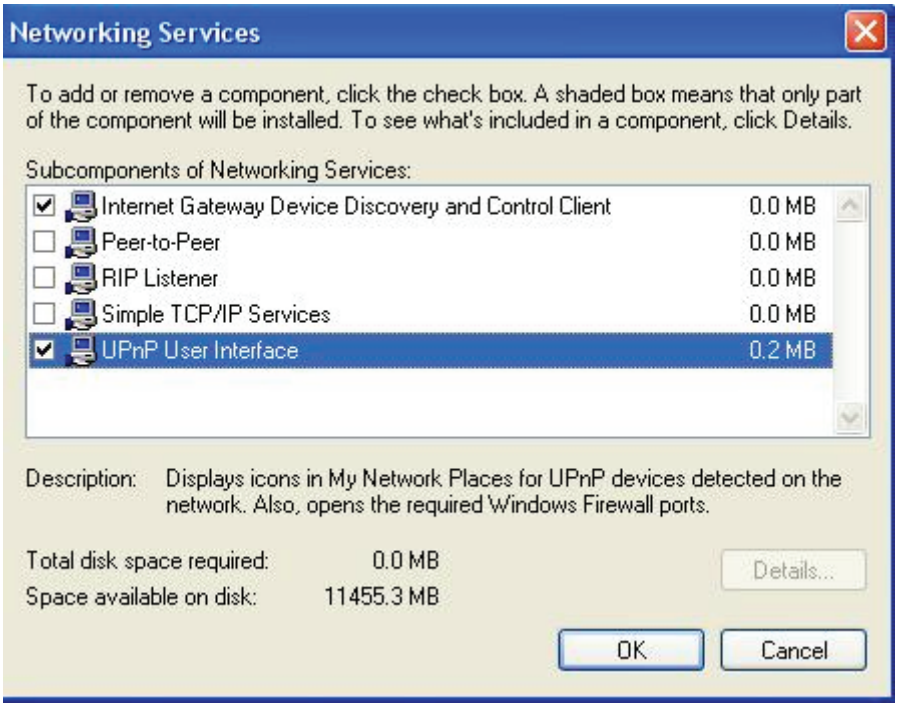
Step 4: When the Windows Optional Networking Components Wizard window appears, select Networking Service in the Components selection box and click Details.



Step 5: In the Networking Services window, select the Universal Plug and Play check box.

Step 6: Click OK to go back to the Windows Optional Networking Component Wizard window and click Next.





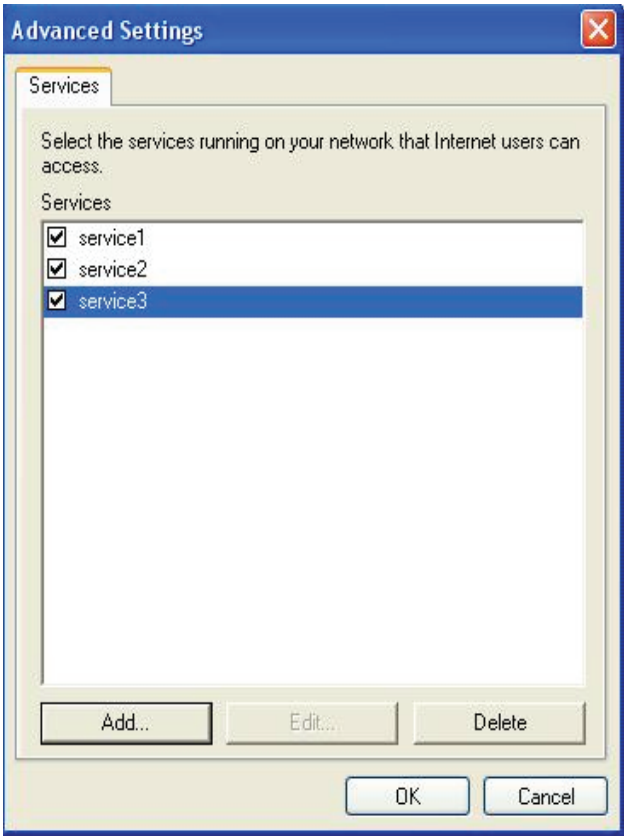
Auto-discover Your UPnP-enabled Network Device

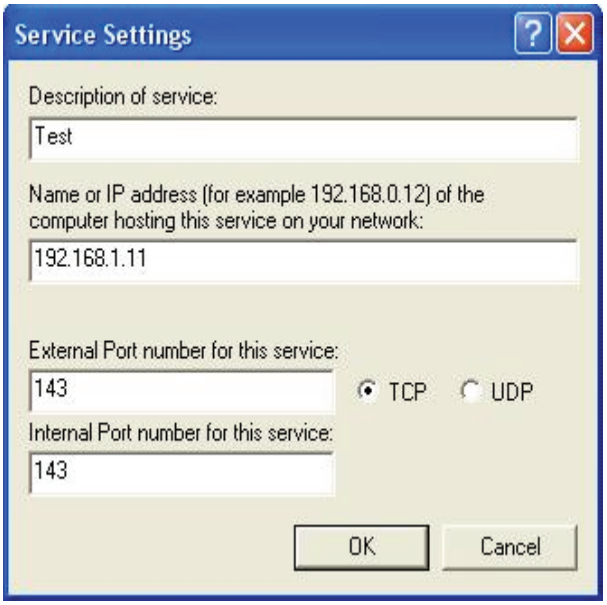
Step 1: Click start and Control Panel. Double-click Network Connections. An icon displays under Internet Gateway.

Step 2: Right-click the icon and select Properties.

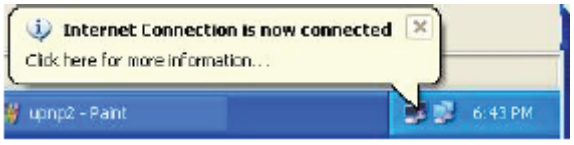
Step 3: In the Internet Connection Properties window, click Settings to see the port mappings that were automatically created.

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



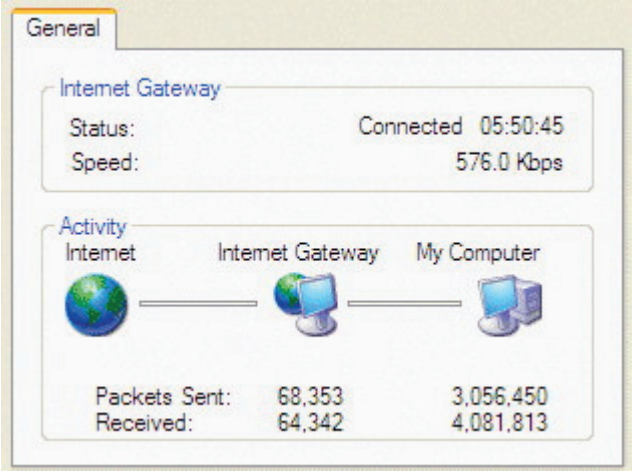


Step 5: Select Show icon in notification area when connected option and click OK. An icon displays in the system tray.



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

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



Web Configurator Easy Access

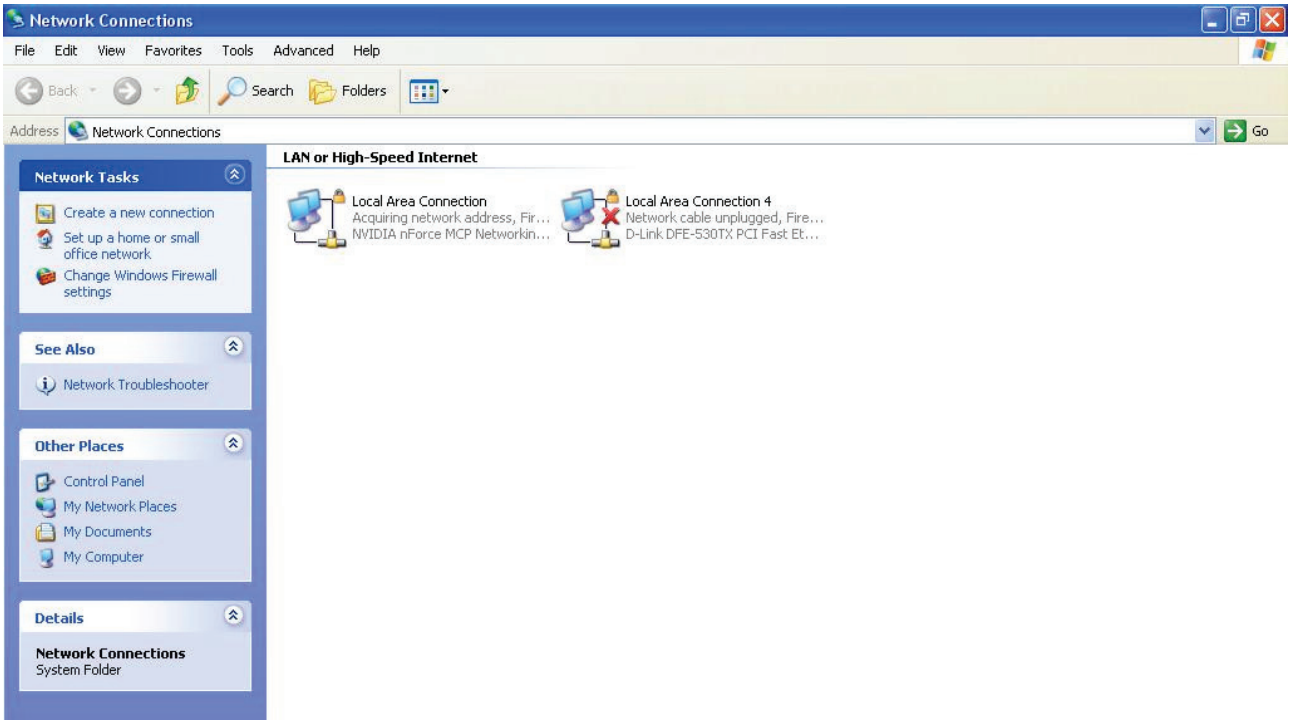
With UPnP, you can access web-based configuration for the BiPAC 9300(V)NX without first finding out the IP address of the router. This helps if you do not know the router's IP address.

Follow the steps below to access web configuration.

Step 1: Click Start and then Control Panel.

Step 2: Double-click Network Connections.

Step 3: Select My Network Places under Other Places.



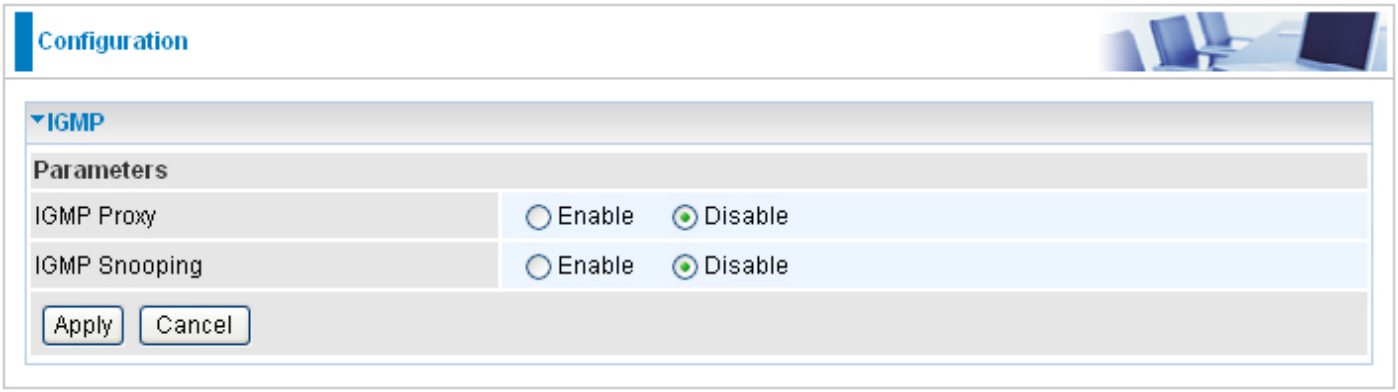
Step 4: An icon describing each UPnP-enabled device shows under Local Network.

Step 5: Right-click on the icon of your BiPAC 9300(V)NX and select Invoke. The web configuration login screen displays.

Step 6: Right-click on the icon of your BiPAC 9300(V)NX and select Properties. A properties window displays basic information about the BiPAC 9300(V)NX.

IGMP

IGMP, known as Internet Group Management Protocol, is used to manage hosts from multicast group.



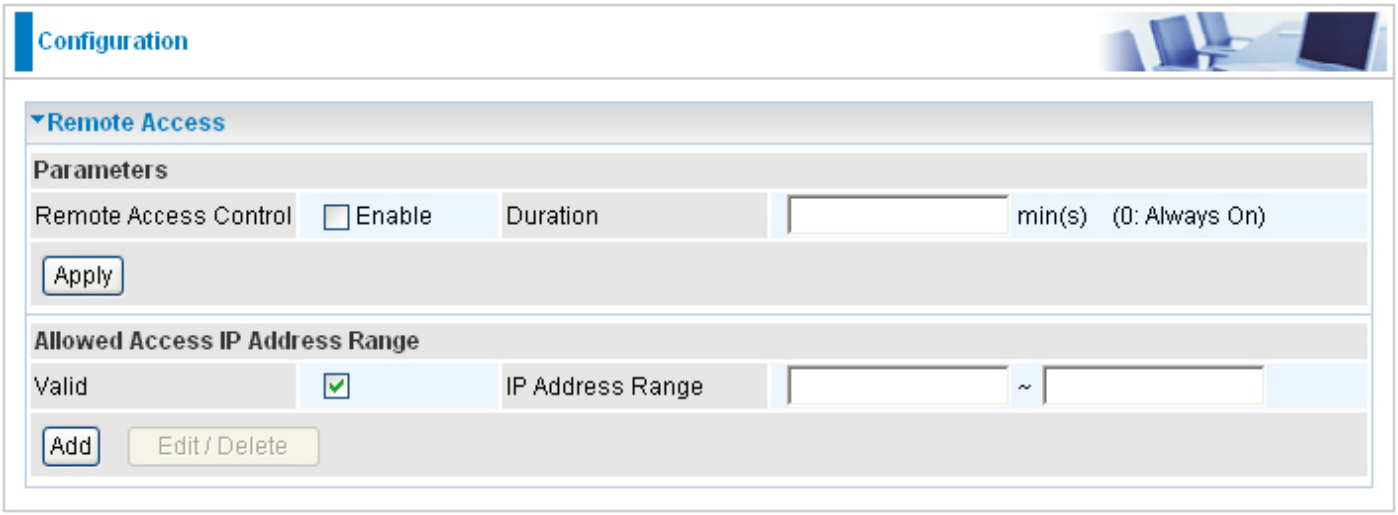
IGMP Proxy: IGMP proxy enables the system to issue IGMP host messages on behalf of the hosts that the system has discovered through standard IGMP interfaces. The system acts as a proxy for its hosts.

IGMP Snooping: Allows a layer 2 switch to manage the transmission of any incoming IGMP multicast packet groups between the host and the router. Default is set to Disable.

Click Apply to confirm the changes.

Example:
When IGMP snooping is enabled, the feature will analyze all incoming IGMP packets between the hosts that are connected to the switch and the multicast routers in the network. When the layer 2 switch receives an IGMP report from a host requesting for a given multicast group, the switch will add the host's port number to the multicast list for that multicast group to be forwarded to. And, when the layer 2 switch has detected that an IGMP has left, it will remove the host's port from the table entry.

Remote Access



Remote Access Control

Enable: Select Enable to allow management access from remote side (mostly from internet).

Duration: Set how many minutes to allow management access from remote side. Zero(0) means always on.

Click Apply to confirm the settings.

Allowed Access IP Address Range

Valid: Tick this check box to allow remote management from these IP ranges.

IP Address Range: Specify the remote IP address which will be allowed access device. Clink Add to insert management IP address(es) to the list.

Click Add to save the settings.

Advanced VoIP (Only for 9300VN(X))

VoIP (Voice over Internet Protocol) enables telephone calls through existing Internet connection instead of going through the PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long distance telephone charges, but also toll-quality voice calls over the Internet.

Attention

After completing VoIP configuration, remember to apply the changes. Press Save Config and restart to activate your VoIP.

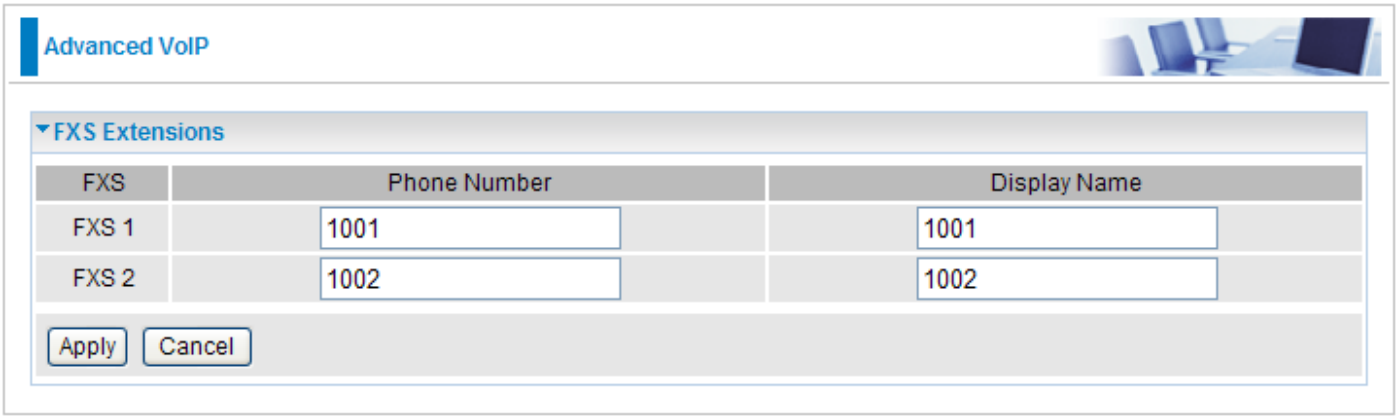
When you click this item, the column will expand to display the sub-items that will allow you to configure the advanced VoIP settings.

Here are the items within the this section: **Extensions**, **SIP Accounts (ITSP)** and **Mini IP-PBX**.

The function of each configuration sub-item is described in the following sections.

Extensions

FXS Extensions



The BiPAC router comes with 2 built in phone ports (FXS ports) that enables the device to connect up to 2 phones. The local number is a unique number that is assigned to each phone. With the local number feature, 2 different users can call each other simply by dialing the local number of the phone.

Phone Number FXS 1 / Phone Number FXS 2: The internal SIP proxy number of FXS1 / FXS2. Fill in the Local Number. If you have only a phone connected to the FXS port, you only need to fill out one Local number. But if you have two phones connected, assign your phones with two different local numbers.

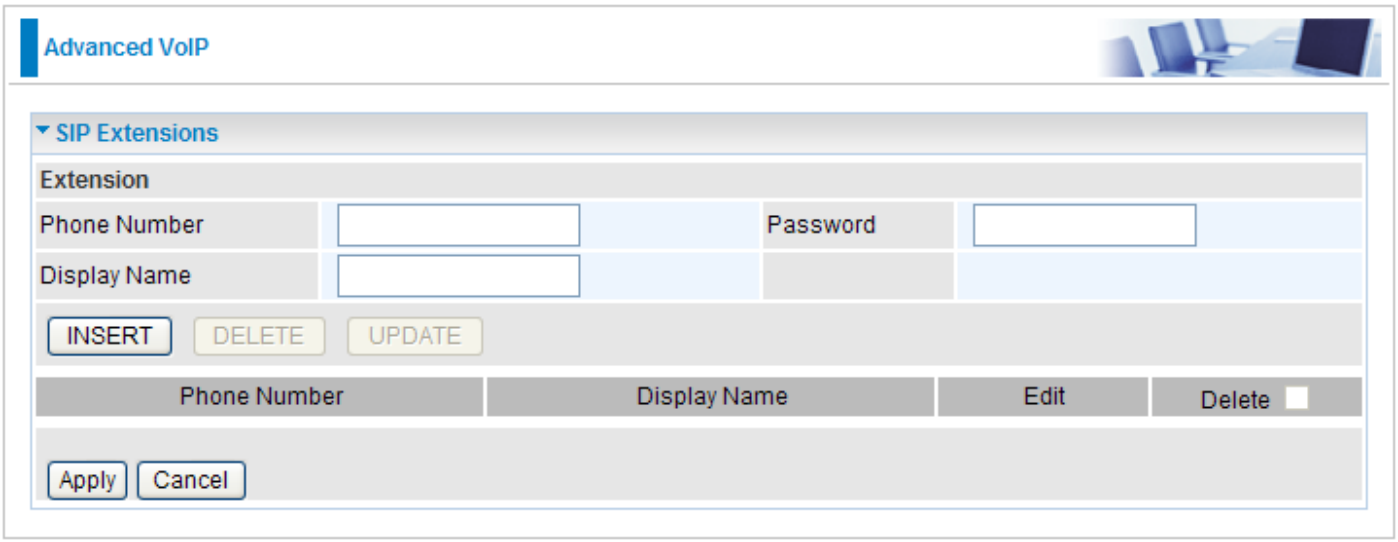
Note: Local number can be assigned by the administrator. It is higly recommended that you use 3 digits for the local number.

Display Name FXS 1 / Display Name FXS 2: This is the name of FXS1 / FXS2 that will be displayed.

After the Local Number has been assigned, press Apply to apply the changes to the setting.

SIP Extensions

This is the server that provides registration service for SIP ATA / SIP Phone.



Phone Number: Enter the phone number or your registered user ID.

Password: Enter the authenticated password which is required to logon to SIP server.

Display Name: Enter the name that you wish to be displayed when making a SIP call.

INSERT: Click this button to add a new SIP extension entry and the added entry will appear at the bottom table.

Edit / UPDATE: Check Edit radio box next to the item you wish to modify, and then change parameters as desired. Complete it by press UPDATE.

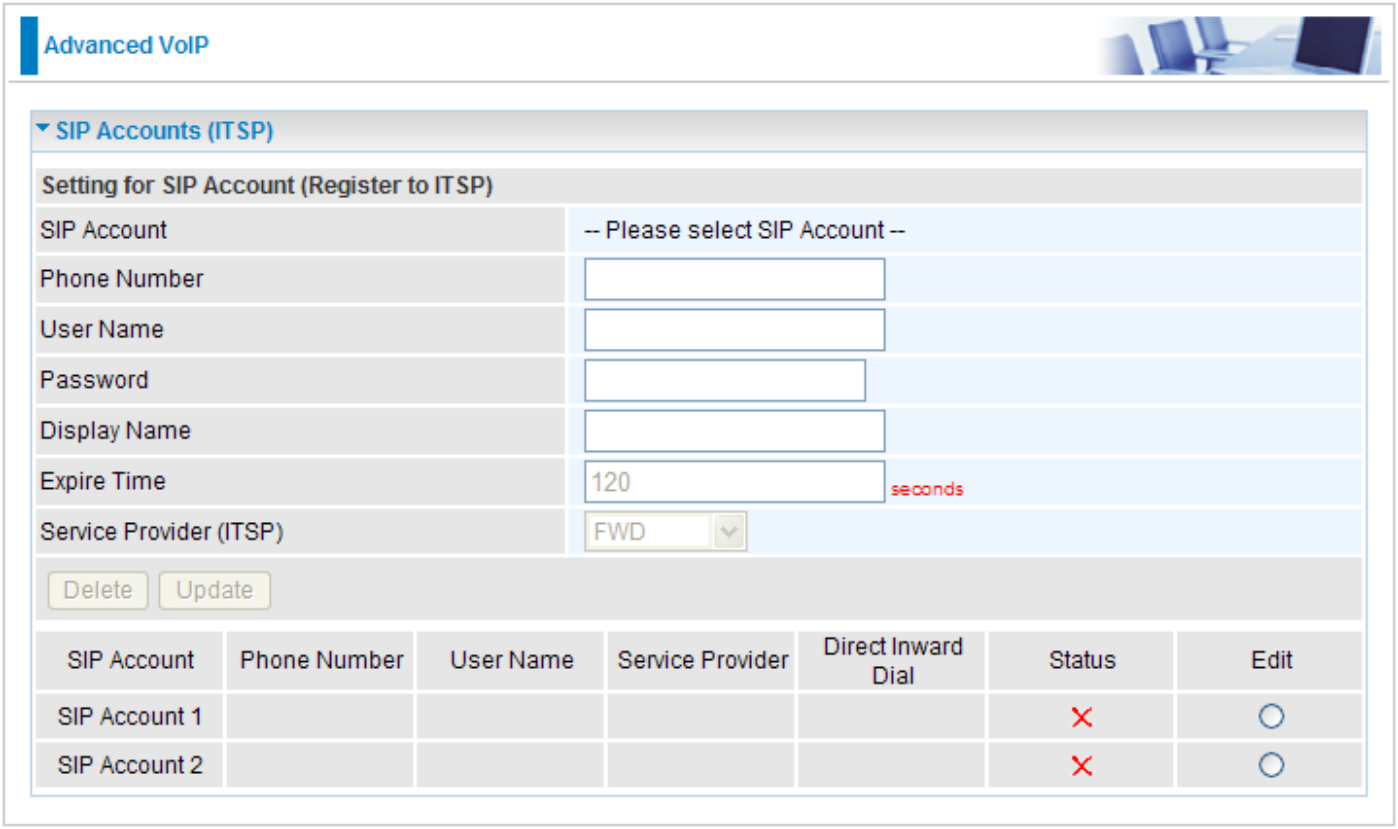
Delete / DELETE: Check Delete checking box next to the item you wish to remove, and press DELETE to remove this entry.

Click Apply to confirm the settings.

SIP Accounts (ITSP)

SIP Accounts

SIP account is the SIP server that makes connection to the external VoIP service provider easy to establish.



Setting for SIP Account (Register to ITSP): This is the SIP account setting for the external VoIP Service Provider.

SIP Account: The SIP account that you want to configure.

Phone Number: Enter the phone number or your registered user ID.

User Name: Enter your registered user name.

Password: Enter the authenticated password which is required to logon to SIP server.

Display Name: Enter the name that will be displayed when you dial the SIP phone.

Expire Time: Duration (in seconds) of incoming/outgoing registration. Default vaule is 120 seconds.

Service Provider (ITSP): Select the external VoIP Service Provider profile that you wish to connect to from the drop down menu.

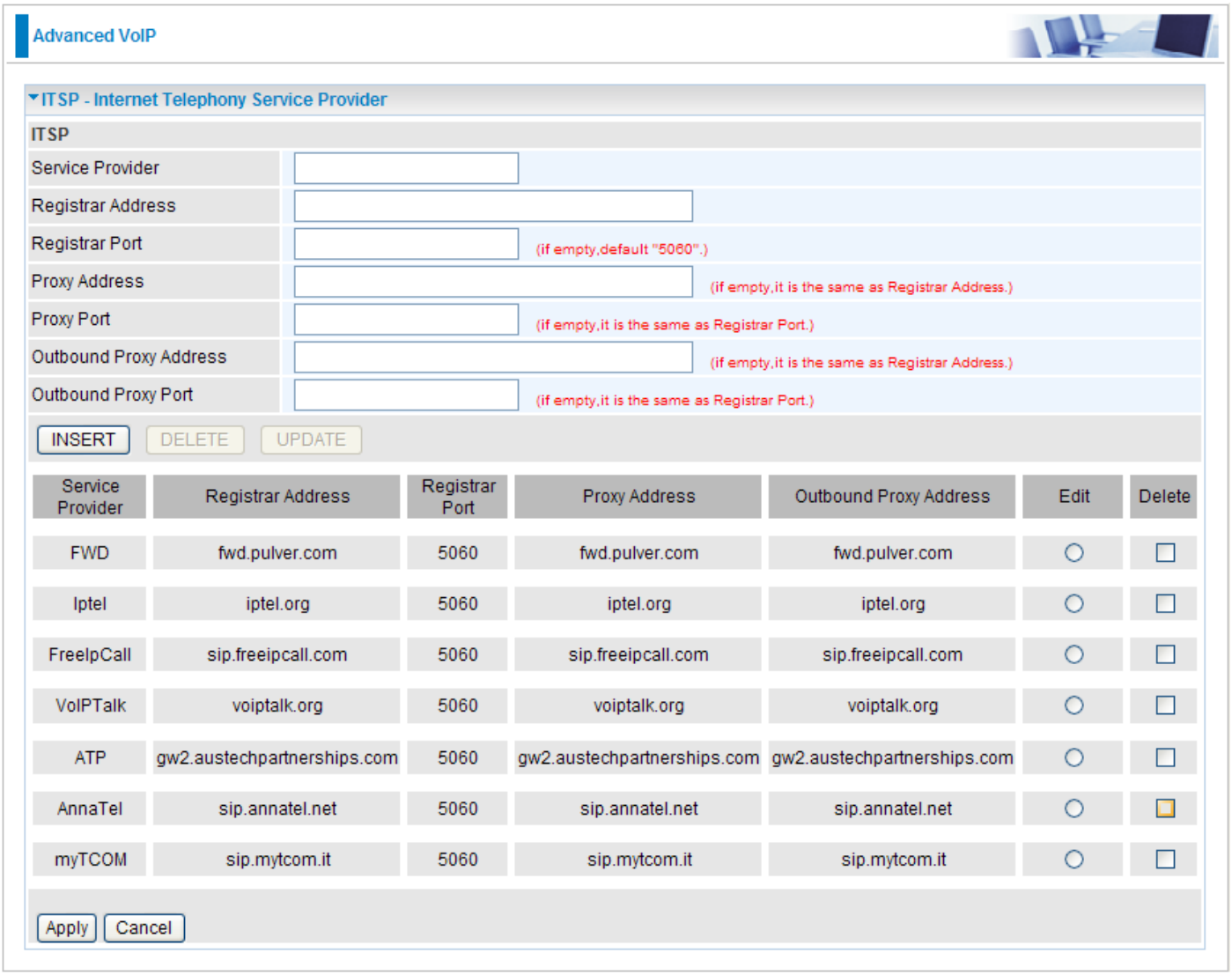
Edit / Update: Check Edit radio box next to the item you wish to modify, and then change parameters as desired. Complete it by press Update.

Delete: Check Edit radio box and then press Delete to cancel the configuration you set to this acconut.

Click Apply to confirm the settings.

ITSP

You are allowed to edit the information of the external VoIP service provider or add new service providers on this screen.



Service Provider: Enter the name of the service provider.

Registrar Address: Enter the SIP register server IP address.

Registrar Port: Enter the port number of the SIP register server. If this field is left empty, it will be assigned 5060 by default.

Proxy Address: Enter the IP Address of the SIP proxy server. If this field is left empty, it will be set the same IP as Registrar Address by default.

Proxy Port: Specify the port of the SIP proxy server on which it will listen for messages. If this field is left empty, it will be set the same value as Registrar Port by default.

Outbound Proxy Address: Indicate the SIP outbound proxy server IP address. This parameter is very useful when VoIP device is located behind a NAT. If this field is left empty, it will be set the same IP as Registrar Address by default.

Outbound Proxy Port: Specify the port of the SIP outbound proxy on which it will listen for messages. If this field is left empty, it will be set the same value as Registrar Port by default.

INSERT: If you do not find the name of your service provider in the list, you can add a new service provider to the list. To add a new service provider, enter all the necessary information in the correct spaces and then click INSERT button. The added entry will appear at the bottom table.

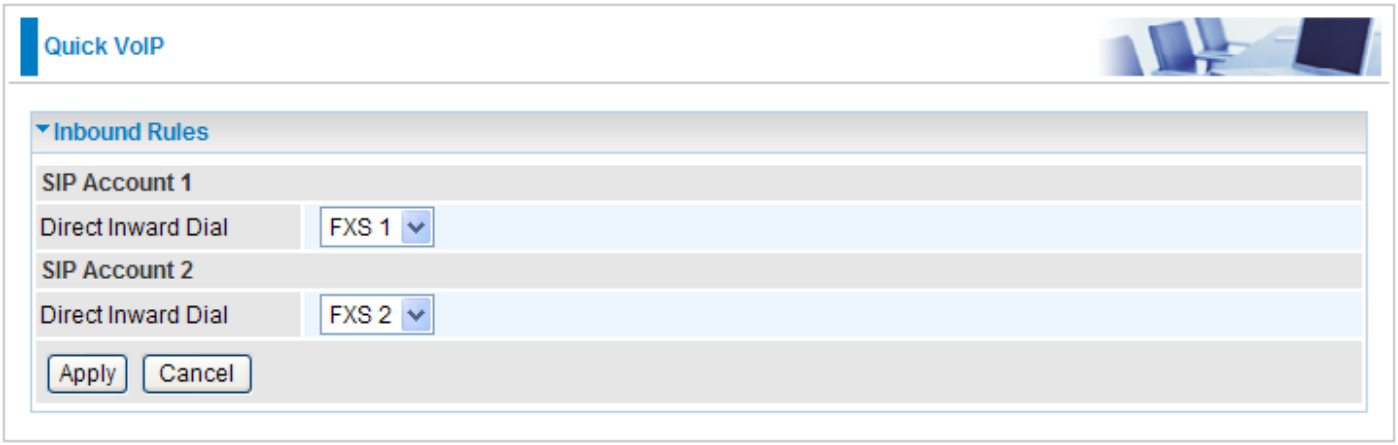
Edit / UPDATE: Check Edit radio box next to the item you wish to modify. Once a service provider is selected, all the information of this service provider will be displayed. You can then edit the information by deleting the old information and entering the new ones. Complete it by press UPDATE.

Delete / DELETE: Check Delete checking box next to the item you wish to remove, and press DELETE to remove this service provider.

Click Apply to save the changes and apply the newly configured setting to the device.

Inbound Rules

Direct Inward Dialing (DID) is a trunking arrangement that allows direct inward call routing to each extension without the need for an operator or attendant. It saves time and reduces cost. DID service is usually combined with direct outward dialing (DOD).

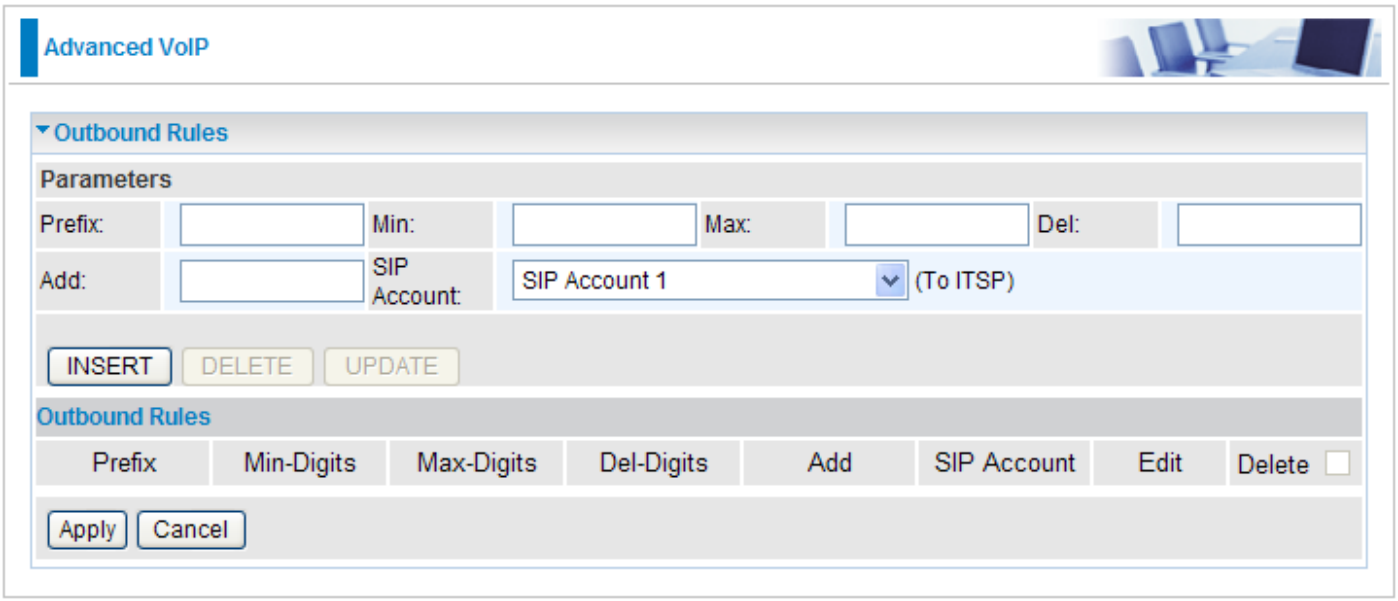


Direct Inward Dial SIP Account 1 / SIP Account 2: Select FXS1 or FXS2 from the drop-down manu.

Click Apply to confirm the settings.

Outbound Rules

Direct Outward Dialing is an automated PBX (private branch exchange) service that allows users to make outbound calls directly, without the need to go through an operator or dial other numbers first. This page allows you to set-up rules for making an outbound call.



Prefix: This number is required whenever the user wants to dial out a call using VoIP instead of PSTN. The numbers defined in this field will be inserted at the beginning of the dialing pattern. Numbers 0 and 9 must not be used in order to avoid conflict with PSTN Prefix.

Min: This field allows you to set the minimum number of digit that needs to be key-in before your dialing becomes invalid after a set interval. For example: If the minimum value is set to 3, whenever you make the call, if you only dial 2 digits and pause for a long time, your dialing will automatically be cut.

Max: This field allows you to set the maximum number of digit that can be key-in before your dialing becomes invalid. For example: If the maximum value is set to 10, and if you dial for more than 10 digits, your call will not go through.

Del: The number of digit defined in this field will be removed from the dialing pattern. For example, if we dial 81352109378 and the delete digit is set to 2, then the actual number that will be displayed is 352109378 as the first 2 digits are already removed.

Add: The numbers set in this field will be added at the beginning of your dialing numbers. For example, if 001 is set in this field, the number you dial out will be displayed as 001+the rest of the numbers.

SIP Account: Choose the outbound rule for SIP Account 1 , 2 or All from the drop-down menu.

INSERT: Enter all the necessary parameters of your new outbound rule in the blanks provided. Then press INSERT to add a new rule. The added entry will appear at the bottom table.

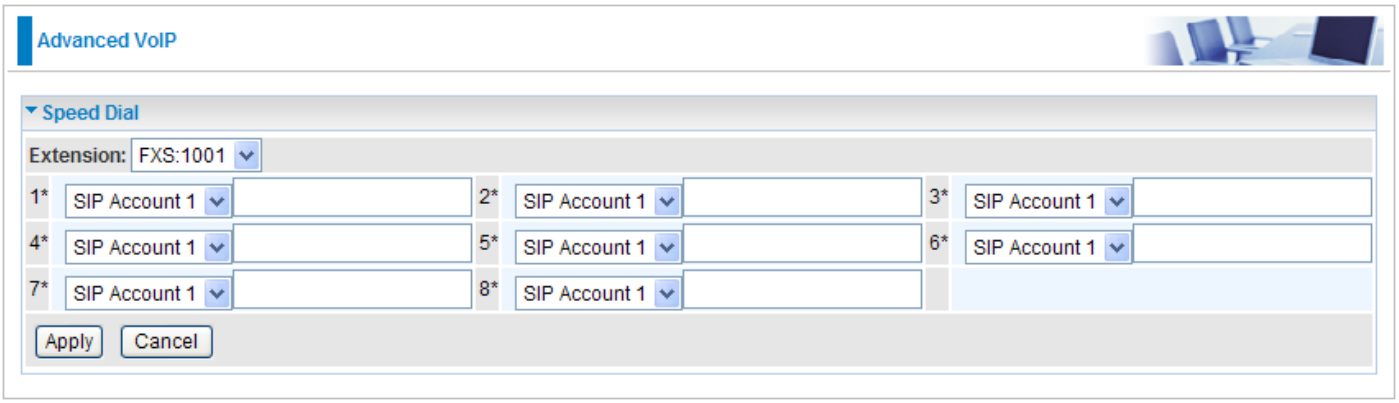
Edit / UPDATE: Check Edit radio box next to the item you wish to modify. Once a outbound rule is selected, all the information of this rule will be displayed. You can then change its values. Complete it by press UPDATE.

Delete / DELETE: Check Delete checking box next to the item you wish to remove, and press DELETE to remove this outbound rule.

Click Apply to confirm the settings.

Speed Dial

Speed Dial comes in handy to store frequently used telephone numbers which you can press number from 1 to 8 and the pound sign (*) on the phone keypad to activate the function. For example, speed dial to phone number lists on 3, just press keypad 3 then *. Your router will automatically call out to number listed on entry 3.



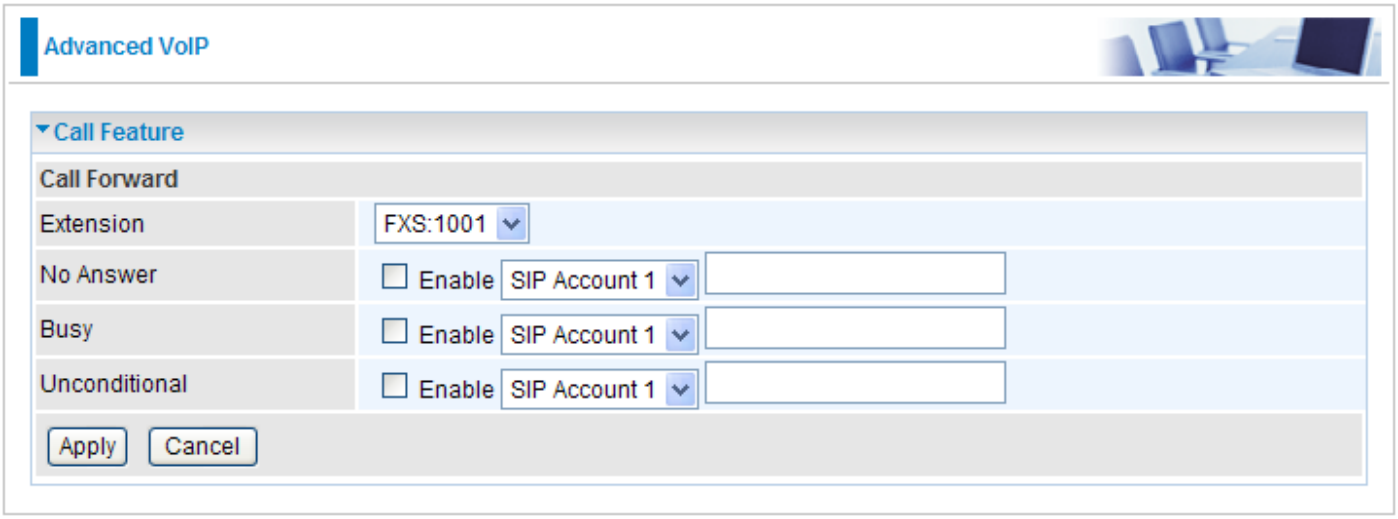
Extension: Select FXS:1001 or FXS:1002 that you want to configure from the drop-down menu.

1* ~ 8*: Select SIP Account 1,2 or Extension from the drop-down menu and enter a telephone number.

Click Apply to confirm the settings.

Call Feature

VoIP has all the basic features of a traditional phone. Besides the provided basic features, VoIP also comes with several enhanced features that allows you to further customize their settings to suit your personal needs such as call forwarding setting when no one answers the call, or when the phone is being used at the moment, you can even set the condition to have all incoming calls being forwarded to the forwarding number under all circumstances.



Extension: Select FXS:1001 or FXS:1002 that you want to configure from the drop-down menu.

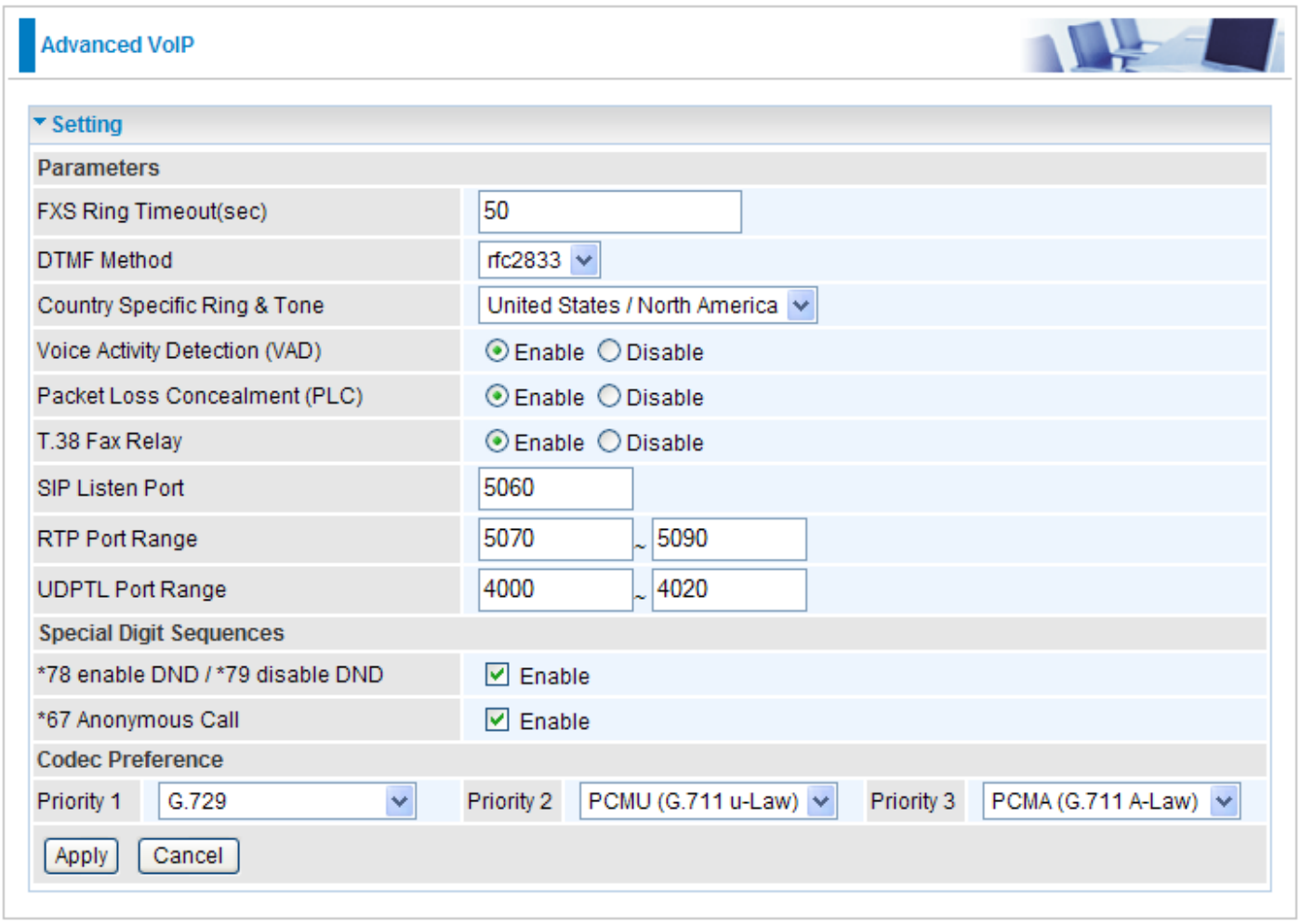
No Answer: VoIP device will forward all incoming calls to the forwarding number when user is unavailable to pick up the phone. Check Enable to activate this function. Select SIP Account 1,2 or Extension from the drop-down menu and enter a telephone number.

Busy: VoIP device will forward all incoming calls to the forwarding number when the phone is currently being used. Check Enable to activate this function. Select SIP Account 1,2 or Extension from the drop-down menu and enter a telephone number.

Unconditional: VoIP device will forward all incoming call to the forwarding number under all circumstances. Check Enable to activate this function. Select SIP Account 1,2 or Extension from the drop-down menu and enter a telephone number.

Click Apply to confirm the settings.

Setting



Parameters

FXS Ring Timeout(sec): The IAD (Integrated Access Device) will automatically reject a call in if the call is not picked up within the set amount of time.

DTMF Method: This is a type of telephone signaling that is used to signal your call over the line in the voice -frequency band to the call switching center. There are basically 3 types of DTMF method to choose from: rfc2833, info and inband. The default is rfc2833.

Country Specific Ring & Tone: Specify the country that has the dialing tone which fits the local telco system requirement

Voice Activity Detection (VAD): The voice activity detection (VAD) is a component in the DSP software that examines a caller's incoming signal and determines if the signal contains significant energy and is likely to be speech rather than a click. This function is enabled by default.

Packet Loss Concealment (PLC): This is a technique to mask the effects of packet loss in VoIP communications. Because the voice signal is sent as packets on a VoIP network, they may travel different routes to get to destination. Thus, a packet might arrive very late, corrupted or simply might even not arrive at the receiver. One of the situations in which the last situation could happen is where a packet is rejected by a server which has a full buffer and cannot accept any more data. In a VoIP connection, error-control techniques such as ARQ are not feasible and the receiver should be able to cope with packet loss. This function is enabled by default.

T.38 Fax Relay: T.38 is an ITU standard for sending FAX across IP networks in the real-time mode. This function is enabled by default.

SIP Listen Port: Specify the port of the SIP proxy server on which it will listen for messages. Port 5060 is the standard port for SIP and is set as the default. This port number relies on your SIP Service Provider; you should enter the correct port number if your SIP provider uses a different port number other than 5060.

RTP Port Range: One VoIP call opens two RTP ports for communication; one for the media stream, and the other for control - RTCP.

UDPTL Port Range: One T.38 FAX call opens one port. T.38 FAX messages are sent as UDP packets. UDPTL port is used by T.38 FAX call.

Special Digit Sequences

***78 enable DND / *79 disable DND:** When the phone that is connected to the FXS port is picked up, you can press number *78 to activate the DND (don't disturb) feature. If you press *79, the DND (don't disturb) feature will be disabled. Default is checked to activate this function.

***67 Anonymous Call:** If you dial *67 first followed by the phone number, your caller ID will not be displayed. Default is checked to activate this function.

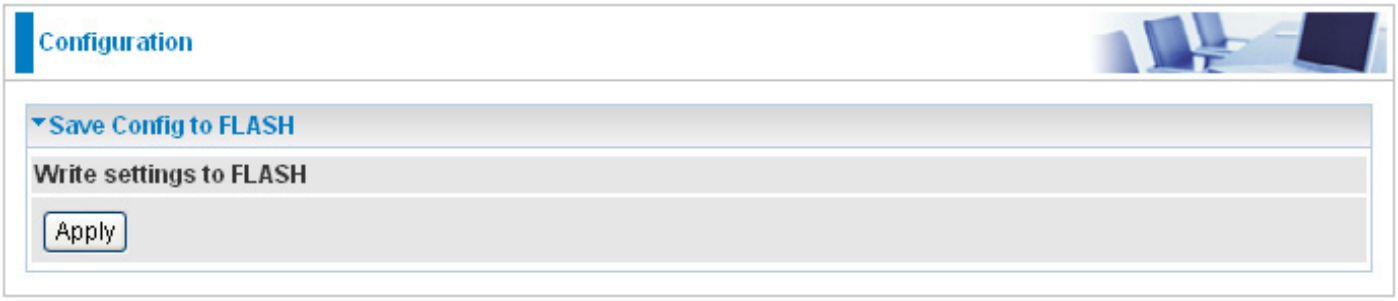
Codec Preference

Priority 1 / 2 / 3: You may set the level of priority of the voice codec. There are 3 types of codec you can select from: G.729, PCMU (G.711 u-Law) & PCMA (G.711 a-Law).

Click Apply to confirm the settings.

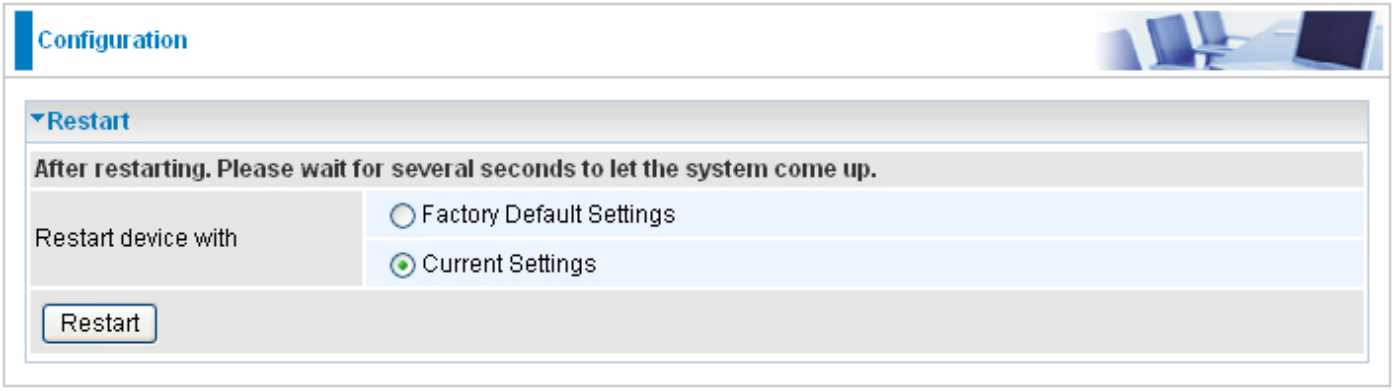
Save Configuration to Flash

After changing the router's configuration settings, you must save all of the configuration parameters to FLASH to avoid losing them after turning off or resetting your router. Click "Save Config" and click "Apply" to write your new configuration to FLASH.



Restart

Click “Restart” with option Current Settings to reboot your router (and restore your last saved configuration).



If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select Factory Default Settings to reset to factory default settings

Logout

To exit the router web interface, click “Logout”. Please save your configuration setting before logging out of the system. A Warning screen will appear as below.

Click OK and a message displays. Click Yes to close the window.

Be aware that the router configuration interface can only be accessed by one PC at a time. Therefore when a PC has logged into the system interface, the other users cannot access the system interface until the current user has logged out of the system. If the previous user forgets to logout, the second PC can only access the router web interface after a user-defined auto logout period which is by default 3 minutes. You can however modify the value of the auto logout period using the Advanced > Device Management section of the router web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If your router is not functioning properly, please refer to the suggested solutions provided in this chapter. If your problems persist or the suggested solutions do not meet your needs, please kindly contact your service provider or Billion for support.

Problems with the router

Problem	Suggested Action
None of the LEDs lit when the router is turned on	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or Billion for technical support.
You have forgotten your login username or password	Try the default username & password (Please refer to Chapter 3). If this fails, restore your router to its default setting by pressing the Reset button for more than 6 seconds.

Problems with WAN interface

Problem	Suggested Action
Initialization of GPON connection (linesync) fail	Make sure that the fiber is properly connected between the GPON port and the wall jack. When the GPON LED on the front panel does not light, there are 2 ways to access the web interface to check the GPON port is properly connected: • Status page: If ✕ is shown on Status page, the GPON port has not successfully connected or detected the optical signal. If ✓ is shown on Status page, the GPON port has correctly connected. If ⊘ is shown in GPON, the GPON connection has not been activated by OLT. • GPON Status page: Select Advanced > Status > GPON Status. If **Detected** in Optical Signal is not shown, the GPON connection has not ready. When the GPON LED on the front panel lit, but you are unable to access the Internet, check that your Alloc_ID and Port_ID are the same as those provided by your ISP and reboot the router. If you still have problem, please verify these settings with your ISP.

Problem with LAN interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not light, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.

Appendix: Product Support & Contact

Following the suggestions listed in the Troubleshooting section of the user manual can help you to solve most of your problems. However, if your problems persist or you come across other technical issues that are not listed in the Troubleshooting section, please contact the dealer from where you purchased your product.

Contact Billion

Worldwide:

http://www.billion.com

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

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