BILLION™

BiPAC 6300VNP

VoIP Wireless-N (VPN) Broadband Router

User Manual

Version release: v1.02b.dt28

Last revised: July 2, 2014

Table of Contents

Chapter 1: Introduction

Introduction to your Router

Congratulations on your purchase of the BiPAC 6300VNP s a compact and advanced broadband device that integrates two (2) FXS ports allows for simultanious VoIP calls, offers flexible, friendly, and rich features and Interface for home, SOHO, and office users to enjoy high-speed, high-level security Internet connection via Ethernet WAN. With an integrated 802.11n wireless access point and 4-port Gigabit Ethernet LAN, this router enables faster wireless speed of up to 300Mbps and LAN connection 10 times faster than regular 10/100Mbps Ethernet LAN.

Cost Saving

Making VoIP calls is extremely simple; just connect the router with your existing analog telephones. BiPAC 6300VNP complies with the most popularly adopted VoIP standard and SIP protocol to ensure interoperability with SIP devices and major VoIP Gateways. This router also supports a wider range of telephony features, such as Call Waiting, Conference, Speed Dial, Return Call, Redial, etc.

Wireless Mobility and Security

With an integrated 802.11n Wireless Access Point, this router delivers up to 3 times the wireless coverage of a 802.11b/g network device, so that wireless access is available everywhere in the house or office. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) allows you to expand your wireless network without additional wires or cables. BiPAC 6300VNP also supports the Wi-Fi Protected Setup (WPS) standard and allows users to establish a secure wireless network just by pressing a button. Multiple SSIDs allow users to access different networks through a single access point. Network managers can assign different policies and functions for each SSID, increasing the flexibility and efficiency of the network infrastructure.

IPv6 Supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. The router is already supporting IPv6, you can use it in IPv6 environment no need to change device. The dual-stack protocol implementation in an operating system is a fundamental IPv4-to-IPv6 transition technology. It implements IPv4 and IPv6 protocol stacks either independently or in a hybrid form. The hybrid form is commonly implemented in modern operating systems supporting IPv6.

Quick Start Wizard

Support a WEB GUI page to install this device quickly. With this wizard, simple steps will get you connected to the Internet immediately.

Firmware Upgradeable

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

Features & Specifications

- Gigabit Ethernet WAN (GbE WAN) for Fiber (FTTC/ FTTP/ FTTH) high WAN throughput
- Gigabit Ethernet LAN
- IPv6 ready (IPv4/IPv6 dual stack)
- Multiple wireless SSIDs with wireless guest access and client isolation
- IEEE 802.11 b/g/n compliant Wireless Access Point with Wi-Fi Protected Setup (WPS)
- Wi-Fi Protected Access (WPA-PSK/ WPA2-PSK) and Wired Equivalent Privacy (WEP)
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization management
- Universal Plug and Play (UPnP) Compliance
- Voice over IP compliant with SIP standard
- Two FXS ports for connecting to regular analog telephones
- Call Waiting, Conference Call
- Speed Dial, Return Call, Redial
- Don’t Disturb
- Ease of Use with Quick Installation Wizard
- One USB port for NAS (FTP/ SAMBA server)
- Ideal for SOHO, office, and home users

Network Protocols and Features

- IPv4, IPv6 or IPv4 / IPv6 Dual Stack
- NAT, static (v4/v6) routing and RIP-1 / 2
- DHCPv4 / v6
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server and DMZ
- SNTP, DNS proxy
- IGMP snooping and IGMP proxy
- MLD snooping and MLD proxy

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention including Land Attack, Ping of Death, etc

- Access control
- IP&MAC filter, URL Content Filter
- Password protection for system management
- VPN pass-through

Quality of Service Control

- Traffic prioritization management based-on Protocol, Port Number and IP Address (IPv4/ IPv6)

Wireless LAN

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

USB Application Server

- Storage/NAS: Samba server, FTP Server

VoIP

- Compliant with SIP standard (RFC3261)
- Codec: G.729, G.726, G.711 A-Law, G.711 u-Law
- DTMF Method: Inband, RFC 2833, SIP Info
- Caller ID Generation: DTMF, FSK
- Silence Suppression (VAD), Echo Cancellation
- Call Waiting, Conference Call
- Speed Dial, Return Call, Redial
- Don't Disturb
- FAX Relay: T.38
- Call Detailed Records (CDR)

Management

- Quick Installation wizard
- Web-based GUI for remote and local management (IPv4/IPv6)

- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP server / client / relay
- Supports SNMP v1, v2, v3, MIB-I and MIB-II
- TR-069 supports remote management

Hardware Specifications

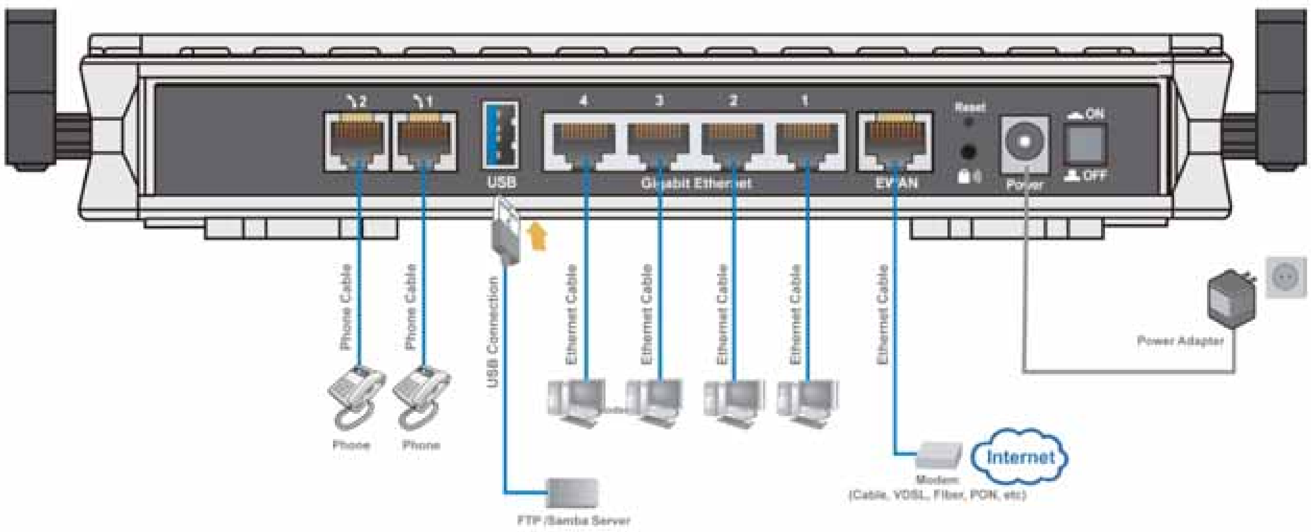
Physical interface

- Wireless antenna: 2 external antennas
- VoIP phone port: 2 RJ-11 FXS phone ports to connect with 2 regular analog phones.
- USB: USB 2.0 port for storage service
- Ethernet: 4-port 10 / 100 / 1000Mbps auto-crossover (MDI / MDI-X) Switch
- EWAN: RJ-45 Gigabit Ethernet port for connecting to Cable/Fiber/xDSL modem for Broadband connectivity.
- Factory default reset button
- Wireless on/off and WPS push button
- Power jack
- Power On/Off switch.

Physical Specifications

- Dimensions (W*H*D): 9.04" x 6.10" x 1.27"(229.5mm x 155mm x 32.24mm)
- Weight: 0.42kgs (0.93lbs)

Application Diagram



Chapter 2: Product Overview

Important Note for Using This Router

Warning

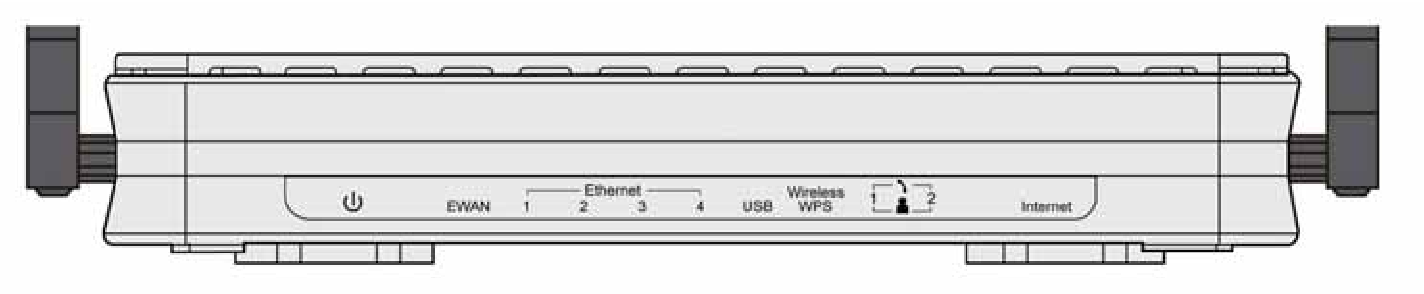
- ✓ Do not use the router in high humidity or high temperature.
- ✓ Do not use the same power source for the BiPAC 6300VNP on other equipment.
- ✓ Do not open or repair the case yourself. If the device becomes too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ 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.

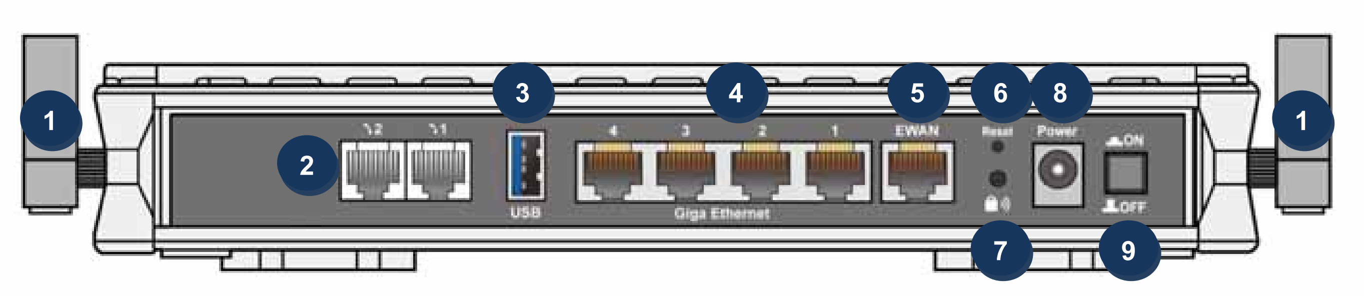
Device Description

Front Panel LEDs



LED	STATUS	DESCRIPTION
Power	Green	System is up and ready
	Red	Boot failure
EWAN	Lit up	BiPAC 6300VNP is successfully connected with a broadband connection device.
	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data being transmitted/received
Ethernet Port 1-4	Green	Transmission speed is at Gigabit speed (1000Mbps)
	Orange	Transmission speed is at 10/100Mbps
	Blinking	Data being transmitted/received
USB	Green	Connecting to a USB dongle or a hard drive.
Wireless/WPS	Green	Wireless connection established
	Green blinking	Data being transmitted / received
	Orange	WPS configuration is in progress
Phone 1 & 2	Green	Successfully registered and ready to be used.
	Orange	Phone is off-hook, in-use
Internet	Green	IP connected and traffic is passing thru the device.
	Red	IP request failed.
	Off	BiPAC 6300VNP is either in bridged mode or WAN connection not ready.

Rear Panel Connectors



PORT		MEANING
1	**Antenna**	Screw the supplied Wi-Fi antennas onto the antenna connectors on both sides.
2	**Phone (1X-2X)**	Connect your analog phone to this port with a RJ-11 cable.
3	**USB**	Connect an external USB dongle / hard drive for storage, network sharing, etc
4	**Gigabit LAN Ethernet**	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the four LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps /1000Mbps
5	**Gigabit EWAN**	Connect to Fiber/ Cable/ xDSL Modem with a RJ-45 cable
6	**Reset**	After the device is powered on, press it **6 seconds or above**: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)
7	**WPS & Wireless On/Off**	By controlling the pressing time, users can achieve two different effects: **(1) WPS**[*1]**:** Press &hold the button for **less than 6 seconds** to trigger WPS function. **(2) Wireless ON/OFF button:** Press & hold the button for **more than 6 seconds** to On/Off the wireless.
8	**Power**	Connect the supplied Power Adapter to this port.
9	**Power Switch**	Power ON/OFF switch

*** Note: 1. For WPS configuration, please refer to the WPS section in the User Manual.**

Cabling

One of the most common causes of problems is bad cabling. Make sure that all connected devices are turned on. Check the front panel to verify LAN LED status. If you don’t see LAN LEDs on, please check your RJ-45 Ethernet cable(s) again.

Chapter 3: Basic Installation

You can configure the BiPAC 6300VNP through the convenient and user-friendly interface of a web browser. Most popular operating systems such as Linux and Windows 98 / NT /2000 / XP / ME / 7 / Vista include a web browser as a standard application.
PCs must have a properly installed Ethernet interface which connects to the router directly or through an external repeater hub. In addition, PCs must have TCP/IP installed and configured 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 between 192.168.1.1 and 192.168.1.253). The easiest way is to configure the PC is to obtain an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface you are advised to **uninstall** any kind of software firewall on your PCs, as they can cause problems when trying to access the 192.168.1.254 IP address of the router.

Please follow the steps below for installation on your PC's network environment. First of all, check your PC's 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.

NOTE:

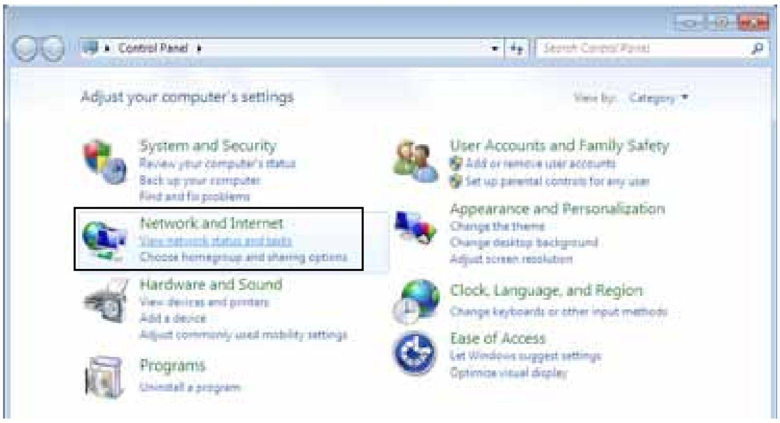
Any TCP/IP capable workstation can be used to communicate with or through the **BiPAC 6300VNP**. To configure other types of workstations, please consult the manufacturer's documentation.

Network Configuration – IPv4

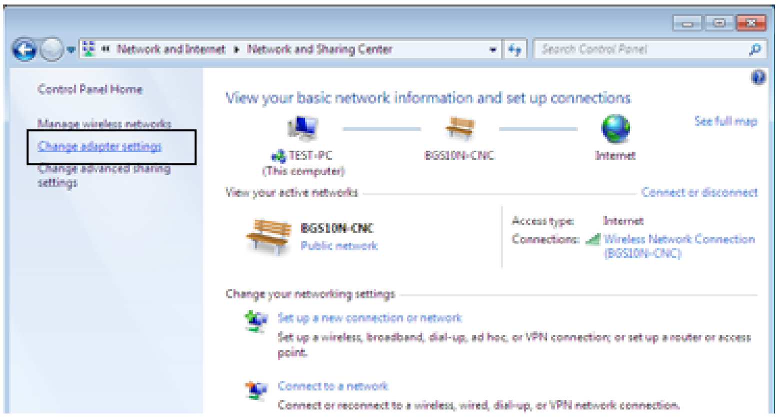
Configuring PC in Windows 7 (IPv4)

1. Go to **Start**. Click on **Control Panel**.

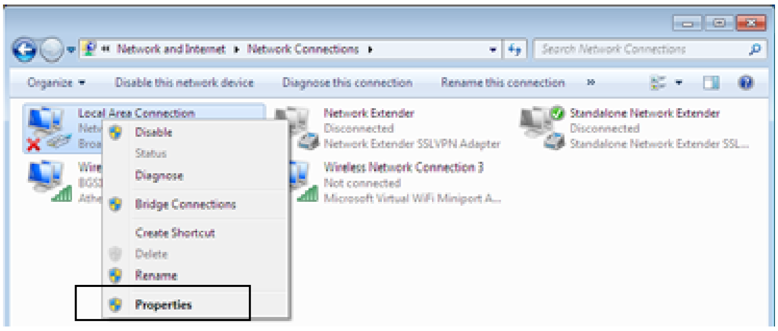
2. Then click on **Network and Internet**.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

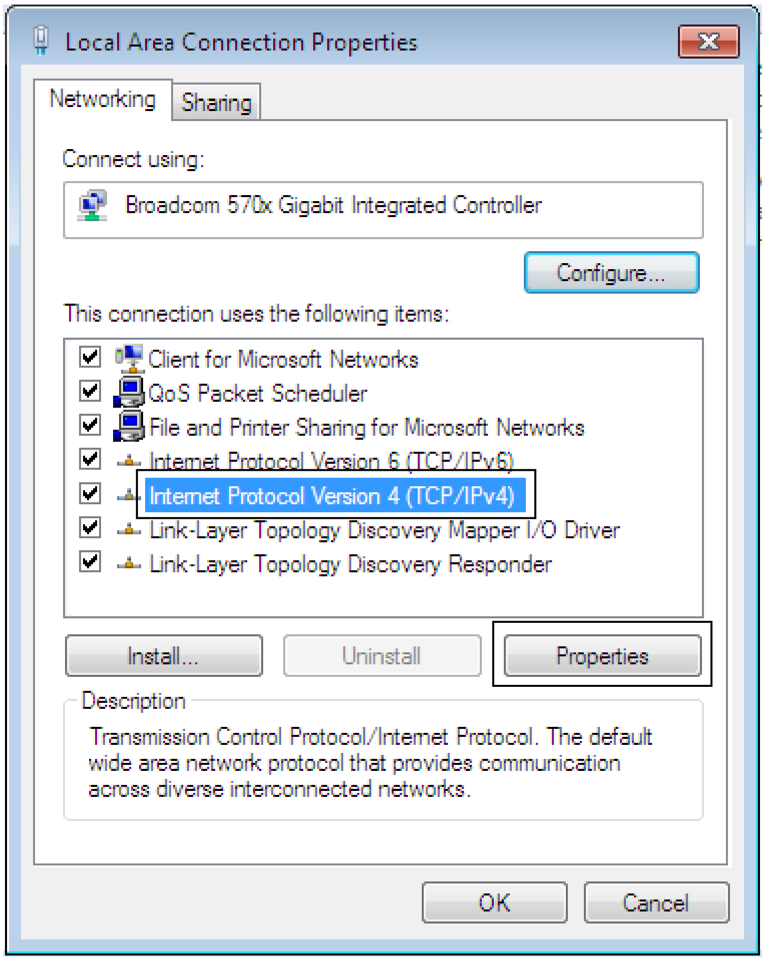
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.


Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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


Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
Local Area Connection
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Network Extender
Disconnected
Network Extender SSLVPN Adapter
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...
Standalone Network Extender
Disconnected
Standalone Network Extender SSL...

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



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

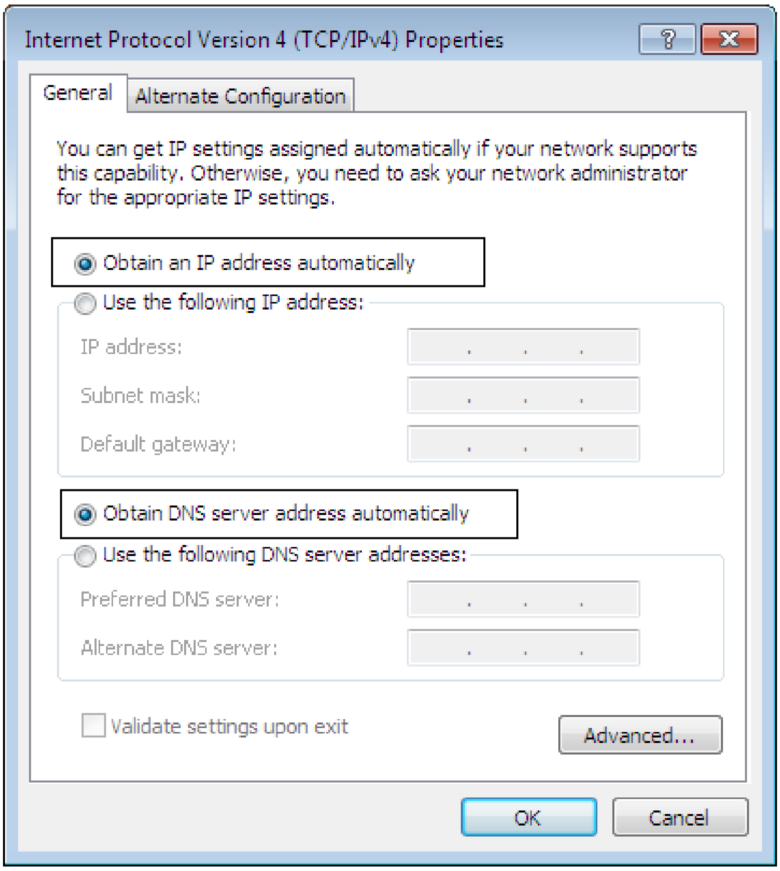
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

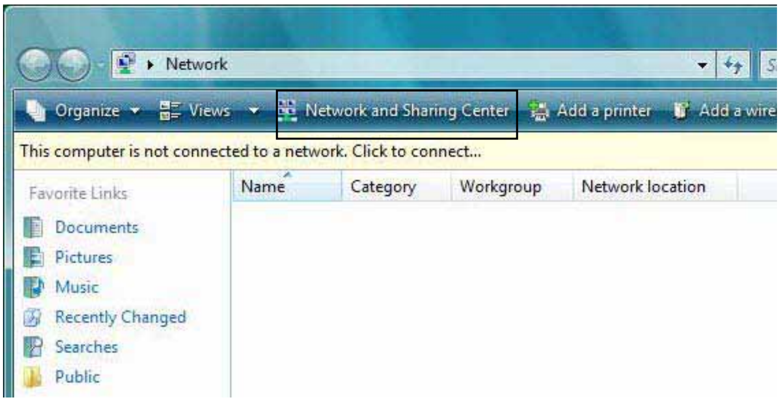
Alternate DNS server: . . .

□ Validate settings upon exit

Configuring PC in Windows Vista (IPv4)

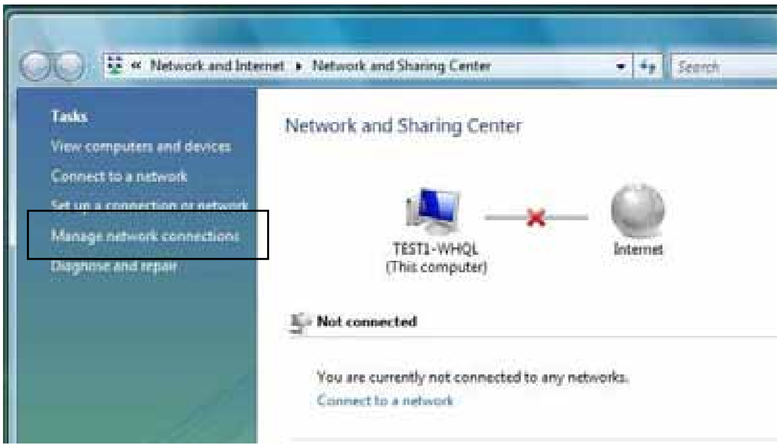
1. Go to **Start**. Click on **Network**.

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



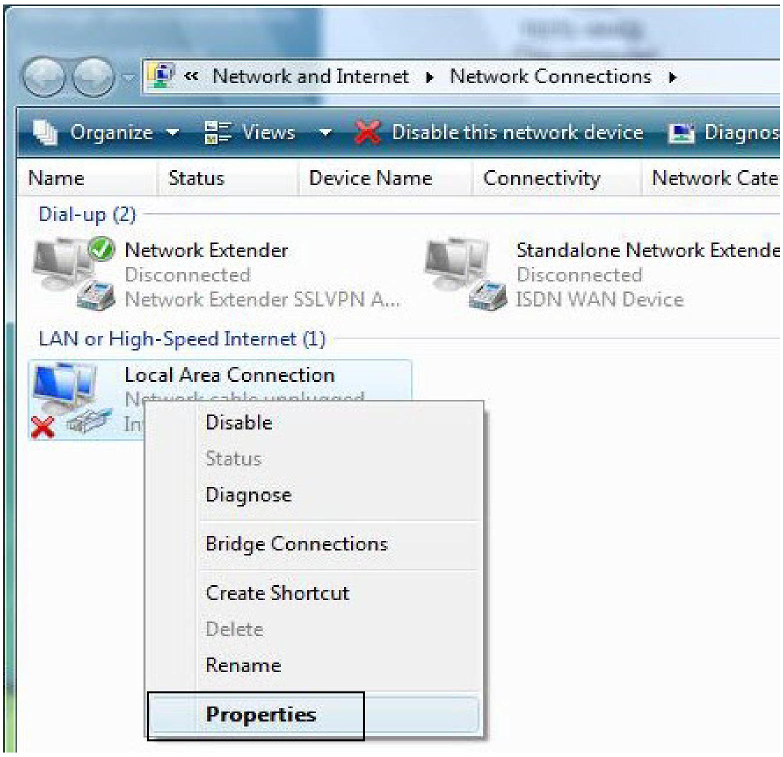
This computer is not connected to a network. Click to connect...

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

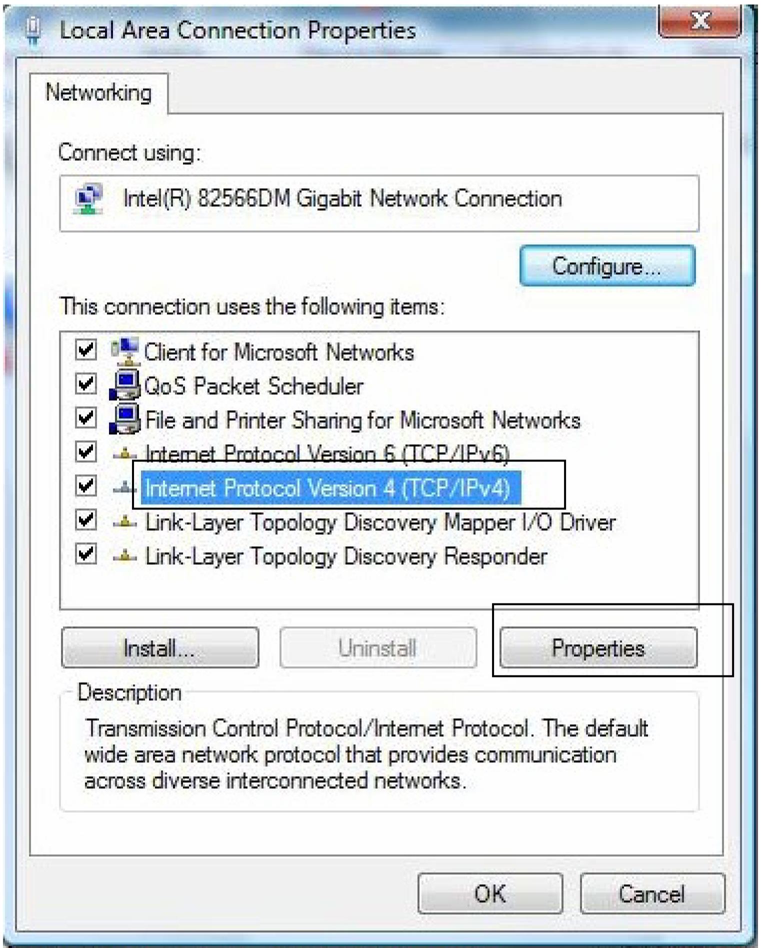


You are currently not connected to any networks.

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**.



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82566DM Gigabit Network Connection

This connection uses the following items:

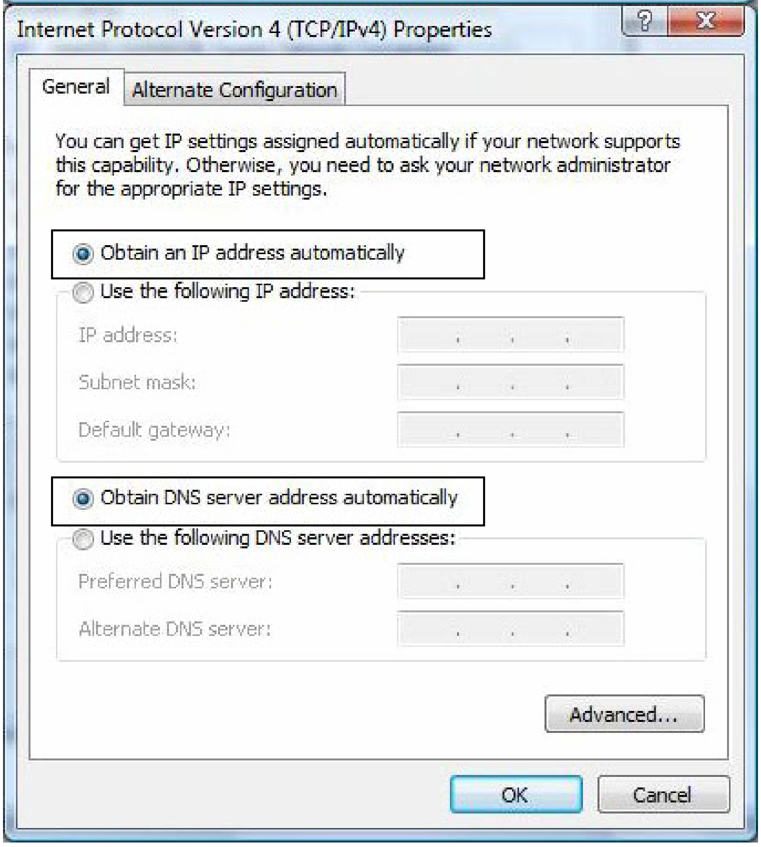
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

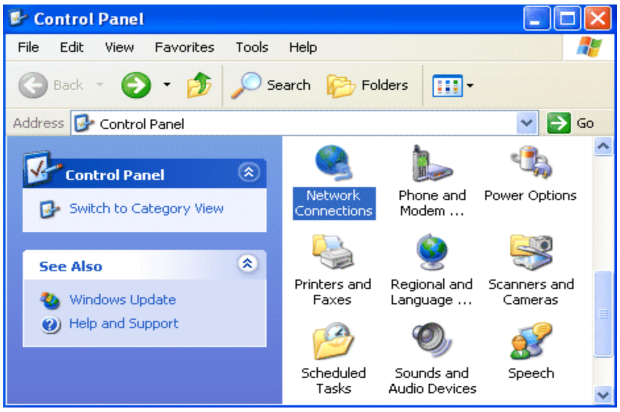
○ Use the following DNS server addresses:

Preferred DNS server: . . .

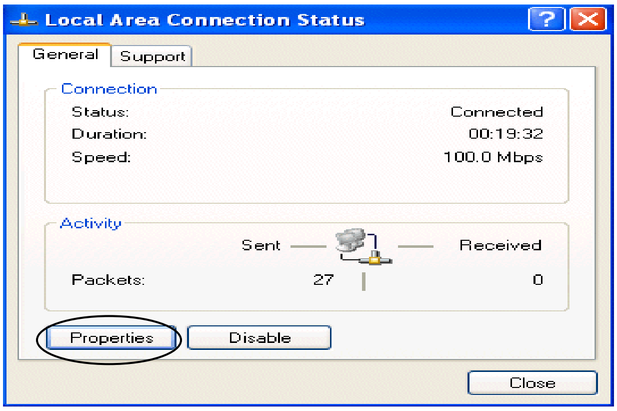
Alternate DNS server: . . .

Configuring PC in Windows XP (IPv4)

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



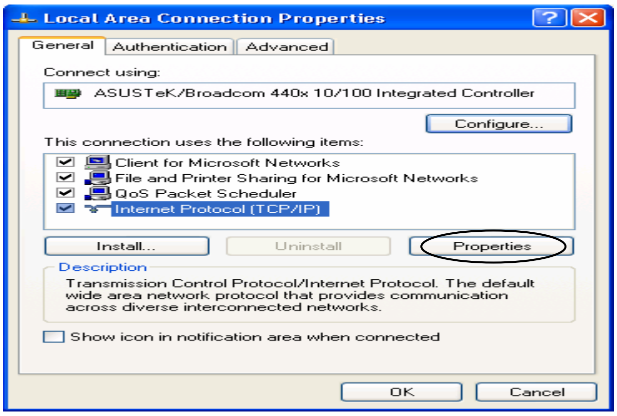
3. In the **Local Area Connection Status** window, click **Properties**.



Connection
Status: Connected
Duration: 00:19:32
Speed: 100.0 Mbps

Activity
Sent — Received
Packets: 27 0

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


Local Area Connection Properties
General Authentication Advanced
Configure...
Install... Uninstall Properties
OK Cancel

Connect using:
ASUSTeK/Broadcom 440x 10/100 Integrated Controller

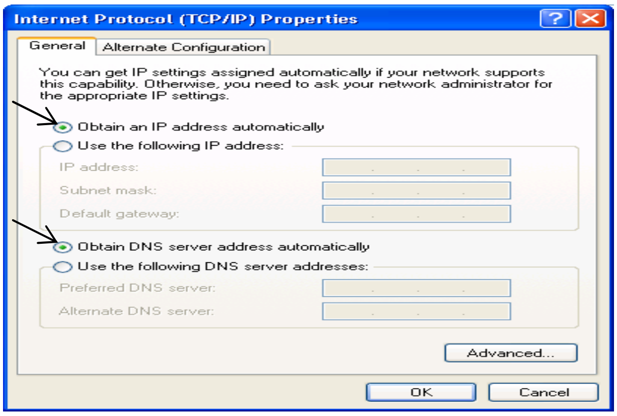
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

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

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


Internet Protocol (TCP/IP) Properties
General Alternate Configuration
Advanced...
OK Cancel

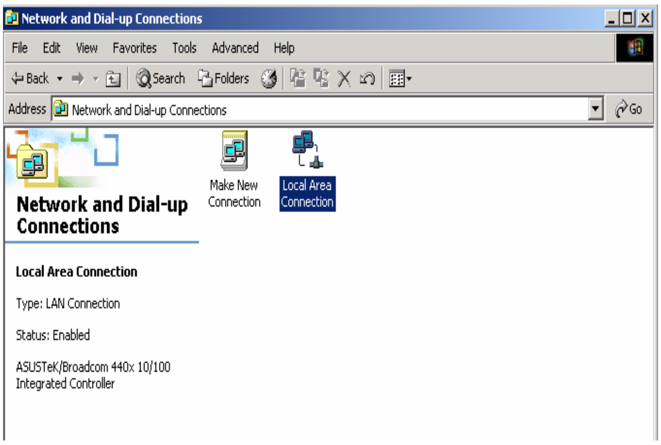
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

Configuring PC in Windows 2000 (IPv4)

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


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
Make New Connection
Local Area Connection

Local Area Connection

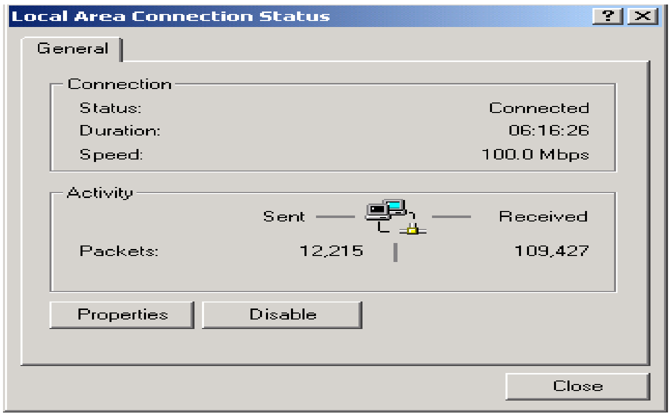
Type: LAN Connection

Status: Enabled

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

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

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



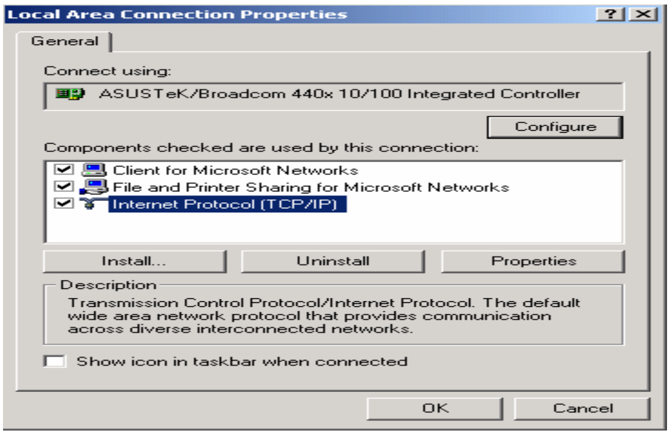
Status: Connected

Duration: 06:16:26

Speed: 100.0 Mbps

Packets: 12,215 (Sent) 109,427 (Received)

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



Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

Components checked are used by this connection:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

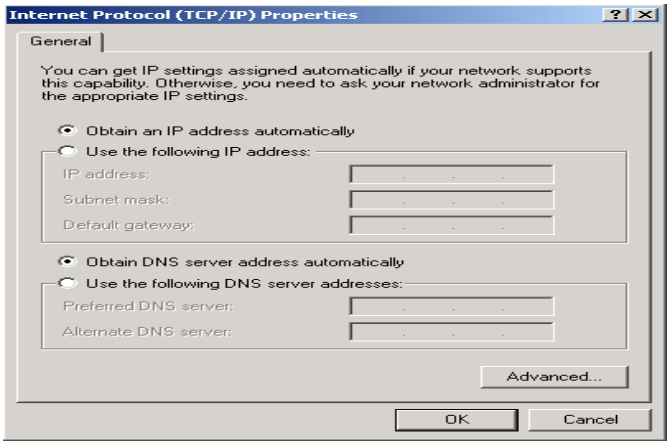
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in taskbar when connected

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

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

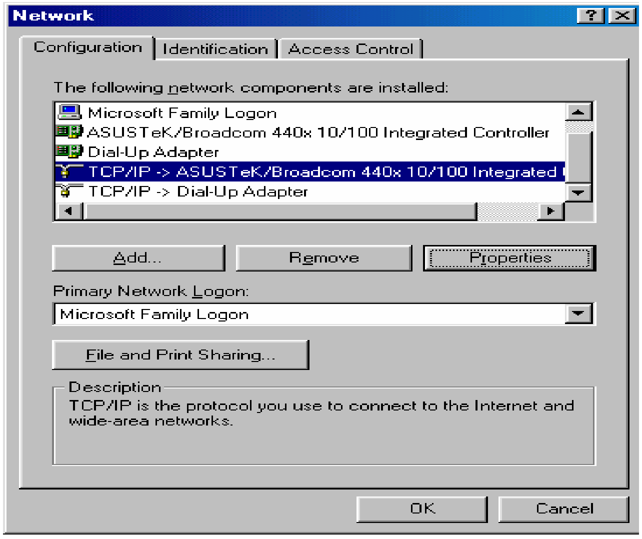
Preferred DNS server:

Alternate DNS server:

Configuring PC in Windows 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.



Network

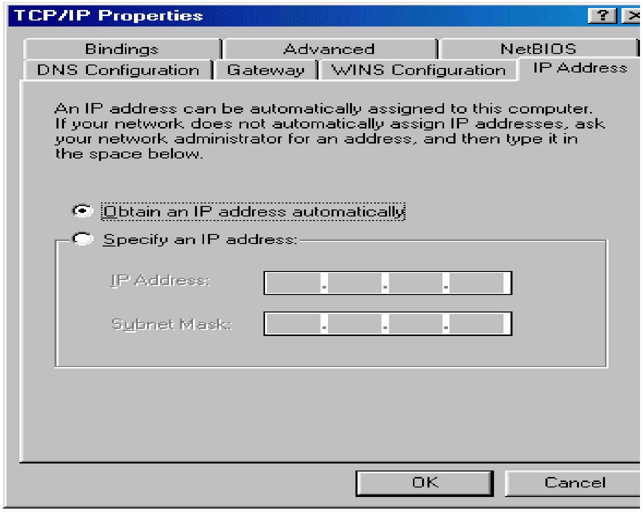
The following network components are installed:

- Microsoft Family Logon
- ASUSTeK/Broadcom 440x 10/100 Integrated Controller
- Dial-Up Adapter
- TCP/IP -> ASUSTeK/Broadcom 440x 10/100 Integrated
- TCP/IP -> Dial-Up Adapter

Primary Network Logon: Microsoft Family Logon

Description: TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

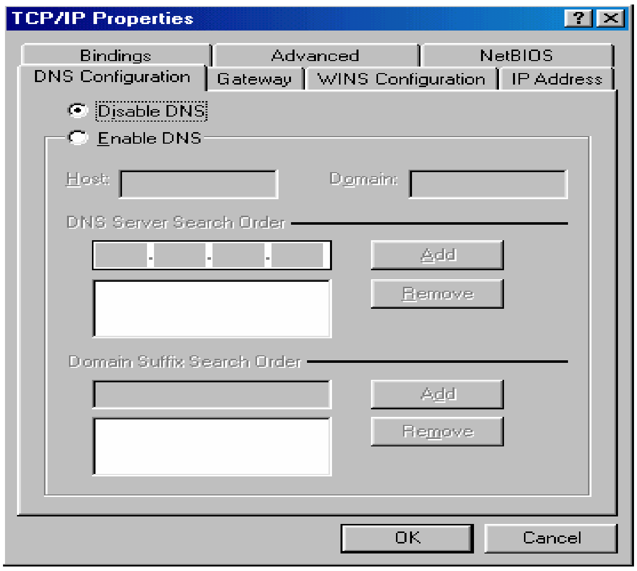
○ Specify an IP address:

IP Address:

Subnet Mask:

4. Then select the **DNS Configuration** tab.

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



TCP/IP Properties

● Disable DNS

○ Enable DNS

Host:

Domain:

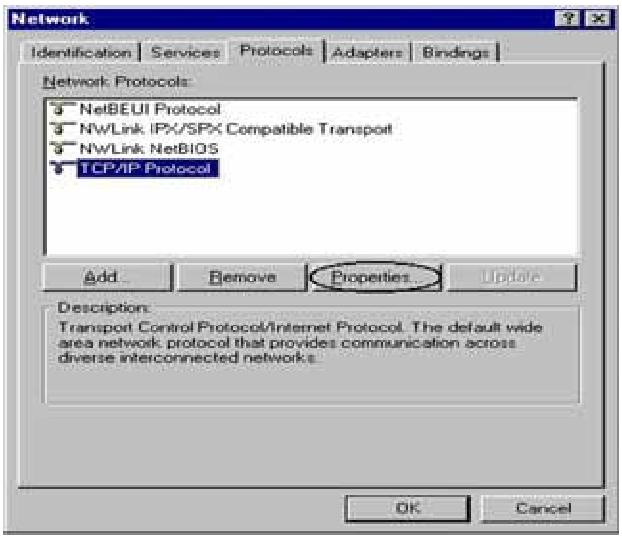
DNS Server Search Order

Domain Suffix Search Order

Configuring PC in Windows NT4.0

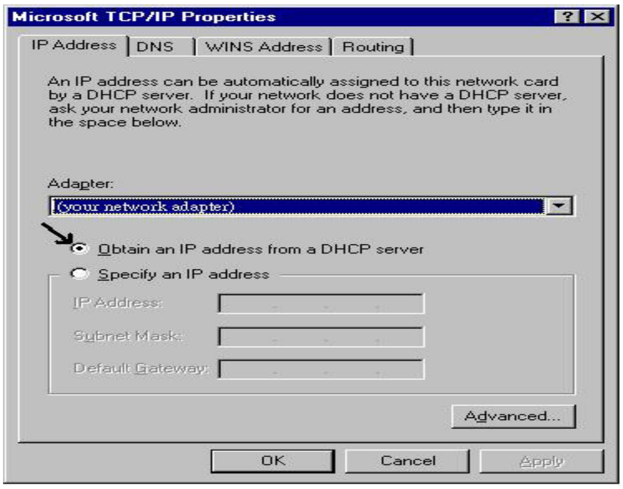
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**.



Transport Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: (your network adapter)

● Obtain an IP address from a DHCP server

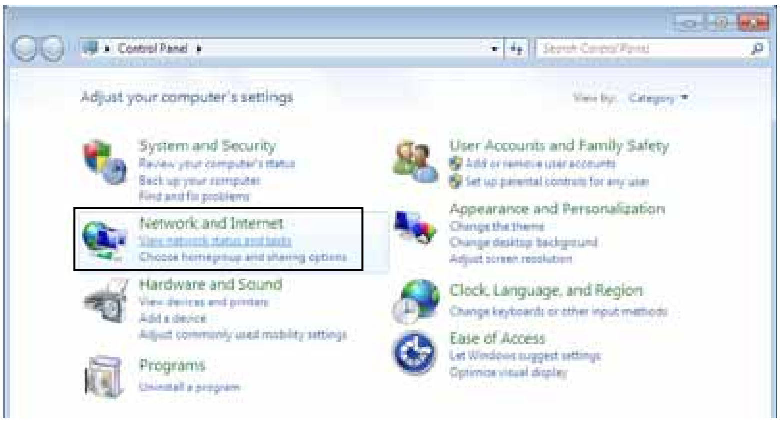
○ Specify an IP address

Network Configuration – IPv6

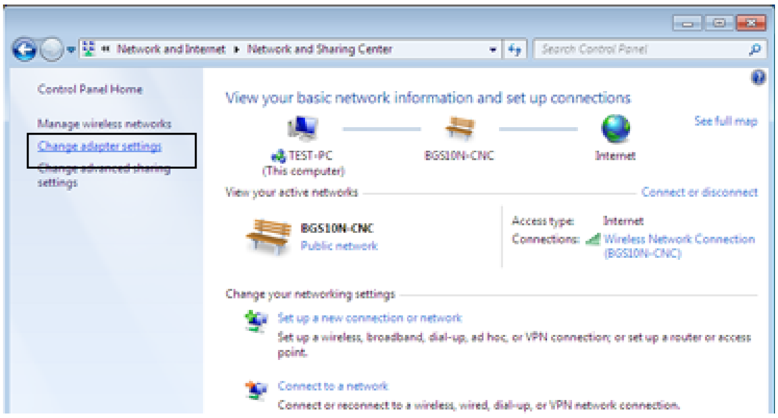
Configuring PC in Windows 7 (IPv6)

1. Go to **Start**. Click on **Control Panel**.

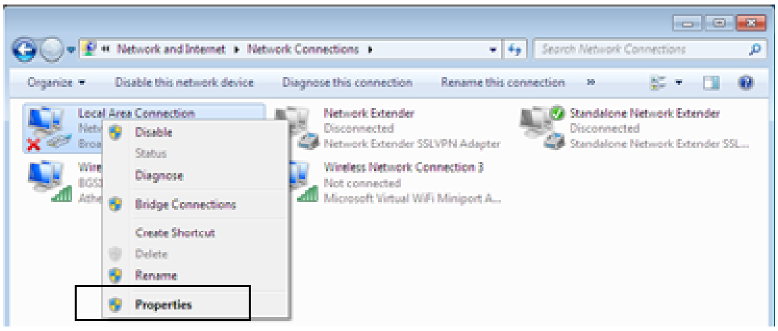
2. Then click on **Network and Internet**.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

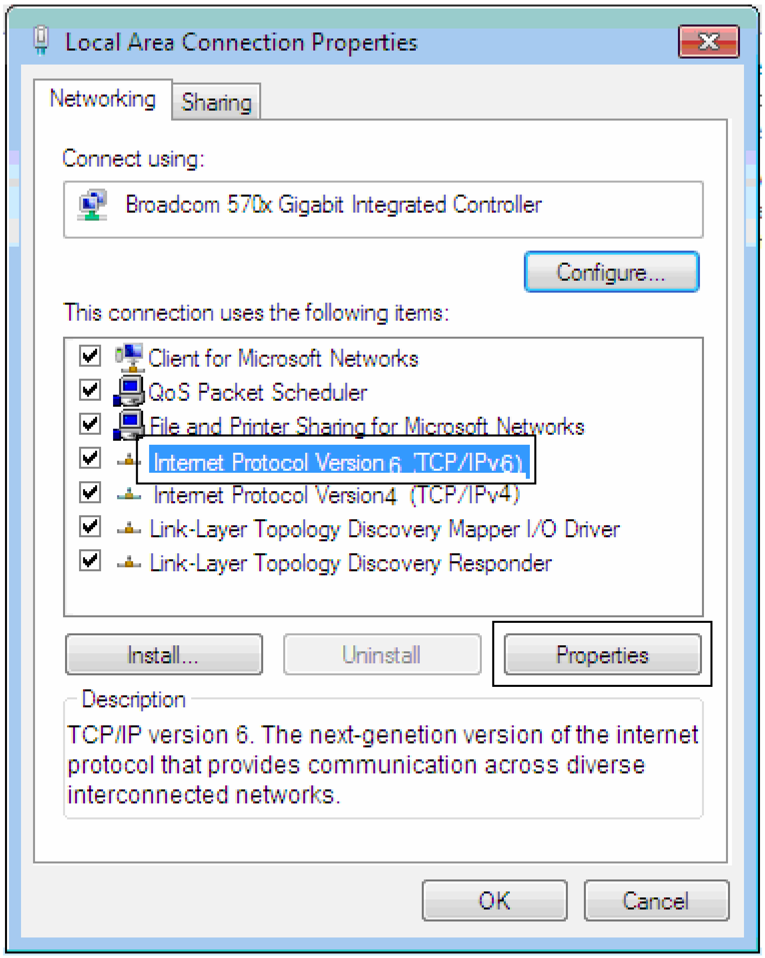
3. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.


Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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


Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Local Area Connection
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Network Extender
Disconnected
Network Extender SSLVPN Adapter
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...
Standalone Network Extender
Disconnected
Standalone Network Extender SSL...

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



Local Area Connection Properties

Networking | Sharing

Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

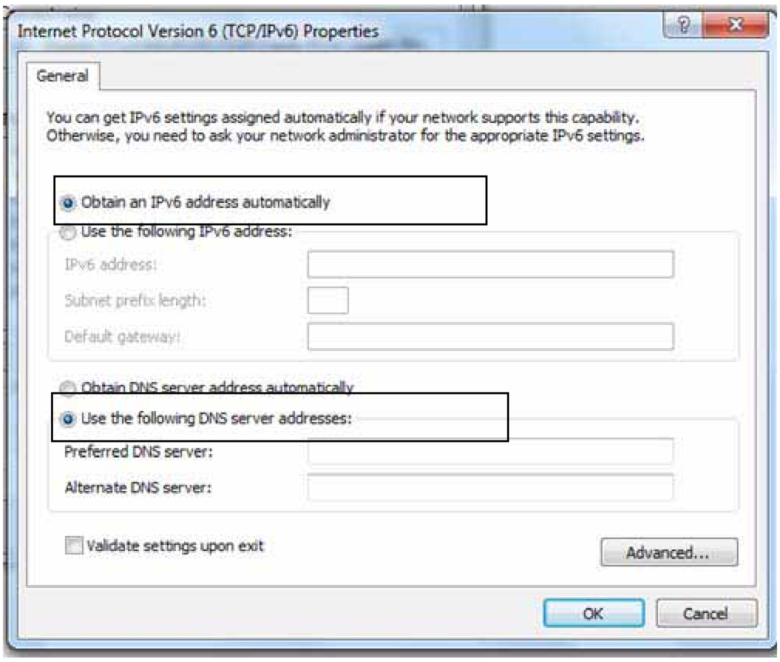
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

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

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



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

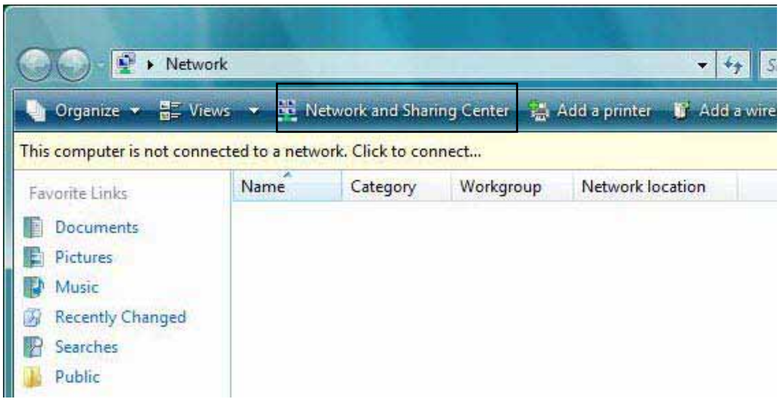
Alternate DNS server:

☐ Validate settings upon exit

Configuring PC in Windows Vista (IPv6)

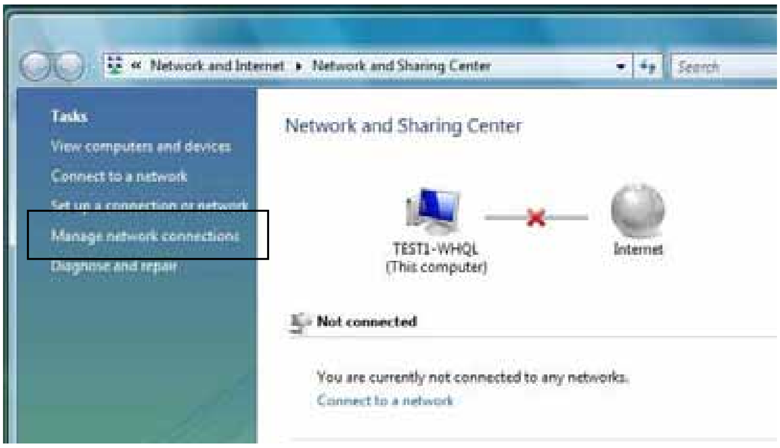
1. Go to **Start**. Click on **Network**.

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



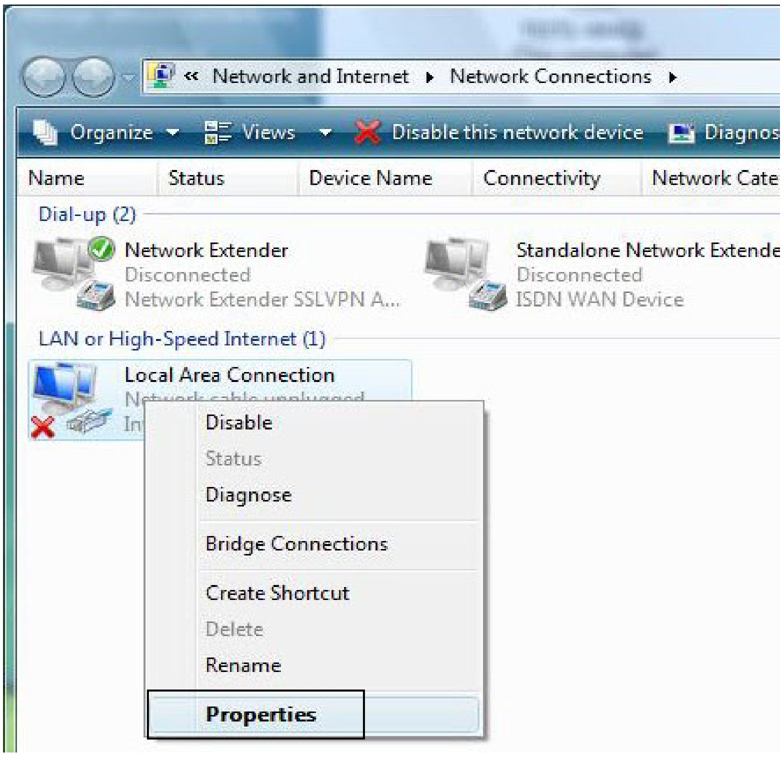
This computer is not connected to a network. Click to connect...

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

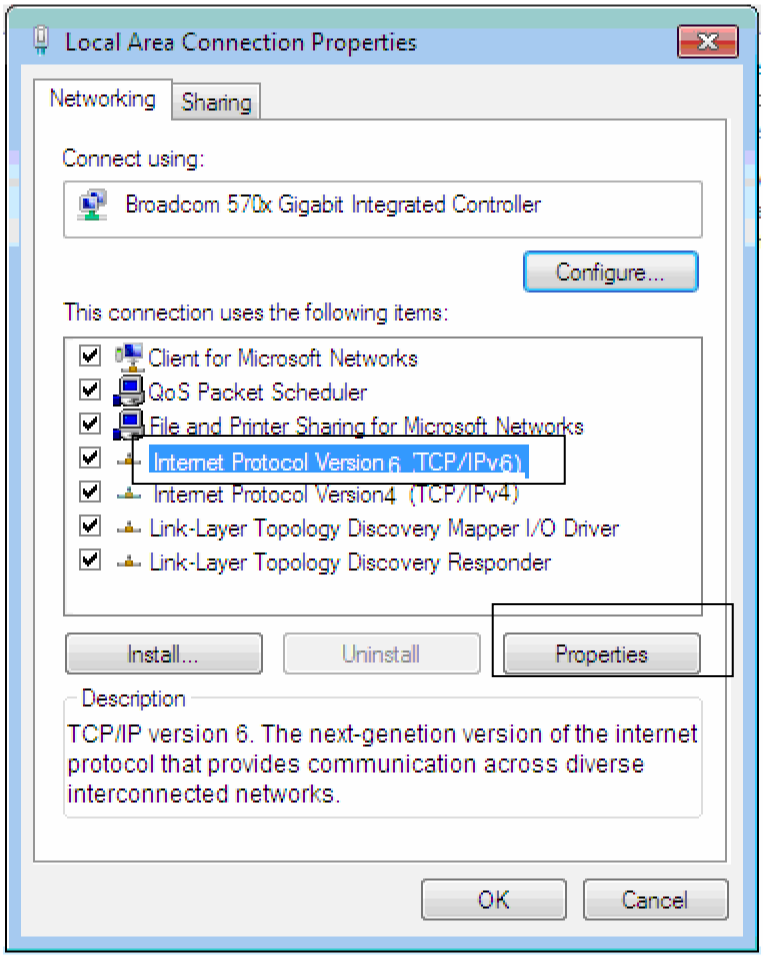


You are currently not connected to any networks.

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



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


Local Area Connection Properties

Connect using:

Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:

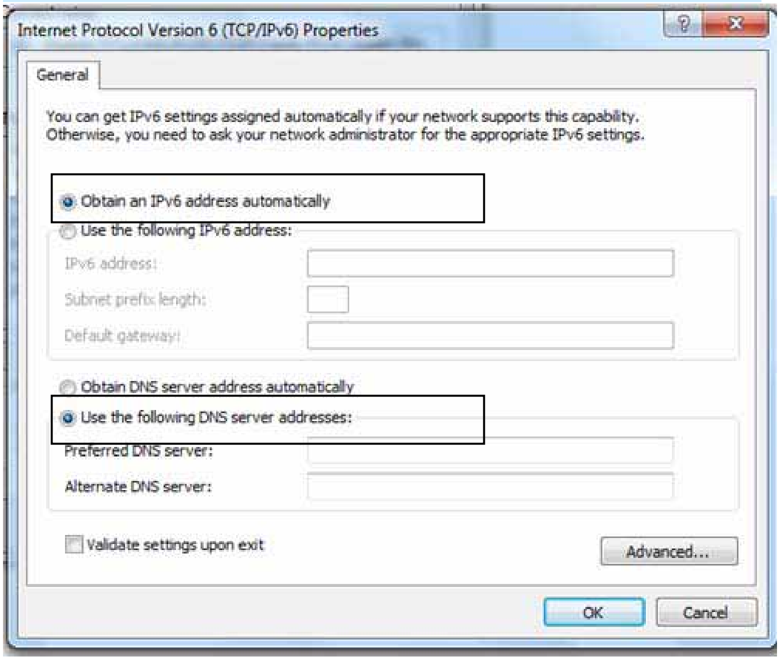
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

6. In the **TCP/IPv6 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.


Internet Protocol Version 6 (TCP/IPv6) Properties

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically
○ Use the following IPv6 address:

IPv6 address:
Subnet prefix length:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

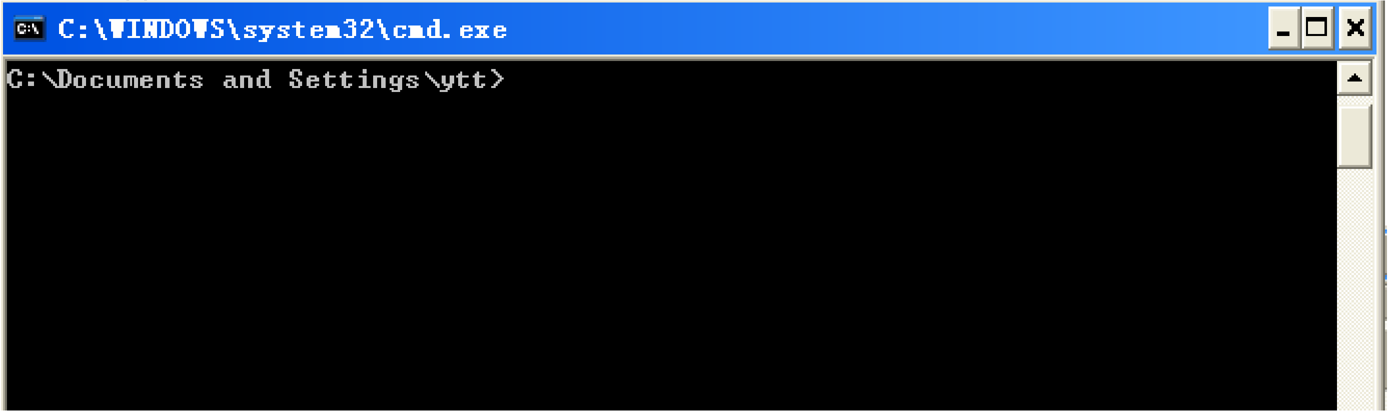
□ Validate settings upon exit

Configuring PC in Windows XP (IPv6)

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

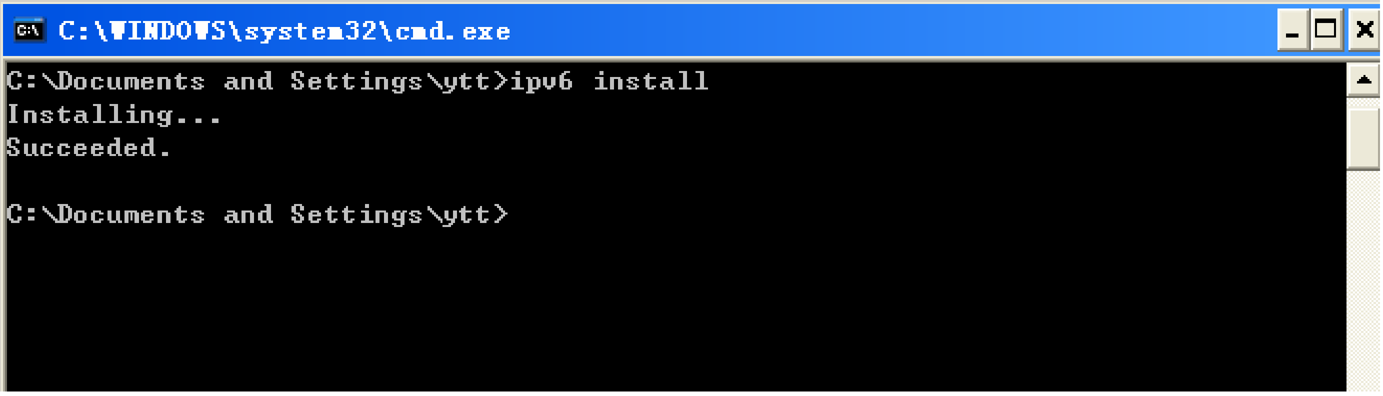
Please follow the steps to install IPv6:

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



```
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



```
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.

C:\Documents and Settings\ytt>
```

Installation of IPv6 is now completed. Please test it to see if it works or not. .

Default Settings

Before configuring the 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.

If you ever forget the username/password to login to the router, you may press the RESET button up to 6 seconds then release it to restore the factory default settings.
Caution: After pressing the RESET button for more than 6 seconds then release it, to be sure you power cycle the device again.

Device LAN IP Settings

- ✔ IP Address: 192.168.1.254
- ✔ Subnet Mask: 255.255.255.0

DHCP Server:

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

Information from Your ISP

Before configuring this device, you have to check with your ISP (Internet Service Provider) what kind of service is provided such as **EWAN** ((Dynamic IP address, Static IP address, PPPoE, Bridge Mode).

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

PPPoE	Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
Dynamic IP Address	DHCP Client (it can be automatically assigned by your ISP when you connect or be set manually).
Static IP Address	IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is fixed IP address).
Bridge Mode	Pure Bridge

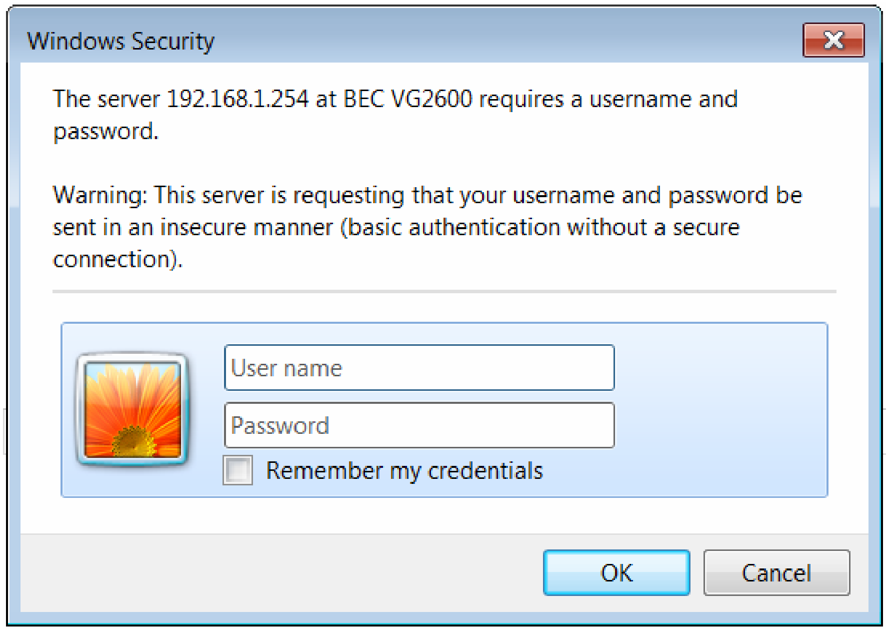
Chapter 4: Device Configuration

Login to your Device

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 appears.

The default username and password is **"admin"** and **"admin"** respectively for the **Administrator.**

NOTE: This username / password may vary by different Internet Service Providers.



Windows Security

The server 192.168.1.254 at BEC VG2600 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

Congratulations! You have successfully logged on to your **BiPAC 6300VNP.**

Once you have logged on to your 6300VNP via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which includes:

Section	Status	Quick Start (Wizard Setup)	Configuration	Logout
Sub-Items	**Device Info**		**Interface Setup** - Internet - LAN - Wireless - Wireless MAC Filter	
	System Log		**Advanced Setup** - Firewall - Routing - NAT - Static DNS - QoS - Interface Grouping - Port Isolation - Time Schedule	
	Statistics		**VoIP** - Basic - Media - Advanced - Speed Dial - Call Features	
	DHCP Table		**Access Management** - User Management - SNMP - Universal Plug & Play (UPnP) - Dynamic DNS - Access Control - Packet Filter - CWMP (TR-069) - Parental Control - SAMBA & FTP Server	
	Disk Status		**Maintenance** - User Management - Time Zone - Firmware & Configuration - System Restart - Diagnostic Tool	
	VoIP Status - VoIP Status - VoIP Call Log			

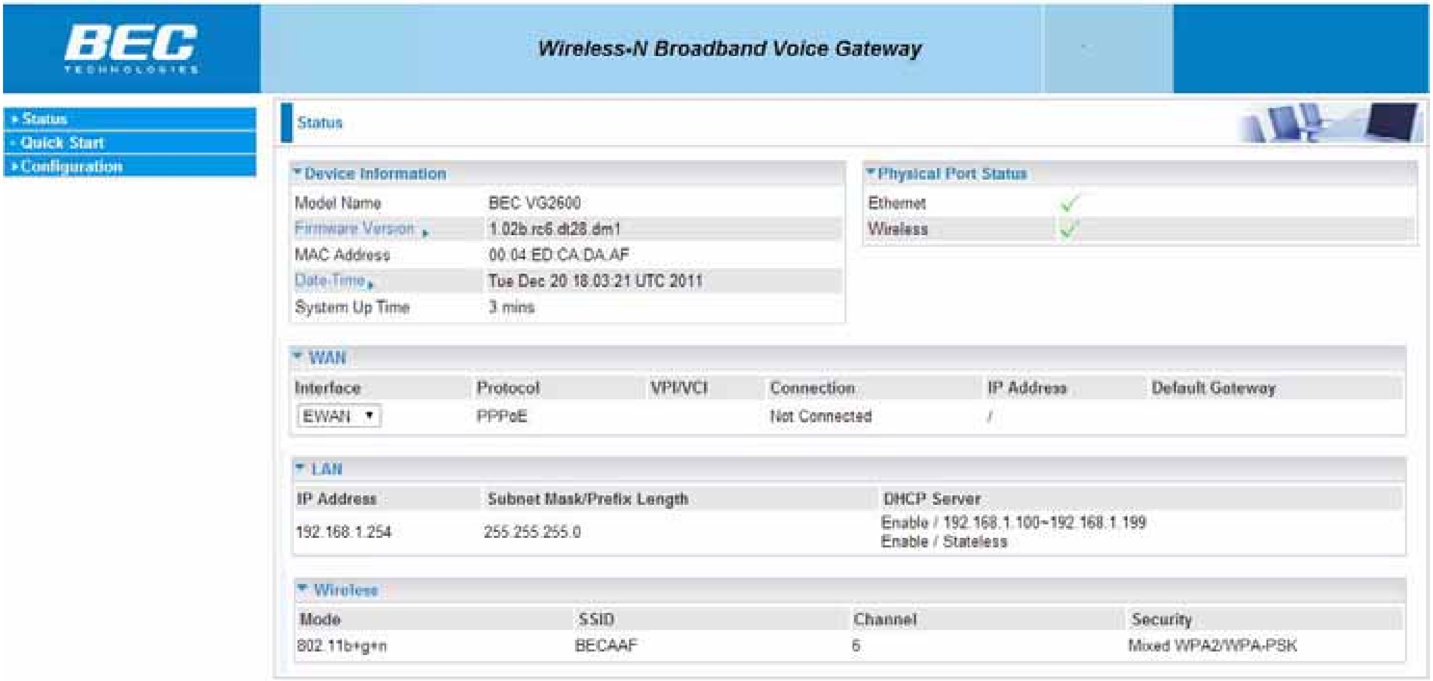
Please see the relevant sections of this manual for detailed instructions on how to configure your **BiPAC 6300VNP** gateway.

Status

In this section, you can check the router working status, including **Device Info**, **System Log**, **Statistics**, **DHCP Table**, **Disk Status**, and **VoIP Status**.

Device Info

It contains basic information of the device.



▾ Device Information

Model Name	BEC VG2600
Firmware Version ▸	1.02b.rc6.dt28.dm1
MAC Address	00:04:ED:CA:DA:AF
Date Time ▸	Tue Dec 20 18:03:21 UTC 2011
System Up Time	3 mins

▾ Physical Port Status

Ethernet	✓
Wireless	✓

▾ WAN

Interface	Protocol	VPI/VCI	Connection	IP Address	Default Gateway
EWAN ▾	PPPoE		Not Connected	/	

▾ LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.199 Enable / Stateless

▾ Wireless

Mode	SSID	Channel	Security
802.11b+g+n	BECAAF	6	Mixed WPA2/WPA-PSK

Device Information

Model Name: Name of the router for identification purpose.

Firmware Version: Software version currently loaded in the router

MAC Address: A unique number that identifies the router

Date Time: Set the router time and date. See the Time Zone section for more information. Click this link to turn to Time Zone configuration.

System Up-Time: This is the uptime since the BiPAC 6300VNP is being rebooted.

Physical Port Status

This displays all availabe and the satus of the LAN / WAN interfaces in the BiPAC 6300VNP.

- ✓ : The corresponding interface is being activated or available.
- ✗ : The corresponding interface is being deactivated.

WAN

Interface: Display current selected WAN connection interface.

Protocol: Display current selected WAN protocols. .

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

Connection: The current WAN connection status.

IP Address: The WAN/public IP address.

Default Gateway: The IP address of the default gateway.

LAN

IP Address: LAN port IPv4 address.

Subnet Mask / Prefix Length: Dispaly current LAN port IP subnet mask and prefix length

DHCP Server: Display DHCPv4 and/or DHCPv6 Server status & IP range

Wireless

Mode: Display the current selected Wireless mode.

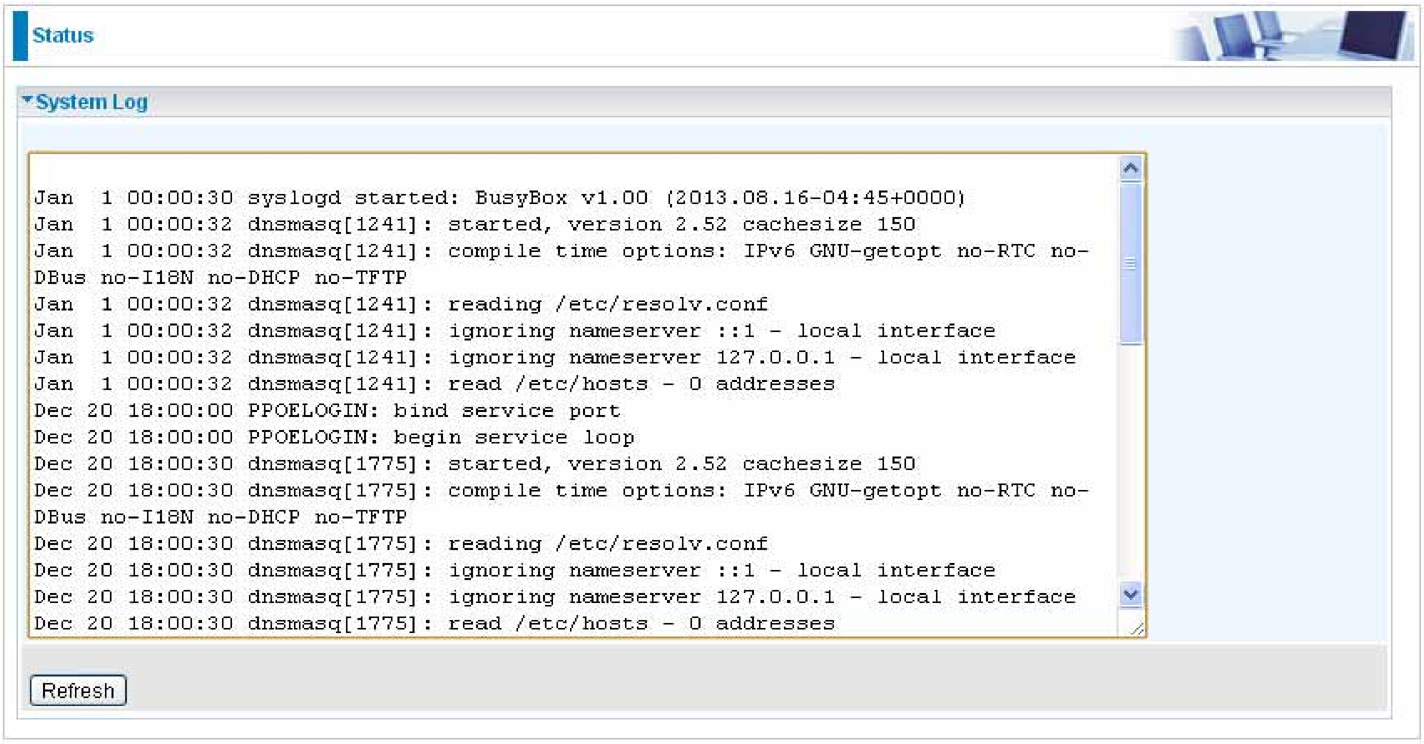
SSID: Display the current Wireless SSID

Channel: Display the current selected wireless channel.

Security: Display the current selected wireless security mode.

System Log

In system log, you can check the operations status and any glitches to the router.

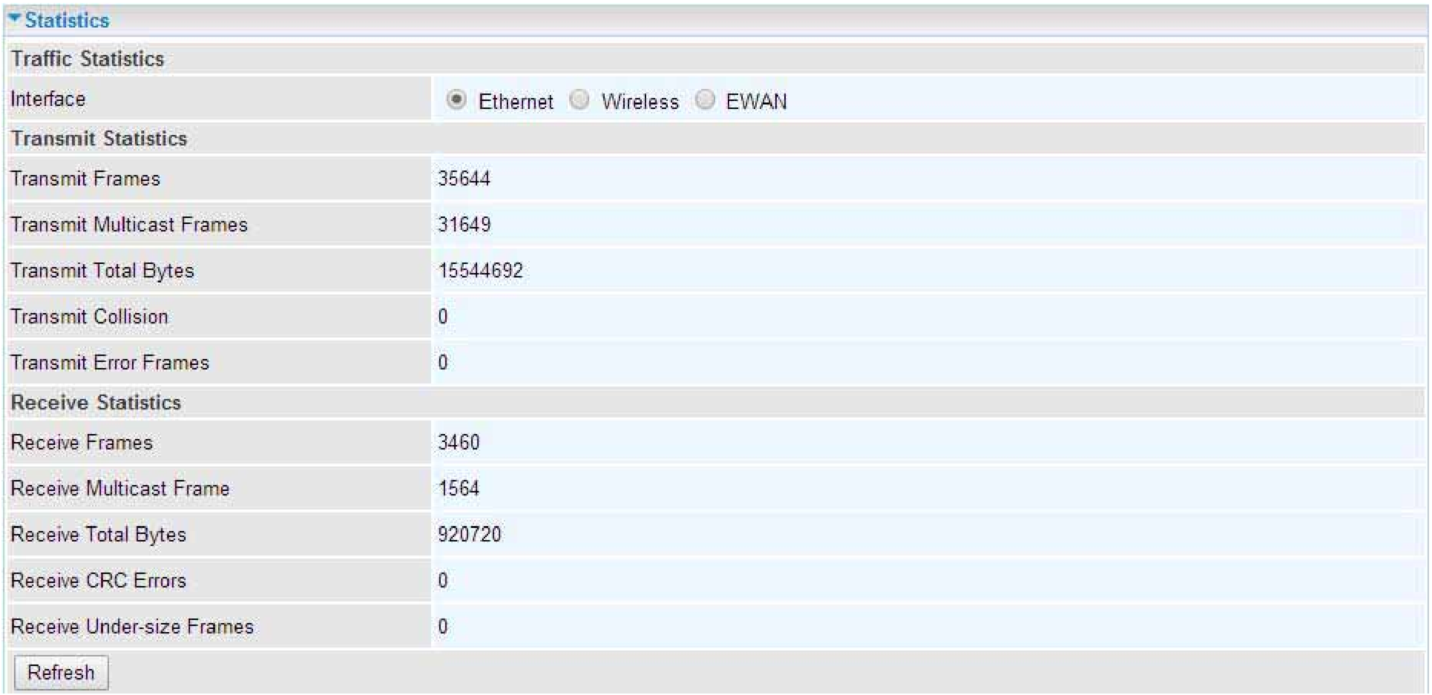


```
Jan  1 00:00:30 syslogd started: BusyBox v1.00 (2013.08.16-04:45+0000)
Jan  1 00:00:32 dnsmasq[1241]: started, version 2.52 cachesize 150
Jan  1 00:00:32 dnsmasq[1241]: compile time options: IPv6 GNU-getopt no-RTC no-
DBus no-I18N no-DHCP no-TFTP
Jan  1 00:00:32 dnsmasq[1241]: reading /etc/resolv.conf
Jan  1 00:00:32 dnsmasq[1241]: ignoring nameserver ::1 - local interface
Jan  1 00:00:32 dnsmasq[1241]: ignoring nameserver 127.0.0.1 - local interface
Jan  1 00:00:32 dnsmasq[1241]: read /etc/hosts - 0 addresses
Dec 20 18:00:00 PPOELOGIN: bind service port
Dec 20 18:00:00 PPOELOGIN: begin service loop
Dec 20 18:00:30 dnsmasq[1775]: started, version 2.52 cachesize 150
Dec 20 18:00:30 dnsmasq[1775]: compile time options: IPv6 GNU-getopt no-RTC no-
DBus no-I18N no-DHCP no-TFTP
Dec 20 18:00:30 dnsmasq[1775]: reading /etc/resolv.conf
Dec 20 18:00:30 dnsmasq[1775]: ignoring nameserver ::1 - local interface
Dec 20 18:00:30 dnsmasq[1775]: ignoring nameserver 127.0.0.1 - local interface
Dec 20 18:00:30 dnsmasq[1775]: read /etc/hosts - 0 addresses
```

Refresh: Press this button to refresh the statistics.

Statistics

❖ Ethernet



▾ Statistics

Traffic Statistics	
Interface	● Ethernet ○ Wireless ○ EWAN
Transmit Statistics	
Transmit Frames	35644
Transmit Multicast Frames	31649
Transmit Total Bytes	15544692
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	3460
Receive Multicast Frame	1564
Receive Total Bytes	920720
Receive CRC Errors	0
Receive Under-size Frames	0

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **Ethernet** port**.**

Transmit Statistics

Transmit Frames: This field displays the number of frames transmitted until the latest second.

Transmit Multicast Frames: This field displays the number of multicast frames transmitted until the latest second.

Transmit Total Bytes: This field displays the number of bytes transmitted until the latest second.

Transmit Collision: This is the number of collisions on this port.

Transmit Error Frames: This field displays the number of error packets on this port.

Recieve Statistics

Receive Frames: This field displays the number of frames received until the latest second.

Receive Multicast Frames: This field displays the number of multicast frames received until the latest second.

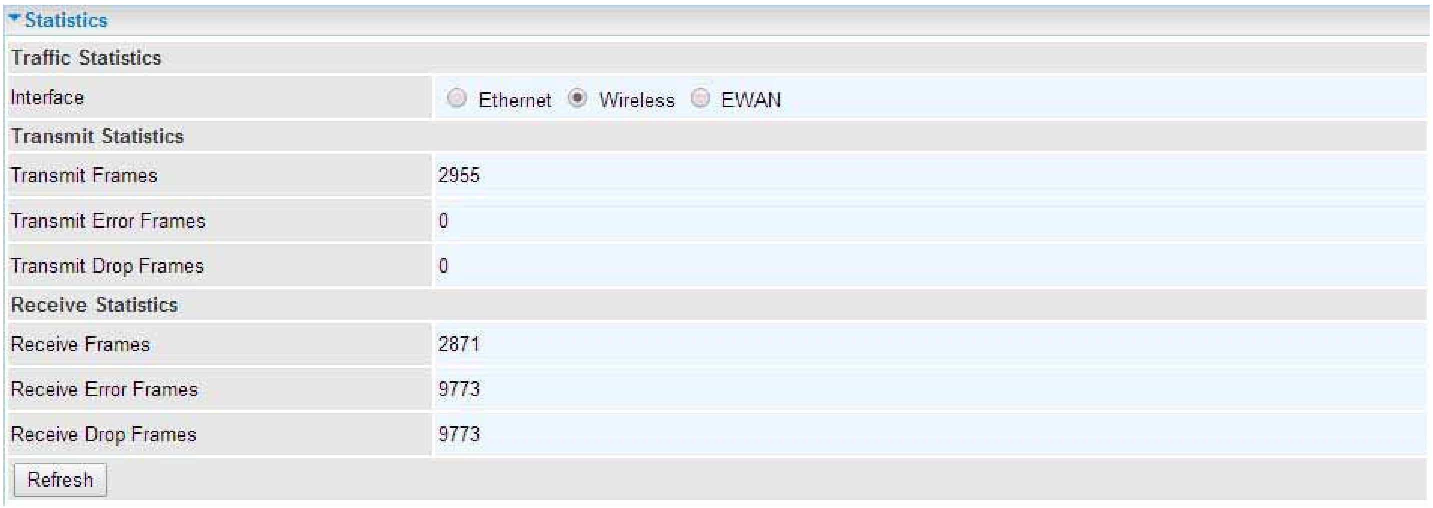
Receive Total Bytes: This field displays the number of bytes received until the latest second.

Receive CRC Errors: This field displays the number of error packets on this port.

Receive Under-size Frames: This field displays the number of under-size frames received until the latest second.

Refresh: Press this button to refresh the statistics.

❖ Wireless



▾Statistics

Traffic Statistics	
Interface	○ Ethernet ● Wireless ○ EWAN
Transmit Statistics	
Transmit Frames	2955
Transmit Error Frames	0
Transmit Drop Frames	0
Receive Statistics	
Receive Frames	2871
Receive Error Frames	9773
Receive Drop Frames	9773

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **Wireless.**

Transmit Statistics

Transmit Frames: This field displays the number of frames transmitted until the latest second.

Transmit Error Frames: This field displays the number of error frames transmitted until the latest second.

Transmit Drop Frames: This field displays the number of drop frames transmitted until the latest second.

Recieve Statistics

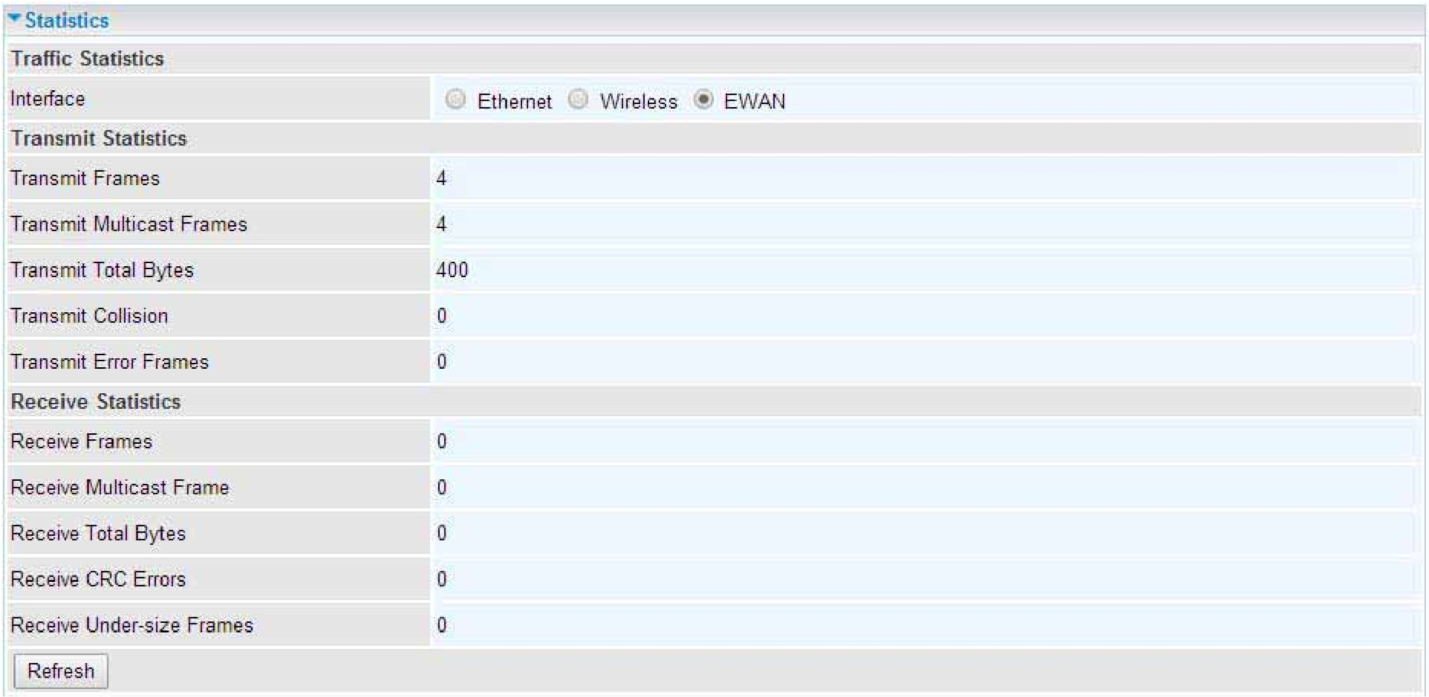
Receive Frames: This field displays the number of frames received until the latest second.

Receive Error Frames: This field displays the number of error frames received until the latest second.

Receive Drop Frames: This field displays the number of drop frames received until the latest second.

Refresh: Press this button to refresh the statistics.

❖ EWAN



▾Statistics

Traffic Statistics	
Interface	○ Ethernet ○ Wireless ● EWAN
Transmit Statistics	
Transmit Frames	4
Transmit Multicast Frames	4
Transmit Total Bytes	400
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	0
Receive Multicast Frame	0
Receive Total Bytes	0
Receive CRC Errors	0
Receive Under-size Frames	0

Interface: List all available network interfaces in the router. You are currently checking on the physical status of the **EWAN** port**.**

Transmit Statistics

Transmit Frames: This field displays the total number of frames transmitted until the latest second.

Transmit Multicast Frames: This field displays the total number of multicast frames transmitted till the latest second.

Transmit Total Bytes: This field displays the total number of bytes transmitted until the latest second.

Transmit Collision: This is the number of collisions on this port.

Transmit Error Frames: This field displays the number of error packets on this port.

Recieve Statistics

Receive Frames: This field displays the number of frames received until the latest second.

Receive Multicast Frames: This field displays the number of multicast frames received until the latest second.

Receive Total Bytes: This field displays the number of bytes received until the latest second.

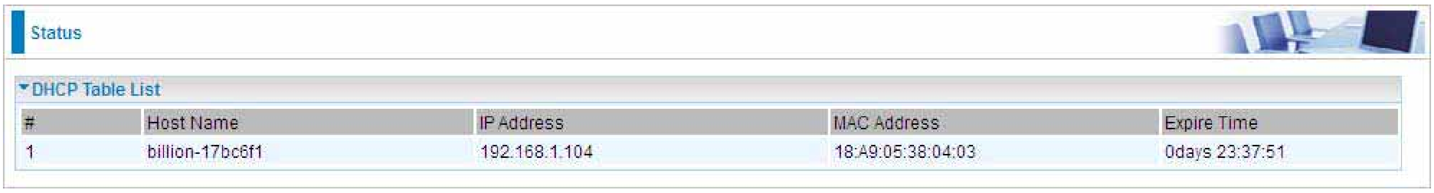
Receive CRC Errors: This field displays the number of error packets on this port.

Receive Under-size Frames: This field displays the number of under-size frames received until the latest second.

Refresh: Press this button to refresh the statistics.

DHCP Table

DHCP table displays the devices connected to the router with clear information.



Status

DHCP Table List

#	Host Name	IP Address	MAC Address	Expire Time
1	billion-17bc6f1	192.168.1.104	18:A9:05:38:04:03	0days 23:37:51

#: The index identifying the connected devices.

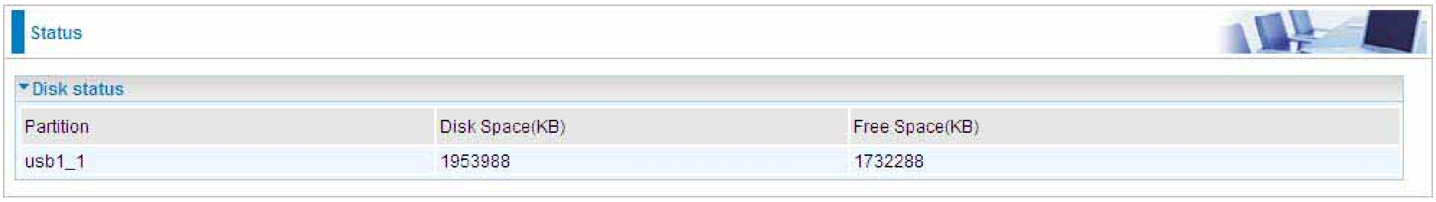
Host Name: Show the hostname of the PC.

IP Address: The IP allocated to the device.

MAC Address: The MAC of the connected device.

Expire Time: The total remaining interval since the IP assignment to the PC.

Disk Status



Status

Disk status

Partition	Disk Space(KB)	Free Space(KB)
usb1_1	1953988	1732288

Partition: Display the USB storage partition.

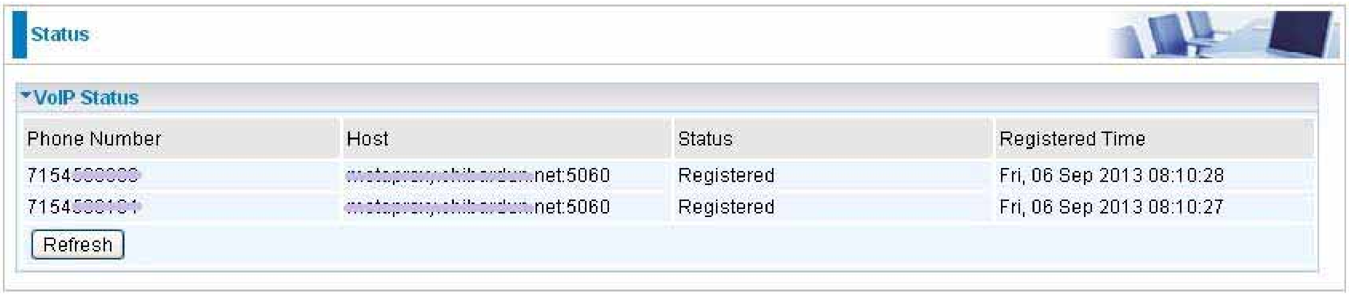
Disk Space (KB): Display the total storage space of the NAS in Kbytes unit.

Free Space (KB): Display the available space in Kbytes unit.

VoIP Status

VoIP Status

VoIP status gives you a directive picture on the registered VoIP accounts.



Status

VoIP Status

Phone Number	Host	Status	Registered Time
7154[redacted]	[redacted]net:5060	Registered	Fri, 06 Sep 2013 08:10:28
7154[redacted]	[redacted]net:5060	Registered	Fri, 06 Sep 2013 08:10:27

Phone Number: The number you use to register in the Basic page of VoIP.

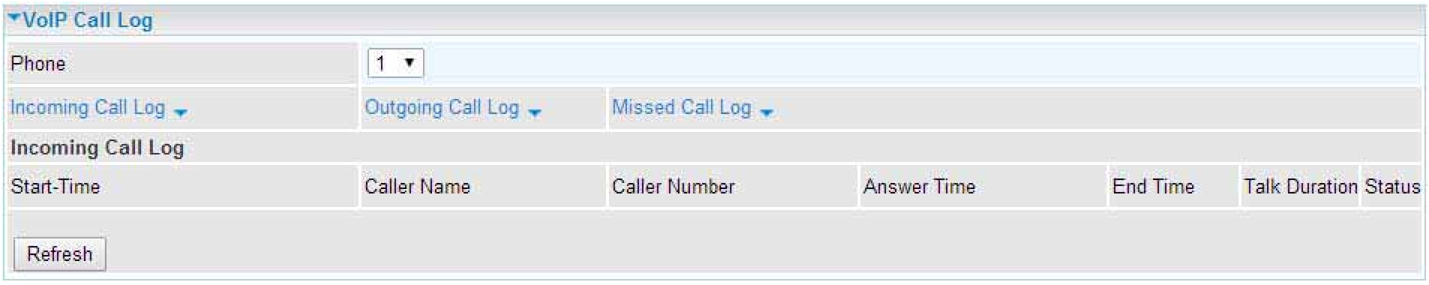
Host: Show the IP address and port number of SIP Registrar.

Status: The status of the registered SIP account.

Registered Time: The duration the account has been successfully registered to the SIP registrar.

VoIP Call Log

VoIP call history records all inbound, outbound, and any miss call of your Phone_1 and/or Phone 2.



VoIP Call Log

Phone	1 ▾

Incoming Call Log

Start-Time	Caller Name	Caller Number	Answer Time	End Time	Talk Duration	Status

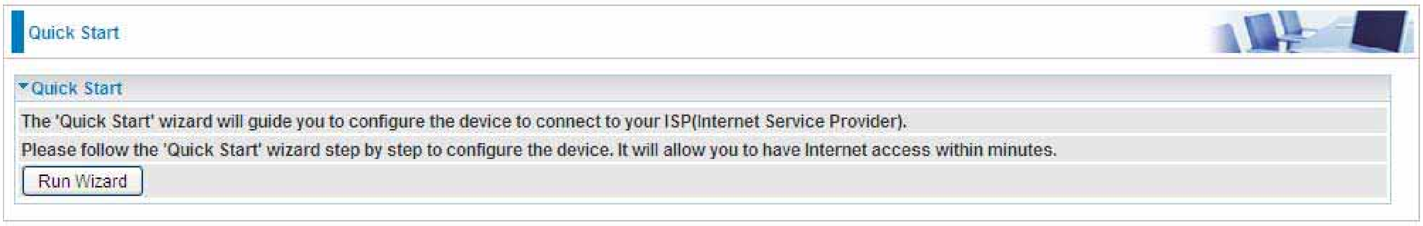
Phone: The phone you registered in the VoIP Basic page.

Call Log: Select a history log you wish to view.

- **Start Time:** The start time of the call.
- **Caller Name:** Display incoming caller's name
- **Caller Number:** Display incoming caller's number
- **Answer Time:** The response time to the call
- **End Time:** The end time of the call.
- **Talk Duration:** The length of the call was made.
- **Status:** Call status if call is picked or busy

Quick Start

This is a useful and easy utility to help you to setup the router quickly and to connect to your ISP (Internet Service Provider) with only a few steps. It will guide you step by step to setup time zone and WAN settings of your device. The Quick Start Wizard is a helpful guide for the first-time users to the device.

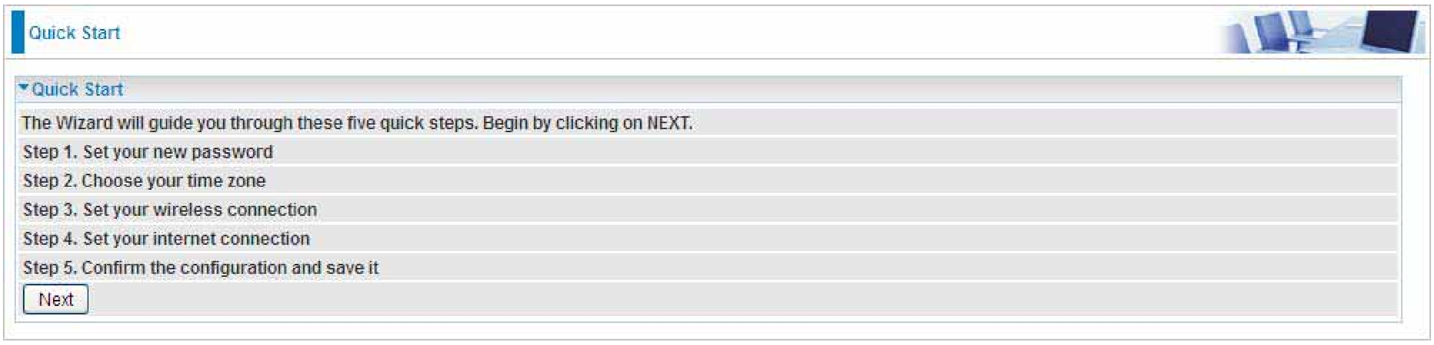

Quick Start

▾Quick Start

The 'Quick Start' wizard will guide you to configure the device to connect to your ISP(Internet Service Provider).

Please follow the 'Quick Start' wizard step by step to configure the device. It will allow you to have Internet access within minutes.

For detailed instructions on configuring WAN settings, see refer to the **Interface Setup** section.


Quick Start

▾Quick Start

The Wizard will guide you through these five quick steps. Begin by clicking on NEXT.

Step 1. Set your new password

Step 2. Choose your time zone

Step 3. Set your wireless connection

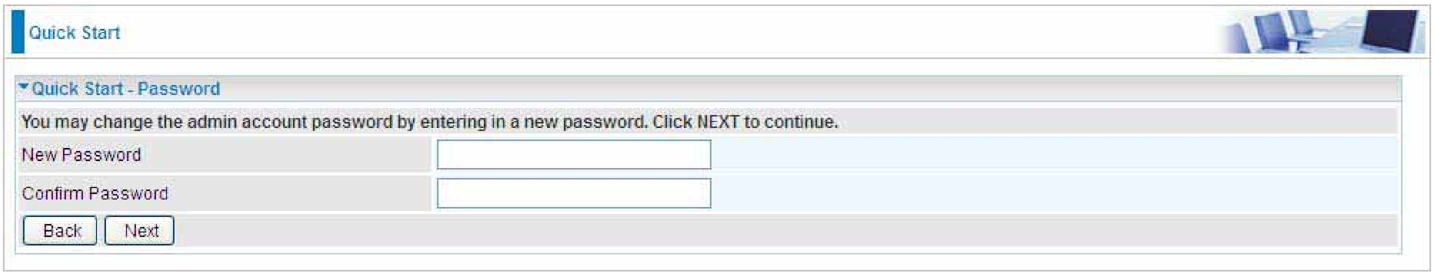
Step 4. Set your internet connection

Step 5. Confirm the configuration and save it

Click **NEXT** to move on to Step 1.

Step 1 – Password

Set new password of the “admin” account to access for router management. The default is “admin”. Once changed, please use this new password next time when accessing to the router. Click **NEXT** to continue.


Quick Start

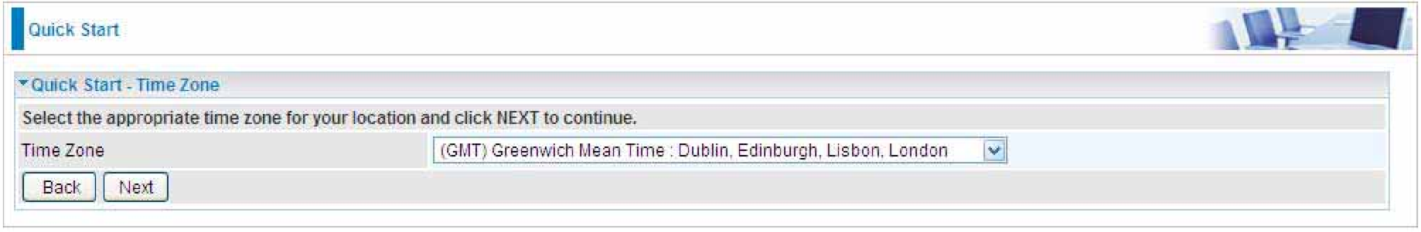
▾Quick Start - Password

You may change the admin account password by entering in a new password. Click NEXT to continue.

New Password	
Confirm Password	

Step 2 – Time Zone

Choose your time zone. Click **NEXT** to continue.


Quick Start

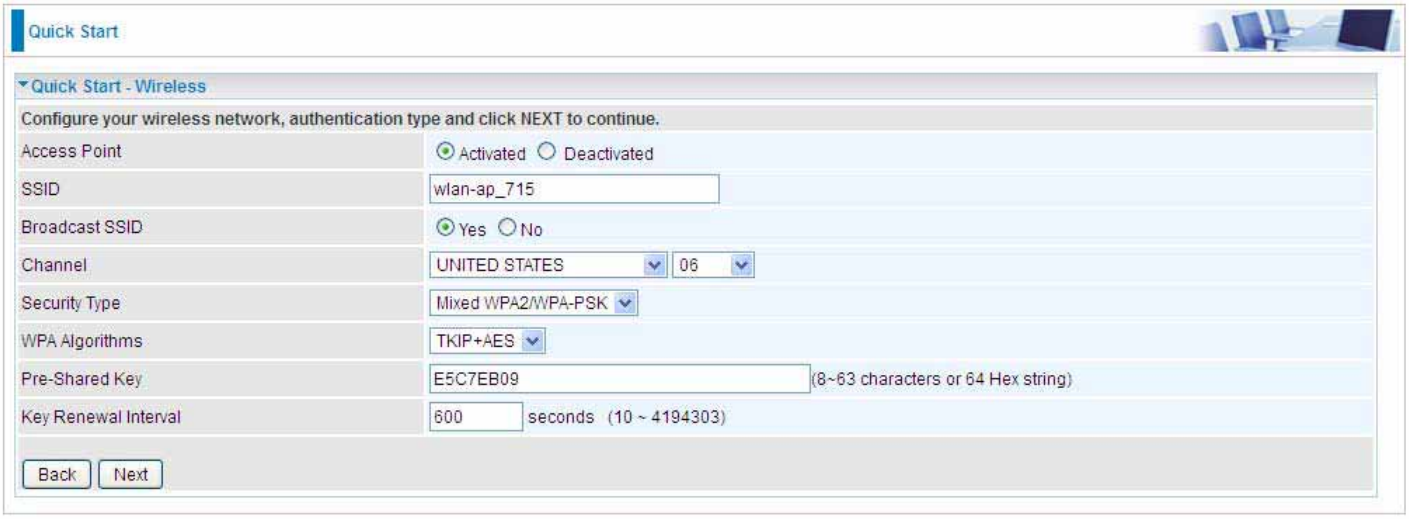
▾Quick Start - Time Zone

Select the appropriate time zone for your location and click NEXT to continue.

Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Step 3 – Wireless

Set up your wireless connection if you want to connect to the Internet wirelessly on your PCs. Click **NEXT** to continue.



▾Quick Start - Wireless

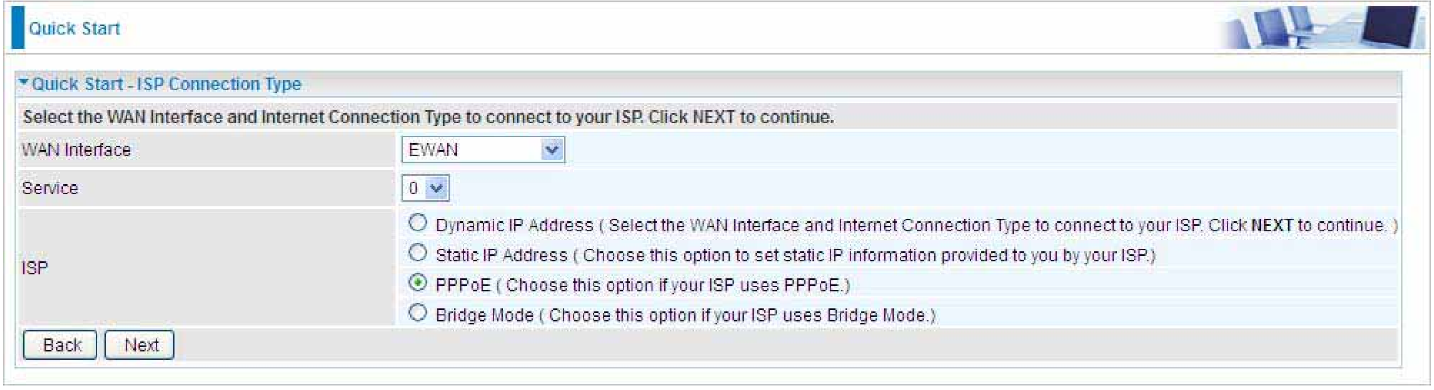
Configure your wireless network, authentication type and click NEXT to continue.

Access Point	● Activated ○ Deactivated
SSID	wlan-ap_715
Broadcast SSID	● Yes ○ No
Channel	UNITED STATES 06
Security Type	Mixed WPA2/WPA-PSK
WPA Algorithms	TKIP+AES
Pre-Shared Key	E5C7EB09 (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)

Step 4 – ISP Connection Type

Set up your Internet connection.

4.1 Select an appropriate WAN connection protocol then click **NEXT** to continue.

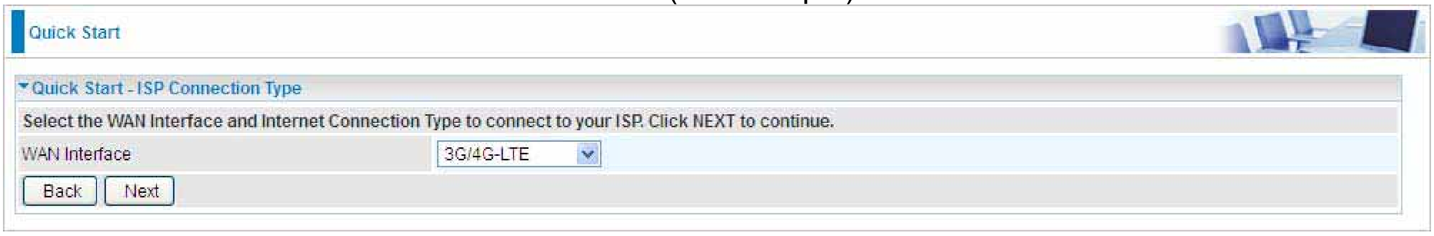


▾Quick Start - ISP Connection Type

Select the WAN Interface and Internet Connection Type to connect to your ISP. Click NEXT to continue.

WAN Interface	EWAN
Service	0
ISP	○ Dynamic IP Address (Select the WAN Interface and Internet Connection Type to connect to your ISP. Click NEXT to continue.) ○ Static IP Address (Choose this option to set static IP information provided to you by your ISP.) ● PPPoE (Choose this option if your ISP uses PPPoE.) ○ Bridge Mode (Choose this option if your ISP uses Bridge Mode.)

4.2 If selected **3G/4G-LTE or 3G/4G-LTE USB** (for example).

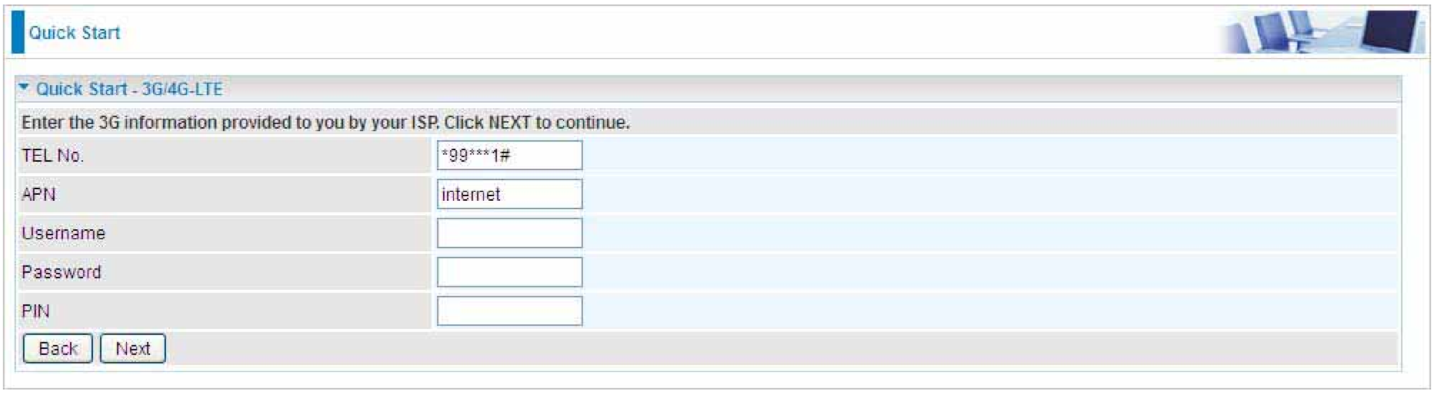


▾Quick Start - ISP Connection Type

Select the WAN Interface and Internet Connection Type to connect to your ISP. Click NEXT to continue.

WAN Interface	3G/4G-LTE

Input all relevant 3G/4G-LTE parameters from your ISP.

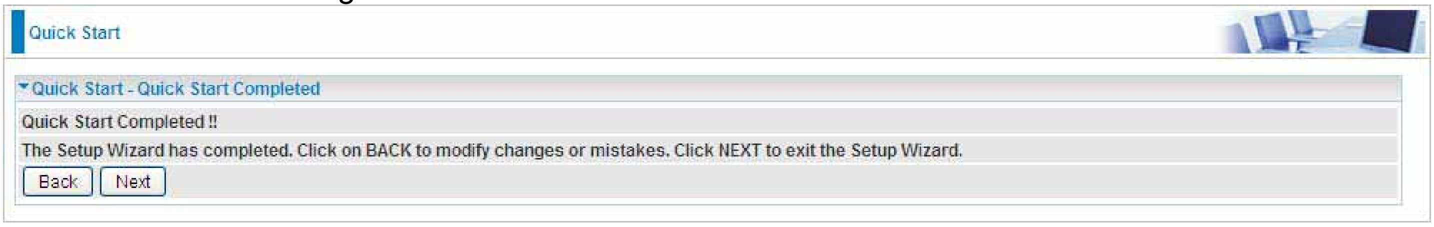


Quick Start - 3G/4G-LTE

Enter the 3G information provided to you by your ISP. Click NEXT to continue.

TEL No.	*99***1#
APN	internet
Username	
Password	
PIN	

Click Next to save changes.

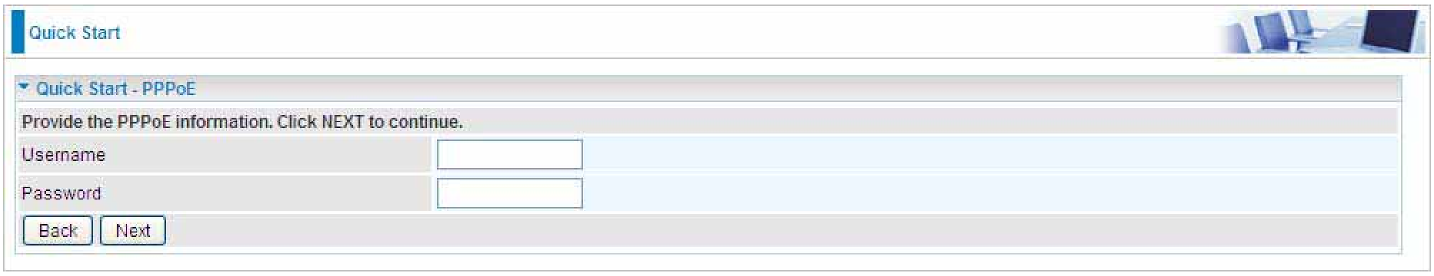


Quick Start - Quick Start Completed

Quick Start Completed !!

The Setup Wizard has completed. Click on BACK to modify changes or mistakes. Click NEXT to exit the Setup Wizard.

4.2 If selected **EWAN / PPPoE**, please enter PPPoE account information provided by your ISP. Click **NEXT** to continue.



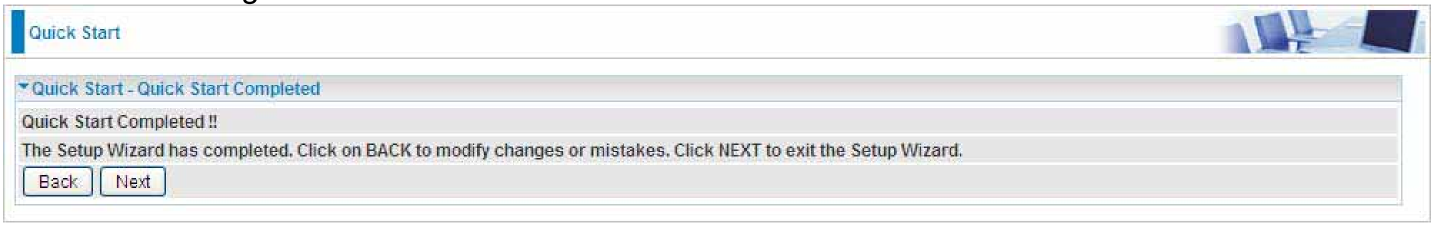
Quick Start - PPPoE

Provide the PPPoE information. Click NEXT to continue.

Username	
Password	

Step 5 – Quick Start Completed

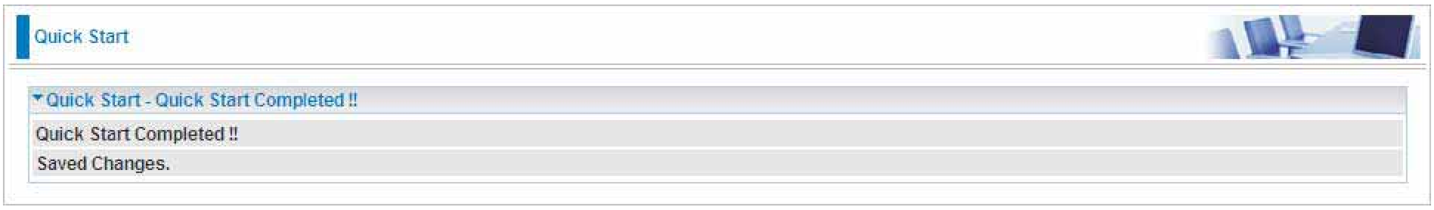
The Setup Wizard has completed. Click on BACK to modify changes or mistakes. Click **NEXT** to save the current settings.



Quick Start - Quick Start Completed

Quick Start Completed !!

The Setup Wizard has completed. Click on BACK to modify changes or mistakes. Click NEXT to exit the Setup Wizard.



Quick Start - Quick Start Completed !!

Quick Start Completed !!

Saved Changes.

Switch to **Status > Device Info** to view the status.

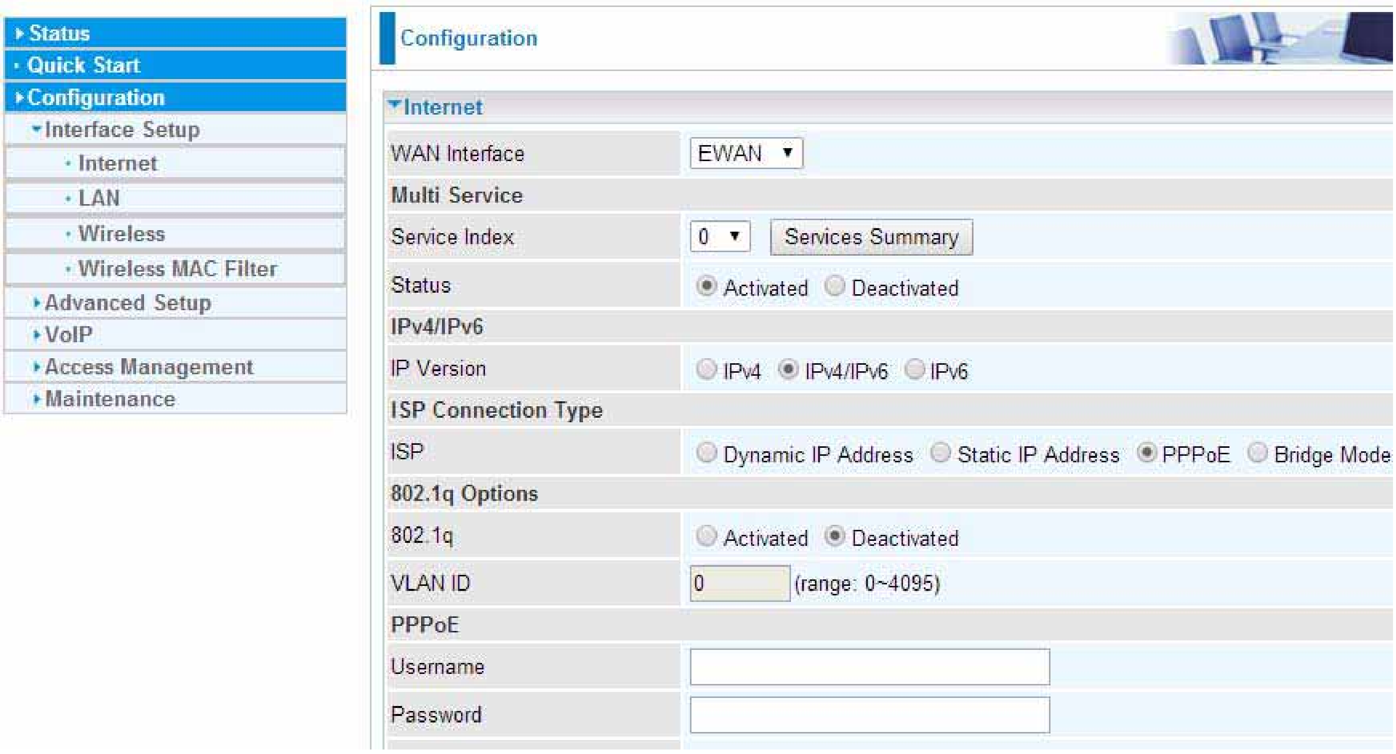
Configuration

Click to access and configure the available features in the following: **Interface Setup, Advanced Setup, VoIP, Access Management,** and **Maintenance.**

These functions are described in the following sections.

Interface Setup

Here are the features under **Interface Setup: Internet**, **LAN**, **Wireless** and **Wireless MAC Filter**.

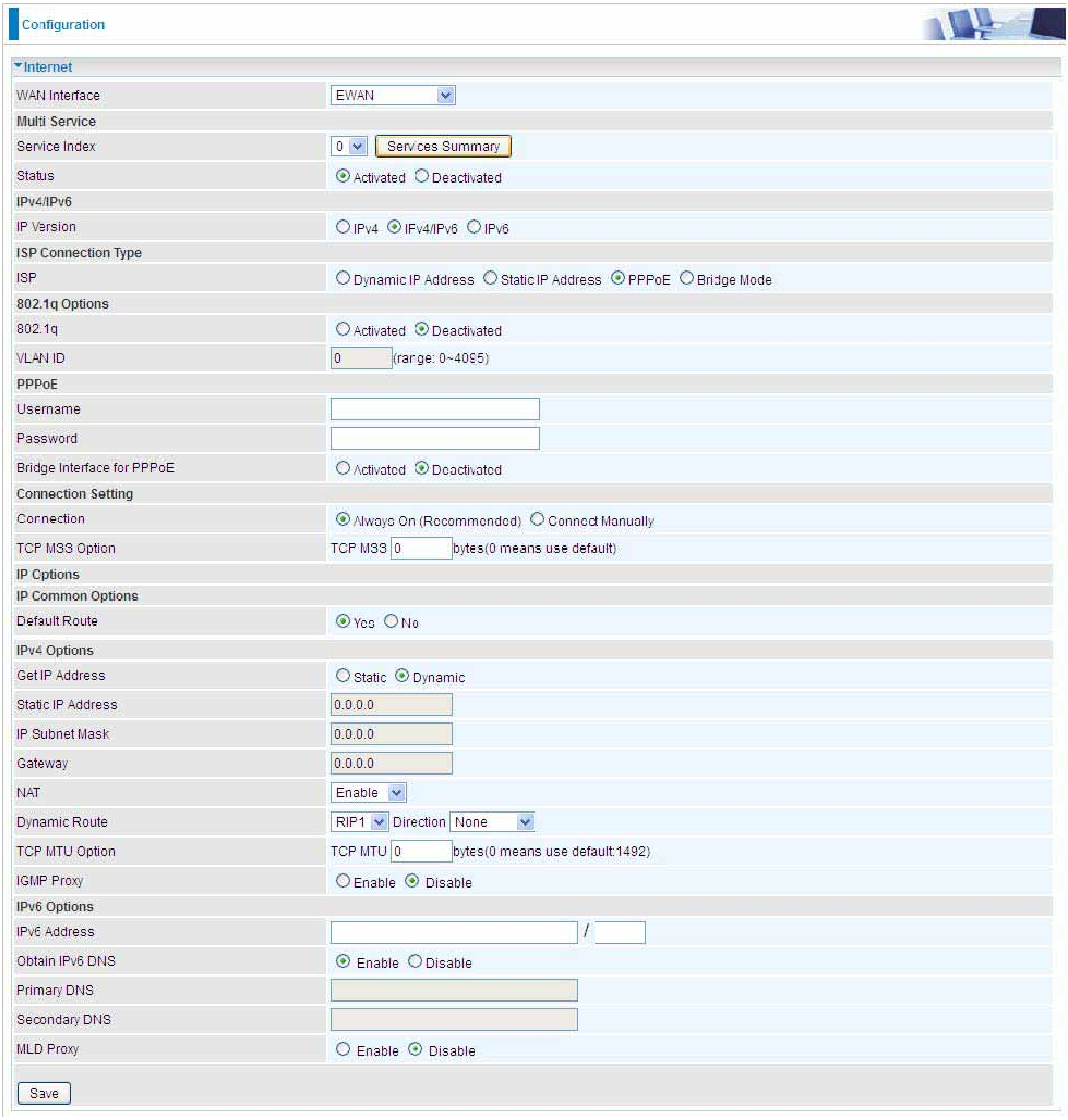


Internet

WAN Interface	EWAN
Multi Service	
Service Index	0
Status	● Activated ○ Deactivated
IPv4/IPv6	
IP Version	○ IPv4 ● IPv4/IPv6 ○ IPv6
ISP Connection Type	
ISP	○ Dynamic IP Address ○ Static IP Address ● PPPoE ○ Bridge Mode
802.1q Options	
802.1q	○ Activated ● Deactivated
VLAN ID	0 (range: 0~4095)
PPPoE	
Username	
Password	

Internet

❖ EWAN



Configuration

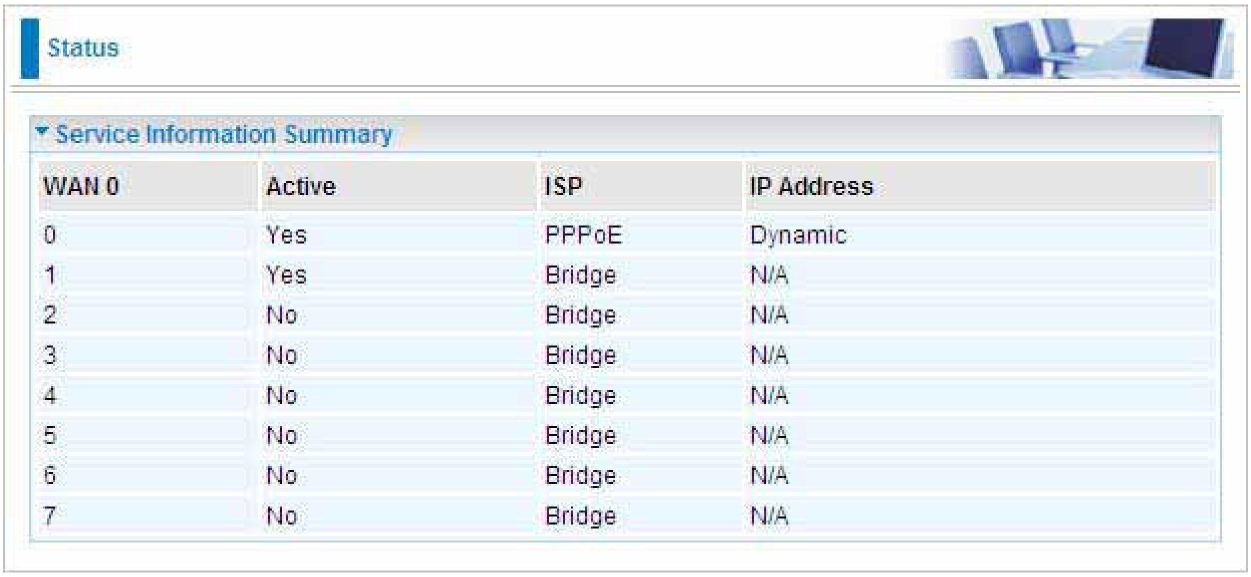
▾Internet

WAN Interface	EWAN
Multi Service	
Service Index	0 [Services Summary]
Status	● Activated ○ Deactivated
IPv4/IPv6	
IP Version	○ IPv4 ● IPv4/IPv6 ○ IPv6
ISP Connection Type	
ISP	○ Dynamic IP Address ○ Static IP Address ● PPPoE ○ Bridge Mode
802.1q Options	
802.1q	○ Activated ● Deactivated
VLAN ID	0 (range: 0~4095)
PPPoE	
Username	
Password	
Bridge Interface for PPPoE	○ Activated ● Deactivated
Connection Setting	
Connection	● Always On (Recommended) ○ Connect Manually
TCP MSS Option	TCP MSS 0 bytes(0 means use default)
IP Options	
IP Common Options	
Default Route	● Yes ○ No
IPv4 Options	
Get IP Address	○ Static ● Dynamic
Static IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway	0.0.0.0
NAT	Enable
Dynamic Route	RIP1 Direction None
TCP MTU Option	TCP MTU 0 bytes(0 means use default:1492)
IGMP Proxy	○ Enable ● Disable
IPv6 Options	
IPv6 Address	/
Obtain IPv6 DNS	● Enable ○ Disable
Primary DNS	
Secondary DNS	
MLD Proxy	○ Enable ● Disable

Multi Service

Service Index: The index marks the EWAN interface of different ISP type, ranging from 0-7.

Service Summary: The overall service information.



Status

Service Information Summary

WAN 0	Active	ISP	IP Address
0	Yes	PPPoE	Dynamic
1	Yes	Bridge	N/A
2	No	Bridge	N/A
3	No	Bridge	N/A
4	No	Bridge	N/A
5	No	Bridge	N/A
6	No	Bridge	N/A
7	No	Bridge	N/A

Status: Select whether to enable the service.

IPv4/IPv6

IP Version: Choose ***IPv4, IPv4/IPv6, IPv6*** based on your environment. If you don't know which one to choose from, please choose IPv4/IPv6 instead.

ISP Connection Type:

ISP: Select the encapsulation type your ISP uses.

- **Dynamic IP:** Select this option if your ISP provides you an IP address automatically.
- **Static IP:** Select this option to set static IP information. You will need to enter in the Connection type, IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form. IP address from by four IP octets separated by a dot (xx.xx.xx.xx). The Router will not accept the IP address if it is not in this format.
- **PPPoE:** Select this option if your ISP requires you to use a PPPoE connection.
- **Bridge:** Select this mode if you want to use this device as an OSI Layer 2 device like a switch.

802.1q Options

802.1q: When activated, please enter a VLAN ID.

VLAN ID: It is a parameter to specify the VLAN which the frame belongs. Enter the VLAN ID identification, tagged: 0-4095.

PPPoE (If selected PPPoE as WAN Connection Type; otherwise, skip this part)

Username: Enter the user name provided by your ISP.

Password: Enter the password provided by your ISP.

Bridge Interface for PPPoE: When "Activated", the device will gain WAN IP from your ISP with the PPPoE account. But if your PC is connected to the router working as a DHCP client, in this mode, the device acts as a NAT router; while if you dial up with the account within your PC, the device will then work as a bridge forwarding the PPPoE information to the PPPoE server and send the response to your PC, thus your PC gets a WAN IP working in the internet.

Connection Setting

Connection:

- **Always On:** Click on **Always On** to establish a PPPoE session during start up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- **Connect Manually:** Select Connect Manually when you don't want the connection up all the time.

TCP MSS Option: Enter the maximum size of the data that TCP can send in a segment. Maximum Segment Size (MSS).

IP Options

Default Route: Select **Yes** to use this interface as default route interface.

TCP MTU Option: Enter the maximum packet that can be transmitted. Default MTU is set to 1492.

IPv4 Options

Get IP Address: Choose Static or Dynamic

Static IP Address: If Static is selected in the above field, please enter the specific IP address you get from ISP and the following IP subnet mask and gateway address.

IP Subnet Mask: The default is 0.0.0.0. User can change it to other such as 255.255.255.0.Type the subnet mask assigned to you by your ISP (if given).

Gateway: Enter the specific gateway IP address you get from ISP.

NAT: Select Enable if you use this router to hold a group of PCs to get access to the internet.

Dynamic Route:

- **RIP Version:** (Routing Information protocol) Select this option to specify the RIP version, including RIP-1, RIP-2.
- **RIP Direction:** Select this option to specify the RIP direction.
  - **None** is for disabling the RIP function.
  - **Both** means the router will periodically send routing information and accept routing information then incorporate into routing table.
  - **IN only** means the router will only accept but will not send RIP packet.
  - **OUT only** means the router will only send but will not accept RIP packet.

IGMP Proxy: IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. Choose whether enable IGMP proxy.

IPv6 options (only when choose IPv4/IPv6 or just IPv6 in IP version field above):

IPv6 Address: Type the WAN IPv6 address from your ISP.

Obtain IPv6 DNS: Choose if you want to obtain DNS automatically.

Primary/Secondary: if you choose Disable in the Obtain IPv6 DNS field, please type the exactly primary and secondary DNS.

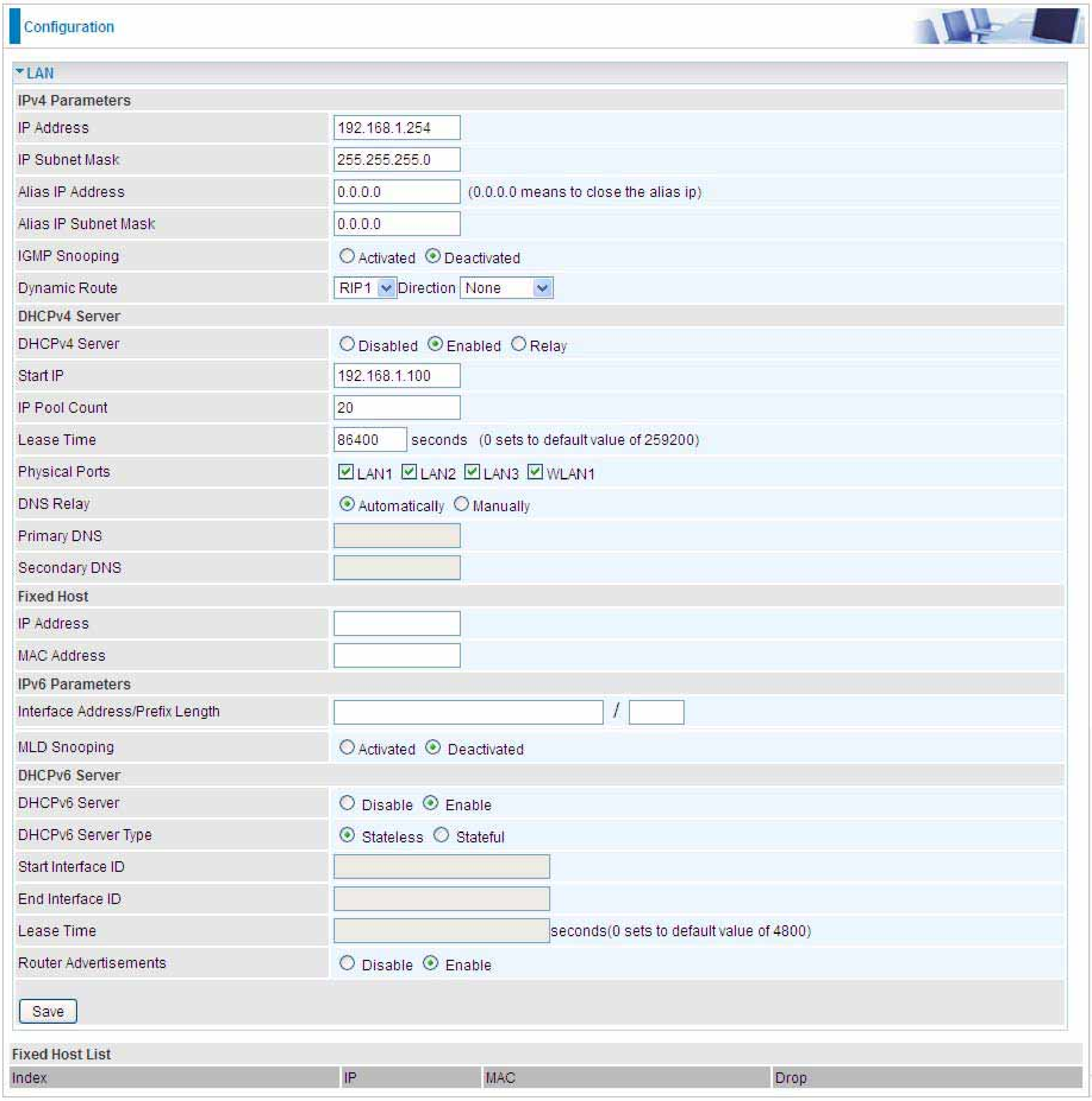
MLD Proxy: MLD (Multicast Listener Discovery Protocol) is to IPv6 just as IGMP to IPv4. It is a Multicast Management protocol for IPv6 multicast packets.

When router's Internet configuration is finished successfully, you can go to status to get the connection information.

➢

LAN

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



Configuration

▾LAN

IPv4 Parameters	
IP Address	192.168.1.254
IP Subnet Mask	255.255.255.0
Alias IP Address	0.0.0.0 (0.0.0.0 means to close the alias ip)
Alias IP Subnet Mask	0.0.0.0
IGMP Snooping	○ Activated ● Deactivated
Dynamic Route	RIP1 Direction None
DHCPv4 Server	
DHCPv4 Server	○ Disabled ● Enabled ○ Relay
Start IP	192.168.1.100
IP Pool Count	20
Lease Time	86400 seconds (0 sets to default value of 259200)
Physical Ports	☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ WLAN1
DNS Relay	● Automatically ○ Manually
Primary DNS	
Secondary DNS	
Fixed Host	
IP Address	
MAC Address	
IPv6 Parameters	
Interface Address/Prefix Length	/
MLD Snooping	○ Activated ● Deactivated
DHCPv6 Server	
DHCPv6 Server	○ Disable ● Enable
DHCPv6 Server Type	● Stateless ○ Stateful
Start Interface ID	
End Interface ID	
Lease Time	seconds(0 sets to default value of 4800)
Router Advertisements	○ Disable ● Enable

Fixed Host List

Index	IP	MAC	Drop

IPv4 Parameters

IP Address: Enter the IP address of Router in dotted decimal notation, for example, 192.168.1.254 (factory default).

IP Subnet Mask: The default is 255.255.255.0. User can change it to other such as 255.255.255.128.

Alias IP Address: This is for local networks virtual IP interface. Specify an IP address on this virtual interface.

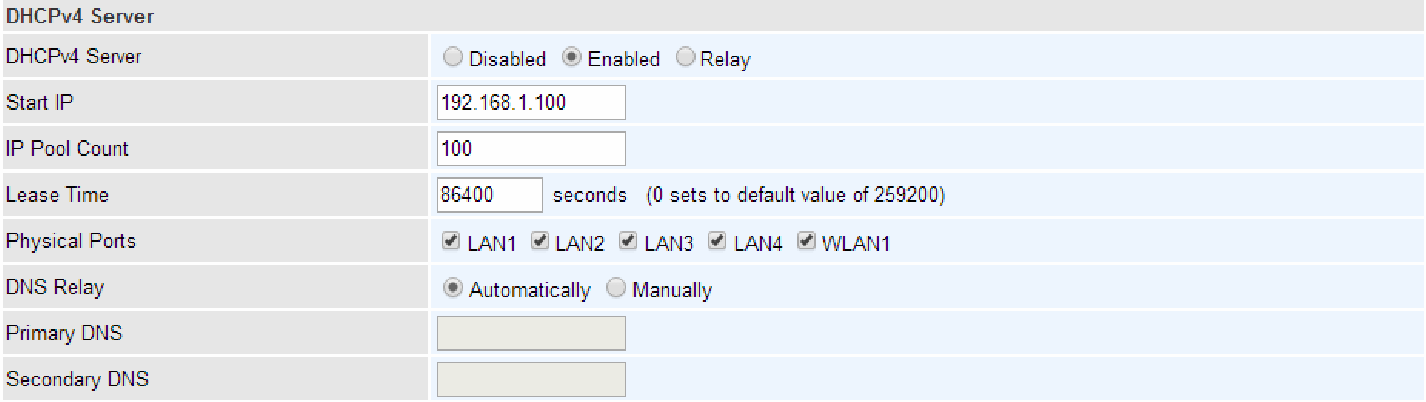
Alias IP Subnet Mask: Specify a subnet mask on this virtual interface.

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

Dynamic Route: Select the RIP version from RIP1 or RIP2.

DHCPv4 Server

DHCP (Dynamic Host Configuration Protocol) allows individual clients to obtain TCP/IP configuration at start-up from a server.



DHCPv4 Server

DHCPv4 Server	○ Disabled ● Enabled ○ Relay
Start IP	192.168.1.100
IP Pool Count	100
Lease Time	86400 seconds (0 sets to default value of 259200)
Physical Ports	☑ LAN1 ☑ LAN2 ☑ LAN3 ☑ LAN4 ☑ WLAN1
DNS Relay	● Automatically ○ Manually
Primary DNS	
Secondary DNS	

DHCPv4 Server: If set to **Enabled**, your BiPAC 6300VNP can assign IP addresses, default gateway and DNS servers to the DHCP client.

- If set to **Disabled**, the DHCP server will be disabled.
- If set to **Relay**, the BiPAC 6300VNP acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server field in this case.
- When DHCP is used, the following items need to be set.

Start IP: This field specifies the first of the contiguous addresses in the IP address pool.

IP Pool Count: This field specifies the count of the IP address pool.

Lease Time: The current lease time of client.

Physical Ports: Select to determine if the DHCPv4 server is applicable to the specific port or ports. By default, all ports can obtain local IP from DHCPv4 server.

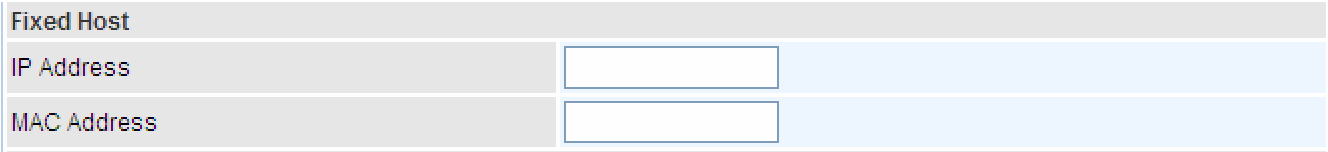
DNS Relay Select Automatically obtained or Manually set (if selected. Please set the exactly information). If you set Static IP in the ISP Connection Type field, then select **Manually** here and set the specific DNS information.

Primary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Secondary DNS Server: Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.

Fixed Host

In this field, users can map the specific IP (must in the DHCP IP pool) for some specific MAC, and this information can be listed in the following table.

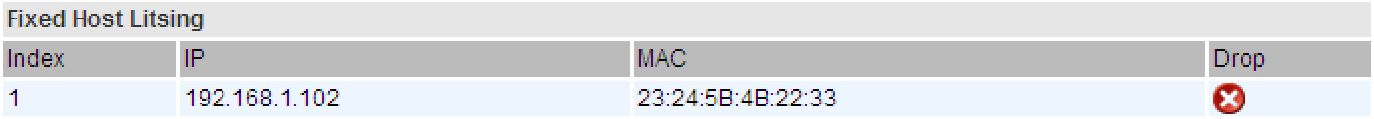


Fixed Host	
IP Address	
MAC Address	

IP Address: Enter the specific IP. For example: 192.168.1.110.

MAC Address: Enter the responding MAC. For example: 00:0A:F7:45:6D:ED

When added, you can see the ones listed as showed below:

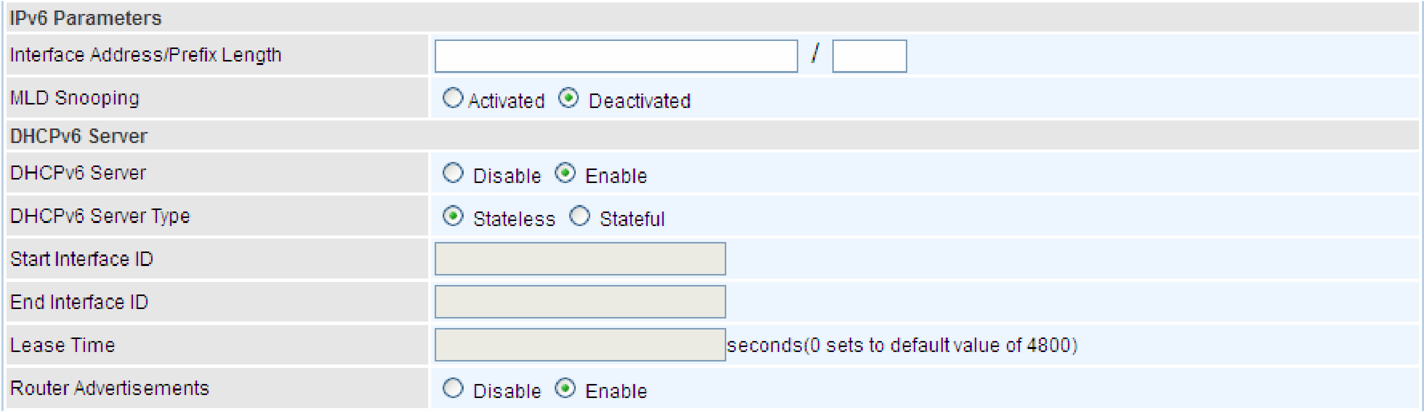


Fixed Host Litsing

Index	IP	MAC	Drop
1	192.168.1.102	23:24:5B:4B:22:33	☒

IPv6 parameters

The IPv6 address composes of two parts, thus, the prefix and the interface ID.



IPv6 Parameters	
Interface Address/Prefix Length	/
MLD Snooping	○ Activated ● Deactivated
DHCPv6 Server	
DHCPv6 Server	○ Disable ● Enable
DHCPv6 Server Type	● Stateless ○ Stateful
Start Interface ID	
End Interface ID	
Lease Time	seconds(0 sets to default value of 4800)
Router Advertisements	○ Disable ● Enable

Interface Address / Prefix Length: Enter a static LAN IPv6 address. If you are not sure what to do with this field, please leave it empty as if contains false information it could result in LAN devices not being able to access other IPv6 device. Router will take the same WAN's prefix to LAN side if the field is empty.

MLD Snooping: Similar to IGMP Snooping, but applicable for IPv6.

DHCPv6 Server

There are two methods to dynamically configure IPv6 address on hosts, **Stateless** and **Stateful**.

Stateless auto-configuration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information (MAC address) and information (prefix) advertised by routers. Routers advertise prefixes that identify the subnet(s) associated with a link, while hosts generate an "interface identifier" that uniquely identifies an interface on a subnet. An address is formed by combining the two. When using stateless configuration, you needn't configure anything on the client.

Stateful configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.)

In the stateful auto configuration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

DHCPv6 Server: Check whether to enable DHCPv6 server.

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

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

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

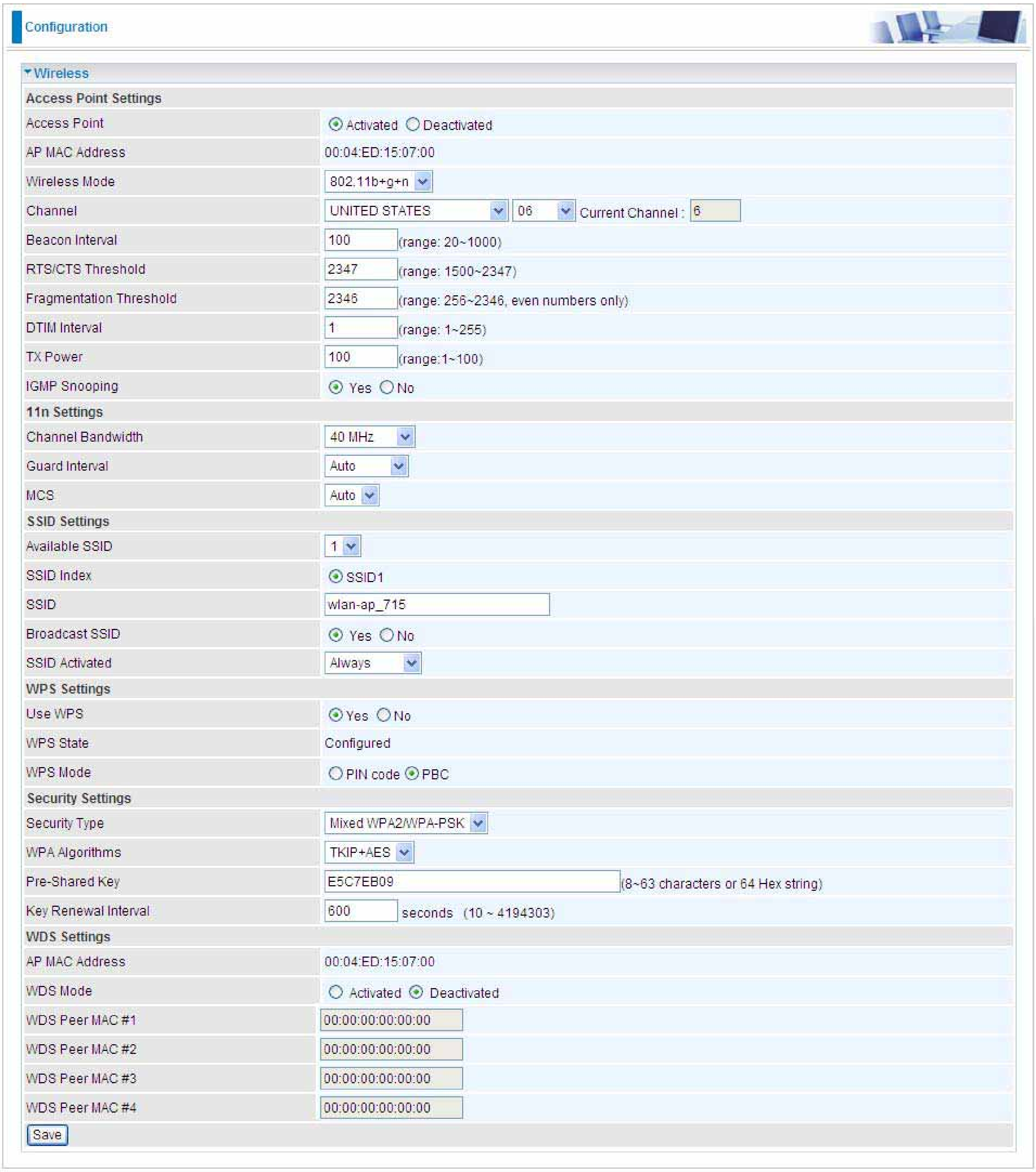
End interface ID: enter the end interface ID.

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

Issue Router Advertisement: Check to Enable or Disable the Issue Router Advertisement feature. This feature is to send Router Advertisement messages periodically which would multicast the IPv6 Prefix information (similar to v4 network number 192.168.1.0) to all LAN devices if the field is enabled. We suggest enabling this field.

Wireless

This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.



Configuration

▾Wireless

Access Point Settings	
Access Point	● Activated ○ Deactivated
AP MAC Address	00:04:ED:15:07:00
Wireless Mode	802.11b+g+n
Channel	UNITED STATES 06 Current Channel : 6
Beacon Interval	100 (range: 20~1000)
RTS/CTS Threshold	2347 (range: 1500~2347)
Fragmentation Threshold	2346 (range: 256~2346, even numbers only)
DTIM Interval	1 (range: 1~255)
TX Power	100 (range:1~100)
IGMP Snooping	● Yes ○ No
11n Settings	
Channel Bandwidth	40 MHz
Guard Interval	Auto
MCS	Auto
SSID Settings	
Available SSID	1
SSID Index	● SSID1
SSID	wlan-ap_715
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	○ PIN code ● PBC
Security Settings	
Security Type	Mixed WPA2/WPA-PSK
WPA Algorithms	TKIP+AES
Pre-Shared Key	E5C7EB09 (8~63 characters or 64 Hex string)
Key Renewal Interval	600 seconds (10 ~ 4194303)
WDS Settings	
AP MAC Address	00:04:ED:15:07:00
WDS Mode	○ Activated ● Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00

Access Point Settings

Access Point: Default setting is set to **Activated**. If you want to close the wireless interface, select **Deactivated.**

AP MAC Address: The MAC address of wireless AP.

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

Channel: The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. There are Regulation Domains and Channel ID in this field. The Channel ID will be different based on Regulation Domains. Select a channel from the drop-down list box.

Beacon interval: The Beacon Interval value indicates the frequency interval of the beacon. Enter a value between 20 and 1000. A beacon is a packet broadcast by the Router to synchronize the wireless network.

RTS/CTS Threshold: The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Enter a value between 1500 and 2347.

Fragmentation Threshold: The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2346, even number only.

DTIM Interval: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM).

TX Power: The transmission power of the antennas, ranging from 1-100, the higher the more powerful of the transmission performance.

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

11n Settings

Channel Bandwidth: Select either **20 MHz** or **20/40 MHz** for the channel bandwidth. The wider the Channel bandwidth the better the performance will be.

Guard Interval: Select either **400nsec** or **800nsec** for the guard interval. The guard interval is here to ensure that data transmission do not interfere with each other. It also prevents propagation delays, echoing and reflections. The shorter the Guard Interval, the better the performance will be. We recommend users to select Auto.

MCS: There are options **0~15** and **AUTO** to select for the **Modulation and Coding Scheme**. We recommend users selecting **AUTO**.

SSID Settings

Available SSID: User can determine how many virtual SSIDs to be used. Default is 1, maximum is 4.

SSID Index: Select the number of SSIDs you want to use; up to 4 SSIDs are available in the list.

SSID: The SSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change the default **wlan-ap** to a unique ID name to the AP which is already built-in to the router's wireless interface. Make sure your wireless clients have exactly the SSID as the device, in order to get connected to your network.

Broadcast SSID: Select **Yes** to make the SSID visible so a station can obtain the SSID through passive scanning. Select **No** to hide the SSID in so a station cannot obtain the SSID through passive scanning.

SSID Activated: Select the time period during which the SSID is active. Default is always which means the SSID will be active all the time without time control. See Time Schedule to set the timeslot to flexibly control when the SSID functions.

WPS Settings

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. WPS supports 2 types of configuration methods which are commonly known among consumers: **PIN Method** & **PBC Method**.

WPS State: Display whether the WPS is **configured** or **unconfigured**.

WPS Mode: Select the mode which to start WPS, choose between **PIN Code** and **PBC** (Push Button). Selecting **Pin Code** mode will require you to know the enrollee PIN code.

To future understand the two modes of configuration; please refer to the example of the **Wi-Fi Protected Setup.**

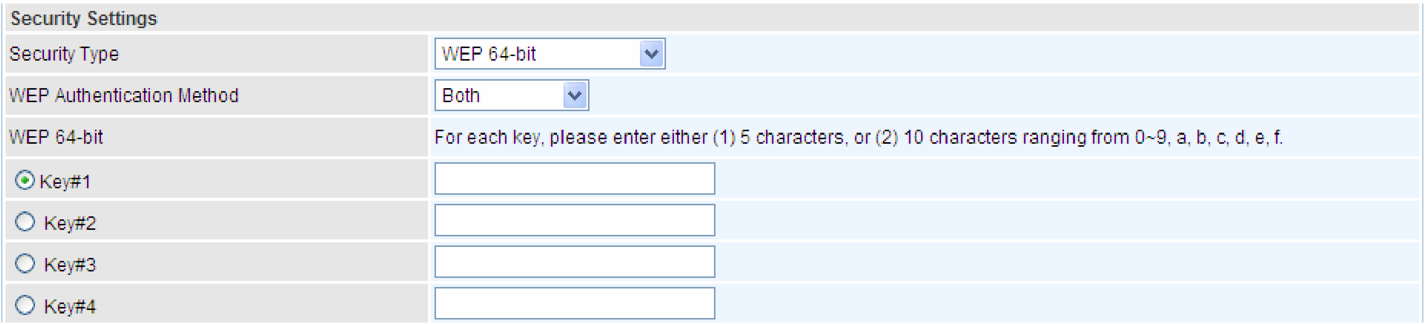
Security Settings

Security Type: You can disable or enable wireless security for protecting wireless network. The default type of wireless security is OPEN and to allow all wireless stations to communicate with the access points without any data encryption.

To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP and WPA.

There are five alternatives to select from: WEP 64-bit, WEP 128-bit, WPA-PSK, WPA2-PSK, and Mixed WPA/WPA2-PSK. If you require high security for transmissions, please select WPA-PSK, WPA2-PSK or WPA/WPA2-PSK.

WEP



Security Settings	
Security Type	WEP 64-bit
WEP Authentication Method	Both
WEP 64-bit	For each key, please enter either (1) 5 characters, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
● Key#1	
○ Key#2	
○ Key#3	
○ Key#4	

WEP Authentication Method: WEP authentication method, there are two methods of authentication used, Open System authentication (OPENWEB) and Share Key authentication (SHAREDWEB). We suggest you select OPENWEB.

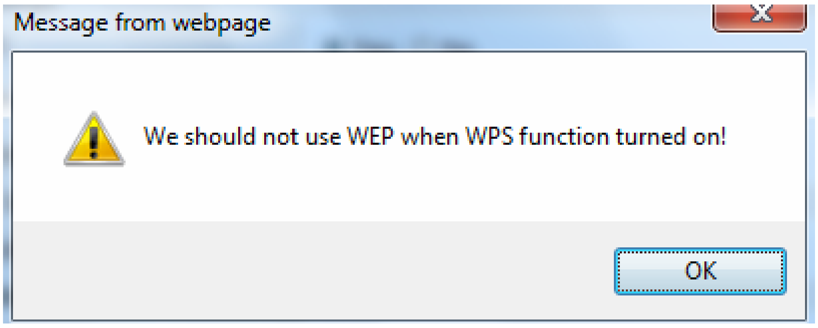
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP and 128-bitWEP respectively.

If you chose **WEP 64-bit**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").

If you chose **WEP 128-bit**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").

You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.

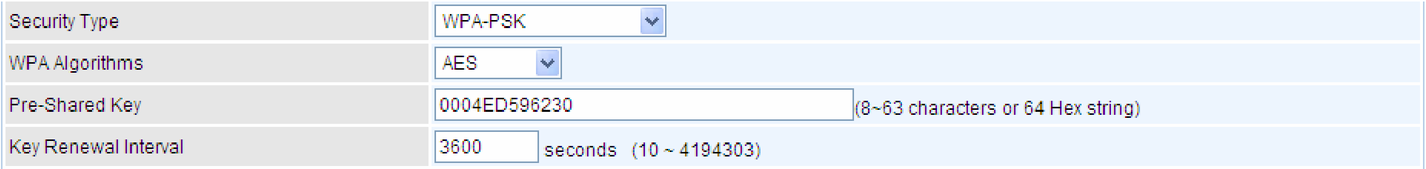
Note: When you enable **WPS** function, this **WEP** function will be invalid. And if you select one of **WEP-64Bits/ WEP-128Bits,** the following prompt box will appear to notice you.



Message from webpage

We should not use WEP when WPS function turned on!

WPA-PSK & WPA2-PSK



Security Type	WPA-PSK
WPA Algorithms	AES
Pre-Shared Key	0004ED596230 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

WPA Algorithms: TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) utilizes a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.

Pre-Shared key: The key for network authentication. The input format should be 8-63 ASKII characters or 64 hexadecimal characters

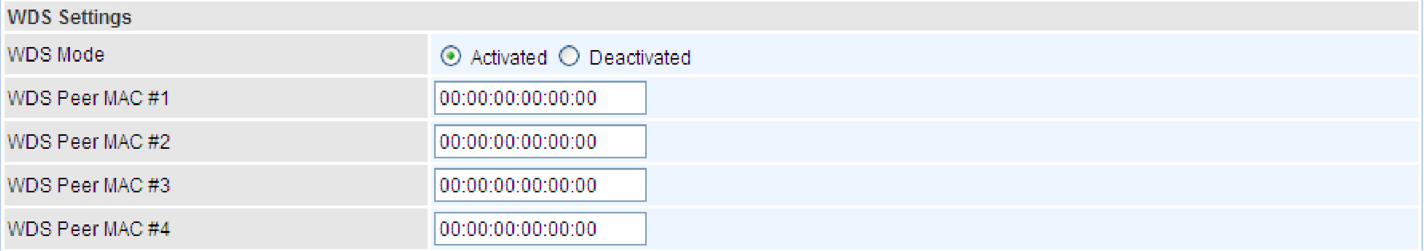
Key Renewal Interval: The time interval for changing the security key automatically between wireless client and AP.

WDS Settings

WDS (Wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access point. It is easy to be installed, just define the peer's MAC of the connected AP.

WDS Mode: select Activated to enable WDS feature and Deactivated to disable this feature.

MAC Address: Enter the AP MAC addresses (in XX:XX:XX:XX:XX:XX format) of the peer connected AP.

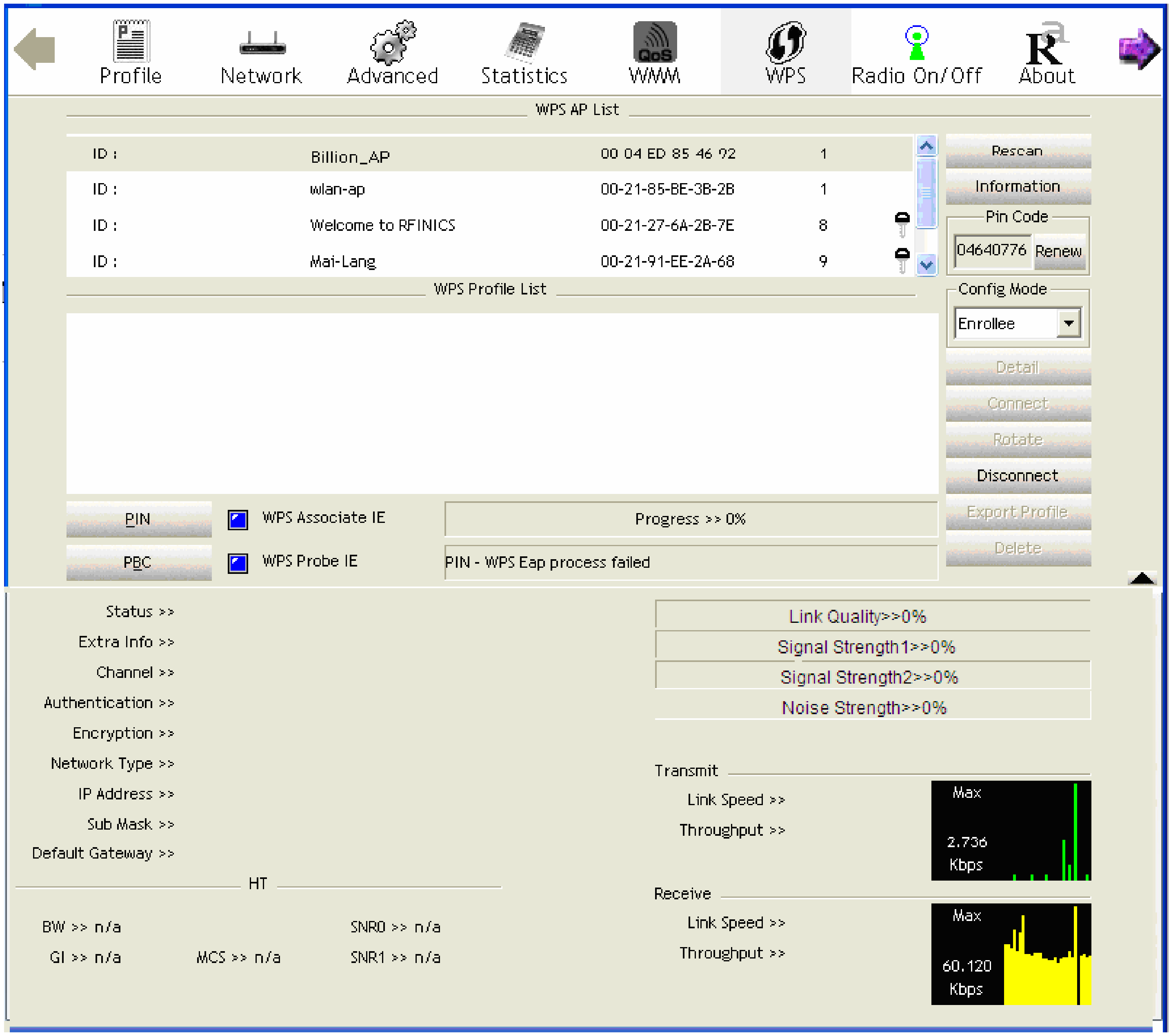


WDS Settings	
WDS Mode	● Activated ○ Deactivated
WDS Peer MAC #1	00:00:00:00:00:00
WDS Peer MAC #2	00:00:00:00:00:00
WDS Peer MAC #3	00:00:00:00:00:00
WDS Peer MAC #4	00:00:00:00:00:00

Wi-Fi Protected Setup (WPS) Example I:

PIN Method (Personal Information Number): Configure AP as Registrar

1. Jot down the client's Pin (e.g. 04640776) from the WPS utility (e.g. Ralink Utility)



WPS AP List

ID :	Billion_AP	00 04 ED 85 46 92	1
ID :	wlan-ap	00-21-85-BE-3B-2B	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8
ID :	Mai-Lang	00-21-91-EE-2A-68	9

WPS Profile List

Pin Code: 04640776

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

PIN - WPS Eap process failed

Status >>
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

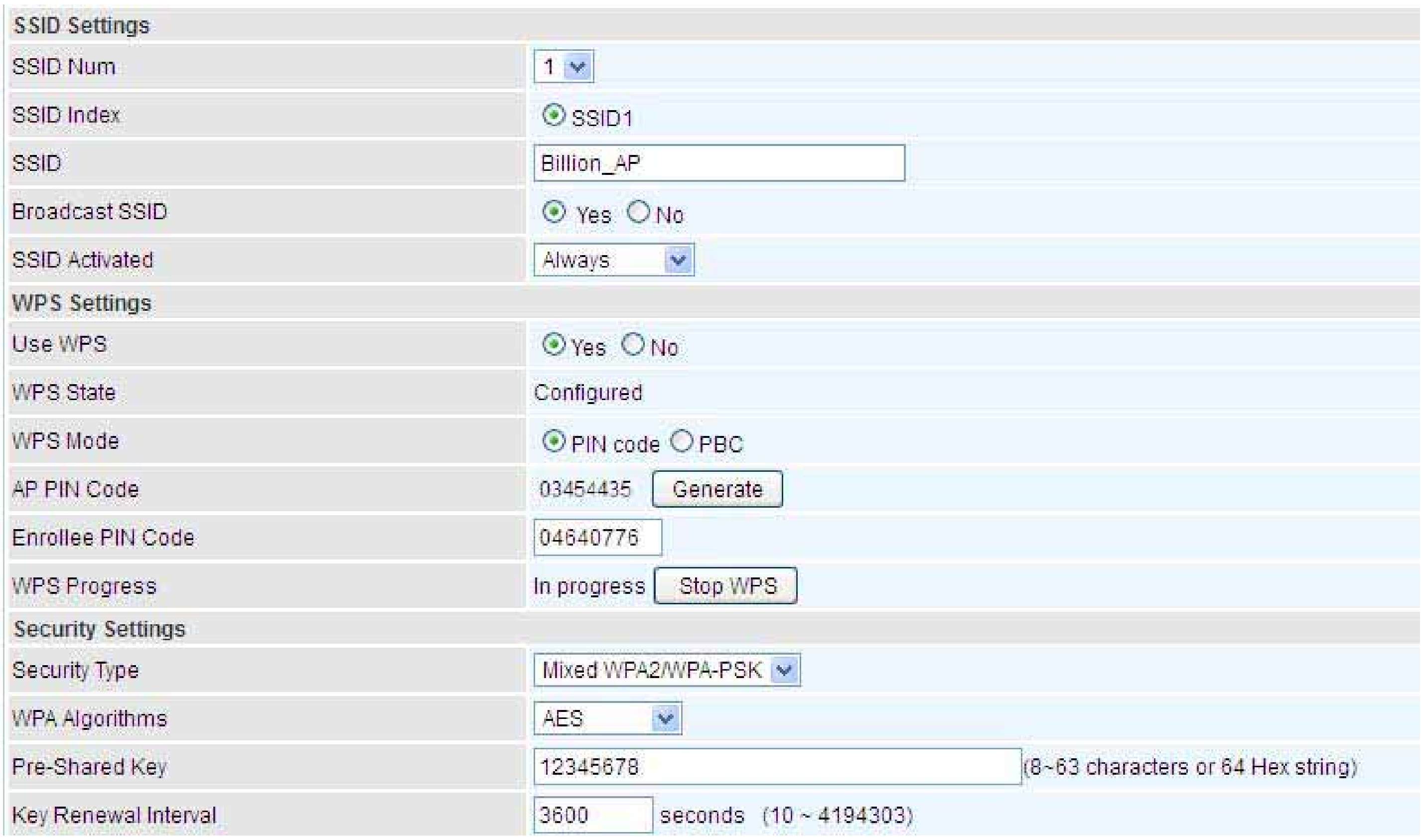
Link Quality>>0%
Signal Strength1>>0%
Signal Strength2>>0%
Noise Strength>>0%

Transmit
Link Speed >>
Throughput >>
2.736 Kbps

Receive
Link Speed >>
Throughput >>
60.120 Kbps

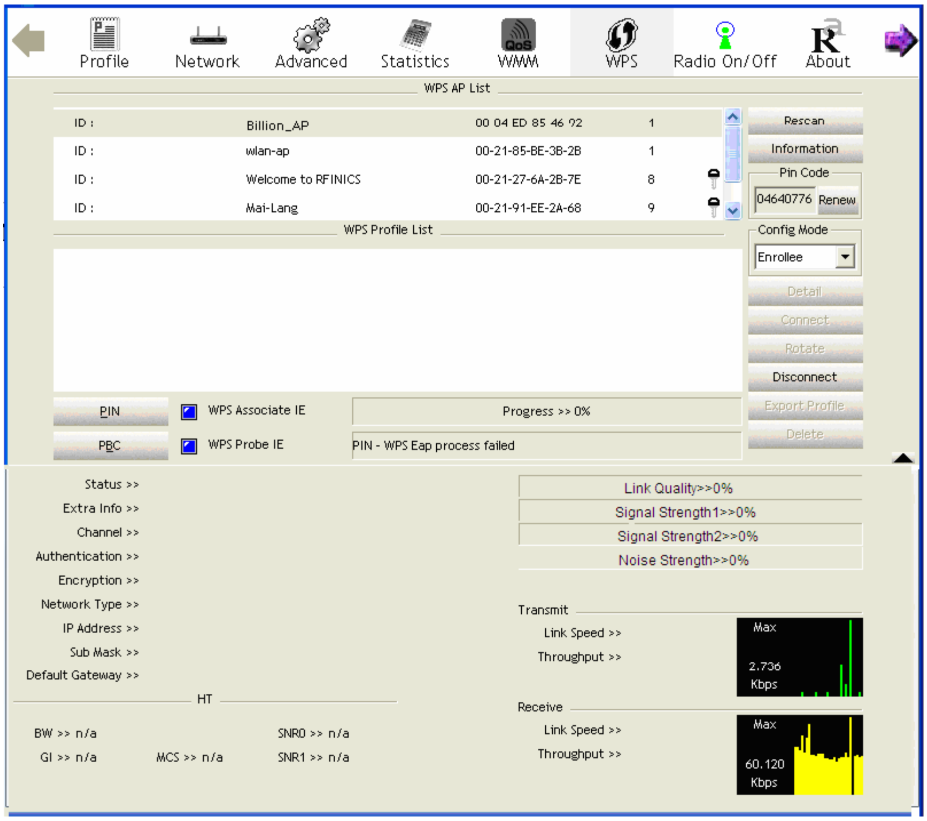
HT
BW >> n/a
GI >> n/a
MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

2. Enter the Enrollee (Client) PIN code and then press Start WPS.



SSID Settings	
SSID Num	1
SSID Index	● SSID1
SSID	Billion_AP
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	● PIN code ○ PBC
AP PIN Code	03454435 Generate
Enrollee PIN Code	04640776
WPS Progress	In progress Stop WPS
Security Settings	
Security Type	Mixed WPA2/WPA-PSK
WPA Algorithms	AES
Pre-Shared Key	12345678 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

3. Launch the wireless client’s WPS utility (e.g. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (e.g. Billion_AP) from the WPS AP List column. Then press the PIN button located on the middle left of the page to run the scan.



WPS AP List

ID :	Billion_AP	00 04 ED 85 46 92	1
ID :	wlan-ap	00-21-85-BE-3B-2B	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8
ID :	Mai-Lang	00-21-91-EE-2A-68	9

WPS Profile List

Pin Code: 04640776 Renew

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 0%

PIN - WPS Eap process failed

Status >>
Extra Info >>
Channel >>
Authentication >>
Encryption >>
Network Type >>
IP Address >>
Sub Mask >>
Default Gateway >>

Link Quality>>0%
Signal Strength1>>0%
Signal Strength2>>0%
Noise Strength>>0%

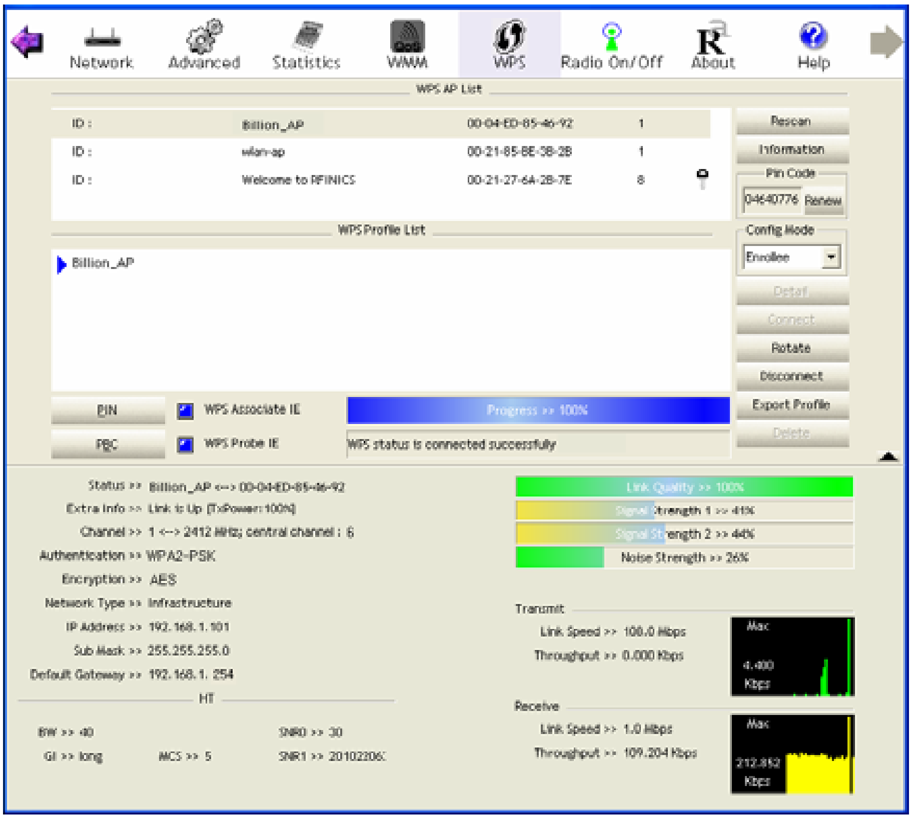
HT

BW >> n/a
GI >> n/a MCS >> n/a
SNR0 >> n/a
SNR1 >> n/a

Transmit
Link Speed >>
Throughput >>

Receive
Link Speed >>
Throughput >>

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



ID :	Billion_AP	00-04-ED-85-46-92	1
ID :	wlan-ap	00-21-85-8E-38-28	1
ID :	Welcome to RFINICS	00-21-27-6A-28-7E	8

Pin Code: 04640776

Config Mode: Enrollee

Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfuly

Status >> Billion_AP <--> 00-04-ED-85-46-92
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 6
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192. 168. 1. 101
Sub Mask >> 255.255.255.0
Default Gateway >> 192. 168. 1. 254

BW >> 40
GI >> long
MCS >> 5
SNR0 >> 30
SNR1 >> 20102206:

Link Quality >> 100%
Signal Strength 1 >> 41%
Signal Strength 2 >> 44%
Noise Strength >> 26%

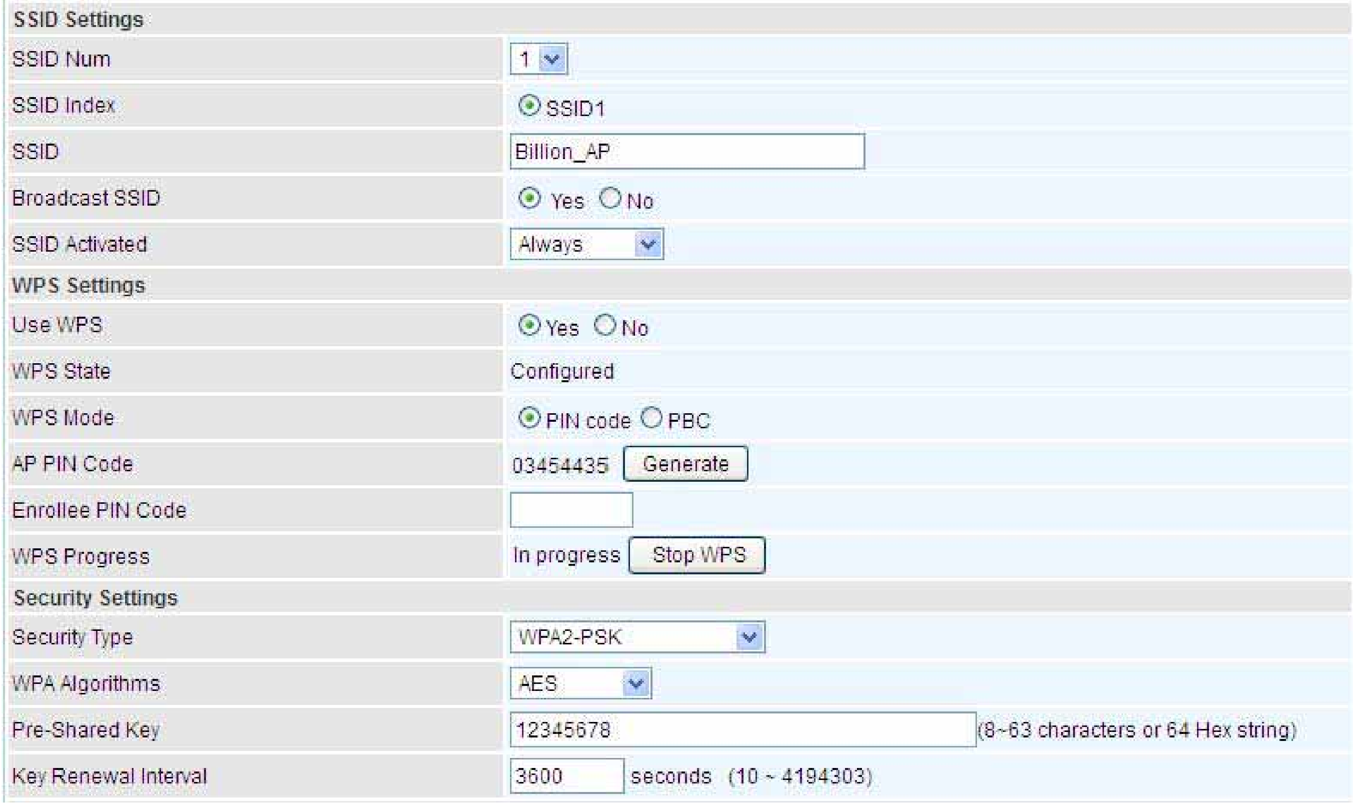
Transmit
Link Speed >> 100.0 Mbps
Throughput >> 0.000 Kbps

Receive
Link Speed >> 1.0 Mbps
Throughput >> 109.204 Kbps

Wi-Fi Protected Setup (WPS) Example II:

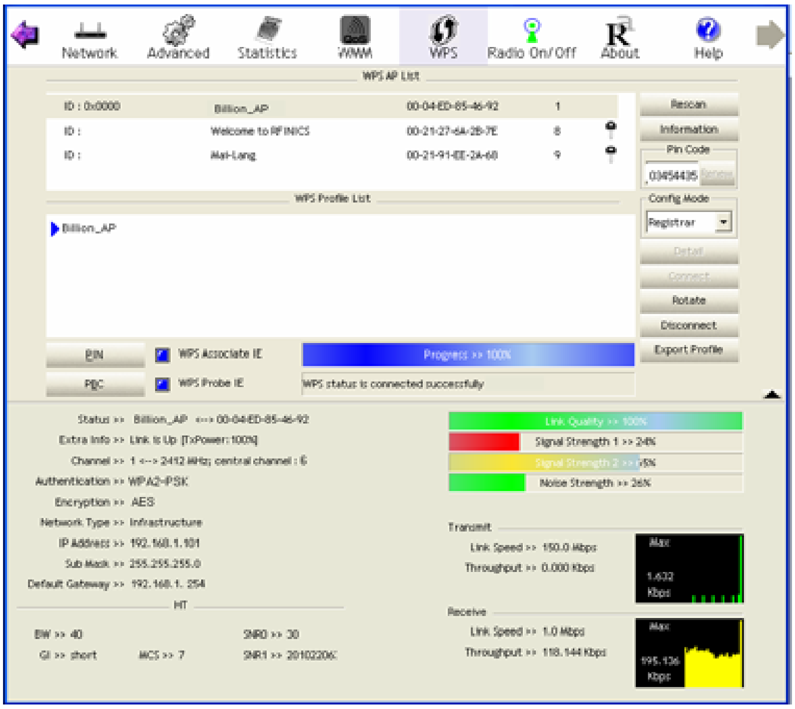
PIN Method (Personal Information Number): Configure AP as Enrollee

1. Jot down the AP PIN Code (e.g. 03454435) from the BiPAC 6300VNL. Press **Start** WPS.



SSID Settings	
SSID Num	1
SSID Index	● SSID1
SSID	Billion_AP
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	● PIN code ○ PBC
AP PIN Code	03454435 Generate
Enrollee PIN Code	
WPS Progress	In progress Stop WPS
Security Settings	
Security Type	WPA2-PSK
WPA Algorithms	AES
Pre-Shared Key	12345678 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

2. Launch the wireless client's WPS utility (e.g. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code (e.g. 03454435)column then choose the correct AP (e.g. Billion_AP) from the WPS AP List before pressing the PIN button to run the scan.



WPS AP List

ID : 0x0000	Billion_AP	00-04-ED-85-46-92	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8
ID :	Mai-Lang	00-21-91-EE-2A-68	9

Pin Code: 03454435 Renew

Config Mode: Registrar

WPS Profile List

Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully

Status >> Billion_AP <--> 00-04-ED-85-46-92
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 6
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.1.101
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1. 254

HT

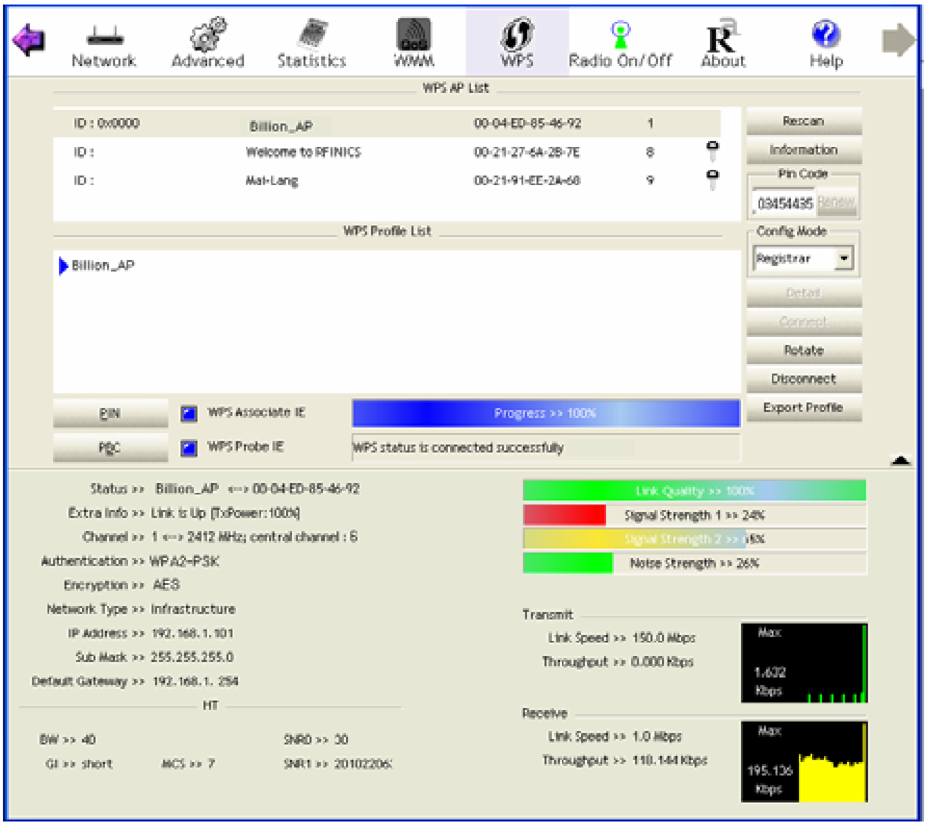
BW >> 40
GI >> short
MCS >> 7
SNR0 >> 30
SNR1 >> 20102206

Link Quality >> 100%
Signal Strength 1 >> 24%
Signal Strength 2 >> 65%
Noise Strength >> 26%

Transmit
Link Speed >> 150.0 Mbps
Throughput >> 0.000 Kbps
Max
1.632 Kbps

Receive
Link Speed >> 1.0 Mbps
Throughput >> 118.144 Kbps
Max
195.136 Kbps

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



WPS AP List

ID : 0x0000	Billion_AP	00-04-ED-85-46-92	1
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8
ID :	Mai-Lang	00-21-91-EE-2A-68	9

Pin Code: 03454435 Renew

Config Mode: Registrar

WPS Profile List

Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully

Status >> Billion_AP <--> 00-04-ED-85-46-92
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 6
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.1.101
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1. 254

HT

BW >> 40
GI >> short
MCS >> 7
SNR0 >> 30
SNR1 >> 20102206

Link Quality >> 100%
Signal Strength 1 >> 24%
Signal Strength 2 >> 65%
Noise Strength >> 26%

Transmit
Link Speed >> 150.0 Mbps
Throughput >> 0.000 Kbps
Max
1.632 Kbps

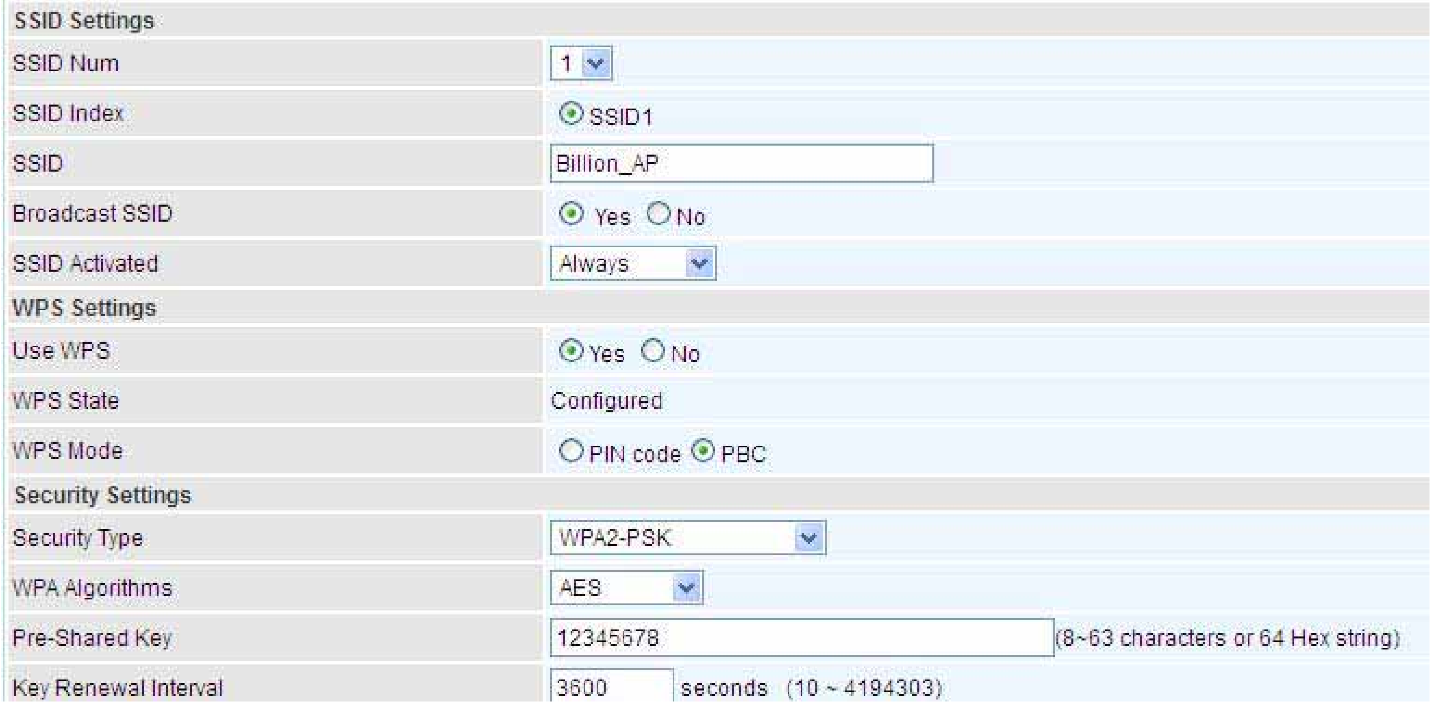
Receive
Link Speed >> 1.0 Mbps
Throughput >> 118.144 Kbps
Max
195.136 Kbps

4. 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.

Wi-Fi Protected Setup (WPS) Example III:

PBC (Push Button Configuiration) Method:

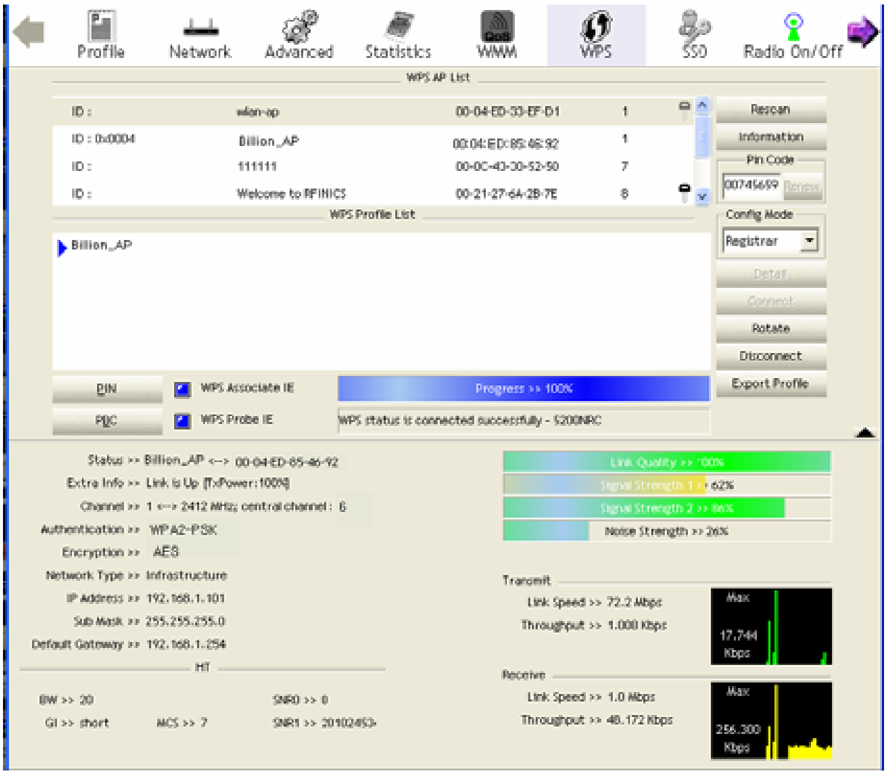
1.Click the PBC radio button in the GUI then press Start WPS.



SSID Settings	
SSID Num	1
SSID Index	● SSID1
SSID	Billion_AP
Broadcast SSID	● Yes ○ No
SSID Activated	Always
WPS Settings	
Use WPS	● Yes ○ No
WPS State	Configured
WPS Mode	○ PIN code ● PBC
Security Settings	
Security Type	WPA2-PSK
WPA Algorithms	AES
Pre-Shared Key	12345678 (8~63 characters or 64 Hex string)
Key Renewal Interval	3600 seconds (10 ~ 4194303)

2. Launch the wireless client's WPS Utility (e.g. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (e.g. Billion_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.



WPS AP List

ID :	wlan-ap	00-04-ED-33-EF-D1	1
ID : 0x0004	Billion_AP	00:04:ED:85:46:92	1
ID :	111111	00-0C-43-30-52-50	7
ID :	Welcome to RFINICS	00-21-27-64-2B-7E	8

Pin Code: 00745659 Renew

Config Mode: Registrar

WPS Profile List

Billion_AP

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 100%

WPS status is connected successfully - S200NRC

Status >> Billion_AP <--> 00-04-ED-85-46-92
Extra Info >> Link is Up [TxPower:100%]
Channel >> 1 <--> 2412 MHz; central channel : 6
Authentication >> WPA2-PSK
Encryption >> AES
Network Type >> Infrastructure
IP Address >> 192.168.1.101
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.254

HT

BW >> 20　SNR0 >> 0
GI >> short　MCS >> 7　SNR1 >> 20102453-

Link Quality >> 100%
Signal Strength 1 >> 62%
Signal Strength 2 >> 86%
Noise Strength >> 26%

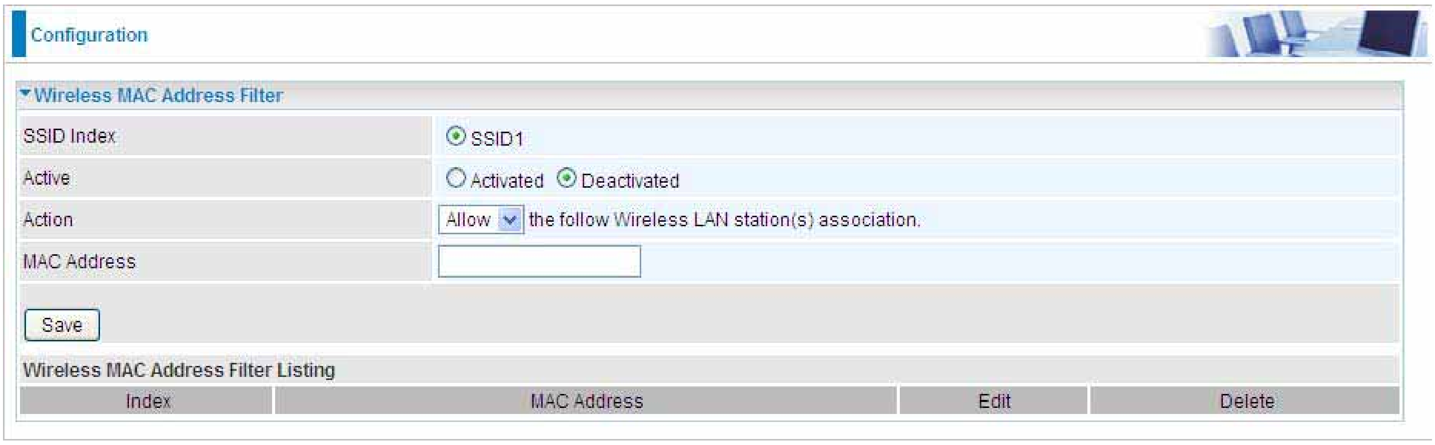
Transmit
Link Speed >> 72.2 Mbps
Throughput >> 1.000 Kbps
Max 17.744 Kbps

Receive
Link Speed >> 1.0 Mbps
Throughput >> 48.172 Kbps
Max 256.300 Kbps

Wireless MAC Filter

The MAC filter screen allows you to configure the router to give exclusive access to up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02.

You need to know the MAC address of the devices you wish to filter.



Wireless MAC Address Filter

SSID Index	● SSID1
Active	○ Activated ● Deactivated
Action	Allow the follow Wireless LAN station(s) association.
MAC Address	

Wireless MAC Address Filter Listing

Index	MAC Address	Edit	Delete

SSID Index: Select the targeted SSID you want the MAC filter rules to apply to.

Active: Select **Activated** to enable MAC address filtering.

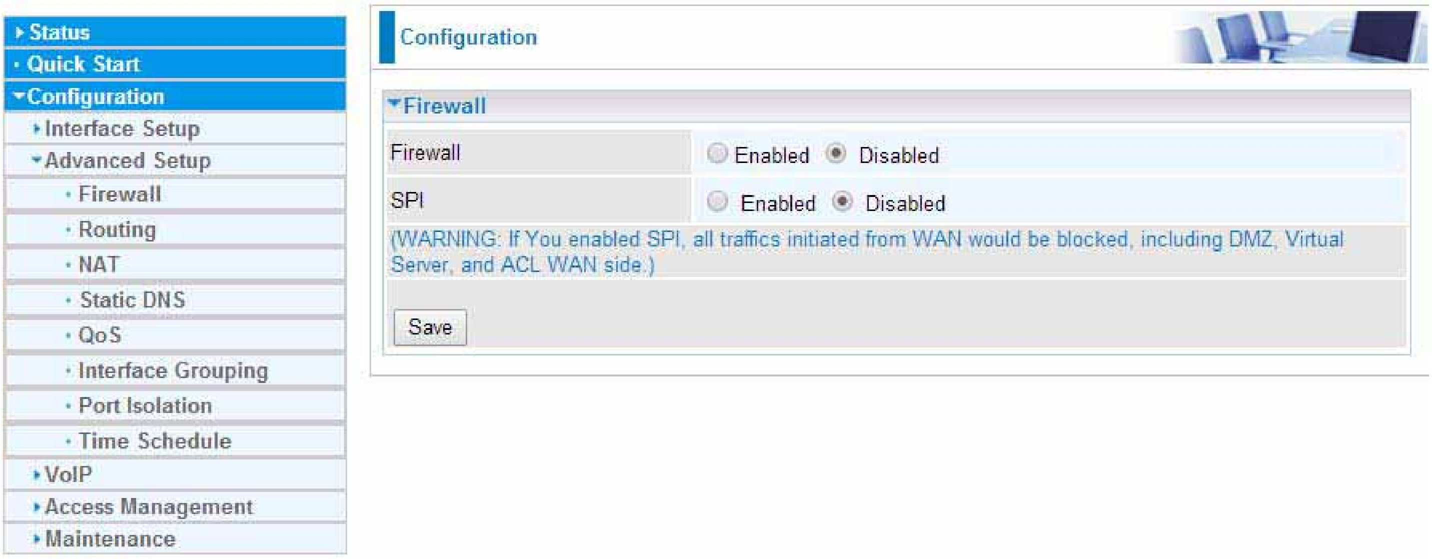
Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

Select **Deny** to block access to the AP, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.

MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the specified in these address fields.

Advanced Setup

Advanced Step provides advanced features including **Firewall**, **Routing**, **NAT**, **Static DNS**, **QoS**, **Internet Grouping**, **Port Isolation** and **Time Schedule** for advanced users.



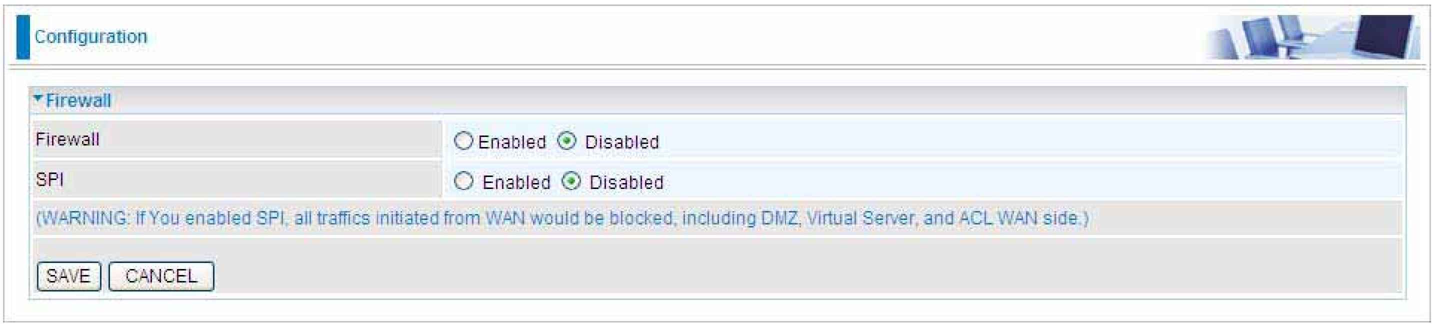
Firewall

Firewall	○ Enabled ● Disabled
SPI	○ Enabled ● Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

Firewall

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.



Configuration

▾Firewall

Firewall	○ Enabled ● Disabled
SPI	○ Enabled ● Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

Firewall: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

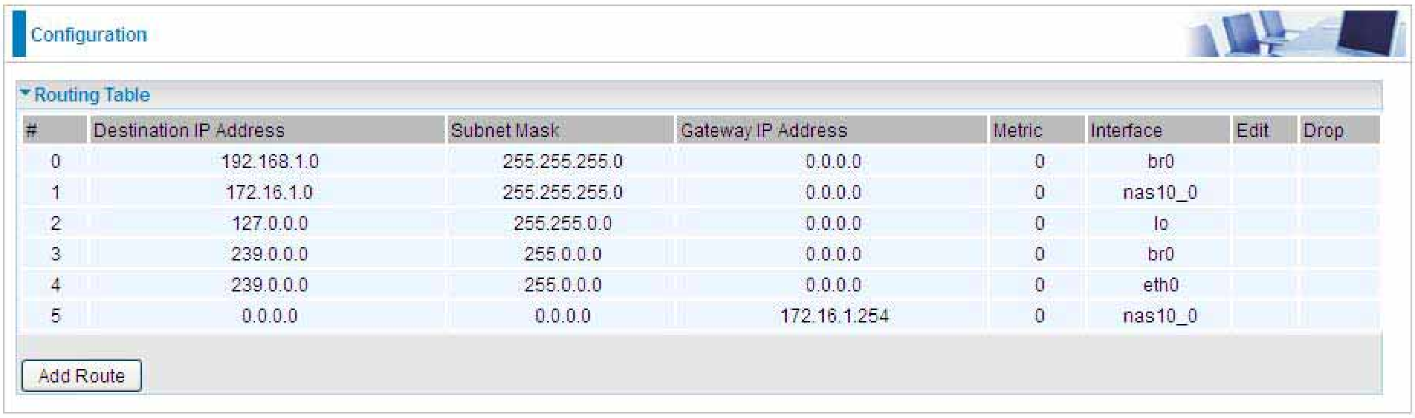
- **Enabled:** It activates your firewall function.
- **Disabled:** It disables the firewall function.

SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- **Enabled:** It activates your SPI function.
- **Disabled:** It disables the SPI function.

Routing

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



Configuration

▾Routing Table

#	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	172.16.1.0	255.255.255.0	0.0.0.0	0	nas10_0		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	lo		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		
4	239.0.0.0	255.0.0.0	0.0.0.0	0	eth0		
5	0.0.0.0	0.0.0.0	172.16.1.254	0	nas10_0		

#: Item number

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

Gateway IP Address: IP address of the gateway or existing interface that this route uses.

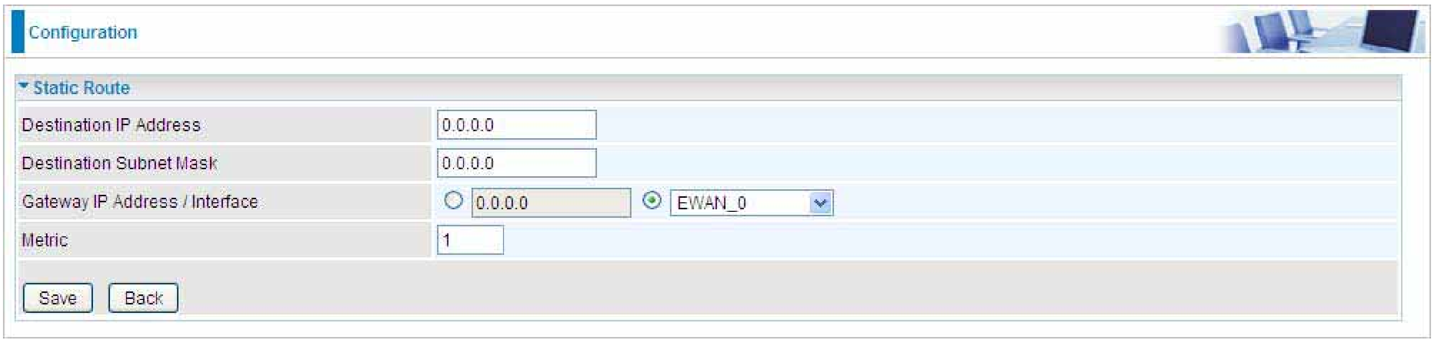
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: Media/channel selected to append the route.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

Add Route



Configuration

▾Static Route

Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Gateway IP Address / Interface	○ 0.0.0.0 ● EWAN_0
Metric	1

Destination IP Address: This is the destination subnet IP address.

Destination Subnet Mask: The subnet mask of destination network.

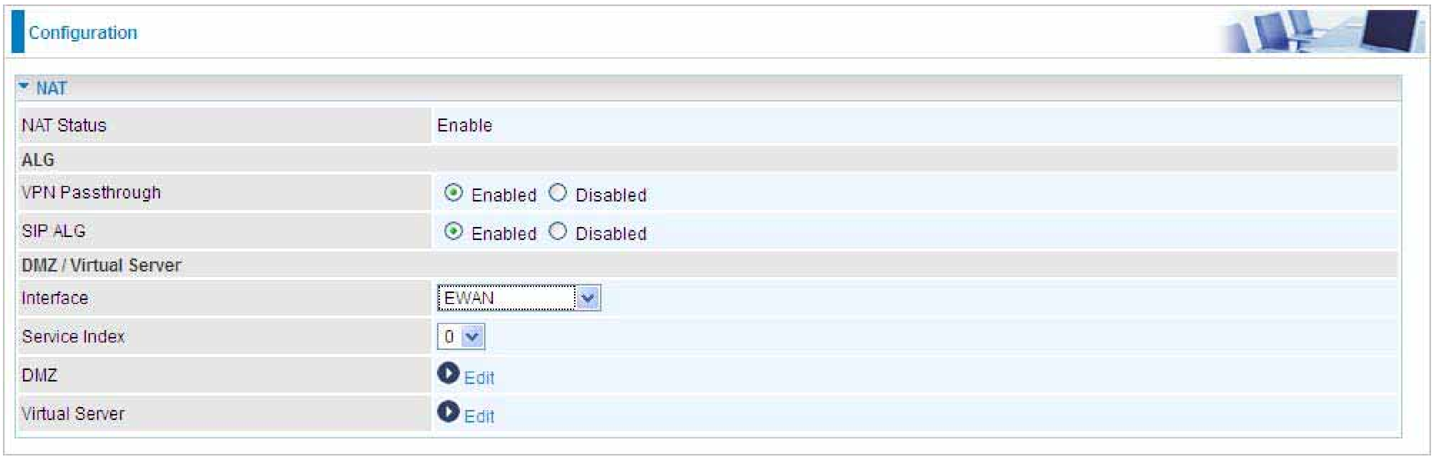
Gateway IP Address/Interface: This is the gateway IP address or existing interface to which packets are to be forwarded.

Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

In this session, there are “VPN Passthrough”, “SIP ALG”, “DMZ” and “Virtual Server” provided to solve these nasty problems.



Configuration

NAT

NAT Status	Enable
ALG	
VPN Passthrough	● Enabled ○ Disabled
SIP ALG	● Enabled ○ Disabled
DMZ / Virtual Server	
Interface	EWAN
Service Index	0
DMZ	Edit
Virtual Server	Edit

NAT Status: Enabled. It depends on ISP Connection Type in Internet settings.

VPN Passthrough: VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

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

Interface: Select to set DMZ/Virtual Server for “EWAN”

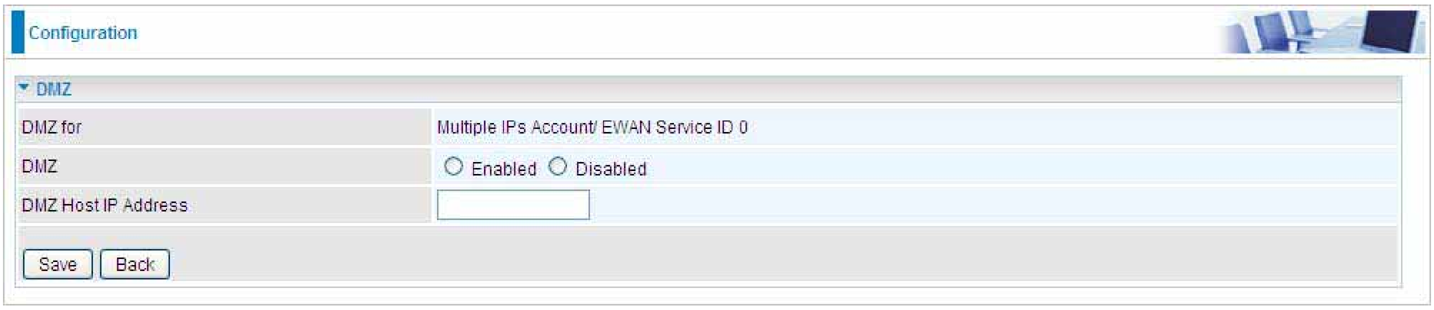
Service Index: Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

Click **DMZ** Edit or **Virtual Server** Edit to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode.

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.



DMZ for	Multiple IPs Account/ EWAN Service ID 0
DMZ	○ Enabled ○ Disabled
DMZ Host IP Address	

DMZ for: Indicate the related WAN interface which allows outside network to connect in and communicate. **Note:** Here you can see the Multiple IPs Account/EWAN Service ID 0. It is the interface set in the previous NAT page.

DMZ:

- **Enabled:** It activates your DMZ function.
- **Disabled:** It disables the DMZ function.

DMZ Host IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Select the **Save** button to apply your changes.

Virtual Server

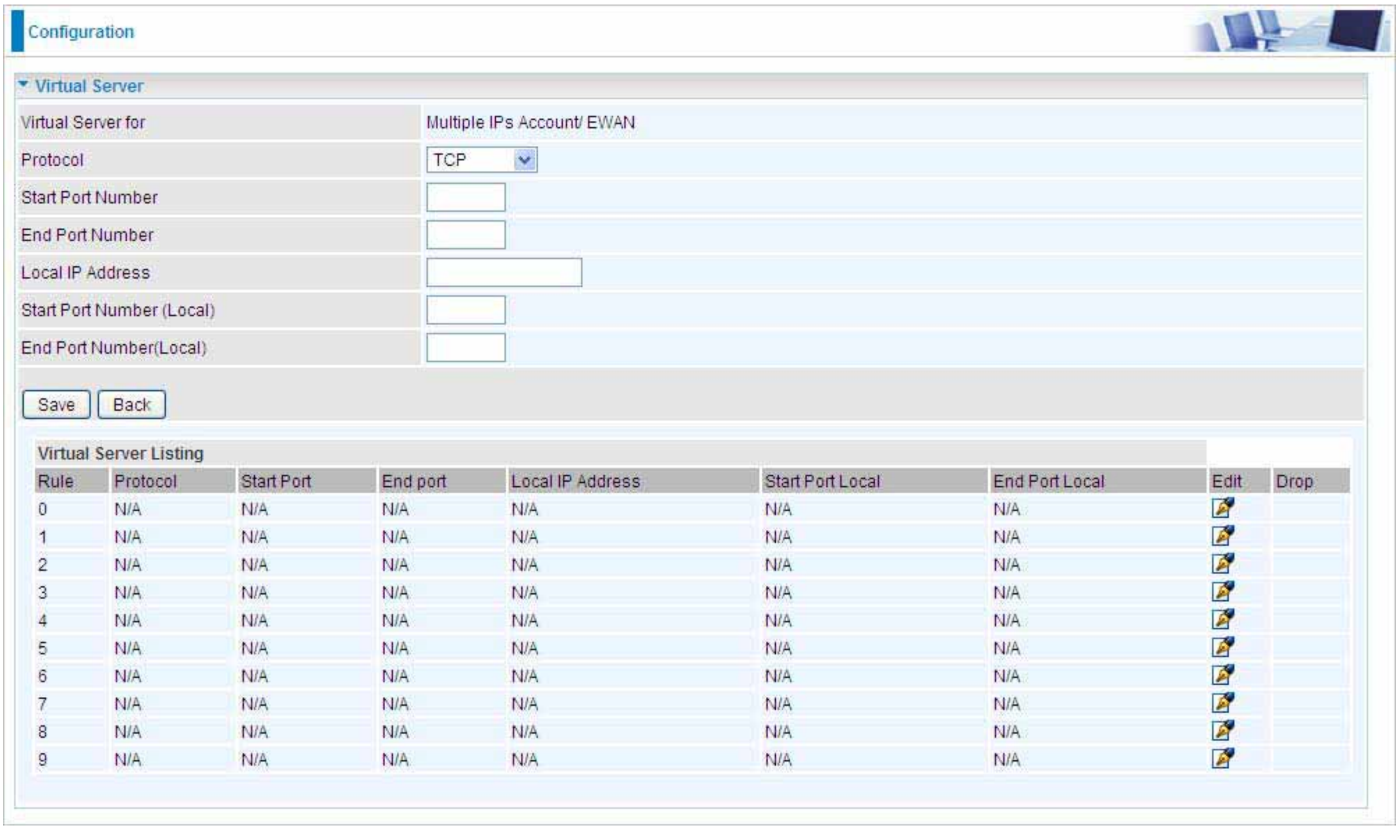
NOTE: This feature disables automatically if WAN connection is in BRIDGE mode.

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

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

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

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



Virtual Server for	Multiple IPs Account/ EWAN
Protocol	TCP
Start Port Number	
End Port Number	
Local IP Address	
Start Port Number (Local)	
End Port Number(Local)	

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	N/A	N/A	N/A	N/A	N/A	N/A	✎	
1	N/A	N/A	N/A	N/A	N/A	N/A	✎	
2	N/A	N/A	N/A	N/A	N/A	N/A	✎	
3	N/A	N/A	N/A	N/A	N/A	N/A	✎	
4	N/A	N/A	N/A	N/A	N/A	N/A	✎	
5	N/A	N/A	N/A	N/A	N/A	N/A	✎	
6	N/A	N/A	N/A	N/A	N/A	N/A	✎	
7	N/A	N/A	N/A	N/A	N/A	N/A	✎	
8	N/A	N/A	N/A	N/A	N/A	N/A	✎	
9	N/A	N/A	N/A	N/A	N/A	N/A	✎	

Virtual Server for: Indicate the related WAN interface which allows outside network to connect in and communicate.

Protocol: Choose the application protocol.

Start / End Port Number: Enter a port or port range you want to forward.

(Example: Start / End: 1000 or Start: 1000, End: 2000).

The starting number must greater than zero (0) and the ending port must be the same or larger than the starting port.

Local IP Address: Enter your server IP address in this field.

Start / End Port Number (Local): Enter the start / end port number of the local application (service).

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

Well-known and Registered Ports

Port Number	Protocol	Description
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)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio

NOTE:

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

Attention

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

Example: How to setup Port Forwarding for port 21 (FTP server)

If you have a FTP server in your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway and go to **Configuration / Advanced Setup / NAT / Virtual Server.**

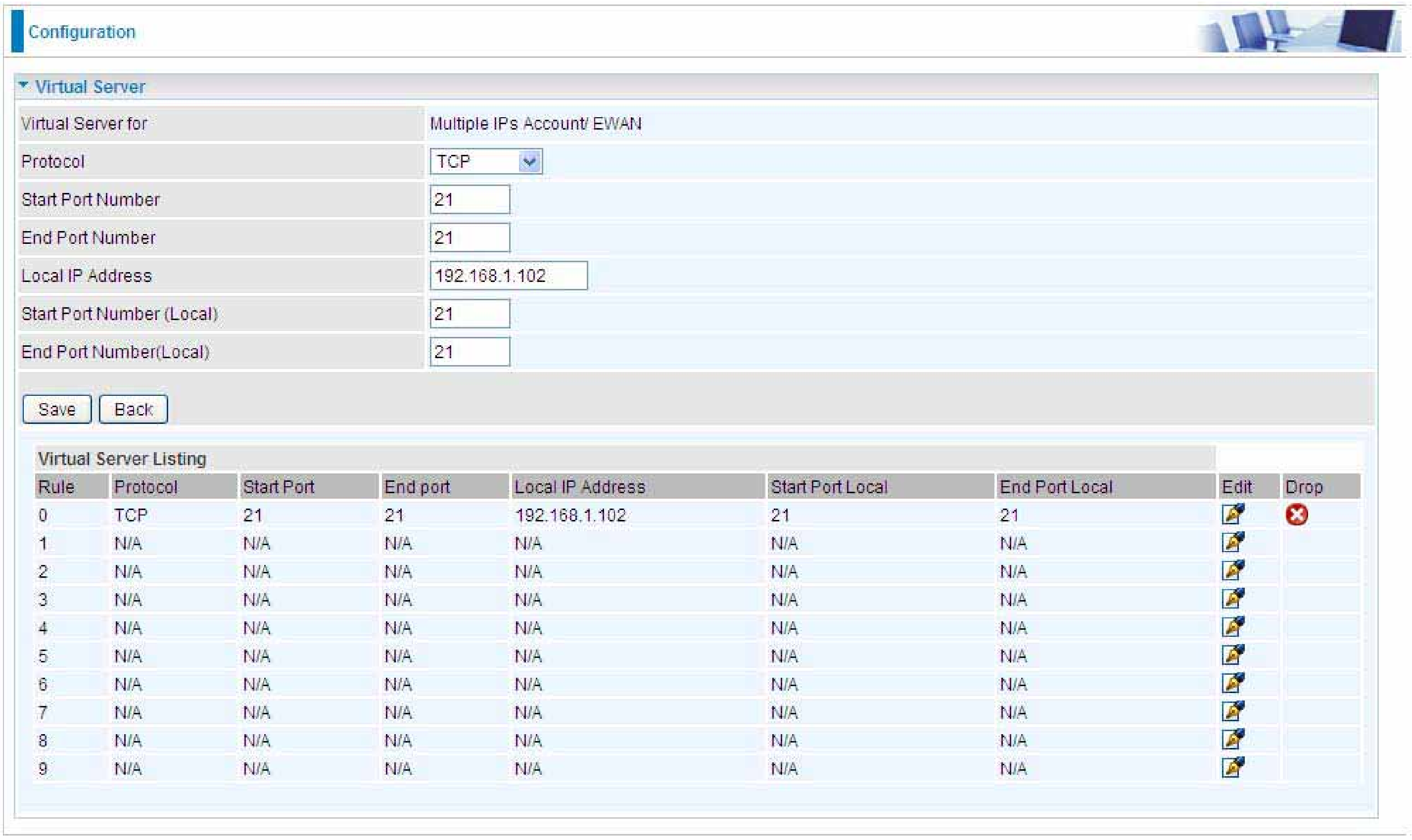
FTP server uses TCP protocol with port 21.

Enter ”21” to Start and End Port Number. BiPAC 6300VNP will accept port 21 requests from WAN side.

Eneter the static IP address which is assiged to the local PC to host the FTP server. Ex: 192.168.1.102

Enter ”21” to Local Start and End Port number. BiPAC 6300VNP will forward port 21 request from WAN to the specific LAN PC (ex:192.168.1.102) in the network.

Step 3: Click **Save** to save settings.



Configuration

▾ Virtual Server

Virtual Server for	Multiple IPs Account/ EWAN
Protocol	TCP
Start Port Number	21
End Port Number	21
Local IP Address	192.168.1.102
Start Port Number (Local)	21
End Port Number(Local)	21

Virtual Server Listing

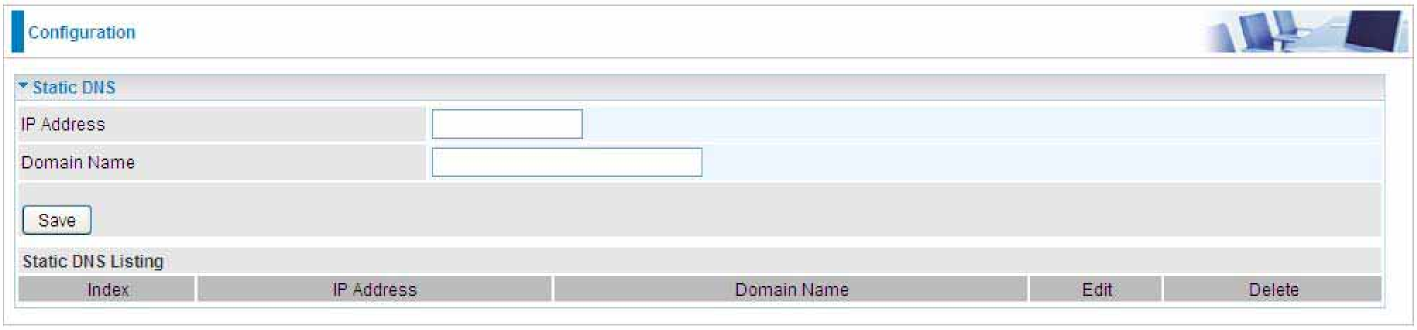
Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.102	21	21	✎	✖
1	N/A	N/A	N/A	N/A	N/A	N/A	✎	
2	N/A	N/A	N/A	N/A	N/A	N/A	✎	
3	N/A	N/A	N/A	N/A	N/A	N/A	✎	
4	N/A	N/A	N/A	N/A	N/A	N/A	✎	
5	N/A	N/A	N/A	N/A	N/A	N/A	✎	
6	N/A	N/A	N/A	N/A	N/A	N/A	✎	
7	N/A	N/A	N/A	N/A	N/A	N/A	✎	
8	N/A	N/A	N/A	N/A	N/A	N/A	✎	
9	N/A	N/A	N/A	N/A	N/A	N/A	✎	

Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com can be translated into the addresses 192.0.32.10 (IPv4).

Static DNS is a concept relative to Dynamic DNS, in static DNS system, the IP mapped is static without change.



IP Address	
Domain Name	

Static DNS Listing

Index	IP Address	Domain Name	Edit	Delete

IP Address: The IP address you are going to give a specific domain name.

Domain Name: The friendly domain name for the IP address.

Press **Save** button to apply your settings.

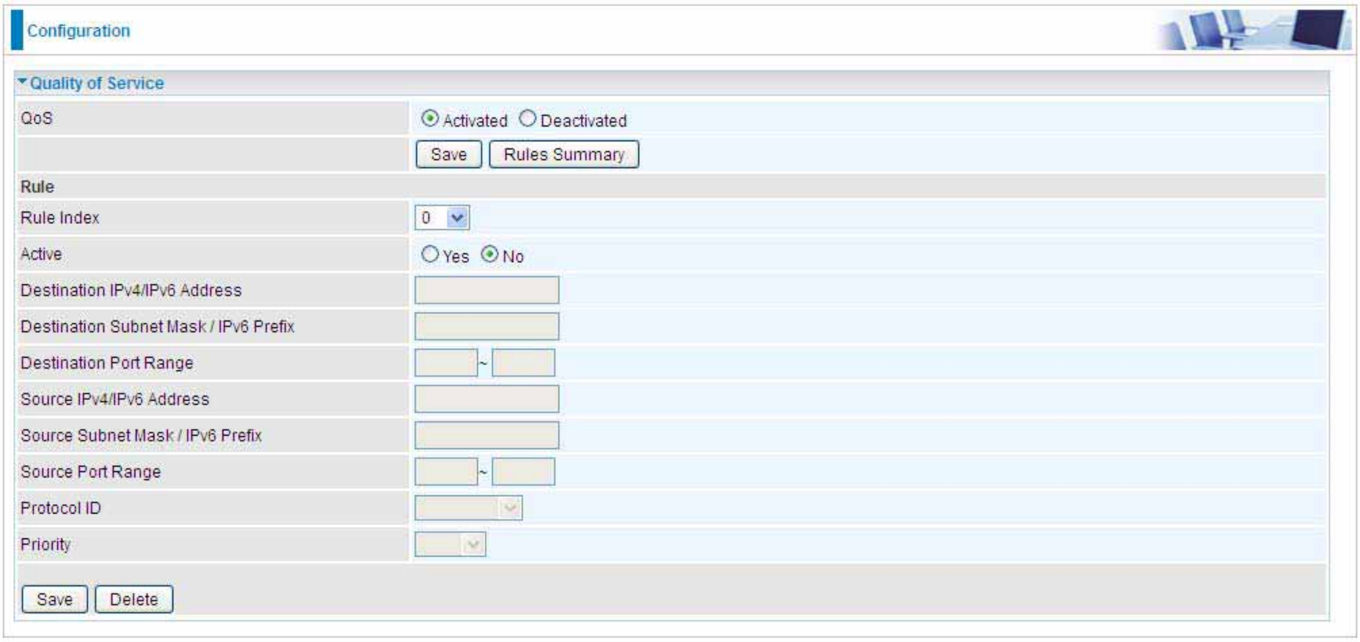
QoS

QoS helps you control the upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet).

It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want giver higher priority to, such as voice data packets given higher priority than web data packets.

QoS can be toggled Activated and Deactivated. QoS must be activated before you can edit the following options. When you are done making changes, click on **Save** to save your changes.

Click on **Rule Summary** to view the list of QoS rules that have been added.



Configuration

Quality of Service

QoS	● Activated ○ Deactivated
	Save Rules Summary
Rule	
Rule Index	0
Active	○ Yes ● No
Destination IPv4/IPv6 Address	
Destination Subnet Mask / IPv6 Prefix	
Destination Port Range	~
Source IPv4/IPv6 Address	
Source Subnet Mask / IPv6 Prefix	
Source Port Range	~
Protocol ID	
Priority	

Save Delete

Rule

You can set 16 different QoS rules. Each QoS rule has its detail setting conditions like: Physical Ports, IP, Port, Protocol, etc, you can modify the value to any new one you wish. Please notice that only when the packet fulfill every detail setting conditions here, then this packet will be remarked as the priority queue of each rule. The non-selected setting part will be treated as “don’t care” and the system will not handle this setting part.

Rule: Select 16 different rules, each rule’s detail can be set and saved.

Active: Select whether to activate the rule.

Destination IPv4/IPv6: Set the IPv4/IPv6 address that you want to filter on destination side.

Destination Subnet Mask / IPv6 Prefix: Specify the Destination Subnet Mask for IPv4 or prefix for IPv6.

Destination Port Range: Set the port range value that you want to filter on destination side.

Source IPv4/IPv6 Address: Set the IP address value that you want to filter on source side in IPv4 or IPv6.

Source Subnet Mask / IPv6 Prefix: Specify the Source Subnet Mask for IPv4 or prefix for IPv6.

Source Port Range: Set the port range value that you want to filter on source side.

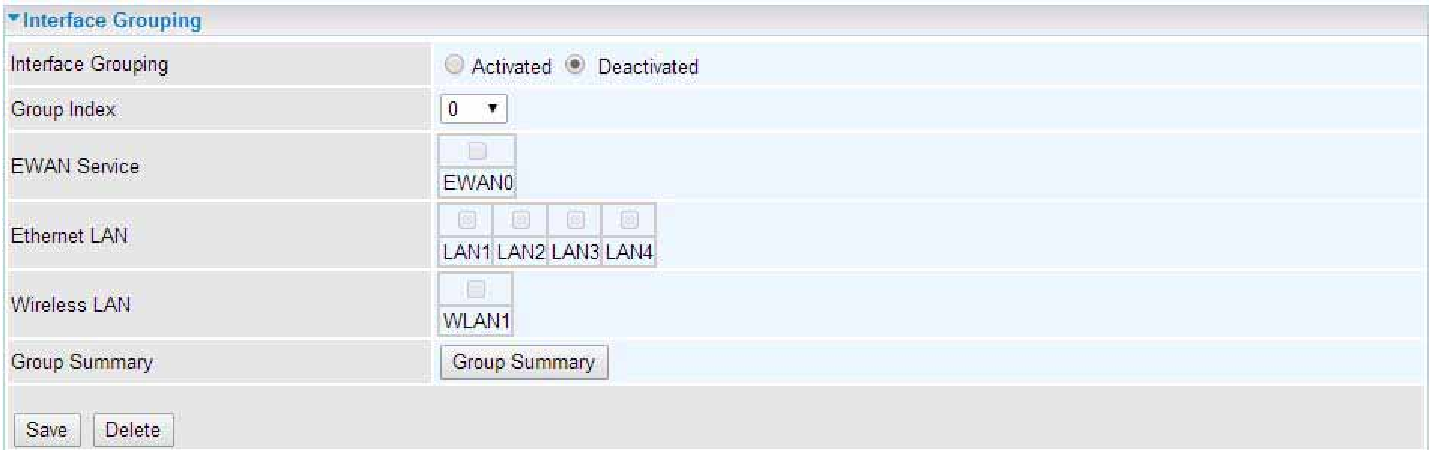
Protocol ID: Set the protocol ID type of packets that you want to filter (TCP, UDP, ICMP, and IGMP).

Priority: Select to prioritize the traffic which the rule categorizes, High or Low.

Interface Grouping

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

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



▾Interface Grouping

Interface Grouping	○ Activated ● Deactivated
Group Index	0 ▾
EWAN Service	□ EWAN0
Ethernet LAN	□ LAN1 □ LAN2 □ LAN3 □ LAN4
Wireless LAN	□ WLAN1
Group Summary	Group Summary

Interface Grouping: Select **Yes** to enable Interface Grouping feature.

Group Index: The index number indicating the current group ranging from 0 to 15.

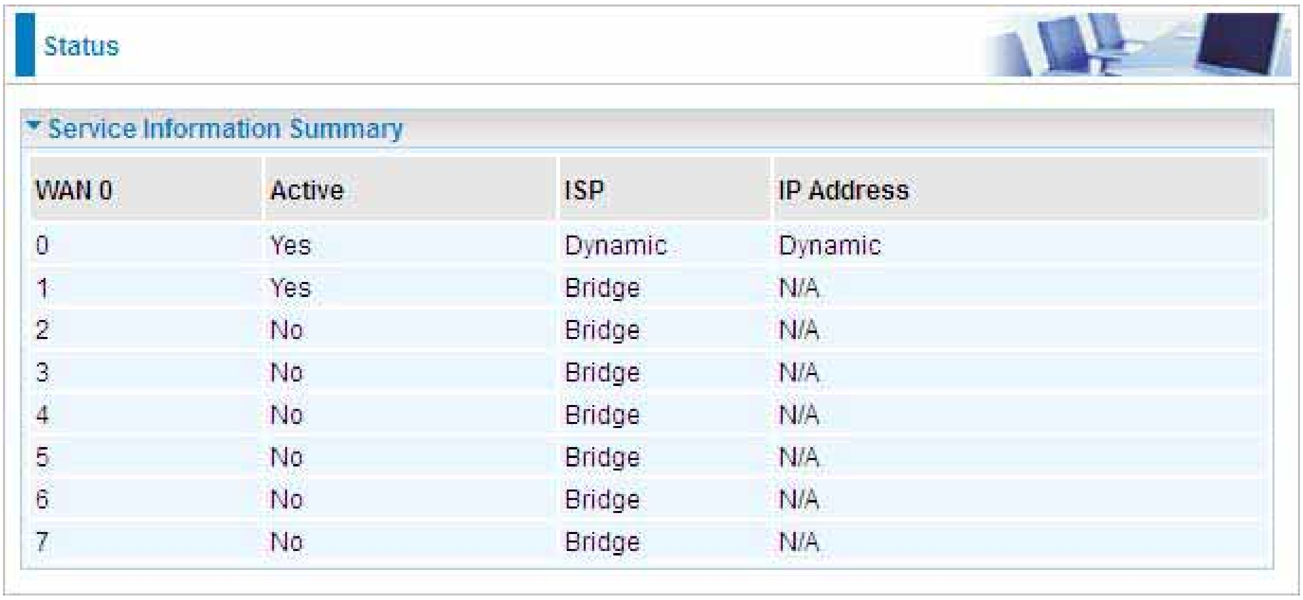
EWAN Service: The available EWAN interface. Move to Interface Setup to add other EWAN interface.

Ethernet LAN: The available Ethernet ports.

Wireless LAN: The available wireless port(s).

Group Summary: Press **PortBinding Summary** to check the current group information.

Example: Create two EWAN services, Service0 (PPPoE) and Service1 (Bridge).



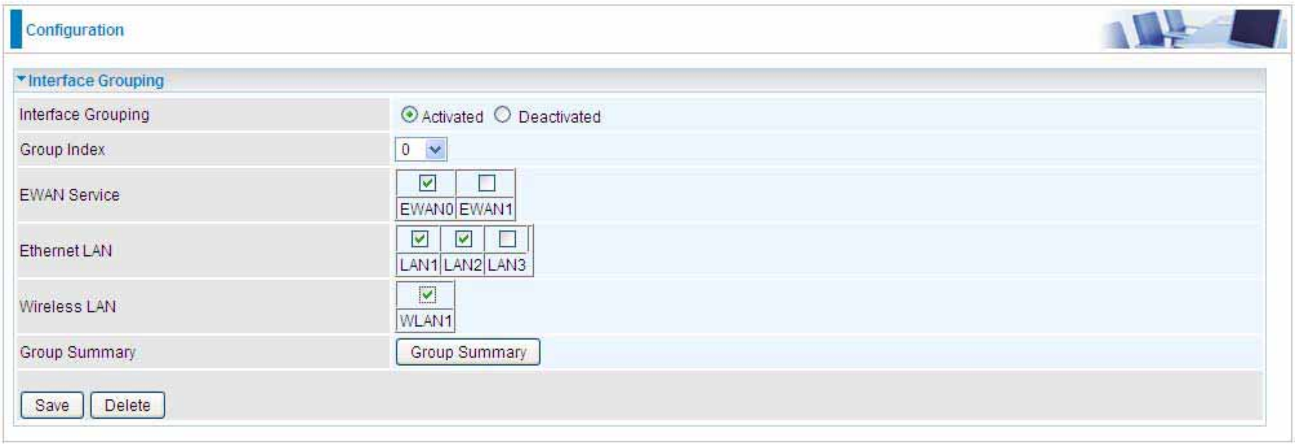
Status

Service Information Summary

WAN 0	Active	ISP	IP Address
0	Yes	Dynamic	Dynamic
1	Yes	Bridge	N/A
2	No	Bridge	N/A
3	No	Bridge	N/A
4	No	Bridge	N/A
5	No	Bridge	N/A
6	No	Bridge	N/A
7	No	Bridge	N/A

You are going to group the ports and services into two working group, as shown below.

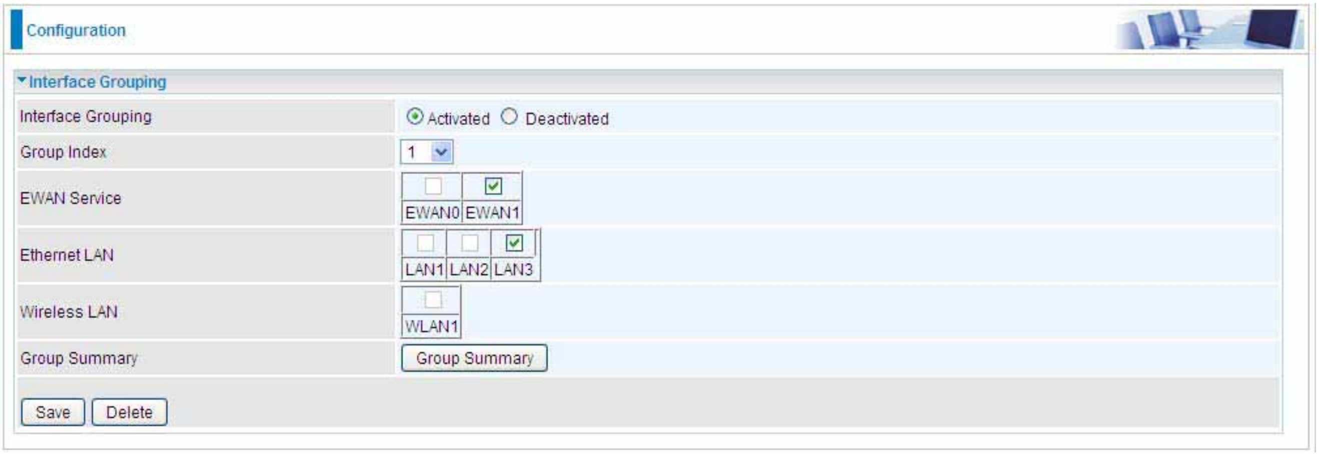
Group Index	Group Port
0	EWAN0,LAN1, LAN2, WLAN1
1	EWAN1, LAN3



Configuration

Interface Grouping

Interface Grouping	● Activated ○ Deactivated
Group Index	0
EWAN Service	☑ EWAN0 □ EWAN1
Ethernet LAN	☑ LAN1 ☑ LAN2 □ LAN3
Wireless LAN	☑ WLAN1
Group Summary	Group Summary

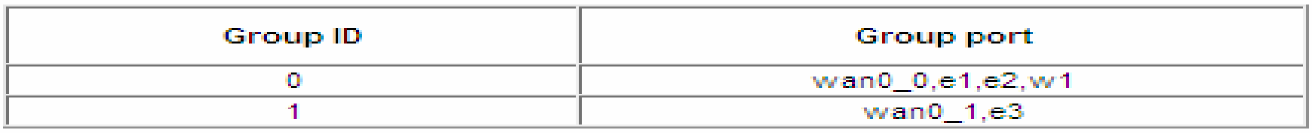


Configuration

Interface Grouping

Interface Grouping	● Activated ○ Deactivated
Group Index	1
EWAN Service	□ EWAN0 ☑ EWAN1
Ethernet LAN	□ LAN1 □ LAN2 ☑ LAN3
Wireless LAN	□ WLAN1
Group Summary	Group Summary

Click **Group Summary** to show the configuration results.

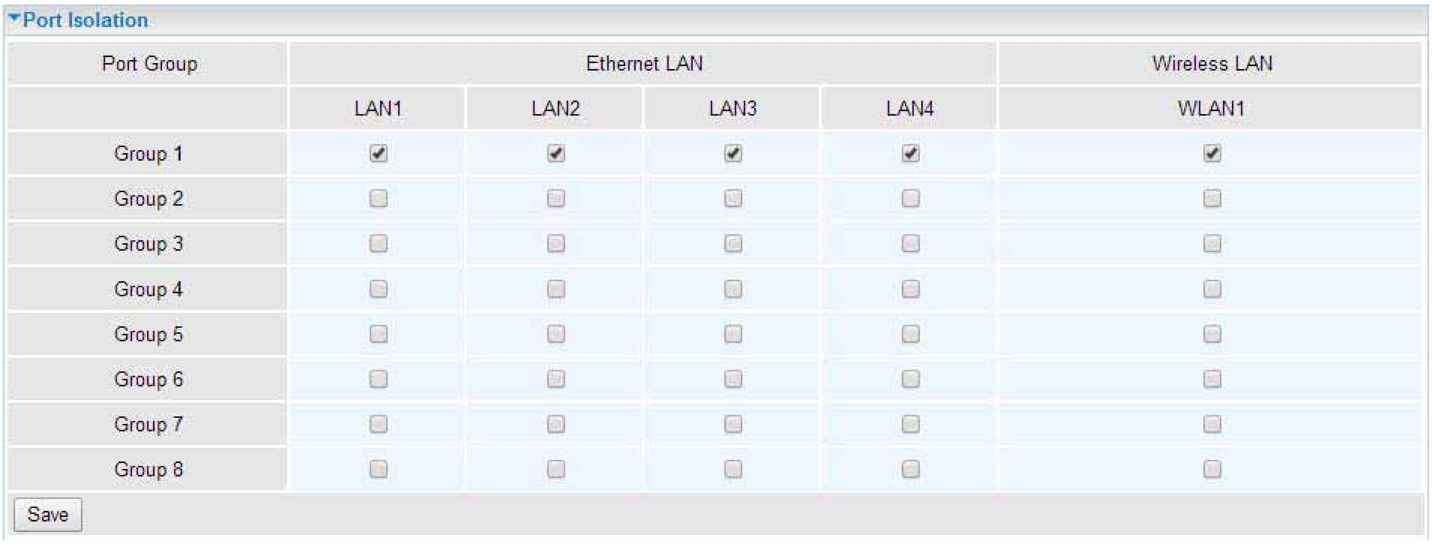


Group ID	Group port
0	wan0_0,e1,e2,w1
1	wan0_1,e3

Port Isolation

Port isolation is to prevent LAN (Wired or Wireless) devices, e.g. PC, Notebook, to associate or communicate with each other devices. By default, all ports (LAN port and WLAN port) are sharing one group, and devices in all these ports can have access to each other.

NOTE: The maximum WLAN (Wireless SSID) is up to 4. By default, only a SSID is being activated.

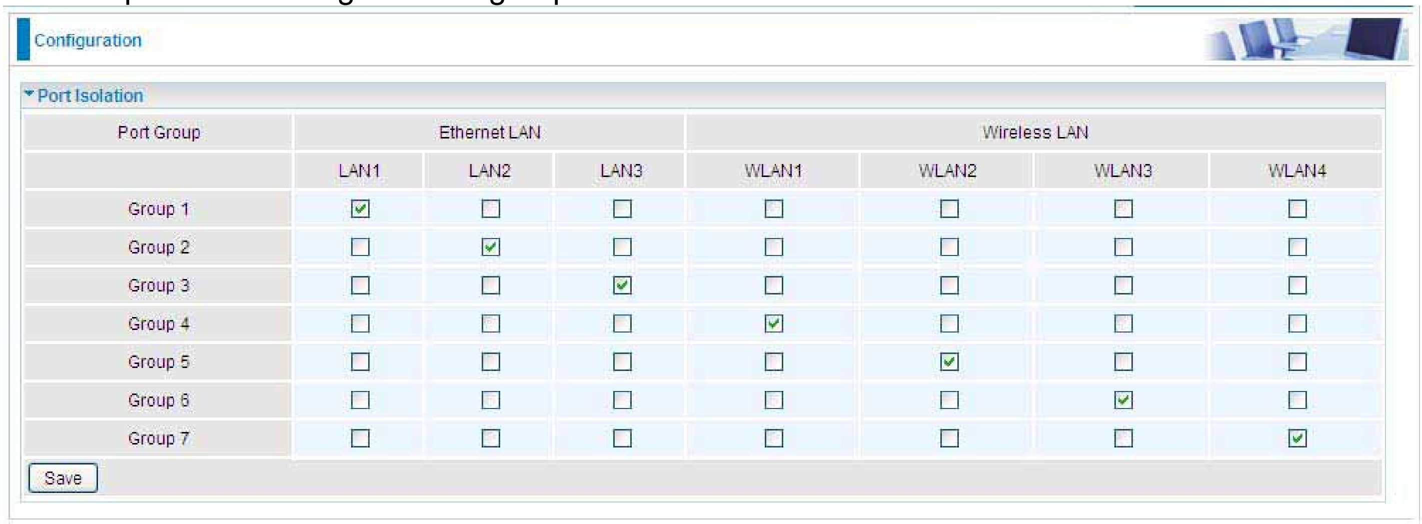


Port Isolation

Port Group	Ethernet LAN				Wireless LAN
	LAN1	LAN2	LAN3	LAN4	WLAN1
Group 1	☑	☑	☑	☑	☑
Group 2	□	□	□	□	□
Group 3	□	□	□	□	□
Group 4	□	□	□	□	□
Group 5	□	□	□	□	□
Group 6	□	□	□	□	□
Group 7	□	□	□	□	□
Group 8	□	□	□	□	□

Save

The most typical one example is to isolate all port from each other shown below. Each port has its own group; under this circumstance, devices connected to each port have no access to other devices connected to other ports. This is a special example, and users can change the settings to determine how the ports are belonged to the group.



Configuration

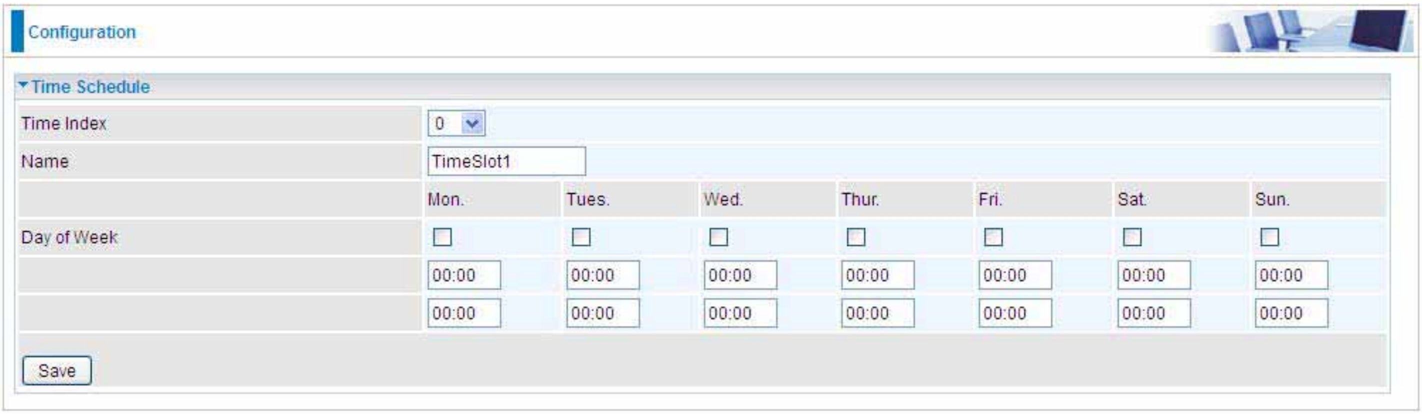
Port Isolation

Port Group	Ethernet LAN			Wireless LAN			
	LAN1	LAN2	LAN3	WLAN1	WLAN2	WLAN3	WLAN4
Group 1	☑	□	□	□	□	□	□
Group 2	□	☑	□	□	□	□	□
Group 3	□	□	☑	□	□	□	□
Group 4	□	□	□	☑	□	□	□
Group 5	□	□	□	□	☑	□	□
Group 6	□	□	□	□	□	☑	□
Group 7	□	□	□	□	□	□	☑

Save

Time Schedule

The Time Schedule supports up to **16** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.
This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.

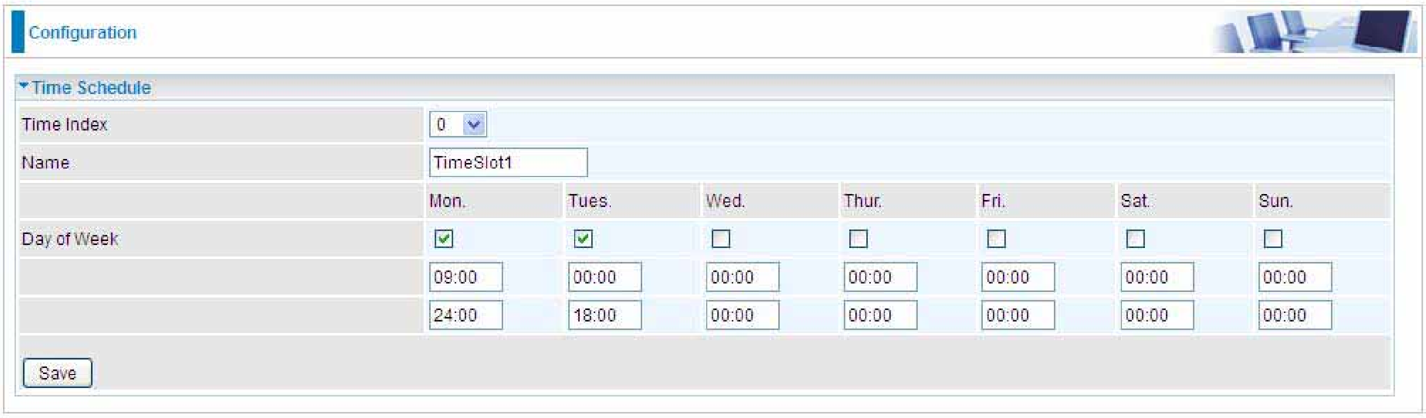


Time Index	0						
Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	□	□	□	□	□	□	□
	00:00	00:00	00:00	00:00	00:00	00:00	00:00
	00:00	00:00	00:00	00:00	00:00	00:00	00:00

Time Index: The rule index (0-15) for identifying each timeslot.

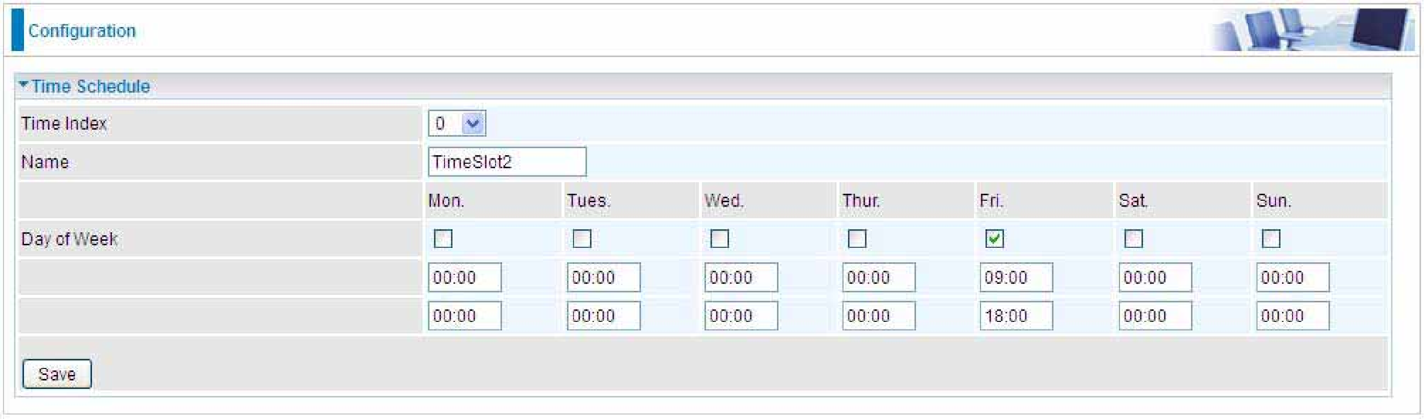
Name: User-defined identification for each time period.

Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week". For example, user can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.



Time Index	0						
Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	☑	☑	□	□	□	□	□
	09:00	00:00	00:00	00:00	00:00	00:00	00:00
	24:00	18:00	00:00	00:00	00:00	00:00	00:00

Another TimeSlot2 spanning from 09:00 to 18:00 of Friday



Time Index	0						
Name	TimeSlot2						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	□	□	□	□	☑	□	□
	00:00	00:00	00:00	00:00	09:00	00:00	00:00
	00:00	00:00	00:00	00:00	18:00	00:00	00:00

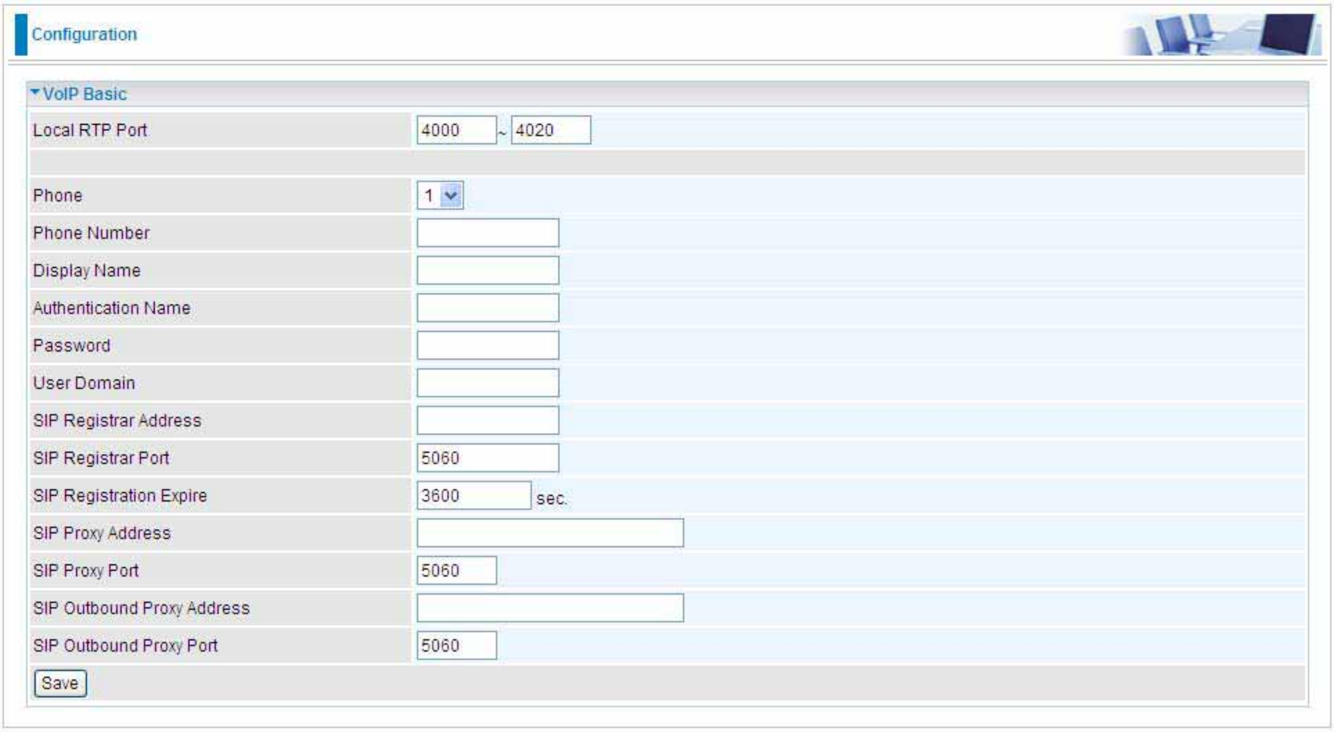
VoIP

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

This section covers **Basic**, **Media**, **Advanced**, **Speed Dial**, and **Call Features** of VoIP.

Basic

Register to a SIP service provider is an essential step before making the VoIP call. You can find out this information from your SIP service provider.



Configuration

▾VoIP Basic

Local RTP Port	4000 ~ 4020
Phone	1
Phone Number	
Display Name	
Authentication Name	
Password	
User Domain	
SIP Registrar Address	
SIP Registrar Port	5060
SIP Registration Expire	3600 sec.
SIP Proxy Address	
SIP Proxy Port	5060
SIP Outbound Proxy Address	
SIP Outbound Proxy Port	5060

Locale RTP Port: Set the local RTP port range used to receive voice packet. This setting applies to both the phone ports, Phone_1 and Phone_2, and these phone ports share the same local RTP port.

Phone: Select "1", the following parameters will be applicable to Phone1. In BiPAC 6300VNP, Phone_1 and Phone_2 are allowed to be of different characteristics, including different SIP registrar. You need to configure individually for phone1 and phone 2 and can have up to 2 different VoIP accounts.

Phone Number: Set your phone number or outgoing call number, which is usually obtained when registering in your ITSP. It is used for destination to identify which this call is made from.

Display Name: A user-friendly display name for the phone number to be easily identified.

Authentication Name: Set the account used to register, usually the Phone Number.

Password: Set the registering account password.

User Domain: Set the SIP Registrar Domain name you are going to register to, usually just the SIP registrar address.

SIP Registrar Address: Enter the SIP registrar address where offers the service of registering the VoIP account. It is definitely a VoIP server.

SIP Registrar Port: Type the port; it will listen to register requests from VoIP devices.

SIP Registration Expire: Set the time interval. The device can update (usually re-login the account) the VoIP account information with the SIP server very the time interval.

SIP Proxy Address: Enter the SIP proxy address provided by your ITSP. When destination and source phones are not sharing the same SIP registrar domain, the SIP proxy is needed to deliver call information and make the communication through.

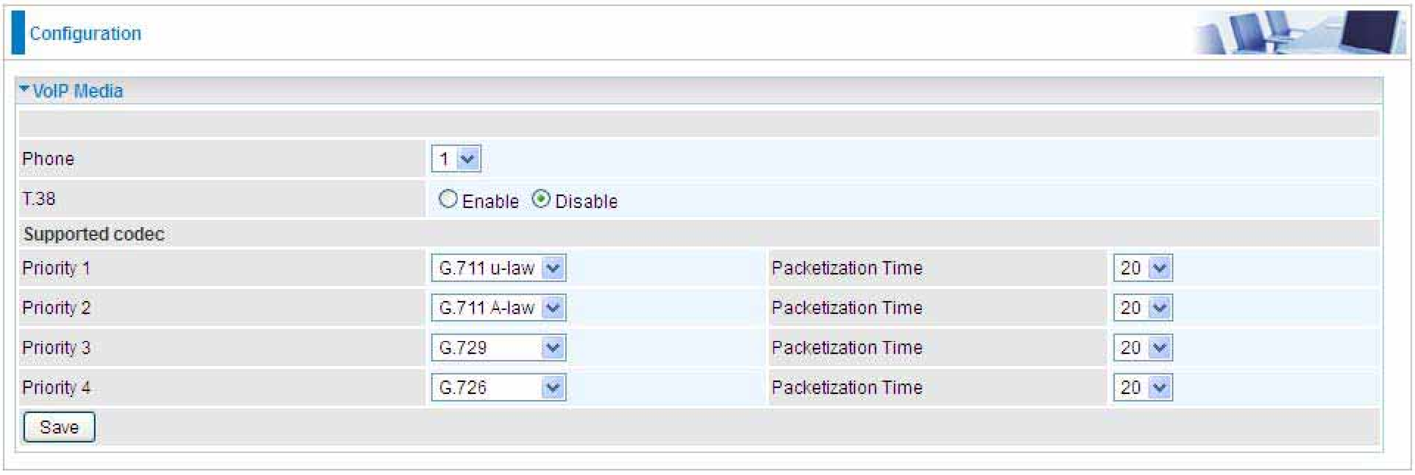
SIP Proxy Port: Set the SIP proxy port.

SIP Outbound Proxy Address: Set the SIP outbound proxy address. It is usually used to realize the communication between two phones when at least one of them is located behind a NAT router.

SIP Outbound Proxy Port: Set the SIP Outbound proxy port.

Media

Media offers for kinds of codec, G.711 u-law, G.711 A-law, G.729, G.726, from greatest to lowest in priority.



Configuration

▾VoIP Media

Phone	1		
T.38	○ Enable ● Disable		
Supported codec			
Priority 1	G.711 u-law	Packetization Time	20
Priority 2	G.711 A-law	Packetization Time	20
Priority 3	G.729	Packetization Time	20
Priority 4	G.726	Packetization Time	20

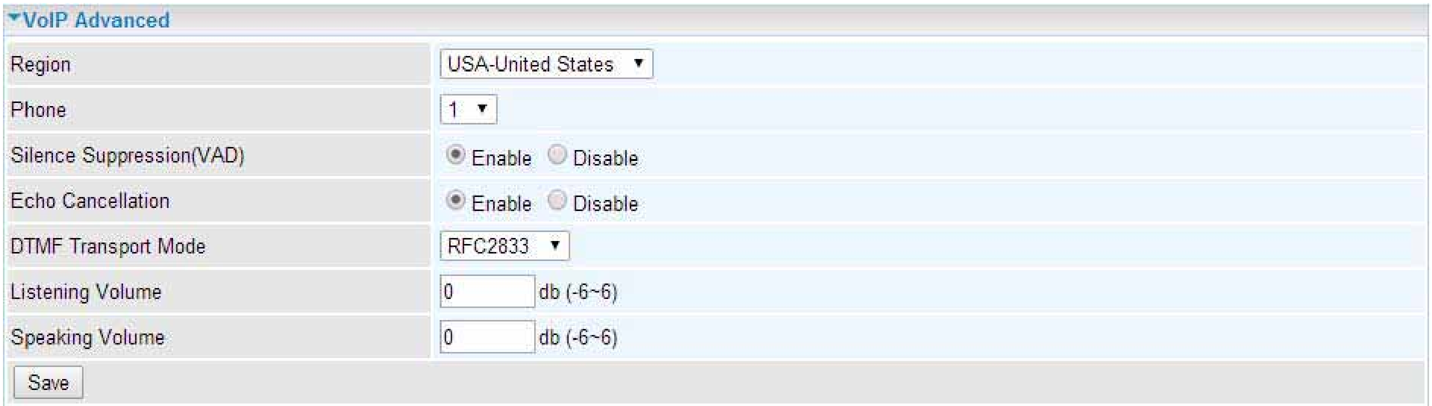
Phone: Select to set the following configurations for Phone_1 or Phone_2. When phone1 is selected, the following set media codec will be applied to phone_1.

T.38: T.38 relay is a way to permit faxes to be transported across IP networks between existing fax terminals. Click Enable to allow transmission of fax over IP network between two fax machines. If T.38 is disabled, the analog fax signal is transmitted as the normal audio data. If T.38 relay is enabled, the fax signal is converted to T.38 signal.

- **G.711u-Law:** It is a basic non-compressed encoder and decoder technique. µ-LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample.
- **G.711A-LAW:** It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample into 8-bit value.
- **G.729**: It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- **G.726:** It is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 32kbit/s.

Advanced

Advance section equipment the users with the ability to do some advanced settings to each phone port. Go on to see.



▾VoIP Advanced

Region	USA-United States ▾
Phone	1 ▾
Silence Suppression(VAD)	● Enable ○ Disable
Echo Cancellation	● Enable ○ Disable
DTMF Transport Mode	RFC2833 ▾
Listening Volume	0 db (-6~6)
Speaking Volume	0 db (-6~6)

Region: Select the exact region from the drop-down menu to adjust the phone custom in the exact region, like ring tone, busy tone, dial tone, etc, as different regions may have different phone using traditions. The setting is to be applied to both phone 1 and phone 2.

Phone: Select the phone 1 or Phone 2 to have the following configurations applied to the phone.

Silence Suppression (VAD): Enable to minimize the use of bandwidth by automatically decreasing transmission of background noise when the device detects on voice input by the user on the phone.

Echo Cancellation: Enable to cancel echo for the other side in communication so as to make a clear listening environment. In order to avoid the other side in communication hearing the echo, please enable echo cancellation.

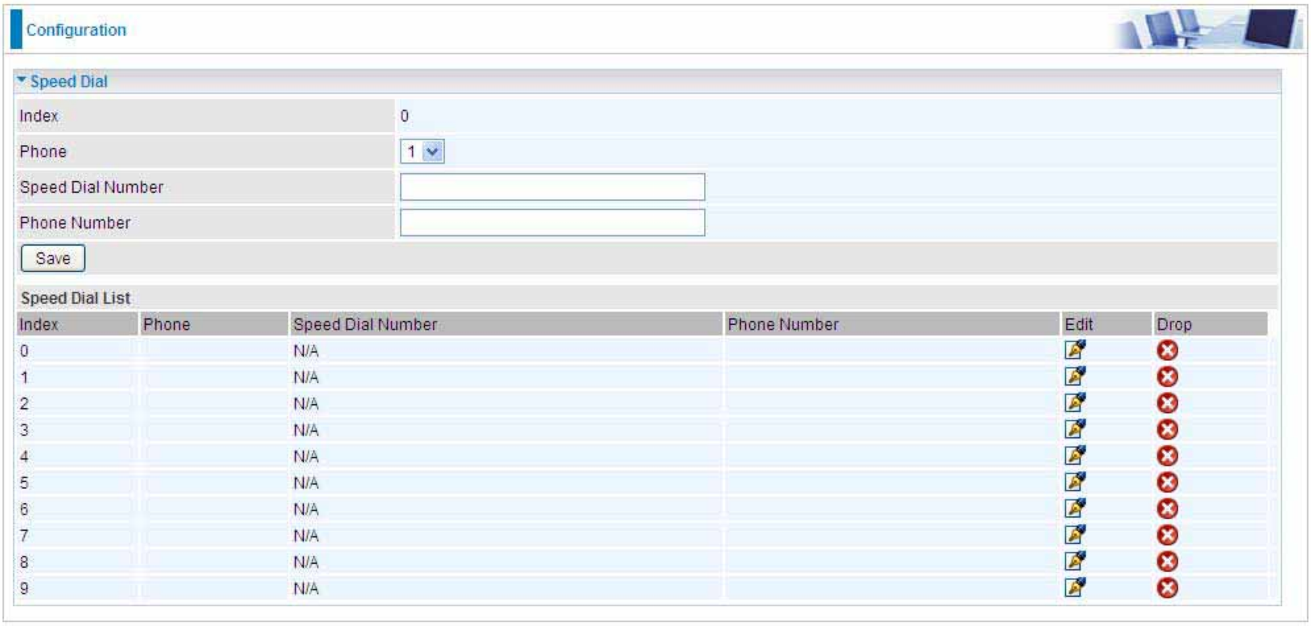
DTMF Transport Mode: Select the DTMF mode.

Listening Volume: Adjust the volume of listener, -6 to 6, from lowest to highest.

Speaking Volume: Adjust the volume of microphone; -6 to 6, from lowest to highest.

Speed Dial

Speed Dial comes at hand to store frequently used telephone number(s) that you can press set ‘speed dial number’ instead of the exact dialing-out number on the phone keyboard to make a quick dialing.



Configuration

Speed Dial

Index	0
Phone	1
Speed Dial Number	
Phone Number	

Save

Speed Dial List

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0		N/A		✎	✖
1		N/A		✎	✖
2		N/A		✎	✖
3		N/A		✎	✖
4		N/A		✎	✖
5		N/A		✎	✖
6		N/A		✎	✖
7		N/A		✎	✖
8		N/A		✎	✖
9		N/A		✎	✖

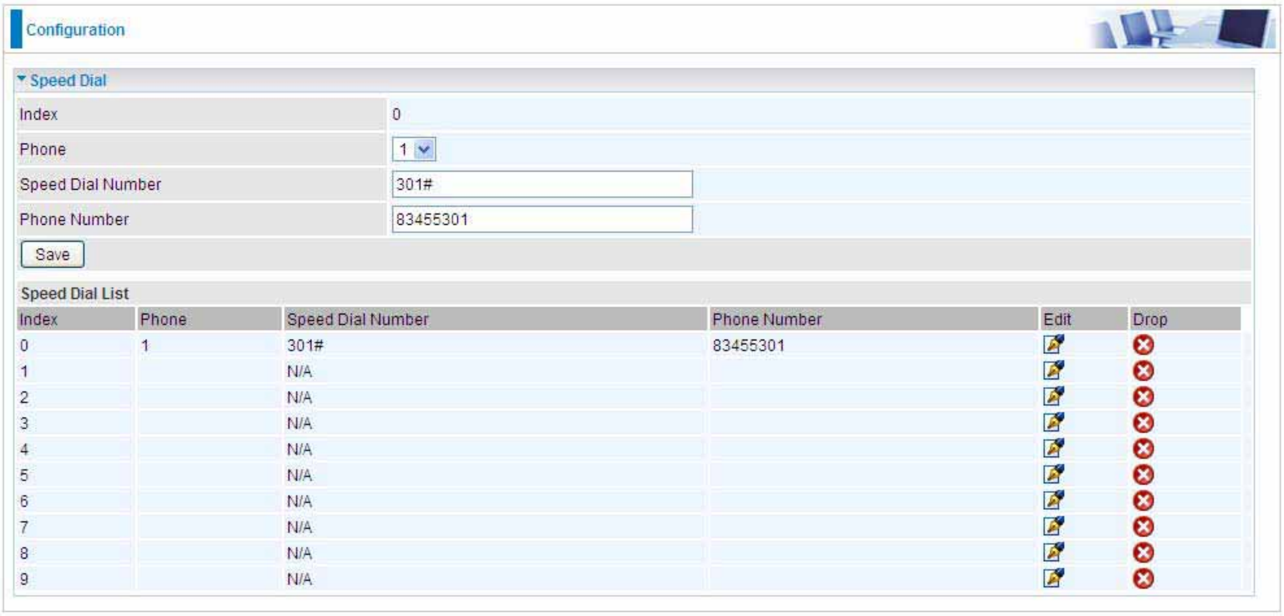
Index: The index to mark the speed dial number mapping, 0-9.

Phone: Select Phone 1 or Phone 2 to have your set speed dial number applied to the phone. If phone 1 is selected, your set speed dial number is about to be applied to phone 1.

Speed Dial Number: Set an easily remembered and simple number to replace the Phone number, it can be a sequence in varying length from 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 *. #, but note * or # must be included in the sequence.

Phone Number: The complete destination number

Example: Save phone number 83455301 to the speed dial list.



Configuration

Speed Dial

Index	0
Phone	1
Speed Dial Number	301#
Phone Number	83455301

Save

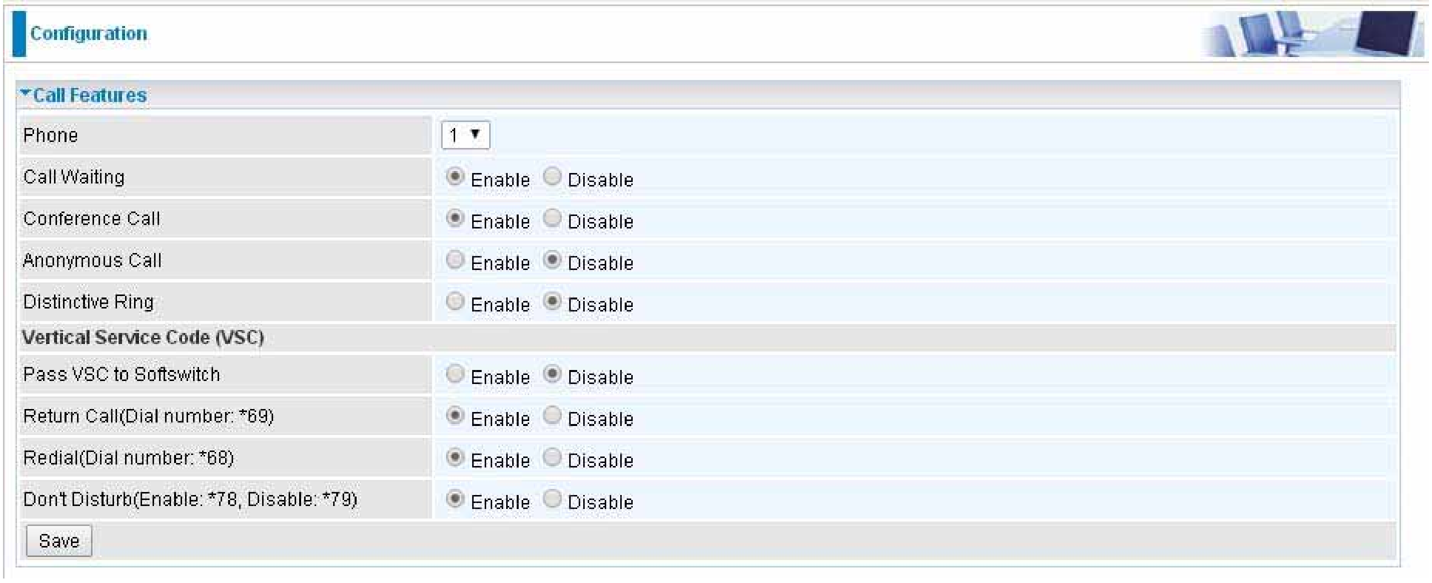
Speed Dial List

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0	1	301#	83455301	✎	✖
1		N/A		✎	✖
2		N/A		✎	✖
3		N/A		✎	✖
4		N/A		✎	✖
5		N/A		✎	✖
6		N/A		✎	✖
7		N/A		✎	✖
8		N/A		✎	✖
9		N/A		✎	✖

When you want call 83455301 through phone 1, you can simply dial 301# to make your desired call.

Call Features

Call Features provides users with some advanced phone characteristics, including Call waiting, Conference Call, etc.



Configuration

▾Call Features

Phone	1 ▼
Call Waiting	● Enable ○ Disable
Conference Call	● Enable ○ Disable
Anonymous Call	○ Enable ● Disable
Distinctive Ring	○ Enable ● Disable
Vertical Service Code (VSC)	
Pass VSC to Softswitch	○ Enable ● Disable
Return Call(Dial number: *69)	● Enable ○ Disable
Redial(Dial number: *68)	● Enable ○ Disable
Don't Disturb(Enable: *78, Disable: *79)	● Enable ○ Disable

Save

Phone: Select the phone 1 or Phone 2 to have the following characteristics applied to the phone.

Call Waiting: Enable to activate Call Waiting feature. When you are busy on a call with, for example, A, and another call comes in, B, while the Call Waiting feature is enabled, you can hear a hint sound indicating there is another call in for you to decide to answer B by pressing the "flash" button on the phone to keep the original call with A.

Conference Call: Enable to allow 3-way conference call. Please note, only 3 parties are allowed (device, A, and B).

Anonymous Call: This feature enables you to restrict your phone number from displaying to the called party. When enabled, your phone number will be withheld and not be revealing to the called party.

Distinctive Ring: This call feature is only available from a VoIP Service Provider which enables each telephone number to have a distinctive ring sound.

Note: Before enabling this feature, please consult with your VoIP Service Provide to be sure it can be supported.

There is a ringtone list available in the BiPAC 6300VNP, after enabling this feature, your BiPAC 6300VNP will adapt a specific ring pattern on the list requested by your VoIP Service Provider for a specific telephone number.

When it is being disabled, all income calls will adapt the default ringtone for all telephone lines.

Pass VSC to Softswitch:

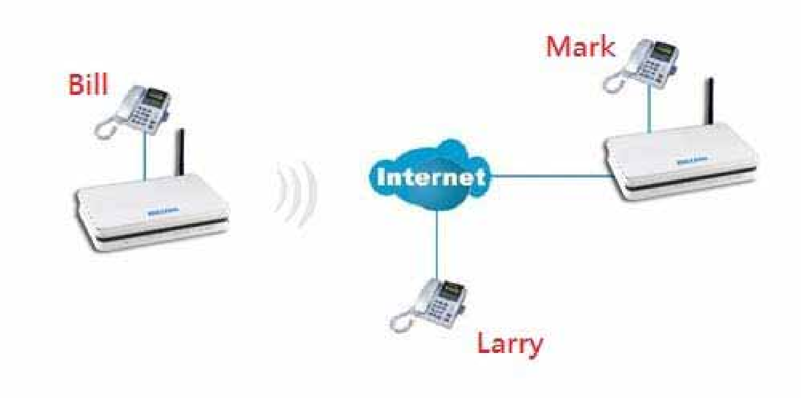
- **Enable** to pass VSC(Vertical Service Code) to the SIP server of ITSP which allows the SIP server to handle all its unique calling features such as Return Call, Call Redial, Don't Disturb, etc. Under this circumstance, users need to pay for such service, please ensure you check with your SIP provider for more information.
- **Disable** to let the BiPAC 6300VNP to handle all available call features.

Return Call (Dial number: *69): Dial *69 to redial the latest incoming call number.

Redial (Dial number: *68): Dial *68 to redial the latest outgoing call number.

Don’t Disturb (Enable: *78, Disable: *79): Press *78 to enable Don’t Disturb feature so as to make it not ring when a call comes in; while press *79 to disable Don’t Disturb feature, if a call comes with a ringing indication.

Example: How to establish 3-way conference call



Case 1: Bill and Larry are talking. Bill wants to invite Mark to join a conference call.

Step – 1: Billy and Larry are discussing on the phone. Bill tells Larry that he wants to set up a conference call with Mark.

Step – 2: Bill presses flash (hold original call), and Bill hears the dial tone.

Step – 3: Bill calls Mark. Bill and Mark are on a new call.

Step – 4: Bill tells Mark that Mark is invited to join a conference call.

Step – 5: Bill presses flash (hold new call) and return to original call.

Step – 4: Bill tells Larry that Mark is on the phone.

Step – 6: Bill presses flash again to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

Case 2: When Bill and Larry are talking on the phone, Bill received a phone call from Mark. Bill decided to ask Mark to join the conference call.

Step – 1: Bill and Larry on a call, then Mark dials Bill and Bill hears a waiting tone.

Step – 2: Bill presses flash and picks up the call waiting call.

Step – 3: Bill tells Mark that he and Larry are talking on the phone; they can have a conference call.

Step – 4: Bill presses flash to hold the call with Mark and return to original call with Larry.

Step – 5: Bill tells Larry that it is Mark and he wants to set up a conference with Mark.

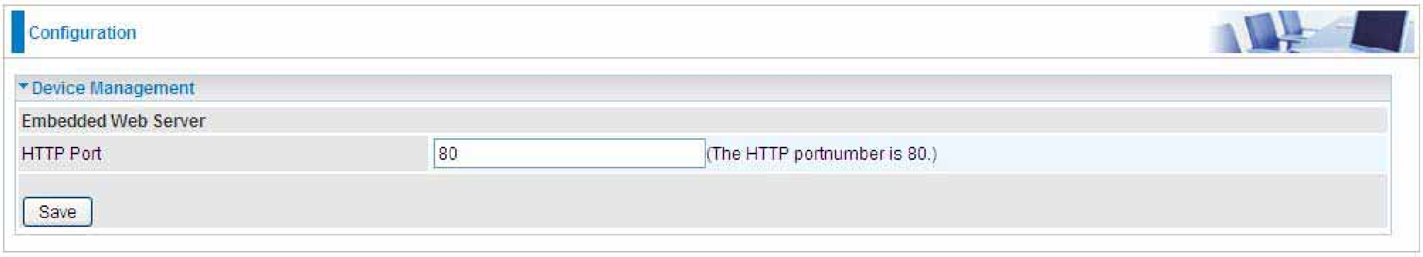
Step – 6: Bill presses flash again to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

Access Management

Device Management

Device management offers users a way to change the embedded web server accessing port, default 80. User can change the http port to 8080 or something else here.

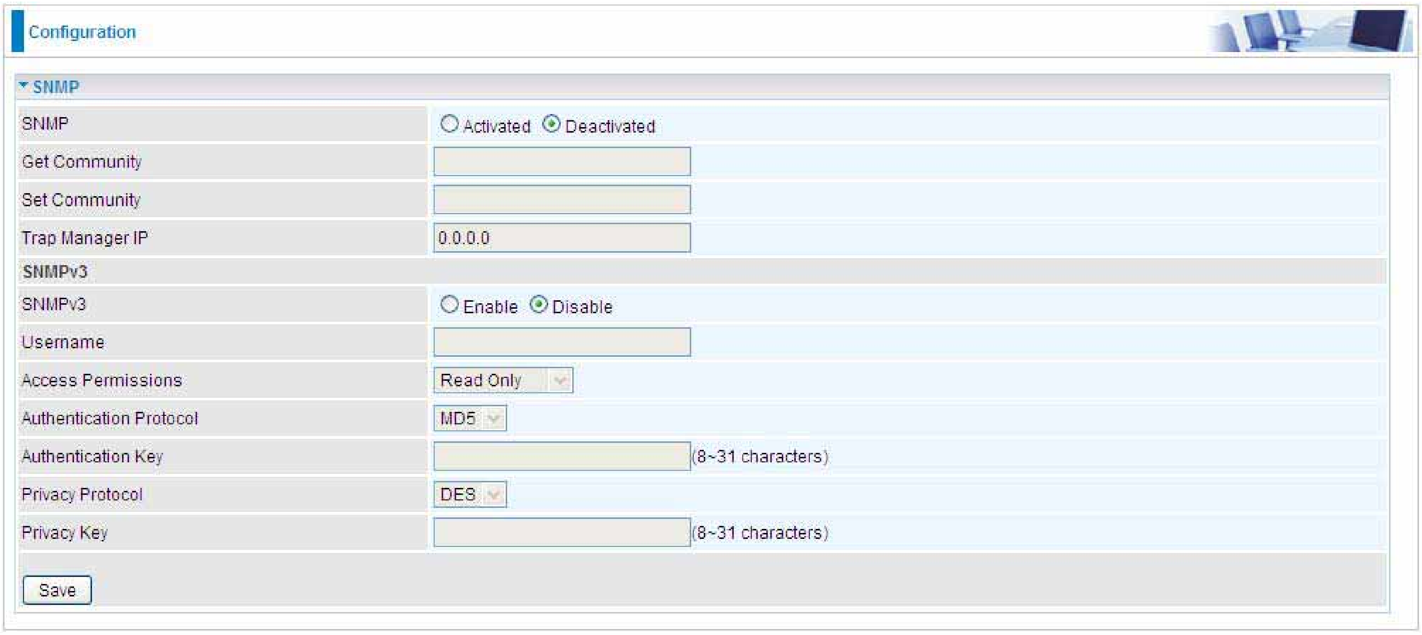


Embedded Web Server

HTTP Port	80 (The HTTP portnumber is 80.)

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BiPAC 6300VNP serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.



▾ SNMP

SNMP	○ Activated ● Deactivated
Get Community	
Set Community	
Trap Manager IP	0.0.0.0
SNMPv3	
SNMPv3	○ Enable ● Disable
Username	
Access Permissions	Read Only
Authentication Protocol	MD5
Authentication Key	(8~31 characters)
Privacy Protocol	DES
Privacy Key	(8~31 characters)

SNMP: Select to enable SNMP feature.

Get Community: Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Trap Manager IP: Enter the IP of the server receiving the trap message (when some exception occurs) sent by this SNMP agent.

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Authentication Key: Set the authentication key, 8-31 characters.

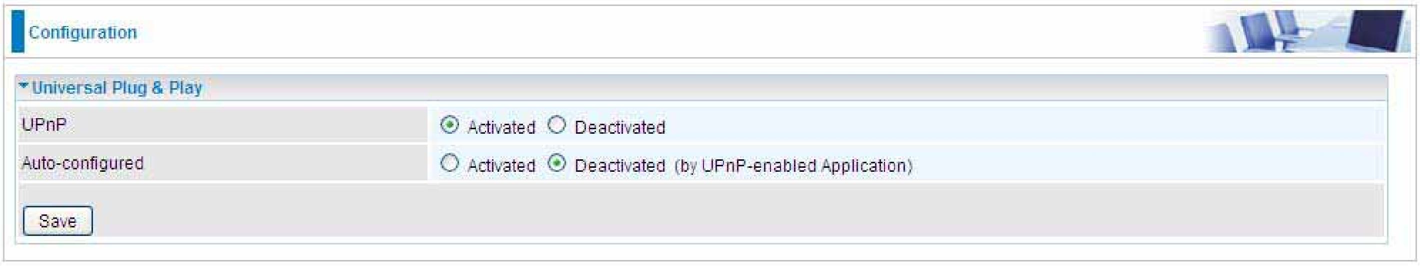
Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.

Universal Plug & Play

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

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



Configuration

▾Universal Plug & Play

UPnP	● Activated ○ Deactivated
Auto-configured	○ Activated ● Deactivated (by UPnP-enabled Application)

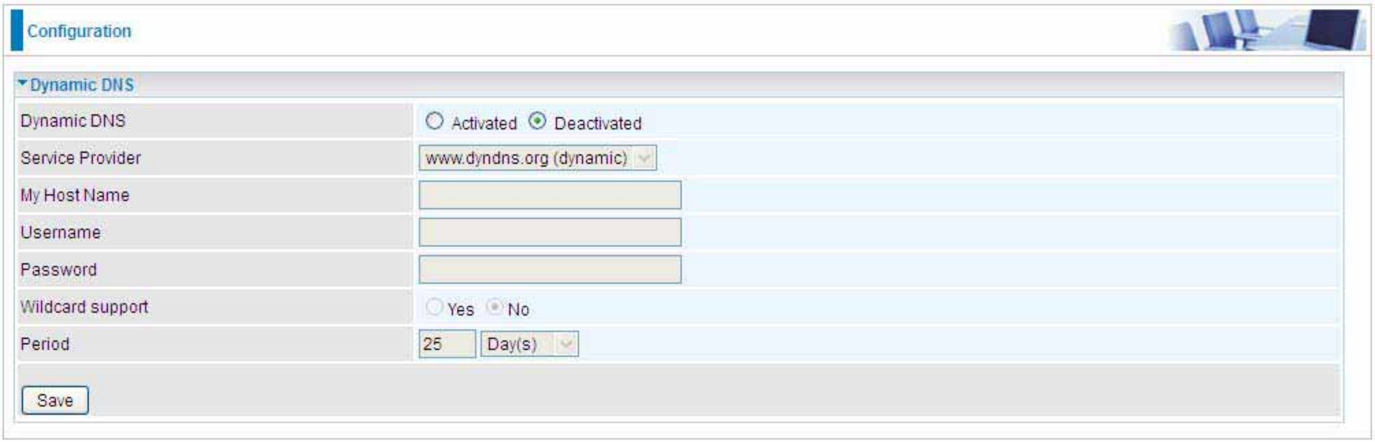
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the BiPAC 6300VNP' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BiPAC 6300VNP so that they can communicate through the BiPAC 6300VNP, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es). But note that first users have to go to the Dynamic DNS registration service provider to register an account.



Configuration

▾Dynamic DNS

Dynamic DNS	○ Activated ● Deactivated
Service Provider	www.dyndns.org (dynamic)
My Host Name	
Username	
Password	
Wildcard support	○ Yes ● No
Period	25 Day(s)

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your BiPAC 6300VNP by your Dynamic DNS provider.

Username: Type your user name.

Password: Type the password.

Wildcard support: Select this check box to enable DYNDNS Wildcard.

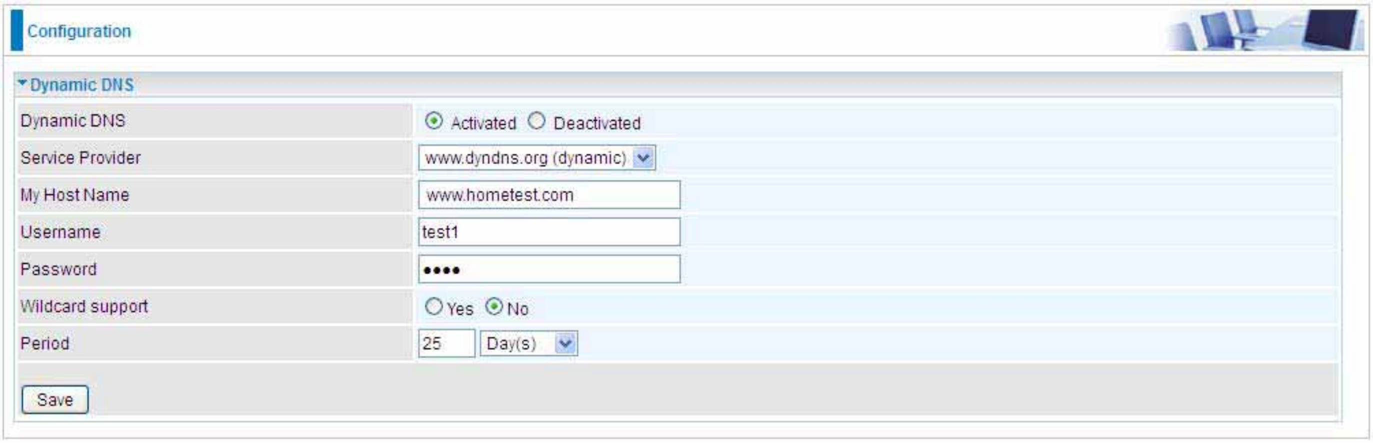
Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Example: How to register a DDNS account

Note first users have to go to the Dynamic DNS registration service provider to register an account.

User ***test1*** register a Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

DDNS: www.hometest.com using username/password test/test

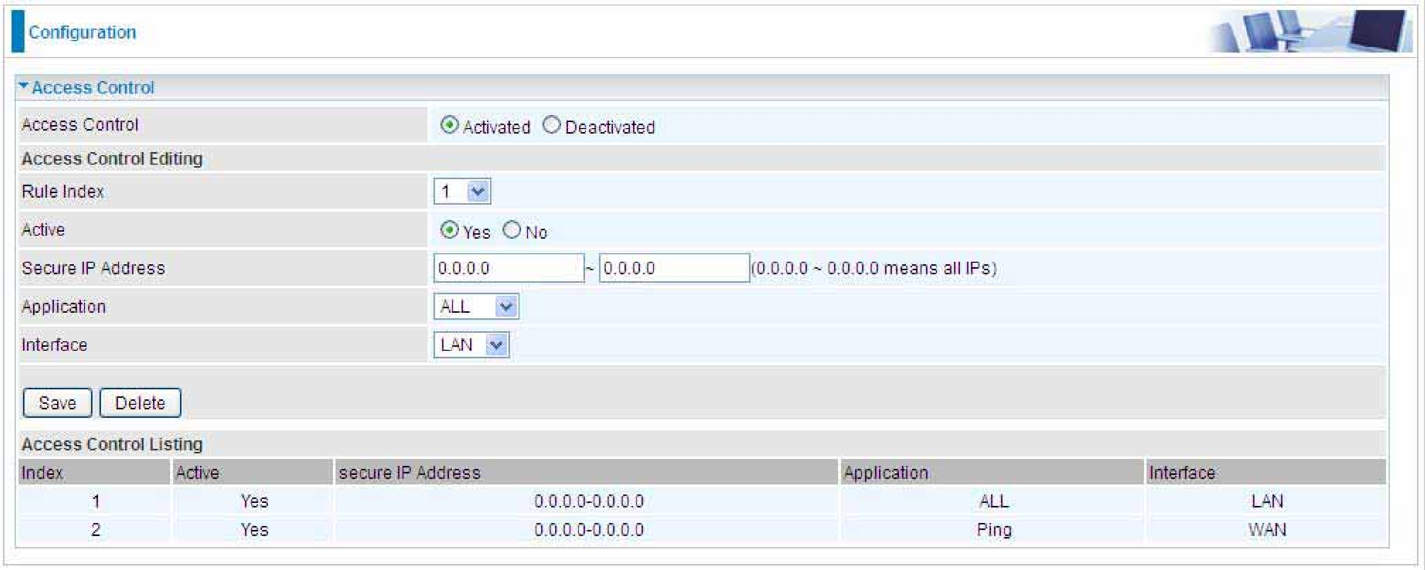


Dynamic DNS	● Activated ○ Deactivated
Service Provider	www.dyndns.org (dynamic)
My Host Name	www.hometest.com
Username	test1
Password	••••
Wildcard support	○ Yes ● No
Period	25 Day(s)

Access Control

Access Control Listing allows you to determine which services/protocols can access BiPAC 6300VNP interface from which computers. It is a management tool aimed to allow IPs (set in secure IP address) to access specified embedded applications (Web, etc, user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is 16.



Configuration

▾Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	1
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL
Interface	LAN

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Select whether to make Access Control function available.

Rule Index: This is item number

Active: Select to activate the rule.

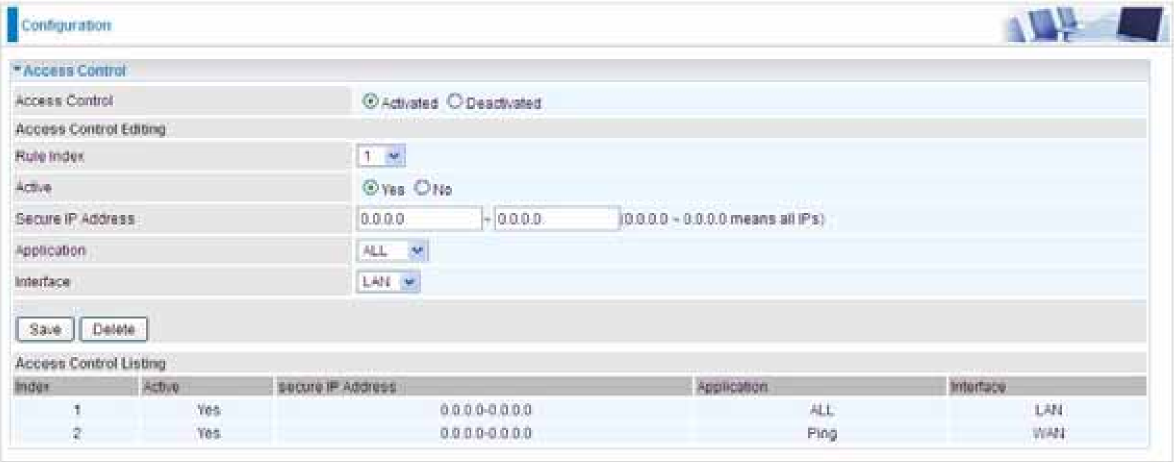
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BiPAC 6300VNP. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN** and **Both**.

By default, the “Access Control” has **two default rules**.

Default Rule 1: (Index 1), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc). Under this situation, clients from WAN cannot access the router even from Ping.



Configuration

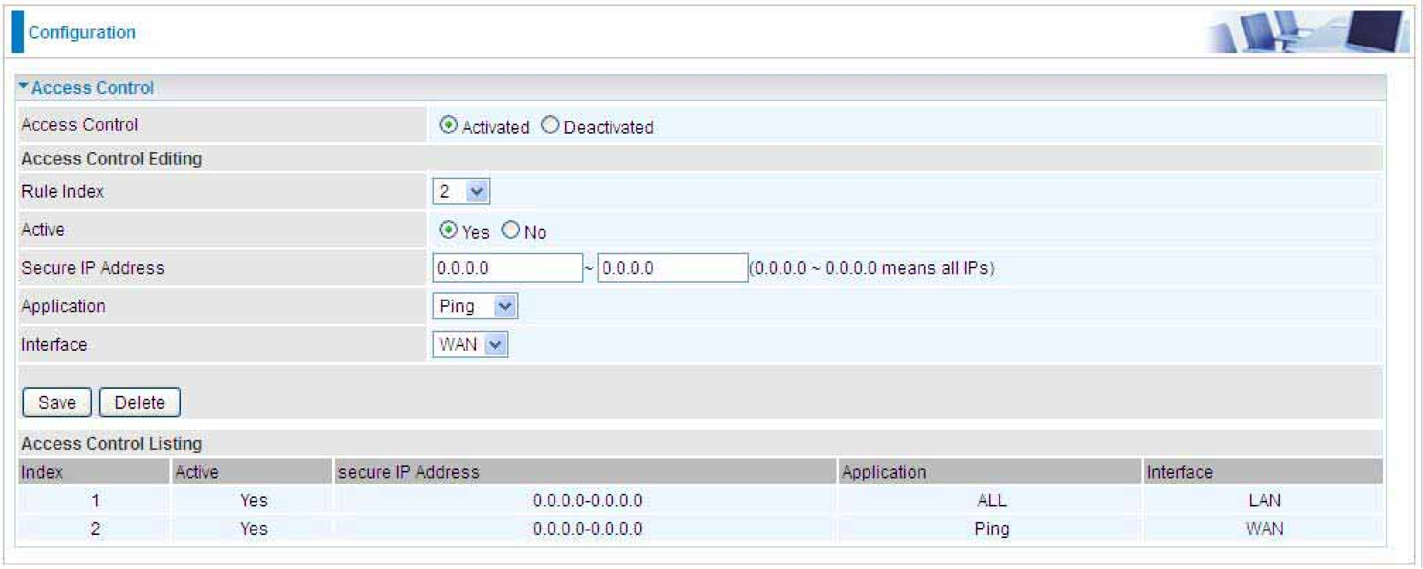
Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	1
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL
Interface	LAN

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Default Rule 2: (Index 2), an ACL rule to open Ping to WAN side.



Configuration

Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	2
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	Ping
Interface	WAN

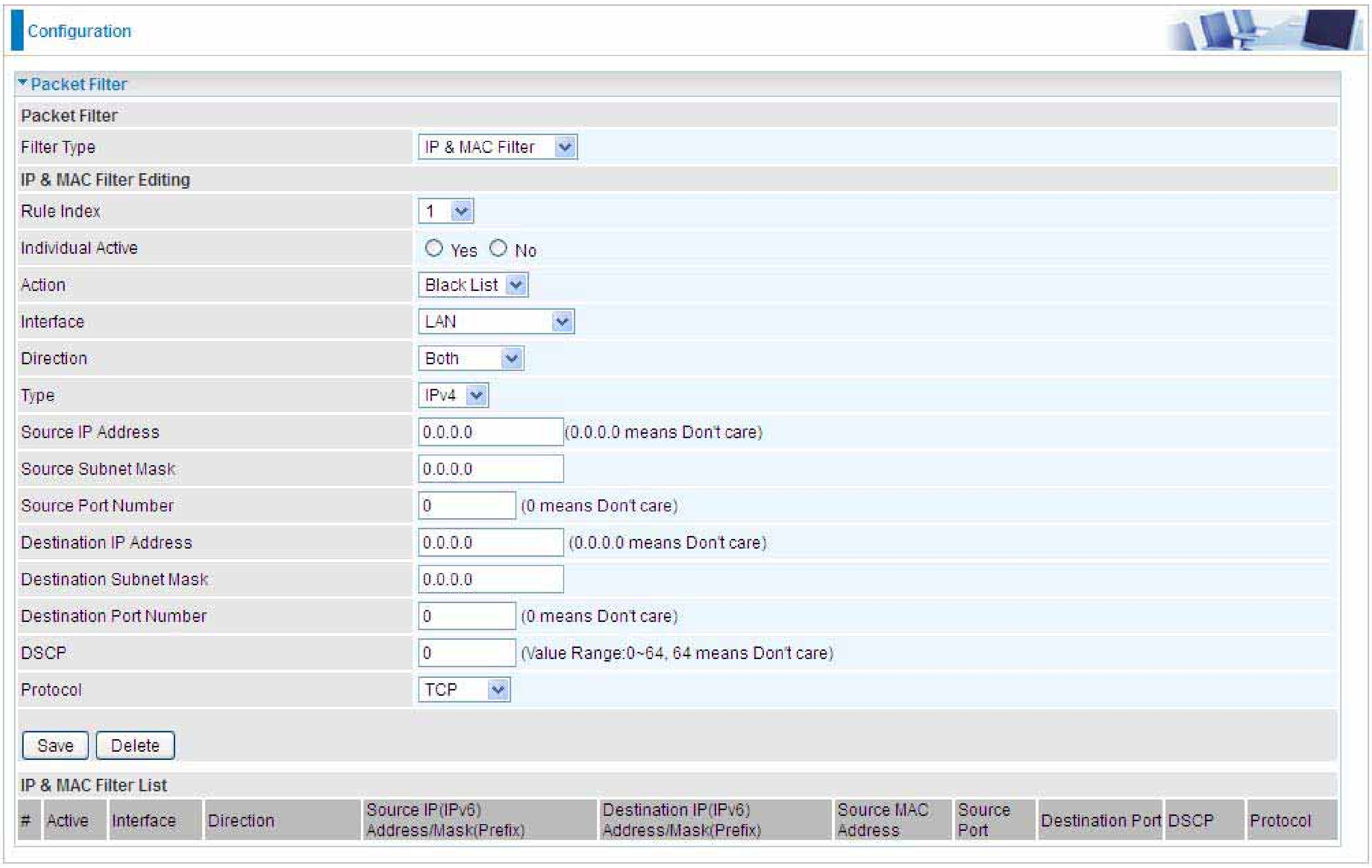
Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Packet Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

❖ Packet Filter - IP & MAC Filter



Configuration

▾ Packet Filter

Packet Filter	
Filter Type	IP & MAC Filter
IP & MAC Filter Editing	
Rule Index	1
Individual Active	○ Yes ○ No
Action	Black List
Interface	LAN
Direction	Both
Type	IPv4
Source IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0
Source Port Number	0 (0 means Don't care)
Destination IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0
Destination Port Number	0 (0 means Don't care)
DSCP	0 (Value Range:0~64, 64 means Don't care)
Protocol	TCP

Save Delete

IP & MAC Filter List

#	Active	Interface	Direction	Source IP(IPv6) Address/Mask(Prefix)	Destination IP(IPv6) Address/Mask(Prefix)	Source MAC Address	Source Port	Destination Port	DSCP	Protocol

Packet Filter

Filter Type: There are three types "**IP & MAC Filter**", "**Application Filter**", and "**URL Filter**" that user can select for this filter rule. Here we set **IP & MAC Filter**.

IP & MAC Filter Editing

Rule Index: This is item number

Individual Active: Select **Yes** to activate the rule.

Action: This is how to deal with the packets matching the rule. Allow please select White List or block selecting Black List.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select "IPv4" for IPv4 address, port number and protocol. Select "IPv6" for IPv6 address, port number and protocol. Select "MAC" for MAC address.

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Source Subnet Mask: Enter the subnet mask of the source network.

Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.

Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Destination Subnet Mask: Enter the subnet mask of the destination network.

Destination Port Number: This is the Port that defines the application. (e.g. HTTP is port 80.)

DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

IP/MAC Filter Listing

#: Item number**.**

Active: Whether the connection is currently active.

Interface: show the interface the rule applied to.

Direction: show the direction the rule applied to.

Source IP (IPv6) Address/Mask (Prefix): The source IP address or range of packets to be monitored.

Destination IP (IPv6) Address/Mask (Prefix): This is the destination subnet IP address.

Source MAC Address: show the MAC address of the rule applied.

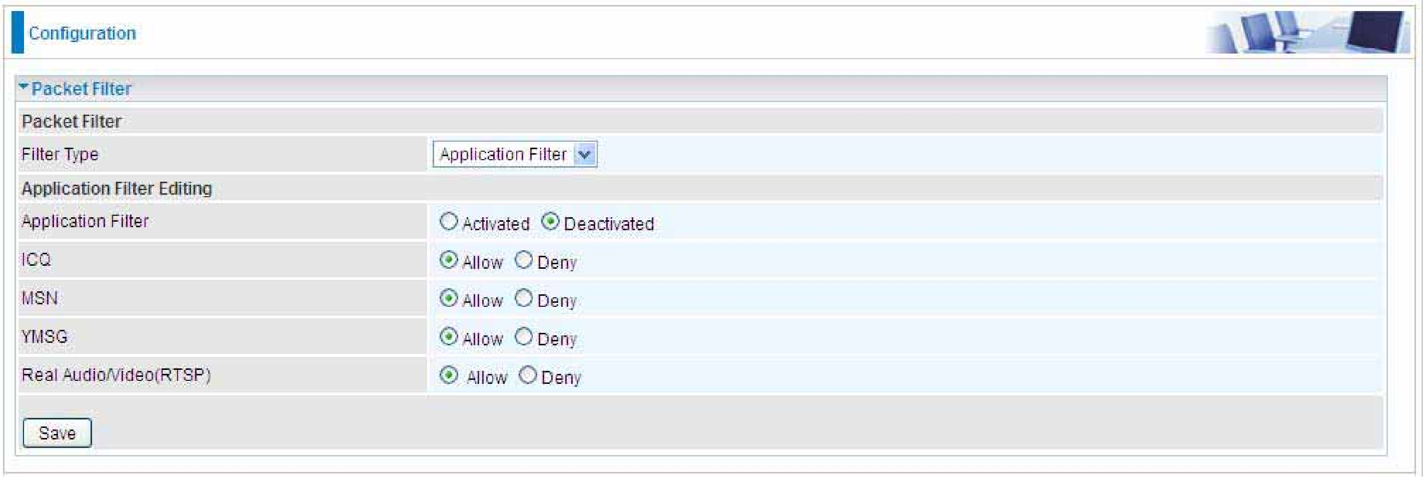
Source Port: The source port number of packets to be monitored.

Destination Port: This is the Port or Port Ranges that defines the application.

DSCP: show the set DSCP.

Protocol: It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP or ICMPv6**

❖ Packet Filter - Application Filter



Configuration

Packet Filter

Packet Filter

Filter Type	Application Filter
Application Filter Editing	
Application Filter	○ Activated ● Deactivated
ICQ	● Allow ○ Deny
MSN	● Allow ○ Deny
YMSG	● Allow ○ Deny
Real Audio/Video(RTSP)	● Allow ○ Deny

Application Filter: Select this option to Activated/Deactivated the Application filter.

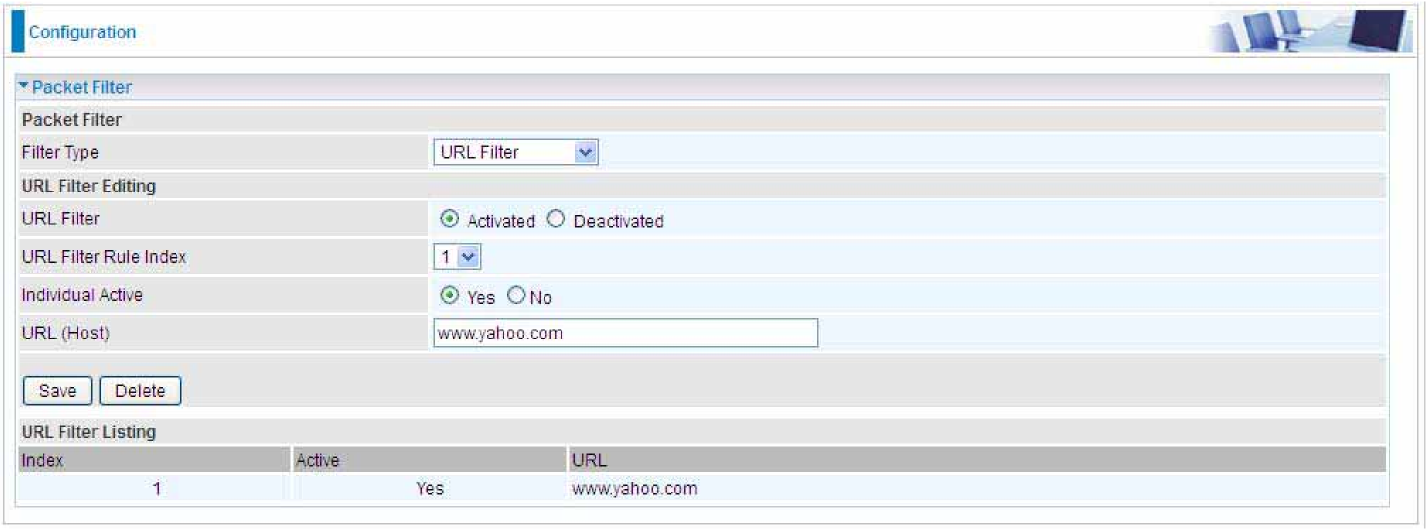
ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video (RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

❖ Packet Filter - URL Filter



Configuration

Packet Filter

Packet Filter

Filter Type	URL Filter
URL Filter Editing	
URL Filter	● Activated ○ Deactivated
URL Filter Rule Index	1
Individual Active	● Yes ○ No
URL (Host)	www.yahoo.com

URL Filter Listing

Index	Active	URL
1	Yes	www.yahoo.com

URL Filter: Select **Activated** to enable URL Filter.

URL Filter Rule Index: This is item number.

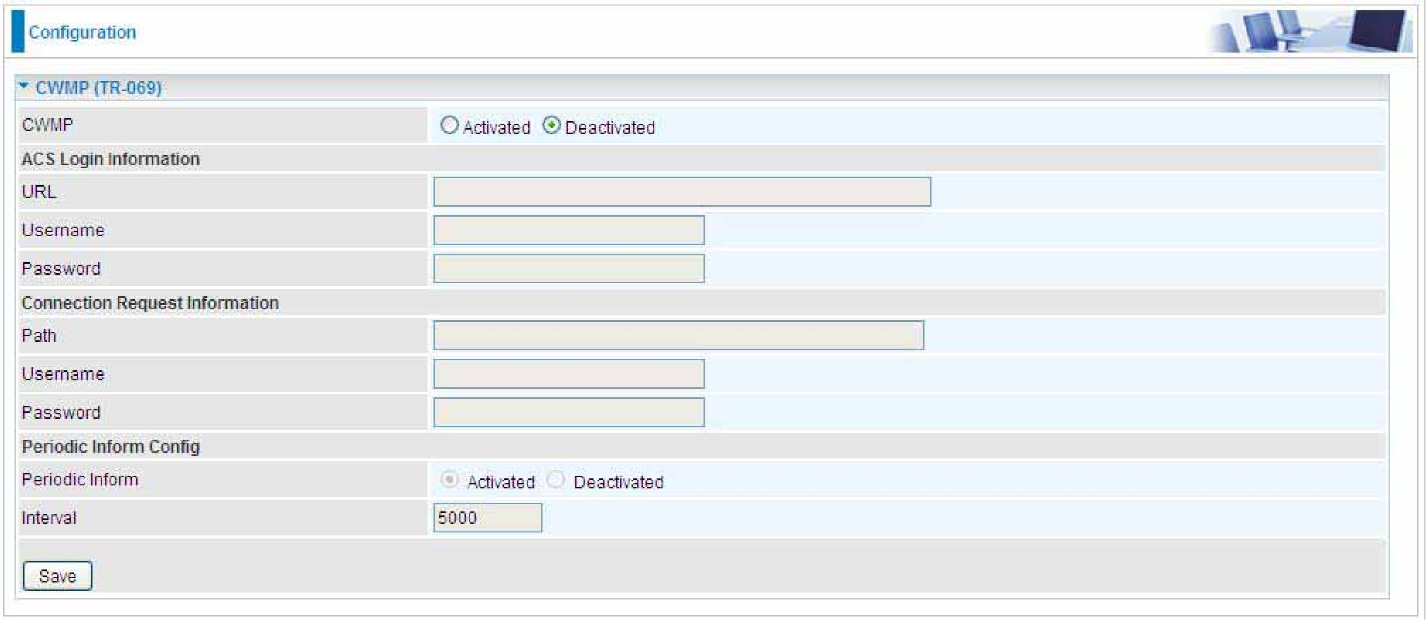
Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL (Host): Specified URL which is prohibited from accessing.

CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



Configuration

▼ CWMP (TR-069)

CWMP	○ Activated ● Deactivated
ACS Login Information	
URL	
Username	
Password	
Connection Request Information	
Path	
Username	
Password	
Periodic Inform Config	
Periodic Inform	● Activated ○ Deactivated
Interval	5000

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

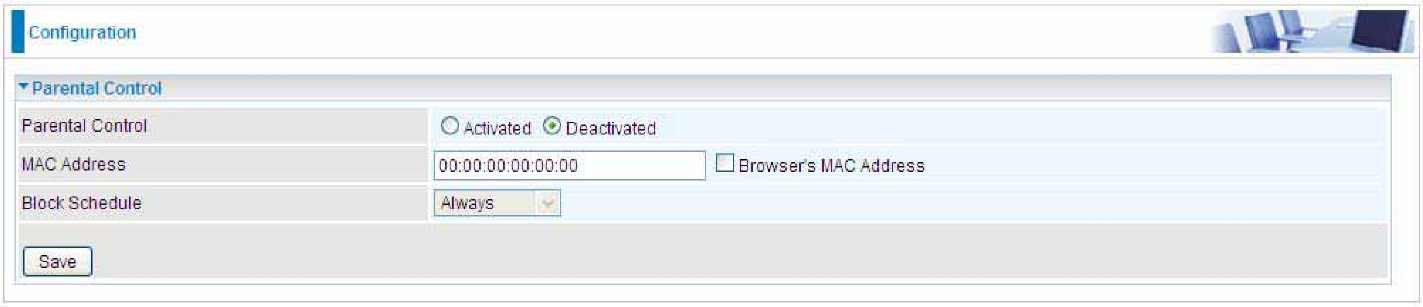
Periodic Inform Config

Periodic Inform: Select Activated to authorize the router to send an Inform message to the ACS automatically.

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

Parental Control

With this feature, router can reject to provide **Internet** services to the specified computer during some specified time interval. This can be very useful for parents to give control to children using computer without restraint.



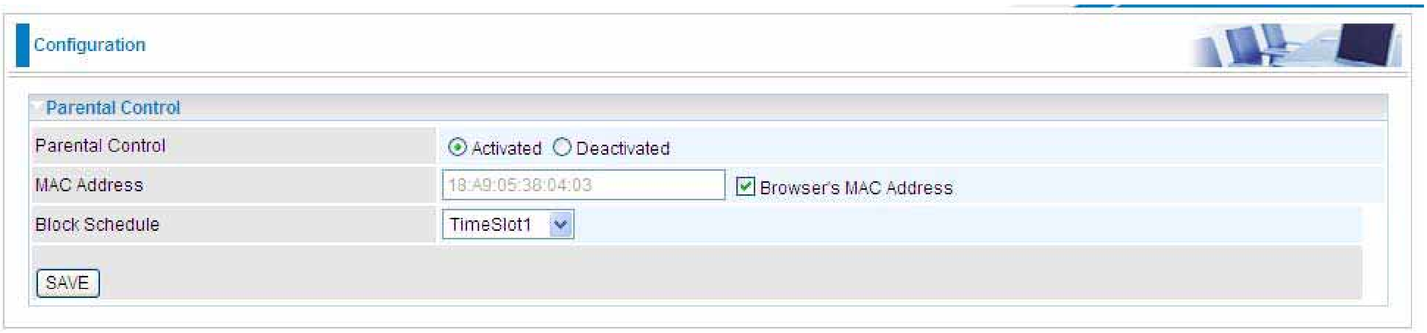
Configuration

Parental Control

Parental Control	○ Activated ● Deactivated
MAC Address	00:00:00:00:00:00 □ Browser's MAC Address
Block Schedule	Always

MAC Address: Type the MAC address(es) you want to block to access the internet (access to the router is sustained). The format of MAC address could be: xx:xx:xx:xx:xx:xx . If you want to set restriction to the Browser PC, you can directly check the checkbox of Browser's MAC Address.

Block Schedule: Select a timeslot throughout which the above set MAC is restricted to access internet. See Time Schedule to set the exact timeslot.

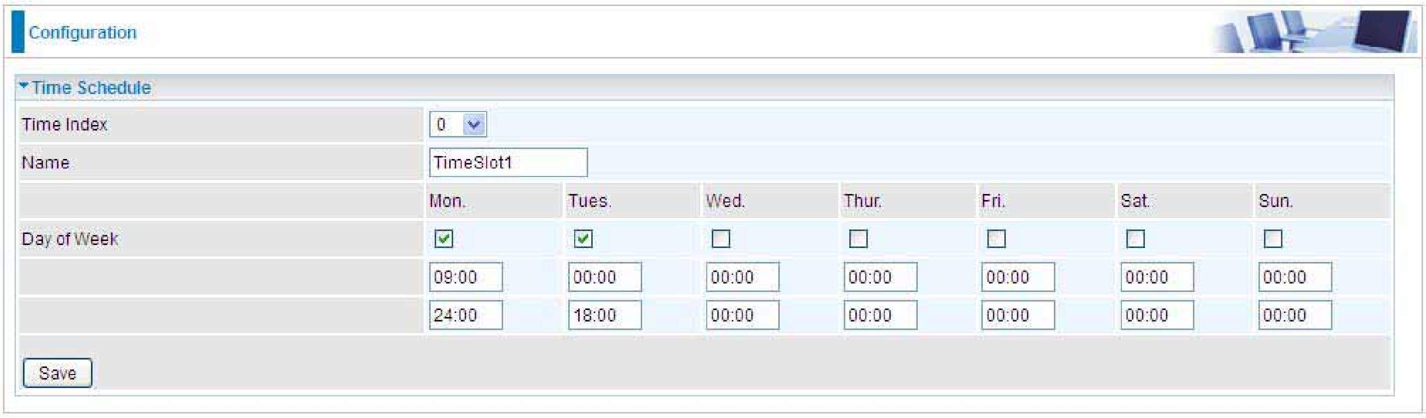


Configuration

Parental Control

Parental Control	● Activated ○ Deactivated
MAC Address	18:A9:05:38:04:03 ☑ Browser's MAC Address
Block Schedule	TimeSlot1

Timeslot1 at Time Schedule:



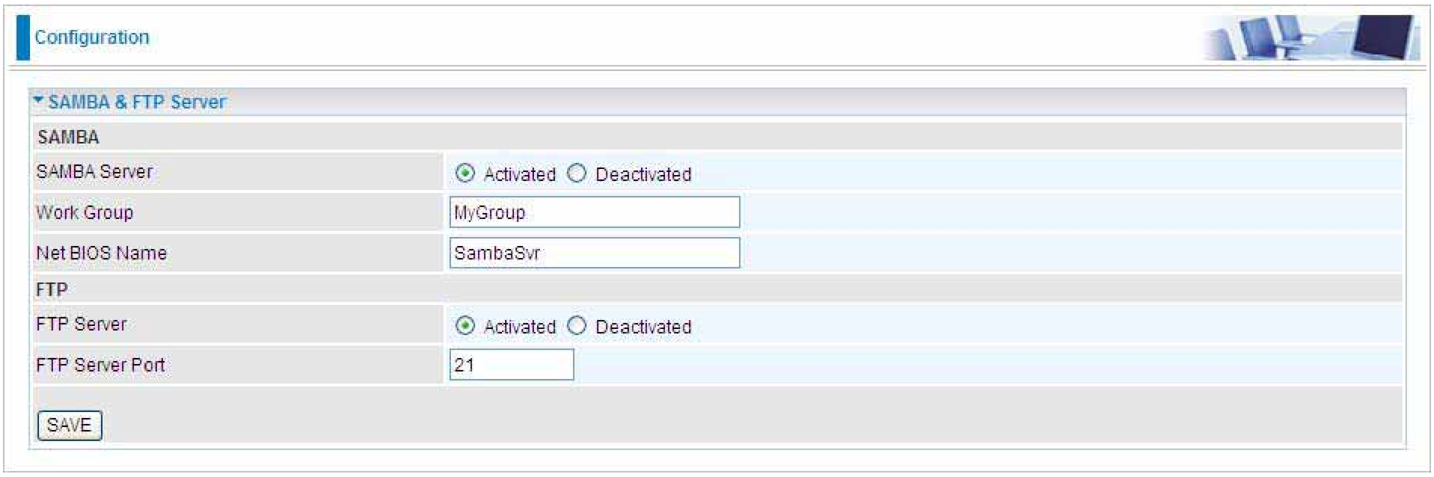
Configuration

Time Schedule

Time Index	0						
Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	☑	☑	□	□	□	□	□
	09:00	00:00	00:00	00:00	00:00	00:00	00:00
	24:00	18:00	00:00	00:00	00:00	00:00	00:00

SAMBA & FTP Server

Samba and FTP are served as network sharing.



Configuration

▾ SAMBA & FTP Server

SAMBA

SAMBA Server	● Activated ○ Deactivated
Work Group	MyGroup
Net BIOS Name	SambaSvr

FTP

FTP Server	● Activated ○ Deactivated
FTP Server Port	21

SAMBA Server: Activated to enable SAMBA sharing.

Work Group: The same mechanism like in Microsoft work group, please set the Work Group name.

NetBIOS Name: The sharing NetBIOS name.

FTP Server: Activated to enable FTP sharing.

FTP Server Port: Set the working port. Well-known one is 21. User can change it.

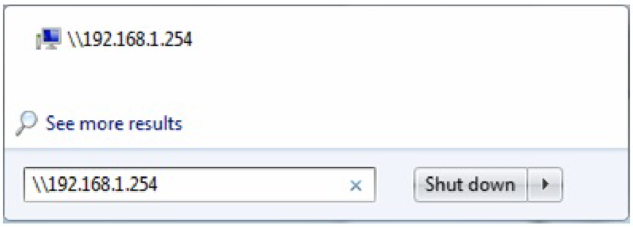
SAMBA/FTP login account:

- **Default user:** admin/admin, it is the administrative user and a super user, it has the full authority of SAMBA /FTP access and operation permission of objects in SAMBA and FTP server.
- **New user:** users can create new user(s) to grant it (them) access and permission to the SAMBA & FTP server.

Please see User Management.

Example: How to setup Samb

1. Go directly to Start > Run (enter \\192,168,1,254 (from LAN side), \\SambaSvr , but if you enter \\SambaSvr, please be sure your working PC is in the same workgroup as set in the samba server set above.)

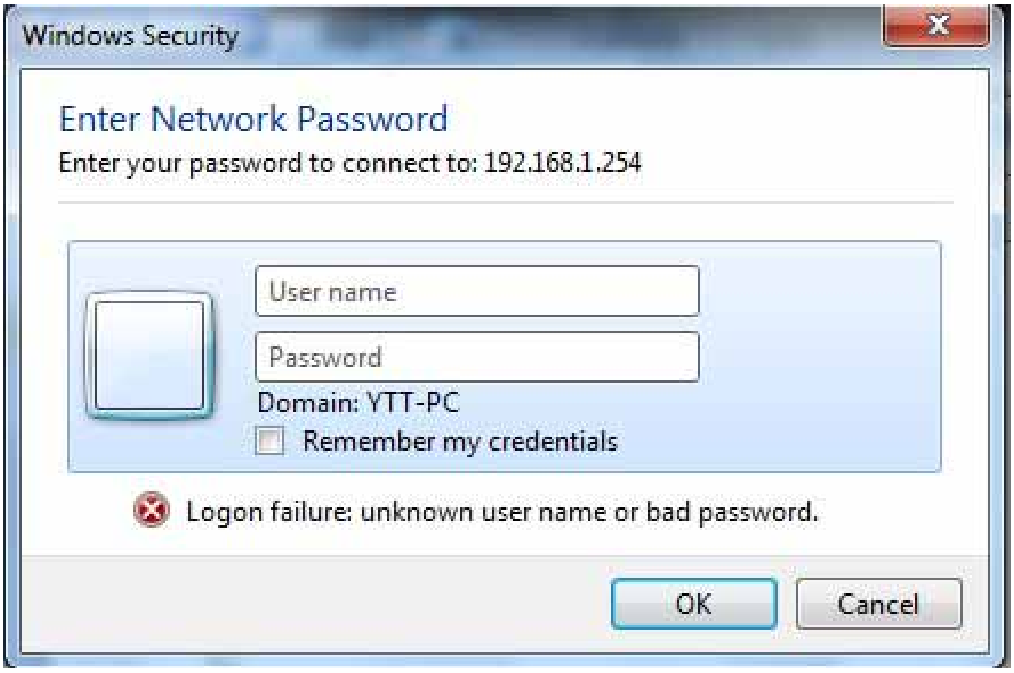


\\192.168.1.254

See more results

\\192.168.1.254

2. Enter the Username and password.



Windows Security

Enter Network Password

Enter your password to connect to: 192.168.1.254

User name

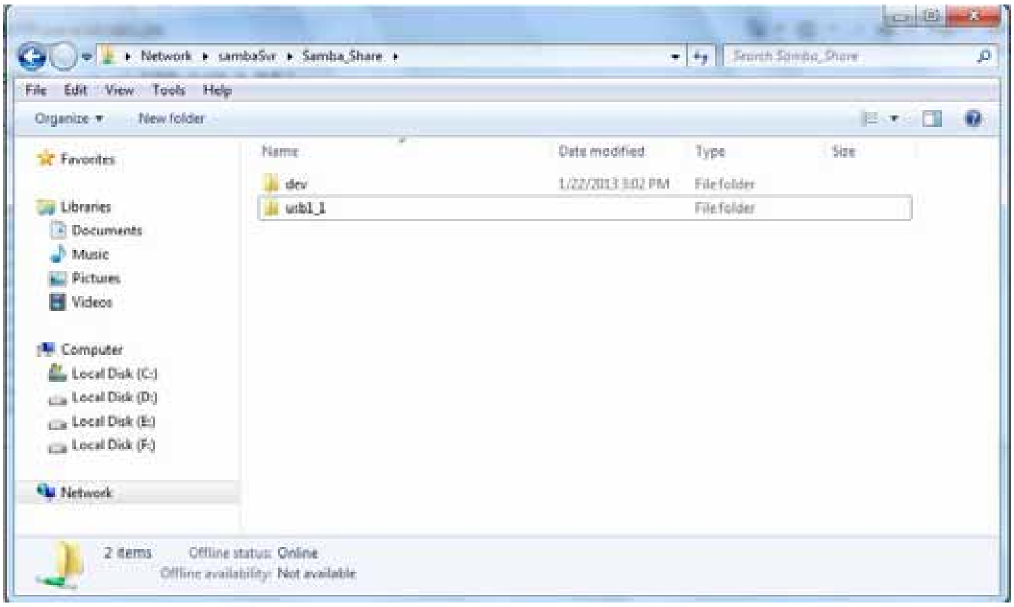
Password

Domain: YTT-PC

□ Remember my credentials

Logon failure: unknown user name or bad password.

3. Users can browse and access USB storage.



Network ▸ sambaSvr ▸ Samba_Share ▸

Name	Date modified	Type	Size
dev	1/22/2013 3:02 PM	File folder	
usb1_1		File folder	

2 items Offline status: Online
Offline availability: Not available

Example: How to setup FTP：

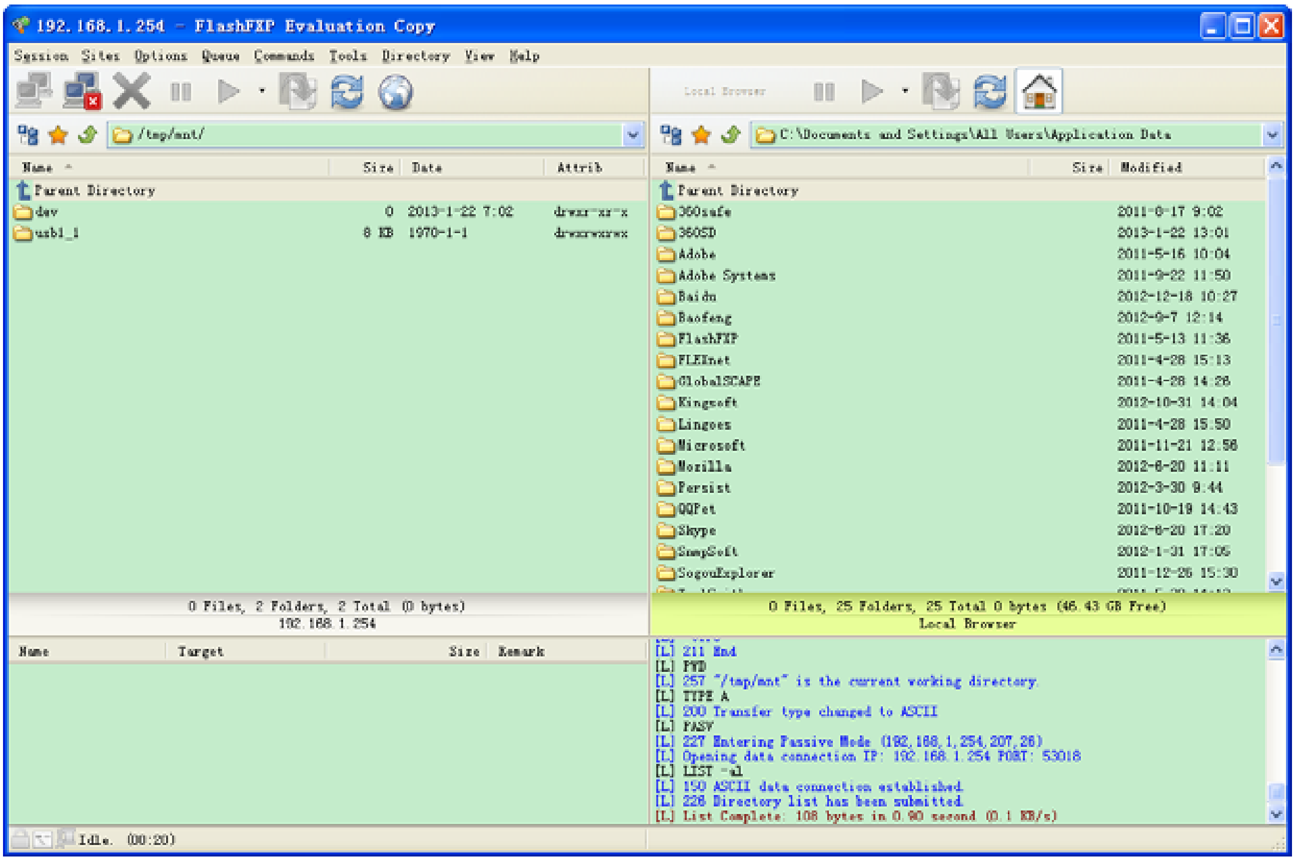
1. **Access via FTP tools**

Take popular FTP tool of FlashFXP for example:

1) Open FlashFXP

2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).

3) Connect to the ftp site.



/tmp/mnt/

Name	Size	Date	Attrib
Parent Directory			
dev	0	2013-1-22 7:02	drwxr-xr-x
usb1_1	8 KB	1970-1-1	drwxrwxrwx

0 Files, 2 Folders, 2 Total (0 bytes)
192.168.1.254

C:\Documents and Settings\All Users\Application Data

Name	Size	Modified
Parent Directory		
360safe		2011-8-17 9:02
360SD		2013-1-22 13:01
Adobe		2011-5-16 10:04
Adobe Systems		2011-9-22 11:50
Baidu		2012-12-18 10:27
Baofeng		2012-9-7 12:14
FlashFXP		2011-5-13 11:36
FLEXnet		2011-4-28 15:13
GlobalSCAPE		2011-4-28 14:28
Kingsoft		2012-10-31 14:04
Lingoes		2011-4-28 15:50
Microsoft		2011-11-21 12:58
Mozilla		2012-6-20 11:11
Persist		2012-3-30 9:44
QQPet		2011-10-19 14:43
Skype		2012-6-20 17:20
SnapSoft		2012-1-31 17:05
SogouExplorer		2011-12-26 15:30

0 Files, 25 Folders, 25 Total 0 bytes (46.43 GB Free)
Local Browser

Name	Target	Size	Remark

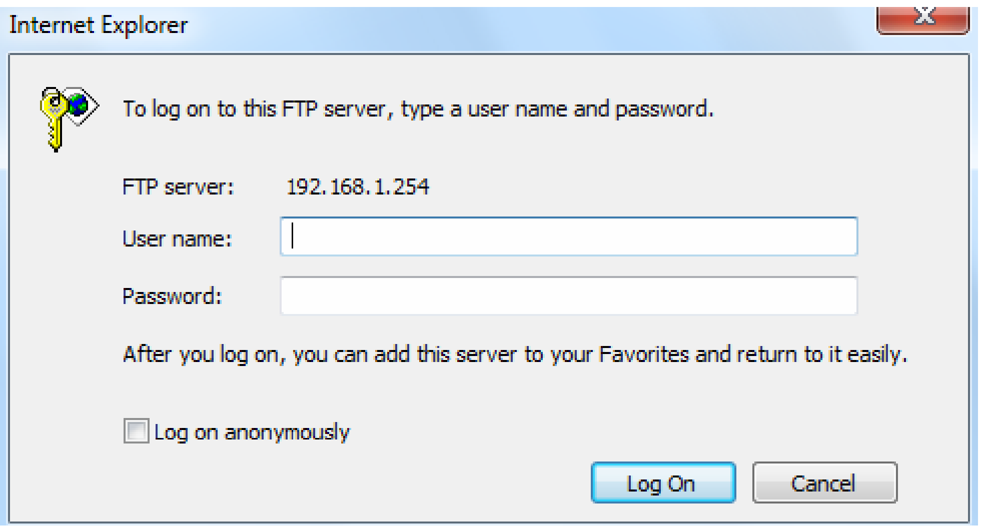
```
[L] 211 End
[L] PWD
[L] 257 "/tmp/mnt" is the current working directory.
[L] TYPE A
[L] 200 Transfer type changed to ASCII
[L] PASV
[L] 227 Entering Passive Mode (192,168,1,254,207,26)
[L] Opening data connection IP: 192.168.1.254 PORT: 53018
[L] LIST -al
[L] 150 ASCII data connection established.
[L] 226 Directory list has been submitted.
[L] List Complete: 108 bytes in 0.90 second (0.1 KB/s)
```

Idle. (00:20)

2. **Web FTP access**

1) Enter ftp://192.168.1.254 at the address bar of the web page.

2) Enter the account's username and password.



Internet Explorer

To log on to this FTP server, type a user name and password.

FTP server: 192.168.1.254

User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

□ Log on anonymously

Maintenance

Maintenance equipments the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including **User Management**, **Time Zone**, **Firmware & Configuration**, **System Restart**, and **Diagnostic Tool.**

User Management

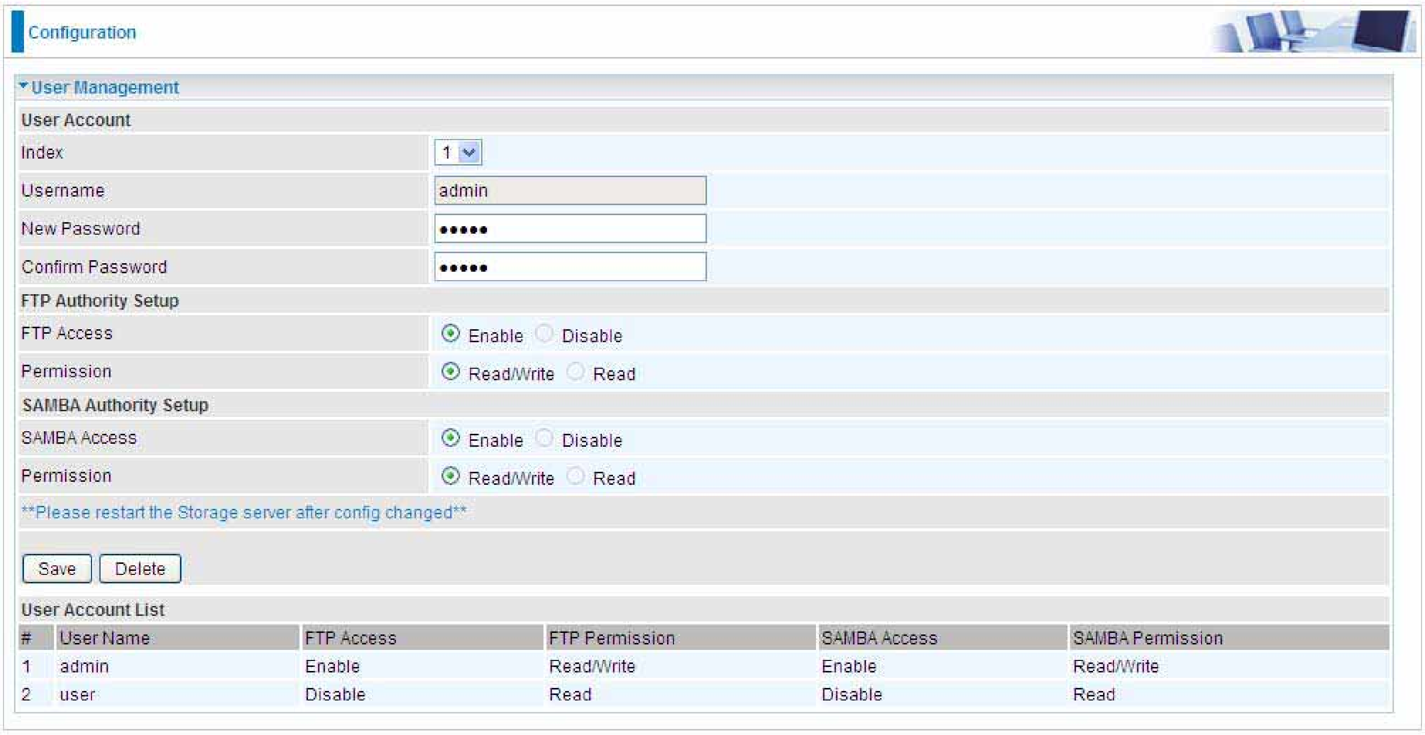
User Management controls the Router Web GUI permission, FTP/SAMBA access to the specific account.

In factory setting, the default accounts are **admin/admin** and **user/user.** The default root account admin has been authorized to web access of router, Samba access, and FTP access. **user/user** is equipment with limited access (specified by advanced users with admin account) to router web, and FTP/SAMBA . A total of **6** other accounts can be created to grant access to the access of Samba and FTP and web page (need to be specified).

Note: Please go to SAMBA & FTP Server to re-activate FTP and SAMBA server to enable the changes to the FTP and SAMBA account set here.

❖ Admin / Admin

admin/admin is the root account provided by our router.



▾User Management

User Account	
Index	1
Username	admin
New Password	•••••
Confirm Password	•••••
FTP Authority Setup	
FTP Access	● Enable ○ Disable
Permission	● Read/Write ○ Read
SAMBA Authority Setup	
SAMBA Access	● Enable ○ Disable
Permission	● Read/Write ○ Read

Please restart the Storage server after config changed

User Account List

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to SAMBA and FTP.

New Password: Enter a new password for this user account.

Confirmed Password: Re-enter the new password again; you must enter the password exactly the same as in the previous field

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

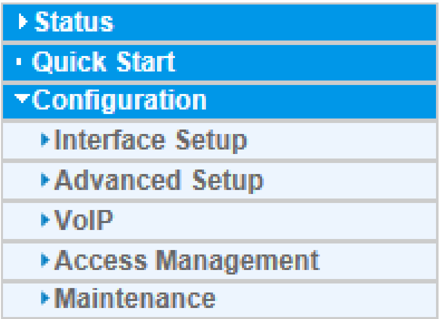
SAMBA Authority

SAMBA Access: Enable to grant the user access to the SAMBA server.

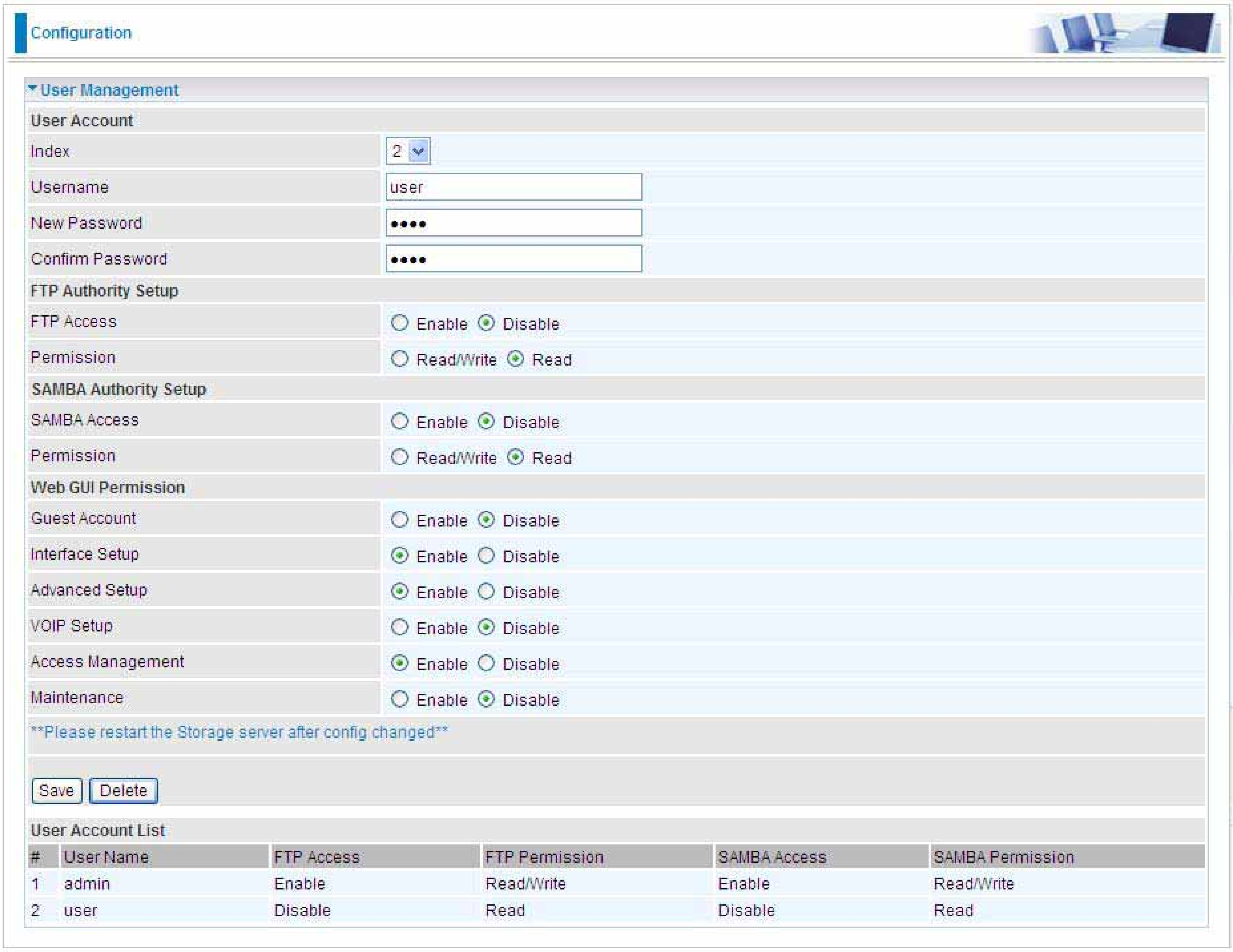
Permission: Set the operation permission for the user, Read/Write or Read.

Web GUI Permission

Login using the Administrator account, you will have the full accessibility to manage & control your BiPAC 6300VNP device and can also create user accounts for others to control some of the open configuration settings.



❖ User / User and/or Adding additonal user accounts



Configuration

▾ User Management

User Account	
Index	2
Username	user
New Password	••••
Confirm Password	••••
FTP Authority Setup	
FTP Access	○ Enable ● Disable
Permission	○ Read/Write ● Read
SAMBA Authority Setup	
SAMBA Access	○ Enable ● Disable
Permission	○ Read/Write ● Read
Web GUI Permission	
Guest Account	○ Enable ● Disable
Interface Setup	● Enable ○ Disable
Advanced Setup	● Enable ○ Disable
VOIP Setup	○ Enable ● Disable
Access Management	● Enable ○ Disable
Maintenance	○ Enable ● Disable

Please restart the Storage server after config changed

User Account List

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to SAMBA and FTP.

New Password: Type the password for the user account.

Confirmed Password: Type password again for confirmation.

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

SAMBA Authority

SAMBA Access: Enable to grant the user access to the SAMBA server.

Permission: Set the operation permission for the user, Read/Write or Read.

Web GUI Permission

Guest Account: A pre-set guest account setting granted with **Interface Setup**, **Advanced Setup**, **Access Management** access. Enable to have access to Interface Setup, Advanced Setup and Access Management or disable to set the specifics yourself.

Interface Setup: Enable to allowing access to Interface Setup with this account.

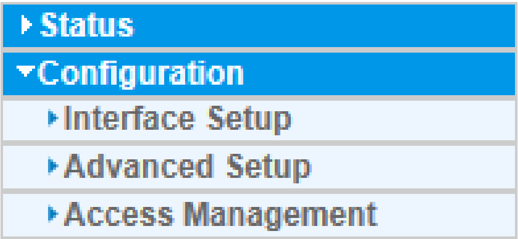
Advanced Setup: Enable to allowing access to Advanced Setup with this account.

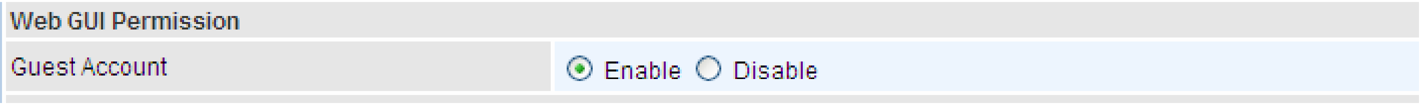
VOIP Setup: Enable to allowing access to VoIP Setup with this account.

Access Management: Enable to allowing access to Access Management with this account.

Maintenance: Enable to allowing access to Maintenance with this account.

When customers use the "user" account to login to the router, they are offered with only configuration items set in **Web GUI Permission**.



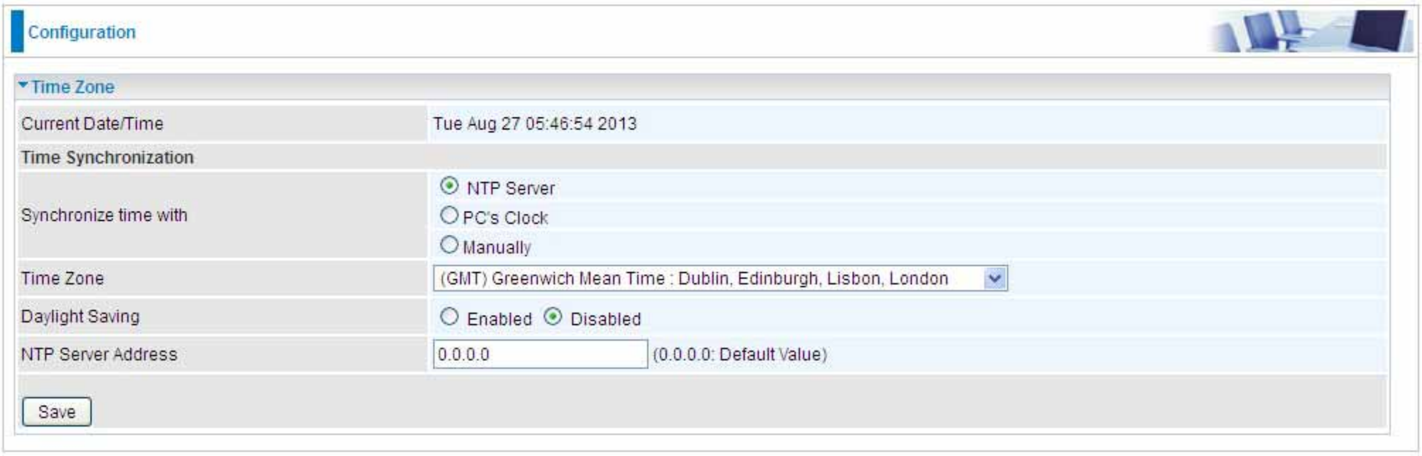

Web GUI Permission

Guest Account ● Enable ○ Disable

(Configuration items shown when "user" account uses Guest account on Web GUI Permission)

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. 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 the default, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.



Current Date/Time	Tue Aug 27 05:46:54 2013
Time Synchronization	
Synchronize time with	● NTP Server ○ PC's Clock ○ Manually
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Daylight Saving	○ Enabled ● Disabled
NTP Server Address	0.0.0.0 (0.0.0.0: Default Value)

Synchronize time with: Select the methods to synchronize the time.

- **NTP Server automatically:** To synchronize time with the NTP server.
- **PC’s Clock:** To synchronize time with the PC’s clock.
- **Manually:** Select this, user need to set the time yourself manually.

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

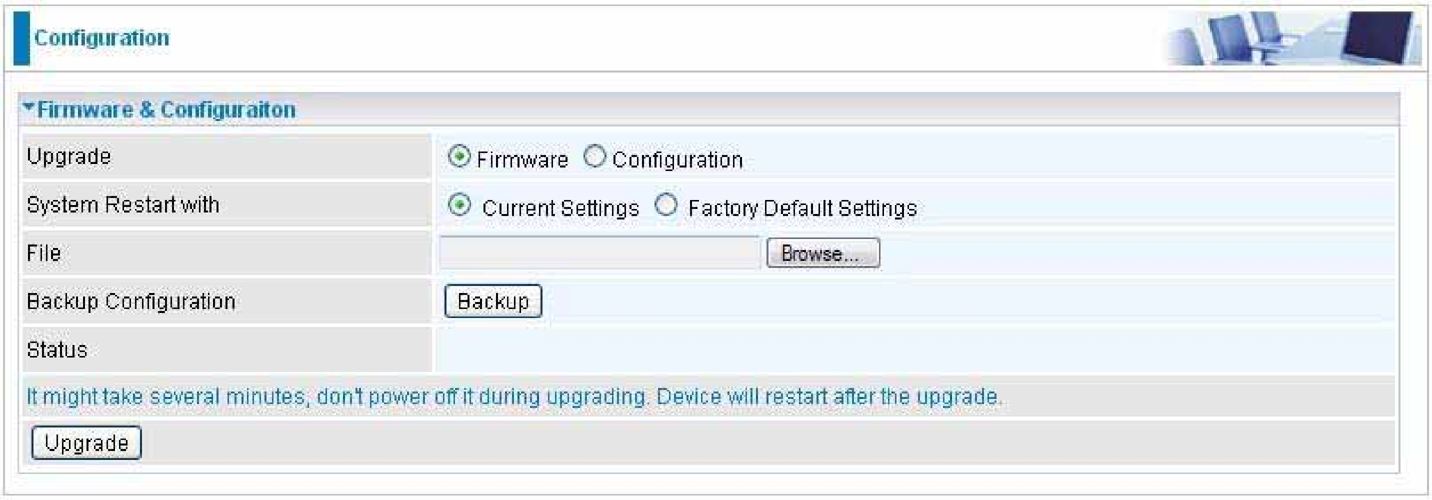
Daylight Saving: Select this option if you use daylight savings time.

NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your BiPAC 6300VNP provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of BiPAC 6300VNP, you should download or copy the firmware to your local environment first. Press the **"Browse…"** button to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading. When the procedure is completed, BiPAC 6300VNP will reset automatically to make the new firmware work.



Configuration

▾Firmware & Configuraiton

Upgrade	● Firmware ○ Configuration
System Restart with	● Current Settings ○ Factory Default Settings
File	Browse...
Backup Configuration	Backup
Status	

It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

Upgrade: Choose Firmware or Configuration you want to update.

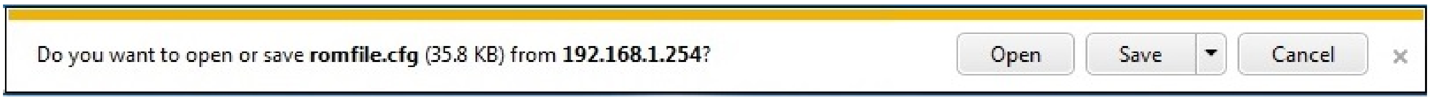
System Restart with:

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

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

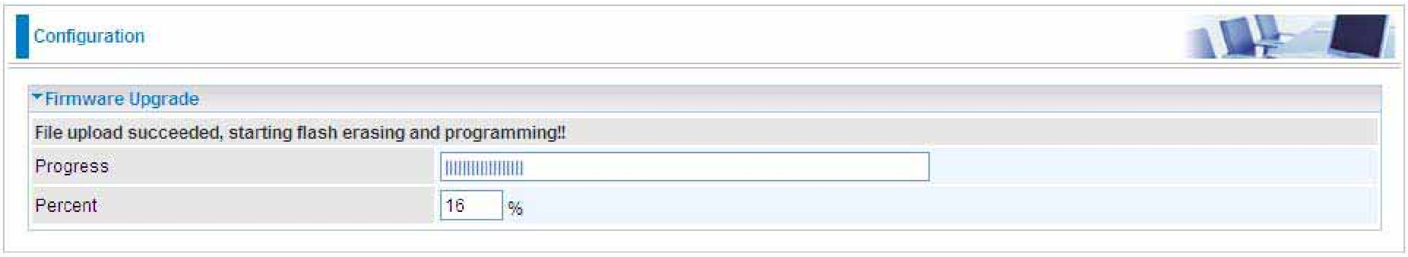
Browse: Click **Browse...** to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your BiPAC 6300VNP device when making false configurations and want to restore to the original settings.



Do you want to open or save **romfile.cfg** (35.8 KB) from **192.168.1.254**?

UPGRADE: Click **UPGRADE** to begin the upload process. This process may take up to two minutes.



Configuration

▾Firmware Upgrade

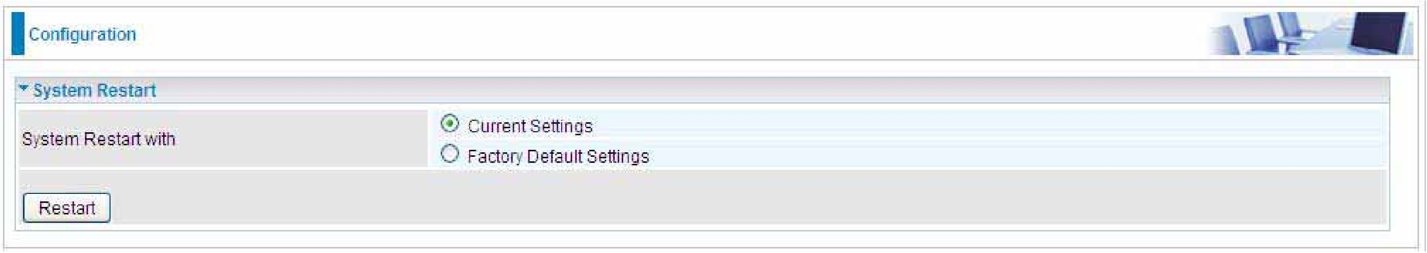
File upload succeeded, starting flash erasing and programming!!

Progress	||||||||||||||||
Percent	16 %

DO NOT turn off / power off the device or interrupt the firmware upgrading while it is still in process. Improper operation could damage your BiPAC 6300VNP.

System Restart

Click **System Restart** with option **Current Settings** to reboot your router.



Configuration

System Restart

System Restart with ● Current Settings ○ Factory Default Settings

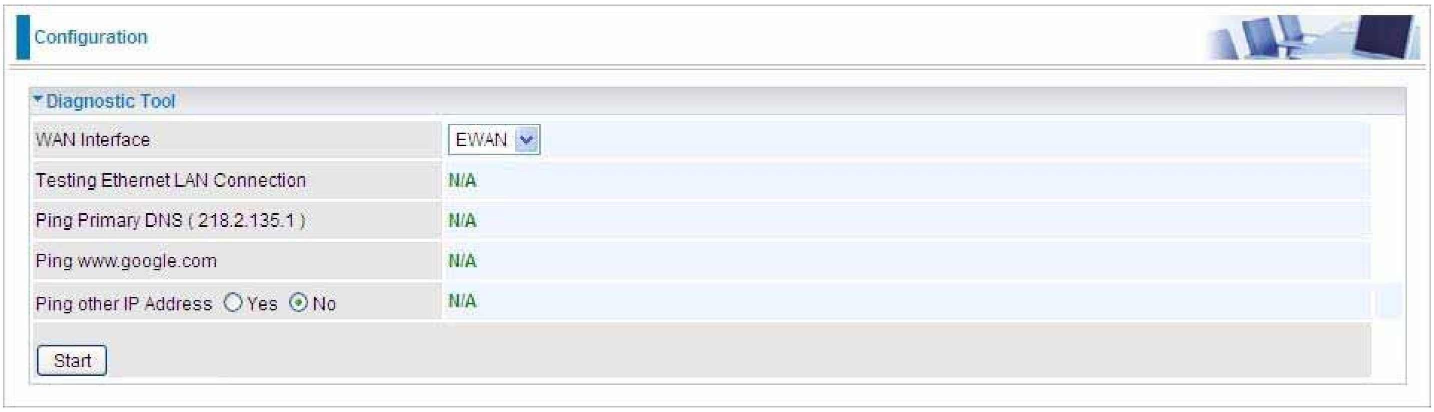
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select ***Factory Default Settings*** to restore to factory default settings.

You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.

Diagnostics Tool

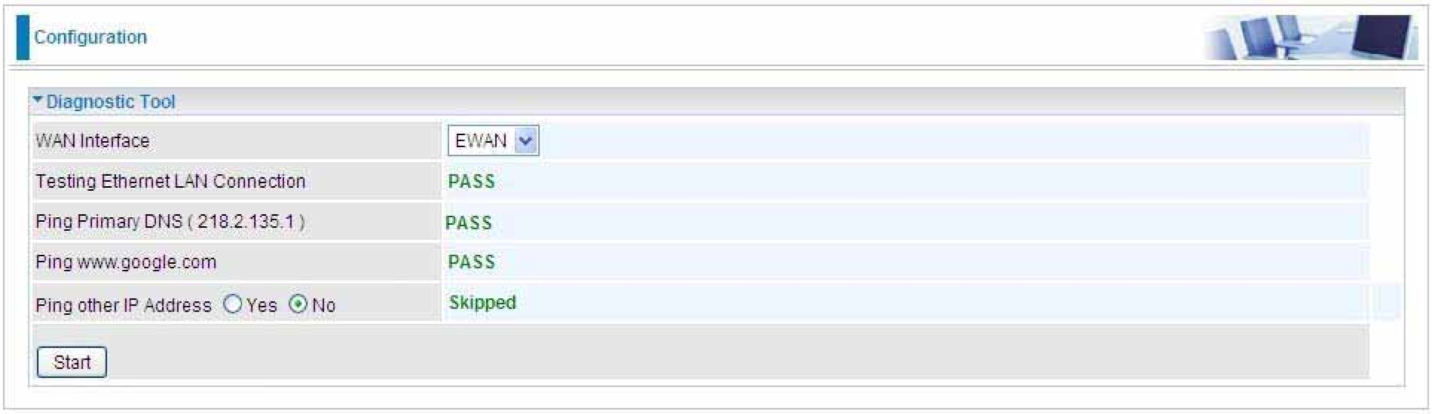
The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

EWAN:



WAN Interface	EWAN
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (218.2.135.1)	N/A
Ping www.google.com	N/A
Ping other IP Address ○ Yes ● No	N/A

Click START to begin to diagnose the connection.



WAN Interface	EWAN
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (218.2.135.1)	PASS
Ping www.google.com	PASS
Ping other IP Address ○ Yes ● No	Skipped

Chapter 5: Troubleshooting

If your BiPAC 6300VNP is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	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 "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

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

Recovery Procedures

Problem	Suggested Action
- The front LEDs display incorrectly **- Still cannot access to the router management interface after pressing the RESET button.** **- Software / Firmware upgrade failure**	1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately. 2. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.

Appendix: Product Support & Contact

Most problems can be solved by referring to the Troubleshooting section in the User's Manual. If you cannot resolve the problem with the Troubleshooting chapter, please contact the dealer where you purchased this product.

Contact Billion

WORLDWIDE

http://www.billion.com

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

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

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.