

BiPAC 6300VNOZ

VoIP Wireless-N VPN Broadband Router

User Manual

Table of Contents

<i>Chapter 1</i>	1
1.1 Introducing the BIPAC 6300VNOZ.....	1
1.2 Features of the BIPAC 6300VNOZ	3
Network Protocols and Features.....	3
Firewall	3
Quality of Service Control.....	4
Wireless LAN.....	4
VoIP.....	4
USB Application Server	4
IPTV Applications	4
Management	4
1.3 Hardware Specifications.....	5
Physical Interface.....	5
1.4 Applications for the BIPAC 6300VNOZ	6
<i>Chapter 2</i>	7
2.1 Important note for using the BIPAC 6300VNOZ	7
2.2 Package Contents	8
2.3 The Front LEDs.....	9
2.4 The Rear Ports	11
2.5 Power Source	12
2.6 Cabling	14
<i>Chapter 3</i>	15
3.1 Before Configuration	15
3.1.1 Configuring a PC in Windows 7	16
3.1.2 Configuring a PC in Windows Vista.....	19
3.1.3 Configuring a PC in Windows XP	21
3.1.4 Configuring a PC in Windows 2000	23
3.1.5 Configuring a PC in Windows 98/Me.....	24
3.1.6 Configuring a PC in Windows NT4.0	25
3.2 Factory Default Settings	26
3.2.1 Username and Password	26
3.3 LAN Port Addresses	27
3.4 Information from your ISP	27
<i>Chapter 4</i>	28
4.1 Configuring BIPAC 6300VNOZ with your Web Browser.....	28
4.2 Status.....	30

4.2.1 Device Info	31
4.2.2 System Log	33
4.2.3 Statistics	34
4.2.4 DHCP Table	37
4.2.5 Disk Status	38
4.2.6 VoIP Status	39
4.2.6.1 VoIP Status	39
4.3 Quick Start	40
4.4 Configuration	44
4.4.1 Interface Setup	45
4.4.1.1 Internet	45
4.4.1.2 LAN	49
4.4.1.3 Wireless	53
4.4.1.4 Wireless MAC Filter	65
4.4.2 Advanced Setup	66
4.4.2.1 Firewall	66
4.4.2.2 Routing	67
4.4.2.3 NAT	69
4.4.2.4 Static DNS	74
4.4.2.5 QoS	75
4.4.2.6 Interface Grouping	76
4.4.2.7 Port Isolation	78
4.4.2.8 Time Schedule	79
4.4.3 VoIP	80
4.4.3.1 Basic	81
4.4.3.2 Media	82
4.4.3.3 Advanced	83
4.4.3.4 Speed Dial	84
4.4.3.5 Call Features	85
4.4.4 Access Management	87
4.4.4.1 Device Management	87
4.4.4.2 SNMP	88
4.4.4.3 Universal Plug & Play	89
4.4.4.4 Dynamic DNS	90
4.4.4.5 Access Control	92
4.4.4.6 Packet Filter	94
4.4.4.7 CWMP (TR-069)	98
4.4.4.8 Parental Control	100
4.4.4.9 SAMBA & FTP Server	101
4.4.5 Maintenance	105
4.4.5.1 User Management	105
4.4.5.2 Time Zone	106
4.4.5.3 Firmware & Configuraion	107
4.4.5.4 System Restart	109
4.4.5.5 Diagnostics Tool	110
Chapter 5	111

Problems starting up the router	111
Problems with the WAN Interface.....	111
Problems with the LAN Interface.....	111
Recovery procedures for non-working routers	112
<i>APPENDIX</i>	<i>113</i>

Chapter 1

Introduction the BIPAC 6300VNOZ

1.1 Introducing the BIPAC 6300VNOZ

Thank you for purchasing BIPAC 6300VNOZ Router. The BIPAC 6300VNOZ is a compact and advanced broadband gateway(router) that offers flexible and multiple internet connection services for home, SOHO and office users to enjoy high-speed, high-level security internet connection via cellular wireless and/or Ethernet WAN. With an integrated 802.11n wireless access point and 4-point Gigabit Ethernet LAN ports, the gateway enables faster wireless speed of up to 300Mbps and LAN connection 10 times faster than regular 10/100Mbps Ethernet LAN. Users can choose the most economical rate of VoIP calls provided by different Internet Technology Service Provider (ITSP). The device integrates two FXS ports which allows for simultaneous VoIP calls.

Cost saving

Making VoIP calls is extremely simple; just connect the router to your existing telephones. The BIPAC 6300VNOZ complies with the most popularly adopted VoIP standard, SIP protocol, to ensure interoperability with SIP devices and major VoIP Gateways. The router also supports a wider range of telephony features, such as Call Waiting, Conference Call, Speed Dial, Return Call, Redial, Don't Disturb, etc.

Wireless Mobility and Security

With an integrated 802.11n Wireless Access Point, the 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. The BIPAC 6300VNOZ 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, end users can enter the information

easily which they get from ISP, then surf the Internet immediately.

Firmware Upgradeable

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

1.2 Features of the BIPAC 6300VNOZ

- Gigabit Ethernet WAN (GbE WAN) for Fibre (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
- Supports IPTV Application^{*2}
- Make phone calls via Internet
- Voice over IP compliant with SIP standard
- Two FXS ports for connecting to regular 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 Routing (v4/ v6) 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

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 (* future release)
- Call Detailed Records (CDR) (* future release)

USB Application Server

- Storage (NAS): SAMBA Server, FTP Server

IPTV Applications^{*2}

- IGMP Snooping and IGMP Proxy
- MLD Snooping and MLD Proxy
- Virtual LAN (VLAN)
- Quality of Service (QoS)

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*¹ supports remote management



1. On request for Telco / ISP projects
2. IPTV application may require subscription to IPTV services from a Telco / ISP.
3. Specifications on this datasheet are subject to change without prior notice.

1.3 Hardware Specifications

Physical Interface

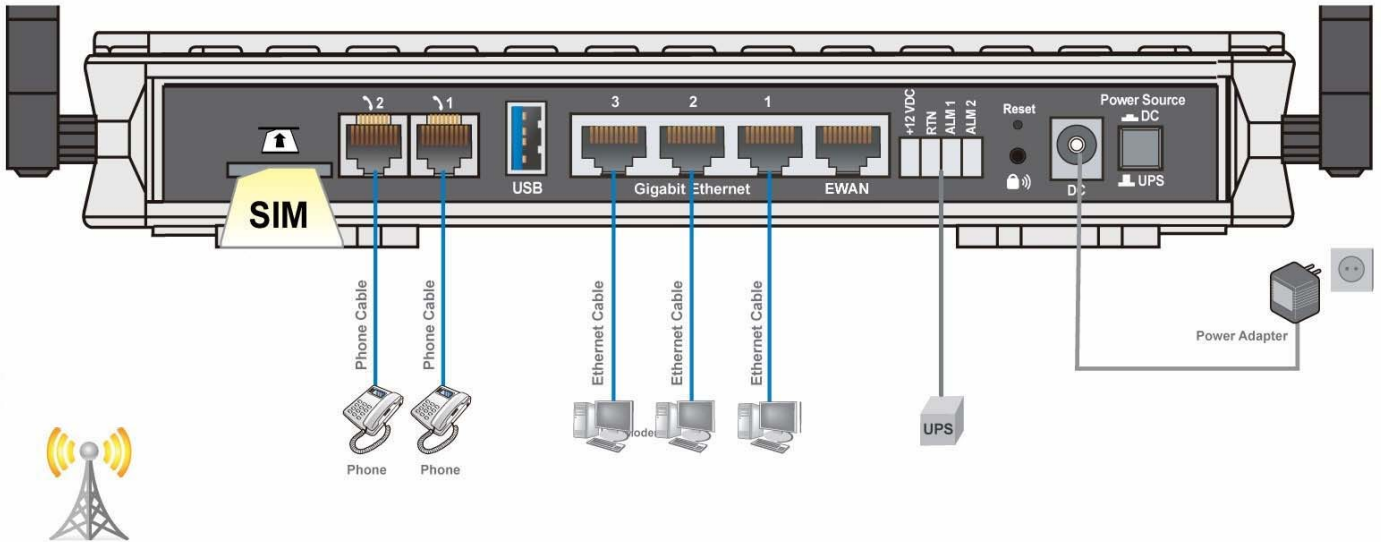
- Detachable antennas: 2 high performance external antennas
- SIM Card slot: Mini SIM card (2FF) slot for mobile broadband connectivity
- VoIP Phone port: 2 RJ-11 FXS for connecting to regular telephones
- USB: 1 USB 2.0 type A port for storage service
- Ethernet: 4-port 10/ 100/ 1000Mbps auto-crossover (MDI/ MDI-X) Switch
- EWAN: RJ-45 Gigabit Ethernet port for connecting to Fibre/ Cable/ xDSL modem for Broadband connectivity.
- Factory default reset button
- Wireless on/off and WPS push button
- DC power input jack
- UPS power input jack
- Power source selection button

1.4 Applications for the BIPAC 6300VNOZ

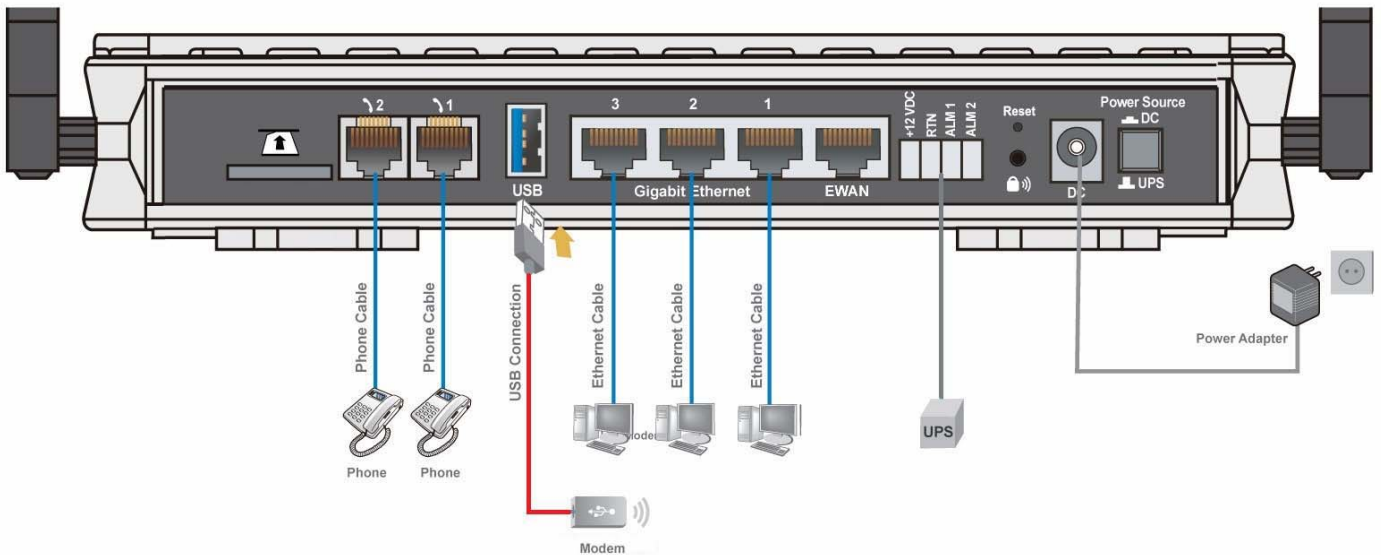
BIPAC 6300VNOZ is an all-in-one router, supporting alternative ways (EWAN, mobile) to connect to the Internet. Then users can choose one of the ways to connect to the Internet or ISP.

Mobile router mode

BIPAC 6300VNOZ is embedded with a module supporting mobile SIM card. It can be used to connect to high speed mobile broadband connection.

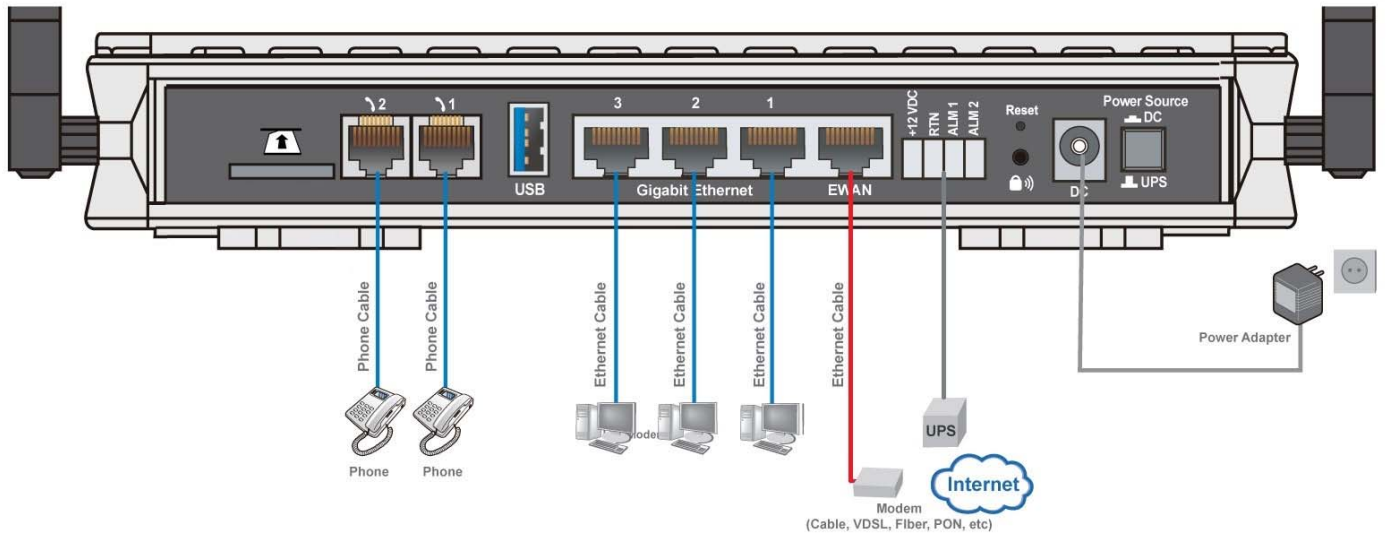


BiPAC 6300VNOZ also supports one USB ports for your mobile dongle. It can be used to connect to high speed mobile broadband connection, too.



Broadband router mode

BIPAC 6300VNOZ has a Gigabits Ethernet WAN port to connect to your Fibre/ Cable/ xDSL modem.



Chapter 2

Installing the BIPAC 6300VNOZ

2.1 Important note for using the BIPAC 6300VNOZ



Warning

- ✓ Do not use the BIPAC 6300VNOZ in high humidity or high temperatures.
- ✓ Do not use the same power source for the BIPAC 6300VNOZ as other equipment.
- ✓ Do not open or repair the case yourself. If the BIPAC 6300VNOZ is too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.

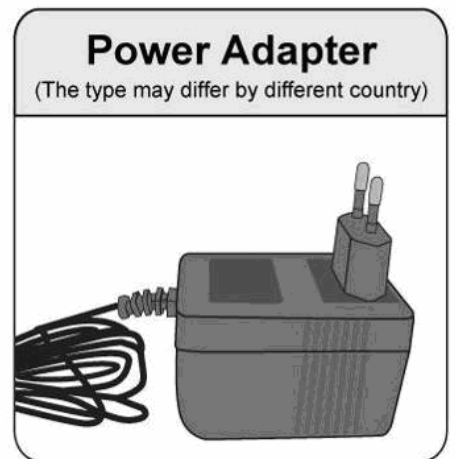
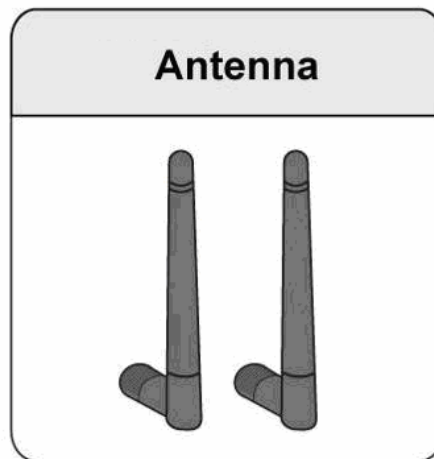
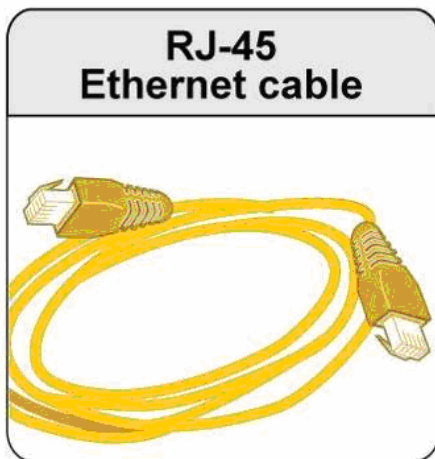
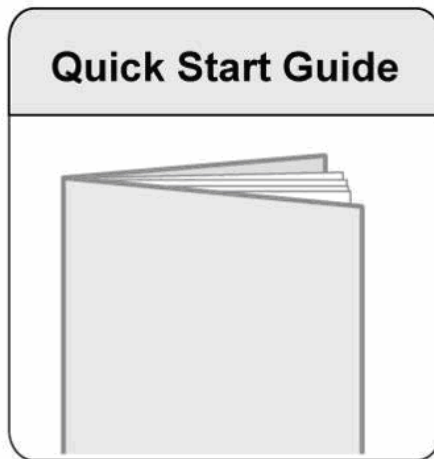
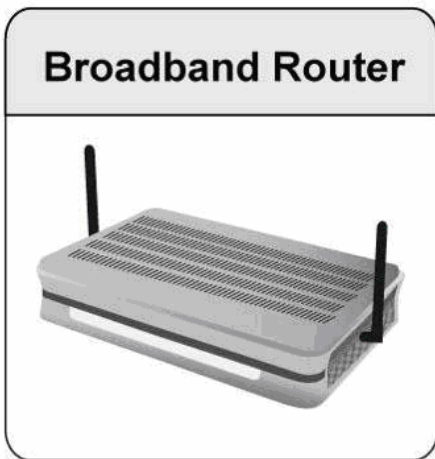


Attention

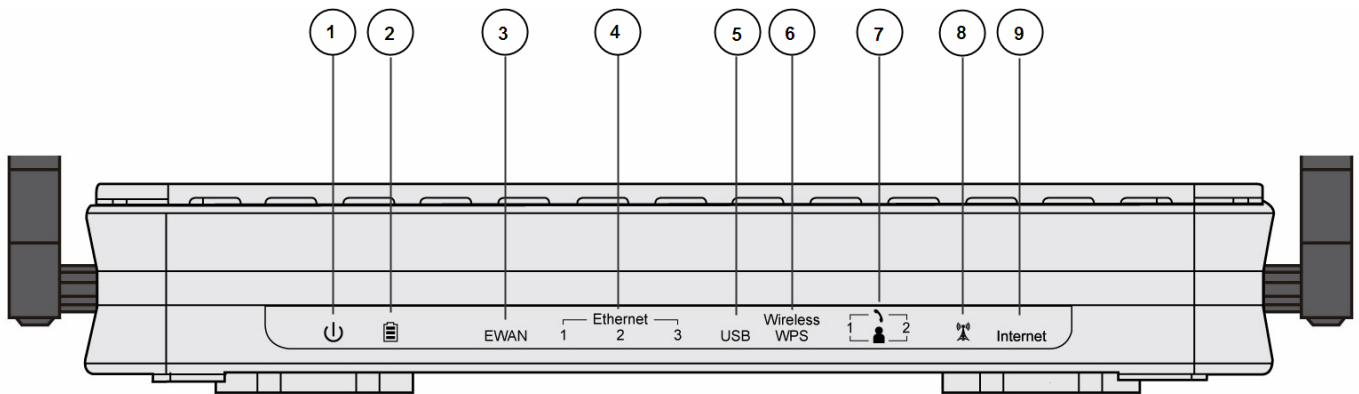
- ✓ Place the BIPAC 6300VNOZ on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

2.2 Package Contents

- BIPAC 6300VNOZ - VoIP Wireless-N VPN Broadband Router
- Quick Start Guide
- CD containing user manual
- Ethernet (RJ-45 CAT-5) cable
- Two detachable Antennas
- Power adapter



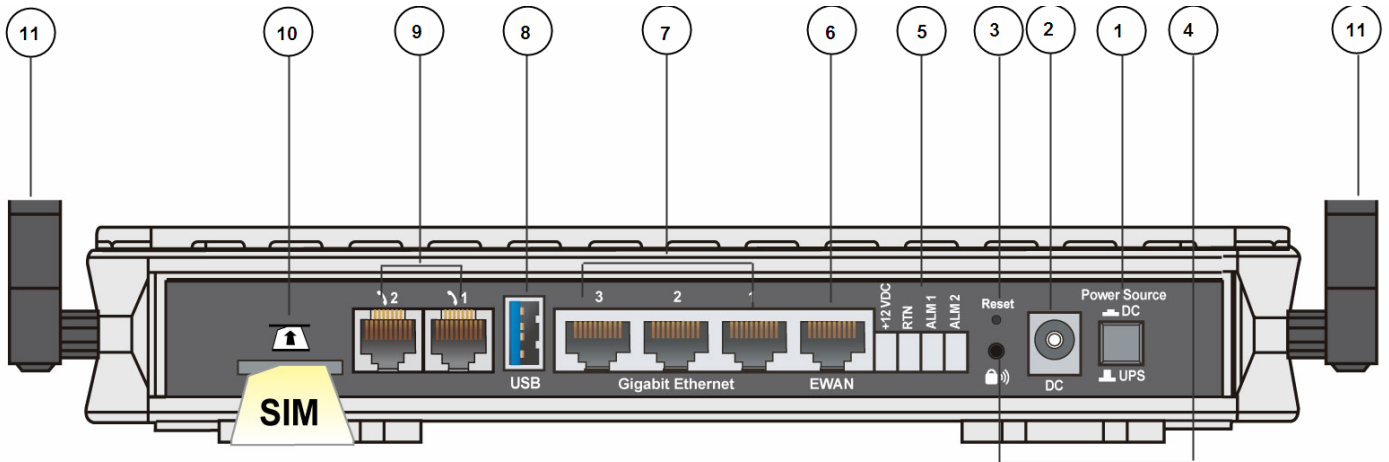
2.3 The Front LEDs



LED		Status	Meaning
1	Power	Green	System ready
		Red	Boot failed
2	Battery	Green	AC working and battery OK
		Orange	Only AC working, battery fail and has to change battery
		Orange blinking	AC fail and battery working
		Off	The power input is from power adapter not UPS
3	EWAN	Green	Transmission speed hitting 1000Mbps
		Orange	Transmission speed hitting 10/100Mbps
		Blinking	Data being transmitted/received
4	Ethernet (1-3)	Green	Transmission speed hitting 1000Mbps
		Orange	Transmission speed hitting 10/100Mbps
		Blinking	Data being transmitted/ received
5	USB	Green	Connected to a storage device
6	Wireless/ WPS	Green	Wireless connection established
		Green blinking	Sending/ Receiving data
		Orange	WPS on
7	Phone (1-2)	Green	Successfully registered
		Orange	Phone being in use
8	Signal Strength	Green	Signal strength > 75%

		Green blinking quickly	Signal strength 75% ~ 50%
		Orange blinking quickly	Signal strength 50% ~ 25%
		Orange blinking slowly	Signal strength < 25%
		Orange	No signal, but module OK
		Off	module fails or No module
9	Internet	Red	Obtaining IP failure
		Green	Having obtained an IP address successfully
		Off	Router in bridged mode or WAN connection not present.

2.4 The Rear Ports

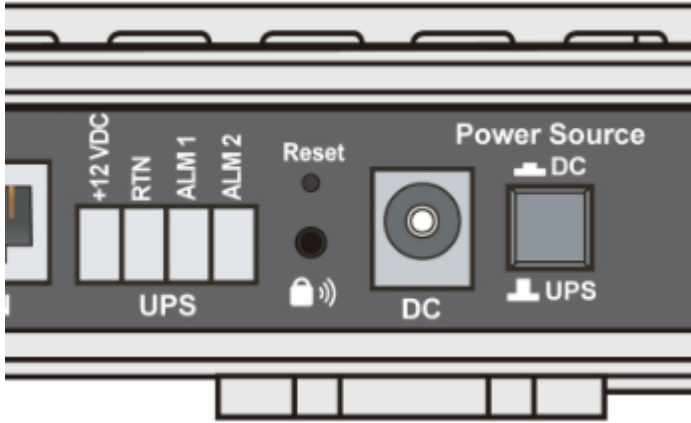


Port		Meaning
1	Power Source	Power source selector. Switch between DC power adapter and UPS (DC).
2	DC	Connect the supplied DC power adapter to this jack.
3	RESET	After the device is powered on, press it 6 seconds or above : to restore to factory default settings (this is used when you can not login to the router, e.g. forgot the password)
4	Wireless On/Off WPS	By controlling the pressing time, users can achieve two different effects: (1) <u>Wireless ON/OFF button</u> : Press over 6 seconds to switch on wireless function when wireless is off and press over 6 seconds again to disable wireless function. (2) <u>WPS</u> : Press less than 6 seconds to trigger WPS function.
5	UPS	Connect the supplied standardized UPS(DC) to this jack
6	EWAN	Connect to Fiber/ Cable/ xDSL Modem with your RJ-45 cable.
7	Gigabit Ethernet	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the three LAN ports when connecting to a PC or an office/home network of 10Mbps /100Mbps /1000Mbps.
8	USB	Connect the storage device to this port.
9	Phone (1-2)	Connect your analog phone set to this port with the RJ-11 cable.
10	SIM Card slot	Plug the proper mini SIM card(2FF) into the slot
11	Antenna	Connect to the supplied two high performance external antennas

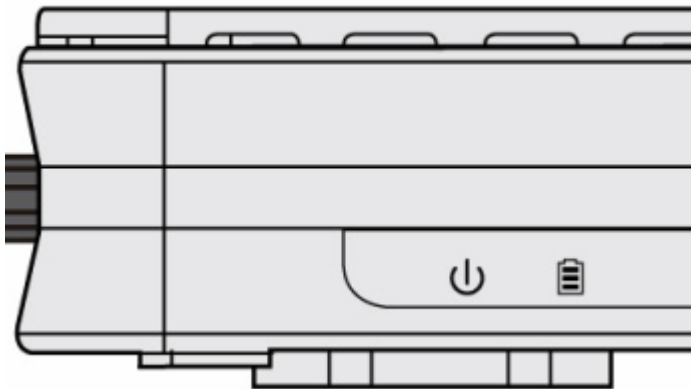
2.5 Power Source

6300VNOZ offers two kinds of power input, namely, **DC power Adapter** and **DC UPS** (or BBU).

6300VNOZ can take the advantage of UPS (Uninterruptible Power Supply) to keep working even if the power outage hit your router when the router is working in DC UPS mode.



(a picture of the rear focusing on the power source)



(a shot from the front panel, with second icon being identified as the **Battery** LED)

How to switch between the two power input:

Press **down** "Power Source" push button, the power source is "DC" power adapter.

Press **up** "Power Source" push button, the power source is UPS. Device can continue to operate for a period of time after AC power failure, due to uninterrupted power system features of UPS. (Note: a standardized DC UPS will come to your by BEC, customers should not turn to other substandard DC UPS.)

UPS feature:

A battery LED is shown on your device front panel to indicate the DC UPS use. The battery LED is on only when DC UPS is in use, and when the device is operating using DC power adapter, the LED is unlit.

The meanings of the different status of Battery LED:

- ① Green lit: AC is working, UPS battery working well
- ① Orange Lit: Only AC is working, but Battery fails. And you have to change battery
- ① Orange Blinking: AC fails, but battery is working

2.6 Cabling

One of the most common causes of problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of the product is a bank of LEDs. Verify that the LAN Link and LEDs are lit. If they are not, verify that you are using the proper cables.

Make sure that all other devices (e.g. telephones, fax machines, analogue modems) connected to the same telephone line as your Billion router have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and that all line filters are correctly installed in a right way. If the line filter is not correctly installed and connected, it may cause problems to your connection or may result in frequent disconnections.

Chapter 3

Basic Installation

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Windows 98/NT/2000/XP/Vista/Win7, Linux, Mac OS, etc. The product provides an easy and user-friendly interface for configuration.

3.1 Before Configuration

PCs must have an Ethernet interface installed properly and be connected to the router either directly or through an external repeater hub, and 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 of 192.168.1.1 to 192.168.1.253). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router's web interface it may also be advisable to **uninstall** any kind of software firewall on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of the router. Users should make their own decisions on how to best protect their network.

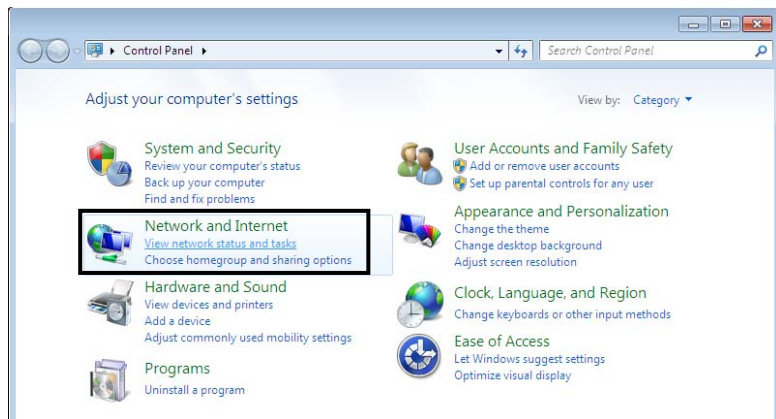
Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.



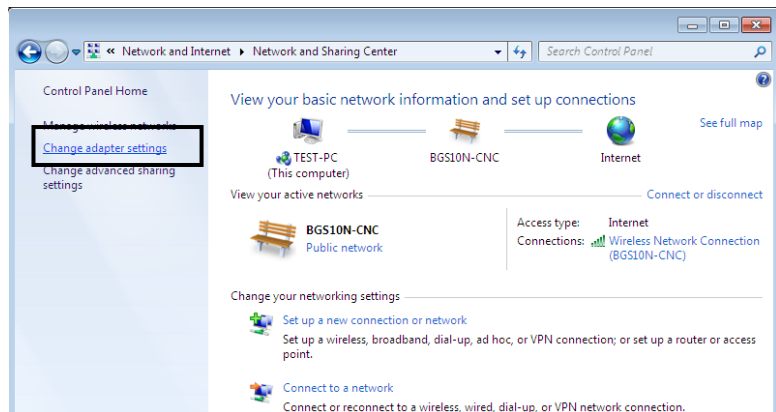
Any TCP/IP capable workstation can be used to communicate with or through the BIPAC 6300VNOZ. To configure other types of workstations, please consult the manufacturer's documentation.

3.1.1 Configuring a PC in Windows 7

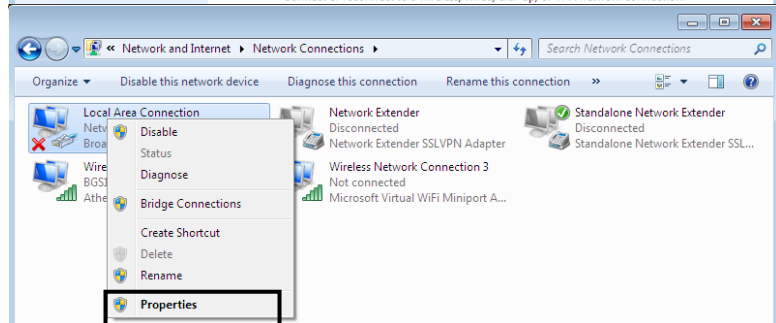
1. Go to **Start**. Click on **Control Panel**. Then click on **Network and Internet**.



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

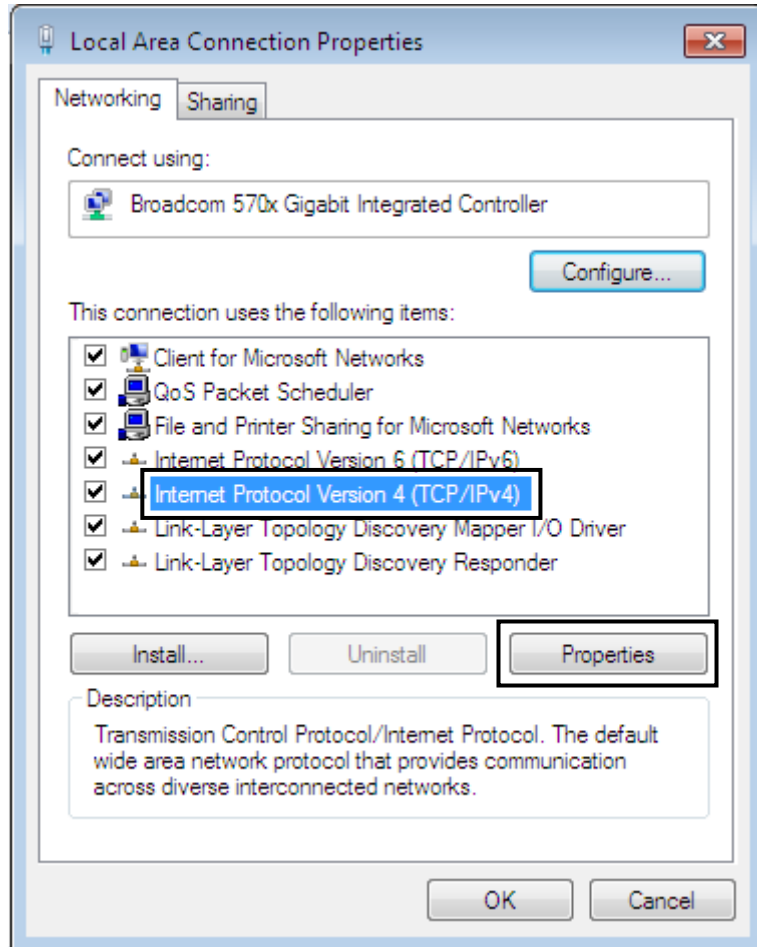


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

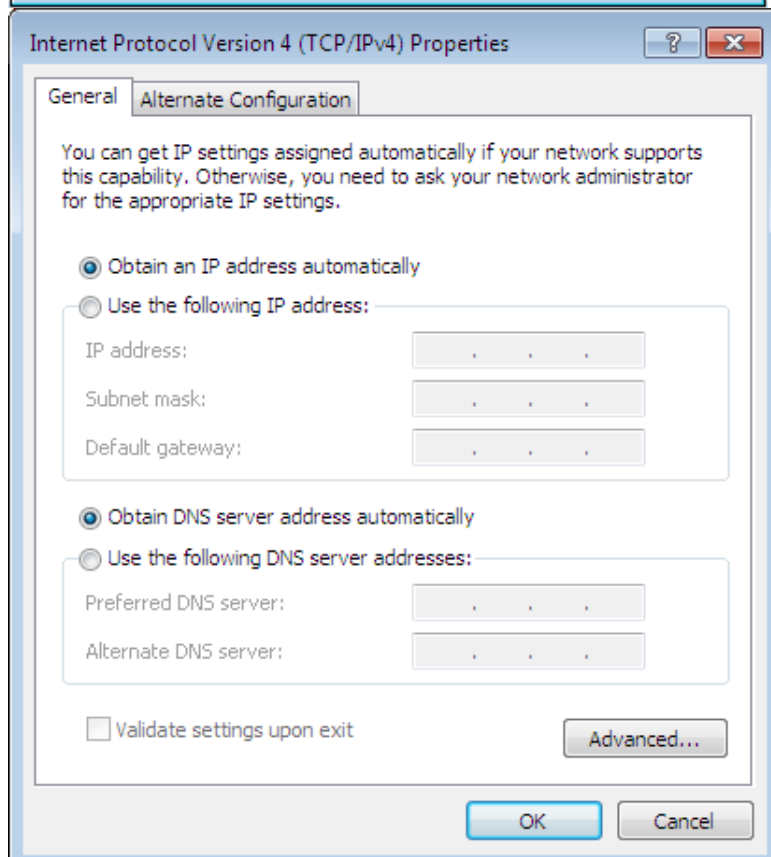


IPv4:

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

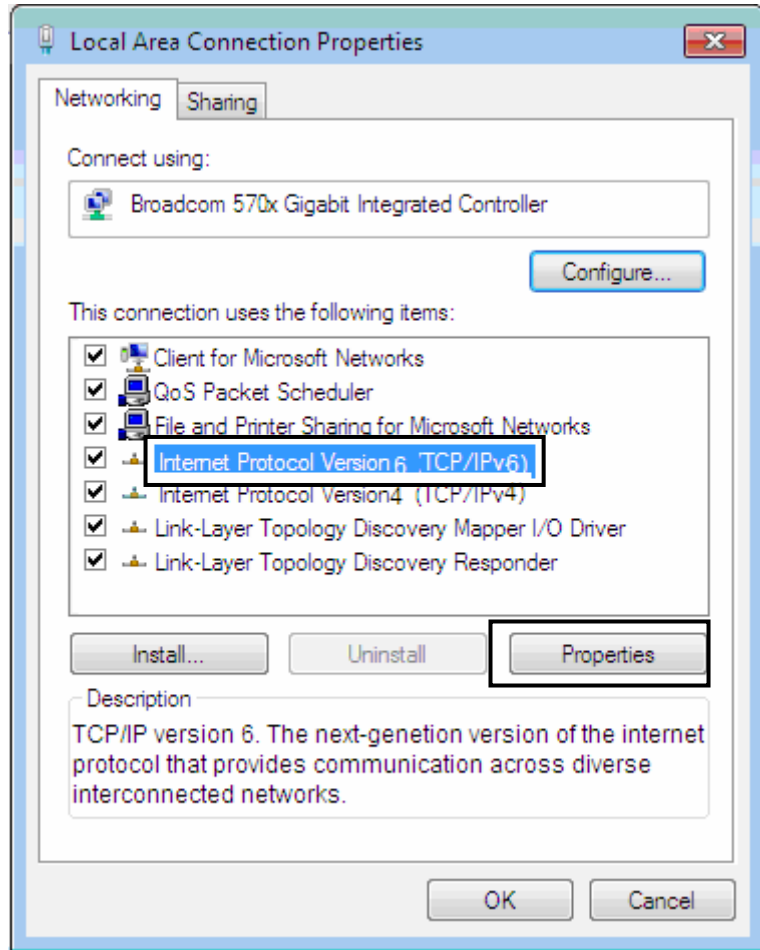


5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.

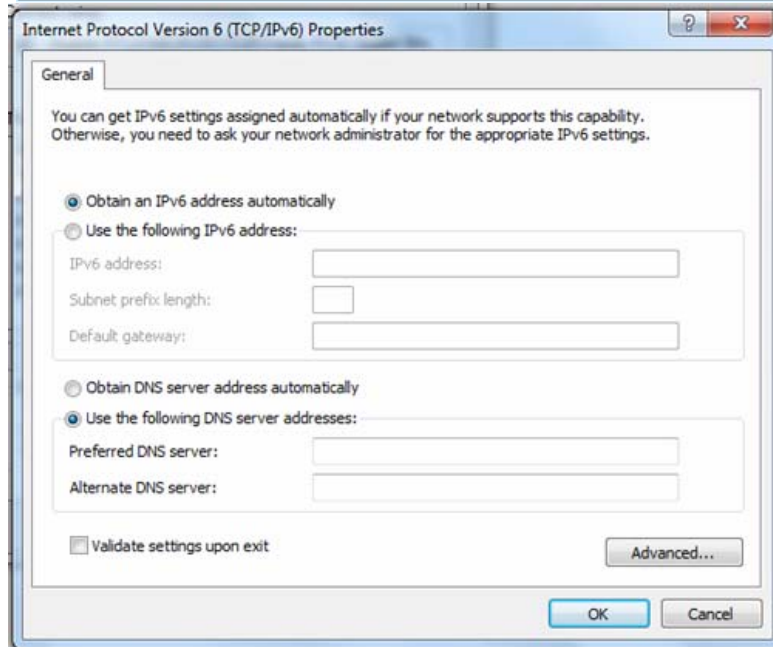


IPv6:

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

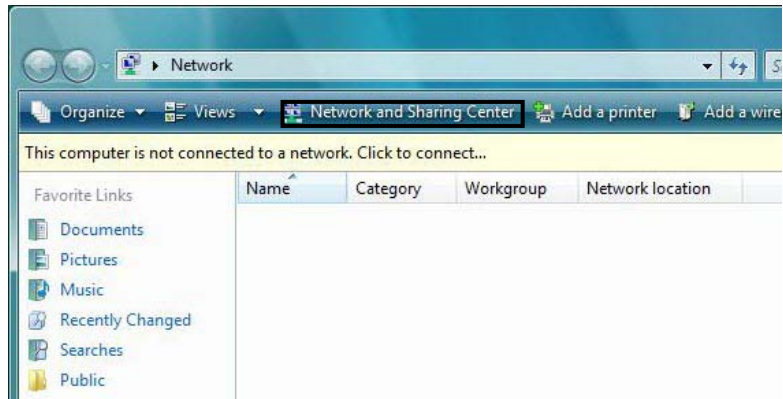


5. In the **TCP/IPv6 properties** window, select the **Obtain an IPv6 address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



3.1.2 Configuring a PC in Windows Vista

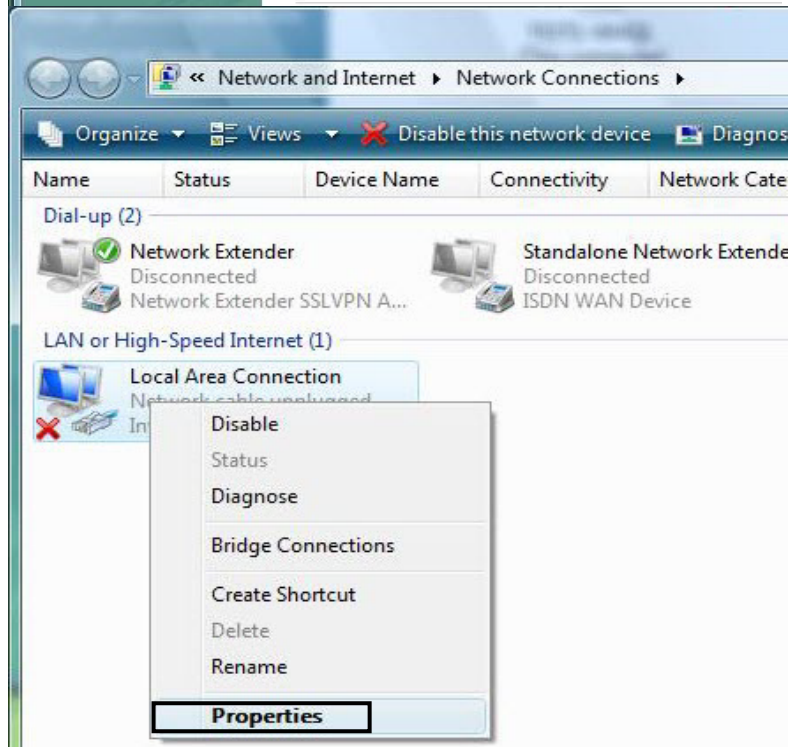
1. Go to **Start**. Click on **Network**. Then click on **Network and Sharing Center** at the top bar.



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

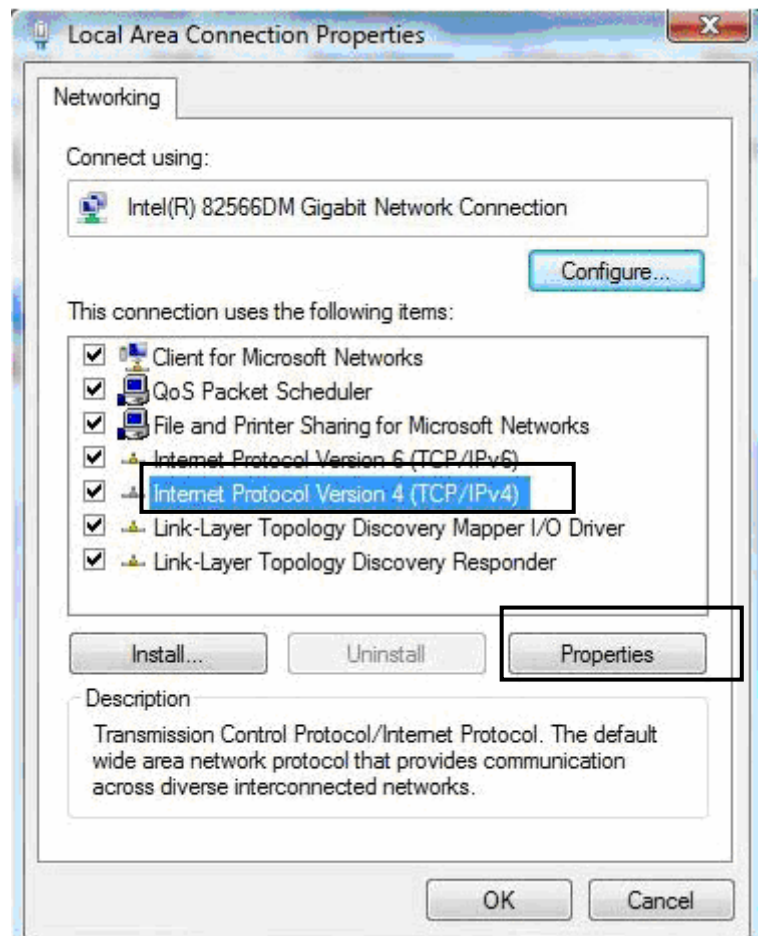


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

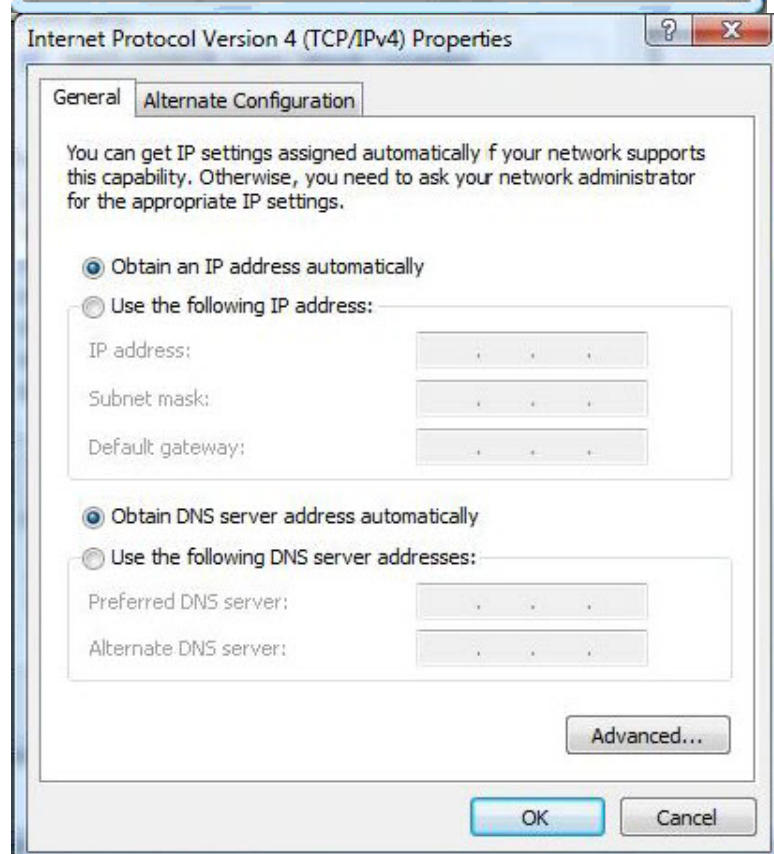


IPv4:

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



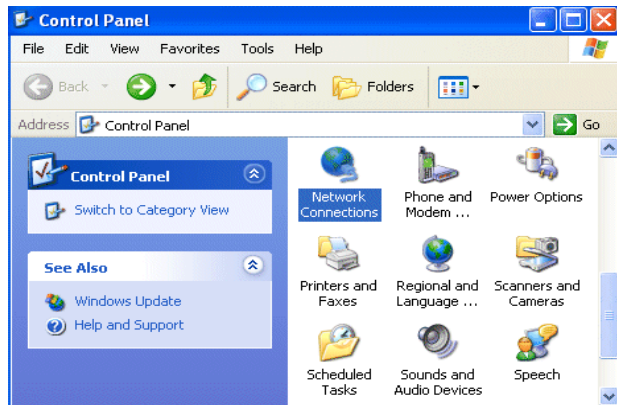
5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



3.1.3 Configuring a PC in Windows XP

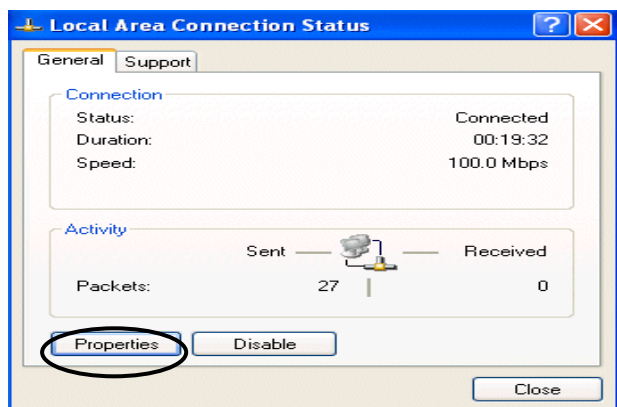
IPv4:

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

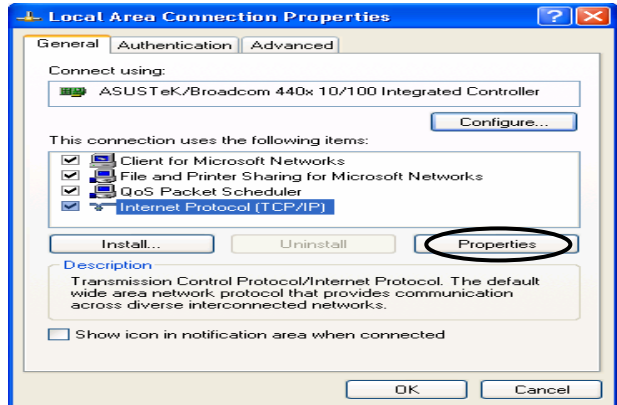


2. Double-click **Local Area Connection**.

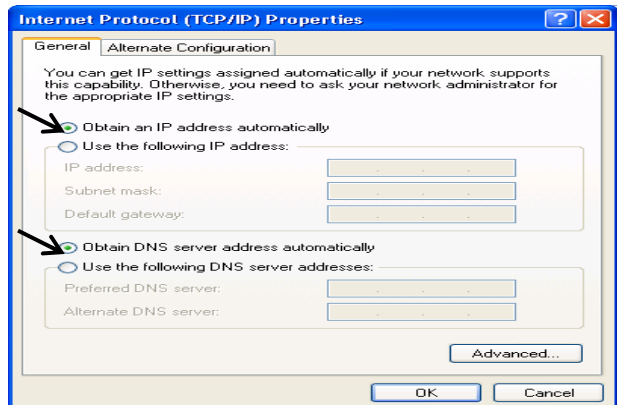
3. In the **Local Area Connection Status** window, click **Properties**.



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



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

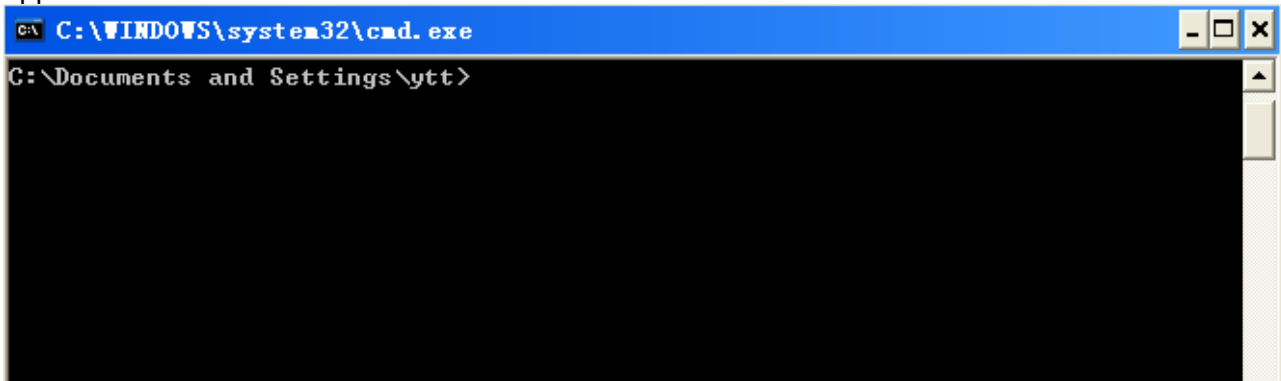


6. Click **OK** to finish the configuration.

IPv6:

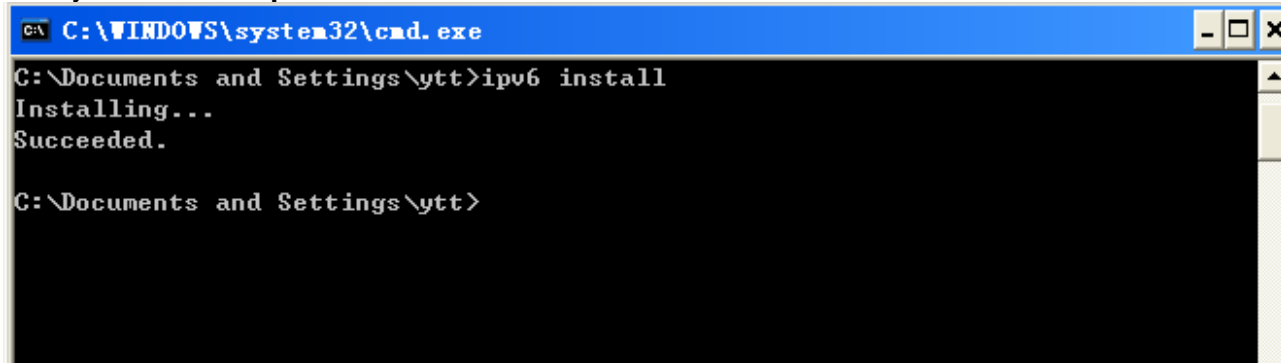
IPv6 is supported by Windows XP, but you should install it first.
Act as shown below:

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



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>
```

2. Key in command **ipv6 install**



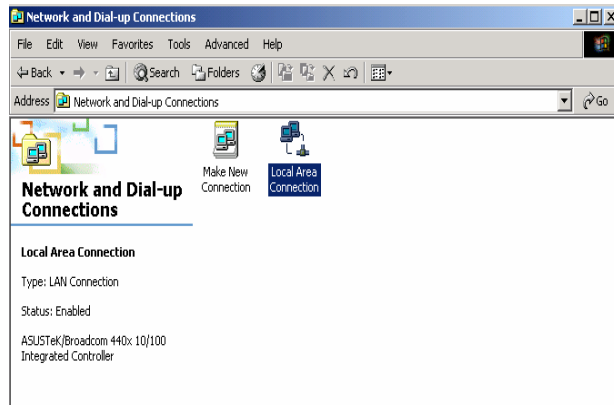
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\ytt>ipv6 install
Installing...
Succeeded.
C:\Documents and Settings\ytt>
```

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

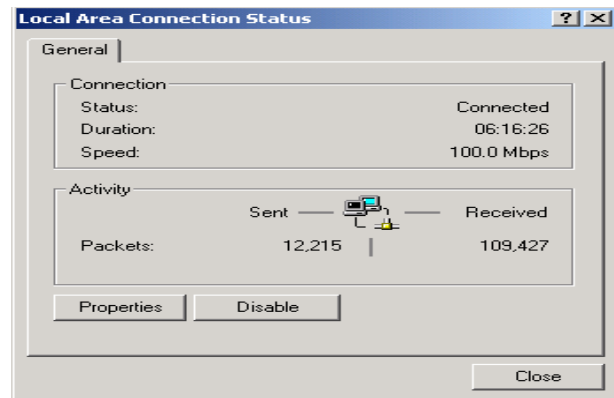
3.1.4 Configuring a PC in Windows 2000

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

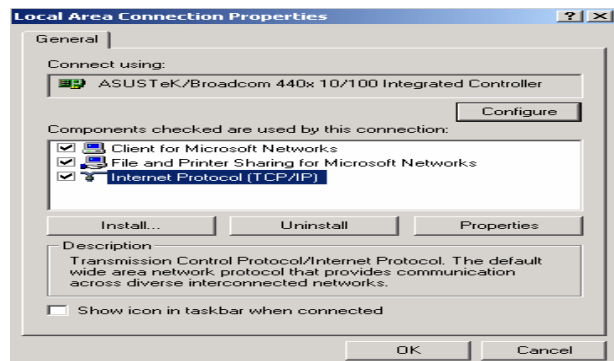
2. Double-click **Local Area Connection**.



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

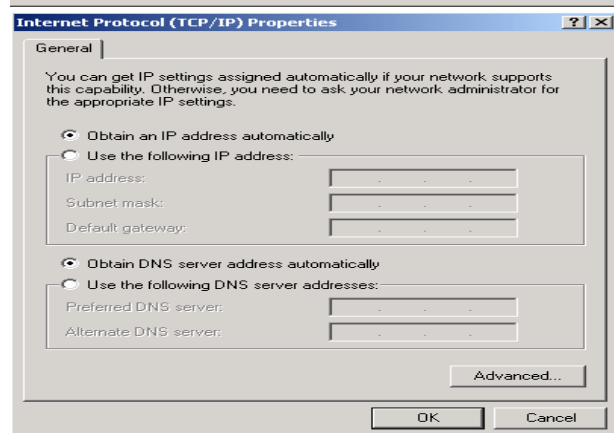


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



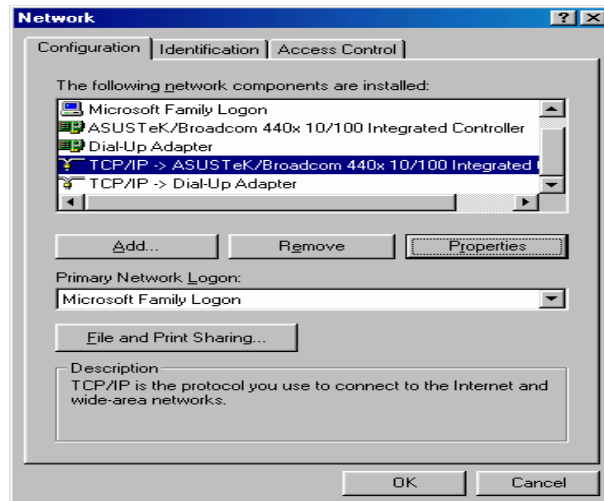
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

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

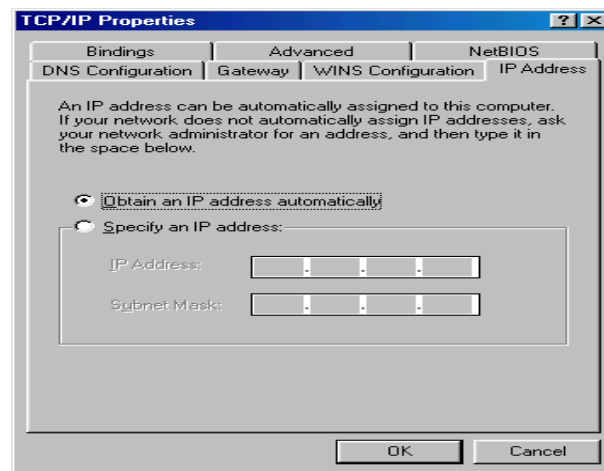


3.1.5 Configuring a PC in Windows 98/Me

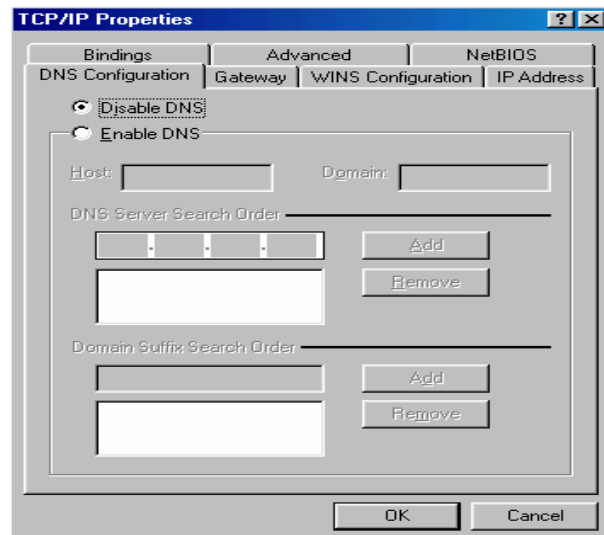
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.



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

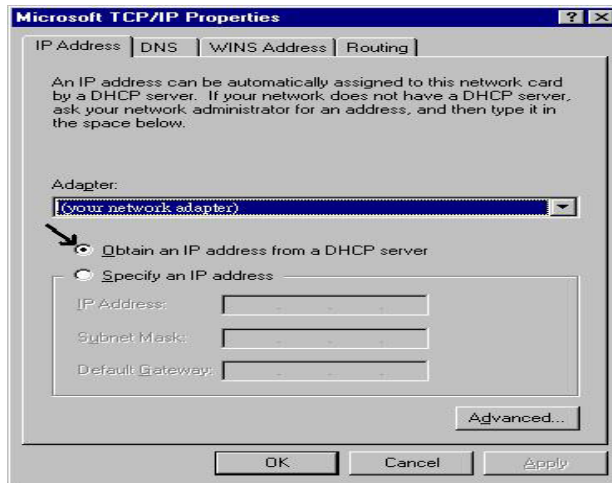
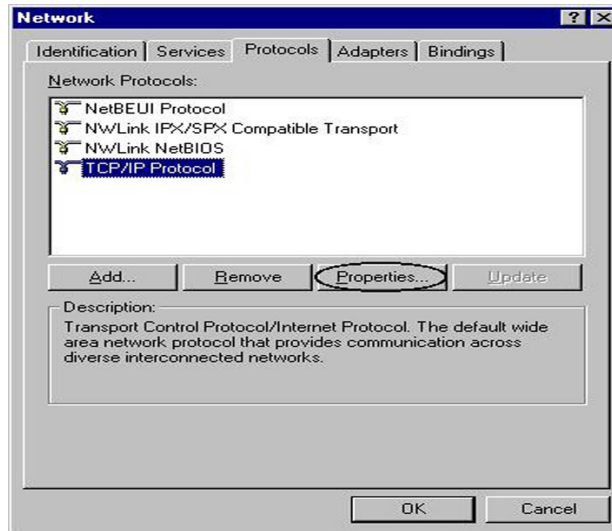


4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.



3.1.6 Configuring a PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.
3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



3.2 Factory Default Settings

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

Web Interface:

- ✘ Username: admin
- ✘ Password: admin

LAN Device 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: 20

3.2.1 Username and Password

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



If you ever forget the password to log in, you may press the **RESET** button up to **6** seconds to restore the factory default settings.

Attention

3.3 LAN Port Addresses

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

IPv4:

IP address	192.168.1.254
Subnet Mask	255.255.255.0
DHCP server function	Enabled
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199

3.4 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.

EWAN:

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	Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
Static IP Address	Static IP Address, IP Subnet Mask, Gateway IP Address, and Domain Name System (DNS) IP address.
Bridge Mode	Pure bridge.

Chapter 4 Configuration

4.1 Configuring BIPAC 6300VNOZ with your Web Browser

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



Congratulation! You are now successfully logged on to the BIPAC 6300VNOZ!

The image shows the web interface of a BEC Technologies 4G/LTE VoIP Gigabit Wireless Router. The top header features the BEC Technologies logo on the left and the router model name "4G/LTE VoIP Gigabit Wireless Router" in the center. A left sidebar contains navigation links: "Status", "Quick Start", "Configuration", and "Language". The main content area is titled "Status" and displays "Device Information" in a table format. The table lists various system parameters and their values. At the bottom right of the interface are "Restart" and "Logout" buttons. A footer at the very bottom contains the copyright notice: "Copyright © BEC Technologies, Ltd. All rights reserved."

Device Information	
Model Name	BEC 6300VNL
Firmware Version	1.02b.rc6.dt5
MAC Address	00:04:ED:63:AA:05
LAN	
IPv4	
IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCPv4 Server	Enable
IPv6	
IP Address	2001:b010:7030:f801:204:edff:fe63:aa05
Prefix Length	64
DHCPv6 Server	Enable Stateless

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status**(Device Info, System Log, Statistics, DHCP Table, Disk Status, VoIP Status)
- **Quick Start** (Wizard Setup)
- **Configuration** (Interface Setup, Advanced Setup, VoIP, Access Management, Maintenance)
- **Language**

Please see the relevant sections of this manual for detailed instructions on how to configure your router.

4.2 Status


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

4.2.1 Device Info

Users will see device's basic information in this page.

EWAN

Status



Device Information

Model Name	BiPAC 6300VNOZ
Firmware Version	1.02b.rc6.dt5
MAC Address	00:04:ED:63:AA:03

LAN

IPv4

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCPv4 Server	Enable

IPv6

IP Address	2001:b010:7030:f801:204:edff:fe63:aa03
Prefix Length	64
DHCPv6 Server	Enable Stateless

WAN

Interface	<input type="text" value="EWAN"/>
Service	<input type="text" value="0"/>
PPP Connection Time	0d: 0h:20m:48s

IPv4

Status	Connected
IP Address	1.169.140.134
Subnet Mask	255.255.255.255
Default Gateway	168.95.98.254
DNS Server	168.95.192.1

IPv6

Status	Connected
IP Address	2001:b010:7030:f800:80b9:43e2:e7a:b792
Prefix Length	64
Default Gateway	fe80::90:1a00:2a2:8506
DNS Server	2001:b000:168::1

■ Device Information

Model Name: Show model name of the router

Firmware Version: This is the Firmware version

MAC Address: This is the MAC Address

■ LAN

➤ IPv4:

IP Address: LAN port IPv4 address.

Subnet Mask: LAN port IP subnet mask.

DHCPv4 Server: LAN port DHCP role - Enabled, Relay or Disabled.

➤ IPv6:

IP Address: LAN port IPv6 address.

Prefix Length: The prefix length

DHCPv6 Server: The DHCP status.

■ WAN

Interface: The now used connection method, "EWAN".

Service: The WAN interface service index.

PPP Connection Time: The time totaled since PPP has been successfully connected.

➤ IPv4:

Status: The connection status, Not connected or Connected.

IP Address: WAN port IP address.

Subnet Mask: WAN port IP subnet mask.

Default Gateway: The IP address of the default gateway.

DNS Server: DNS information.

➤ IPv6:

Status: The IPv6 connection status.

IP Address: WAN port IPv6 address.

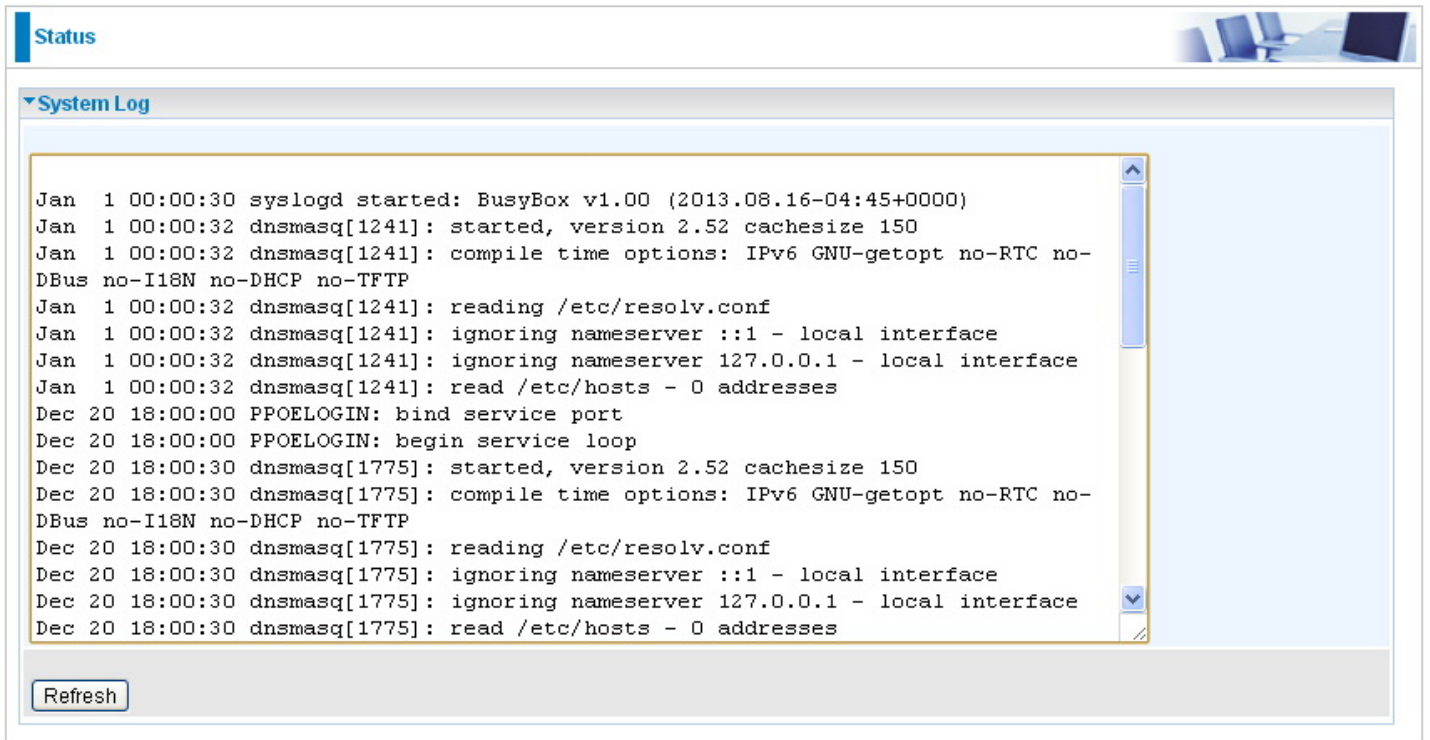
Prefix Length: The prefix length of IPv6 address.

Default Gateway: The IP address of the default gateway.

DNS Server: DNS information.

4.2.2 System Log

In system log, users can check the operations to the router and track the glitches to the router when occurred.



The screenshot shows a web interface with a 'Status' tab and a 'System Log' section. The log contains the following entries:

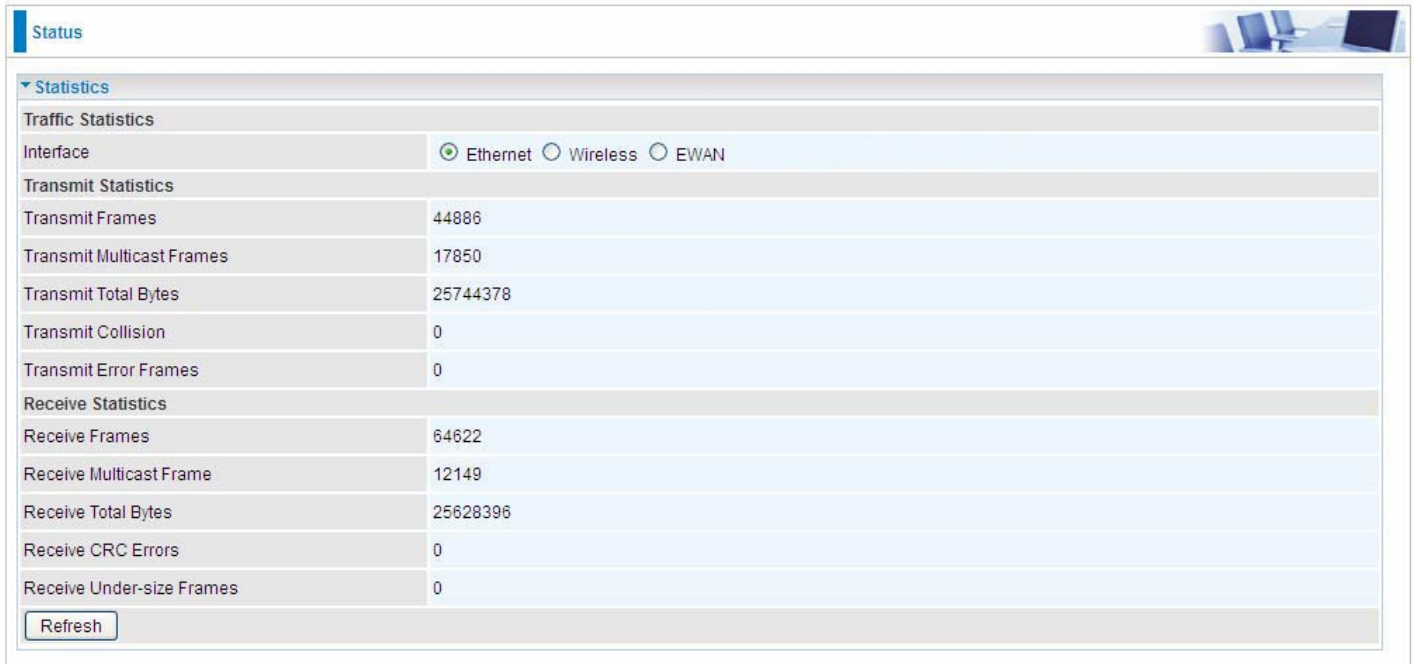
```
Jan 1 00:00:30 syslogd started: BusyBox v1.00 (2013.08.16-04:45+0000)
Jan 1 00:00:32 dnsmasq[1241]: started, version 2.52 cachesize 150
Jan 1 00:00:32 dnsmasq[1241]: compile time options: IPv6 GNU-getopt no-RTC no-
DBus no-I18N no-DHCP no-TFTP
Jan 1 00:00:32 dnsmasq[1241]: reading /etc/resolv.conf
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
```

Below the log is a 'Refresh' button.

Refresh: Press this button to refresh the statistics.

4.2.3 Statistics

➤ Ethernet



The screenshot shows a web interface for Ethernet statistics. At the top, there is a 'Status' tab and a small image of a computer workstation. Below this is a 'Statistics' section with a dropdown arrow. Underneath, there is a 'Traffic Statistics' section with an 'Interface' field set to 'Ethernet' (selected with a radio button), and options for 'Wireless' and 'EWAN'. The main part of the interface is a table with two columns: the left column lists various statistics, and the right column shows their corresponding values. At the bottom left of the table area is a 'Refresh' button.

Traffic Statistics	
Interface	<input checked="" type="radio"/> Ethernet <input type="radio"/> Wireless <input type="radio"/> EWAN
Transmit Statistics	
Transmit Frames	44886
Transmit Multicast Frames	17850
Transmit Total Bytes	25744378
Transmit Collision	0
Transmit Error Frames	0
Receive Statistics	
Receive Frames	64622
Receive Multicast Frame	12149
Receive Total Bytes	25628396
Receive CRC Errors	0
Receive Under-size Frames	0

Refresh

Interface: This field displays the type of port

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.

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.

Status 

▼ Statistics

Traffic Statistics

Interface Ethernet Wireless EWAN

Transmit Statistics

Transmit Frames	392357
Transmit Error Frames	12357
Transmit Drop Frames	12357

Receive Statistics

Receive Frames	253244
Receive Error Frames	18429
Receive Drop Frames	18429

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.

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.

Status

▼ Statistics

Traffic Statistics

Interface Ethernet Wireless EWAN

Transmit Statistics

Transmit Frames	25681
Transmit Multicast Frames	133
Transmit Total Bytes	5260625
Transmit Collision	0
Transmit Error Frames	0

Receive Statistics

Receive Frames	39225
Receive Multicast Frame	12357
Receive Total Bytes	20308279
Receive CRC Errors	0
Receive Under-size Frames	0

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.

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.

4.2.4 DHCP Table

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



The screenshot shows a web interface with a 'Status' tab and a 'DHCP Table List' section. The table contains one row of data with the following columns: #, Host Name, IP Address, MAC Address, and Expire Time.

#	Host Name	IP Address	MAC Address	Expire Time
1	billion-17bc5f1	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.

4.2.5 Disk Status



The screenshot shows a web interface with a 'Status' header and a 'Disk status' section. The 'Disk status' section contains a table with three columns: 'Partition', 'Disk Space(KB)', and 'Free Space(KB)'. The table has one data row for 'usb1_1'.

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

Partition: Display the USB storage partition.

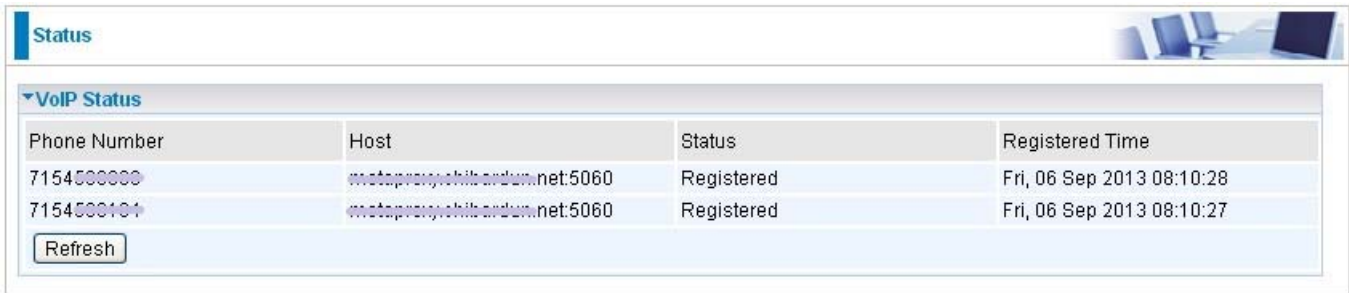
Disk Space(KB): Display the total storage space of the NAS in KBytes unit.

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

4.2.6 VoIP Status

4.2.6.1 VoIP Status

VoIP status give users a directive picture on the registered VoIP accounts.



Phone Number	Host	Status	Registered Time
7154500000	metaprosy.chibardun.net:5060	Registered	Fri, 06 Sep 2013 08:10:28
7154500101	metaprosy.chibardun.net:5060	Registered	Fri, 06 Sep 2013 08:10:27

Refresh

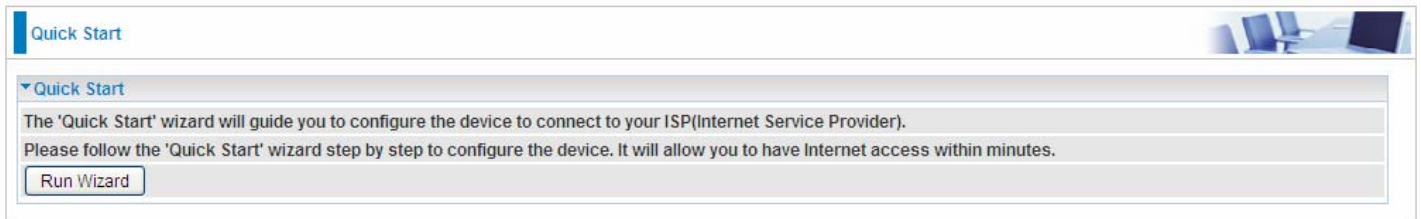
Phone Number: The phone number user registers and fills in the Basic page of VoIP.

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.

4.3 Quick Start



Quick Start

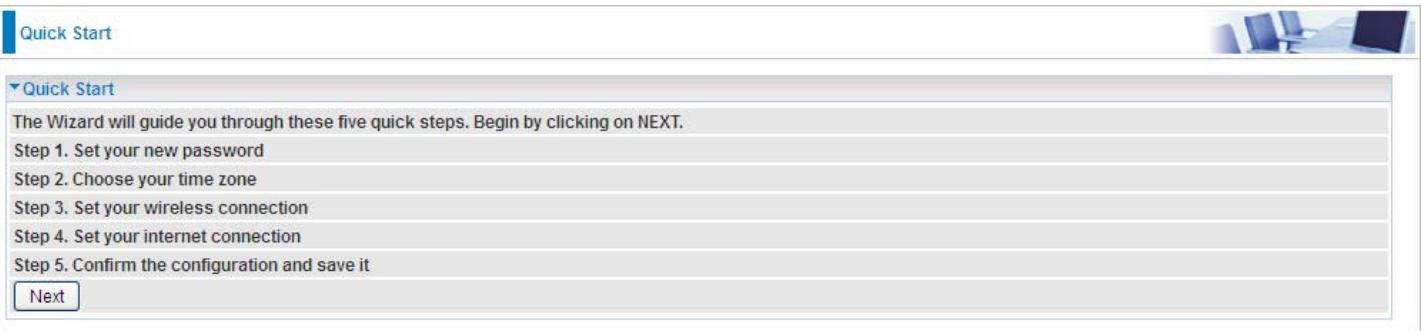
Quick Start

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.

Run Wizard

For detailed instructions on configuring WAN settings, see the **Interface Setup** section of this manual.

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



Quick Start

Quick Start

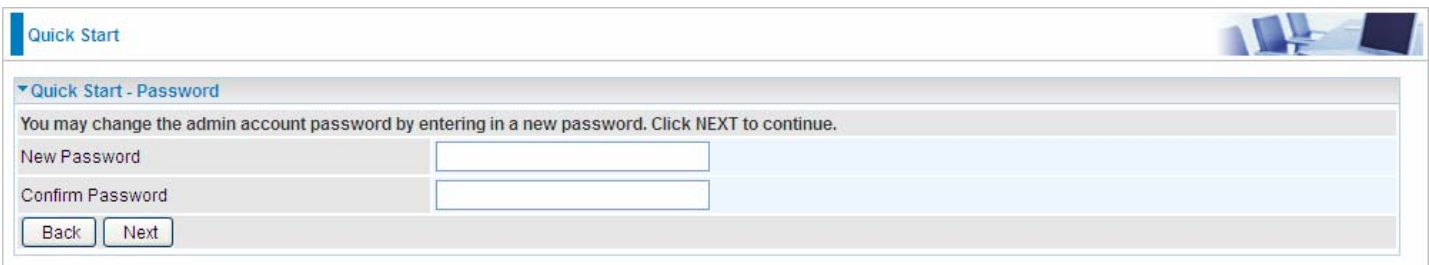
The Wizard will guide you through these five quick steps. Begin by clicking on NEXT.

- 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

Next

Click **NEXT** to enter step 1.

Step1. Set new password of the “admin” account. The password was used to manage the web access. The default is “admin”. Once changed, please remember carefully. 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

Back Next

Step2: 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

Back Next

Step3: Set your wireless connection. Click **NEXT** to continue.

Quick Start 

▼ Quick Start - Wireless

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

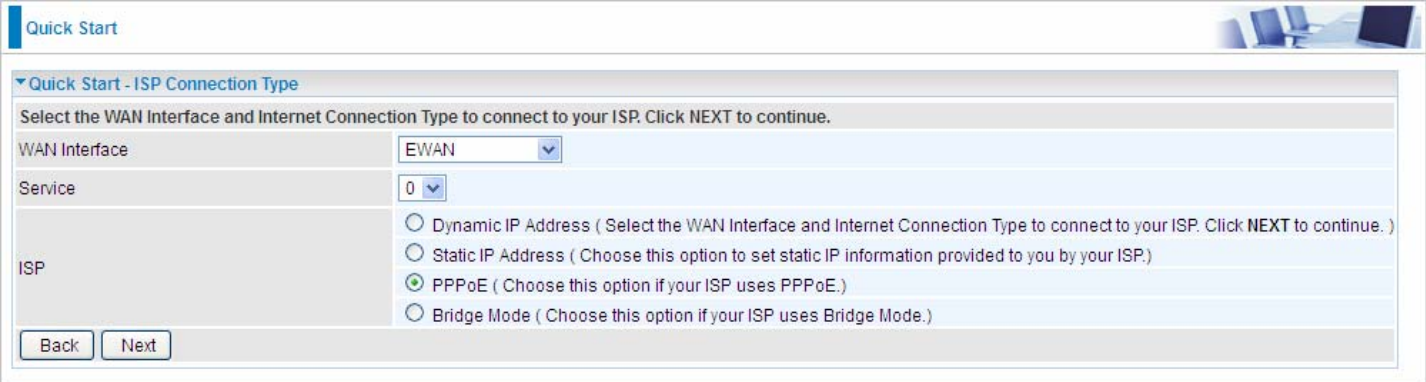
Access Point	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
SSID	<input type="text" value="wlan-ap_715"/>
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Channel	<input type="text" value="UNITED STATES"/> <input type="text" value="06"/>
Security Type	<input type="text" value="Mixed WPA2/WPA-PSK"/>
WPA Algorithms	<input type="text" value="TKIP+AES"/>
Pre-Shared Key	<input type="text" value="E5C7EB09"/> (8-63 characters or 64 Hex string)
Key Renewal Interval	<input type="text" value="600"/> seconds (10 ~ 4194303)

Step4: Set your Internet connection

WAN Transfer Modes: EWAN

➤ EWAN

1). Select EWAN. Refer to your ISP to choose the appropriate connection protocol. Click **NEXT** to continue.



Quick Start

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

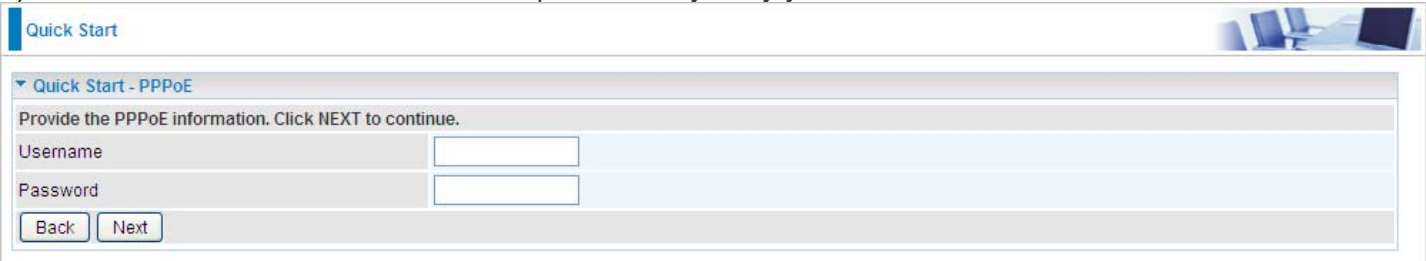
Service: 0

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.)

Back Next

2). Enter the PPPoE account information provided to you by your ISP. Click **NEXT** to continue.



Quick Start

Quick Start - PPPoE

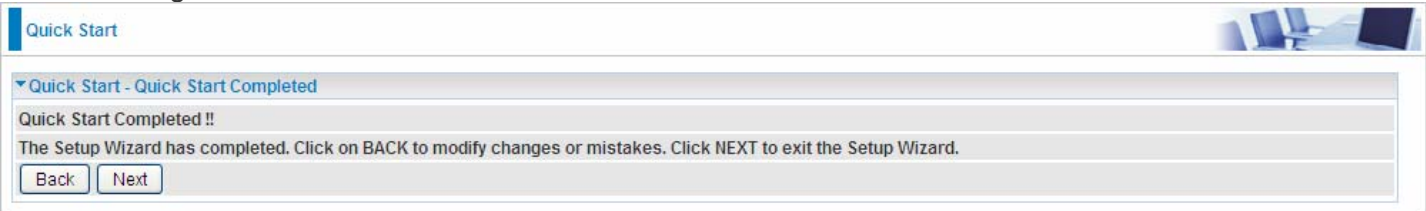
Provide the PPPoE information. Click NEXT to continue.

Username: []

Password: []

Back Next

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



Quick Start

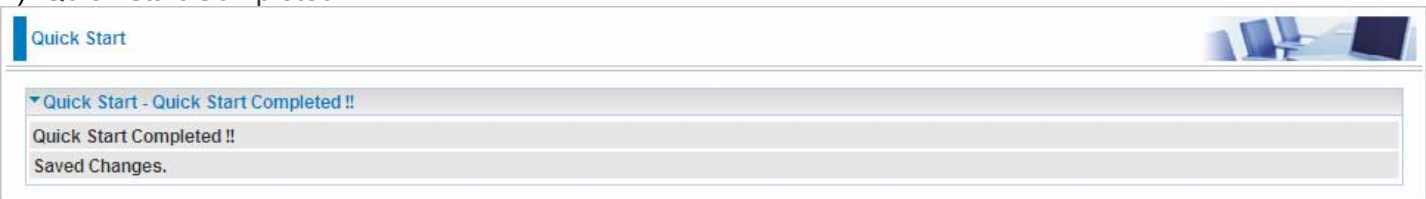
Quick Start - Quick Start Completed

Quick Start Completed !!

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

Back Next

4). Quick Start Completed!




Quick Start

Quick Start - Quick Start Completed !!

Quick Start Completed !!

Saved Changes.

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

Status 

Device Information

Model Name	BiPAC 6300VNOZ
Firmware Version	1.02b.rc6.dt5
MAC Address	00:04:ED:63:AA:03

LAN

IPv4

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCPv4 Server	Enable

IPv6

IP Address	2001:b010:7030:f801:204:edff:fe63:aa03
Prefix Length	64
DHCPv6 Server	Enable Stateless

WAN

Interface	<input type="text" value="EWAN"/>
Service	<input type="text" value="0"/>
PPP Connection Time	0d: 0h:20m:48s

IPv4

Status	Connected
IP Address	1.169.140.134
Subnet Mask	255.255.255.255
Default Gateway	168.95.98.254
DNS Server	168.95.192.1

IPv6

Status	Connected
IP Address	2001:b010:7030:f800:80b9:43e2:e7a:b792
Prefix Length	64
Default Gateway	fe80::90:1a00:2a2:8506
DNS Server	2001:b000:168::1

4.4 Configuration


Click this item to access the following sub-items that configure the router: **Interface Setup**, **Advanced Setup**, **VoIP**, **Access Management**, and **Maintenance**.

4.4.1 Interface Setup

First, let us take a look at the **Interface Setup**. There are four items contained in this section, namely, **Internet**, **LAN**, **Wireless** and **Wireless MAC Filter**. Each is described in the following scenario.

4.4.1.1 Internet

➤ EWAN

Configuration 

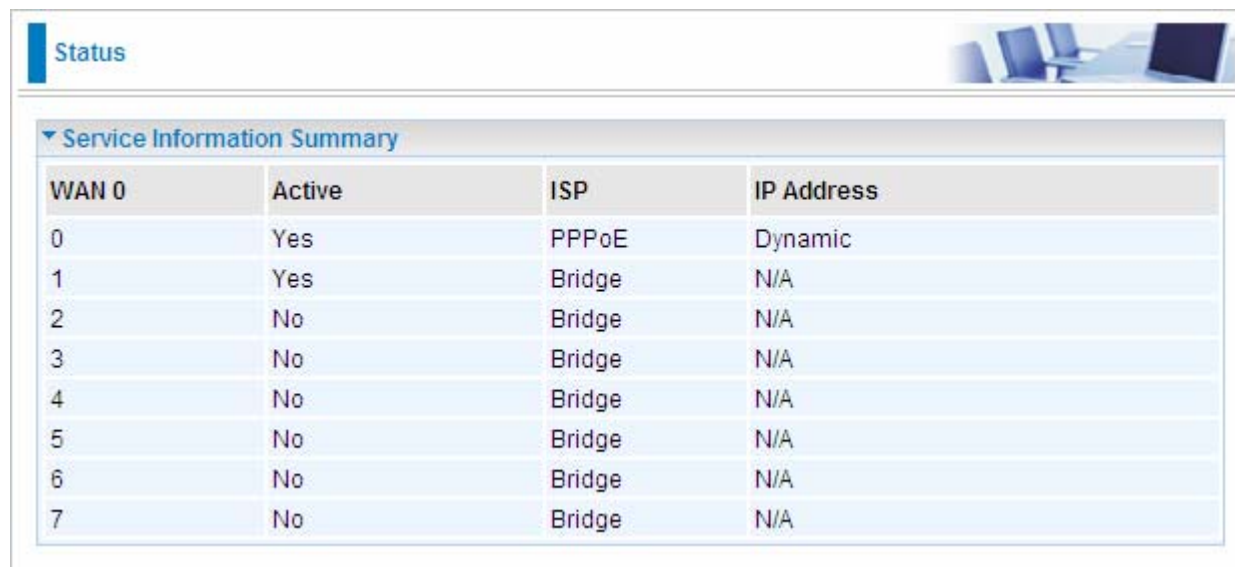
▼ Internet

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

Multi Service

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

Service Summary: The diagram for view of service information.



The screenshot shows a network configuration interface. At the top left, there is a 'Status' tab. Below it, a section titled 'Service Information Summary' contains a table with the following data:

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 users' environment.

Here we take IPv4/IPv6 for example, when you just choose IPv4 or IPv6, you can just get information from the following listed parameters.

ISP Connection Type:

ISP: Select the encapsulation type your ISP uses.

- ① **Dynamic IP:** Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.
- ① **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, which is 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.
- ① **PPPoE:** Select this option if your ISP requires you to use a PPPoE connection.
- ① **Bridge:** Select this mode if you want to use this device as an OSI layer 2 device like switch.

802.1q Options

802.1q: Select whether to activate 802.1q feature. When activated, please enter the the 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

Username: Enter the user name exactly as your ISP assigned.

Password: Enter the password associated with the user name above.

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:

- ① **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.
- ① **Connect Manually:** Select Connect Manually when you don't want the connection up all the time.

TCP MSS Option: Enter the TCP Maximum Segment Size (MSS).

■ IP Options

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

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.

- ① **None** is for disabling the RIP function.
- ① **Both** means the router will periodically send routing information and accept routing information then incorporate into routing table.
- ① **IN only** means the router will only accept but will not send RIP packet.
- ① **OUT only** means the router will only send but will not accept RIP packet.

TCP MTU Option: Maximum Transmission Unit, the maximum is 1500.

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.

Status


▼ Device Information

Model Name	BiPAC 6300VNOZ
Firmware Version	1.02b.rc6.dt5
MAC Address	00:04:ED:63:AA:03

LAN

IPv4

IP Address	192.168.1.254
Subnet Mask	255.255.255.0
DHCPv4 Server	Enable

IPv6

IP Address	2001:b010:7030:f801:204:edff:fe63:aa03
Prefix Length	64
DHCPv6 Server	Enable Stateless

WAN

Interface	<input type="text" value="EWAN"/>
Service	<input type="text" value="0"/>
PPP Connection Time	0d: 0h:20m:48s

IPv4

Status	Connected
IP Address	1.169.140.134
Subnet Mask	255.255.255.255
Default Gateway	168.95.98.254
DNS Server	168.95.192.1

IPv6

Status	Connected
IP Address	2001:b010:7030:f800:80b9:43e2:e7a:b792
Prefix Length	64
Default Gateway	fe80::90:1a00:2a2:8506
DNS Server	2001:b000:168::1

4.4.1.2 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.

IPv6

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

There are two ways to dynamically configure IPv6 address on hosts. One is statefull configuration, for example using DHCPv6 (which resembles its counterpart DHCP in IPv4.) In the stateful autoconfiguration model, hosts obtain interface addresses and/or configuration information and parameters from a DHCPv6 server. The Server maintains a database that keeps track of which addresses have been assigned to which hosts.

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

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	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled <input type="radio"/> Relay
Start IP	<input type="text" value="192.168.1.100"/>
IP Pool Count	<input type="text" value="20"/>
Lease Time	<input type="text" value="86400"/> seconds (0 sets to default value of 259200)
Physical Ports	<input checked="" type="checkbox"/> LAN1 <input checked="" type="checkbox"/> LAN2 <input checked="" type="checkbox"/> LAN3 <input checked="" type="checkbox"/> WLAN1
DNS Relay	<input checked="" type="radio"/> Automatically <input type="radio"/> Manually
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

DHCPv4 Server: If set to **Enabled**, your BIPAC 6300VNOZ 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 6300VNOZ 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	<input type="text"/>
MAC Address	<input type="text"/>

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

IPv6 parameters

IPv6 Parameters	
Interface Address/Prefix Length	<input type="text"/> / <input type="text"/>
MLD Snooping	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
DHCPv6 Server	
DHCPv6 Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
DHCPv6 Server Type	<input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
Start Interface ID	<input type="text"/>
End Interface ID	<input type="text"/>
Lease Time	<input type="text"/> seconds(0 sets to default value of 4800)
Router Advertisements	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

Interface Address / Prefix Length: enter the static LAN IPv6 address, we suggest leave the field empty because when setted wrong, it will result in LAN devices not being able to access other IPv6 device through internet. 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

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 whether to enable issue Router Advertisement feature. It is to send Router Advertisement messages periodically. Router will multicast the v6 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.**

4.4.1.3 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	<input checked="" type="radio"/> Activated <input type="radio"/> 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	<input checked="" type="radio"/> Yes <input type="radio"/> No

11n Settings

Channel Bandwidth	40 MHz
Guard Interval	Auto
MCS	Auto

SSID Settings

Available SSID	1
SSID Index	<input checked="" type="radio"/> SSID1
SSID	wlan-ap_715
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSID Activated	Always

WPS Settings

Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input type="radio"/> PIN code <input checked="" type="radio"/> 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	<input type="radio"/> Activated <input checked="" type="radio"/> 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 how many SSIDs you want to lay out. A total of 4 is in list. By default 4 SSIDs are in use.

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 [4.4.2.8 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 networks 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 following **Wi-Fi Protected Setup**.

Wi-Fi Protected Setup

PIN Method: Configure AP as Registrar

1. Jot down the client's Pin (eg. 04640776).

SSID Settings	
SSID Num	1 ▾
SSID Index	<input checked="" type="radio"/> SSID1
SSID	Billion_AP
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSID Activated	Always ▾
WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input checked="" type="radio"/> PIN code <input type="radio"/> PBC
AP PIN Code	03454435 <input type="button" value="Generate"/>
Enrollee PIN Code	04640776
WPS Progress	In progress <input type="button" value="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)

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

3. Launch the wireless client's WPS utility (eg. Ralink Utility). Set the Config Mode as Enrollee, press the WPS button on the top bar, select the AP (eg. 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.

The screenshot displays the WPS utility interface with the following components:

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

ID :	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:** (Empty)
- Configuration Panel:**
 - Config Mode:** Enrollee
 - Buttons:** Rescan, Information, Pin Code (04640776), Renew, Detail, Connect, Rotate, Disconnect, Export Profile, Delete.
 - WPS Associate IE:** WPS Associate IE
 - WPS Probe IE:** WPS Probe IE
 - Progress:** Progress >> 0%
 - Status:** PIN - WPS Eap process failed
- Performance Metrics:**
 - Link Quality >> 0%
 - Signal Strength1 >> 0%
 - Signal Strength2 >> 0%
 - Noise Strength >> 0%
 - Transmit:** Link Speed >> Max, Throughput >> 2,736 Kbps
 - Receive:** Link Speed >> Max, Throughput >> 60,120 Kbps
- Network Information:**
 - HT
 - BW >> n/a, SNR0 >> n/a
 - GI >> n/a, MCS >> n/a, SNR1 >> n/a
- Left Sidebar:** Status >>, Extra Info >>, Channel >>, Authentication >>, Encryption >>, Network Type >>, IP Address >>, Sub Mask >>, Default Gateway >>

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

The screenshot displays a network management interface with the following components:

- Navigation Menu:** Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, About, Help.
- 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
- WPS Profile List:** Billion_AP
- WPS Configuration:**
 - Buttons: PIN, PBC
 - Options: WPS Associate IE, WPS Probe IE
 - Progress: Progress >> 100%
 - Status: WPS status is connected successfully
- WPS AP Details (Billion_AP):**
 - 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
- Performance Metrics:**
 - Link Quality >> 100%
 - Signal Strength 1 >> 41%
 - Signal Strength 2 >> 44%
 - Noise Strength >> 26%
 - Transmit: Link Speed >> 108.0 Mbps, Throughput >> 0.000 Kbps
 - Receive: Link Speed >> 1.0 Mbps, Throughput >> 109.204 Kbps
- HT (High Throughput) Settings:**
 - BW >> 40
 - GI >> long
 - MCS >> 5
 - SNRO >> 30
 - SNR1 >> 20102206

PIN Method: Configure AP as Enrollee

1. Jot down the WPS PIN (eg. 03454435). Press Start WPS.

SSID Settings	
SSID Num	1
SSID Index	<input checked="" type="radio"/> SSID1
SSID	Billion_AP
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSID Activated	Always
WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input checked="" type="radio"/> PIN code <input type="radio"/> PBC
AP PIN Code	03454435 <input type="button" value="Generate"/>
Enrollee PIN Code	<input type="text"/>
WPS Progress	In progress <input type="button" value="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 (eg. Ralink Utility). Set the Config Mode as Registrar. Enter the PIN number in the PIN Code column then choose the correct AP (eg. Billion_AP) from the WPS AP List before pressing the PIN button to run the scan.

The screenshot displays the WPS utility interface with the following components:

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

ID	AP Name	MAC Address	Priority	Key Icon
0x0000	Billion_AP	00-04-ED-85-46-92	1	
	Welcome to RFINICS	00-21-27-6A-2B-7E	8	🔑
	Mai-Lang	00-21-91-EE-2A-68	9	🔑
- WPS Profile List:** Billion_AP (selected)
- Configuration Panel:**
 - Buttons: PIN, PBC, WPS Associate IE (checked), WPS Probe IE (checked).
 - Progress bar: Progress >> 100%
 - Status: WPS status is connected successfully
 - Buttons: Rescan, Information, Pin Code (03454435), Renew, Config Mode (Registrar), Detail, Connect, Rotate, Disconnect, Export Profile.
- Status and Performance Metrics:**
 - 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 (High Throughput) section:
 - BW >> 40
 - GI >> short
 - MCS >> 7
 - SNRO >> 30
 - SNR1 >> 20102206
 - Link Quality >> 100% (Green bar)
 - Signal Strength 1 >> 24% (Red bar)
 - Signal Strength 2 >> 65% (Yellow bar)
 - Noise Strength >> 26% (Green bar)
 - Transmit section:
 - Link Speed >> 150.0 Mbps
 - Throughput >> 0.000 Kbps
 - Graph: 1.632 Kbps
 - Receive section:
 - Link Speed >> 1.0 Mbps
 - Throughput >> 118.144 Kbps
 - Graph: 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).

The screenshot displays the WPS configuration interface on a router. At the top, there are navigation tabs: Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, About, and Help. The main content area is divided into several sections:

- WPS AP List:** A table listing discovered APs.

ID	SSID	MAC	Priority	Key Icon
0x0000	Billion_AP	00-04-ED-85-46-92	1	
	Welcome to RFINICS	00-21-27-6A-2B-7E	8	🔑
	Mai-Lang	00-21-91-EE-2A-68	9	🔑
- WPS Profile List:** Shows the selected profile 'Billion_AP'.
- Configuration Options:** Includes checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. There are also buttons for 'PIN', 'PBC', and 'Progress >> 100%'. A message states 'WPS status is connected successfully'.
- Right-Hand Side Panel:** Contains buttons for 'Rescan', 'Information', 'Pin Code' (with input '03454435' and a 'Renew' button), 'Config Mode' (set to 'Registrar'), 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'.
- Status and Performance Metrics:**
 - 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 (High Throughput) Metrics:**
 - BW >> 40
 - GI >> short
 - MCS >> 7
 - SNR0 >> 30
 - SNR1 >> 20102206
- Link Quality and Signal Strength:**
 - Link Quality >> 100% (Green bar)
 - Signal Strength 1 >> 24% (Red bar)
 - Signal Strength 2 >> 65% (Yellow bar)
 - Noise Strength >> 26% (Green bar)
- Transmit and Receive Performance:**
 - Transmit:** Link Speed >> 150.0 Mbps, Throughput >> 0.000 Kbps. A bar chart shows a peak of 1.632 Kbps.
 - Receive:** Link Speed >> 1.0 Mbps, Throughput >> 118.144 Kbps. A bar chart shows a peak of 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.

PBC Method:

1. Press the PBC radio button, Then Start WPS.

SSID Settings	
SSID Num	1
SSID Index	<input checked="" type="radio"/> SSID1
SSID	Billion_AP
Broadcast SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
SSID Activated	Always
WPS Settings	
Use WPS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WPS State	Configured
WPS Mode	<input type="radio"/> PIN code <input checked="" type="radio"/> 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 (eg. Ralink Utility). Set the Config Mode as Enrollee. Then press the WPS button and choose the correct AP (eg. 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.

The screenshot displays the WPS configuration interface on a router. The 'WPS' tab is selected in the top navigation menu. The 'WPS AP List' table shows several available profiles, with 'Billion_AP' selected. The 'WPS Profile List' shows the details for 'Billion_AP'. The 'PIN' and 'PBC' buttons are both checked, and the 'WPS Associate IE' and 'WPS Probe IE' options are also checked. A progress bar indicates that the connection is 100% complete. The 'WPS status' message reads 'WPS status is connected successfully - 5200NRC'. The bottom section provides detailed connection statistics for the 'Billion_AP' profile, including link quality, signal strength, noise strength, and throughput for both transmit and receive directions.

ID :	WLAN-AP	MAC	Channel	Priority
ID : 0x0004	Billion_AP	00:04:ED:85:46:92	1	1
ID :	111111	00-0C-43-30-52-50	7	7
ID :	Welcome to RFINICS	00-21-27-6A-2B-7E	8	8

Profile Name
Billion_AP

PIN	<input checked="" type="checkbox"/> WPS Associate IE	Progress >> 100%
PBC	<input checked="" type="checkbox"/> WPS Probe IE	WPS status is connected successfully - 5200NRC

Status >> Billion_AP <-> 00-04-ED-85-46-92	Link Quality >> 100%
Extra Info >> Link is Up [TxPower:100%]	Signal Strength 1 >> 62%
Channel >> 1 <-> 2412 MHz; central channel: 6	Signal Strength 2 >> 86%
Authentication >> WPA2-PSK	Noise Strength >> 26%
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	SNRO >> 0
GI >> short	MCS >> 7
	SNR1 >> 20102453

Transmit	
Link Speed >> 72.2 Mbps	17.744 Kbps
Throughput >> 1.008 Kbps	
Receive	
Link Speed >> 1.0 Mbps	256.300 Kbps
Throughput >> 48.172 Kbps	

■ 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, 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.
<input checked="" type="radio"/> Key#1	<input type="text"/>
<input type="radio"/> Key#2	<input type="text"/>
<input type="radio"/> Key#3	<input type="text"/>
<input type="radio"/> Key#4	<input type="text"/>

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.

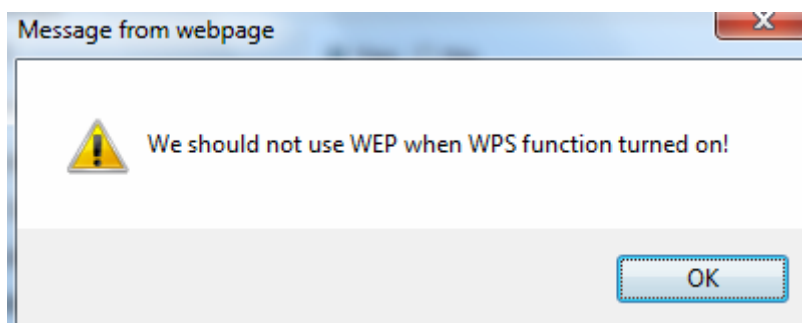
Key 1 to Key 4: Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for 64-bitWEP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



➤ **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 ASCII 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	<input checked="" type="radio"/> Activated <input type="radio"/> 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

4.4.1.4 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 to configure this screen.

Configuration

Wireless MAC Address Filter

SSID Index: SSID1

Active: Activated Deactivated

Action: Allow the follow Wireless LAN station(s) association.

MAC Address:

Save

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.

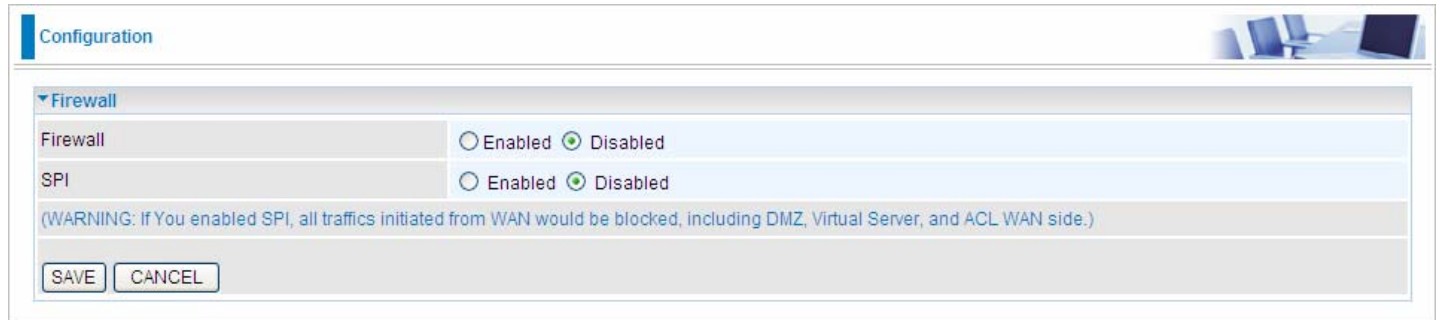
MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the specified in these address fields.

4.4.2 Advanced Setup

Advanced Step provides some advanced features including **Firewall**, **Routing**, **NAT**, **Static DNS**, **QoS**, **Internet Grouping**, **Port Isolation** and **Time Schedule** for all advanced users. Please move on to have a picture of what the exact feature is about and how to use it.

4.4.2.1 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.)

SAVE CANCEL

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

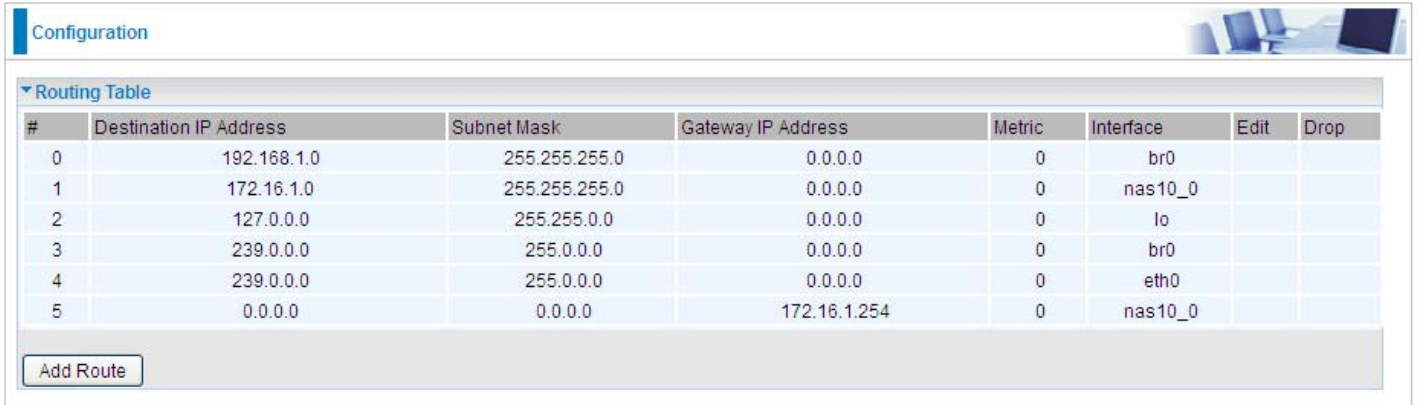
- ① **Enabled:** It activates your firewall function.
- ① **Disabled:** It disables the firewall function.

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

- ① **Enabled:** It activates your SPI function.
- ① **Disabled:** It disables the SPI function.

4.4.2.2 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.



The screenshot shows a 'Configuration' window with a 'Routing Table' section. The table has 8 columns: '#', 'Destination IP Address', 'Subnet Mask', 'Gateway IP Address', 'Metric', 'Interface', 'Edit', and 'Drop'. There are 6 rows of data. Below the table is an 'Add Route' button.

#	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	<input type="text" value="0.0.0.0"/>
Destination Subnet Mask	<input type="text" value="0.0.0.0"/>
Gateway IP Address / Interface	<input type="radio"/> 0.0.0.0 <input checked="" type="radio"/> EWAN_0
Metric	<input type="text" value="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.

4.4.2.3 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.



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

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.



The screenshot shows a web configuration page titled "Configuration". Under the "DMZ" section, there are three rows of configuration options:

DMZ for	Multiple IPs Account/ EWAN Service ID 0
DMZ	<input type="radio"/> Enabled <input type="radio"/> Disabled
DMZ Host IP Address	<input type="text"/>

At the bottom of the configuration area, there are two buttons: "Save" and "Back".

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:

- ① **Enabled:** It activates your DMZ function.
- ① **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

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.

Configuration

Virtual Server

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):

Save Back

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 Port Number: Enter a port number as the starting number of the range which you want to give access to internal server.

End Port Number: Enter a port number as the end number of the range which you want to give access to internal server..

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

Start Port Number (Local): Please enter the start port number of the local application (service).

End Port Number (Local): Please enter the 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

If you have a FTP server in your LAN network, and want to be accessing through WAN, you can have it set as virtual server.

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		

Some tips for using DMZ and Virtual Server:



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.

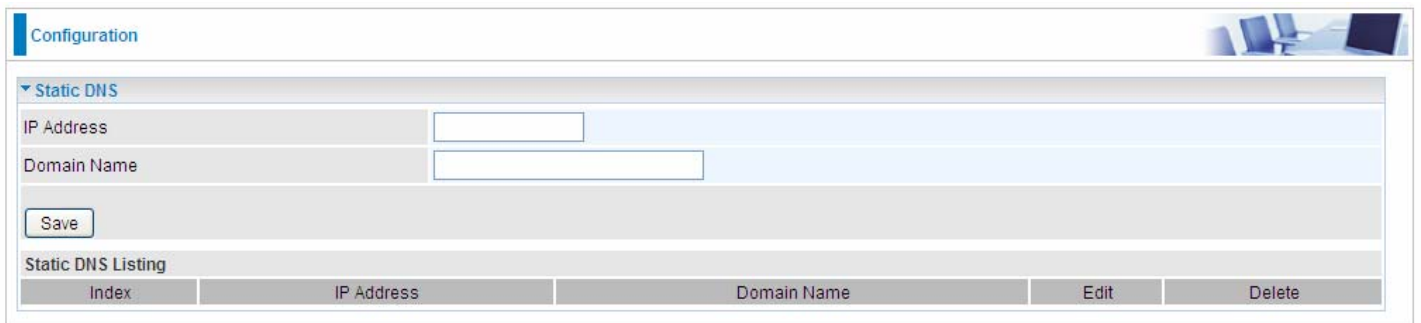
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into 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.

4.4.2.4 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.



The screenshot shows a web configuration page titled "Configuration". Under the "Static DNS" section, there are two input fields: "IP Address" and "Domain Name". Below these fields is a "Save" button. At the bottom, there is a "Static DNS Listing" table with the following columns: Index, IP Address, Domain Name, Edit, and 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.

4.4.2.5 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 give 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.

The screenshot shows a web-based configuration interface for Quality of Service (QoS). At the top, there's a 'Configuration' tab. Below it, the 'Quality of Service' section is expanded. The 'QoS' status is set to 'Activated' (radio button selected). There are 'Save' and 'Rules Summary' buttons. The 'Rule' section contains several fields: 'Rule Index' (dropdown menu showing 0), 'Active' (radio buttons for 'Yes' and 'No', with 'No' selected), 'Destination IPv4/IPv6 Address' (text input), 'Destination Subnet Mask / IPv6 Prefix' (text input), 'Destination Port Range' (two text inputs with a tilde separator), 'Source IPv4/IPv6 Address' (text input), 'Source Subnet Mask / IPv6 Prefix' (text input), 'Source Port Range' (two text inputs with a tilde separator), 'Protocol ID' (dropdown menu), and 'Priority' (dropdown menu). At the bottom of the rule configuration area, there are 'Save' and 'Delete' buttons.

■ 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, IGMP).

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

4.4.2.6 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.



The screenshot shows the 'Configuration' page for 'Interface Grouping'. The 'Interface Grouping' checkbox is selected as 'Deactivated'. The 'Group Index' is set to 0. The 'EWAN Service' is EWAN0. The 'Ethernet LAN' section shows three checkboxes for LAN1, LAN2, and LAN3. The 'Wireless LAN' section shows a checkbox for WLAN1. The 'Group Summary' button is visible. At the bottom, there are 'Save' and 'Delete' buttons.

Interface Grouping: Select Yes to enable Interface Grouping feature.

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

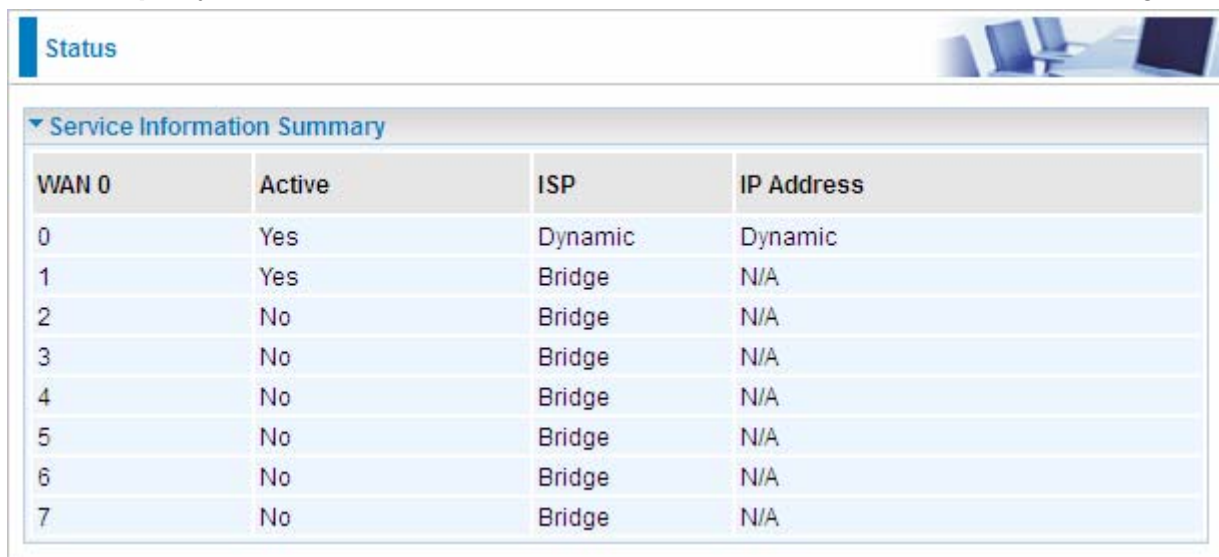
EWAN Service: The available EWAN interface. Move to [4.4.1 Interface Setup](#) to add other EWAN interface.

Ethernet LAN: The available Ethernet ports.

Wireless LAN: The available wireless ports.

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

For example, you can create two EWAN services, Service0(PPPoE) and Service1(Bridge).



The screenshot shows the 'Status' page with a 'Service Information Summary' table. The table has four columns: WAN 0, Active, ISP, and IP Address. The rows show the status of WAN services 0 through 7.

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](#)

[Save](#) [Delete](#)

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](#)

[Save](#) [Delete](#)

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

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

4.4.2.7 Port Isolation

Port isolation is a mechanism to allow or block devices in one port (indicates the LAN1 - LAN3 and WLAN1 - WLAN4, need to enable multiple SSID in wireless section) to access other devices in other ports. 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.

Configuration

▼ Port Isolation

Port Group	Ethernet LAN			Wireless LAN
	LAN1	LAN2	LAN3	WLAN1
Group 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4.4.2.8 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.

Configuration

Time Schedule

Time Index: 0

Name: TimeSlot1

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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

Save

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.

Configuration

Time Schedule

Time Index: 0

Name: TimeSlot1

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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

Save

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

Configuration

Time Schedule

Time Index: 0

Name: TimeSlot2

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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

Save

4.4.3 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.

Five sub-items to be covered to configure the VoIP feature, namely **Basic**, **Media**, **Advanced**, **Speed Dial**, **Call Features**.

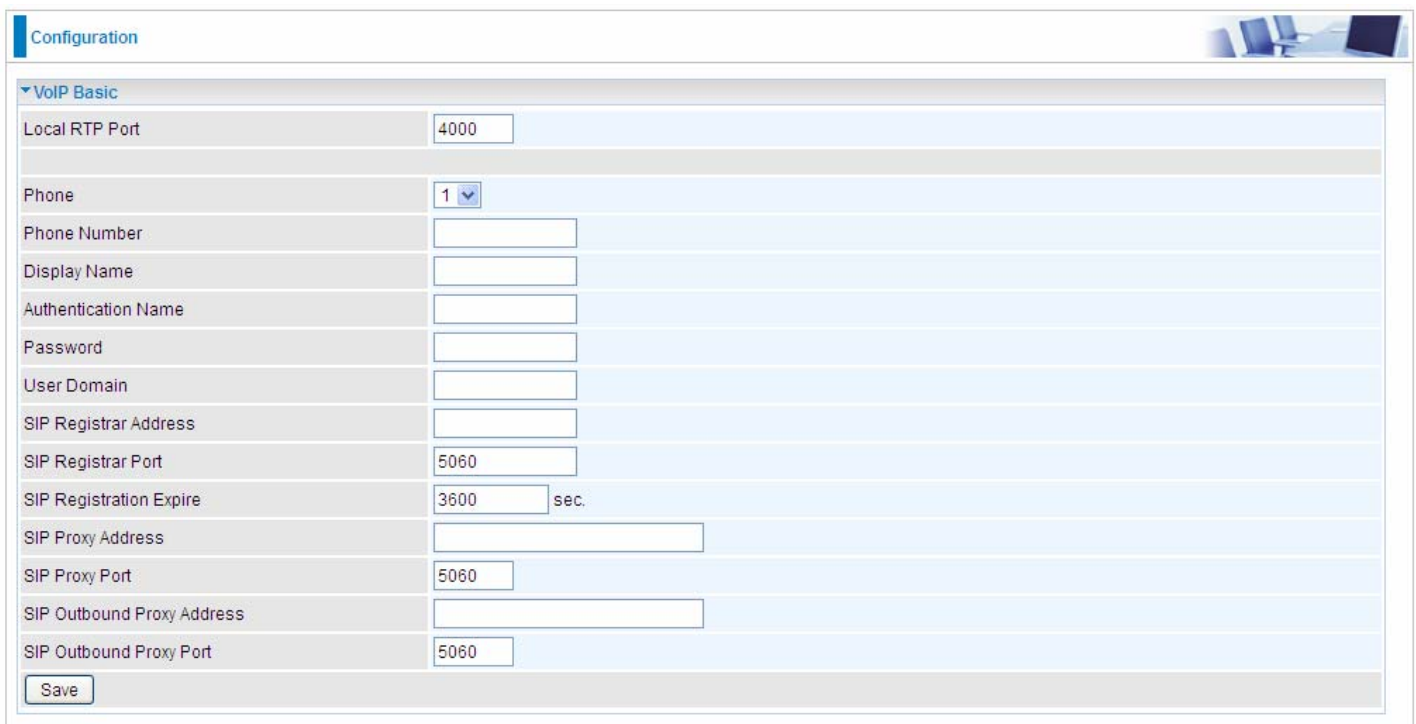
The screenshot displays the configuration interface for a BEC 4G/LTE VoIP Gigabit Wireless Router. The page is titled "Configuration" and features a sidebar menu on the left with options: Status, Quick Start, Configuration (expanded), Interface Setup, Advanced Setup, VOIP (expanded), Basic (selected), Media, Advanced, Speed Dial, Call Features, Access Management, Maintenance, and Language. The main content area is titled "VoIP Basic" and contains the following fields:

Local RTP Port	4000
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

At the bottom of the configuration area is a "Save" button. In the bottom right corner of the page, there are "Restart" and "Logout" buttons. The footer contains the text: "Copyright © BEC Technologies, Ltd. All rights reserved."

4.4.3.1 Basic

Register to a SIP service provider is an essential step before making the VoIP call. Users can find out SIP service provider, and register a SIP account, jotting down the registration information and configuring in router.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'VoIP Basic' section is expanded. The settings are as follows:

Local RTP Port	4000
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

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

Local RTP Port: Set the local RTP port used to receive voice packet. The setting is to be applied to the two FXS, name phone 1 and phone 2, and the two FXS share the same local RTP port.

Phone: Select "1", the following parameters will be applicable to Phone1. In 6300VNOZ, phone 1 and phone 2 are allowed to be of different characteristics, including different SIP registrar. So, user needs to configure individually for phone1 and phone 2.

Phone Number: Set you 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.

4.4.3.2 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		
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
<input type="button" value="Save"/>			

Phone: Select to set the following configurations for Phone 1 or Phone2. When phone1 is selected, the following set media codec will be applied to phone1.

- ① **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.
- ① **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.
- ① **G.729:** It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- ① **G.726:** It is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 32kbit/s.

4.4.3.3 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	CHN-China
Phone	1
Silence Suppression(VAD)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Echo Cancellation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DTMF Transport Mode	Inband
Listening Volume	0 db (-6-6)
Speaking Volume	0 db (-6-6)
<input type="button" value="Save"/>	

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.

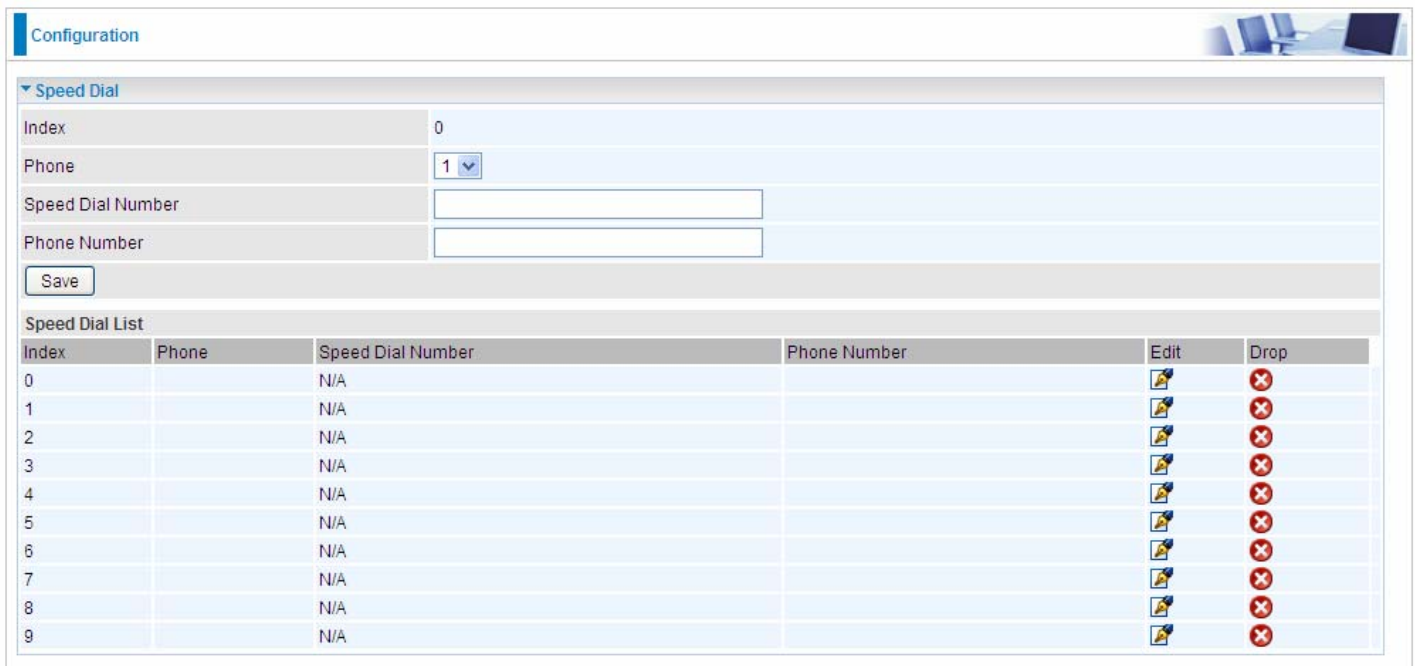
DTMF Transport Mode: Select the DTMF mode.

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.

4.4.3.4 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

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			

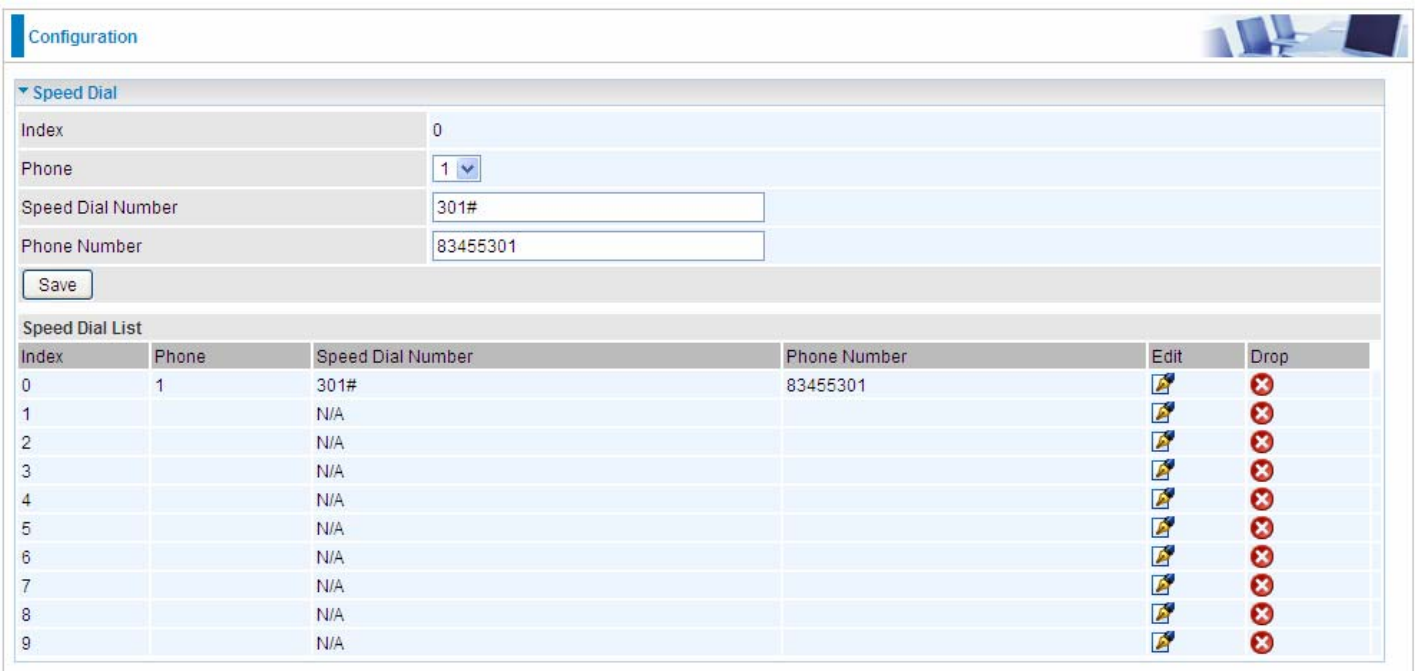
Index: The index to mark the speed dial number mapping, 0-9.

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

Phone Number: The complete destination number

For example, a destination: 83455301. You want to replace it with a friendly speed dial numbr stored in your speed dial list , then set as follows.



Configuration

Speed Dial

Index: 0

Phone: 1

Speed Dial Number: 301#

Phone Number: 83455301

Save

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.

4.4.3.5 Call Features

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



The screenshot shows a configuration interface for 'Call Features'. At the top, there is a 'Configuration' header and a small image of a laptop. Below the header, there is a section titled 'Call Features' with a dropdown arrow. Under this section, there is a table of settings for 'Phone 1'. The settings are as follows:

Feature	Enable	Disable
Call Waiting	<input type="radio"/>	<input checked="" type="radio"/>
Conference Call	<input type="radio"/>	<input checked="" type="radio"/>
Return Call(Dial number: *69)	<input type="radio"/>	<input checked="" type="radio"/>
Redial(Dial number: *68)	<input type="radio"/>	<input checked="" type="radio"/>
Don't Disturb(Enable: *78, Disable: *79)	<input type="radio"/>	<input checked="" type="radio"/>

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

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 slightly pressing Hook 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)

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.

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.

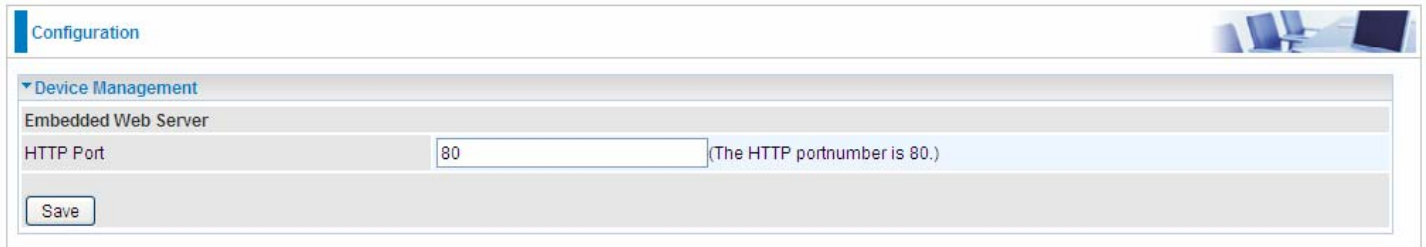
Step – 6: Bill **presses flash again** to merge all 3 calls.

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

4.4.4 Access Management

4.4.4.1 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.



The screenshot shows a web configuration interface. At the top left, there is a 'Configuration' tab. Below it, a 'Device Management' section is expanded. Under 'Device Management', there is a sub-section for 'Embedded Web Server'. Within this sub-section, there is a label 'HTTP Port' followed by a text input field containing the value '80'. To the right of the input field, there is a note: '(The HTTP portnumber is 80.)'. Below the input field and note, there is a 'Save' button.

4.4.4.2 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 6300VNOZ serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.

Configuration

SNMP

SNMP Activated Deactivated

Get Community

Set Community

Trap Manager IP

SNMPv3

SNMPv3 Enable Disable

Username

Access Permissions

Authentication Protocol

Authentication Key (8~31 characters)

Privacy Protocol

Privacy Key (8~31 characters)

Save

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.

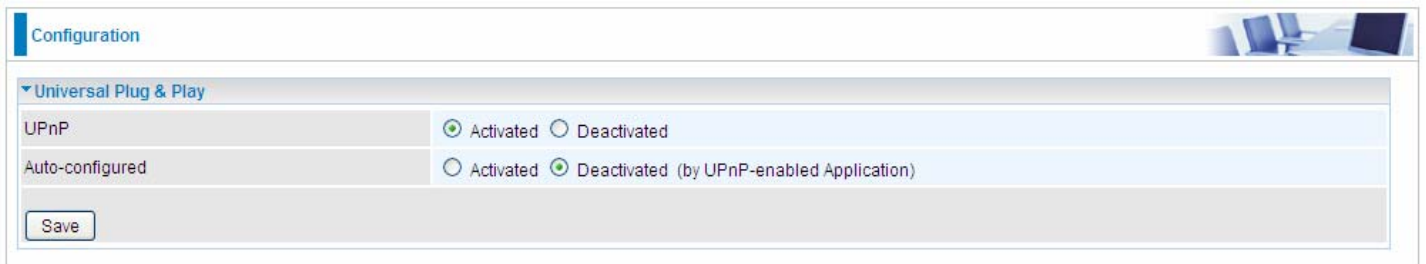
Privacy Protocol: Select the privacy mode, DES and AES.

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

4.4.4.3 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.



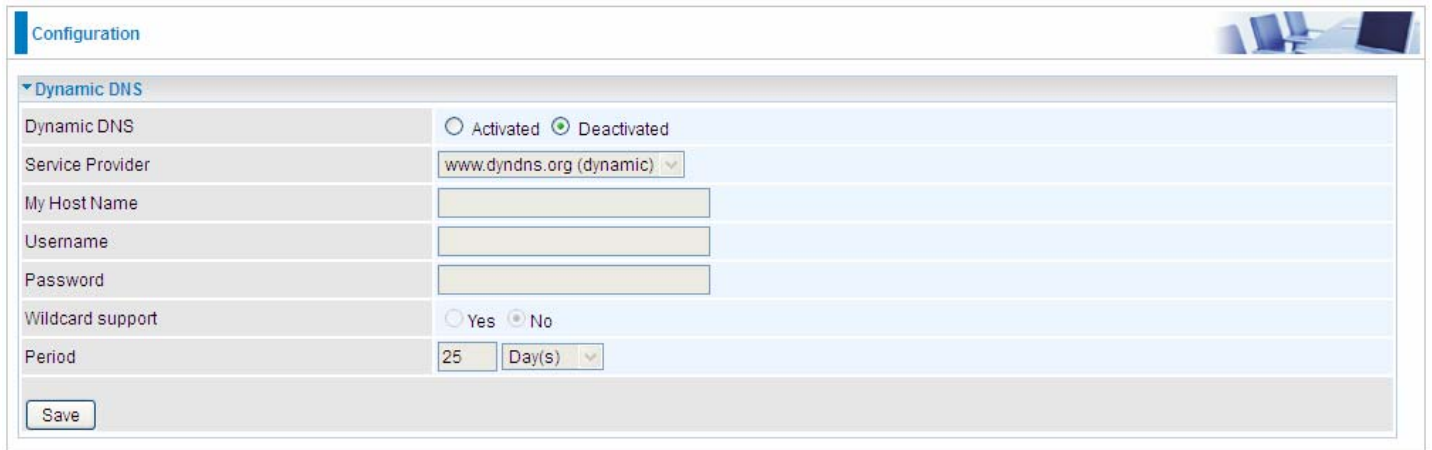
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the BIPAC 6300VNOZ' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BIPAC 6300VNOZ so that they can communicate through the BIPAC 6300VNOZ, 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.

4.4.4.4 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.



The screenshot shows a web interface for configuring Dynamic DNS. The page is titled "Configuration" and has a sub-section for "Dynamic DNS". The configuration options are as follows:

Dynamic DNS	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼

At the bottom of the configuration area, there is a "Save" button.

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 6300VNOZ 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.

User can register a DDNS

Examples: **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



The image shows a web-based configuration interface for Dynamic DNS. The page title is "Configuration". Under the "Dynamic DNS" section, there are several fields and options:

Dynamic DNS	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	www.hometest.com
Username	test1
Password	••••
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼

At the bottom left of the configuration area, there is a "Save" button.

4.4.4.5 Access Control

Access Control Listing allows you to determine which services/protocols can access BIPAC 6300VNOZ 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.

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.

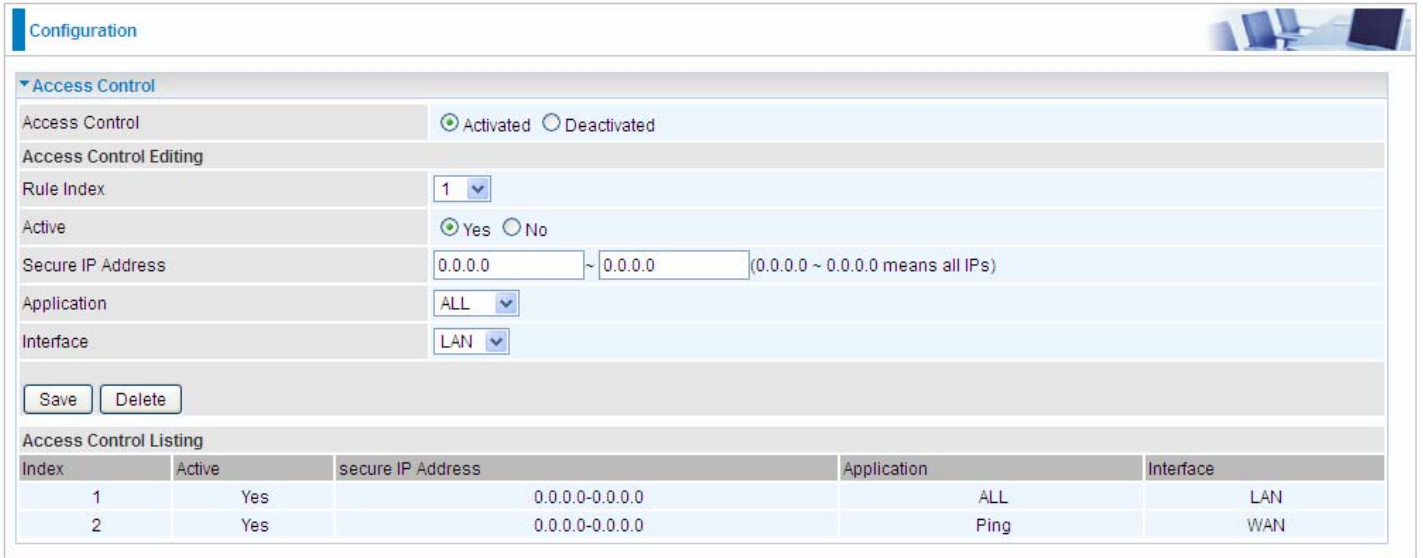
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the BIPAC 6300VNOZ. Type an IP address range to restrict access to the client(s) without a matching IP address.

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.

1. 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 can not 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

Save Delete

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

2, Rule 2(Index 2), a 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

Save Delete

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

4.4.4.6 Packet Filter

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

➤ 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 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, 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.

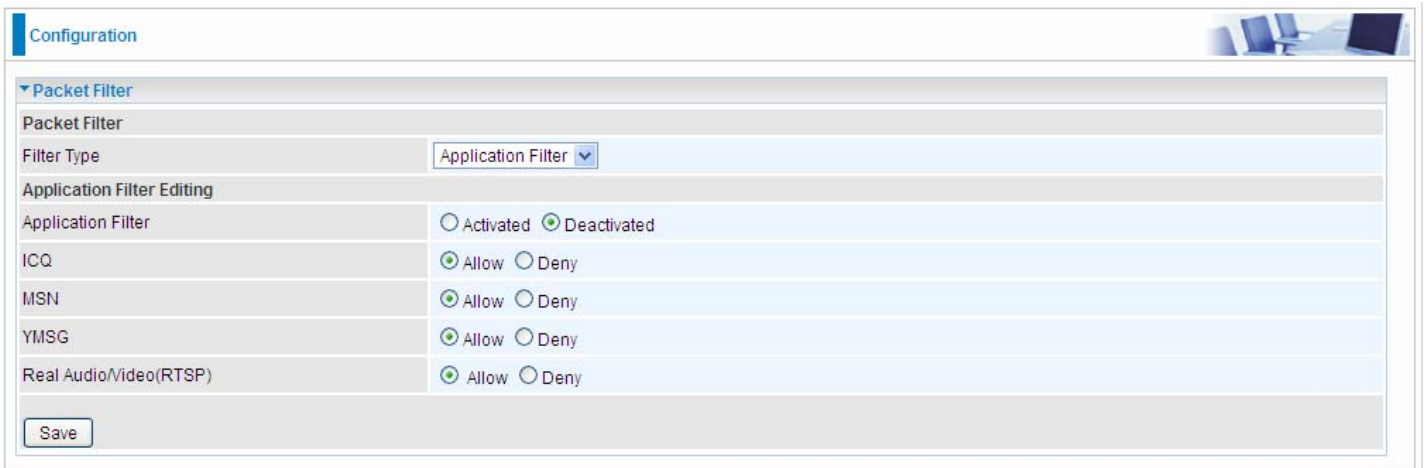
Source Port: The source port number of packets to be monitored.

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**

➤ Application Filter



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Packet Filter". The "Filter Type" is set to "Application Filter". Under "Application Filter Editing", there are several options:

Application Filter	Options
Application Filter	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
ICQ	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
MSN	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
YMSG	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Real Audio/Video(RTSP)	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

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

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).

➤ URL Filter

Configuration

Packet Filter

Packet Filter

Filter Type

URL Filter Editing

URL Filter Activated Deactivated

URL Filter Rule Index

Individual Active Yes No

URL (Host)

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.

4.4.4.7 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

Save

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.

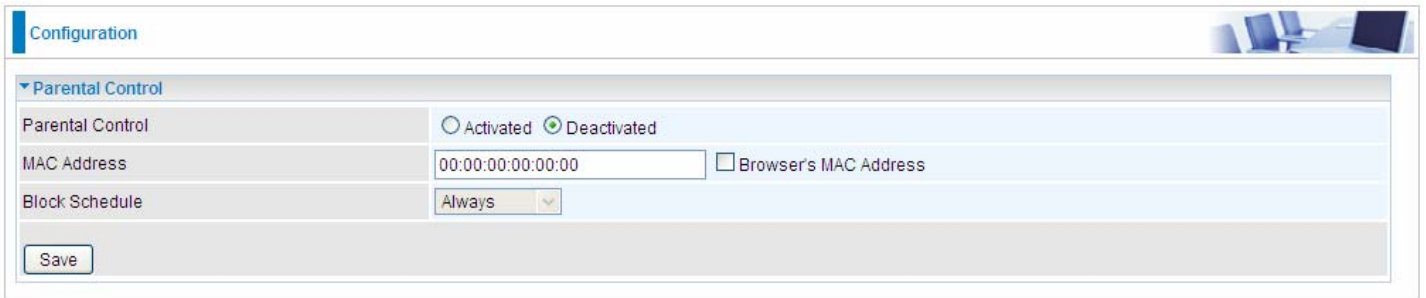
Periodic Inform Config

Periodic Inform: Select activated to enable to let CPE be authorized to send Inform message to automatically connect to ACS.

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.

4.4.4.8 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 Browser's MAC Address

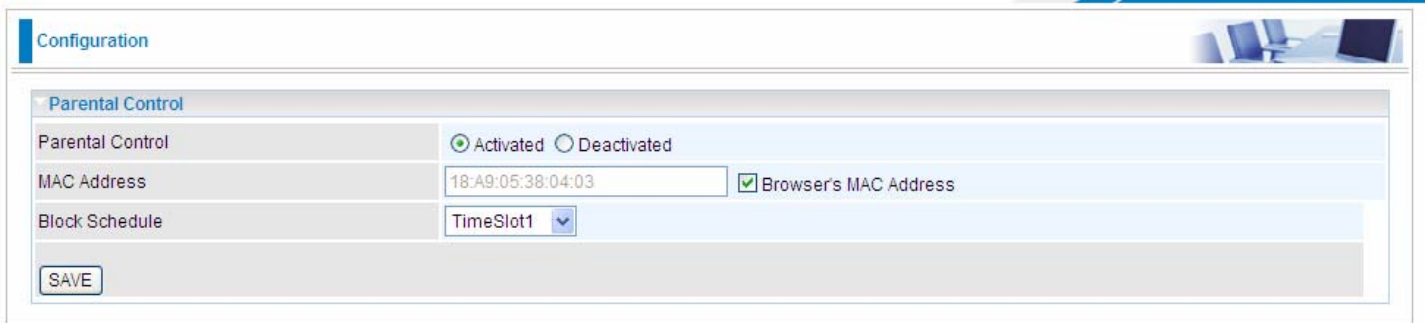
Block Schedule

Save

Parent Control: Select Activated to enable this feature.

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 [4.4.2.8 Time Schedule](#) to set the exact timeslot.



Configuration

Parental Control

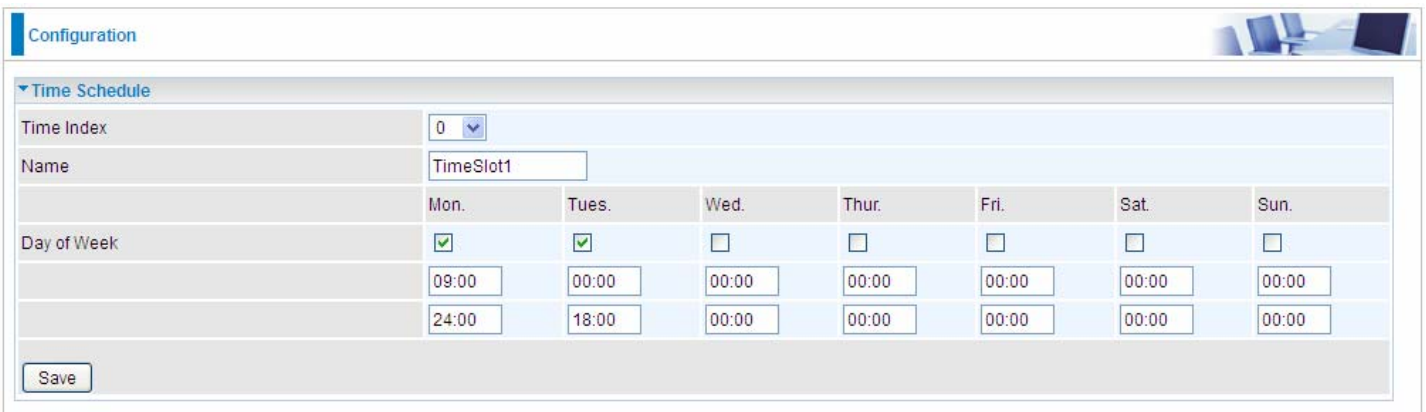
Parental Control Activated Deactivated

MAC Address Browser's MAC Address

Block Schedule

SAVE

Timeslot1 at Time Schedule:



Configuration

Time Schedule

Time Index

Name

Day of Week	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="text" value="09:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
	<input type="text" value="24:00"/>	<input type="text" value="18:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>

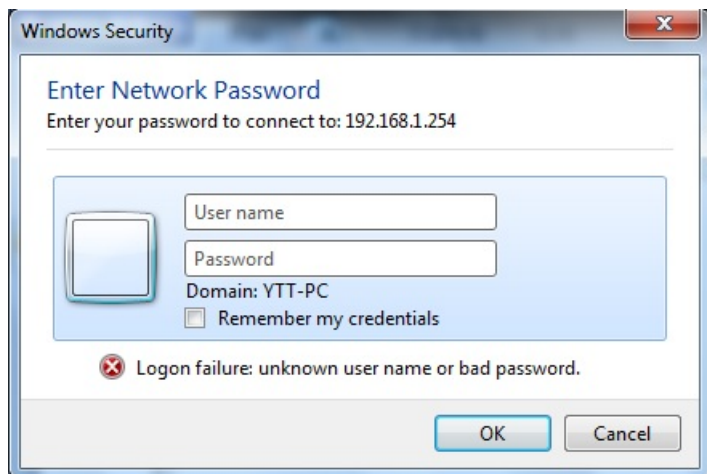
Save

Samba Usage:

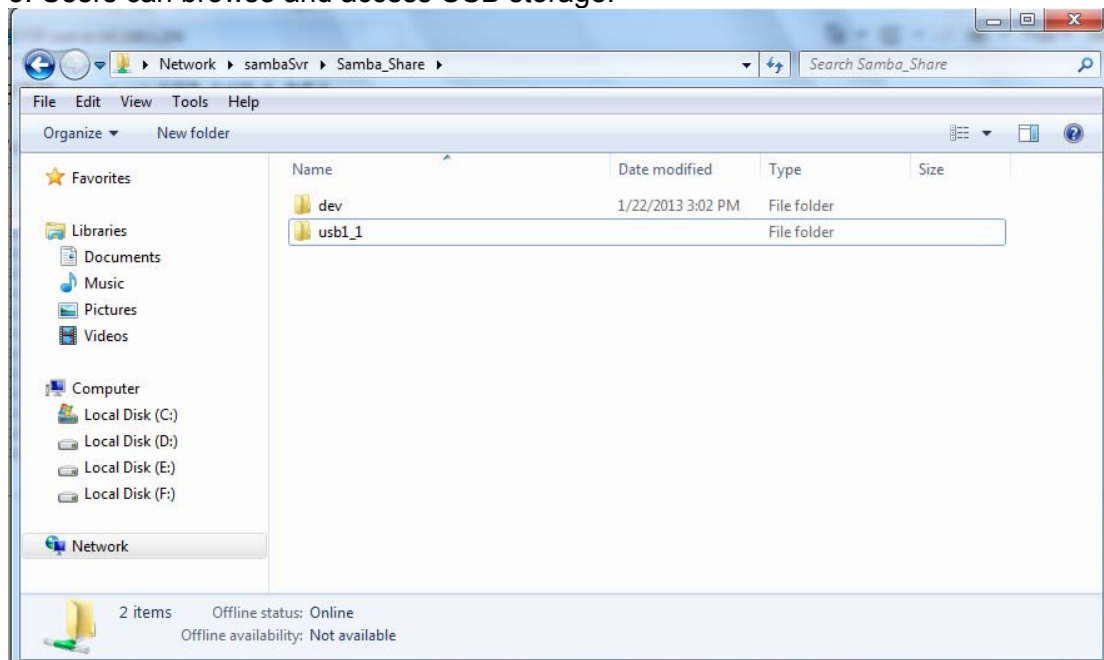
1. Go directly to Start > Run (enter [\\192.168.1.254](#) (from LAN side), [\\SambaSvr](#) , but if you enter [\\SambaSvr](#), please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



3. Users can browse and access USB storage.



FTP usage:

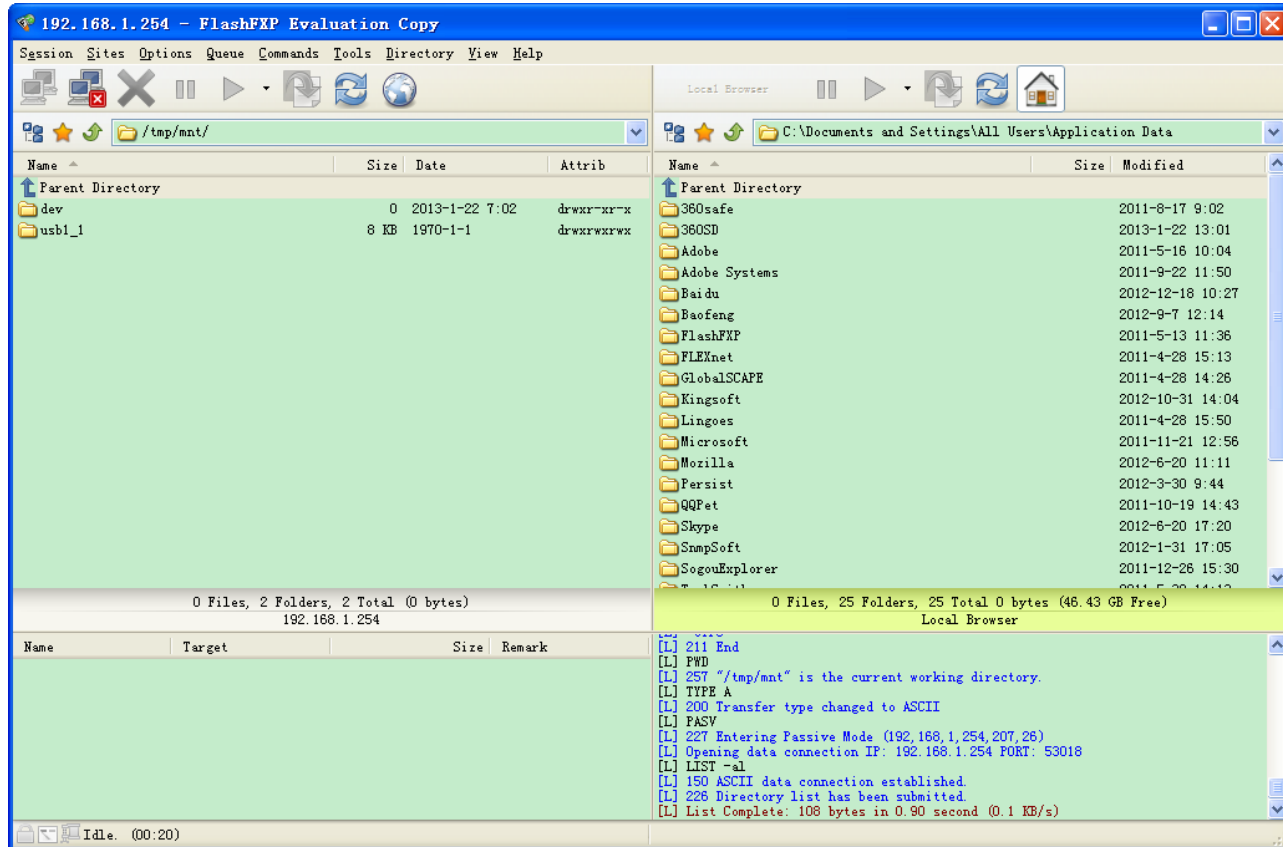
1. Access via FTP tools

Take popular FTP tool of FlashFXP for example:

1) Open FlashFXP

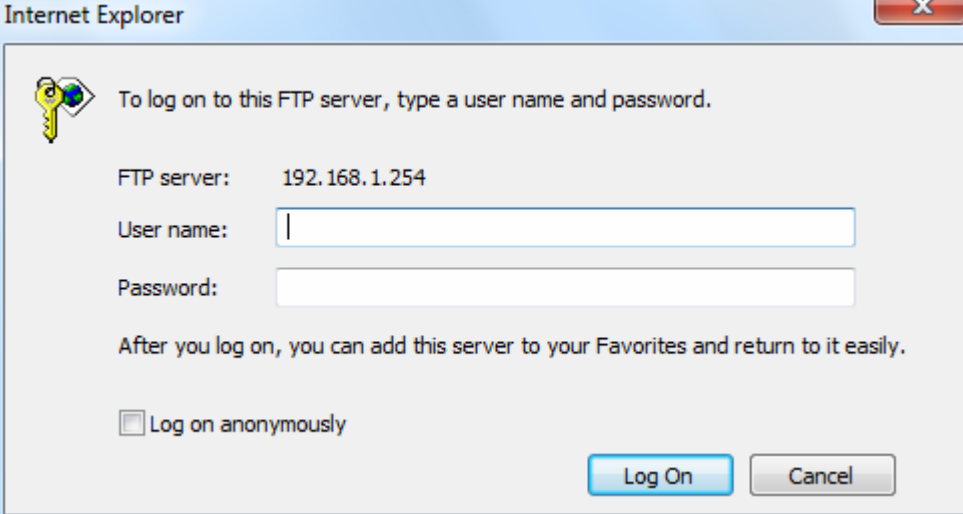
2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).

3) Connect to the ftp site.



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

Log On Cancel

4.4.5 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, Diagnostic Tool**. Usage of each feature is to be presented in the following scenarios.

4.4.5.1 User Management

In factory setting, the default accounts are **admin/admin** and **user/user**. The default account admin has been authorized to web access of router, Samba access, and FTP access. The user **user/user** has only access to the FTP and Samba server, but disabled by default. A total of **6** other accounts can be created to grant access to the access of Samba and FTP but not router's web.

Note: Please go to [4.4.4.9 SAMBA & FTP Server](#) to re-activate FTP and SAMBA server to enable the changes to the FTP and SAMBA account set here.

The screenshot shows the 'User Management' configuration page. It includes fields for 'User Account' (Index: 1, Username: admin, New Password, Confirm Password), 'FTP Authority Setup' (FTP Access: Enable, Permission: Read/Write), and 'SAMBA Authority Setup' (SAMBA Access: Enable, Permission: Read/Write). A message states: '**Please restart the Storage server after config changed**'. There are 'Save' and 'Delete' buttons. Below is a 'User Account List' table:

#	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. Default user admin's password can be changed here and confirmed in the next field.

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.

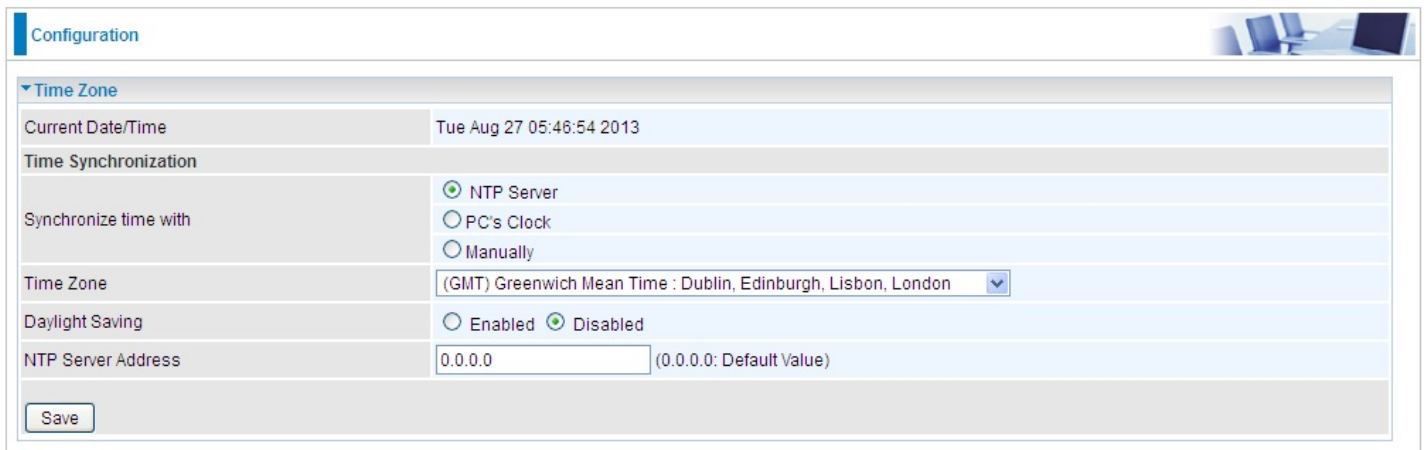
SAMBA Authority

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

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

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



The screenshot shows a web-based configuration interface for a router. The page title is "Configuration" and the section is "Time Zone". The current date and time are displayed as "Tue Aug 27 05:46:54 2013". Under "Time Synchronization", the "NTP Server" option is selected with a radio button. Other options are "PC's Clock" and "Manually". The "Time Zone" is set to "(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London" via a dropdown menu. "Daylight Saving" is set to "Disabled" with a radio button. The "NTP Server Address" is set to "0.0.0.0" with a note "(0.0.0.0: Default Value)". A "Save" button is located at the bottom left of the configuration area.

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

- ① **NTP Server automatically:** To synchronize time with the NTP server.
- ① **PC's Clock:** To synchronize time with the PC's clock.
- ① **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).

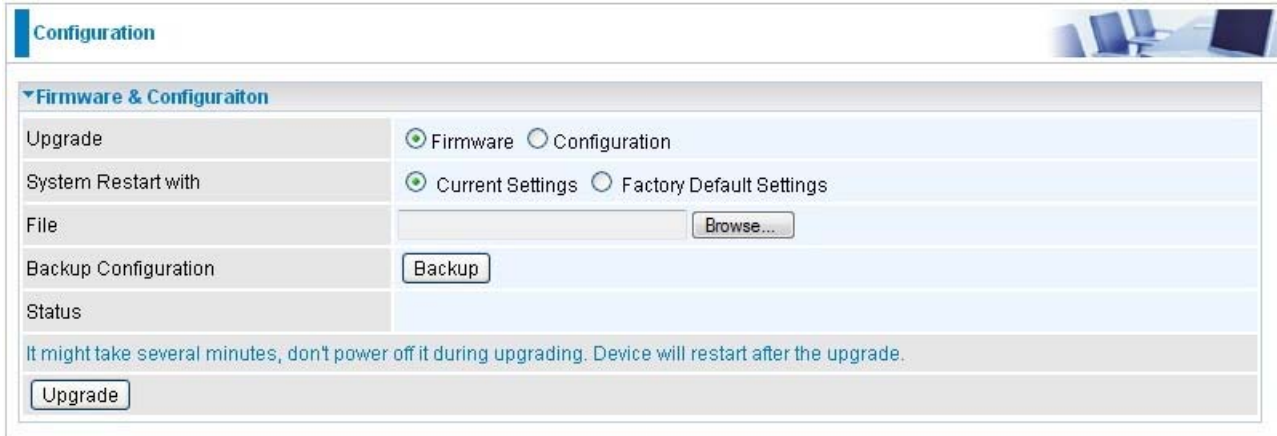
Daylight Saving: Select this option if you use daylight savings time.

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

4.4.5.3 Firmware & Configuraion

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and modified, and your router allows you to upgrade the software it runs to take advantage of these changes.

To upgrade the firmware of BIPAC 6300VNOZ, 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 6300VNOZ will reset automatically to make the new firmware work.



The screenshot shows the 'Configuration' page of a router, specifically the 'Firmware & Configuraion' section. The page has a blue header with the word 'Configuration' and a small image of a router. Below the header, there is a section titled 'Firmware & Configuraion' with a dropdown arrow. Under this section, there are several rows of settings:

- Upgrade:** Two radio buttons, 'Firmware' (selected) and 'Configuration'.
- System Restart with:** Two radio buttons, 'Current Settings' (selected) and 'Factory Default Settings'.
- File:** A text input field and a 'Browse...' button.
- Backup Configuration:** A 'Backup' button.
- Status:** A text input field.

Below these settings, there is a blue informational message: 'It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.' At the bottom of the section, there is an 'Upgrade' button.

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

- ① **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- ① **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 decompress compressed (.zip) files before you can upload them.

Backup Configuration: Click **Backup** button to back up the now running configuration file to your computer in the event that you need this configuration file to restore the device especially when you make some wrong configurations and you need to restore the original settings.



The screenshot shows a file dialog box with a yellow border. The text inside reads: 'Do you want to open or save romfile.cfg (35.8 KB) from 192.168.1.254?'. At the bottom right, there are three buttons: 'Open', 'Save' (with a dropdown arrow), and 'Cancel' (with a close 'x' icon).

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 %

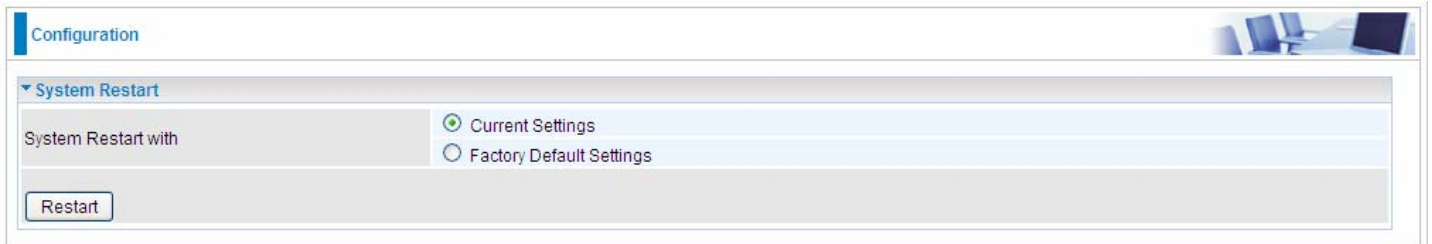


Warning

DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

4.4.5.4 System Restart

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



The screenshot shows a web interface for router configuration. At the top, there is a 'Configuration' header. Below it, a 'System Restart' section is expanded, showing two radio button options: 'Current Settings' (which is selected) and 'Factory Default Settings'. A 'Restart' button is located at the bottom of this section.

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

4.4.5.5 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:



The screenshot shows the 'Configuration' page of the Diagnostic Tool. The 'WAN Interface' is set to 'EWAN'. The test results are as follows:

Test	Result
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 <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

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

Click START to begin to diagnose the connection.



The screenshot shows the 'Configuration' page of the Diagnostic Tool after the tests have been executed. The 'WAN Interface' remains 'EWAN'. The test results are as follows:

Test	Result
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 <input type="radio"/> Yes <input checked="" type="radio"/> No	Skipped

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

Chapter 5

Troubleshooting

If the router is not functioning properly, you can refer first to this chapter for simple troubleshooting before contacting your service provider. This could save your time and effort but if the symptoms persist, then consult your service provider.

Problems starting up the router

Problem	Corrective Action
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login username and/or password.	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router more than 6 seconds

Problems with the WAN Interface

Problem	Corrective Action
Obtaining WAN IP failure	Check that your internet settings are the same as those provided by your ISP. Reboot the router if you still have problems, you may need to verify these settings with your ISP.

Problems with the LAN Interface

Problem	Corrective Action
Can't ping any PCs on the LAN.	<ol style="list-style-type: none">1. Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC.2. Verify that the IP address and the subnet mask are consistent between the router and the PC.

Recovery procedures for non-working routers

Problem	Corrective Action
Recovery procedures for non-working routers(e.g. after a failed firmware upgrade flash)	<ol style="list-style-type: none">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 and Contact Information

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 Inc.

Windows 7, Windows Vista, Windows XP, Windows 2000, Windows 98/Me and Windows NT 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.