

Wireless-N ADSL2+ Firewall Router

User Manual

Table of Contents

<i>Chapter 1</i>	1
1.1 Introducing the Router.....	1
Express Internet Access	1
Firewall Security and Smooth Traffic.....	1
Easy Network Management	1
IPv6 Ready - Pathway to the Future	1
Quick Start Wizard	2
Firmware Upgradeable	2
1.2 Features of the Router	3
Network Protocols and Features	3
Firewall	4
Quality of Service Control.....	4
Wireless LAN.....	4
IPTV Applications	4
Management	4
1.3 Hardware Specifications.....	5
Physical Interface.....	5
1.4 Applications for the Router	6
<i>Chapter 2</i>	7
<i>Installing the Router</i>	7
2.1 Important note for using the Router	7
2.2 Package Contents	8
2.3 The Front LEDs.....	9
2.4 The Rear Ports	10
2.5 Cabling.....	11
<i>Chapter 3</i>	12
3.1 Before Configuration	12
3.1.1 Configuring a PC in Windows 7/8	13
3.1.2 Configuring a PC in Windows Vista.....	16
3.1.3 Configuring a PC in Windows XP	18
3.2 Factory Default Settings	20
3.2.1 Username and Password	20
3.3 LAN Port Addresses	21
3.4 Information from your ISP	21
<i>Chapter 4</i>	22
4.1 Configuring the Router with your Web Browser	22

4.2 Status.....	24
4.2.1 Device Info	25
4.2.2 System Log.....	27
4.2.4 Statistics.....	28
4.2.5 DHCP Table	31
4.2.5 ADSL Status.....	32
4.3 Quick Start.....	33
4.4 Configuration.....	36
4.4.1 Interface Setup	37
4.4.1.1 Internet	38
4.4.1.2 LAN	42
4.4.1.3 Wireless.....	46
4.4.1.4 Wireless MAC Filter	57
4.4.2 Advanced Setup.....	58
4.4.2.1 Firewall.....	59
4.4.2.2 Routing.....	60
4.4.2.3 NAT.....	62
4.4.2.4 Static DNS.....	67
4.4.2.5 ADSL	68
4.4.2.6 QoS.....	69
4.4.2.7 Interface Grouping.....	72
4.4.2.8 Time Schedule.....	74
4.4.2.9 Remote System Log	75
4.4.3 Access Management.....	76
4.4.3.1 Device Management.....	77
4.4.3.2 SNMP.....	78
4.4.3.3 Universal Plug & Play	79
4.4.3.4 Dynamic DNS.....	80
4.4.3.5 Access Control.....	82
4.4.3.6 Packet Filter	84
4.4.3.7 CWMP (TR-069).....	88
4.4.3.8 Parental Control.....	90
4.4.4 Maintenance.....	91
4.4.4.1 User Management	92
4.4.4.2 Time Zone	96
4.4.4.3 Firmware & Configuraion.....	97
4.4.4.4 System Restart	99
4.4.4.5 Diagnostics Tool	100
Chapter 5.....	101
Problems starting up the router	101
Problems with the WAN Interface.....	101
Problems with the LAN Interface.....	101
APPENDIX.....	102

Chapter 1

Introduction the Router

1.1 Introducing the Router

This Router is an economical ADSL2+ router ideal for Home and SOHO users to enjoy improved Wireless Access Speed with a maximum operational speed of 150Mbps. It delivers the highest level of security with higher speed and better coverage of wireless-n solutions. With an integrated 802.11n wireless access point, the router enables faster wireless speeds of up to 150Mbps. The SOHO Firewall is integrated to provide protection against hacker attacks while the Quality of Service prioritizes queues and traffic for applications such as music downloads, online gaming, video streaming and file sharing.

Express Internet Access

Complying with worldwide ADSL standards, the Router supports downstream data transmission rates of up to 12/24 Mbps with ADSL2/2+, 8 Mbps with ADSL, and performs at upstream rates of up to 1 Mbps. Moreover, the Router includes Annex M technology that supports the latest ADSL2/2+ standard for higher upload speeds by increasing the upstream operation rate to approximately 2.5Mbps (up to 3Mbps under ideal conditions). With this technology, you can enjoy even higher-speed broadband multimedia applications such as interactive gaming, video streaming and real-time audios that run faster and easier than ever.

Firewall Security and Smooth Traffic

With the built-in NAT default firewall, the advanced anti-hacker pattern-filtering protection features automatically detect and block Denial of Service (DoS) attacks. In addition, packet filtering provides high-level security for access control. Quality of Service control prioritizes the traffic and allows users to enjoy smooth traffic while running applications such as IPTV, VoIP calls or interactive game through the Internet.

Easy Network Management

The Web-based user interface of the Router makes it extremely easy for users to install and manage the network. The router supports both DHCP client and server, enabling system administrators to easily integrate this router into existing network environments, as well as manage IP assignment without having to reconfigure other stations.

IPv6 Ready - Pathway to the Future

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

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 Router

- IPv6 ready (IPv4/IPv6 dual stack)
- 4-port 10/100Mbps Fast Ethernet switch
- 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)
- Wireless speed up to 150Mbps and 3 times the coverage of standard 802.11g
- SOHO Firewall Security with DoS Preventing and Packet Filtering
- Quality of Service Control for traffic prioritization management
- Universal Plug and Play (UPnP) Compliance
- Ease of Use with Quick Installation Wizard
- TR-069*² for remote management
- Ideal for SOHO, office and home users

ADSL Compliance

- Compliant with ADSL2+ standards
 - G.dmt.bis plus (ITU G.992.5)
 - ADSL2+ Annex M (ITU G.992.5 Annex M)
- Compliant with ADSL2 standards
 - G.dmt.bis (ITU G.992.3)
 - ADSL2 Annex M (ITU G.992.3 Annex M)
- Compliant with ADSL standards
 - Full-rate ANSI T1.413 Issue 2
 - G.dmt (ITU G.992.1)
 - G.lite (ITU G.992.2)
 - G.hs (ITU G.994.1)
- Support G.inp (ITU G.998.4)

Network Protocols and Features

- PPPoE (RFC 2516), PPPoA (RFC 2364), DHCP Client, Static IP
- IPv4, IPv6, IPv4 / IPv6 dual stack
- Dual-Stack Lite and 6RD (IPv6 Rapid Deployment)
- NAT, static routing and RIP v1/v2
- Universal Plug and Play (UPnP) compliant
- Virtual server and DMZ
- SNTP, DNS proxy
- Dynamic Domain Name System (DDNS)
- IGMP proxy and IGMP snooping
- MLD proxy and MLD snooping

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 standards
- 2.4 GHz - 2.484GHz radio band for wireless
- Up to 150 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
- Multiple wireless SSIDs
- WDS repeater function support

IPTV Applications^{*3}

- 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)
- Web GUI permission
- Firmware upgrades and configuration data upload and download via web-based GUI
- Supports DHCP Server/ Client/ Relay(WAN port)
- TR-069^{*2} supports remote management
- Diagnostic tool



1. This router may require firmware modification for certain ADSL2/2+/Annex M DSLAMs
2. On request for Telco / ISP projects
3. IPTV application may require subscription to IPTV services from a Telco / ISP.
4. Specifications on this datasheet are subject to change without prior notice.

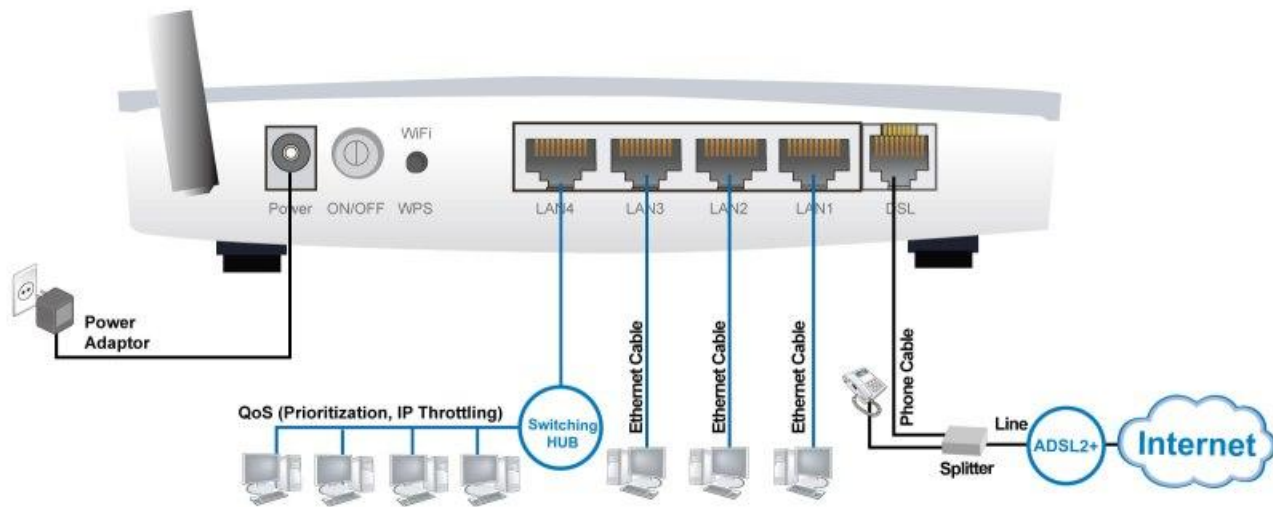
1.3 Hardware Specifications

Physical Interface

- WLAN: 1 detachable antenna
- DSL: ADSL port
- Ethernet: 4-port 10/ 100 auto-crossover (MDI/ MDI-X) Switch.
- Factory default reset button
- WPS& Wi-Fi ON/OFF button
- Power jack
- Power switch

1.4 Applications for the Router

Diagram on how to connect your router:



Chapter 2

Installing the Router

2.1 Important note for using the Router



Warning

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

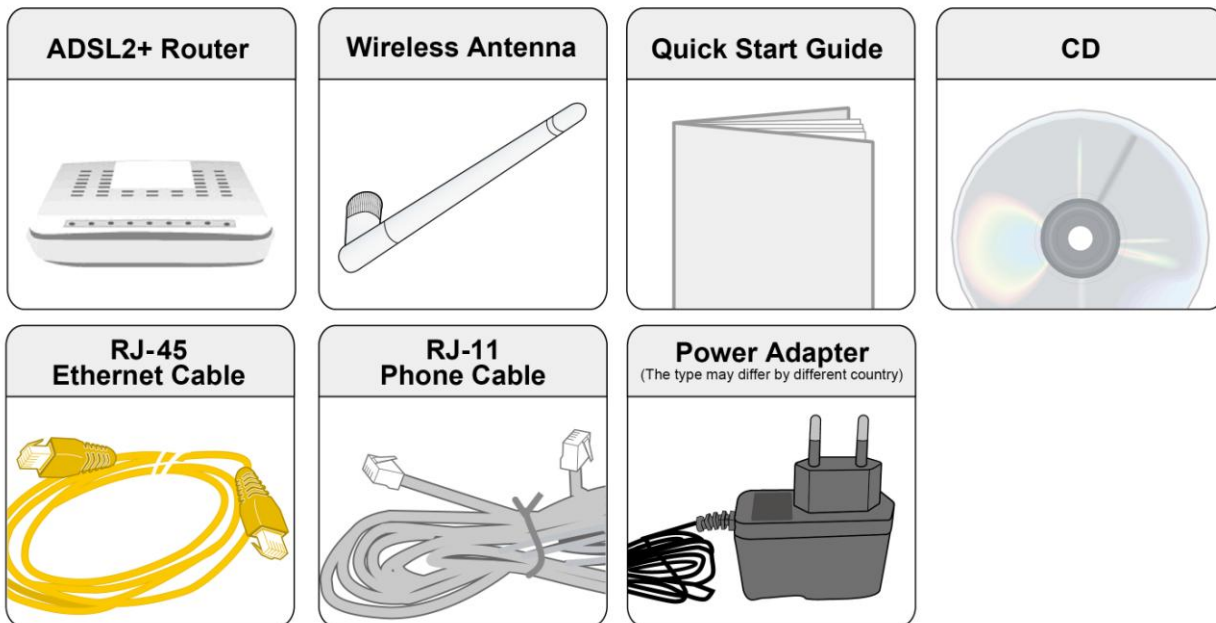


Attention

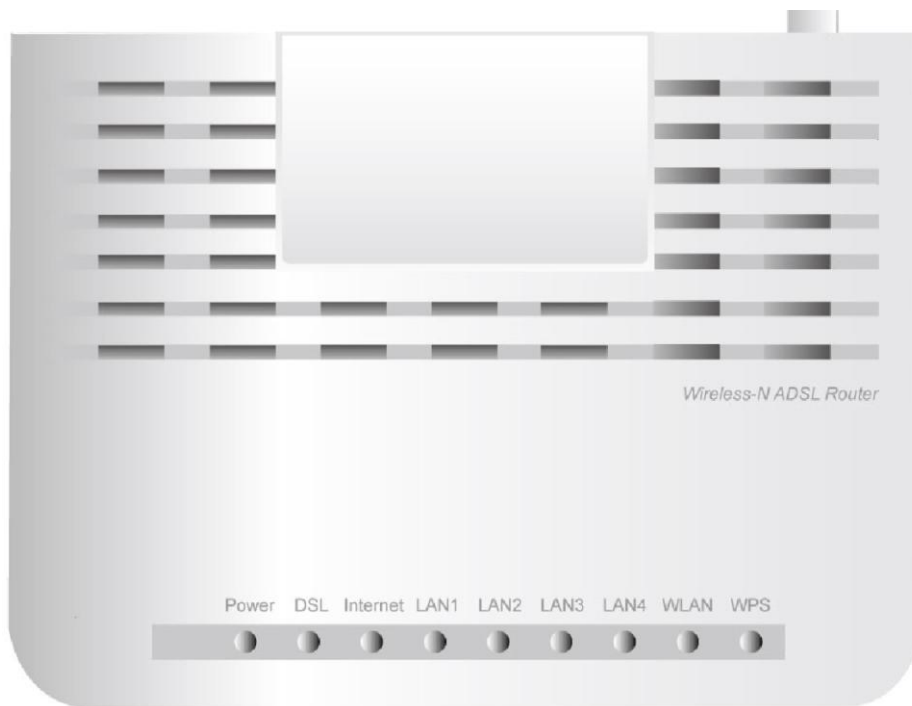
- ✓ Place the Router on a stable surface.
- ✓ Only use the power adapter that comes with the package. Using a different voltage rating power adaptor may damage the router.

2.2 Package Contents

- Wireless-N ADSL2+ Firewall Router
- One detachable antenna
- Quick Start Guide
- CD containing user manual
- Ethernet (RJ-45 CAT-5) cable
- RJ-11 ADSL/telephone cable
- Power adapter

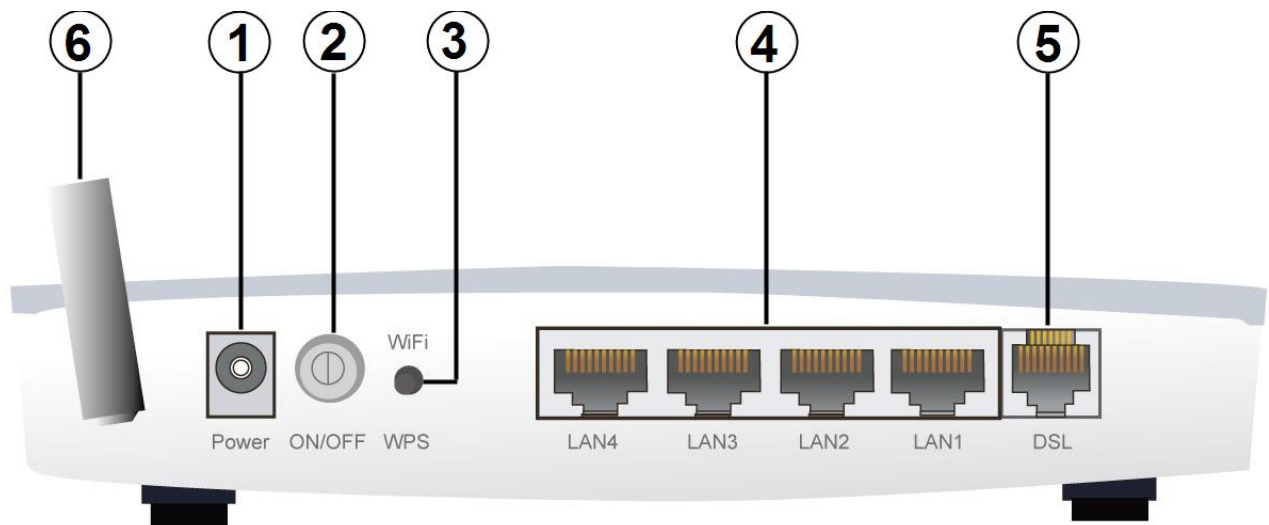


2.3 The Front LEDs

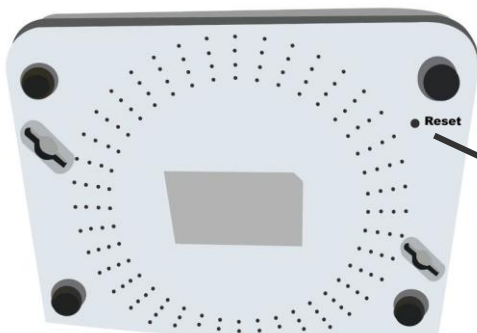


LED	Status	Description
Power	Green	System is up and ready
	Red	Boot failure
DSL	Green	Successfully connected to an ADSL line
	Green blinking	Waiting for ADSL synchronization
Internet	Green	IP connected and traffic is passing through the device
	Red	IP request failed
	Off	Either in bridged mode or WAN connection not present
LAN1~4	Green	Transmission speed is at 10/100Mbps
	Green blinking	Data being transmitted/received
WLAN	Green	Wireless connection established
	Green blinking	Data being transmitted / received
	Off	The wireless function is disabled
WPS	Green blinking	WPS configuration being in progress
	Lit up brightly and then goes off in 5 seconds	WPS established
	Flash for 2 mins and then goes off	WPS establishment failure

2.4 The Rear Ports



Port		Description
1	Power Jack (DC)	Connect the supplied Power Adapter to this jack.
2	Power Switch	Power on/off switch button
3	WPS & WiFi On/Off	By controlling the pressing time, users can achieve two different effects: (1) WPS: Press &hold the button for less than 6 seconds to trigger WPS function. (2) Wireless On/Off: Press & hold the button for more than 6 seconds to On/Off the wireless.
4	Fast Ethernet LAN 1 ~ 4	Connect the LAN port of the router to your computer.
5	DSL	Connect this port to the DSL network with the RJ-11 cable (telephone) provided.
6	WiFi Antenna	Connect the detachable antenna to this port



After the device is powered on, press it 6 seconds or above: to restore to factory default settings (this is used when you cannot login to the router, e.g. forgot your password)

2.5 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 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 XP/Vista/Win7/8, 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.

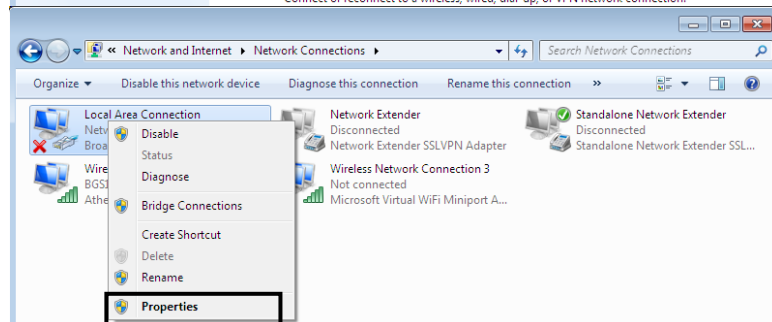
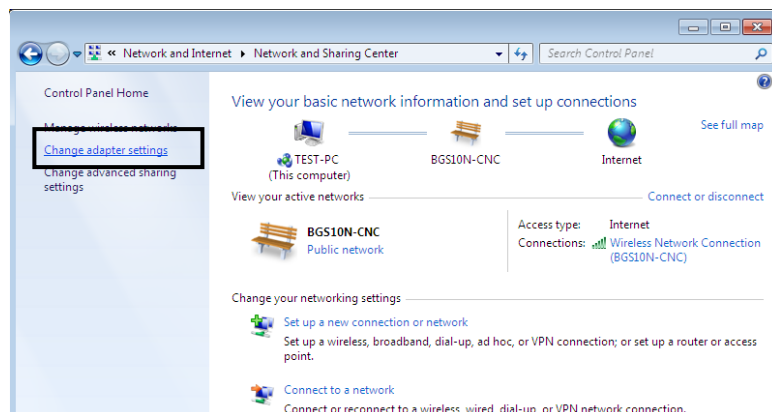
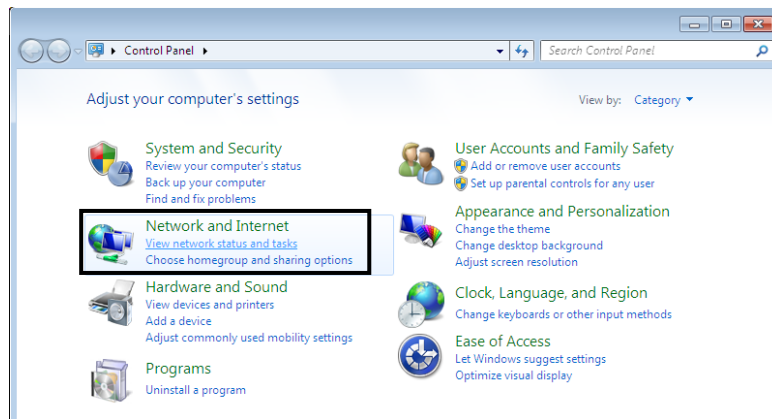
Please follow the steps below for your PC's network environment installation. First of all, please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.



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

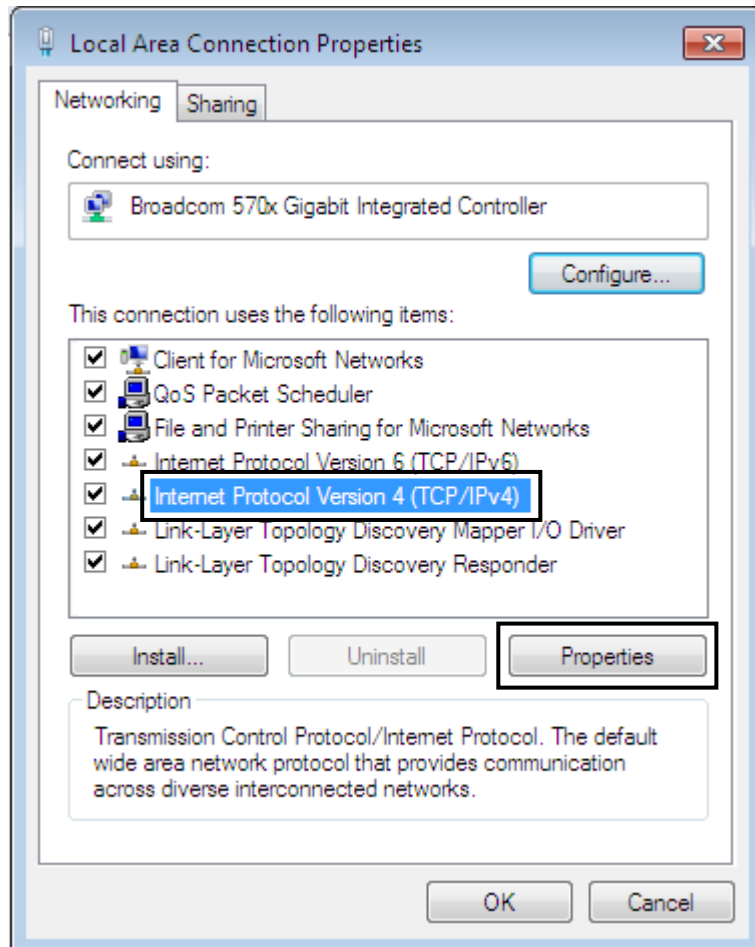
3.1.1 Configuring a PC in Windows 7/8

1. Go to **Start**. Click on **Control Panel**. Then click on **Network and Internet**.
2. When the **Network and Sharing Center** window pops up, select and click on **Change adapter settings** on the left window panel.
3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

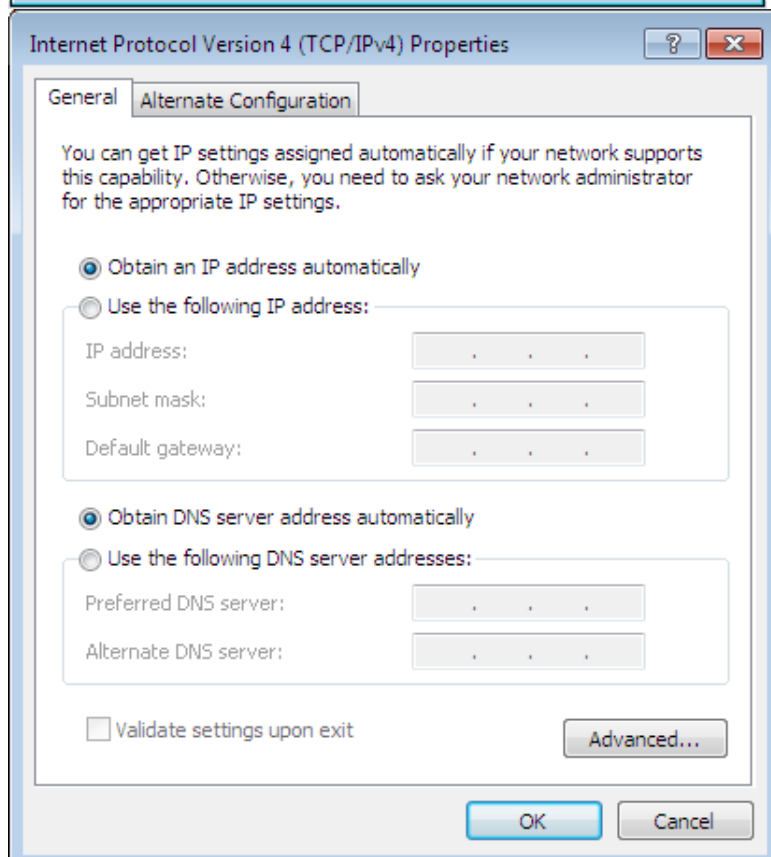


IPv4:

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

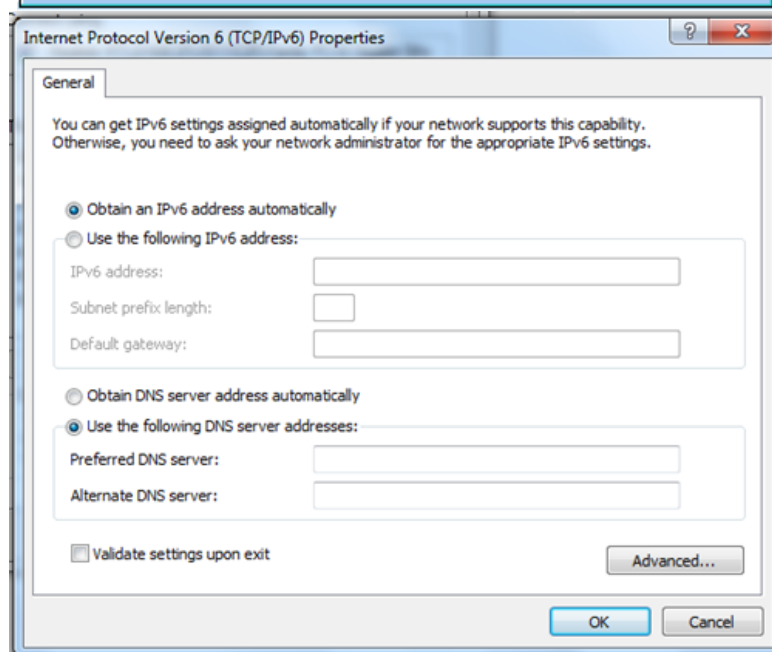
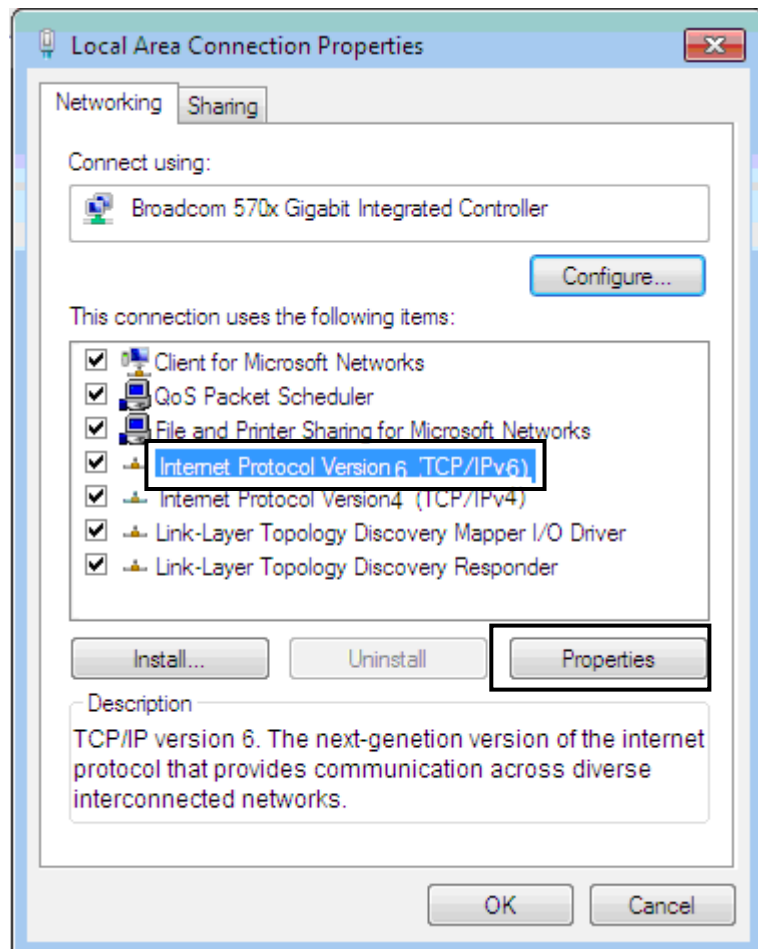


5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



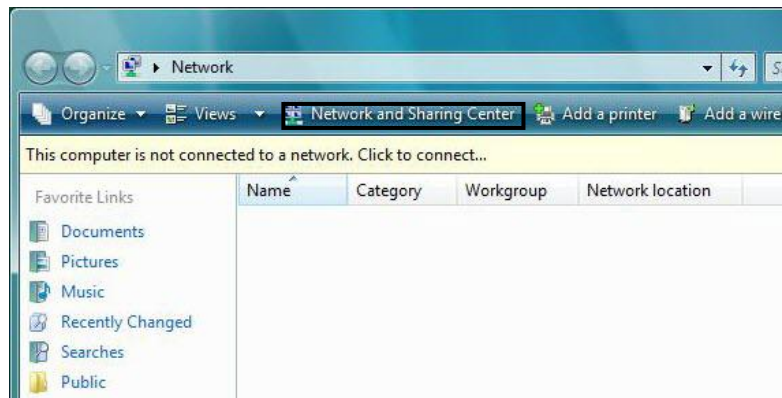
IPv6:

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



3.1.2 Configuring a PC in Windows Vista

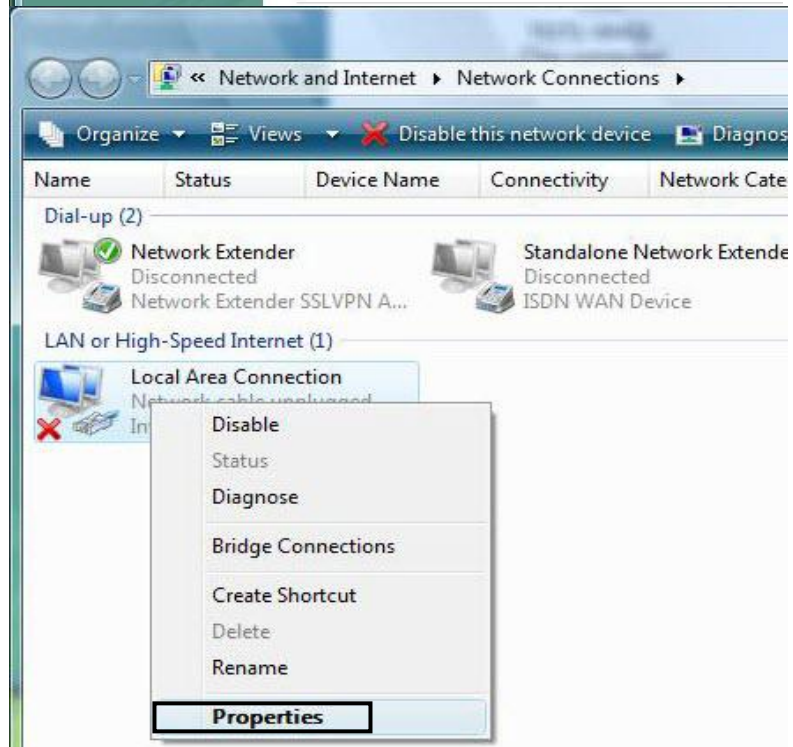
1. Go to **Start**. Click on **Network**. Then click on **Network and Sharing Center** at the top bar.



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

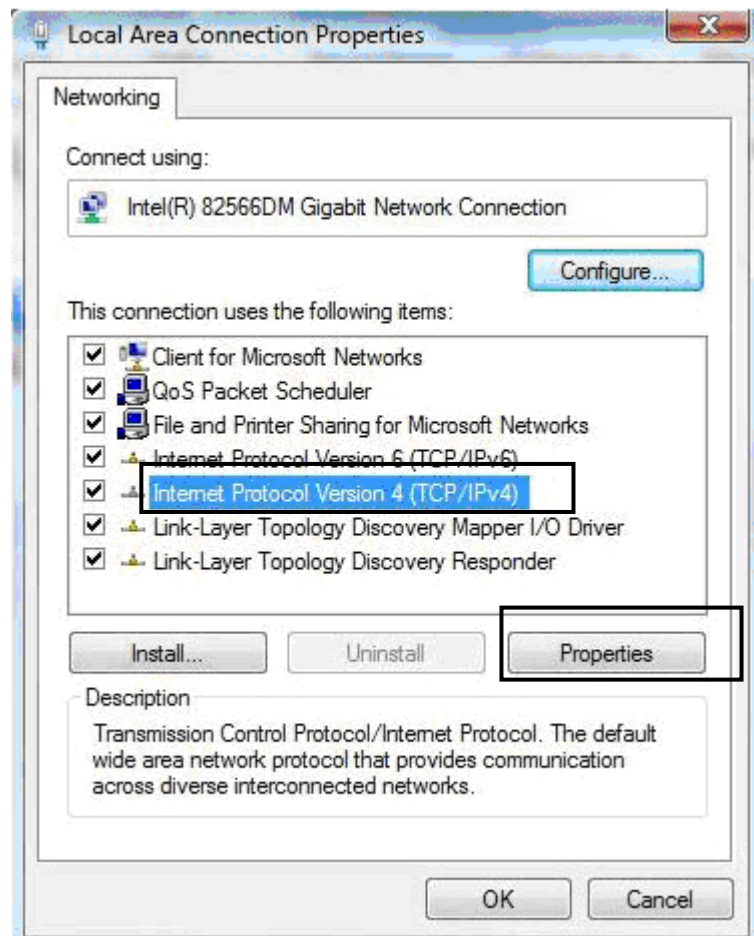


3. Select the **Local Area Connection**, and right click the icon to select **Properties**.

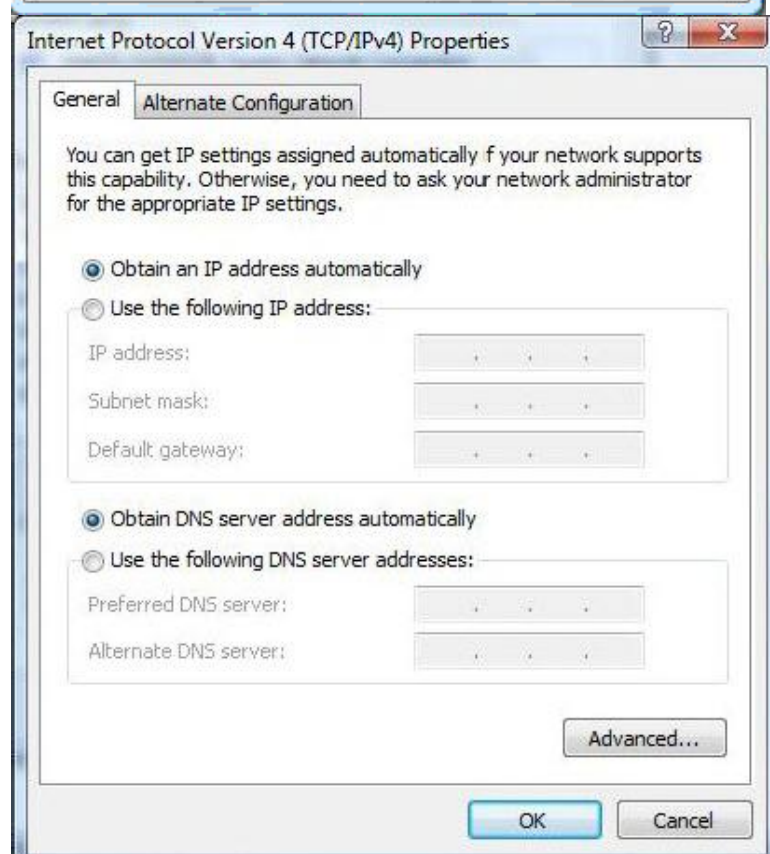


IPv4:

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



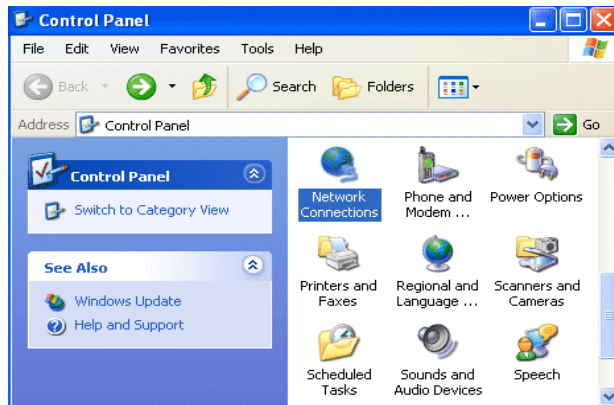
5. In the **TCP/IPv4 properties** window, select the **Obtain an IP address automatically** and **Obtain DNS Server address automatically** radio buttons. Then click **OK** to exit the setting.
6. Click **OK** again in the **Local Area Connection Properties** window to apply the new configuration.



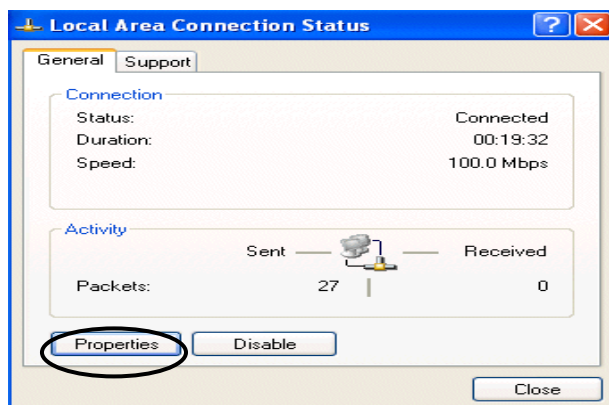
3.1.3 Configuring a PC in Windows XP

IPv4:

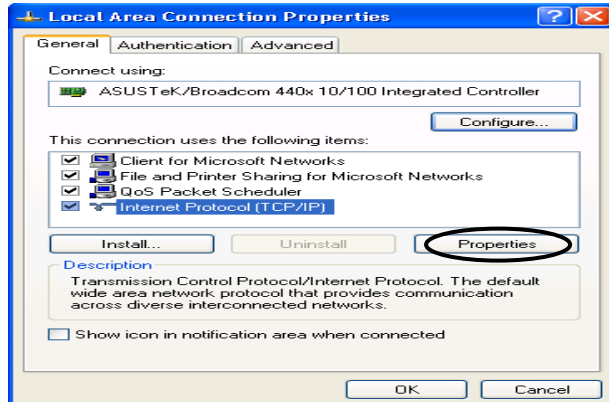
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



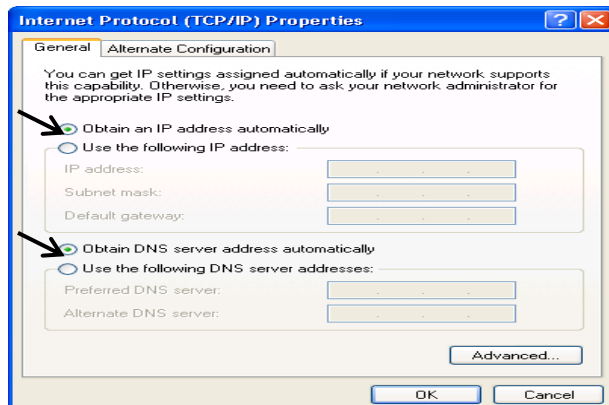
3. In the **Local Area Connection Status** window, click **Properties**.



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.



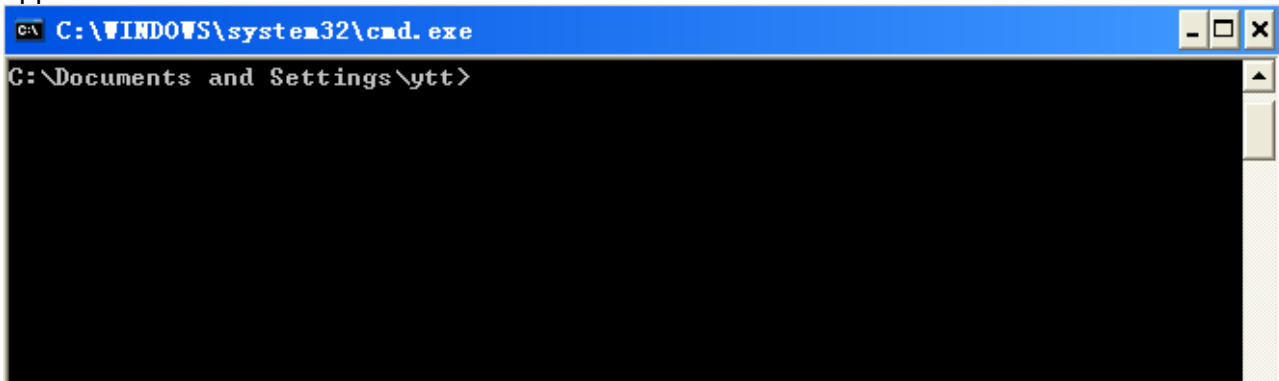
6. Click **OK** to finish the configuration.

IPv6:

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

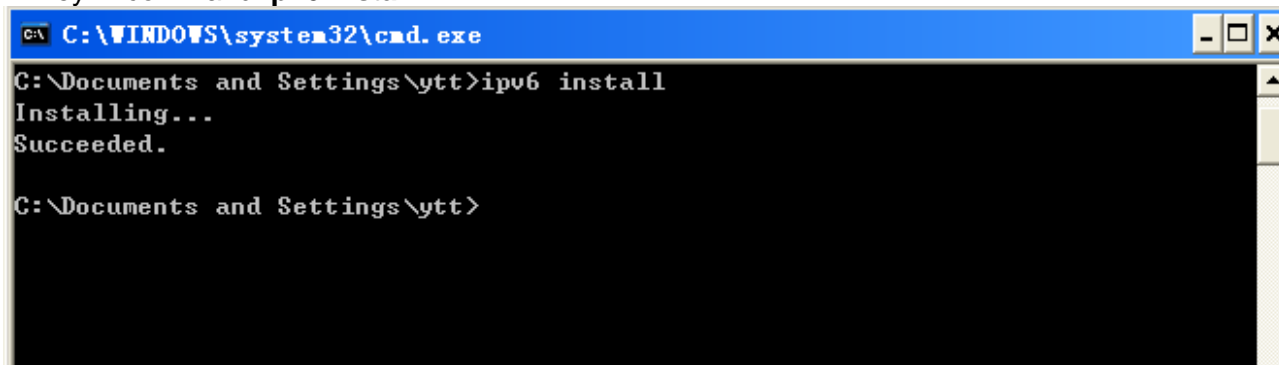
Act as shown below:

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.

3.2 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	20 IP addresses continuing from 192.168.1.100 through 192.168.1.119

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 **ADSL**(Dynamic IP Address, Static IP Address, PPPoE, PPPoA, Bridge Mode)

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

ADSL:

PPPoE	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).	
PPPoA	VPI/VCI, VC-based/LLC-based multiplexing, Username, Password, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).	
Dynamic IP Address	RFC1483 Bridged IP	VPI/ VCI, LLC-based/ VC-based multiplexing, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
	RFC1483 Routed IP	VPI/ VCI, LLC-based/ VC-based multiplexing, and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
Static IP Address	RFC1483 Bridged IP	VPI/ VCI, LLC-based/ VC-based multiplexing, Static IP Address, IP Subnet Mask, Gateway IP Address, and Domain Name System (DNS) IP address.
	RFC1483 Routed IP	VPI/ VCI, LLC-based/ VC-based multiplexing, Static IP Address, IP Subnet Mask, Gateway IP Address, and Domain Name System (DNS) IP address.
Bridge Mode	1483 Bridged Only	VPI/ VCI, LLC-based/ VC-based multiplexing.

Chapter 4

Configuration

4.1 Configuring the Router 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**”.

Authentication Required

The server http://192.168.1.254:80 requires a username and password. The server says: Wireless-N ADSL2+ Firewall Router .

User Name:

Password:

Log In

Cancel

Congratulation! You are now successfully logged on to the Router!

Wireless-N ADSL2+ Firewall Router

►Status

• Quick Start

►Configuration

►Language

Status

▼Device Information

Model NameWireless-N ADSL2+ Firewall Router

Firmware Version

MAC Address00:04:ED:01:23:45

Date-TimeTue Dec 20 18:38:13 UTC 2011

System Up Time38 mins

▼Physical Port Status

ADSL✓

Ethernet✓

Wireless✓

▼WAN

Interface	Protocol	VPI/VCI	Connection	IP Address	Default Gateway
PVC0 ▼	PPPoE	8/35	Not Connected	/	

▼LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.119 Enable / Stateless

▼Wireless

Mode	SSID	Channel	Security
802.11b+g+n	wlan-ap	6	OPEN

Restart

Logout

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, ADSL Status)
- **Quick Start** (Wizard Setup)
- **Configuration** (Interface Setup, Advanced Setup, 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**, **ADSL Status**.

Wireless-N ADSL2+ Firewall Router

▼Status

• Device Info

• System Log

• Statistics

• DHCP Table

• ADSL Status

• Quick Start

► Configuration

► Language

Status

▼ Device Information

Model Name

Wireless-N ADSL2+ Firewall Router

Firmware Version

MAC Address

00:04:ED:01:23:45

Date-Time

Tue Dec 20 18:37:53 UTC 2011

System Up Time

38 mins

▼ Physical Port Status

ADSL

Ethernet

Wireless

✓

✓

✓

▼ WAN

Interface	Protocol	VPI/VCI	Connection	IP Address	Default Gateway
PVC0 ▼	PPPoE	8/35	Not Connected	/	

▼ LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.119
		Enable / Stateless

▼ Wireless

Mode	SSID	Channel	Security
802.11b+g+n	wlan-ap	6	OPEN

Restart

Logout

4.2.1 Device Info

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

Status

Device Information

Model Name	Wireless-N ADSL2+ Firewall Router
Firmware Version	
MAC Address	00:04:ED:01:23:45
Date-Time	Tue Dec 20 18:38:13 UTC 2011
System Up Time	38 mins

Physical Port Status

ADSL	✓
Ethernet	✓
Wireless	✓

WAN

Interface	Protocol	VPI/VCI	Connection	IP Address	Default Gateway
PVC0	PPPoE	8/35	Not Connected	/	

LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.119 Enable / Stateless

Wireless

Mode	SSID	Channel	Security
802.11b+g+n	wlan-ap	6	OPEN

Device Information

Model Name: Show model name of the router

Firmware Version: This is the Firmware version

MAC Address: This is the MAC Address

Date Time: The current day time.

System Up Time: The duration since system is up.

Physical Port Status

Here the page shows the status of physical port of ADSL, Ethernet and Wireless.

WAN

Interface: The now used connection method, "ADSL(PVC0-PVC70)".

Protocol: The protocol in use.

VPI/VCI: The VPI/VCI in use.

Connection: The status of the link.

IP Address: The WAN interface IP address obtained.

Default Gateway: The default gateway address.

LAN

IP Address: LAN port address.

Subnet Mask/Prefix Length: LAN port IP subnet mask for IPv4 and Prefix length for IPv6..

DHCP Server: LAN port DHCP information.

Wireless

Mode: The wireless mode in use.

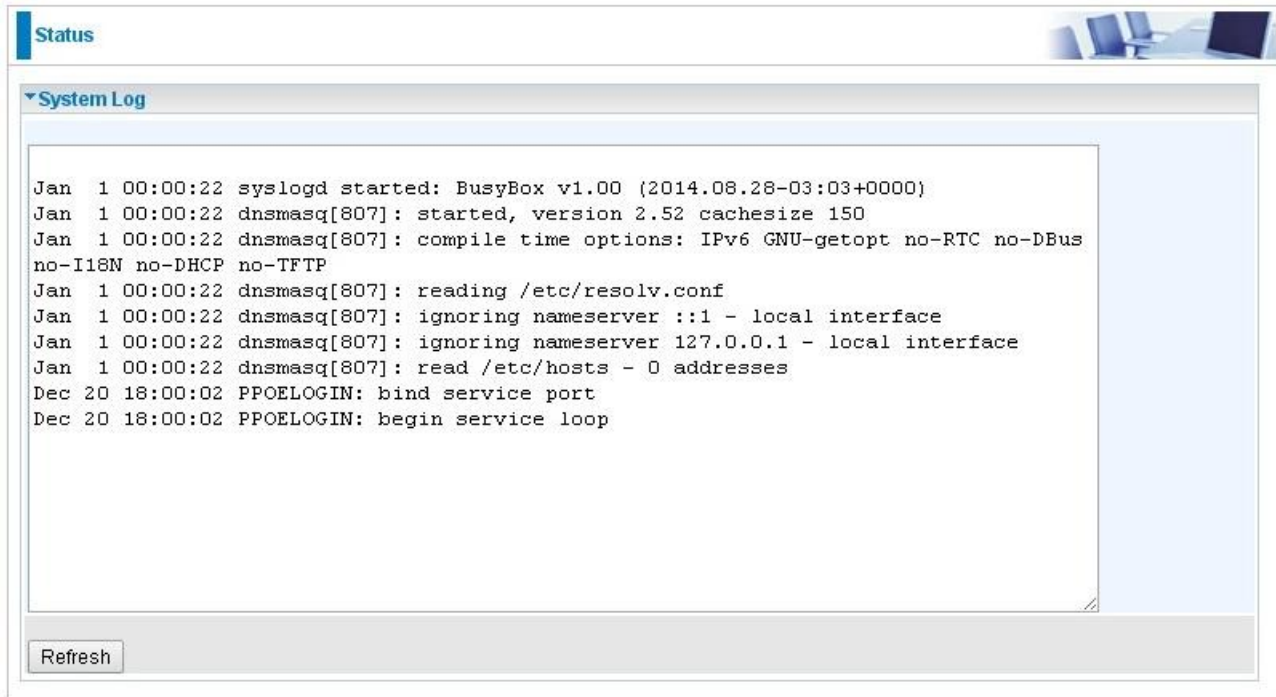
SSID: The SSID.

Channel: The current channel.

Security: The wireless security setting, authentication type.

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.



Refresh: Press this button to refresh the statistics.

4.2.4 Statistics

➤ ADSL

Status

Statistics

Traffic Statistics

Interface

☒ ADSL ☐ Ethernet ☐ Wireless

Transmit Statistics

Transmit Total PDUs80

Transmit Total Error Counts0

Receive Statistics

Receive Total PDUs65

Receive Total Error Counts0

Refresh

Transmit total PDUs: This field displays the number of total PDU transmitted until the latest second.

Transmit total Error Counts: This field displays the number of total error transmitted until the latest second.

Receive total PDUs: This field displays the number of total PDU received until the latest second.

Receive total Error Counts: This field displays the number of total error received until the latest second.

Refresh: Press this button to refresh the statistics.

➤ Ethernet

Status

Statistics

Traffic Statistics

Interface ☐ ADSL ☒ Ethernet ☐ Wireless

Transmit Statistics

Transmit Frames	14765
Transmit Multicast Frames	8646
Transmit Total Bytes	5449299
Transmit Collision	0
Transmit Error Frames	0

Receive Statistics

Receive Frames	6066
Receive Multicast Frame	60
Receive Total Bytes	790028
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

☐ ADSL
☐ Ethernet
☒ Wireless

Transmit Statistics

Transmit Frames

11610

Transmit Error Frames

0

Transmit Drop Frames

0

Receive Statistics

Receive Frames

70950

Receive Error Frames

6145

Receive Drop Frames

6145

Refresh

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.

4.2.5 DHCP Table

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



Status				
▼ DHCP Table				
#	Host Name	IP Address	MAC Address	Expire Time

#: 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.

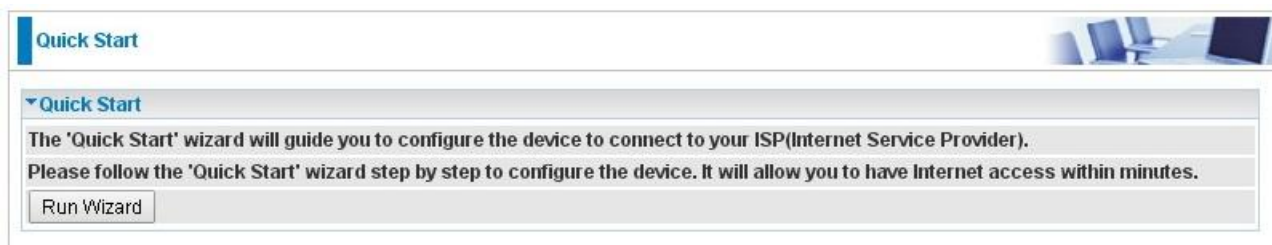
Expire Time: The total remaining interval since the IP assignment to the PC.

4.2.5 ADSL Status

The ADSL Status section displays the ADSL synchronization status.

Status	
▼ ADSL Status	
ADSL Status	
ADSL Firmware Version	FwVer:3.20.6.0_A_TC3087 HwVer:T14.F7_11.2
Line State	up
ADSL Mode	ITU G.992.5(ADSL2PLUS)
ADSL Type	ANNEX_M
Data Rate(Downstream)	25113 kbps
Data Rate(Upstream)	2563 kbps
SNR Margin(Downstream)	6.1 dB
SNR Margin(Upstream)	5.0 dB
Line Attenuation(Downstream)	0.0 dB
Line Attenuation(Upstream)	2.6 dB
ES(Downstream)	6
ES(Upstream)	0
SES(Downstream)	6
SES(Upstream)	0
UAS(Downstream)	2470
UAS(Upstream)	2470
Refresh	

4.3 Quick Start



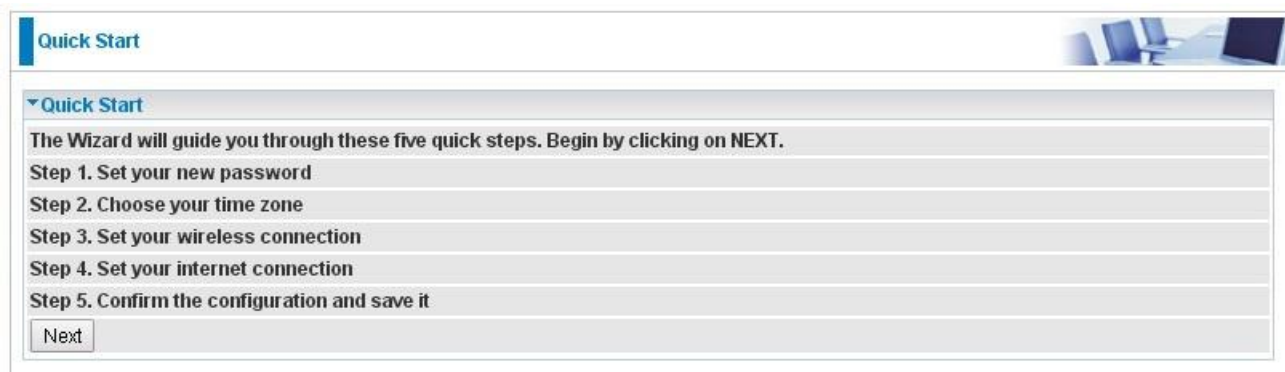
Quick Start

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

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

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

☒ Activated
☐ Deactivated

SSID

wlan-ap

Broadcast SSID

☒ Yes
☐ No

Channel

UNITED STATES
06

Security Type

OPEN

Back

Next

Step4: Set your Internet connection

WAN Transfer Modes: ADSL

Quick Start

Quick Start - ISP Connection Type

Dynamic IP Address

WAN Interface

ADSL

ISP

☐ Dynamic IP Address (Dynamic IP Address)
☐ Static IP Address (Choose this option to set static IP information provided to you by your ISP.)
☒ PPPoE or PPPoA (Choose this option if your ISP uses PPPoE or PPPoA.)
☐ Bridge Mode (Choose this option if your ISP uses Bridge Mode.)

Back

Next

1) Enter the PPPoE/PPPoA account / VPI,VCI information provided to you by your ISP. Click **NEXT** to continue.

Quick Start

Quick Start - PPPoE/PPPoA

Enter the PPPoE/PPPoA information provided to you by your ISP. Click NEXT to continue.

Username

Password

VPI

8

(0~255)

VCI

35

(1~65535)

Connection Type

PPPoE LLC

Back

Next

2).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

3). Quick Start Completed!

Quick Start



▼ Quick Start - Quick Start Completed !!

Quick Start Completed !!

Saved Changes.

4.4 Configuration

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

Wireless-N ADSL2+ Firewall Router

Configuration

Internet

WAN Interface

ADSL

ATM PVC

Virtual Circuit

PVC 0

PVCs Summary

Status

Activated

Deactivated

VPI

8

(range: 0~255)

VCI

35

(range: 32~65535)

QoS

ATM QoS

ubr

PCR

0

cells/second

SCR

0

cells/second

MBS

0

cells

IPv4/IPv6

IP Version

IPv4

IPv4/IPv6

IPv6

ISP Connection Type

ISP

Dynamic IP Address

Static IP Address

PPPoE/PPPoA

Bridge Mode

802.1q Options

802.1q

Activated

Deactivated

VLAN ID

0

(range: 0~4095)

PPPoE/PPPoA

Restart

Logout

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.

Wireless-N ADSL2+ Firewall Router

► Status

► Quick Start

► Configuration

► Interface Setup

► Internet

► LAN

► Wireless

► Wireless MAC Filter

► Advanced Setup

► Access Management

► Maintenance

► Language

Configuration

▼ Internet

WAN Interface

ADSL ▼

ATM PVC

Virtual Circuit

PVC 0 ▼

PVCs Summary

Status

☒ Activated ☐ Deactivated

VPI

8

(range: 0~255)

VCI

35

(range: 32~65535)

QoS

ATM QoS

ubr ▼

PCR

0

cells/second

SCR

0

cells/second

MBS

0

cells

IPv4/IPv6

IP Version

☐ IPv4 ☒ IPv4/IPv6 ☐ IPv6

ISP Connection Type

ISP

☐ Dynamic IP Address ☐ Static IP Address ☒ PPPoE/PPPoA ☐ Bridge Mode

802.1q Options

802.1q

☐ Activated ☒ Deactivated

VLAN ID

0

(range: 0~4095)

PPPoE/PPPoA

Restart

Logout

4.4.1.1 Internet

Configuration

Internet

WAN Interface

ADSL ▾

ATM PVC

Virtual Circuit

PVC 0 ▾

PVCs Summary

Status

☒ Activated ☐ Deactivated

VPI

8

(range: 0~255)

VCI

35

(range: 32~65535)

QoS

ATM QoS

ubr ▾

PCR

0

cells/second

SCR

0

cells/second

MBS

0

cells

IPv4/IPv6

IP Version

☐ IPv4 ☒ IPv4/IPv6 ☐ IPv6

ISP Connection Type

ISP

☐ Dynamic IP Address ☐ Static IP Address ☒ PPPoE/PPPoA ☐ Bridge Mode

802.1q Options

802.1q

☐ Activated ☒ Deactivated

VLAN ID

0

(range: 0~4095)

PPPoE/PPPoA

Connection Type

PPPoE LLC ▾

Username

Password

Bridge Interface for PPPoE

☐ Activated ☒ Deactivated

Connection Setting

Connection

☒ Always On (Recommended) ☐ Connect Manually

TCP MSS Option

TCP MSS 0

bytes(0 means use default)

IP Options

IP Common Options

Default Route

☒ Yes ☐ No

TCP MTU Option

TCP MTU 0

bytes(0 means use default:1492)

IPv4 Options

Get IP Address

☐ Static ☒ Dynamic

Static IP Address

0.0.0.0

IP Subnet Mask

0.0.0.0

Gateway

0.0.0.0

NAT

Enable ▾

Dynamic Route

RIP1 ▾

Direction None ▾

IGMP Proxy

☐ Enable ☒ Disable

IPv6 Options

IPv6 Address

/

Obtain IPv6 DNS

☒ Enable ☐ Disable

Primary DNS

Secondary DNS

MLD Proxy

☐ Enable ☒ Disable

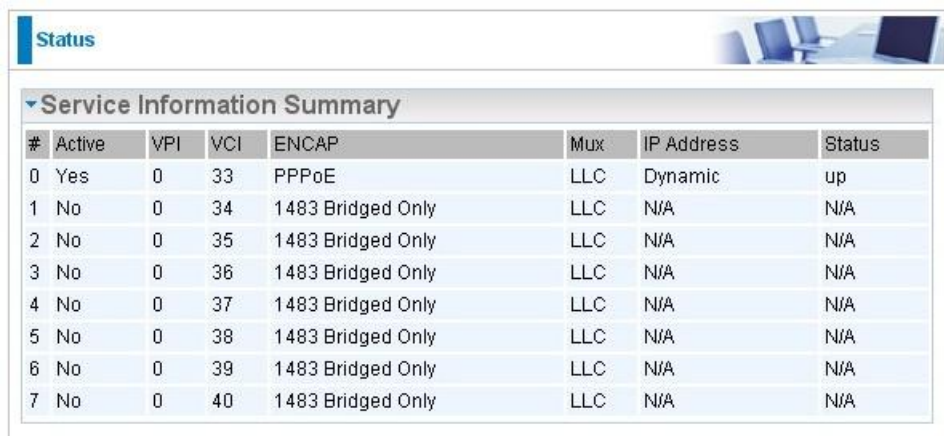
Save

■ ATM VC

ATM settings are used to connect to your ADSL service. Your ISP provides VPI, VCI settings to you (VPI, VCI pair is used to set a PVC). In this Device, you can totally setup 8 PVCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the PVC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.

Virtual Circuit: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. VPI, VCI pair is used to set a PVC

PVC Summary: show the information for each PVC where users can check status of each PVC.



Service Information Summary							
#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
0	Yes	0	33	PPPoE	LLC	Dynamic	up
1	No	0	34	1483 Bridged Only	LLC	N/A	N/A
2	No	0	35	1483 Bridged Only	LLC	N/A	N/A
3	No	0	36	1483 Bridged Only	LLC	N/A	N/A
4	No	0	37	1483 Bridged Only	LLC	N/A	N/A
5	No	0	38	1483 Bridged Only	LLC	N/A	N/A
6	No	0	39	1483 Bridged Only	LLC	N/A	N/A
7	No	0	40	1483 Bridged Only	LLC	N/A	N/A

VPI: The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. This field may already be configured.

VCI: The valid range for the VCI is 32 to 65535. Enter the VCI assigned to you. This field may already be configured.

■ QoS

ATM QoS: Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include **CBR** (Constant Bit Rate), **VBR** (Variable Bit Rate) and **UBR** (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR and MBS.

Select CBR to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR for applications that are non-time sensitive, such as e-mail. Select VBR for burst traffic and bandwidth sharing with other applications.

PCR: Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.

SCR: The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.

MBS: Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535

■ IPv4/IPv6

IP version: choose **IPv4**, **IPv4/IPv6**, **IPv6** base 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.

■ Encapsulation:

ISP: Select the encapsulation type your ISP uses from the **Encapsulation** list.

Choices vary depending on what you select in the **Mode** field.

- ① **Dynamic IP:** Select this option if your ISP provides you an IP address automatically. Please enter the Dynamic IP information accordingly.

- ① **Static IP:** Select this option to set static IP information. You will need to enter 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 (x.x.x.x). The Router will not accept the IP address if it is not in this format.
- ① **PPPoE/PPPoA:** Select this option if your ISP requires you to use a PPPoE/PPPoA connection. This option is typically used for DSL services.
- ① **Bridge Mode:** select this option if you want use this router as a OSI 2 layer device like a 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/PPPoA

Connection Type: Select PPPoE LLC, PPPoE VC-Mux, PPPoA LLC, PPPoA VC-Mux by your ISP in the Mode field.

PPP Authentication: PPP authentication method, PAP, CHAP or Auto.

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.

TCP MTU Option: Enter the TCP Maximum Transmission Unit (MTU).

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.

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.

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
☒ LAN4
☒ 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

Save

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: If set to **Enabled**, your Router 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 Router 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).

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.

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:

■ IPv6 parameters

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

☒ Activated ☐ Deactivated

AP MAC Address

00:04:ED:45:23:00

Wireless Mode

802.11b+g+n

Channel

UNITED STATES06Current Channel : 6

Beacon Interval

100(range: 20~1000)

RTS/CTS Threshold

2347(range: 1500~2347)

Fragmentation Threshold

2346(range: 256~2346, even numbers only)

DTIM Interval

1(range: 1~255)

TX Power

100(range:1~100)

IGMP Snooping

☒ Yes ☐ No

11n Settings

Channel Bandwidth

40 MHz

Guard Interval

Auto

MCS

Auto

SSID Settings

Available SSID

1

SSID Index

☒ SSID1

SSID

wlan-ap

Broadcast SSID

☒ Yes ☐ No

Clients Isolation

☐ Yes ☒ No

SSID Activated

Always

WPS Settings

Use WPS

☒ Yes ☐ No

WPS State

Configured

WPS Mode

☐ PIN code ☒ PBC

Security Settings

Security Type

OPEN

WDS Settings

AP MAC Address

00:04:ED:45:23:00

WDS Mode

☐ Activated ☒ Deactivated

WDS Peer MAC #1

00:00:00:00:00:00

WDS Peer MAC #2

00:00:00:00:00:00

WDS Peer MAC #3

00:00:00:00:00:00

WDS Peer MAC #4

00:00:00:00:00:00

Save

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**, **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 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 time-slot 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 <button>Generate</button>
Enrollee PIN Code	04640776
WPS Progress	In progress <button>Stop WPS</button>
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 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 Ralink WPS utility interface. At the top, there is a navigation bar with icons for Profile, Network, Advanced, Statistics, WMM, WPS, Radio On/Off, and About. The WPS tab is currently selected.

The main area is divided into two sections: "WPS AP List" and "WPS Profile List".

WPS AP List:

ID :	AP Name	MAC Address	Channel
ID :	Billion_AP	00 04 ED 85 46 72	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:

Profile Name	MAC Address	Channel
Profile 1	00-21-85-BE-3B-2B	1
Profile 2	00-21-27-6A-2B-7E	8
Profile 3	00-21-91-EE-2A-68	9

On the right side, there are several buttons: Rescan, Information, Pin Code (04640776), Renew, Config Mode (Enrollee), Detail, Connect, Rotate, Disconnect, Export Profile, and Delete.

At the bottom left, there are buttons for PIN and PBC. The PIN button is highlighted. Below these buttons, there are checkboxes for "WPS Associate IE" and "WPS Probe IE", both of which are checked.

At the bottom right, there is a "Progress" bar showing "Progress >> 0%". Below this, there is a message: "PIN - WPS Eap process failed".

At the bottom, there is a "Status" section with various indicators: Link Quality >> 0%, Signal Strength1 >> 0%, Signal Strength2 >> 0%, and Noise Strength >> 0%. There are also graphs for Transmit and Receive Link Speed and Throughput.

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 WPS configuration interface with the following sections:

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

ID	SSID	MAC	Count
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
- WPSProfile List:**
 - Billion_AP
- WPS Configuration:**
 - PIN:** ☒ WPS Associate IE
 - PBC:** ☒ WPS Probe IE
 - Progress:** Progress >> 100%
 - Status:** WPS status is connected successfully
- Right Panel:**
 - Rescan
 - Information
 - Pin Code: 04640776 (Renew)
 - Config Mode: Enrollee
 - Detail
 - Connect
 - Rotate
 - Disconnect
 - Export Profile
 - Delete
- Status & Performance:**
 - Status >>:** Billion_AP <--> 00-04-ED-85-46-92
 - Extra Info >>:** Link is Up [TxPower:100%]
 - Channel >>:** 1 <--> 2412 MHz; central channel : 6
 - Authentication >>:** WPA2-PSK
 - Encryption >>:** AES
 - Network Type >>:** Infrastructure
 - IP Address >>:** 192.168.1.101
 - Sub Mask >>:** 255.255.255.0
 - Default Gateway >>:** 192.168.1.254
 - HT:**
 - BW >> 40
 - GI >> long
 - MCS >> 5
 - SNR0 >> 30
 - SNR1 >> 20102206
 - 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

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 <button>Generate</button>
Enrollee PIN Code	
WPS Progress	In progress <button>Stop WPS</button>
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 from the WPS AP List before pressing the PIN button to run the scan.

The screenshot displays the Ralink WPS utility interface. At the top, there is a navigation bar with icons for Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, About, and Help. Below the navigation bar, the main window is divided into several sections.

WPS AP List: A table showing discovered APs. The first AP is 'Billion_AP' with ID '0x0000', MAC '00-04-ED-85-46-92', and channel '1'. The second AP is 'Welcome to RFINICS' with ID '00-21-27-6A-2B-7E' and channel '8'. The third AP is 'Mai-Lang' with ID '00-21-91-EE-2A-68' and channel '9'. To the right of the table are buttons for 'Rescan', 'Information', 'Pin Code' (with a text field containing '03454435' and a 'Renew' button), 'Config Mode' (set to 'Registrar'), 'Detail', 'Connect', 'Rotate', 'Disconnect', and 'Export Profile'.

WPS Profile List: A section showing the selected profile 'Billion_AP'.

Buttons: 'PIN' and 'PBC' buttons are located below the profile list. To their right are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked.

Progress Bar: A blue progress bar indicates 'Progress >> 100%'. Below it, a status message reads 'WPS status is connected successfully'.

Status Section: On the left, a detailed status report is shown:

- 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 Section: Below the status report, HT parameters are listed:

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

Link Quality Section: On the right, a green bar indicates 'Link Quality >> 100%'. Below it, three bars show:

- Signal Strength 1 >> 24%
- Signal Strength 2 >> 65%
- Noise Strength >> 26%

Transmit Section: Below the link quality, transmit statistics are shown:

- Link Speed >> 150.0 Mbps
- Throughput >> 0.000 Kbps

 A small graph shows the transmit throughput over time, with a peak of 1.632 Kbps.

Receive Section: Below the transmit statistics, receive statistics are shown:

- Link Speed >> 1.0 Mbps
- Throughput >> 118.144 Kbps

 A small graph shows the receive throughput over time, with a peak of 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 page of a router. The top navigation bar includes links for Network, Advanced, Statistics, WMM, WPS (selected), Radio On/Off, About, and Help. The main content area is titled 'WPS AP List' and contains a table with the following data:

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

Below the table is the 'WPS Profile List' section, which shows 'Billion_AP' selected. To the right of the table are several buttons: Rescan, Information, Pin Code (with a field showing '03454435' and a 'Renew' button), Config Mode (set to 'Registrar'), Detail, Connect, Rotate, Disconnect, and Export Profile.

At the bottom of the WPS section, there are checkboxes for 'WPS Associate IE' and 'WPS Probe IE', both of which are checked. A progress bar indicates 'Progress >> 100%', and a status message states 'WPS status is connected successfully'.

The bottom section of the interface provides detailed status information for the 'Billion_AP' connection. It includes the following data:

- Status >> Billion_AP <--> 00-04-ED-85-46-92
- Extra Info >> Link is Up [TxPower:100%]
- Channel >> 1 <--> 2412 MHz; central channel : 6
- Authentication >> WPA2-PSK
- Encryption >> AES
- Network Type >> Infrastructure
- IP Address >> 192.168.1.101
- Sub Mask >> 255.255.255.0
- Default Gateway >> 192.168.1. 254
- HT
- BW >> 40
- GI >> short
- MCS >> 7
- SNR0 >> 30
- SNR1 >> 20102206

On the right side of the status section, there are four color-coded bars representing different metrics:

- Link Quality >> 100% (Green)
- Signal Strength 1 >> 24% (Red)
- Signal Strength 2 >> 65% (Yellow)
- Noise Strength >> 26% (Green)

Below these bars are two graphs: 'Transmit' and 'Receive'. The 'Transmit' graph shows a Link Speed of 150.0 Mbps and a Throughput of 0.000 Kbps. The 'Receive' graph shows a Link Speed of 1.0 Mbps and a Throughput of 118.144 Kbps. Both graphs have a 'Max' label and a corresponding bar chart.

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 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 (Wi-Fi Protected Setup) configuration page of a router. The top navigation bar includes buttons for Profile, Network, Advanced, Statistics, WMM, WPS (selected), SSD, and Radio On/Off. The main content area is divided into several sections:

- WPS AP List:** A table listing available wireless access points.

ID	SSID	MAC Address	Channel
wlan-ap		00-04-ED-33-EF-D1	1
0x0004	Billion_AP	00:04:ED:85:46:92	1
111111		00-0C-43-30-52-50	7
	Welcome to RFINICS	00-21-27-6A-2B-7E	8
- WPS Profile List:** Shows the selected profile, "Billion_AP".
- Configuration Options:**
 - PIN:** A button to enter the PIN mode.
 - PBC:** A button to enter the Push Button Configuration mode.
 - WPS Associate IE:** A checkbox that is checked.
 - WPS Probe IE:** A checkbox that is checked.
- Progress Bar:** A blue progress bar indicating "Progress >> 100%".
- Status Message:** "WPS status is connected successfully - 5200NRC".
- Right-Hand Side Controls:**
 - Rescan:** Button to refresh the AP list.
 - Information:** Button to view more details.
 - Pin Code:** A text field showing "00745659" with a "Renew" button.
 - Config Mode:** A dropdown menu set to "Registrar".
 - Detail, Connect, Rotate, Disconnect, Export Profile:** Additional control buttons.
- Connection Details (Bottom Left):**
 - 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 >> 20
 - GI >> short
 - MCS >> 7
 - SNRO >> 0
 - SNR1 >> 20102453
- Transmit Section:**
 - Link Speed >> 72.2 Mbps
 - Throughput >> 1.008 Kbps
- Receive Section:**
 - Link Speed >> 1.0 Mbps
 - Throughput >> 48.172 Kbps
- Signal Quality Indicators (Top Right):**
 - Link Quality >> 100% (Green bar)
 - Signal Strength 1 >> 62% (Yellow bar)
 - Signal Strength 2 >> 86% (Green bar)
 - Noise Strength >> 26% (Blue bar)
- Signal Spectrum Graphs (Bottom Right):**
 - Transmit Spectrum:** A graph showing the transmit signal spectrum with a peak at 17.744 Kbps.
 - Receive Spectrum:** A graph showing the receive signal spectrum with a peak at 256.300 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

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

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.

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: the follow Wireless LAN station(s) association.

MAC Address:

Wireless MAC Address Filter Listing

Index	MAC Address	Edit	Delete
-------	-------------	------	--------

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

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

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

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

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

4.4.2 Advanced Setup

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

Wireless-N ADSL2+ Firewall Router

► Status

► Quick Start

▼ Configuration

► Interface Setup

► Advanced Setup

► Firewall

► Routing

► NAT

► Static DNS

► ADSL

► QoS

► Interface Grouping

► Time Schedule

► Remote System Log

► Access Management

► Maintenance

► Language

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

Restart

Logout

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.



The screenshot shows a web interface for configuring a router's firewall. At the top, there is a 'Configuration' tab. Below it, the 'Firewall' section is expanded, showing two settings: 'Firewall' and 'SPI'. Both settings have radio buttons for 'Enabled' and 'Disabled', with 'Disabled' being selected for both. A warning message is displayed below the SPI setting: '(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)'. At the bottom of the section, there is a 'Save' button.

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

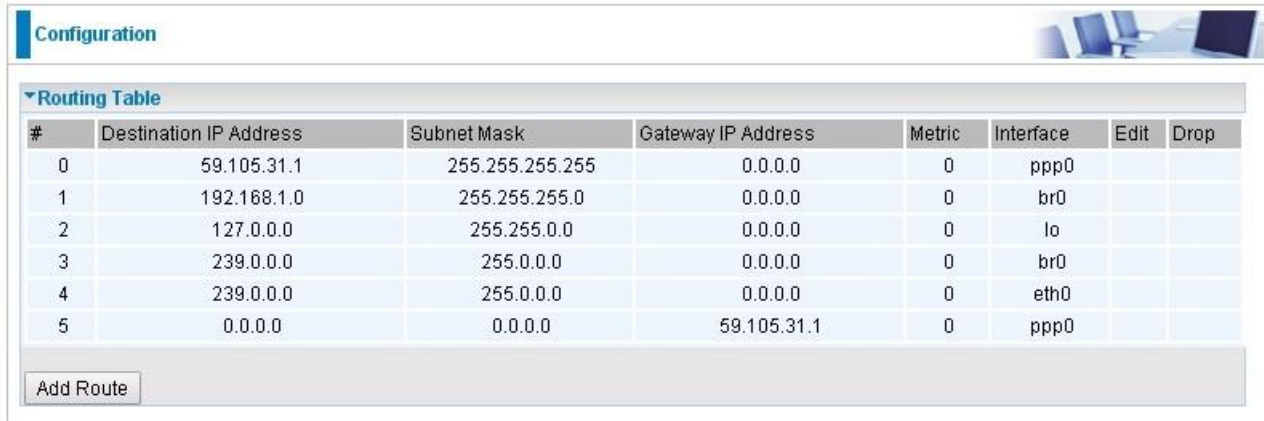
- ① **Enabled:** It activates your firewall function.
- ① **Disabled:** It disables the firewall function.

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.



#	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	59.105.31.1	255.255.255.255	0.0.0.0	0	ppp0		
1	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
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	59.105.31.1	0	ppp0		

Add Route

#: 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"/> <input type="text" value="0.0.0.0"/> <input checked="" type="radio"/> PVC0 ▼
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.

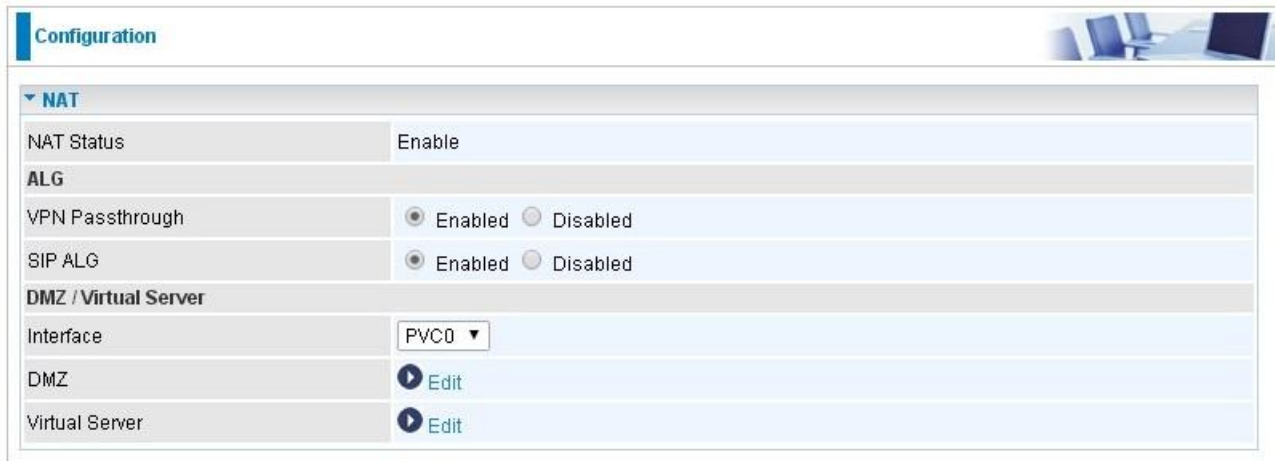
Gateway IP Address/Interface : This is the gateway IP address or existing interface to which packets are to be forwarded.

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”, “DMZ/Virtual Server” provided to solve these nasty problems.



Configuration	
NAT	
NAT Status	Enable
ALG	
VPN Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SIP ALG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DMZ / Virtual Server	
Interface	PVC0 ▼
DMZ	Edit
Virtual Server	Edit

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

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

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

Interface: Select to set DMZ/Virtual Server for “ADSL(PVC0-PVC7)”.

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-based configuration interface for DMZ settings. At the top, there is a 'Configuration' header with a small graphic of a laptop and a network diagram. Below the header, the 'DMZ' section is expanded, showing three configuration fields: 'DMZ for' set to 'Single IPs Account/ PVC0', 'DMZ' with radio buttons for 'Enabled' and 'Disabled' (where 'Disabled' is selected), and 'DMZ Host IP Address' set to '0.0.0.0'. At the bottom of the configuration area, there are 'Save' and 'Back' buttons.

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

Note: Here you can see the Single IPs Account/PVC0. 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

Single IPs Account/ PVC0

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.

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.

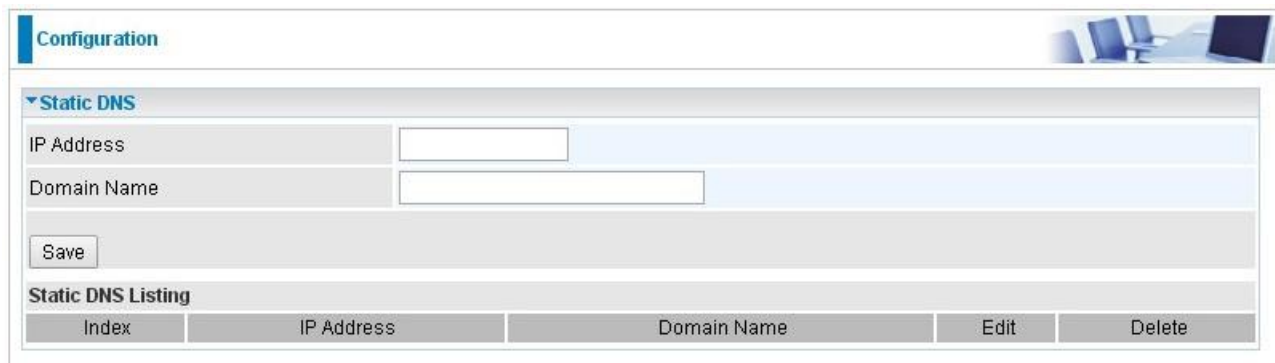
If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into 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 interface. At the top, there is a 'Configuration' tab. Below it, a section titled 'Static DNS' contains two input fields: 'IP Address' and 'Domain Name'. A 'Save' button is located below these fields. At the bottom, there is a 'Static DNS Listing' table with five columns: 'Index', 'IP Address', 'Domain Name', 'Edit', and 'Delete'.

Index	IP Address	Domain Name	Edit	Delete
-------	------------	-------------	------	--------

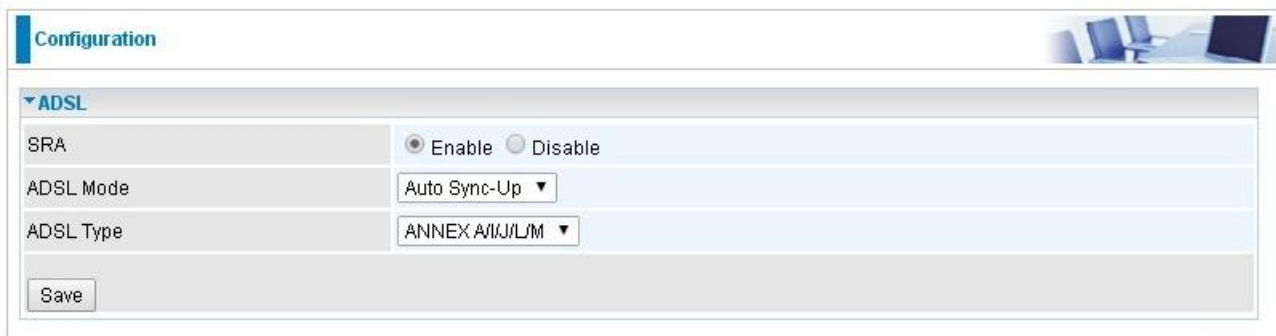
IP Address: The IP address you are going to give a specific domain name.

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

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

4.4.2.5 ADSL

This screen allows you to adjust DSL parameters. DSL knowledge is required to configure these settings. Contact your ISP to make sure that these parameters are correct.



The screenshot shows a web-based configuration interface. At the top, there is a header bar with the word "Configuration" on the left and a small graphic of a desk with a laptop on the right. Below the header, there is a section titled "ADSL" with a downward-pointing arrow. This section contains three rows of configuration options: "SRA" with radio buttons for "Enable" (selected) and "Disable"; "ADSL Mode" with a dropdown menu showing "Auto Sync-Up"; and "ADSL Type" with a dropdown menu showing "ANNEX A/I/J/L/M". At the bottom of this section is a "Save" button.

SRA: Seamless Rate Adaptation, is a technology used to adapt the rate seamlessly without any influence to the working system, to assure of the quality of the DSL system.

ADSL Mode: The default setting is **Auto Sync-Up**. This mode will automatically detect your ADSL2+, ADSL2, G.DMT, G.lite, and T1.413.

ADSL Type: There are five modes "Annex A", "Annex I", "Annex A/L", "Annex M" and "Annex A/I/J/L/M" that user can select for this connection.

4.4.2.6 QoS

Quality of Service (QoS) helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice data packets given higher priority than Web data packets.

The main goal of QoS is prioritizing incoming data, preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows.

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 **Add** to save your changes.

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

Configuration

Quality of Service

QoS

☐ Activated ☒ Deactivated

QoS Scheduling

☐ Weighted Round Robin(WRR) ☒ Strict Priority

WRR Weight

Highest: High: Medium: Low: (valid:1~15)

Scheduling Save

Rules Summary

Classification Criteria

Rule Index

Active

☐ Activated ☒ Deactivated

Application

Physical Ports

☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐ WLAN

Destination MAC Address

Destination IPv4/IPv6 Address

Destination Subnet Mask/IPv6 Prefix

Destination Port Range

~

Source MAC Address

Source IPv4/IPv6 Address

Source Subnet Mask/IPv6 Prefix

Source Port Range

~

Protocol ID

VLAN ID Range

~

IPP/DSCP Field

☐ IPP/TOS ☒ DSCP

IP Precedence Range

~

Type of Service

DSCP's Range

~ (Value Range: 0 ~ 63)

802.1p

~

Action

IPP/DSCP Field

☐ IPP/TOS ☒ DSCP

IP Precedence Remarking

Type of Service Remarking

DSCP Remarking

(Value Range: 0 ~ 63)

802.1p Remarking

~

Queue

Add

Delete

QoS: Select to activate QoS configuration..

QoS Scheduling: The Queue Scheduling Algorithm, here supporting WRR (Weighted Round Robin) and SP (Strict Priority).

- ① **WRR:** Weighted Round Robin, used to alternate each WRR queue to ensure that every queue can enjoy its due service time (resource) in accordance with its weight.
- ① **SP:** Strict Priority; it always sends the packets in queue with higher priority, and under this circumstance, the packets in lowest-priority queue may be delayed for quite a long time.

WRR Weight: Available only when WRR is used in QoS Scheduling field.

Scheduling Save: To save the strategy set above.

Rule Summary: To view the rule & action setting details.

Rule

You can set 16 different QoS rules. Each QoS rule has its detail setting conditions like: Application, Physical Ports, MAC, IP, Port, Protocol etc, you can modify the default 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. If the original packet does not have 802.1p tagged header, system will not add header for this packet even the detail setting condition has adding 802.1p priority ability.

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

Active: Select QoS is activated or deactivated.

Application: Select the different applications: IGMP, SIP, H.323, MGCP, SNMP, DNS, DHCP, RIP, RSTP, RTCP, RTP.

Physical Ports: This option is to allow you to decide which physical port you want to configure as condition for packets filtering; user can choose to specify the specific physical port for accurate filtering or skip this option if no .accurate settings needed.

Destination MAC Address: Set the Ethernet MAC value that you want to filter on destination side.

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

Destination Subnet Mask/Prefix: Specify the 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 MAC Address: Set the Ethernet MAC value that you want to filter on source 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 Subnet Mask for IPv4 or prefix for IPv6 on source side.

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

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

Vlan ID Range: Set the Vlan value that you want to filter.

IPP/DS Field: Select IP QoS format.

IP Precedence Range: Select the IP precedence range.

Type of Service : Select from the 5 different types of service .

DSCP: Set the DSCP value that you want to filter.

802.1p: Set the remarked new 802.1p priority value on the packet that fulfill every detail setting condition of each rule.

Action

After finishing all rules detail condition setting, select the rule you want to execute and action here.

IPP/DS Field: Select IP QoS format.

IP Precedence Marking: Select the value to remark IP precedence.

Type of Service Marking: Select the value to remark Type of Service.

DSCP Marking: Set the value to remark DSCP.

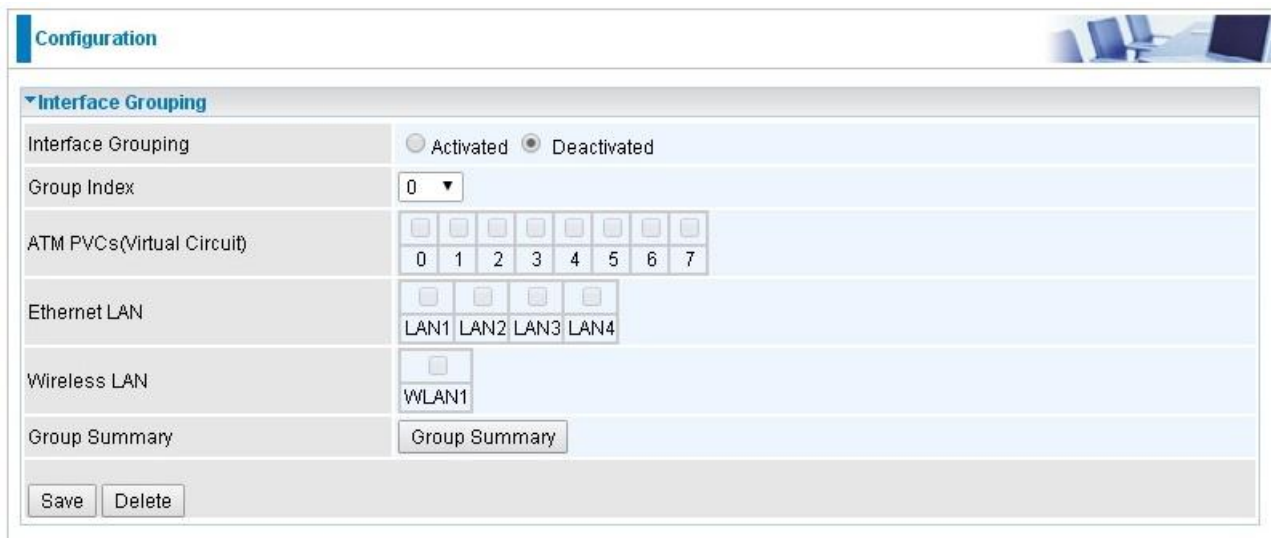
802.1p Marking: Select the value to remark 802.1p.

Queue #: The four types of Queue - Low, Medium, High, Highest – which you want to put in if the packet meets the condition.

4.4.2.7 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 with the 'Interface Grouping' section expanded. It includes a 'Group Index' dropdown set to 0, and checkboxes for 'ATM PVCs(Virtual Circuit)', 'Ethernet LAN', and 'Wireless LAN'. Below these are buttons for 'Group Summary', 'Save', and 'Delete'.

Interface Grouping	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Group Index	0 ▼
ATM PVCs(Virtual Circuit)	<input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7
Ethernet LAN	<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4
Wireless LAN	<input type="checkbox"/> WLAN1
Group Summary	Group Summary
<input type="button" value="Save"/> <input type="button" value="Delete"/>	

Interface Grouping: Select Yes to enable Interface Grouping feature.

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

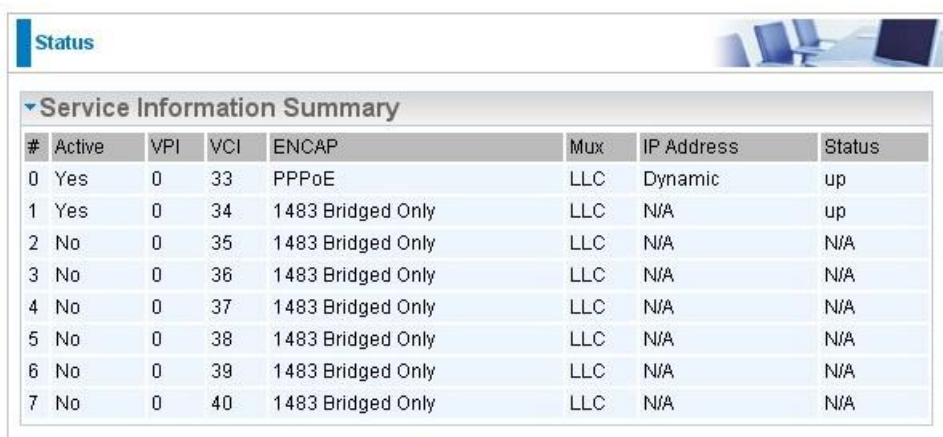
ATM PVCs (Virtual Circuit): The available ADSL PVCs. Move to [4.4.1 Interface Setup](#) to add other ADSL .service

Ethernet LAN: The available Ethernet ports.

Wireless LAN: The available wireless ports.

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

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



The screenshot shows the 'Status' page with the 'Service Information Summary' table. The table has columns for #, Active, VPI, VCI, ENCAP, Mux, IP Address, and Status. It lists 8 services, with Service0 and Service1 being active and up.

#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
0	Yes	0	33	PPPoE	LLC	Dynamic	up
1	Yes	0	34	1483 Bridged Only	LLC	N/A	up
2	No	0	35	1483 Bridged Only	LLC	N/A	N/A
3	No	0	36	1483 Bridged Only	LLC	N/A	N/A
4	No	0	37	1483 Bridged Only	LLC	N/A	N/A
5	No	0	38	1483 Bridged Only	LLC	N/A	N/A
6	No	0	39	1483 Bridged Only	LLC	N/A	N/A
7	No	0	40	1483 Bridged Only	LLC	N/A	N/A

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

Group Index	Group Port
0	PVC0,LAN1, LAN2, WLAN1
1	PVC2, LAN3, LAN4

Configuration

Interface Grouping

Interface Grouping

☒ Activated
☐ Deactivated

Group Index

0 ▾

ATM PVCs(Virtual Circuit)

☒ 0
☐ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7

Ethernet LAN

☒ LAN1
☒ LAN2
☐ LAN3
☐ LAN4

Wireless LAN

☒ WLAN1

Group Summary

Group Summary

Save

Delete

Configuration

Interface Grouping

Interface Grouping

☒ Activated
☐ Deactivated

Group Index

1 ▾

ATM PVCs(Virtual Circuit)

☐ 0
☒ 1
☐ 2
☐ 3
☐ 4
☐ 5
☐ 6
☐ 7

Ethernet LAN

☐ LAN1
☐ LAN2
☒ LAN3
☒ LAN4

Wireless LAN

☐ WLAN1

Group Summary

Group Summary

Save

Delete

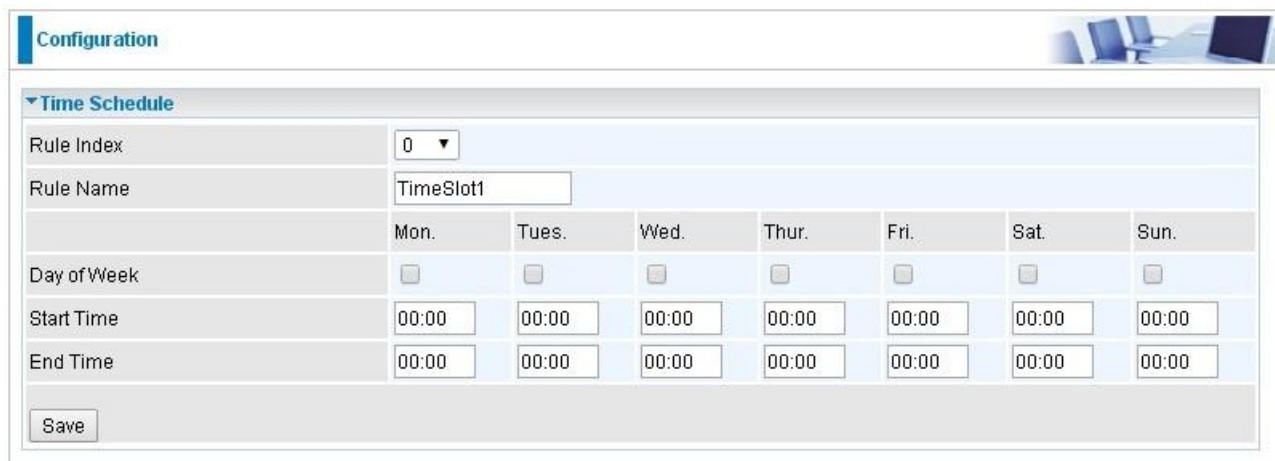
Click **Group Summary** to show the configuration results.

Group ID	Group port
0	p0,e1,e2,w1
1	p1,e3,e4

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

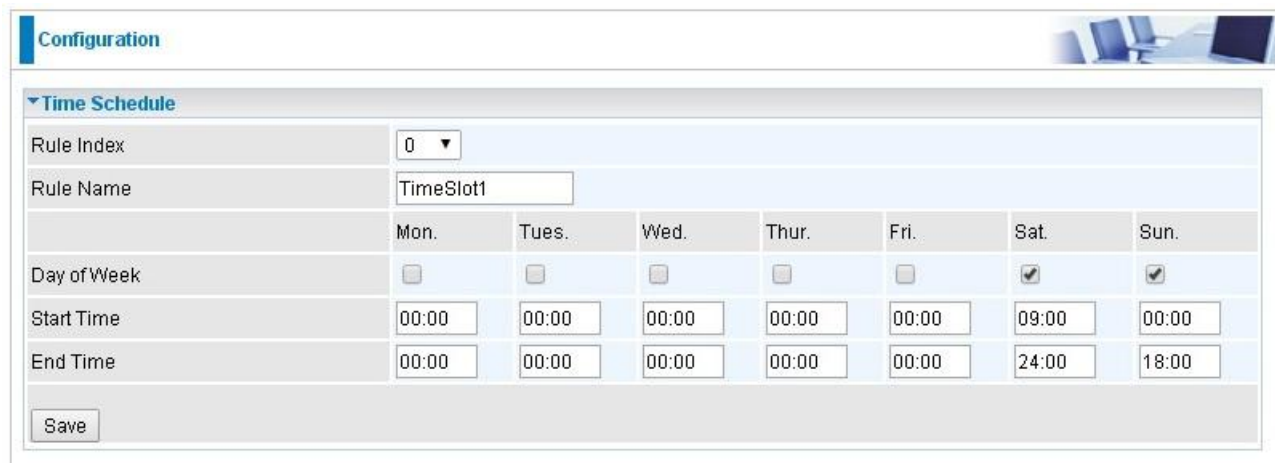
Rule Index	0 ▼						
Rule Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
<input type="button" value="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 Saturday to 18:00 of Sunday.



Configuration

Time Schedule

Rule Index	0 ▼						
Rule 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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	00:00	09:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	24:00	18:00
<input type="button" value="Save"/>							

4.4.2.9 Remote System Log

Remote System Log is designed to keep remote administrators informed of the system-operating information. Administrator can set up a remote system log server for receiving and monitoring the system information by enabling remote system log feature on the router.



The screenshot shows a web interface for configuring the Remote System Log. At the top, there is a 'Configuration' tab. Below it, the 'Remote System Log' section is expanded. It contains three fields: 'Remote System Log' with radio buttons for 'Activated' and 'Deactivated' (where 'Deactivated' is selected), 'Server IP Address' with a text box containing '0.0.0.0', and 'Server UDP Port' with a text box containing '514'. A 'Save' button is located at the bottom left of the configuration area.

Remote System Log	
Remote System Log	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Server IP Address	0.0.0.0
Server UDP Port	514
<input type="button" value="Save"/>	

Remote System Log: Select whether to activate “Remote System Log”.

Server IP Address: Enter the remote syslog server IP address.

Server UDP Port: Enter the UDP port of the remote syslog server.

4.4.3 Access Management

Wireless-N ADSL2+ Firewall Router

► Status

► Quick Start

▼ Configuration

► Interface Setup

► Advanced Setup

▼ Access Management

► Device Management

► SNMP

► Universal Plug & Play

► Dynamic DNS

► Access Control

► Packet Filter

► CWMP (TR-069)

► Parental Control

► Maintenance

► Language

Configuration

▼ Device Management

Embedded Web Server

HTTP Port80(The default HTTP port number is 80.)

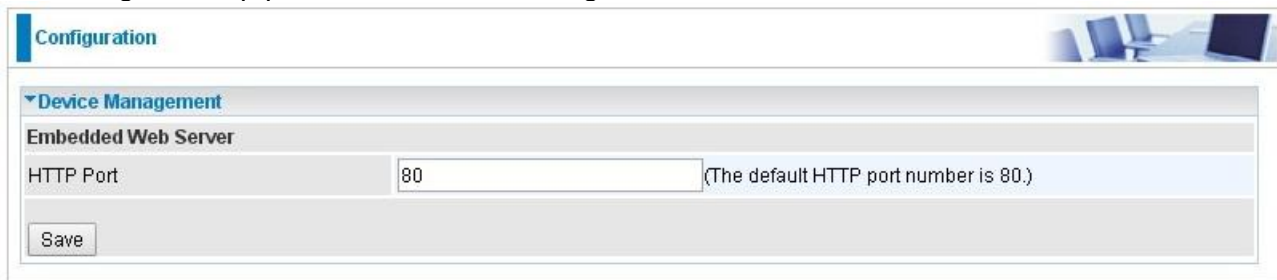
Save

Restart

Logout

4.4.3.1 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.

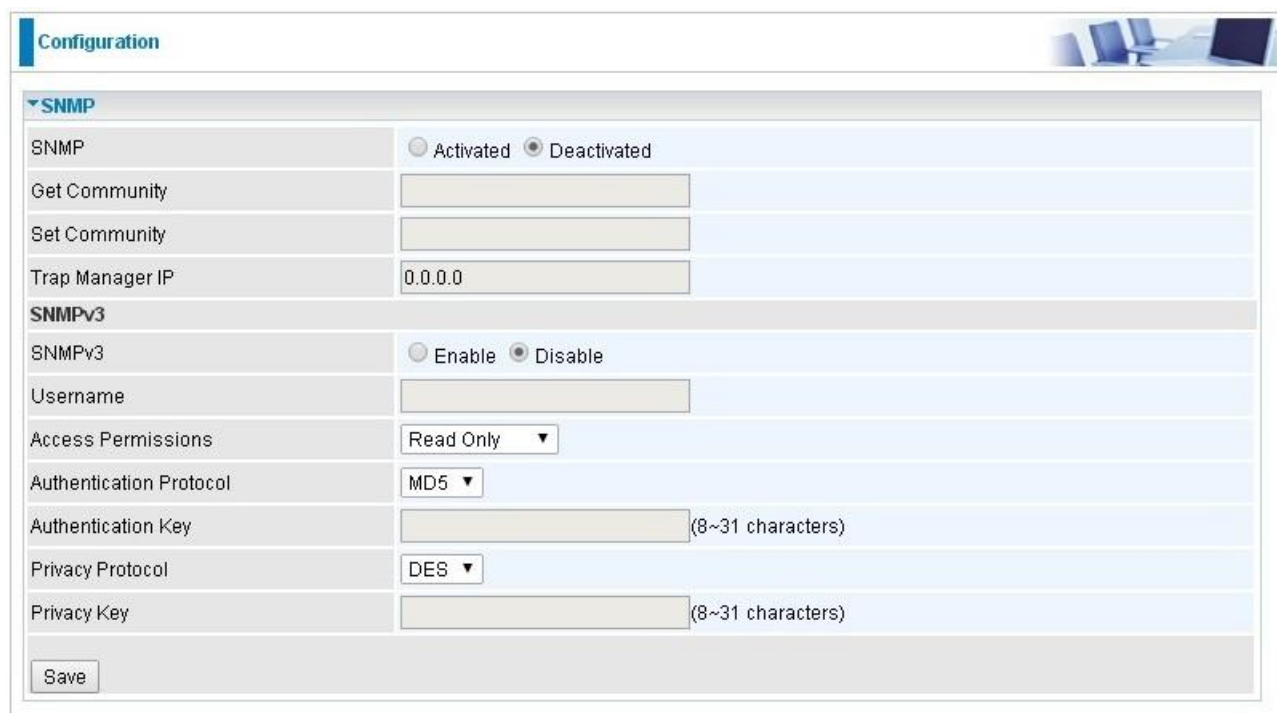


The screenshot shows a web interface for configuration. At the top, there is a 'Configuration' tab. Below it, the 'Device Management' section is expanded, showing the 'Embedded Web Server' settings. The 'HTTP Port' is currently set to '80', and a note indicates that the default HTTP port number is 80. A 'Save' button is located at the bottom of the settings area.

Embedded Web Server	
HTTP Port	80 (The default HTTP port number is 80.)
<input type="button" value="Save"/>	

4.4.3.2 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. Router serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'SNMP' section is expanded, showing options to activate or deactivate the feature. The 'Get Community' and 'Set Community' fields are empty. The 'Trap Manager IP' is set to '0.0.0.0'. The 'SNMPv3' section is also expanded, showing options to enable or disable it. The 'Username' field is empty. The 'Access Permissions' dropdown is set to 'Read Only'. The 'Authentication Protocol' dropdown is set to 'MD5'. The 'Authentication Key' field is empty, with a note '(8~31 characters)'. The 'Privacy Protocol' dropdown is set to 'DES'. The 'Privacy Key' field is empty, with a note '(8~31 characters)'. A 'Save' button is located at the bottom left of the configuration area.

Configuration	
▼ SNMP	
SNMP	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated
Get Community	<input type="text"/>
Set Community	<input type="text"/>
Trap Manager IP	<input type="text" value="0.0.0.0"/>
SNMPv3	
SNMPv3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username	<input type="text"/>
Access Permissions	<input type="text" value="Read Only"/>
Authentication Protocol	<input type="text" value="MD5"/>
Authentication Key	<input type="text"/> (8~31 characters)
Privacy Protocol	<input type="text" value="DES"/>
Privacy Key	<input type="text"/> (8~31 characters)
<input type="button" value="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.

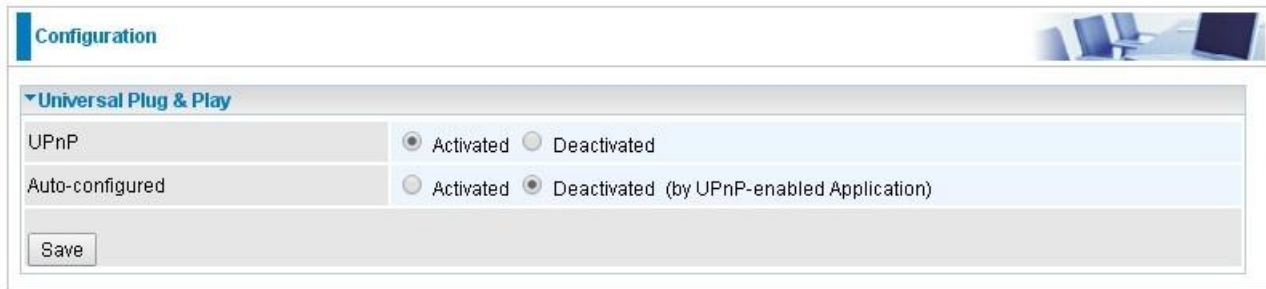
Authentication Key: Set the authentication key, 8-31 characters.

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

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

4.4.3.3 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.



The screenshot shows a web-based configuration interface for a router. At the top, there is a 'Configuration' tab. Below it, the 'Universal Plug & Play' section is expanded. This section contains two rows of settings. The first row is 'UPnP', which has a radio button selected for 'Activated' and a radio button for 'Deactivated'. The second row is 'Auto-configured', which has a radio button for 'Activated' and a radio button selected for 'Deactivated (by UPnP-enabled Application)'. At the bottom of the configuration area, there is a 'Save' button.

Universal Plug & Play	
UPnP	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Auto-configured	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)

Save

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 Router IP address

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

4.4.3.4 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. At the top, there is a 'Configuration' tab. Below it, the 'Dynamic DNS' section is expanded. 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="password"/>
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼

At the bottom of the form 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 Router 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: myhome.dyndns.org using username/password myhome-123/myhome-456

Configuration

Dynamic DNS

Dynamic DNS

☒ Activated ☐ Deactivated

Service Provider

www.dyndns.org (dynamic) ▼

My Host Name

myhome.dyndns.org

Username

myhome-123

Password

Wildcard support

☐ Yes ☒ No

Period

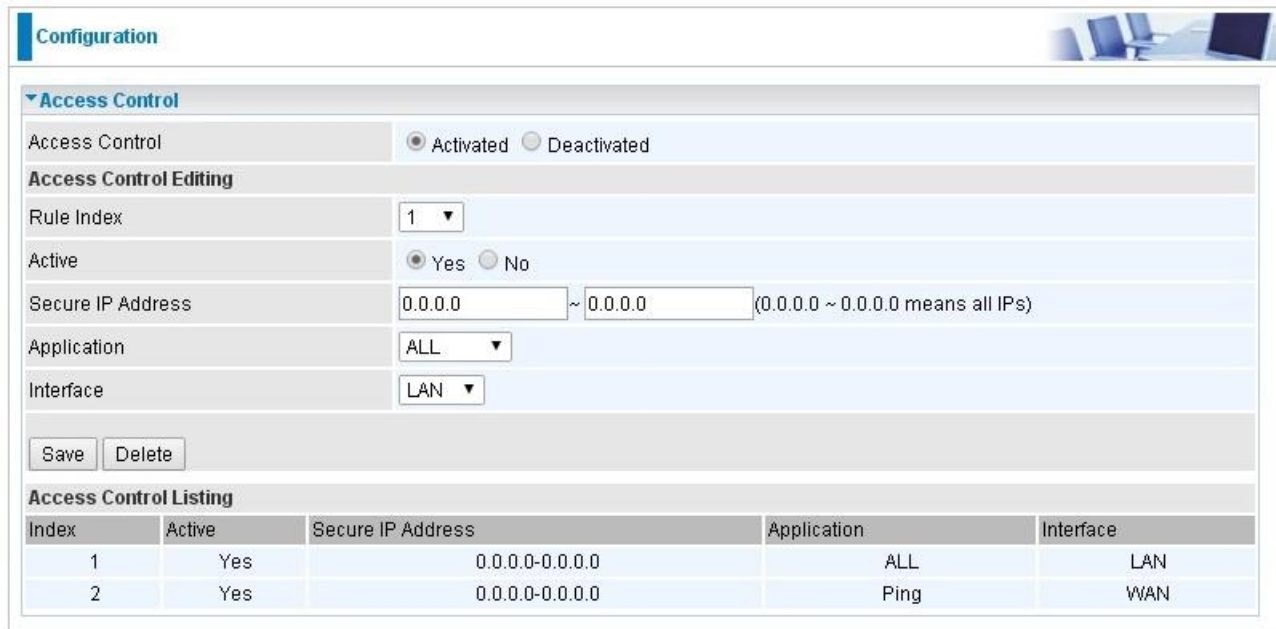
25 Day(s) ▼

Save

4.4.3.5 Access Control

Access Control Listing allows you to determine which services/protocols can access Router 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 Router. 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

4.4.3.6 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: PVC0

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



Configuration

▼ Packet Filter

Packet Filter

Filter Type: Application Filter ▼

Application Filter Editing

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

Save

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
-------	--------	-----

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.

4.4.3.7 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.

The screenshot shows a web-based configuration interface for CWMP (TR-069). The interface is titled "Configuration" and has a sub-section "CWMP (TR-069)".

- CWMP**: A radio button group with "Activated" and "Deactivated" options. "Deactivated" is selected.
- ACS Login Information**: A section with three input fields: "URL", "Username", and "Password".
- Connection Request Information**: A section with three input fields: "Path" (containing "/tr069"), "Username", and "Password".
- Periodic Inform Config**: A section with two radio buttons for "Periodic Inform" (selected "Activated") and "Deactivated", and an "Interval" input field (containing "5000").
- Save**: A button at the bottom left.

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.

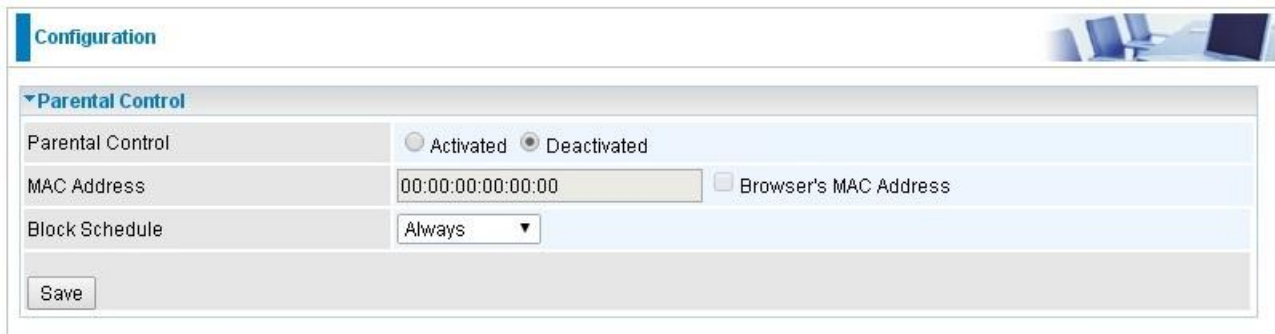
Periodic Inform Config

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.

4.4.3.8 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.



The screenshot shows a web interface for configuring Parental Control. At the top, there is a 'Configuration' tab and a small image of a desk with a laptop. Below this is a section titled 'Parental Control' with a dropdown arrow. Inside this section, there are three rows of configuration options: 1. 'Parental Control' with two radio buttons: 'Activated' (unselected) and 'Deactivated' (selected). 2. 'MAC Address' with a text input field containing '00:00:00:00:00:00' and a checkbox labeled 'Browser's MAC Address' which is unchecked. 3. 'Block Schedule' with a dropdown menu currently showing 'Always'. At the bottom of the configuration area is a 'Save' button.

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

4.4.4 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.

Wireless-N ADSL2+ Firewall Router

► Status

► Quick Start

► Configuration

► Interface Setup

► Advanced Setup

► Access Management

▼ Maintenance

◦ User Management

◦ Time Zone

◦ Firmware & Configuration

◦ System Restart

◦ Diagnostic Tool

► Language

Configuration

▼ User Management

User Account

Index

1 ▼

Username

admin

New Password

Confirm Password

Save

Delete

User Account List

#	User Name
1	admin
2	user

Restart

Logout

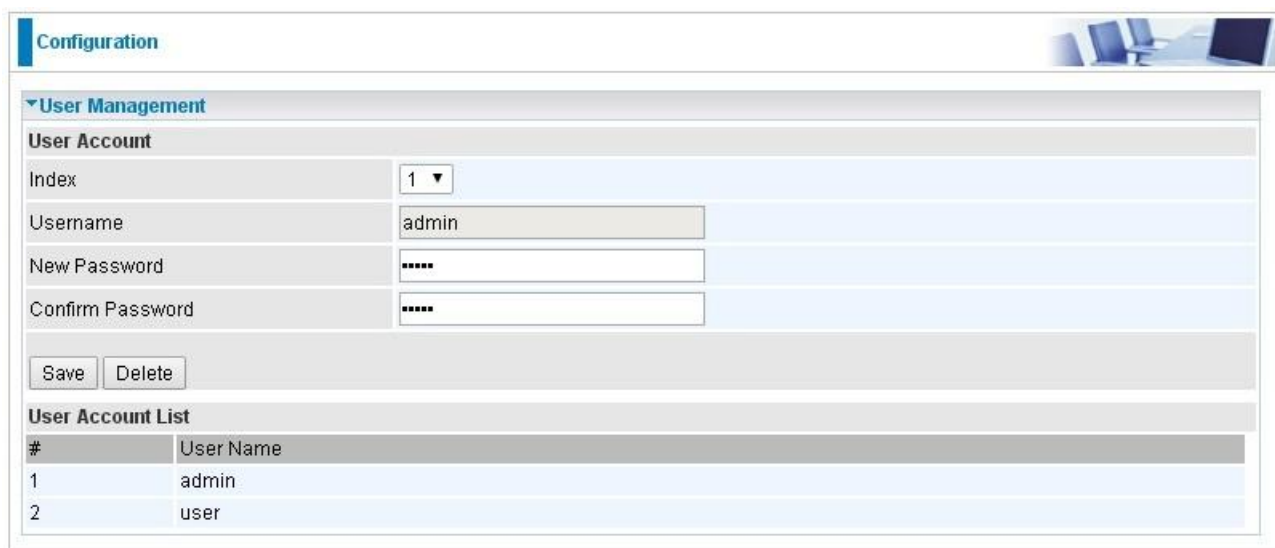
4.4.4.1 User Management

User Management controls the Router Web GUI permission to the specific account.

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

① “admin/admin”

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



The screenshot displays the 'Configuration' page of a router's web interface, specifically the 'User Management' section. It features a 'User Account' configuration form and a 'User Account List' table.

User Account Configuration Form:

- Index:** A dropdown menu showing '1'.
- Username:** A text field containing 'admin'.
- New Password:** A text field with masked characters (dots).
- Confirm Password:** A text field with masked characters (dots).
- Buttons:** 'Save' and 'Delete' buttons.

User Account List Table:

#	User Name
1	admin
2	user

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to router webpage.

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.

Web GUI Permission

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

Wireless-N ADSL2+ Firewall Router

- Status
- Quick Start
- Configuration
 - ▼ Interface Setup
 - Internet
 - LAN
 - Wireless
 - Wireless MAC Filter
 - Advanced Setup
 - Access Management
 - Maintenance
- Language

Configuration

Internet

WAN Interface	ADSL ▼	
ATM PVC		
Virtual Circuit	PVC 0 ▼	PVCs Summary
Status	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated	
VPI	8	(range: 0~255)
VCI	35	(range: 32~65535)
QoS		
ATM QoS	ubr ▼	
PCR	0	cells/second
SCR	0	cells/second
MBS	0	cells
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/PPPoA <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/PPPoA		

 Restart

 Logout

① other additional users including “user/user”

For example, adding an account called “user/user”, setting authorized feature access to the account

Configuration

User Management

User Account

Index: 2 ▼

Username: user

New Password: ****

Confirm Password: ****

Web GUI Permission

Guest Account: ☐ Enable ☒ Disable

Interface Setup: ☒ Enable ☐ Disable

Advanced Setup: ☒ Enable ☐ Disable

Access Management: ☐ Enable ☒ Disable

Maintenance: ☐ Enable ☒ Disable

Save Delete

User Account List

#	User Name
1	admin
2	user

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to router webpage.

New Password: Type the password for the user account.

Confirmed Password: Type password again for confirmation.

Web GUI Permission

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

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

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

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

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

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

Wireless-N ADSL2+ Firewall Router

► Status

► Quick Start

▼ Configuration

► Interface Setup

► Advanced Setup

► Language

Status

▼ Device Information

Model Name	Wireless-N ADSL2+ Firewall Router
Firmware Version	1.02b.rc7.dt4
MAC Address	00:04:ED:01:23:45
Date-Time	Fri Mar 20 09:40:57 UTC 2015
System Up Time	1 hour 33 mins

▼ Physical Port Status

ADSL	✓
Ethernet	✓
Wireless	✓

▼ WAN

Interface	Protocol	VPI/VCI	Connection	IP Address	Default Gateway
PVC0 ▼	PPPoE	0/33	Connected	59.105.31.225/255.255.255.255	59.105.31.1

▼ LAN

IP Address	Subnet Mask/Prefix Length	DHCP Server
192.168.1.254	255.255.255.0	Enable / 192.168.1.100~192.168.1.119 Enable / Stateless

▼ Wireless

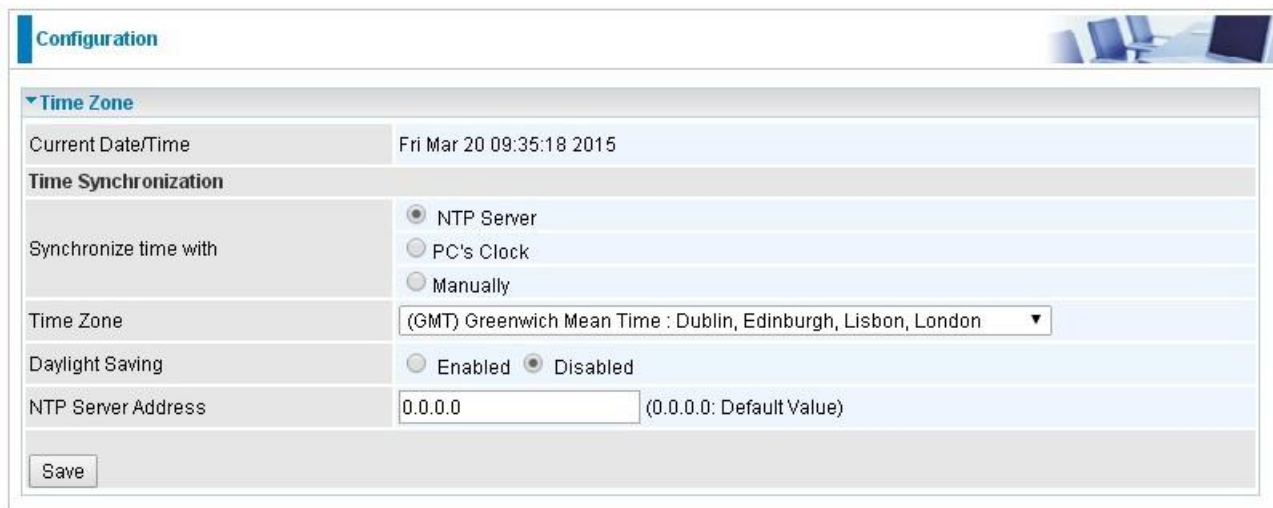
Mode	SSID	Channel	Security
802.11b+g+n	wlan-ap	6	OPEN

Restart

Logout

4.4.4.2 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.



Configuration

Time Zone

Current Date/Time: Fri Mar 20 09:35:18 2015

Time Synchronization

Synchronize time with:

- ☒ NTP Server
- ☐ PC's Clock
- ☐ Manually

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

Daylight Saving: ☐ Enabled ☒ Disabled

NTP Server Address: 0.0.0.0 (0.0.0.0: Default Value)

Save

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).

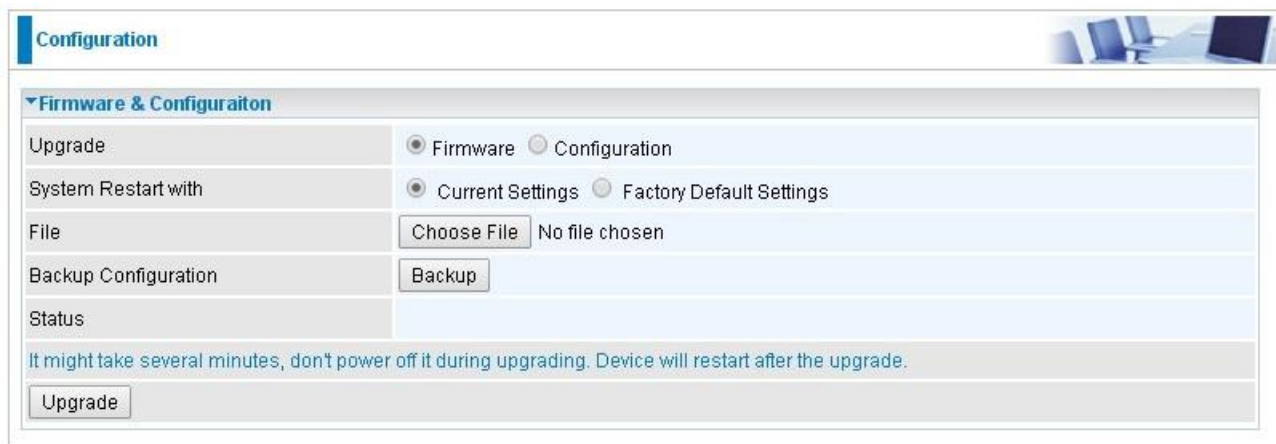
Daylight Saving: Select this option if you use daylight savings time.

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

4.4.4.3 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 Router, 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, Router will reset automatically to make the new firmware work.



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.



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

Configuration

Firmware Upgrade

File upload succeeded, starting flash erasing and programming!!

Progress

Percent

16

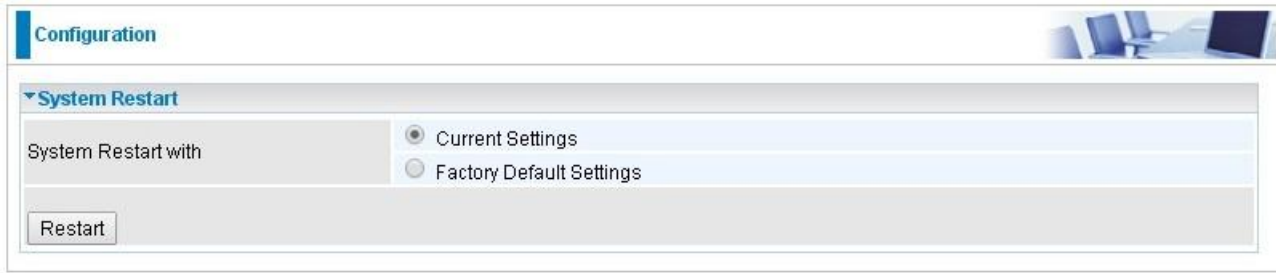
%



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

4.4.4.4 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' tab. Below it, the 'System Restart' section is expanded. It contains a label 'System Restart with' followed by two radio button options: 'Current Settings' (which is selected) and 'Factory Default Settings'. At the bottom of this section is a 'Restart' button. The interface has a light blue header and a white background.

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.

4.4.4.5 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.

Configuration

▼Diagnostic Tool

WAN Interface	PVC0 ▼
Testing Ethernet LAN Connection	N/A
Testing xDSL Synchronization	N/A
Testing ATM OAM Segment Ping	N/A
Testing ATM OAM End to End Ping	N/A
Ping Primary DNS (139.175.1.1)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

Start

Click Start to begin to diagnose the connection.

Configuration

▼Diagnostic Tool

WAN Interface	PVC0 ▼
Testing Ethernet LAN Connection	PASS
Testing xDSL Synchronization	PASS
Testing ATM OAM Segment Ping	Fail
Testing ATM OAM End to End Ping	Fail
Ping Primary DNS (139.175.1.1)	PASS
Ping www.google.com	PASS
Ping other IP Address <input checked="" type="radio"/> Yes <input type="radio"/> No	PASS
IP Address	8.8.8.8

Start

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 "CaIVxePV1!". 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.

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.

MAC OS is a registered Trademark of Apple Inc.

Windows 7/8, Windows Vista, Windows XP are registered Trademarks of Microsoft Corporation.