750AC WIRELESS DUAL-BAND ROUTER
USER MANUAL
MODEL 525541

manhattan®
Life just got easier.™

manhattan-products.com

MAN-525541-UM-0314-01-0

COPYRIGHT

Federal Communications Commission Interference Statement

FCC Part 15

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference; and (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

- Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the equipment.
- Operations in the 5.15-5.25 GHz band are restricted to indoor usage only.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions, and a minimum 20cm spacing must be provided between and computer-mounted antenna and a person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The equipment version marketed in the U.S. is restricted to usage of the channels 1-11.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC OF the European Parliament and the Council of March 9, 1999, on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

Contents

Chapter I: Product Information

1-1 Introduction and safety information

Thank you for purchasing this 750AC Wireless Dual-Band Router. This cost-effective router is the best choice for ***Small office / Home office*** users, as all computers and network devices can share a single xDSL / cable modem Internet connection at high speed. Easy install procedures allow any computer users to set up a network environment in very short time — even if inexperienced. When the number of your computers and network-enabled devices grows, you can also expand the number of network slots by simply attaching a switch to extend the scope of your network.

With both 2.4GHz and 5GHz radios built-in, this router supports both of the IEEE 802.11b/g/n and 802.11a/n/ac wireless network capabilities simultaneously. All computers and wireless-enabled network devices (including PDAs, smartphones, game consoles and tablets) can connect to this wireless router without additional cabling. New 11ac wireless capability also gives you the highest speed of wireless experience ever! With a compatible wireless card installed in your PC, you can transfer files at speeds up to 300 Mbps + 433 Mbps (transfer data rate). The radio coverage is also doubled, so don’t worry if your office or house is really big!

Other features:

- Supports 2.4GHz and 5GHz wireless devices simultaneously
- High wireless access throughput, up to 300 Mbps + 433 Mbps (transfer data rate)
- Allows multiple users to share a single Internet line
- Shares a single Cable or xDSL internet connection
- Access to private LAN servers from the Internet
- Four wired LAN ports (10/100M) and one WAN port (10/100M)
- Provides IEEE 802.11a/b/g/n/ac wireless LAN capability
- Supports DHCP (Server/Client) for easy IP-address setup

- Supports multiple wireless modes: AP, Station-Infrastructure, Wireless Bridge and Universal Repeater
- Advanced network and security features: Special Applications, QoS, DMZ, Virtual Servers, Access Control, Firewall
- Allows you to monitor the router's status: DHCP Client Log, System Log, Security Log and Device/Connection Status
- Easy-to-use Web-based GUI for network configuration and management purposes
- Remote management function allows configuration and upgrades from a remote computer (over the Internet)
- Auto MDI / MDI-X function for all wired Ethernet ports

1-2 Safety Information

1. The router's designed for indoor use only; *do not* place outdoors.
2. *Do not* put this router at or near hot or humid places, like a kitchen or bathroom. Also, do not leave this router in the car in summer.
3. *Do not* yank any cables; disconnect from the router first.
4. If placing the router up high or on a wall, make sure it's firmly secured to avoid damage to the router and its accessories.
5. Accessories like the antenna and power supply are dangers to small children. KEEP THIS ROUTER OUT THE REACH OF CHILDREN!
6. The router will become hot when being used for long time. This is normal and is not a malfunction. *Do not* put this router on paper, cloth or other flammable materials.
7. There're no user-serviceable parts inside the router. If the router is not working properly, contact your dealer and ask for help. *Do not* disassemble the router, as the warranty will be void.
8. If the router falls into water when it's powered, *do not* use your hands to pick it up. Switch the electrical power off before you do anything, or contact an experienced technician for help.
9. If you smell something strange, or even see some smoke coming out from the router or power supply, remove the power supply or switch the electrical power off immediately and call dealer for help.

1-3 System Requirements

- Internet connection, provided by xDSL or cable modem with an RJ45 Ethernet port.
- Computer or network devices with wired or wireless network interface card.
- Web browser (*Microsoft Internet Explorer, Google Chrome or Safari).*
- An available AC power outlet (100 – 240V, 50/60Hz)

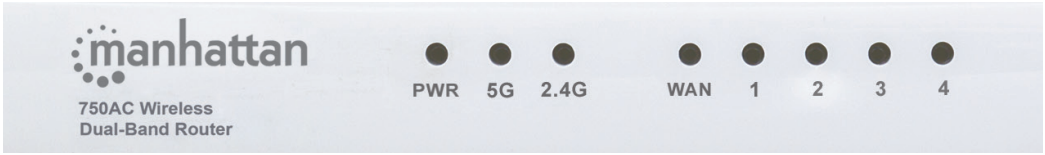
1-4 Package Contents

Before starting to use this router, check if there's anything missing from the package. Contact your dealer to claim any missing items:

□ Broadband Wireless Router
□ Quick Installation Guide
□ User Manual on CD
□ Power Adapter (Output: DC 5 V / 1.5 A)

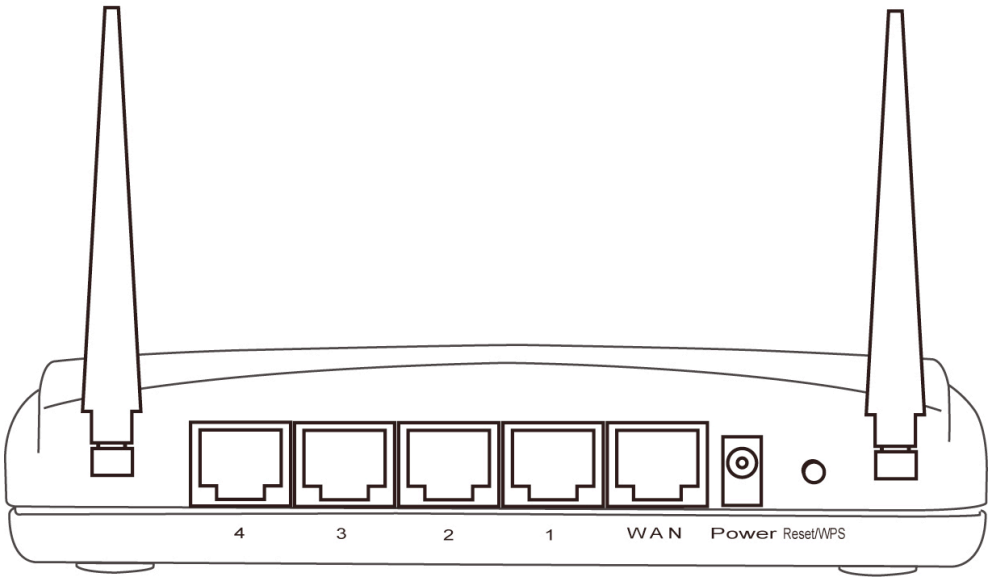
1-5 Becoming familiar with your wireless router

Front Panel



LED Name	Light Status	Description
PWR	On	Router is switched on and correctly powered.
5G	On	5GHz Wireless WPS function is enabled.
	Off	5GHz Wireless network is switched off.
	Flashing	5GHz Wireless LAN activity (transferring or receiving data).
2.4G	On	2.4GHz Wireless WPS function is enabled.
	Off	2.4GHz Wireless network is switched off.
	Flashing	2.4GHz Wireless LAN activity (transferring or receiving data).
WAN LNK/ACT	On	WAN port is connected.
	Off	WAN port is not connected.
	Flashing	WAN activity (transferring or receiving data).
LAN 1-4 LNK/ACT	On	LAN port is connected.
	Off	LAN port is not connected.
	Flashing	LAN activity (transferring or receiving data).

Back Panel



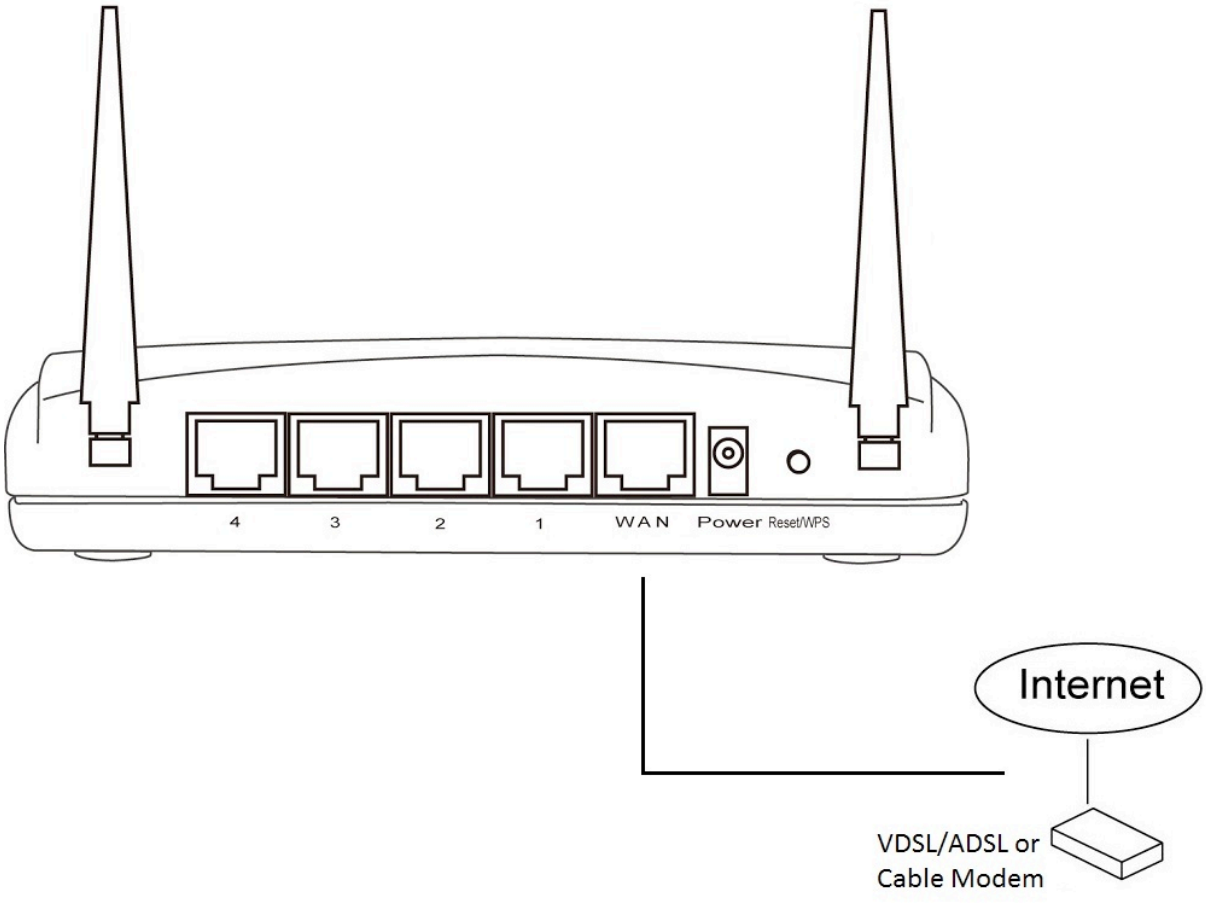
Item Name	Description
Antenna	It is External dipole antenna x 2
LAN 1 – 4	Local Area Network (LAN) ports 1 to 4.
WAN	Wide Area Network (WAN / Internet) port.
Power Jack	Power connector, connects to A/C power adapter.
Reset / WPS	Reset the router to factory default settings (clear all settings) or start WPS function. Press this button and hold for 10 seconds to restore all settings to factory defaults; press this button for less than 5 seconds once to start 2.4GHz & 5GHz wireless WPS function.

Chapter II: System and Network Setup

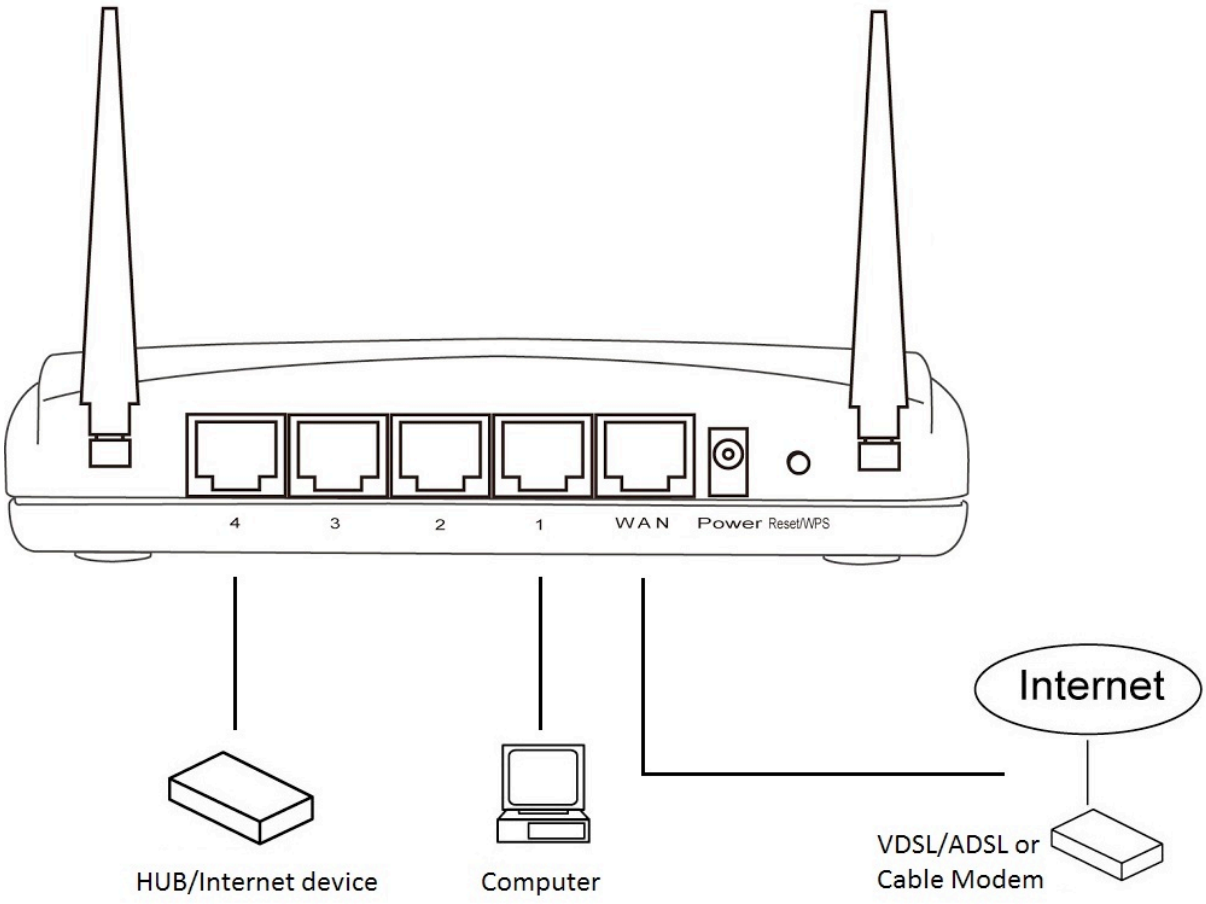
2-1 Building the network connection

To build the network connection between your router and your computers and network devices:

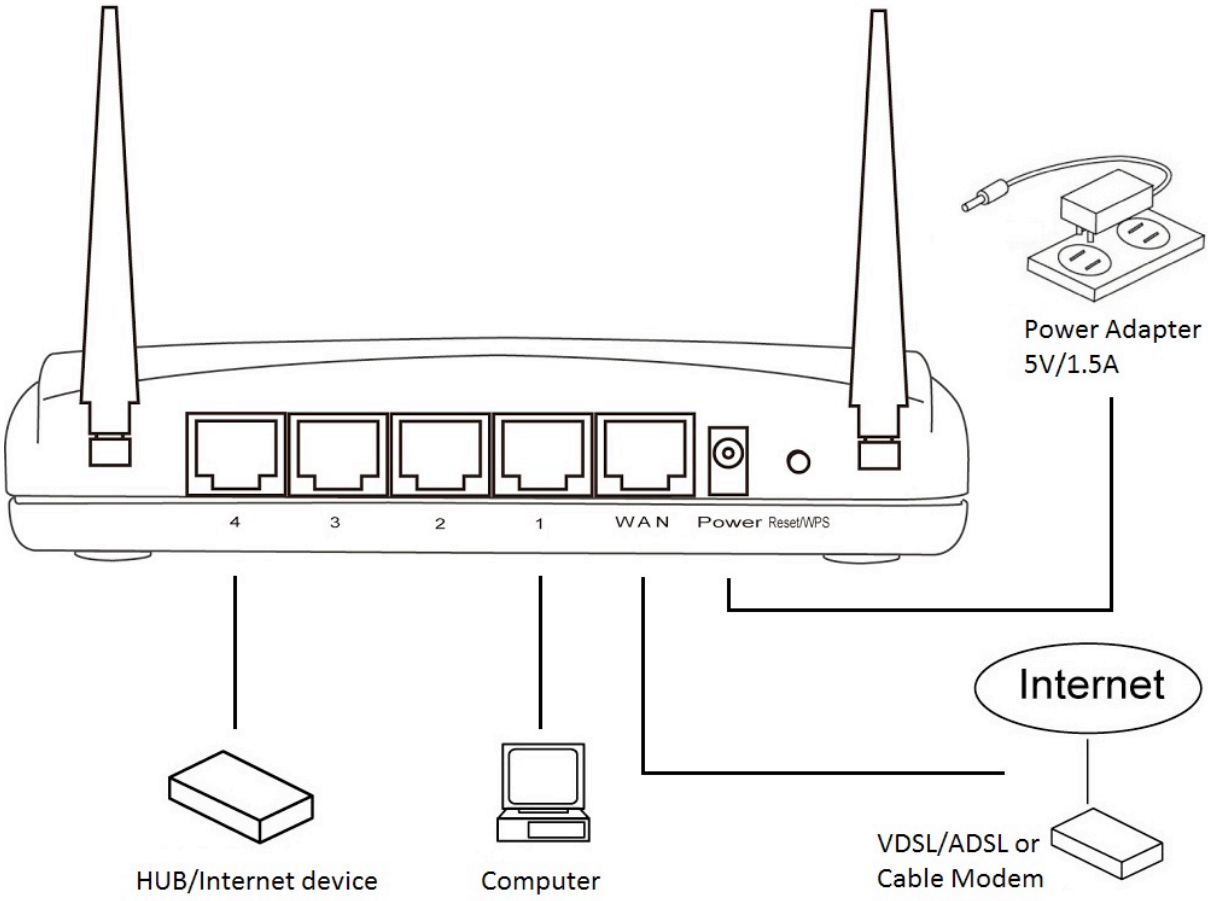
1. Connect your xDSL / cable modem to the WAN port of the router using Ethernet cable.



2. Connect all your computers, network devices (network-enabled consumer devices other than computers, like game consoles or switches) to the LAN port of the router.



3. Connect the power adapter to the wall outlet, then connect it to the power jack of the router.



4. Check all LEDs on the front panel. The PWR LED should be steadily on; the WAN and LAN LEDs should be on if the computer / network device connected to the respective port of the router is powered on and correctly connected. If the PWR LED is not on, or if any LED you expect to be on is not, recheck the connections or refer to 4-2 Troubleshooting for possible reasons and solutions.

2-2 Connecting to the router by Web browser

After the network connection is built, the next step is to set up the router with proper network parameters so it can work properly in your network environment.

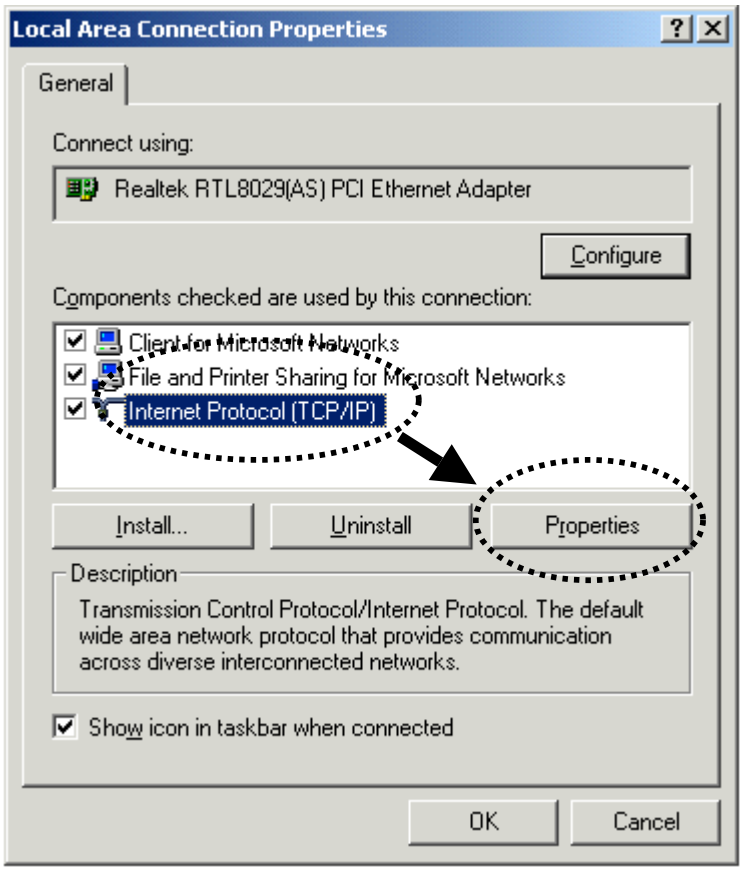
Before you can connect to the router and start the configuration procedures, your computer must be able to get an IP address automatically (use a dynamic IP address). If it's set to use a static IP address, or if you're unsure, configure your computer to use a dynamic IP address using these steps:

If the operating system of your computer is:

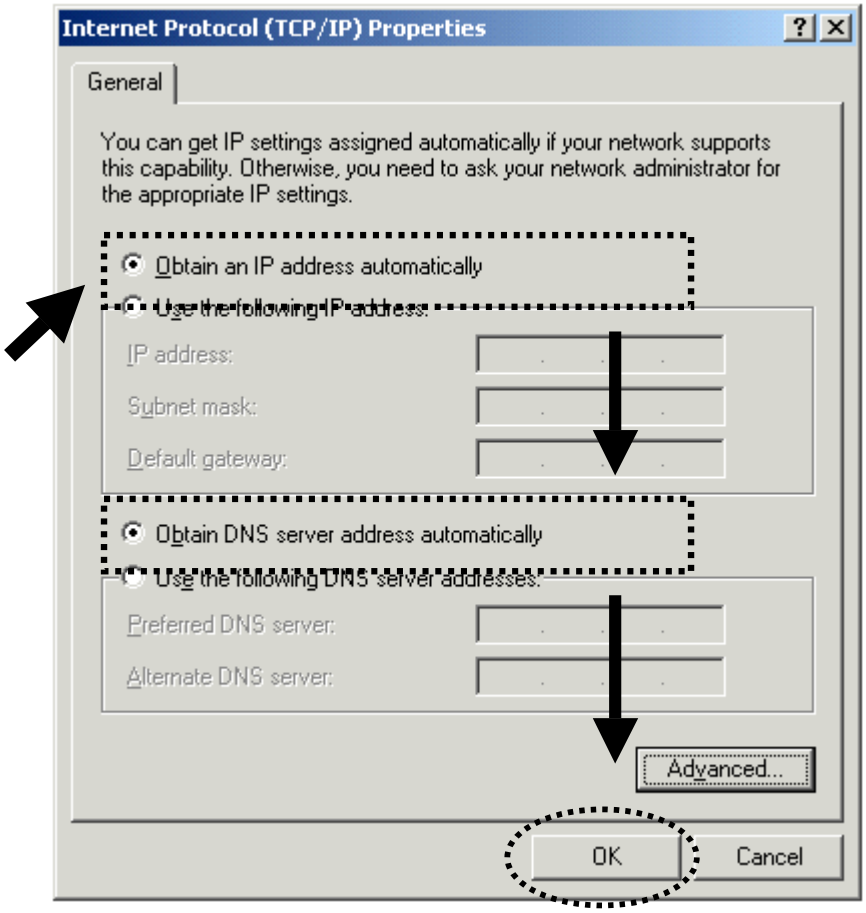
Windows 2000	**- go to section 2-2-1**
Windows XP	**- go to section 2-2-2**
Windows Vista/Windows 7	**- go to section 2-2-3**
Windows 8	**- go to section 2-2-4**

2-2-1 Windows 2000 IP address setup:

1. Click Start (it should be located at the lower-left corner of your desktop), then click Control Panel. Double-click the ***Network and Dial-up Connections*** icon; click ***Local Area Connection.*** The ***Local Area Connection Properties*** window will appear. Select "Internet Protocol (TCP/IP)" and then click Properties.

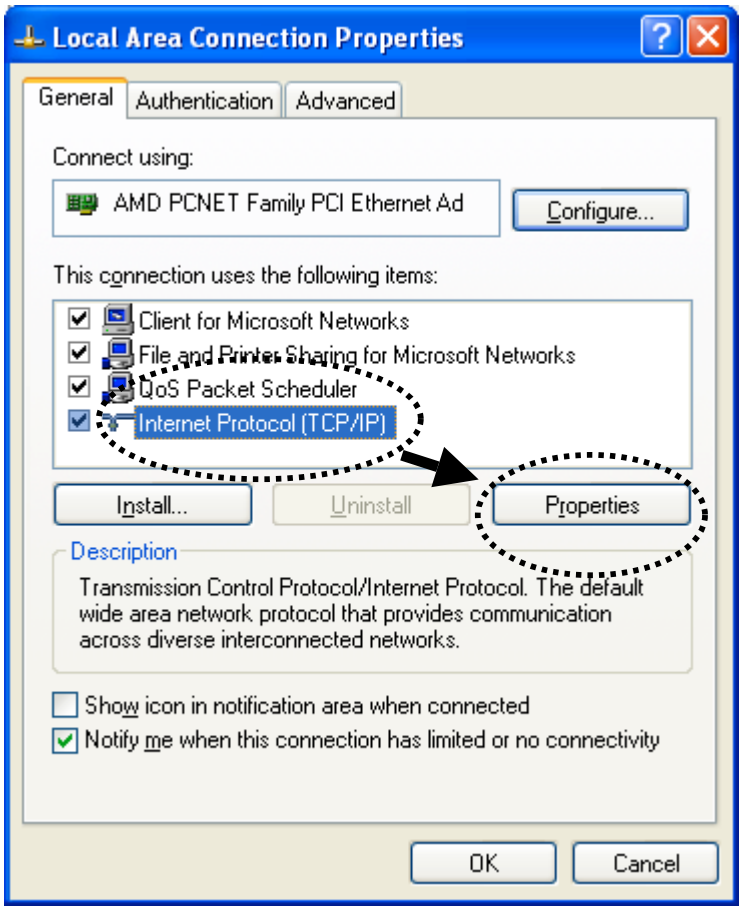


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically,” then click OK.

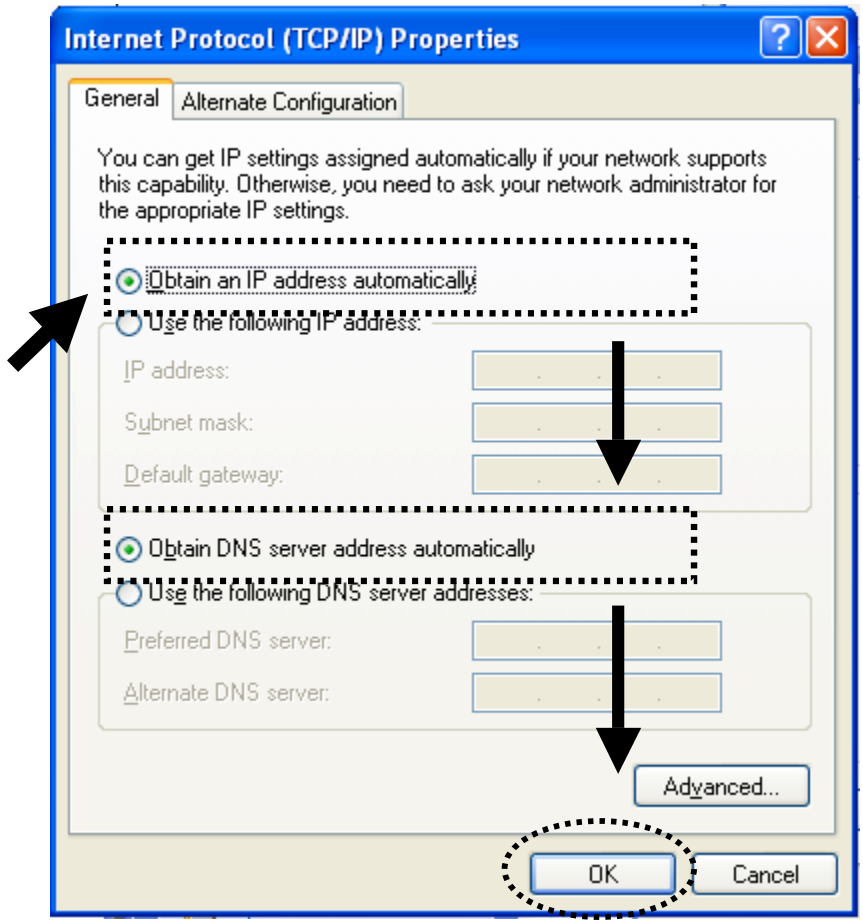


2-2-2 Windows XP IP address setup:

1. Click Start (it should be located at the lower-left corner of your desktop), then click Control Panel. Double-click the ***Network and Internet Connections*** icon, click ***Network Connections,*** and then double-click ***Local Area Connection.*** The ***Local Area Connection Properties*** window will appear. Select “Internet Protocol (TCP/IP)” and then click Properties.

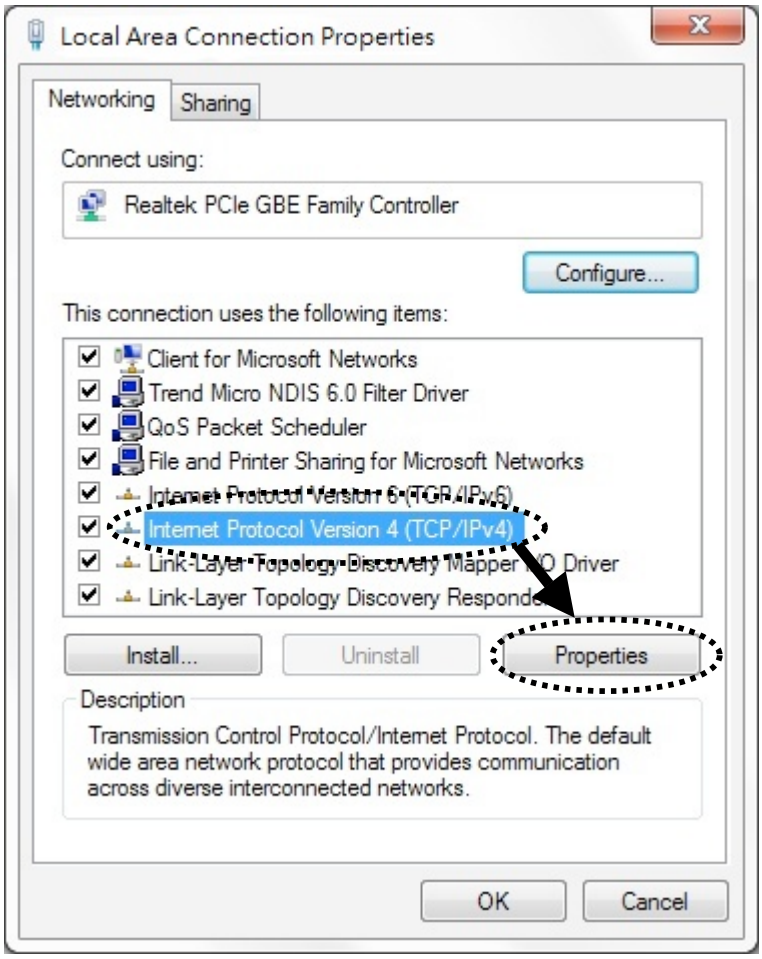


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically,” then click OK.

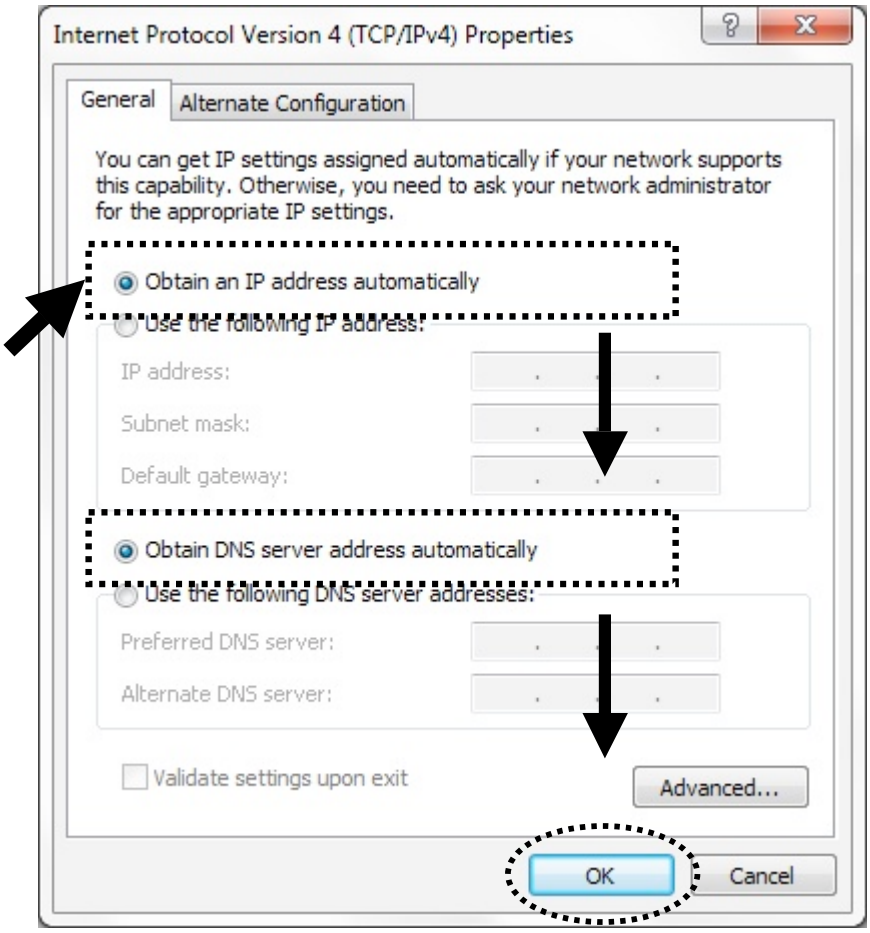


2-2-3 Windows Vista/Windows 7 IP address setup:

1. Click Start (it should be located at the lower-left corner of your desktop), then click control panel. Click ***Network and Sharing Center***, and then click ***Change adapter settings.*** Right-click ***Local Area Connection, then select "Properties."*** The ***Local Area Connection Properties*** window will appear. Select "Internet Protocol Version 4 (TCP / IPv4)," then click Properties.

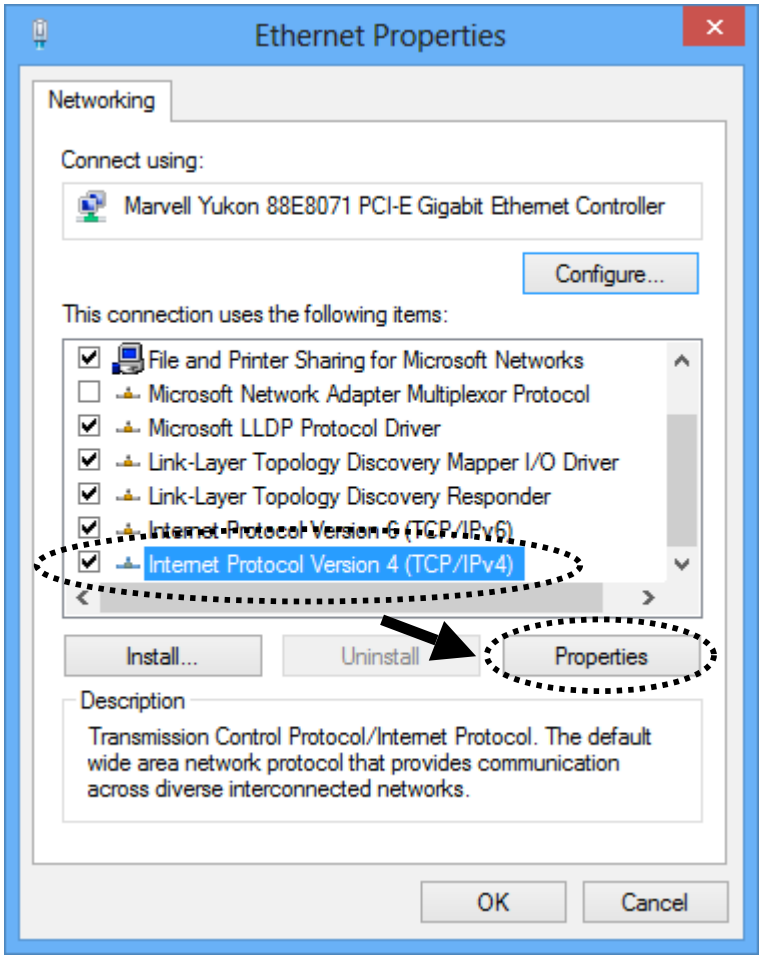


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically,” then click OK.

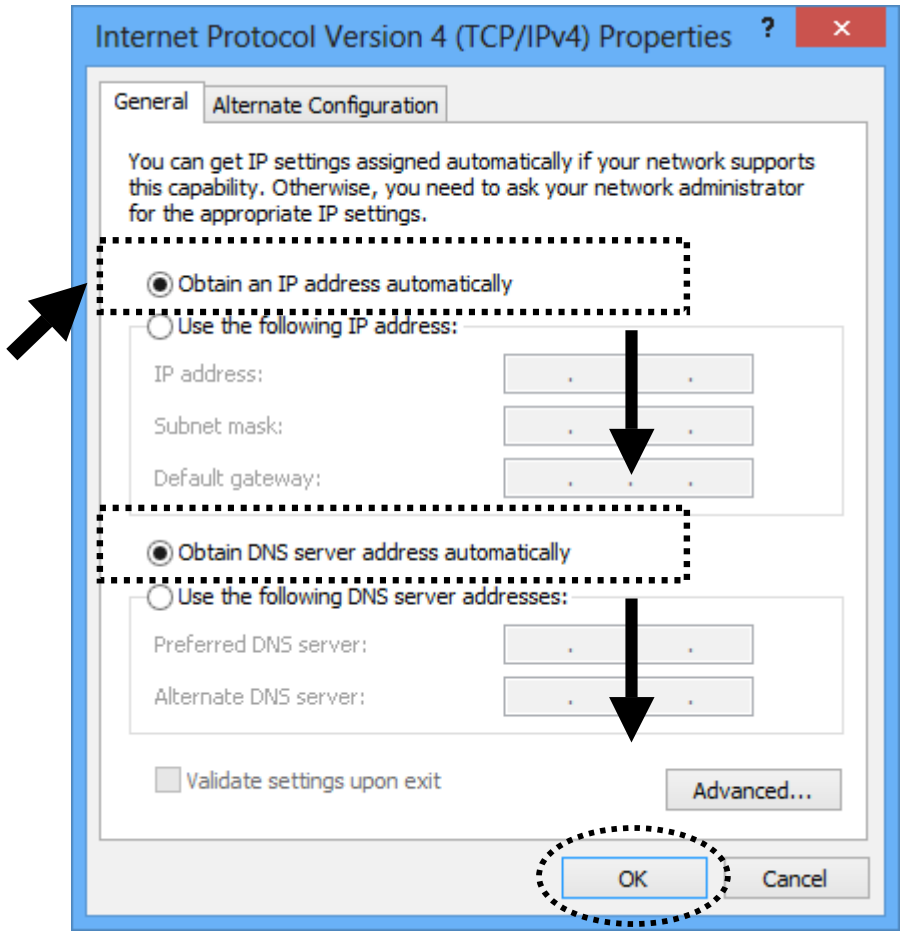


2-2-4 Windows 8 IP address setup:

1. Right-click Start (it should be located at the lower-left corner of your desktop), then click Control Panel. Click ***Network and Sharing Center***, then click ***Change adapter settings.*** Right-click ***Ethernet,*** then select ***"Properties."*** The ***Ethernet Properties*** window will appear. Select "Internet Protocol Version 4 (TCP / IPv4)," then click Properties.

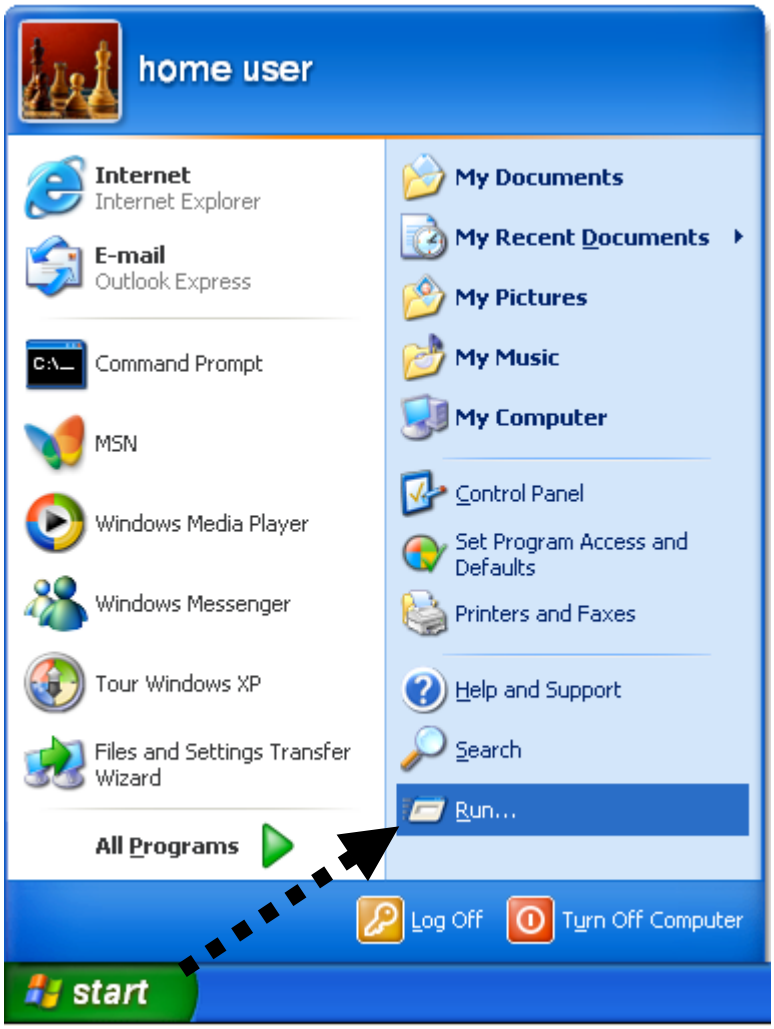


2. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically,” then click OK.

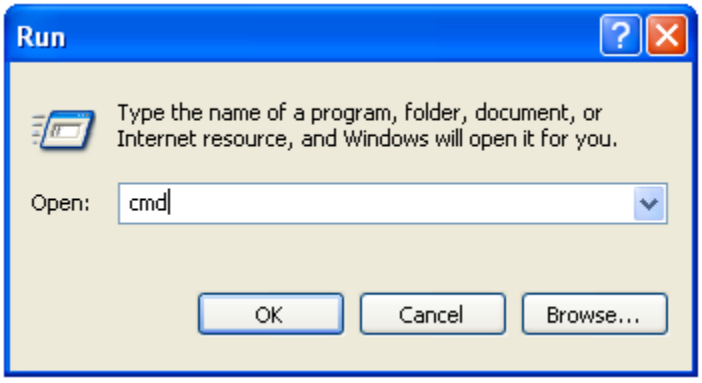


2-2-5 Router IP address lookup

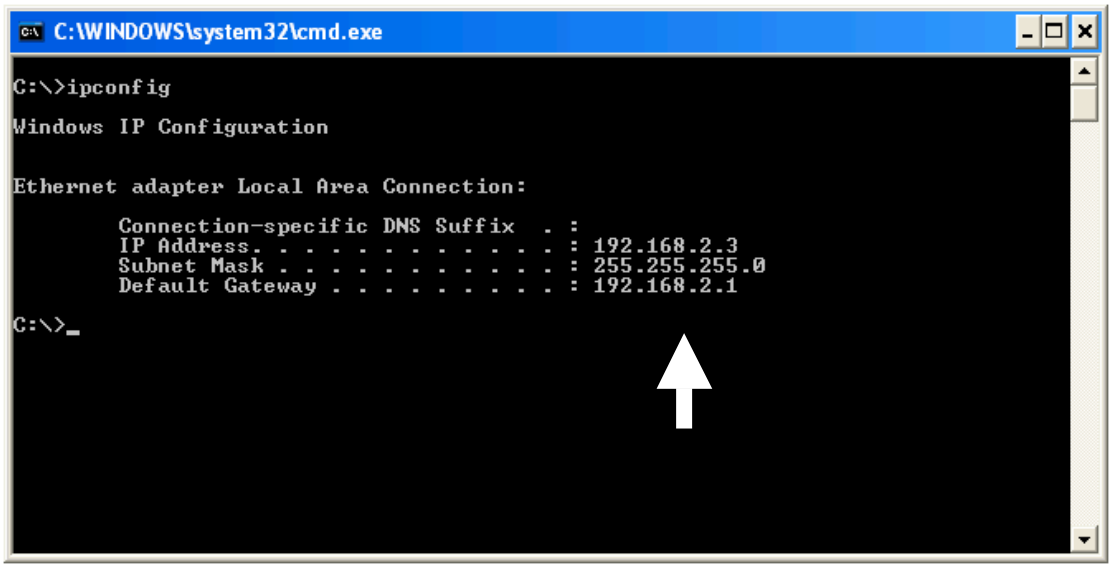
After the IP address setup is complete, click Start, then Run at the bottom-left corner of your desktop:



Input “cmd,” then click OK.



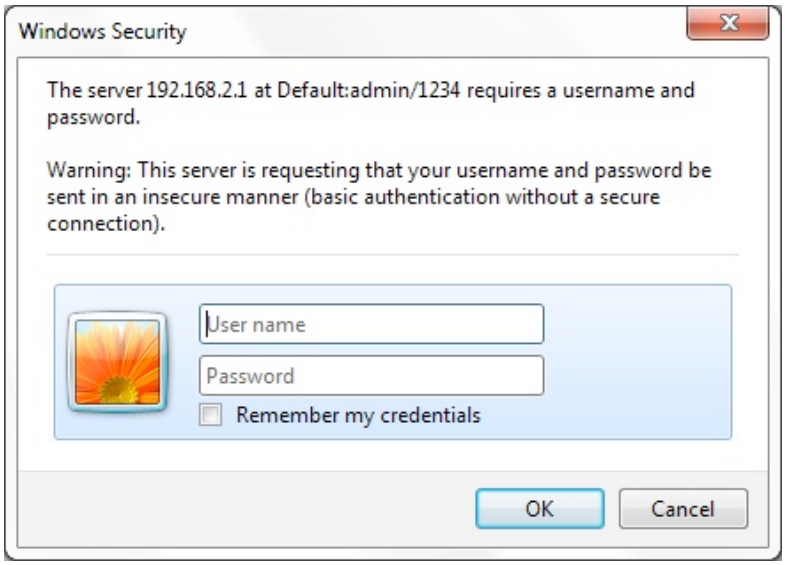
Input “ipconfig,” then press the Enter key. Check the IP address of the Default Gateway: In the example below, the address of the router is 192.168.2.1, but this value may be different.



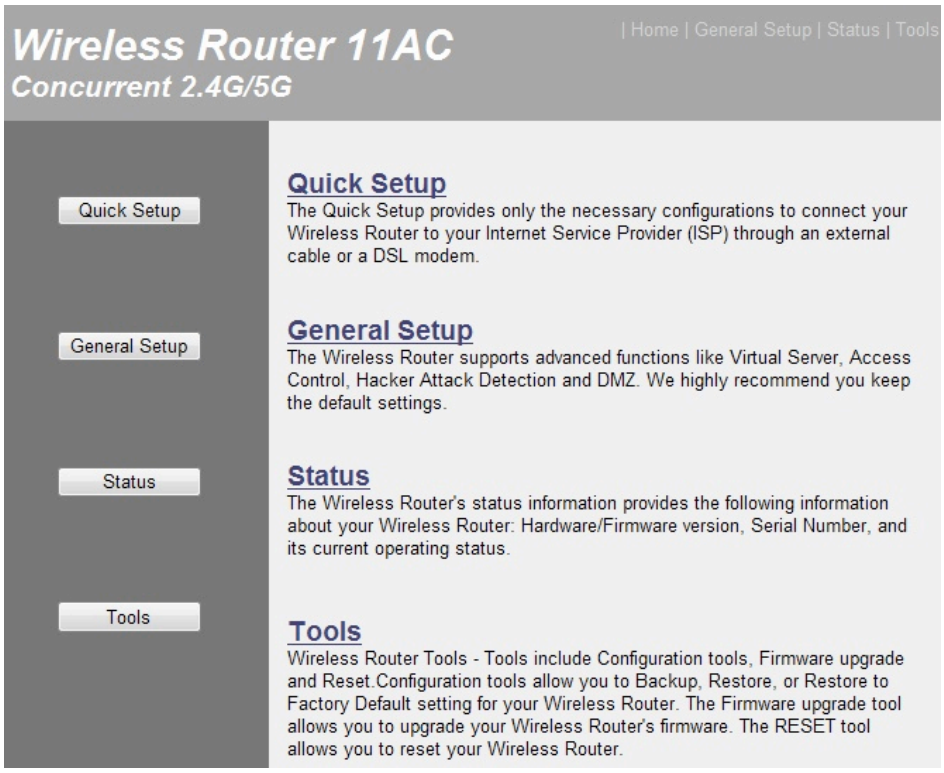
NOTE: If the IP address of the gateway is not displayed, or the address following IP Address begins with "169," recheck the network connection between your computer and router, and/or go to the beginning of this chapter to recheck every step of the network setup procedure.

3. Connect the router's management interface via a Web browser.

After your computer obtained an IP address from the router, open your Web browser and input the IP address of the router in the address bar. The following message should be shown:



Input a user name and password as shown. The default user name is **"admin"**; the default password is **"1234."** Click OK, and you should see the Web management interface of this router:



NOTE: If you can't see the Web management interface and you're being prompted to input the user name and password again, it means you didn't input the username and password correctly. Re-enter them. If you confirm that the user name and password are correct, go to section 4-2 Troubleshooting'to perform a factory reset and set the password back to the default value.

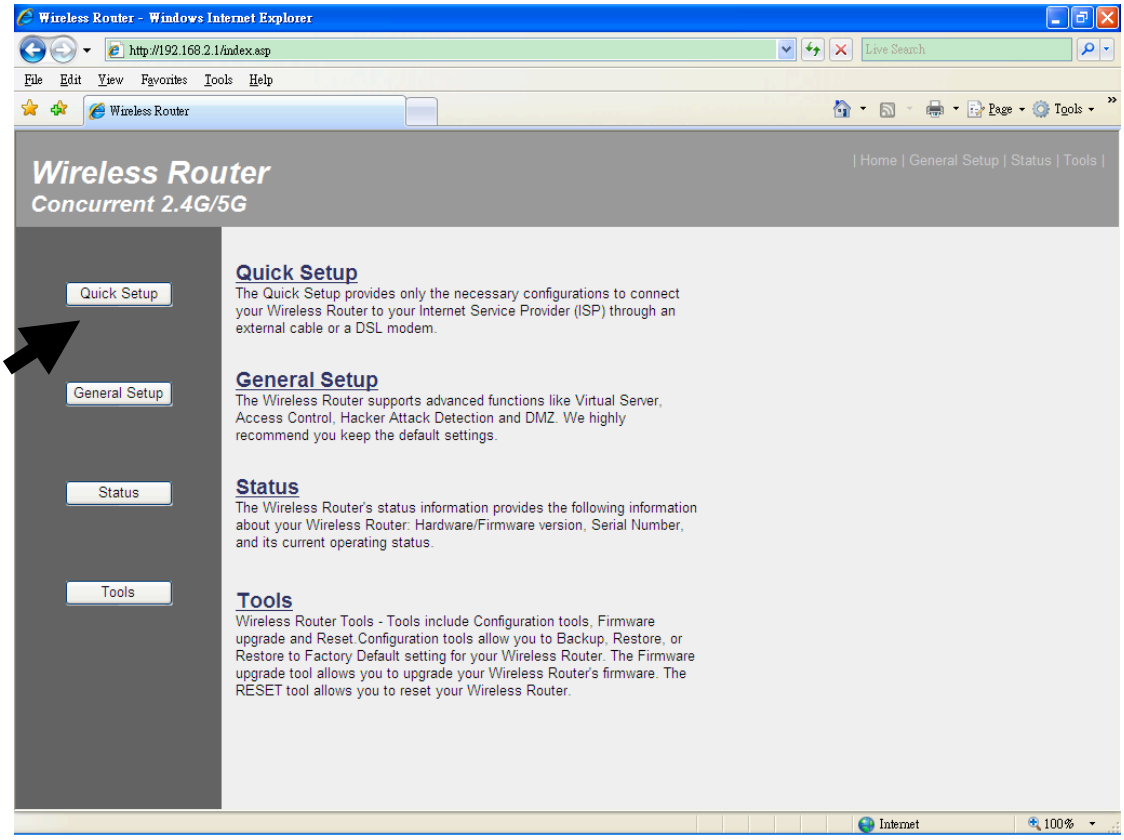
TIP: This screen shows the four major settings sections: Quick Setup, General Setup, Status and Tools. You can find the shortcut that leads to these sections at the upper-right corner of every screen, and you can jump to another section directly by clicking the link.

2-3 Using Quick Setup

This router provides a Quick Setup procedure, which will help you complete all required settings needed to quickly access the Internet.

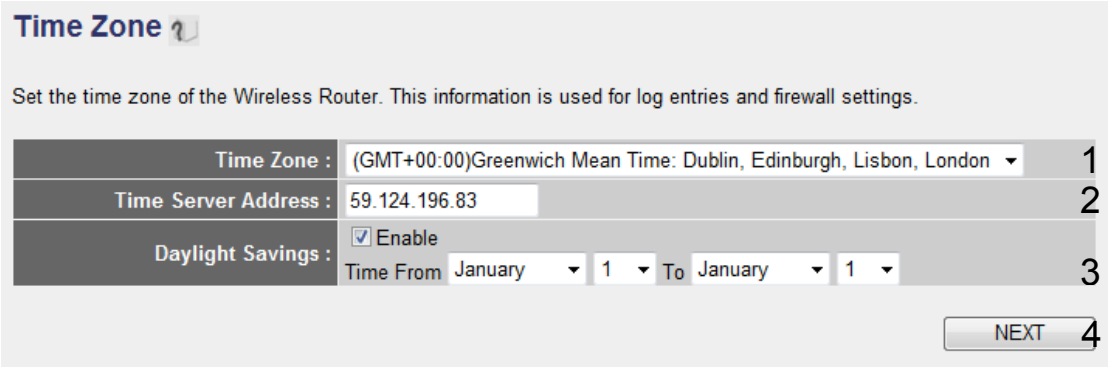
Click Quick Setup.

HERE!



The following configuration options will be presented.

1. Set Time Zone



Here are descriptions of every setup item:

Time Zone (1):	*Press and you can choose the time zone of your location.*
Time Server Address (2):	*Input the IP address / host name of the time server.*
Daylight Savings(3):	*If the country you live uses Daylight Saving, check the Enable Function box and choose the duration of Daylight Saving.*

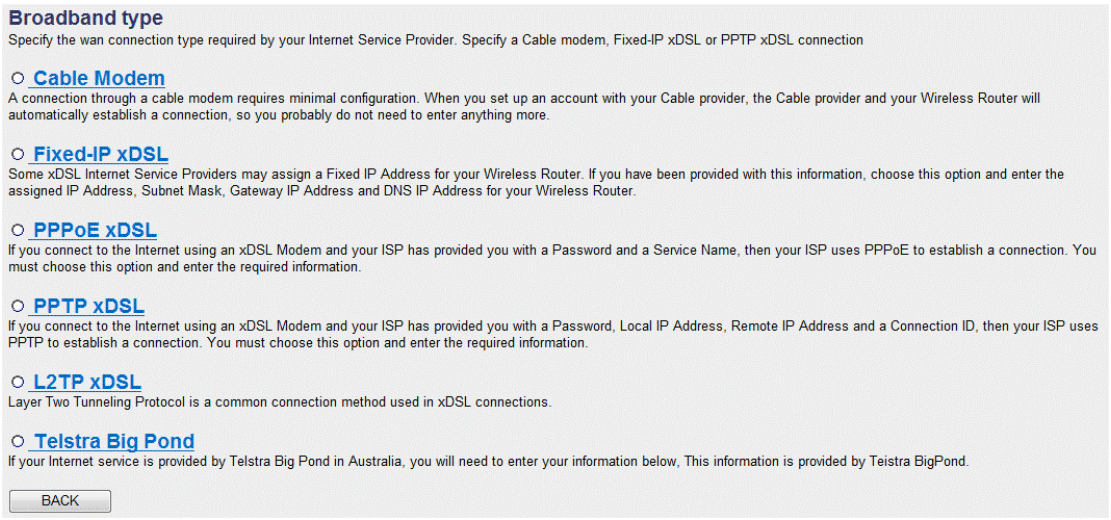
After you finish with all settings, click Apply (4).

NOTE: There are several time servers available on the Internet:

129.6.15.28 (time-a.nist.gov)
132.163.4.101 (time-a.timefreq.bldrdoc.gov)
131.107.1.10 (time-nw.nist.gov)

If you find that the time is incorrect, try another time server.

2. Set Broadband Type



Choose the broadband (Internet connection) type you're using on this screen. There are six types of Internet connections:

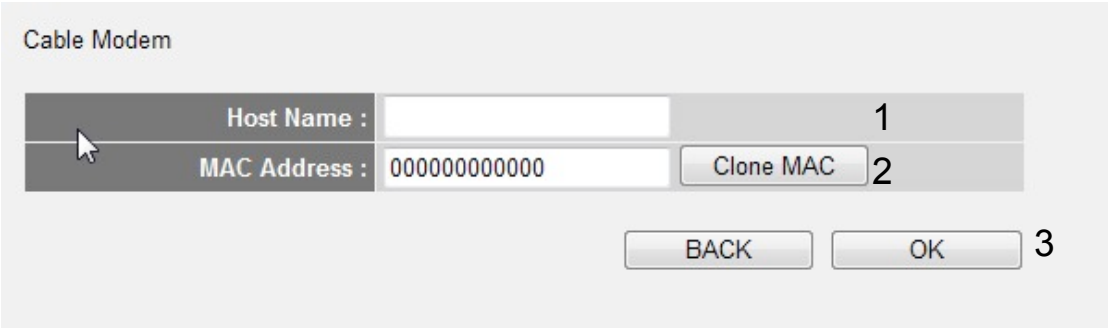
Cable Modem	- go to section 2-3-1
Fixed-IP xDSL	- go to section 2-3-2
PPPoE xDSL	- go to section 2-3-3
PPTP xDSL	- go to section 2-3-4
L2TP xDSL	- go to section 2-3-5
Telstra Big Pond	- go to section 2-3-6

If you're not sure which one to select, contact your Internet service provider. A wrong Internet connection type will cause connection problems, and you will not be able to connect to the Internet.

To go back a previous step, click Back at the bottom of the screen.

NOTE: Some service providers use DHCP (Dynamic Host Configuration Protocol) to assign an IP address to you. In this case, you can choose Cable Modem as the Internet connection type, even if you're using another connection type, like xDSL. Also, some cable modems use PPPoE, so you can choose PPPoE xDSL in such cases even you're using a cable modem.

2-3-1 Setup procedure for Cable Modem

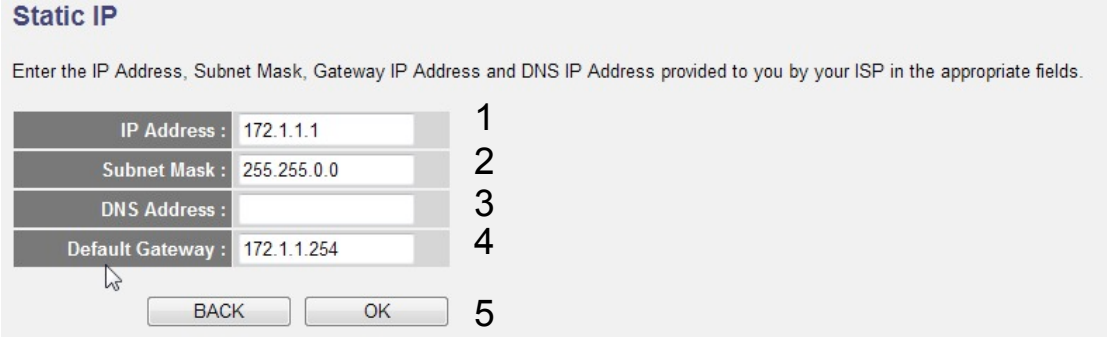


Here are descriptions of every setup item:

Host Name (1):	*Input the host name of your computer. This is optional, and is only required if your service provider asks you to do so.*
MAC address (2):	*Input the MAC address of your computer here if your service provider only permits computers with certain MAC addresess to access the Internet. If you're using a computer that used to connect to the Internet via cable modem, you can simply click Clone Mac Address to fill the MAC address field with the MAC address of your computer.*

After you finish with all settings, click OK (3). If you want to go back to a previous menu, click Back.

2-3-2 Setup procedure for Fixed-IP xDSL



Here are descriptions of every setup item:

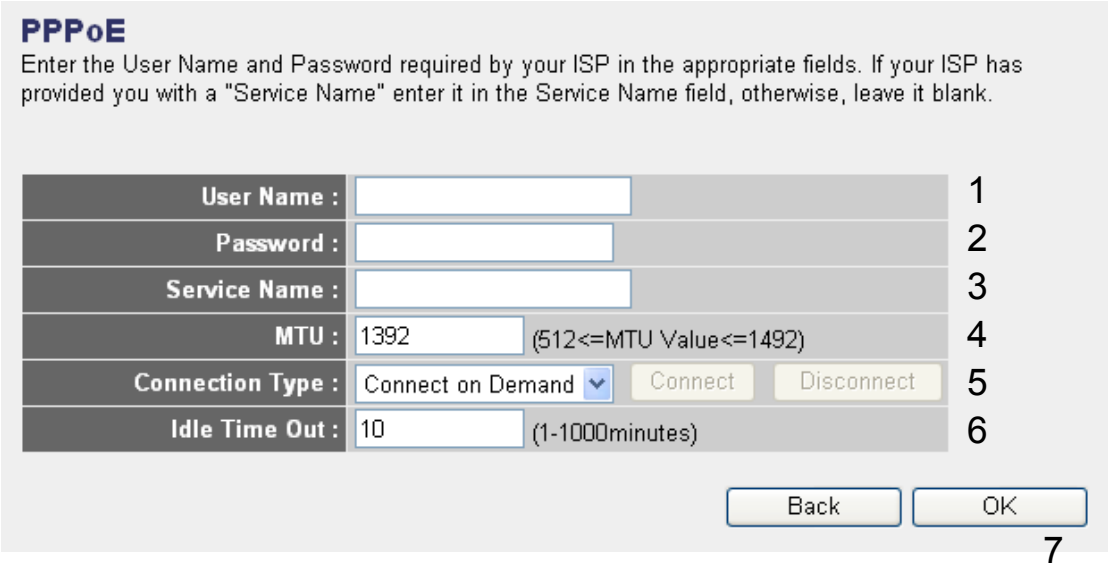
IP Address (1):	*Input the IP address assigned by your service provider.*
Subnet Mask (2):	*Input the subnet mask assigned by your service provider.*
DNS Address (3):	*Input the IP address of the DNS server provided by your service provider.*
Default Gateway (4):	*Input the IP address of the gateway provided by your service provider.*

You must use the addresses provided by your Internet service provider. Wrong settings will cause connection problems.

When you finish with all settings, press OK (5). To go back to a previous menu, click Back.

NOTE: You can choose this Internet connection method if your service provider assigns a fixed IP address (also know as a static address) to you, and is not using DHCP or PPPoE protocol. Contact your service provider for further information.

2-3-3 Setup procedure for PPPoE xDSL



Here are descriptions of every setup item:

User Name (1): *Input the user name assigned by your Internet service provider.*

Password (2): *Input the password assigned by your Internet service provider.*

Service Name (3): *Assign a name to this Internet service (optional).*

MTU (4): *Input the MTU value of your network connection. If you don't know it, you can use the default value.*

Connection Type (5): *Select the connection type of Internet connection you want to use (detailed explanation listed below).*

Idle Time Out (6): *Input idle time out (details listed below).*

When you finish with all settings, click OK (7). To go back to a previous menu, click Back.

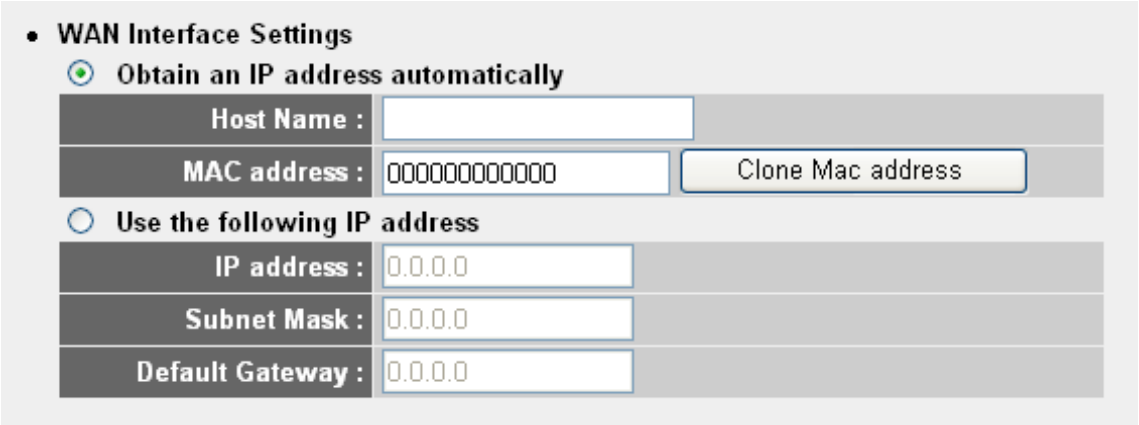
MTU – Use the default value if you don't know what it is, or ask your service provider for a proper value.

Connection Type - There are 3 options: Continuous will keep an Internet connection alive; Connect on Demand only connects to the Internet when there's a connect attempt; and Manual only connects to the Internet when Connect is clicked and disconnects when Disconnect is pressed.

Idle Time Out: Specify the time to shut down the connection after no Internet activity is detected. This option is only available when the connection type is Connect on Demand.

2-3-4 Setup procedure for PPTP xDSL

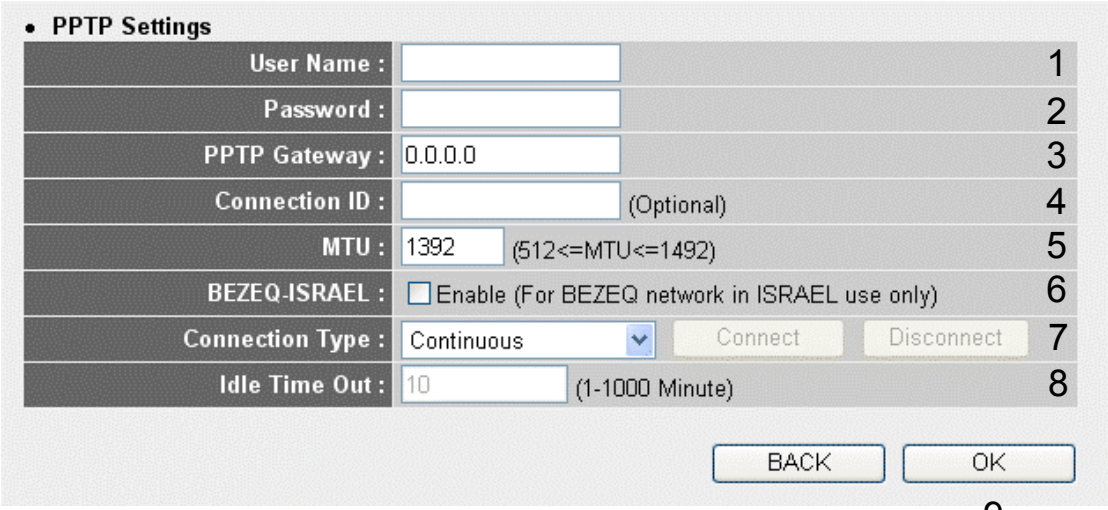
PPTP xDSL requires two settings: WAN interface setting (set up an IP address) and PPTP setting (PPTP user name and password). First, WAN Interface Settings:



Select the manner in which you obtain an IP address from your service provider. You can choose "Obtain an IP address automatically" (equal to DHCP; refer to Cable Modem above), or "Use the following IP address" (i.e., static IP address). WAN

interface settings must be correctly set; otherwise, the Internet connection will fail even if the PPTP settings are correct. Contact your Internet service provider if you don't know what to enter.

Second, PPTP Settings:



Here are descriptions of every setup item:

User Name (1):	*Input the user ID (user name) assigned by your Internet service provider.*
Password (2):	*Input the password assigned by your Internet service provider.*
PPTP Gateway (3):	*Input the IP address of the PPTP gateway assigned by your Internet service provider.*
Connection ID (4):	*Input the connection ID. This is optional and you can leave it blank.*
MTU (5):	*Input the MTU value of your network connection. If you don't know it, you can use the default value.*
BEZEQ-ISRAEL (6):	*Check this only if you're using the service provided by the BEZEQ network in Israel.*

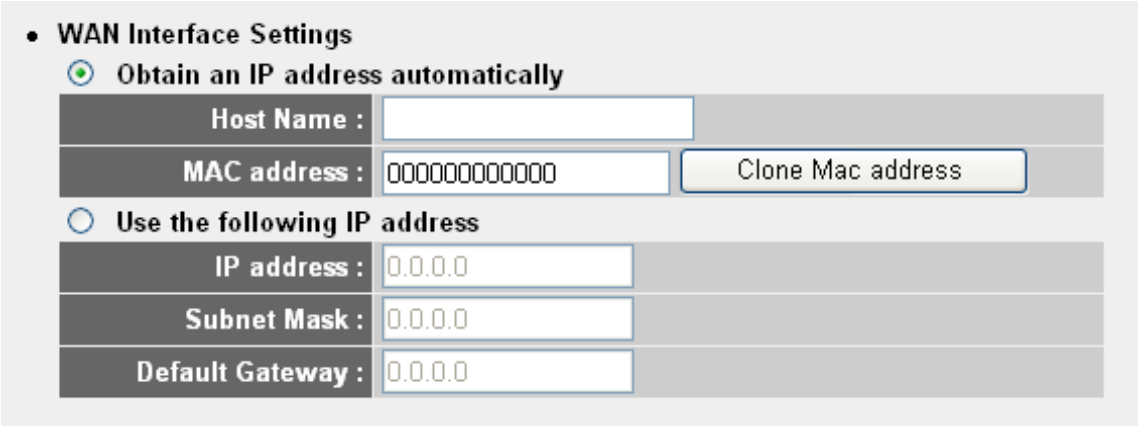
Connection type (7):	*Select the type of Internet connection you want to use. (Refer to last section for detailed descriptions.)*
Idle Time Out (8):	*Input the idle time out for the Internet connection and refer to last section for details.*

When you finish with all settings, click OK (9). To go back to a previous menu, click Back.

2-3-5 Setup procedure for L2TP xDSL

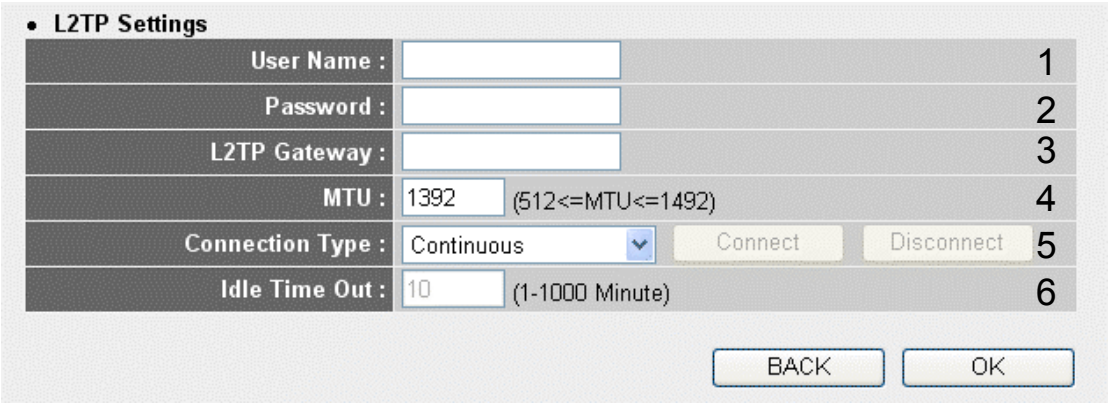
L2TP is another popular connection method for xDSL and other Internet connection types, and all required setting items are the same with the PPTP connection.

Like PPTP, there are two kinds of required settings. First, WAN Interface Settings:



Select the manner in which you obtain an IP address from your service provider: “Obtain an IP address automatically” (equal to DHCP, refer to Cable Modem above) or “Use the following IP address” (equal to static IP address, refer to PPPoE xDSL above). WAN interface settings must be correctly set; otherwise, the Internet connection will fail even if the PPTP settings are correct. Contact your Internet service provider if unsure what to enter.

Second, L2TP Settings:

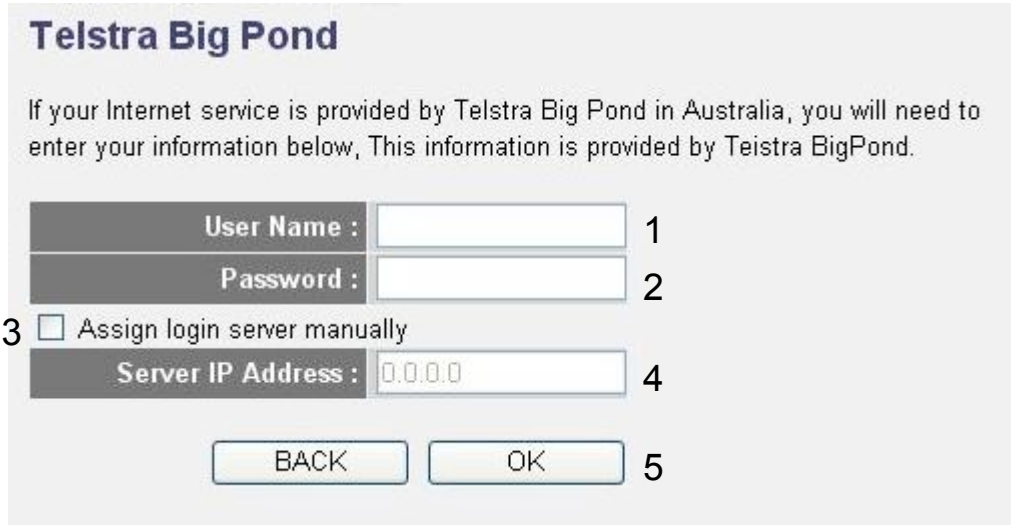


Here are descriptions of all setup items:

User Name (1):	*Input the user ID (user name) assigned by your Internet service provider.*
Password (2):	*Input the password assigned by your Internet service provider.*
L2TP Gateway (3):	*Input the IP address of the PPTP gateway assigned by your Internet service provider.*
MTU (4):	*Input the MTU value of your network connection. If you don't know it, you can use the default value.*
Connection type (5):	*Select the connection type of Internet connection you want to use (refer to last section for details).*
Idle Time Out (6):	*Input the idle time out of Internet connection you want to use (refer to last section for details).*

When you finish with all settings, click OK (7). To go back to a previous menu, click Back.

2-3-6 Setup procedure for Telstra Big Pond:

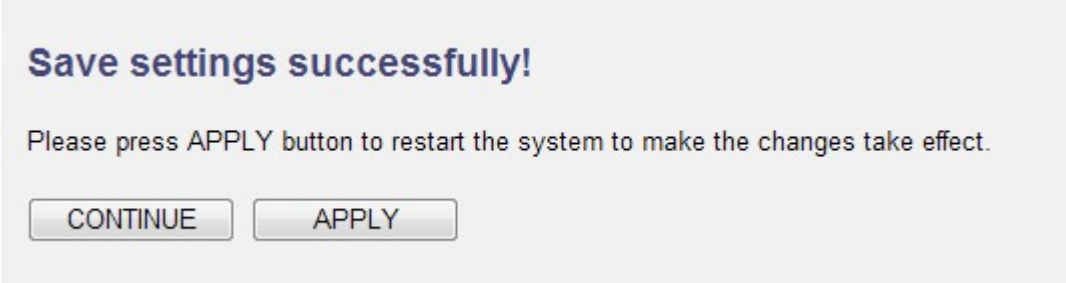


This setting only works when you're using Telstra Big Pond's network service in Australia. You need to input:

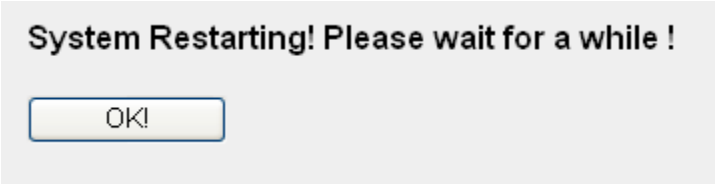
User Name (1):	*Input the user name assigned by Telstra.*
Password (2):	*Input the password assigned by Telstra.*
Assign login server manually (3):	*Check this box to choose a login server by yourself.*
Server IP Address (4):	*Input the IP address of the login server.*

When you finish with all settings, click OK (5). To go back to a previous menu, click Back.

When all settings are finished, you'll see the following message displayed on your Web browser:



Click Apply to prepare to restart the router, and you'll see this message:

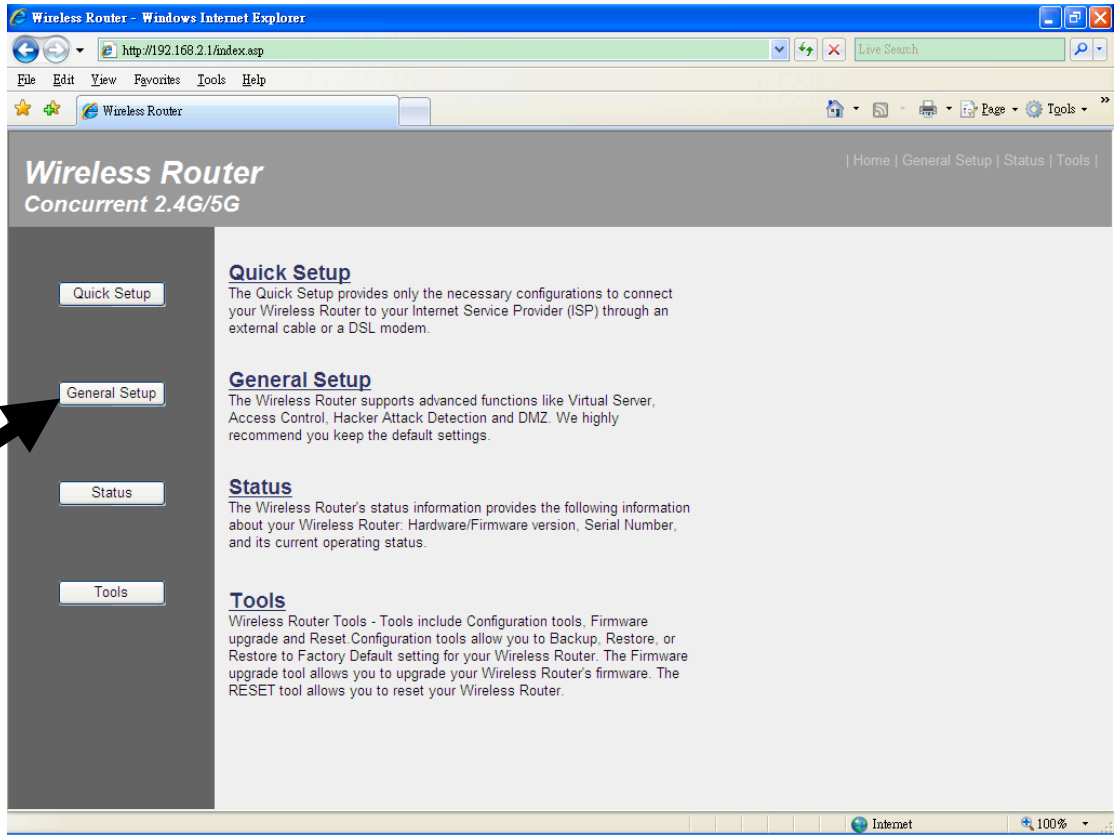


Wait for about 40 seconds, then click OK! You'll be back to the router management interface again, and the router is ready with new settings.

2-4 General Setup

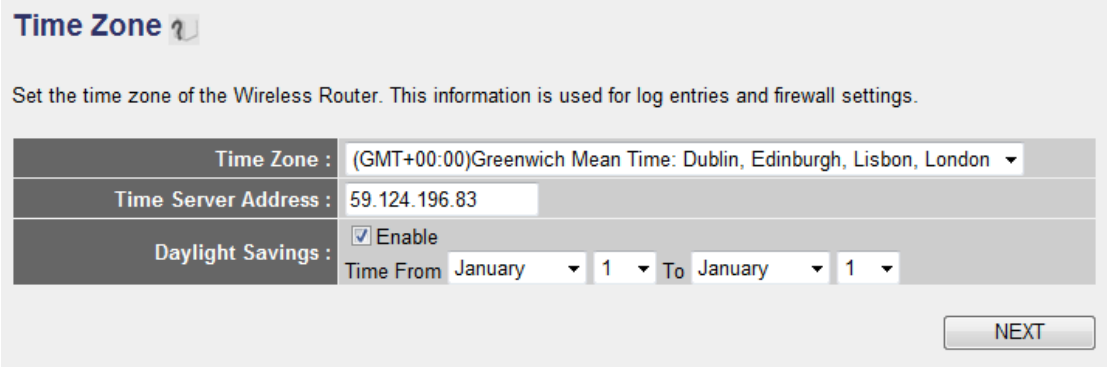
In this section, you'll learn how to change the time zone, password and remote management settings. Start your Web browser and log on to the router's Web management interface, then click General Setup on the left or click the General Setup link at the upper-right corner of the interface.

HERE!

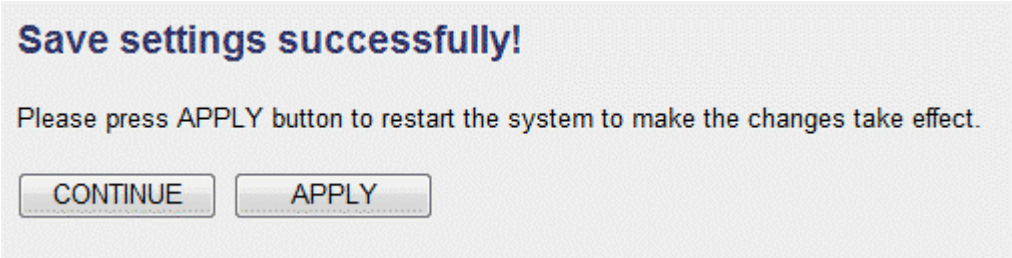


2-4-1 Time zone and time auto-synchronization

Click System on the left side of the Web management interface, then click Time Zone.



Select your time zone from the Time Zone drop-down list, and input the IP address or host name of the time server. To enable the Daylight Saving setting, check Enable and set the duration of Daylight Saving. When you finish, click Apply. You'll see the following message:



Press Continue to save the settings made and go back to the Web management interface. Click Apply to save the settings made and restart the router so the settings will take effect after it reboots.

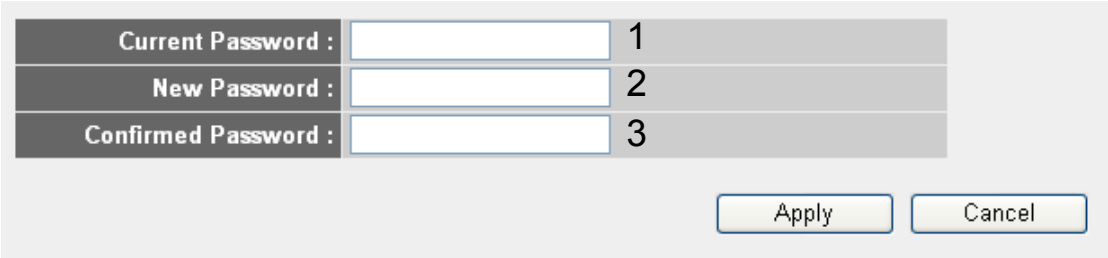
NOTE: You can refer to the instructions in the last section — Using Quick Setup — for details on time zone settings.

2-4-2 Change management password

The default password of this router is 1234, and it's displayed on the login prompt when accessed from a Web browser. There's a security risk if you don't change the default password, since everyone can see it. This is very important when you have the wireless function enabled.

To change the password:

Click System on the left side of the Web management interface, then click Password Settings.



Here are descriptions of every setup item:

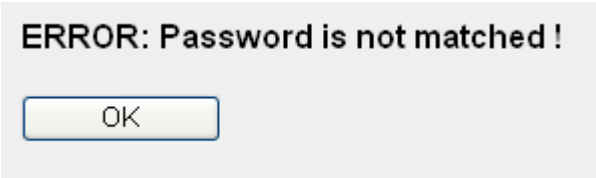
Current Password (1):	*Input the current password.*
New Password (2):	*Input the new password.*
Confirmed Password (3):	*Input the new password again.*

When you finish, click Apply. If you decide to keep the original password unchanged, click Cancel.

If the password you entered in the New Password (2) and Confirmed Password (3) fields are not the same, you'll see the following message:

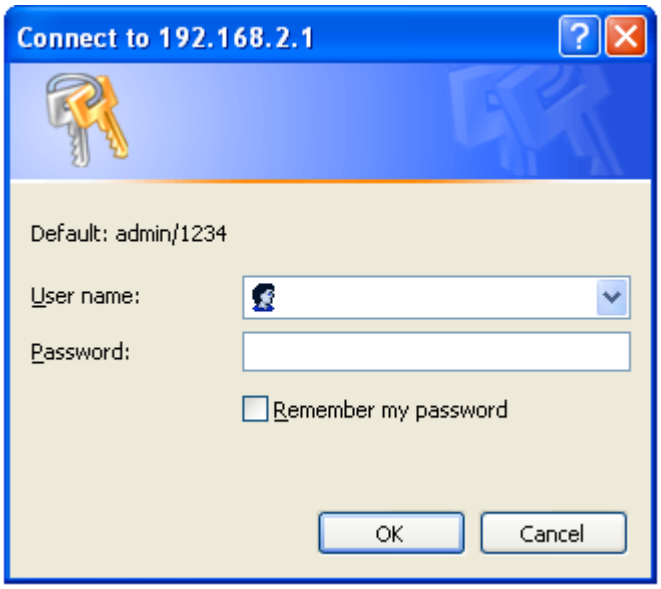
Please retype the new password again when you see the above message.

If you see the following message:



It means the content in the Current Password field is wrong. Click OK to go back to the previous menu, and try to input the current password again.

If the current and new passwords are correctly entered, after you click Apply you'll be prompted to input your new password:



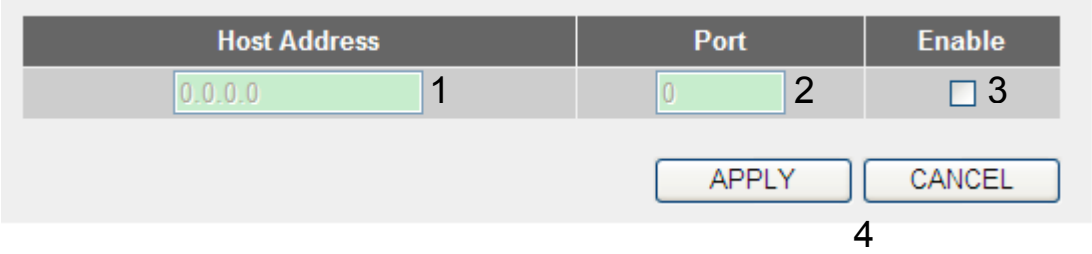
Use the new password to enter the Web management interface

again, and you should be able to log in with the new password.

2-4-3 Remote Management

This router does not allow management access from the Internet to prevent possible security risks (especially when you use a weak password or didn't change the default password); however, you can still manage this router from a specific IP address by enabling the Remote Management function.

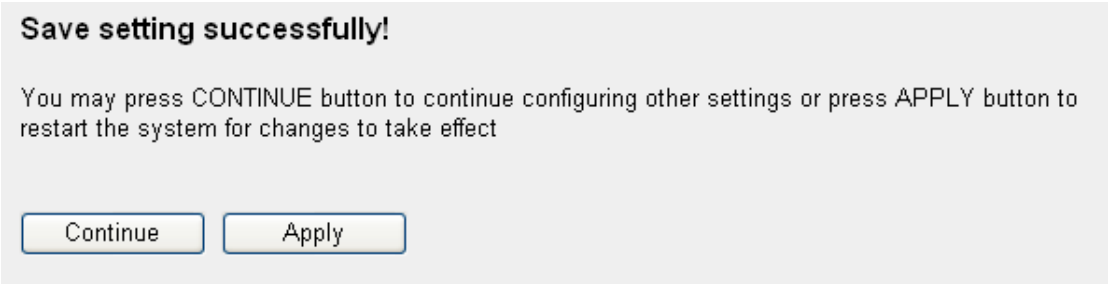
Click System on the left side of the Web management interface, then click Remote Management.



Here are descriptions of every setup item:

Host Address (1):	*Input the IP address of the remote host you wish to initiate management access to.*
Port (2):	*You can define the port number this router should you expect an incoming request. If you're providing a Web service (default port number is 80), you should try to use another port number. You can use the default port setting (8080) or something like 32245 or 1429 (any integer between 1 and 65534).*
Enable (3):	*Select the field to start the configuration.*

When you finish with all settings, click Apply.



Click Continue to save the settings made and go back to the Web management interface. Click Apply to save the settings made and restart the router so the settings will take effect after it reboots.

NOTE: When you want to manage this router from another computer on the internet, you need to input the IP address and port number of this router. If your Internet service provider assigns you a static IP address, it will not be a problem; but if the IP address your service provider assigns you will vary every time you establish an internet connection, this will be a problem.

Either ask your service provider to give you a static IP address or use a dynamic IP to host name mapping service like DDNS (refer to 2-5-8 DDNS Client for details).

NOTE: The default port number that the Web browser will use is 80. If the Port setting on this page is not 80, you need to assign the port number in the address bar of the Web browser manually. For example, if the IP address of this router is 1.2.3.4, and the port number you set is 8888, you need to input the following address in the address bar of the Web browser:

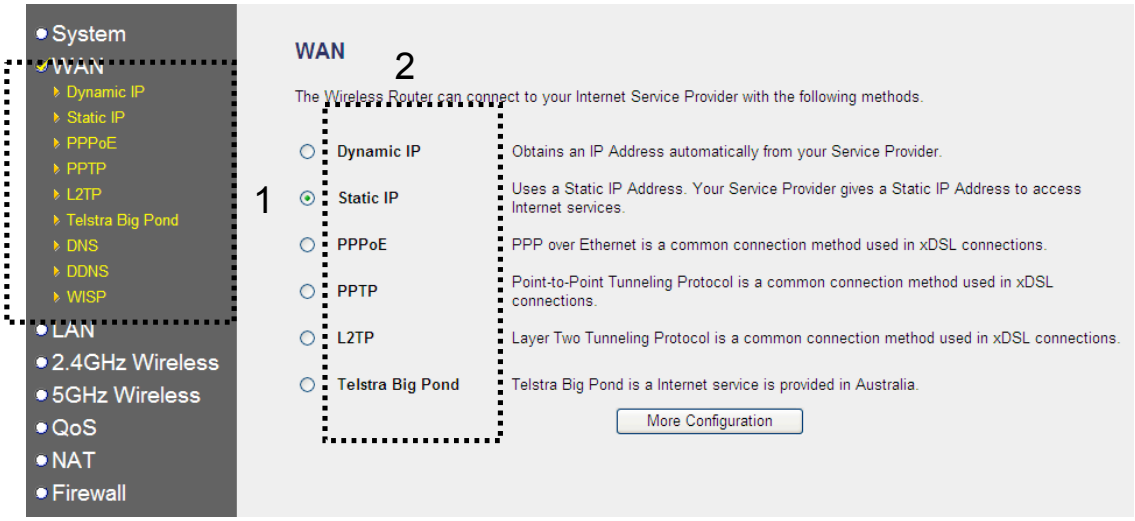
http://1.2.3.4:8888

2-5 Setup for an Internet Connection (WAN Setup)

Internet connection setup can be done by using Quick Setup as described previously. However, you can set up WAN connections by using the WAN configuration menu. You can also set advanced functions like DDNS (Dynamic DNS) here.

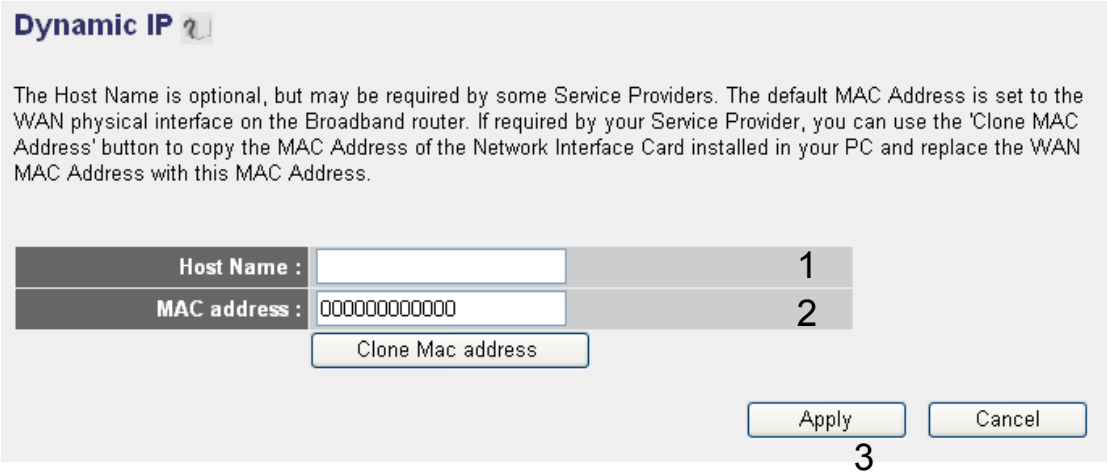
Click WAN on the left side of the Web management interface.

Select the Internet connection method that corresponds to the type of connection you're using. You can either click the connection method on the left (1) or right (2). If you select the connection method on the right, click More Configuration after a method is selected.



Dynamic IP	- go to section 2-5-1
Static IP	- go to section 2-5-2
PPPoE	- go to section 2-5-3
PPTP	- go to section 2-5-4
L2TP	- go to section 2-5-5
Telstra Big Pond	- go to section 2-5-6
DNS	- go to section 2-5-7
DDNS	- go to section 2-5-8
WISP	- go to section 2-5-9

2-5-1 Setup procedure for Dynamic IP:

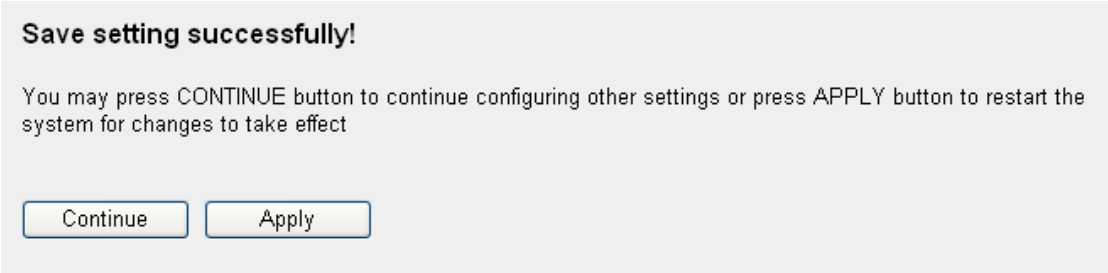


Here are descriptions of every setup item:

Host Name (1):	*Input the host name of your computer. This is optional, and is only required if your service provider asks you to do so.*
MAC Address (2):	*Input the MAC address of your computer, if your service provider only permits a computer with a certain MAC address to access the Internet. If you're using a computer that used to connect to the Internet via cable modem, you can simply press Clone MAC address to fill the MAC address field with the MAC address of your computer,*

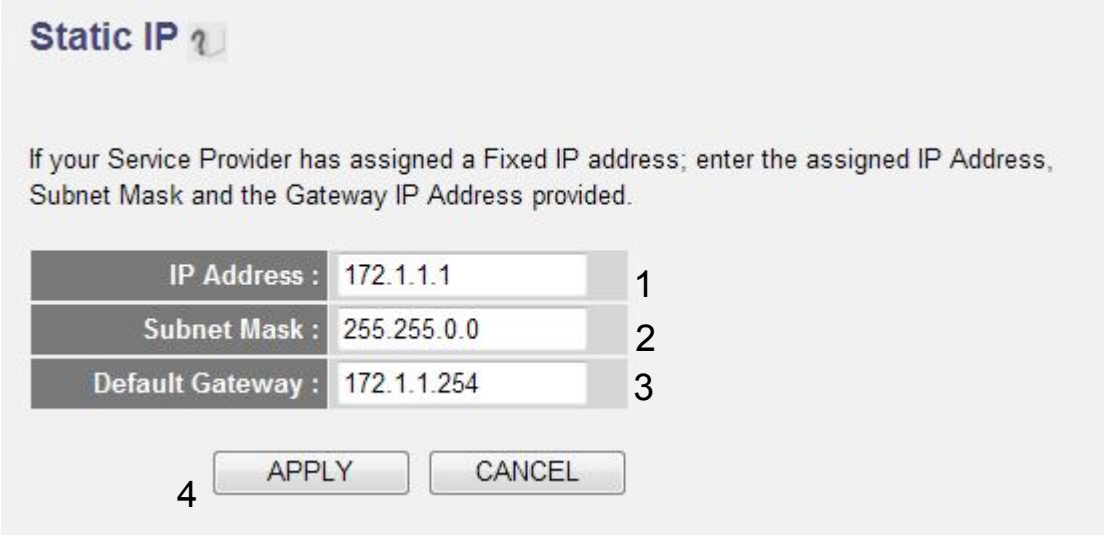
After you finish with all settings, click Apply (3). To remove any value you entered, click Cancel.

After you click Apply, the following message will be displayed on your Web browser:



Click Continue (1) to go back to a previous menu or to continue the router setup, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

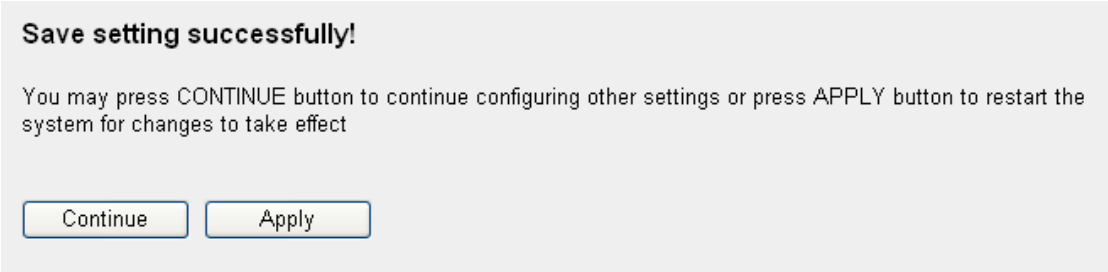
2-5-2 Setup procedure for Static IP:



Here are descriptions of every setup item:

IP Address(1):	*Input the IP address assigned by your service provider.*
Subnet Mask (2):	*Input the subnet mask assigned by your service provider.*
Default Gateway (3):	*Input the IP address of the DNS server provided by your service provider.*

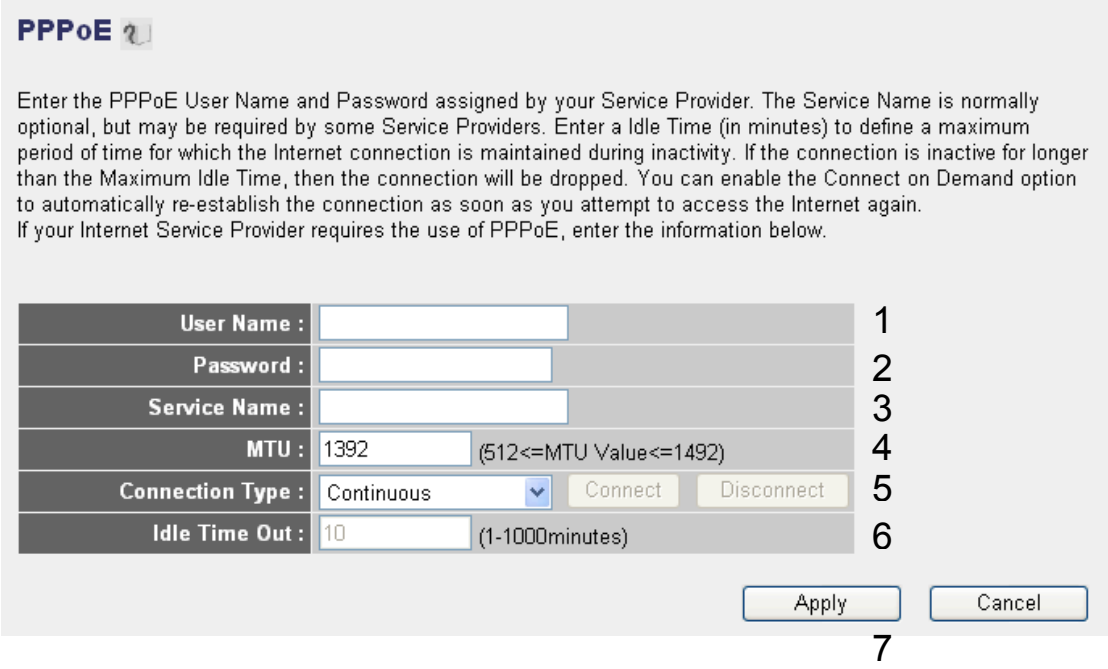
After you finish with all settings, click Apply (4) and the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to another setup procedure. Click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

To reset all settings on this screen back to previously saved values, click Cancel.

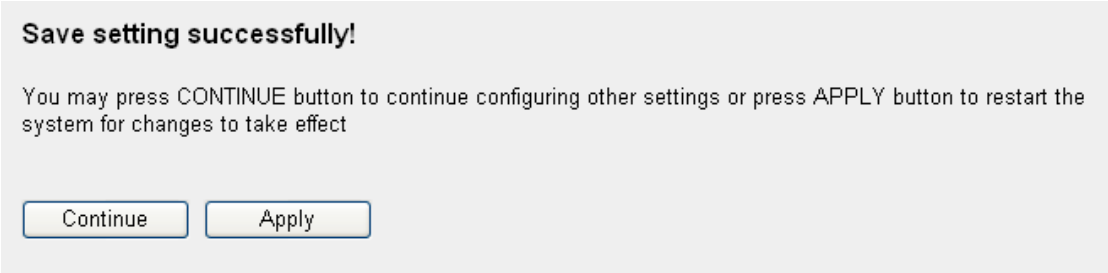
2-5-3 Setup procedure for PPPoE:



Here are descriptions of every setup item:

User Name (1):	*Input the user name assigned by your Internet service provider.*
Password (2):	*Input the password assigned by your Internet service provider.*
Service Name (3):	*Give a name to this Internet service. This is optional.*
MTU (4):	*Input the MTU value of your network connection. If you don't know, you can use the default value.*
Connection Type (5):	*Select the connection type of Internet connection you want to use.* *Continuous – The connection will be kept always on. If the connection is interrupted, the router will reconnect automatically.* *Connect On-Demand – Only connect when you want to surf the Internet. "Idle Time Out" is set to stop the connection when the network traffic is not sending or receiving after an idle time.* *Manual – After you have selected this option, you will see Connect and Disconnect. Click Connect and the router will connect to the ISP. If you want to stop the connection, click Disconnect.*
Idle Time Out (6):	*If you have selected Connect-On-Demand, input the idle time out.*

After you finish with all settings, click Apply (7) and the following message will be displayed on your Web browser:

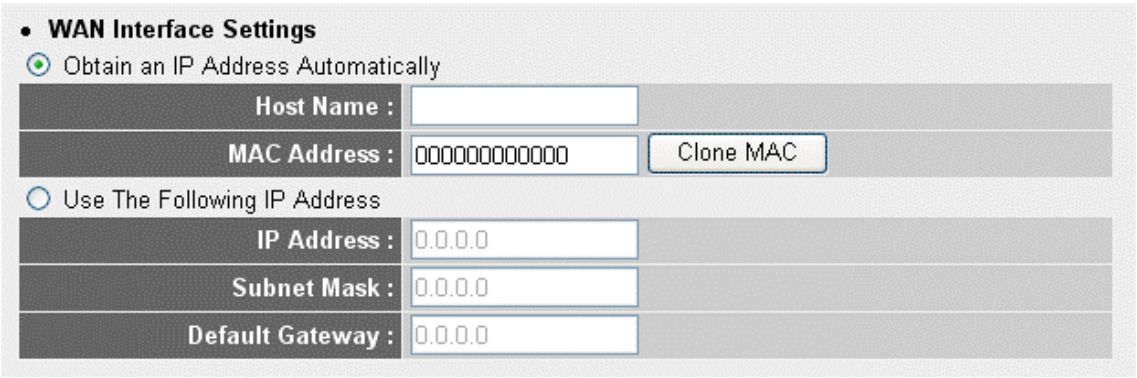


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

2-5-4 Setup procedure for PPTP:

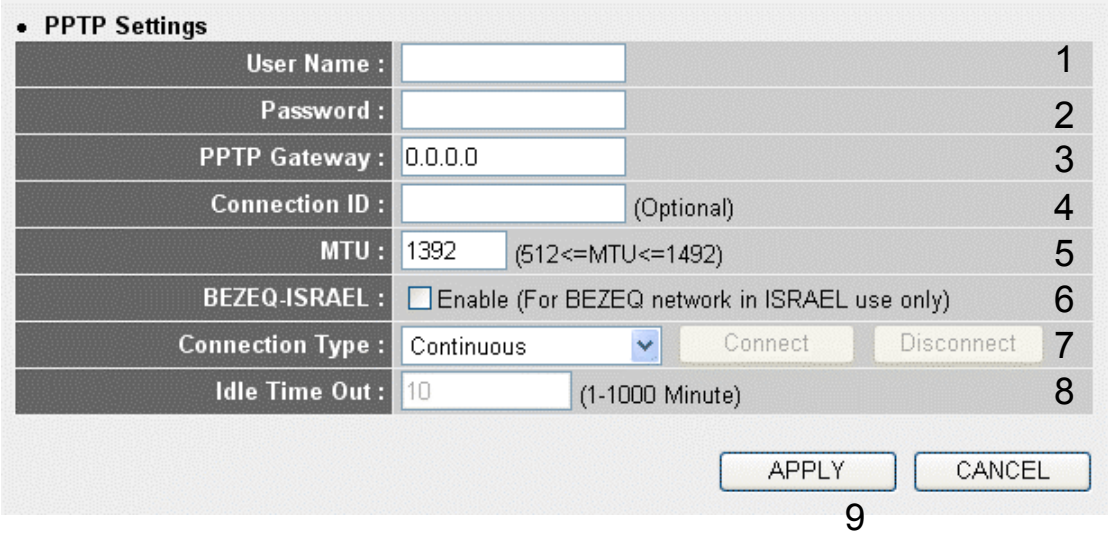
PPTP requires two kinds of settings: WAN interface setting (setup IP address) and PPTP setting (PPTP user name and password). First, the WAN interface settings:



Select the manner in which you obtain an IP address from your service provider: Obtain an IP address automatically (equal to DHCP; refer to Cable Modem above); or Use the following IP address (i.e., static IP address).

WAN interface settings must be correctly set; otherwise, the Internet connection will fail even if the PPTP settings are correct. Contact your service provider if unsure which to select.

Second, the PPTP settings:

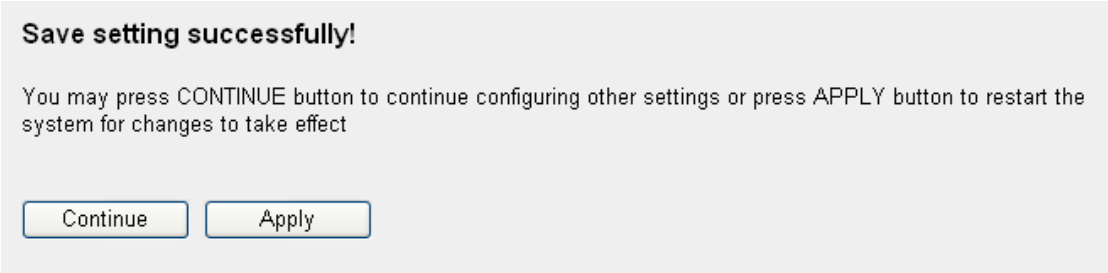


Here are descriptions of every setup item:

User Name (1):	*Input the user ID (user name) assigned by your Internet service provider.*
Password (2):	*Input the password assigned by your ISP.*
PPTP Gateway (3):	*Input the IP address of the PPTP gateway assigned by your Internet service provider.*
Connection ID (4):	*Input the connection ID. This is optional: You can leave it blank.*
MTU (5):	*Input the MTU value of your network connection. If you don't know what to enter, you can use default value.*
BEZEQ-ISRAEL (6):	*If you are connecting to the BEZEQ network in Israel, enable this function.*
Connection type (7):	*Select the Internet connection type you want to use (refer to section 2-5-3 for details).*

Idle Time Out (8): *Input the idle time out for the Internet connection you want to use (refer to 2-5-3 for details).*

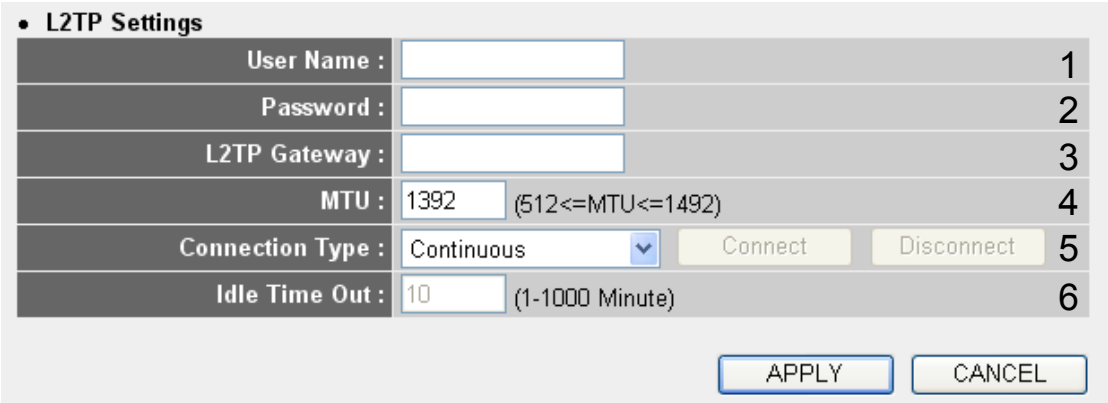
When you finish with all settings, click Apply (9) and the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

2-5-5 Setup procedure for L2TP:

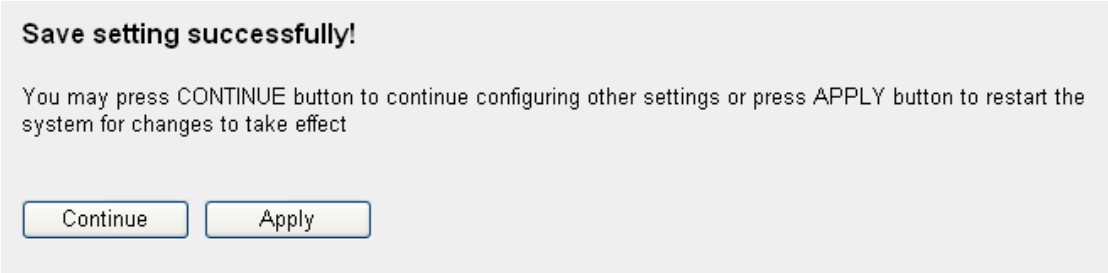


Here are descriptions of every setup item:

User ID (1): *Input the user ID (user name) assigned by your Internet service provider.*

Password (2):	*Input the password assigned by your Internet service provider.*
L2TP Gateway (3):	*Input the IP address of the PPTP gateway assigned by your Internet service provider.*
MTU (4):	*Input the MTU value of your network connection. If you don't know it, you can use the default value.*
Connection type (5):	*Select the Internet connection type you want to use (refer to 2-5-3 for details).*
Idle Time Out (6):	*Input the idle time out of the Internet connection (refer to 2-5-3 for details).*

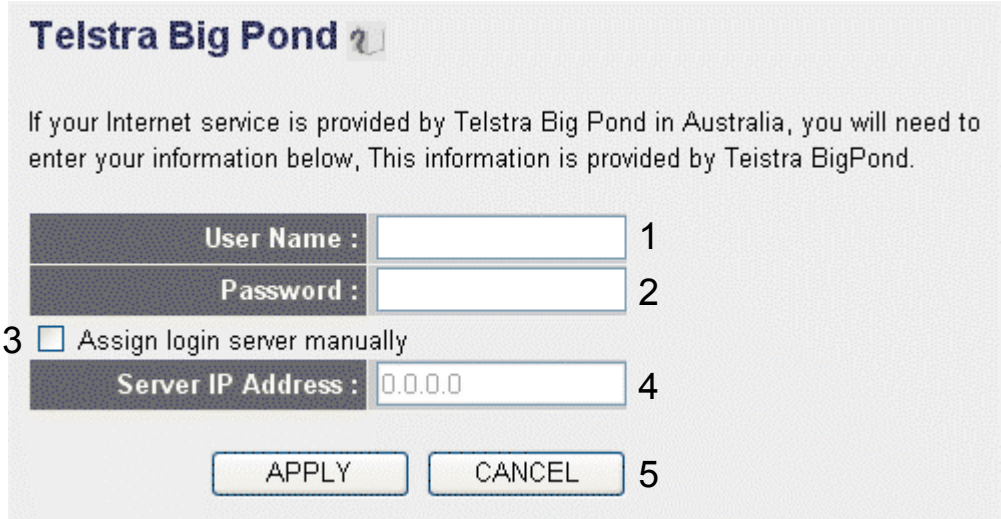
When you finish with all settings, click Apply (7) and the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

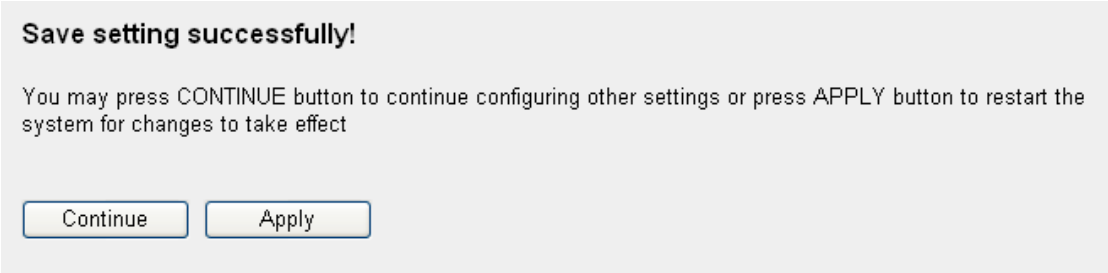
2-5-6 Setup procedure for Telstra Big Pond:



This setting only works when you're using Telstra Big Pond's network service in Australia. You need to input:

User Name (1):	*Input the user name assigned by Telstra.*
Password (2):	*Input the password assigned by Telstra.*
Assign login server manually (3):	*Check this box to choose a login server by yourself.*
Server IP Address (4):	*Input the IP address of the login server.*

When you finish with all settings, click Apply (5) and the following message will be displayed on your Web browser:

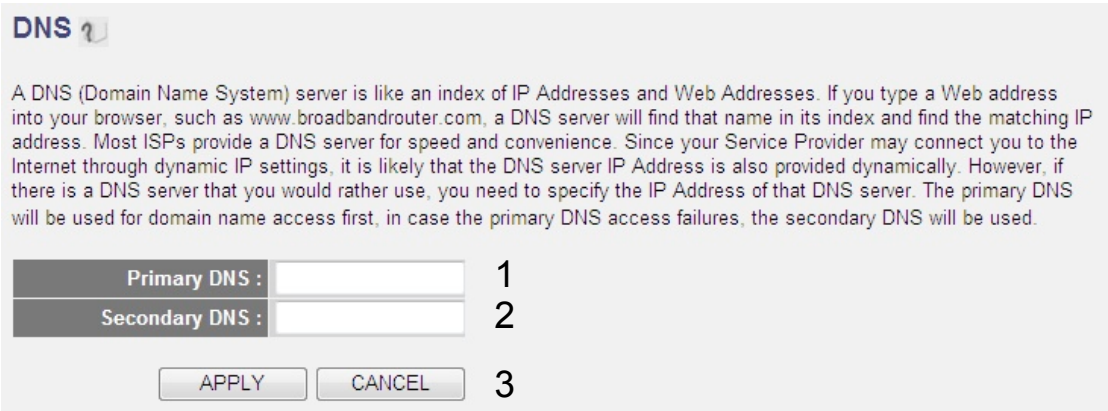


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

2-5-7 Setup procedure for DNS:

If you select *Dynamic IP* or *PPPoE* as your Internet connection method, at least one DNS server's IP address should be assigned automatically. However, if you have a preferred DNS server, or if your service provider didn't assign the IP address of the DNS server for any reason, you can input the IP address of a DNS server here.



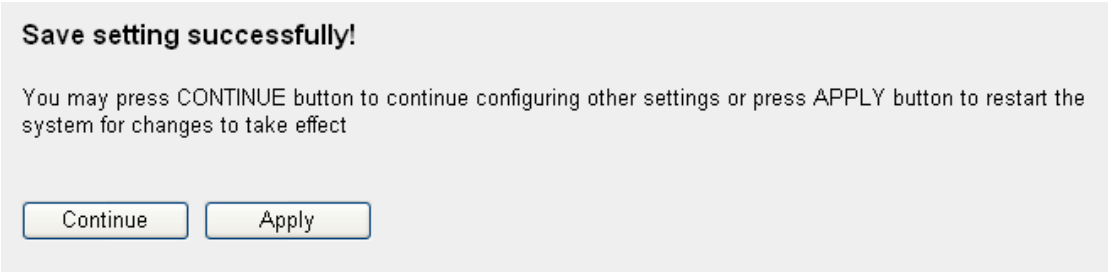
Here are descriptions of every setup item:

DNS Address (1):	*Input the IP address of the DNS server provided by your service provider.*
Secondary DNS Address (2):	*Input the IP address of another DNS server provided by your service provider (optional).*

NOTE: Only an IP address can be entered here; *DO NOT* use the hostname of a DNS server! (i.e., only numeric characters and dots are accepted)

10.20.30.40…… Correct

After you finish with all settings, click Apply (3) and the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

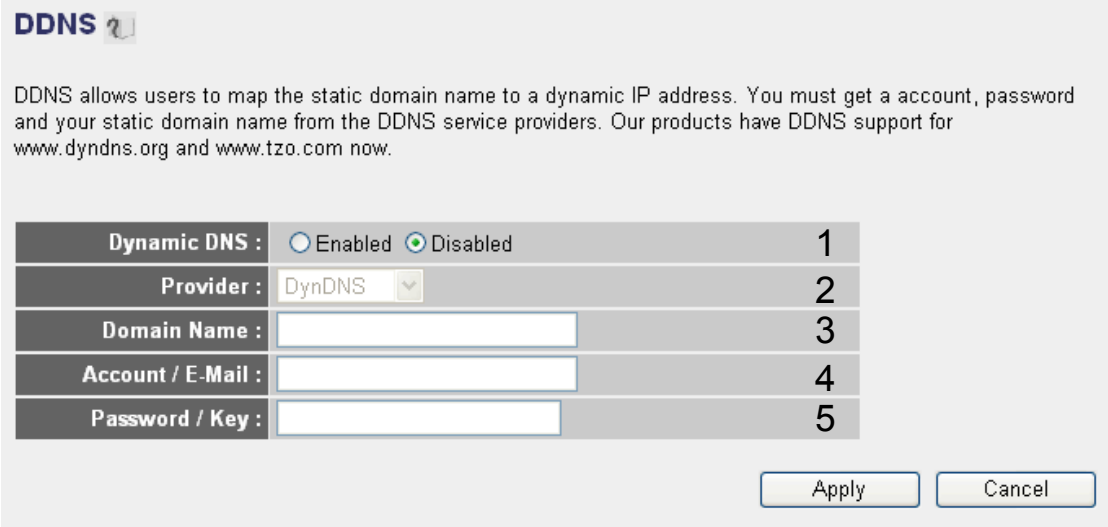
2-5-8 Setup procedure for DDNS:

DDNS (Dynamic DNS) is an IP-to-Hostname mapping service for those Internet users who don't have a static (fixed) IP address. It will be a problem if want to provide services to other users on Internet, because your IP address will vary every time you connect to the Internet, and other users won't know the IP address you're using at any given time.

This router supports DDNS services of several service providers, such as:

DynDNS (http://www.dyndns.org)
TZO (http://www.tzo.com)

Go to one of the DDNS service provider's websites listed above, and get a free DDNS account using the instructions given on their website.



Here are descriptions of every setup item:

Dynamic DNS (1): *If you want to enable the DDNS function, select Enabled; otherwise, select Disabled.*

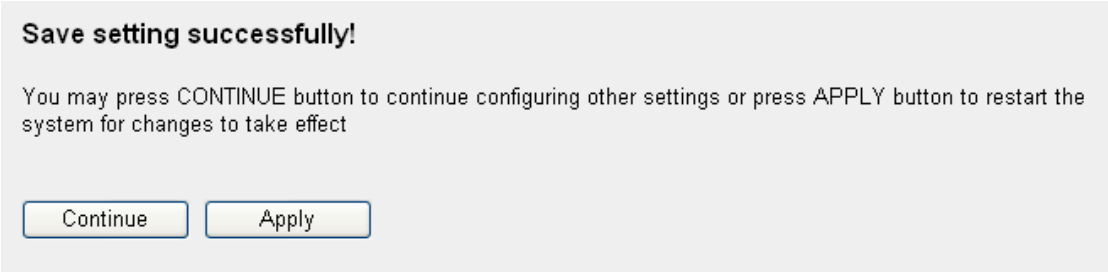
Provider (2): *Select your DDNS service provider.*

Domain Name (3): *Input the domain name you've obtained from the DDNS service provider.*

Account / E-Mail (4): *Input the account or email of DDNS registration.*

Password / Key (5): *Input the DDNS service password or key.*

After you finish with all settings, click Apply (6) and the following message will be displayed on your Web browser:

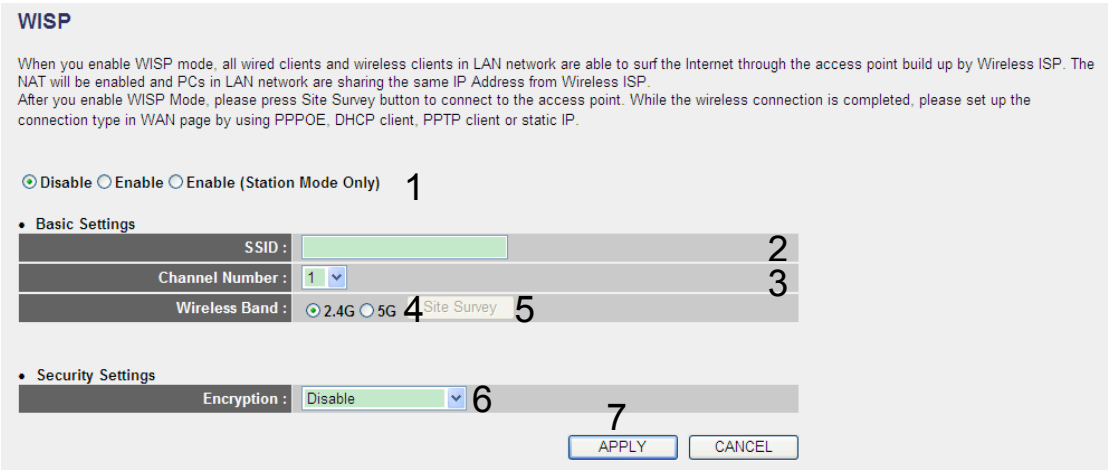


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

2-5-9 Setup procedure for WISP:

If your network service provided is through a wireless network, select this mode. After you have connected the router to the access point of the service provider wirelessly, set up the WAN connection type on the WAN screen.

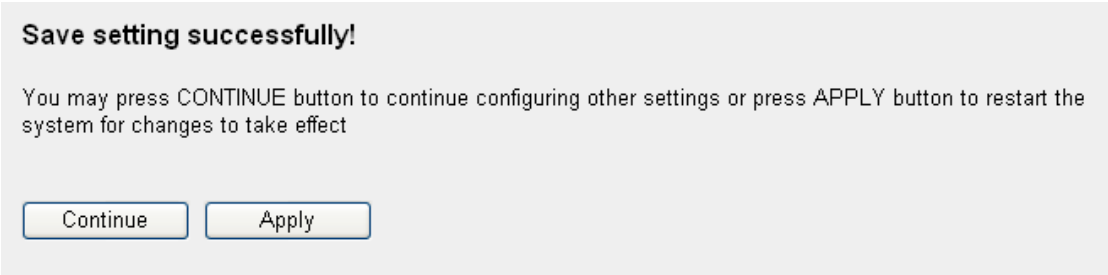


Here are descriptions of every setup item:

Disable/Enable/ Enable (Station Mode Only) (1):	*There are three selections to enable or disable wireless ISP functions.* *Disable: Disable this function.* *Enable: Enable this function and the router can also act as an access point and allow the wireless clients to associate to it for WAN access service.* **Note: In this mode, if you are informed by your wireless ISP that the wireless settings of the access point have changed, configure the router on this screen to match the settings.** *Enable (Station Mode Only): Enable this function and the router will act as a wireless client, and after connecting to WISP network devices, WAN access service will be built up through wireless. Users are allowed to access the WAN service through wired Ethernet or through another wireless band.*
SSID (2):	*This is the name of the wireless network. Input the SSID name that your wireless ISP provides.*
Channel Number (3):	*This is the radio frequency used to transmit and receive the wireless signal. The wireless devices in the same network should follow the same settings. Select the channel designated by your wireless ISP.*
Wireless Band (4):	*Check with your Wireless ISP service provider as to whether 2.4GHz or 5GHz wireless band is used for the network, and then select the wireless band here.*
Site Survey (5):	*Click Select Site Survey, and a Wireless Site*

	Survey Table will pop up. It will list all available access points nearby. Select the access point designated by your wireless ISP in the table and the router will join the wireless network through this access point.
Security Setting (6):	*If the access point enables wireless security, you need to follow the same settings in order to access the access point. Click to set security settings for this connection (go to section 2-7-3 Wireless Security for detailed instructions).*

After you finish with all settings, click Apply (7) and the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you decide to reset all settings on this screen back to previously saved values, click Cancel.

2-6 Wired LAN Configurations

Before all computers using wired Ethernet connections (i.e., those computers connecting to this router's LAN ports 1 to 4 via Ethernet cable) can communicate with each other and access the Internet, they must have a valid IP address.

There are two ways to assign IP addresses to computers: static IP address (set the IP address for every computer manually), and dynamic IP address (IP address of computers will be assigned by the router automatically. It's recommended for most computers to use a dynamic IP address, as it will save a lot of time instead of setting IP addresses for every computer, especially when there are a lot of computers in your network; for servers and network devices which will provide services to other computers and users that come by way of the Internet, astatic IP address should be used so other computers can locate the server.

If you have no idea how to define an IP address plan for your network, here are some suggestions.

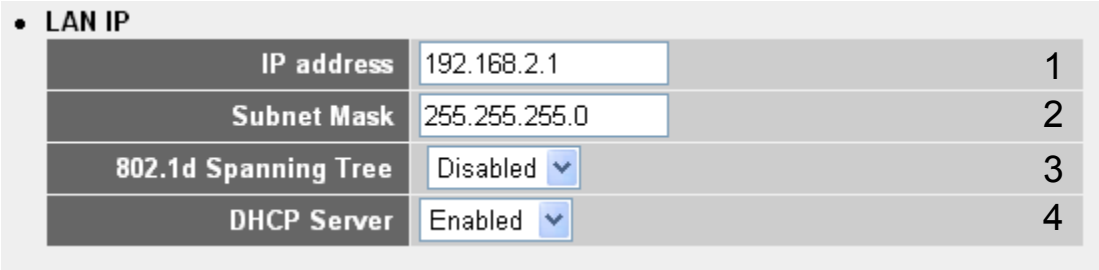
1. **A valid IP address has 4 fields: a.b.c.d. For most home and business users, it's suggested to use 192.168.c.d, where c is an integer from 0 to 254, and d is an integer from 1 to 254. This router is able to work with up to 253 clients, so you can set the "d" field of the IP address of the router as 1 or 254 (or any number in between), and pick a number between 0 and 254 for field "c."**
2. **In most cases, you should use 255.255.255.0 as a subnet mask, which allows up to 253 clients (the router's capability).**
3. **For all servers and network devices which will provide services to other people (like Internet, print and file services), you should use a static IP address. Assign each a unique number from 1 to 253, and maintain a list so everyone can locate those servers easily.**
4. **For computers not dedicated to provide specific service to others, you should use dynamic IP addresses.**

If you don't fully understand the descriptions listed above, don't worry! Recommended setup values are presented below.

To set the wired LAN parameters:

Click LAN on the left side of the Web management interface. There are three setup groups here: LAN IP, DHCP Server and Static DHCP Leases Table. Following are the setup instructions for each:

2-6-1 LAN IP section:



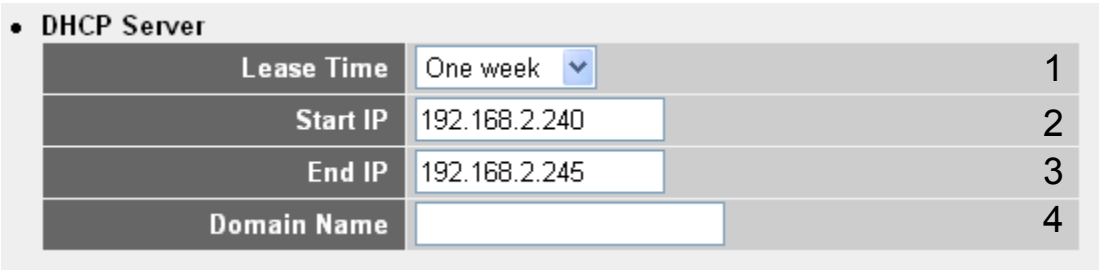
Here are descriptions of every setup item:

IP address (1):	*Input the IP address of this router.*
Subnet Mask (2):	*Input the subnet mask for this network.*
802.1d Spanning Tree (3):	*To activate the 802.1d spanning tree function, select Enabled.*
DHCP Server (4):	*To activate the DHCP server function, select Enabled.*

Recommended Values/Settings if you don't know what to enter:

IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
802.1d Spanning Tree: Disabled
DHCP Server: Enabled

2-6-2 DHCP Server:



These settings are only available when DHCP Server in the LAN IP section is enabled. Here are descriptions of every setup item:

Lease Time (1): *Choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this router from the drop-down menu.*

Start IP (2): *Input the Start IP address of the IP range.*

End IP (3): *Input the End IP address of the IP range.*

Domain Name (4): *You can also input the domain name for your network. This is optional.*

Recommended Values/ Settings if you don't know what to enter:

Lease Time: Two Weeks (or Forever, if you have fewer than 20 computers)
Start IP: 192.168.2.100
End IP: 192.168.2.200
Domain Name: (leave it blank)

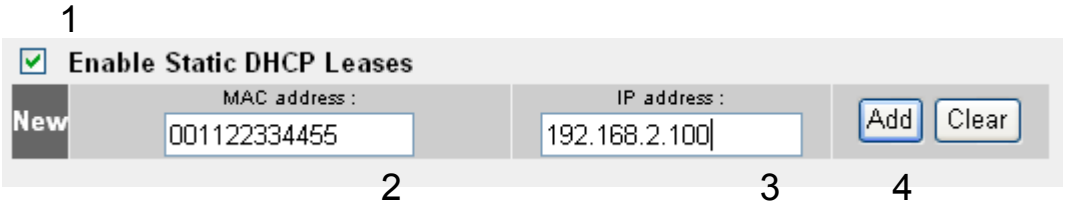
NOTE:

1. **The number of the last field (the aforementioned "d" field) of End IP must be greater than that of Start IP, and can not be the same as the router's IP address.**
2. **The other three fields of the IP address of Start IP and End IP and the IP address of the LAN IP section (the aforementioned a, b and c fields) should be the same.**

2-6-3 Static DHCP Leases Table:

This function allows you to assign a static IP address to a specific computer forever: You don't have to set the IP address, but you can still enjoy the benefit of using the DHCP server. Maximum 16 static IP addresses can be assigned here.

(If you set Lease Time to "Forever" in the DHCP Server section, you can also assign an IP address to a specific computer permanently; however, you will not be able to assign a certain IP address to a specific computer since IP addresses will be assigned in random order by this method).



Here are descriptions of every setup item:

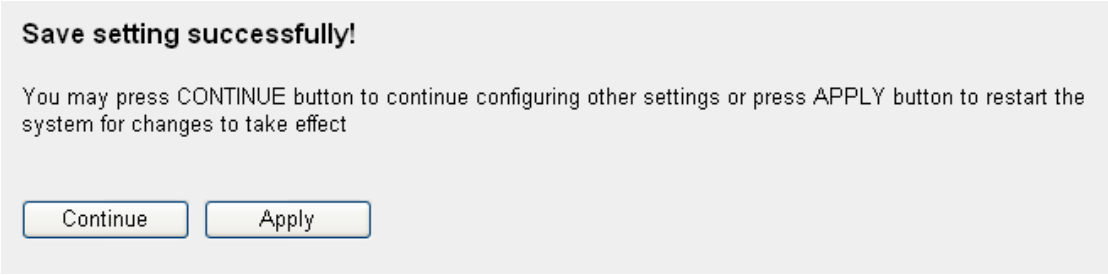
Enable Static DHCP Leases (1):	*Check to enable this function.*
MAC Address (2):	*Input the MAC address of the computer or network device (total 12 characters, from 0 to 9 and from a to f, like "001122aabbcc").*
IP address (3):	*Input the IP address you want to assign to this computer or network device.*
Add (4):	*After you inputted the MAC address and IP address pair, click to add the pair to the static DHCP leases table.*

If you decide to remove all the characters you just entered, click Clear.

After you click Add, the MAC address and IP address mapping will be added to Static DHCP Leases Table section.

If you decide to delete a specific item, check the Select box of a MAC address and IP address mapping (1), then click Delete Selected (2). To delete all mappings, click Delete All (3).

After you finish all the LAN settings, click Apply.The following message will be displayed on your Web browser:



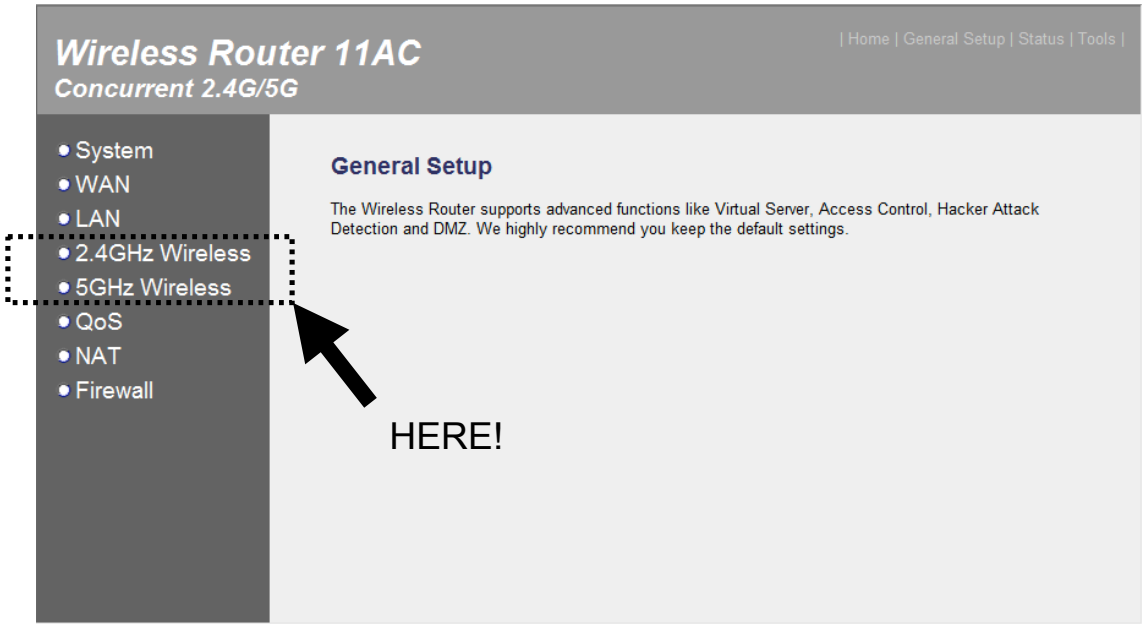
Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

2-7 Wireless LAN Configurations

If your computer, PDA, game console or other network device is equipped with a wireless network interface, you can use the wireless function of this router to connect to the Internet and share resources with other computers with a wired-LAN connection. You can also use the built-in security functions to protect your network from being hacked by malicious intruders.

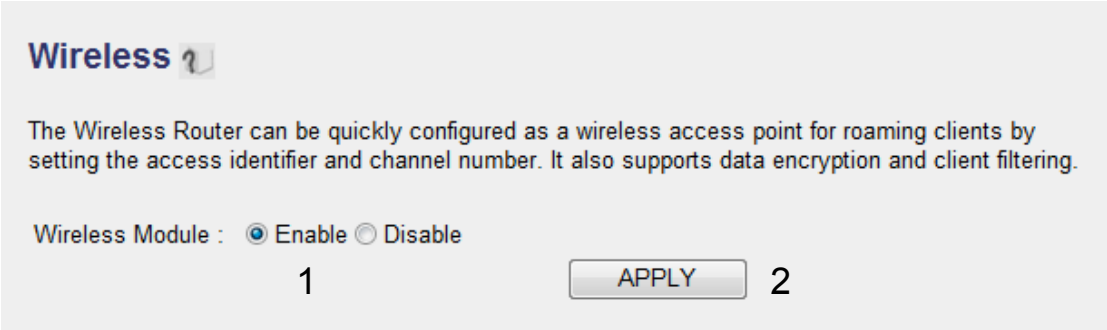
This router supports both 2.4GHz and 5GHz wireless bands simultaneously; the wireless settings for both wireless bands are almost the same. The following sections will only highlight the differences between these two selections.

Go to the General Setup screen and select 2.4GHz Wireless or 5GHz Wireless to configure the wireless settings.

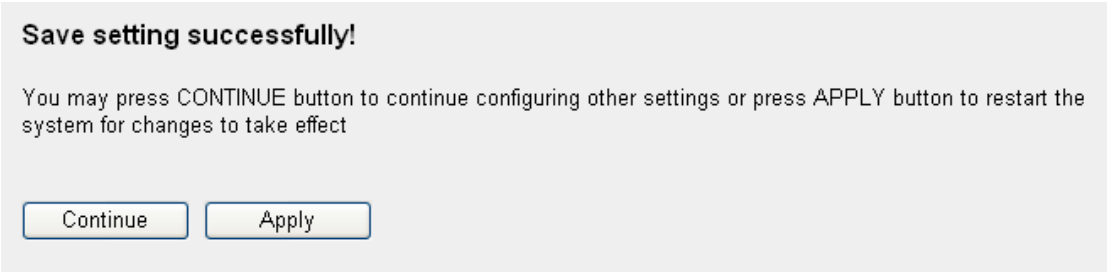


The screen below will be displayed on your Web browser. You must enable the wireless function of this router for the wireless interface of this router to function. Select Enable (1), then click Apply (2).

To disable the wireless function, press the WPS on the back panel.



After you click Apply (2), the following message will be displayed on your Web browser:

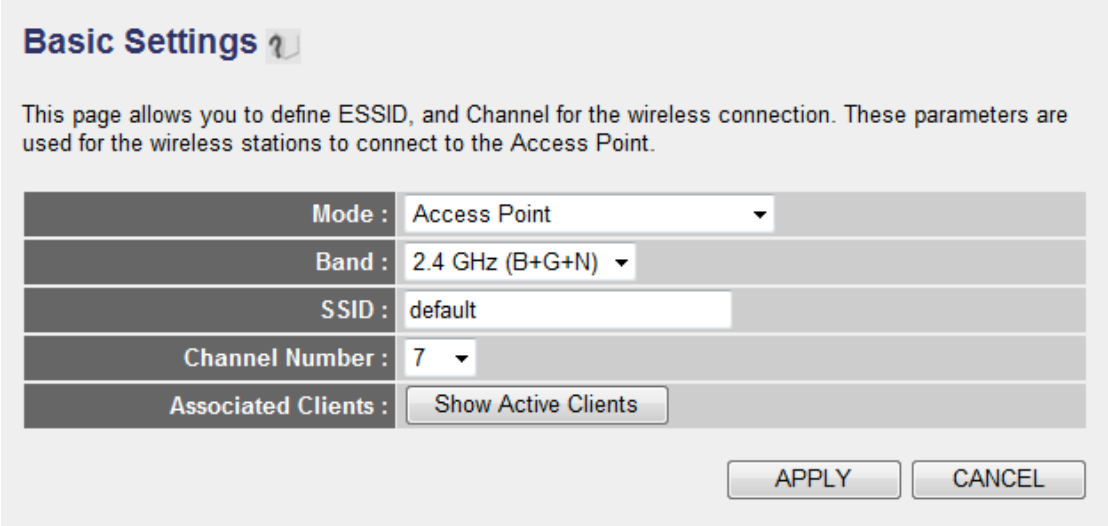


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

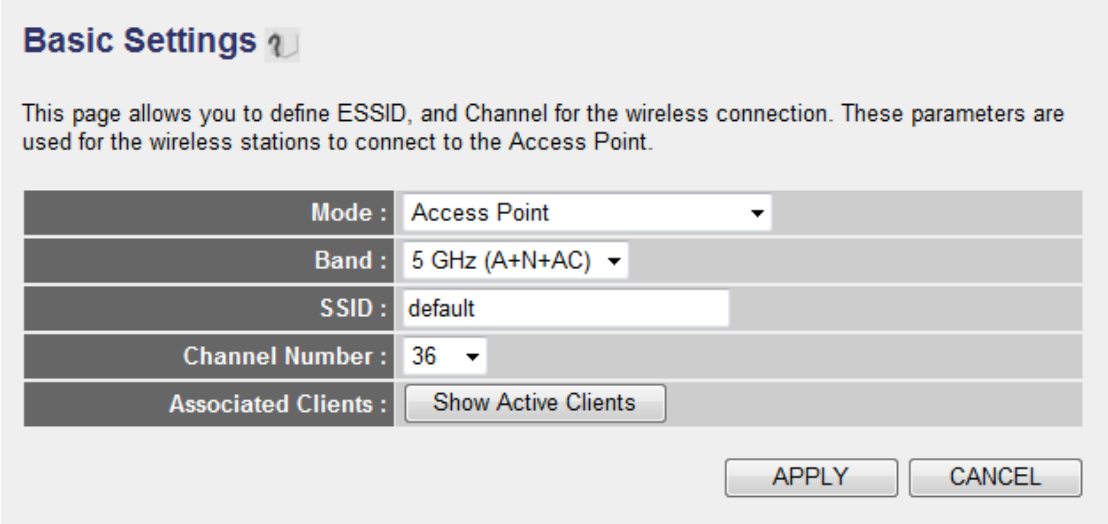
2-7-1 Basic Wireless Settings

Click 2.4GHz Wireless or 5GHz Wireless on the left side of the Web management interface, then click Basic Settings, and one the following messages will be displayed on your Web browser:

2.4GHz Wireless



5GHz Wireless



This wireless router can operate in 6 modes:

a. *Access Point*: Standard wireless AP.
b. *Station-Infrastructure*: Configure the router to an Ethernet device such as a TV or game console to enable the Ethernet device be a wireless station.
c. *AP Bridge-Point to Point*: Connect this router with another wireless router to expand the scope of a network.
d. *AP Bridge-Point to Multi-Point*: Connect this router with up to four other wireless routers to expand the scope of a network.
e. *AP Bridge-WDS*: Connect this router with up to four WDS-capable wireless routers to expand the scope of a network.

f. *Universal Repeater*: The router can act as Station and AP at the same time. It can use the Station function to connect to a Root AP and use the AP function to service all wireless stations within its coverage.

NOTE: For AP Bridge-Point to Point and AP Bridge-Point to Multi-Point modes, the wireless router is operated in wireless bridge dedicated mode – where the router is only used to expand the scope of a network and no wireless clients will be accepted. If you want to use your wireless router to expand the scope of a network and also accept wireless clients, select AP Bridge-WDS or Universal Repeater mode.

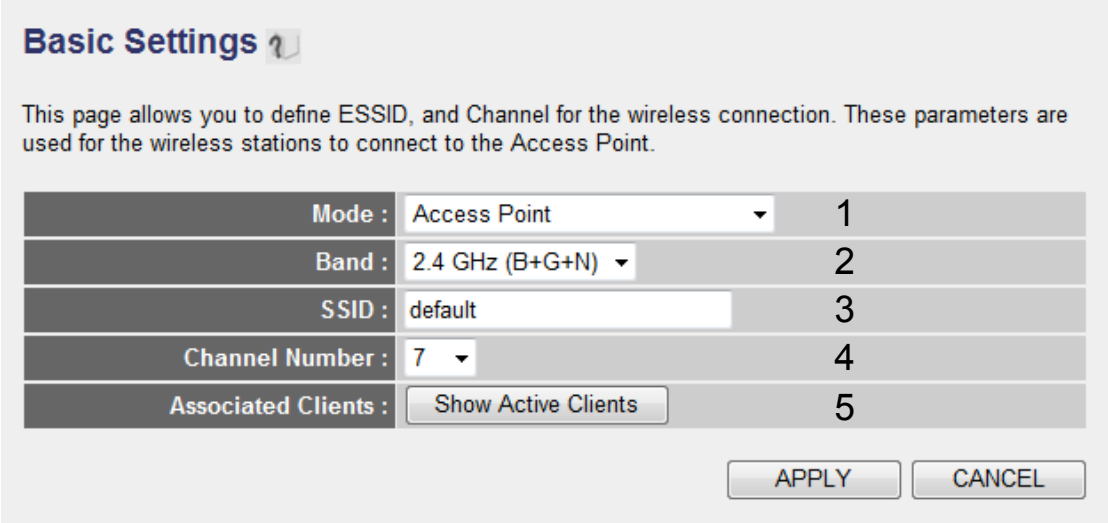
Select the mode you want to use from the Mode drop-down menu (1) and continue to other specific settings:

Access Point	- go to section 2-7-1-1
Station-Infrastructure	- go to section 2-7-1-2
AP Bridge-Point to Point	- go to section 2-7-1-3
AP Bridge-Point to Multi-Point	- go to section 2-7-1-4
AP Bridge-WDS	- go to section 2-7-1-5
Universal Repeater	- go to section 2-7-1-6

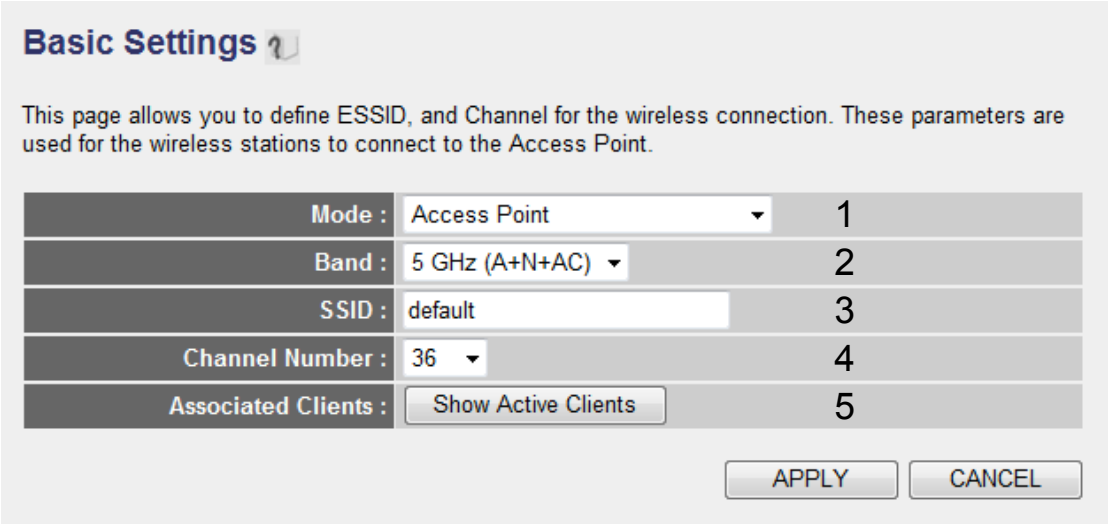
2-7-1-1 Setup procedure for Access Point:

Select the radio band you want to use from the Band drop-down menu (2). One of the following messages will be displayed:

2.4GHz Access Point Settings



5GHz Access Point Settings



Here are descriptions of every setup item:

Band (2): ***2.4GHz Band***

2.4 GHz (B): This mode only allows 802.11b wireless network clients to connect to this router (maximum transfer rate of 11 Mbps).
2.4 GHz (N): This mode only allows 802.11n wireless network clients to connect to this router (maximum transfer rate of 300 Mbps).

2.4 GHz (B+G): This mode only allows 802.11b and 802.11g wireless network clients to connect to this router (maximum transfer rate of

11 Mbps for 802.11b clients and 54 Mbps for 802.11g clients).

2.4 GHz (G): This mode only allows 802.11g wireless network clients to connect to this router (maximum transfer rate of 54 Mbps).

2.4 GHz (B+G+N): This mode allows 802.11b, 802.11g and 802.11n wireless network clients to connect to this router (maximum transfer rate of 11 Mbps for 802.11b clients, 54 Mbps for 802.11g clients and 300 Mbps for 802.11n clients).

5GHz Band

5GHz (A): This mode allows 802.11a wireless network clients to connect to this router (maximum transfer rate of 54 Mbps for 802.11a clients).

5GHz (N): This mode allows 802.11n wireless network clients to connect to this router (maximum transfer rate of 150 Mbps for 802.11n clients).

5GHz (A+N): This mode allows 802.11a and 802.11n wireless network clients to connect to this router (maximum transfer rate of 54 Mbps for 802.11a clients and 150 Mbps for 802.11n clients).

5GHz (AC): This mode allows 802.11ac wireless network clients to connect to this router (maximum transfer rate of 433 Mbps for 802.11ac clients).

5GHz (N+AC): This mode allows 802.11n and 802.11ac wireless network clients to connect to

this router (maximum transfer rate of 150 Mbps for 802.11n clients and 433 Mbps for 802.11ac clients).

5GHz (A+N+AC): This mode allows 802.11a, 802.11n and 802.11ac wireless network clients to connect to this router (maximum transfer rate of 54 Mbps for 802.11a clients, 150 Mbps for 802.11n clients and 433 Mbps for 802.11ac clients).

NOTE: For 802.11n mode: The router is operating in a 2T2R Spatial Multiplexing MIMO configuration.

SSID (3): *This is the name of the wireless router. You can type any alphanumerical characters here (up to 32). SSID is used to identify your own wireless router from others in the same area. The default SSID is "default." It's recommended that you change the default SSID value to one that is meaningful to you, like myhome, office_room1, etc.*

Channel Number (4): *Select a channel from the drop-down list for Channel Number. You can choose any channel number, and almost all wireless clients can locate the channel you're using automatically without any problem. It's also a good idea to keep a record of the channel number you use because some wireless clients can only manually select a channel number, and this would help when there's a radio communication problem.*

The available channel numbers for the following bands follow:

2.4GHz Band
The available channel numbers are 1 to 13 for European countries, 1 to 11 for the U.S.

5GHz Band
The available channel numbers are 36 to 140 (36-48, 52-64, 100-140) for European countries, and 36 to 48 and 149 to 165 for the U.S.

Associated Clients (5): *Click Show Active Clients. An Active Wireless Client Table will pop up. You can see the status of all active wireless stations that are connecting to the access point.*

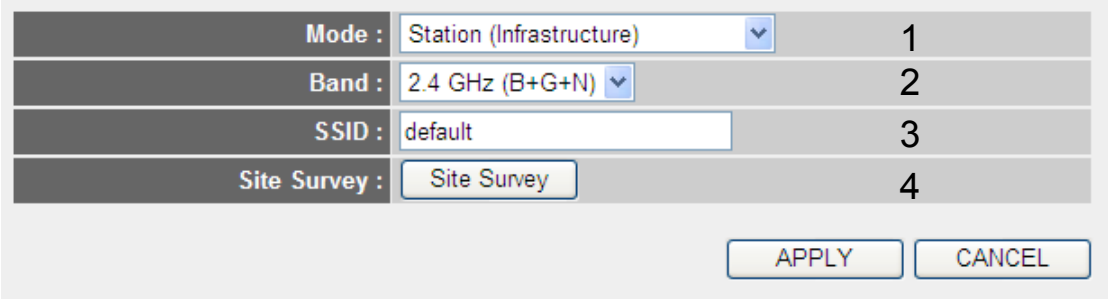
NOTE: If you don't have special reason to limit the type of allowed wireless client, it's recommended to choose 2.4GHz (B+G+N) and 5GHz (A+N+AC) to maximize wireless client compatibility.

TIPS: You can try to change the channel number to another one if you think the data transfer rate is too slow. There could be some other wireless routers using the same channel, which will disturb the radio communication between wireless clients and the wireless router.

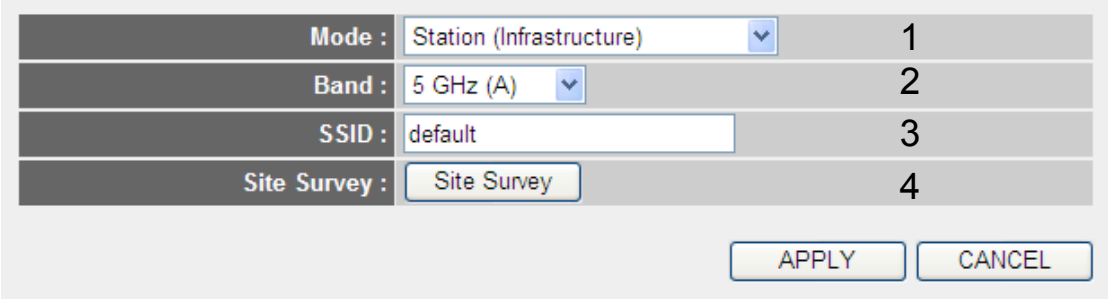
2-7-1-2 Setup procedure for Station-Infrastructure:

In this mode, you can connect the router to an Ethernet device such as a TV or game console to enable the Ethernet device to act as a wireless station and join to a wireless network through an access point or AP router.

2.4GHz Station (Infrastructure) Settings



5GHz Station (Infrastructure) Settings



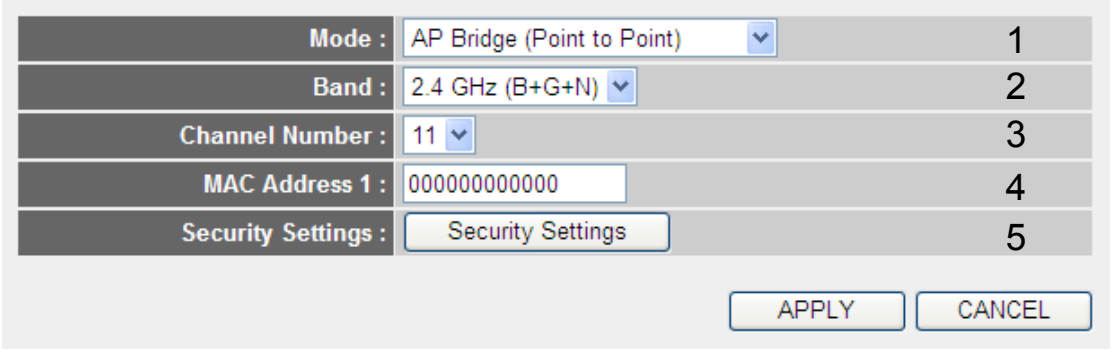
Here are descriptions of every setup item:

Band (2):	*Select the band you want to use.*
SSID (3):	*This is the name of the wireless network. You can type the SSID of the network you would like to connect to here.*
Site Survey (4):	*When you use this wireless router as a wireless station for an Ethernet network device to have wireless capability, you have to associate it with a working access point. Click Select Site Survey and a Wireless Site Survey Table will pop up. It will list all available access points nearby. You can select one access point in the table and it will join the wireless LAN through this access point.*

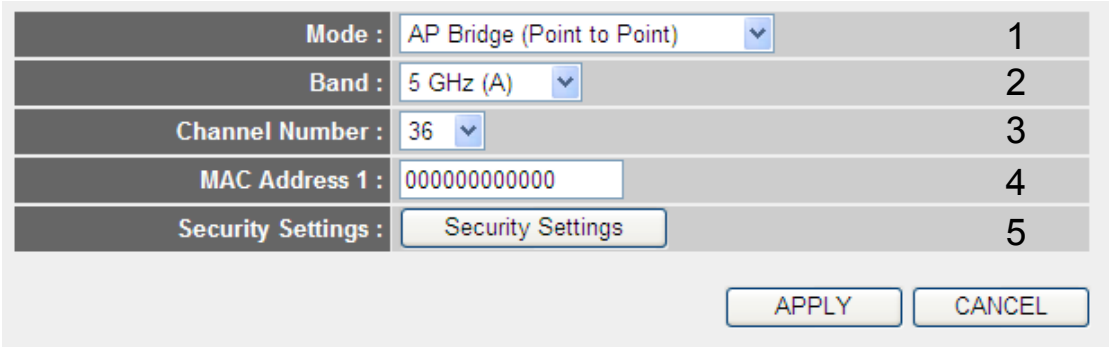
2-7-1-3 Setup procedure for AP Bridge-Point to Point:

In this mode, you can connect your wireless router with another to combine two access points and expand the scope of a wireless network, so all clients (wired only – AP will not accept wireless clients in this mode) will think they're on the same physical network. This function is very convenient when you need to connect two networks between two buildings. To connect two wireless routers together:

2.4GHz AP Bridge (Point to Point) Settings



5GHz AP Bridge (Point to Point) Settings



NOTE: Two wireless routers must use the same mode, band, channel number and security settings!

Here are descriptions of every setup item:

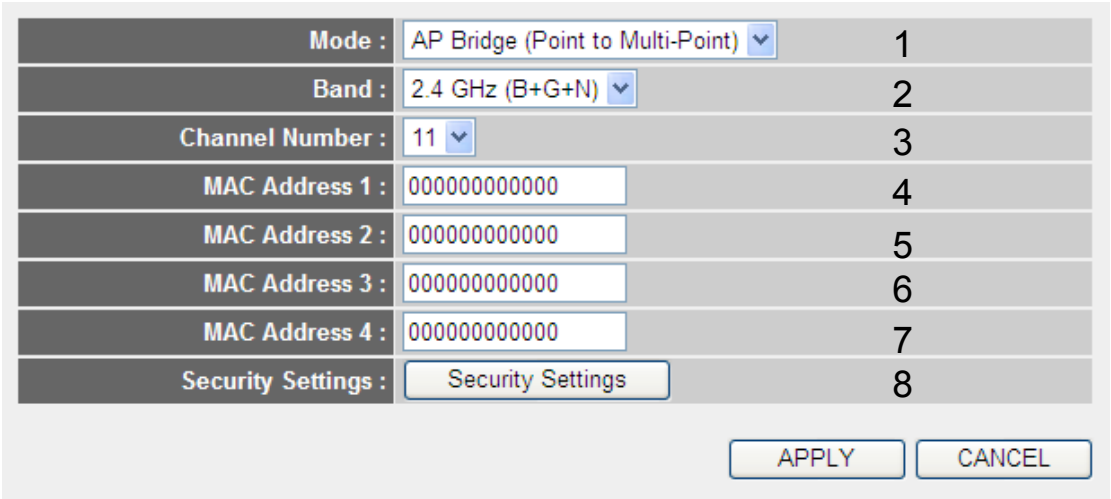
Band (2):	*Select the band you want to use; two wireless routers must use the same setting.*

Channel Number (3):	*Select the channel. Two wireless routers must use the same setting.*
MAC address 1 (4):	*Input the MAC address of another wireless router.*
Security Settings (5):	*Click to select the security for this connection (go to 2-7-3 Wireless Security for details).*

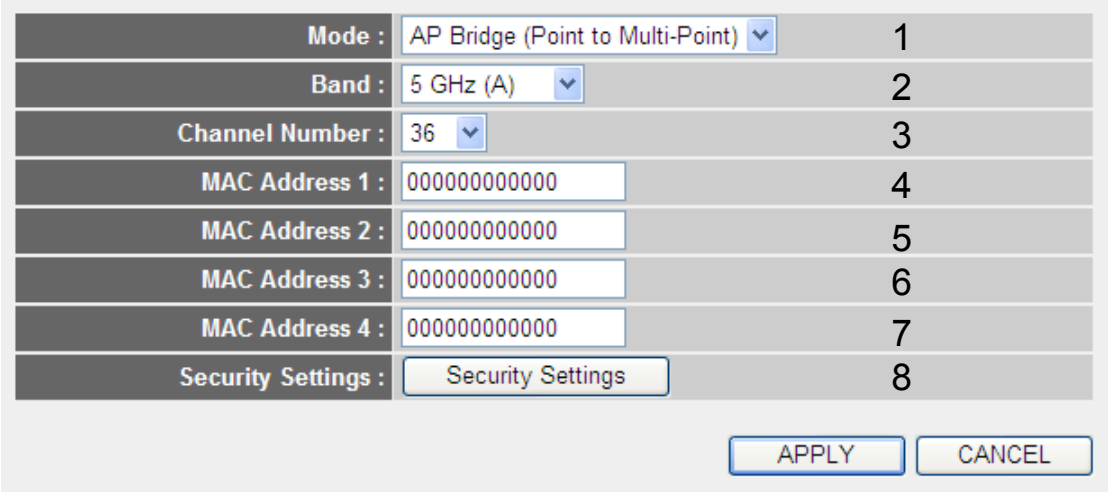
2-7-1-4 Setup procedure for AP Bridge-Point to Multi-Point:

In this mode, you can connect your wireless router with at least four wireless routers to expand the scope of a wireless network, and all clients (wired only – AP will not accept wireless clients in this mode) will think they're on the same physical network.

2.4GHz AP Bridge (Point to Multi-Point) Settings



5GHz AP Bridge (Point to Multi-Point) Settings



Here are descriptions of every setup item:

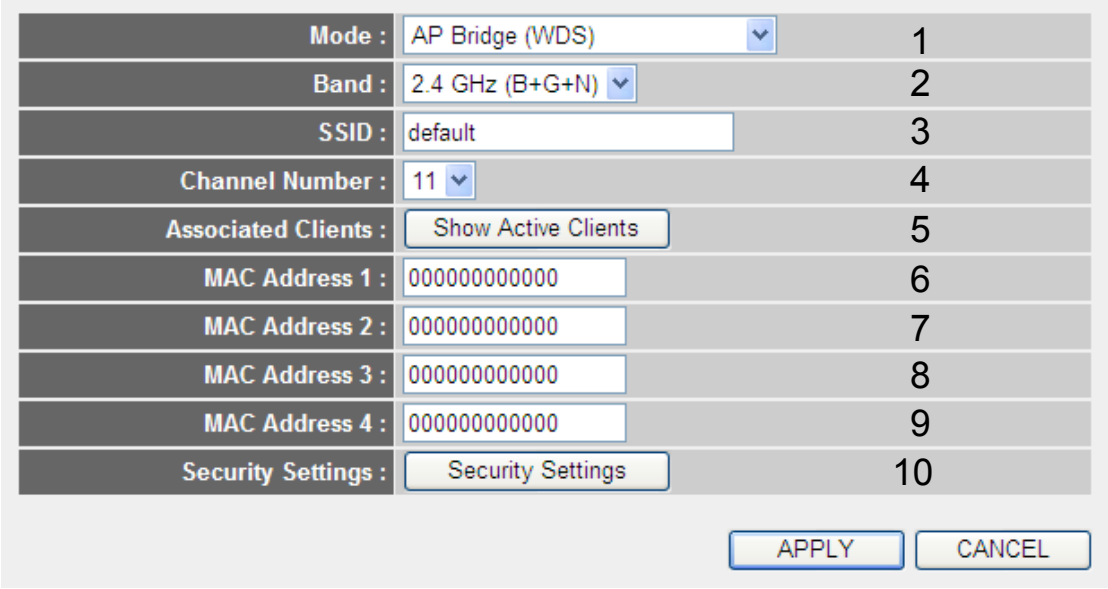
Band (2):	*Select the band you want to use; all the wireless routers must use the same setting.*
Channel Number (3):	*Select the channel you want to use (all the wireless routers must use the same setting).*
MAC address 1 to 4 (4-7):	*Input the MAC address of the other wireless routers.*
Security Setting (8):	*Click to set security settings for this connection (go to 2-7-3 Wireless Security for details).*

2-7-1-5 Setup procedure for AP Bridge – WDS

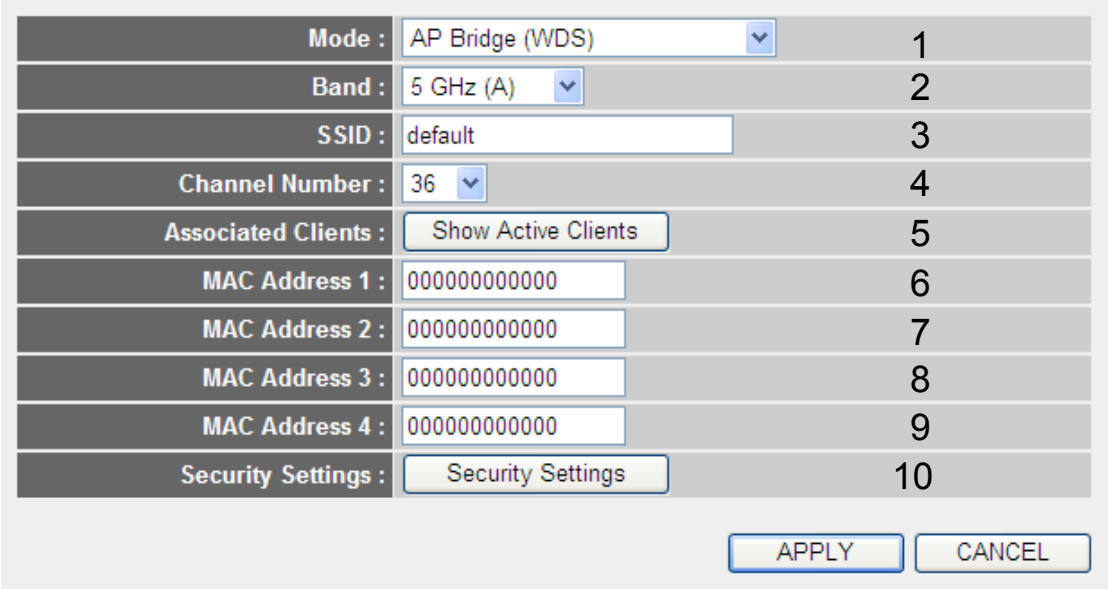
In this mode, you can expand the scope of a network by combining up to four other access points, and every access point can still accept wireless clients.

NOTE: For WDS mode, the output signal nature is the same as that of normal AP mode.

2.4GHz AP Bridge (WDS) Settings



5GHz AP Bridge (WDS) Settings



Here are descriptions of every setup item:

Band (2): *Select the band you want to use; all the wireless routers must use the same setting.*

SSID (3): *Input the SSID of your wireless router. The setting should be the same with other wireless routers for the convenience of roaming.*

Channel *Select the channel you want to use. All the*

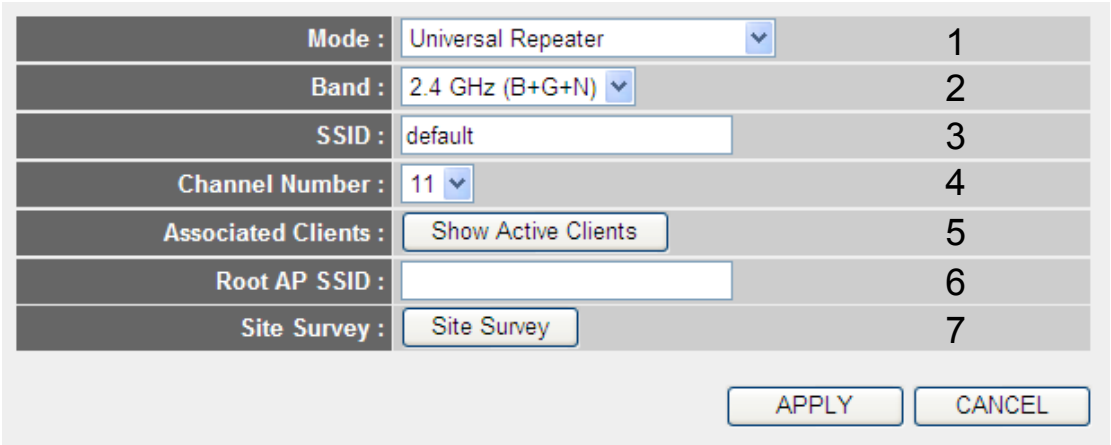
Number (4):	*wireless routers must use the same setting.*
Associated Clients (5):	*Click Show Active Clients. An Active Wireless Client Table will pop up. You can see the status of all active wireless stations that are connecting to the access point.*
MAC address 1 to 4 (6 - 9):	*Input the MAC address of the other wireless routers.*
Security Setting (10):	*Click to set security settings for this connection (go to 2-7-3 Wireless Security for details).*

2-7-1-6 Setup procedure for Universal Repeater

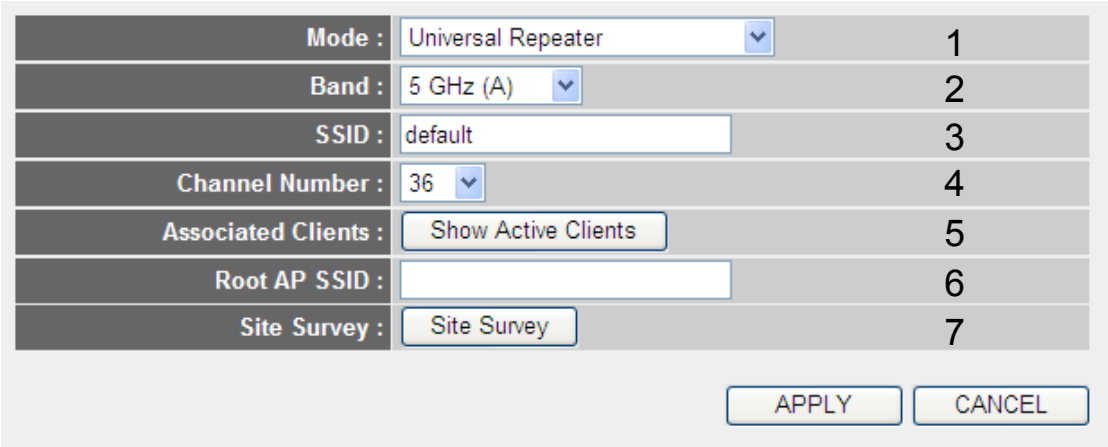
In this mode, the router can act as a wireless repeater — serving as a Station and AP at the same time. It can use the Station function to connect to a Root AP and use the AP function to service all wireless stations within its coverage.

NOTE: For Repeater Mode, this router will demodulate the received signal, checking if this signal is noise for the operating network, then have the signal modulated and amplified again. The output power of this mode is the same as that of WDS and normal AP mode.

2.4GHz Universal Repeater Settings



5GHz Universal Repeater Settings



Here are descriptions of every setup item:

Band (2): *Select the band you want to use. All the wireless routers must use the same setting.*

SSID (3): *This is the name of wireless router. You can enter up to 32 alphanumerical characters. The SSID is used to differentiate your own wireless router from others in the area. The default SSID is "default." It's recommended that you change the default SSID to the one that is meaningful to you, like myhome, office_room1, etc.*

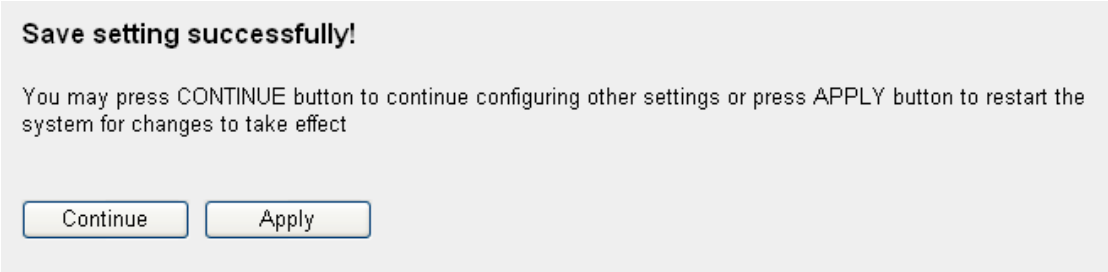
Channel Number (4): *Select a channel. All the wireless clients must use the same setting.*

Associated Clients (5): *Click Show Active Clients and Active Wireless Client Table will pop up. You can see the status of all active wireless stations that are connecting to the access point.*

Root AP SSID (6): *In Universal Repeater mode, this device can act as a station to connect to a Root AP. You should assign the SSID of the Root AP here or click Select Site Survey to choose a Root AP.*

Site Survey (7):	*Click Select Site Survey and Wireless Site Survey Table will pop up. It will list all available access points nearby. You can select one access point in the table and the router will join the wireless LAN through this access point.*

After you finish the wireless settings, click Apply and the following message will be displayed on your Web browser:

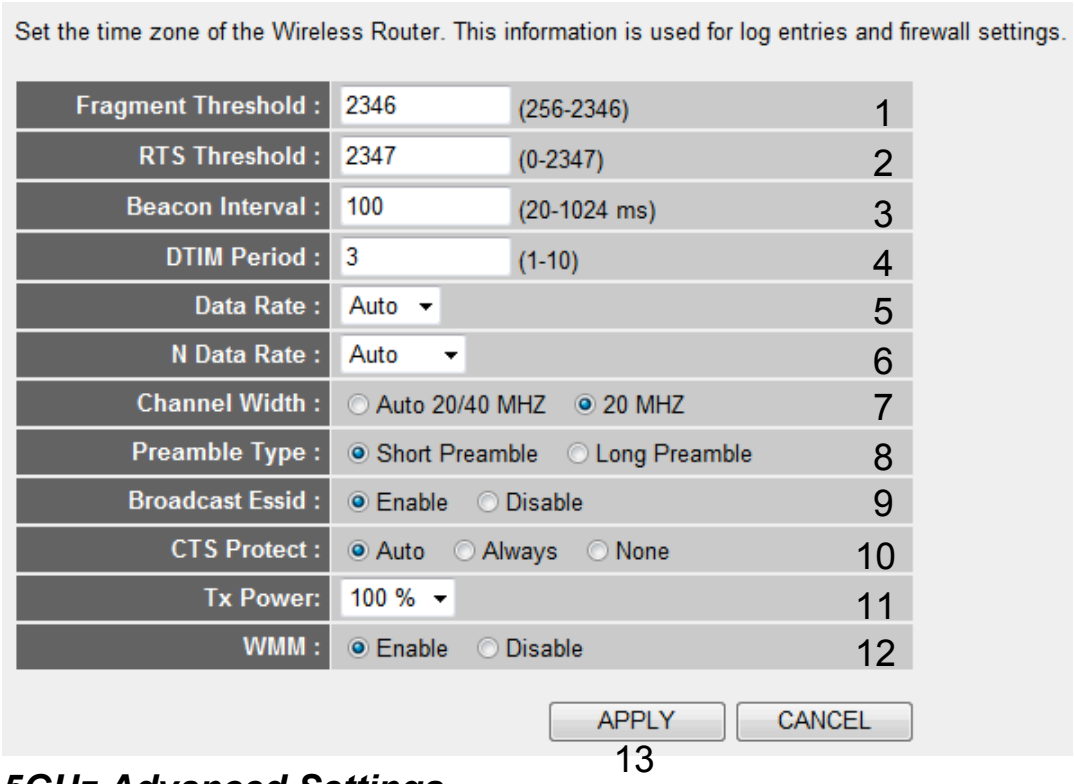


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

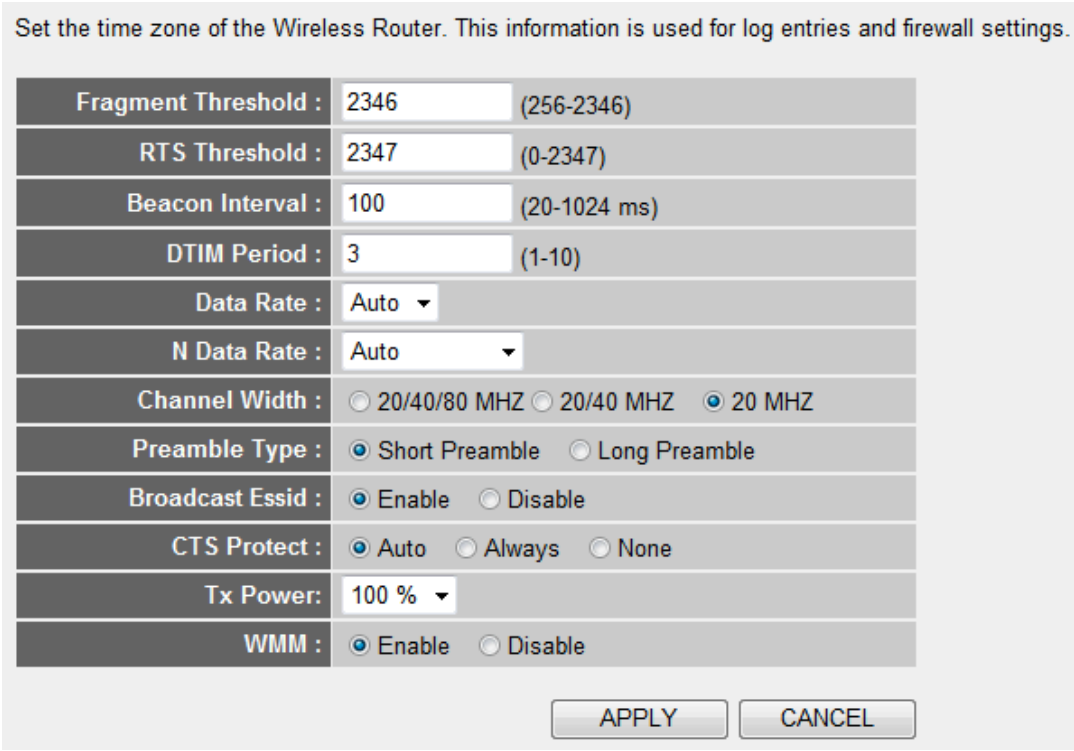
2-7-2 Advanced Wireless Settings

This router provides some advanced control of wireless parameters. To configure these settings, click 2.4GHz Wireless or 5GHz Wireless on the left side of the Web management interface, then click Advanced Settings. The corresponding screen will be displayed on your Web browser:

2.4GHz Advanced Settings



5GHz Advanced Settings



Here are descriptions of every setup item:

Fragment *Set the fragment threshold of the wireless radio.*

Threshold (1): ***Do not modify the default value if you don't know what it is.*** *The default value is 2346.*

RTS Threshold (2): *Set the RTS threshold of the wireless radio.* ***Do not modify the default value if you don't know what it is.*** *The default value is 2347.*

Beacon Interval (3): *Set the beacon interval of the wireless radio.* ***Do not modify default value if you don't know what it is.*** *The default value is 100.*

DTIM Period (4): *Set the DTIM period of the wireless radio.* ***Do not modify the default value if you don't know what it is.*** *The default value is 3.*

Data Rate (5): *Set the wireless data transfer. Since most wireless devices will negotiate with each other and pick a proper data transfer rate automatically,* ***it's not necessary to change this value unless you know what will happen after modification.***

N Data Rate (6): *Same as above, but only for 802.11n & 802.11ac clients.*

Channel Width (7): *Set the channel width of the wireless radio.* ***You can modify the default value if you know what channel width you need.*** *The default setting is 20 MHz.*

Preamble Type (8): *Set the type of preamble.* ***Do not modify the default value if you don't know what it is.*** *The default setting is Short Preamble.*

Broadcast ESSID (9): *Decide if the wireless router will broadcast its own ESSID or not. You can hide the ESSID of your wireless router (set the option to Disable) so only those who know the ESSID of your*

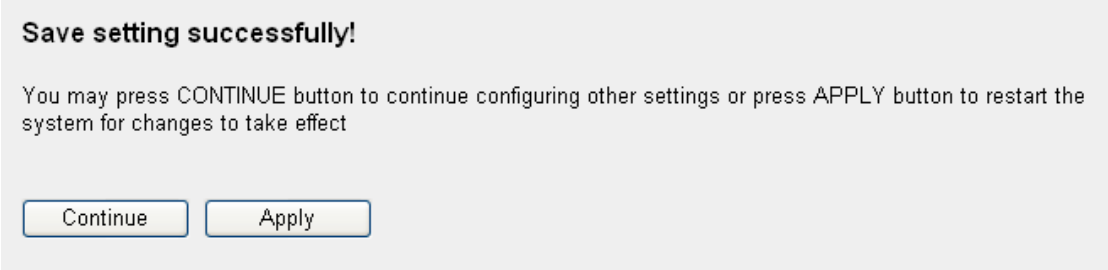
wireless router can connect.

CTS Protect (10): *Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g/n wireless access points. It's recommended to set this option to Auto or Always. However, if you set it to None, your wireless router should be able to work fine.*

Tx Power (11): *You can set the output power of the wireless radio. Unless you're using this router in a really big space, you may not have to set output power to 100%. This will enhance security (distant malicious / unknown users will not be able to reach your router).*

WMM (12): *Short for Wi-Fi MultiMedia, it will enhance the data transfer performance of multimedia contents when they're being transferred over a wireless network.* ***If you don't know what it is or aren't sure if you need it, it's safe to set this option to Enable.***

After you finish these wireless settings, click Apply and the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

2-7-3 Wireless Security

It's very important to set your wireless security settings properly! If you don't, hackers and malicious users can reach your network and valuable data without your consent, possibly causing serious security problems.

To set the wireless security settings, click 2.4GHz Wireless or 5GHz Wireless on the left side of the Web management interface, then click Security Settings and follow the instructions:

Select an encryption method from the Encryption drop-down menu. There are four options:

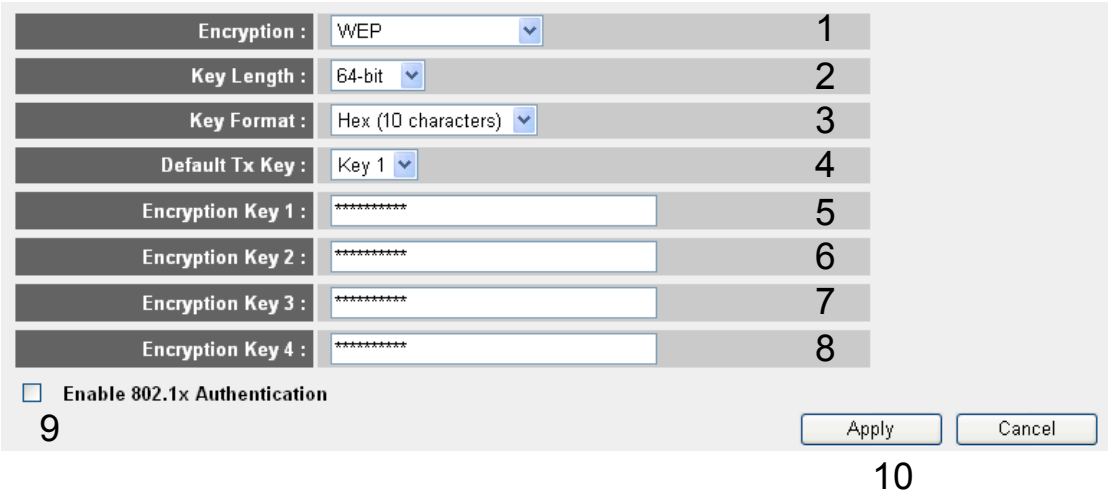
2-7-3-1 Disable wireless security

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect to your wireless router if no other security measure is enabled, such as MAC address access control. (See section 2-7-4, or disable Broadcast ESSID.)

Only use this option when you really want to allow everyone to use your wireless router and you don't care if there's someone reading the data you transfer over the network without your consent.

2-7-3-2 WEP — Wired Equivalent Privacy

When you select this mode, the wireless router will use WEP encryption, and the following setup menu will be shown on your Web browser:



Here are descriptions of every setup item:

Key Length (2): *There are two types of WEP key length: 64-bit and 128-bit. Using 128-bit is safer than 64-bit, but will reduce some data transfer performance.*

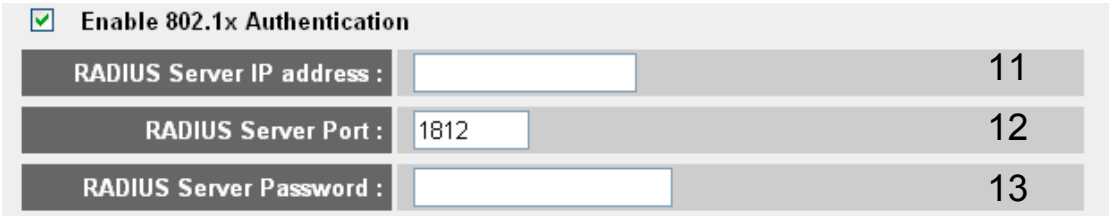
Key Format (3): *There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of key will be displayed. For example, if you select "64-bit" as the key length and "Hex" as the key format, you'll see the message at the right of Key Format is "Hex (10 characters)," which means the length of the WEP key is 10 characters.*

Default Tx Key (4): *You can set up to four sets of WEP keys, and you can decide which key is being used by default here.* ***If you don't know which one you should use, select "Key 1."***

Encryption Key 1 to 4 (5-8): *Input WEP key characters. The number of characters must be the same as the number displayed in the Key Format field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select "ASCII" key format; if you select "Hex," you can use characters 0-9, a-f, and A-F. You must enter at least one encryption*

key here, and if you entered multiple WEP keys, they should not be the same.

Enable 802.1x Authentication (9): *IEEE 802.1x is an authentication protocol. Every user must use a valid account to log in to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates a user by IEEE 802.1x, but it does not encrypt data during communication. If there is a RADIUS server in yoru environment, enable this function. Check this box and another sub-menu will appear:*



RADIUS Server IP address (11): *Input the IP address of the RADIUS server.*

RADIUS Server Port (12): *Input the port number of the RADIUS server.*

RADIUS Server Password (13): *Input the password for server access.*

TIPS: Some examples of WEP key (Don't use these; use your own!):

ASCII (5 characters): pilot, phone, 23561, 2Hyux, #@xmL

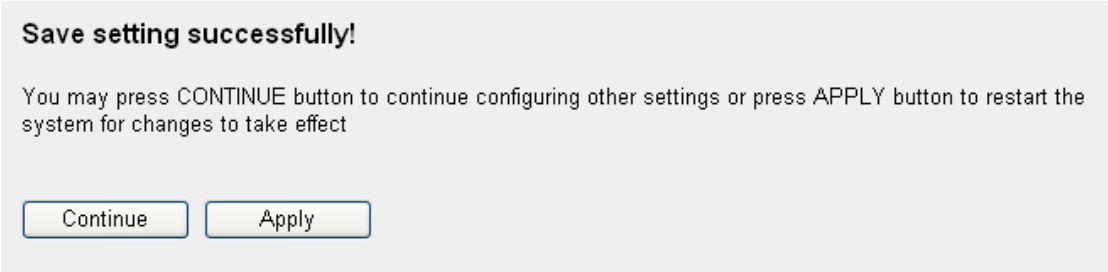
ASCII (13 characters): digitalFAMILY, 82Jh26xHy3m&n

Hex (10 characters): 287d2aa732, 1152dabc85

Hex (26 characters): 9284bcda8427c9e036f7abcd84

To improve security, don't use words that are in a dictionary or too easy to remember! Wireless clients will remember the WEP key and you only enter it once, so it's worth making it complicated in order to maximize security.

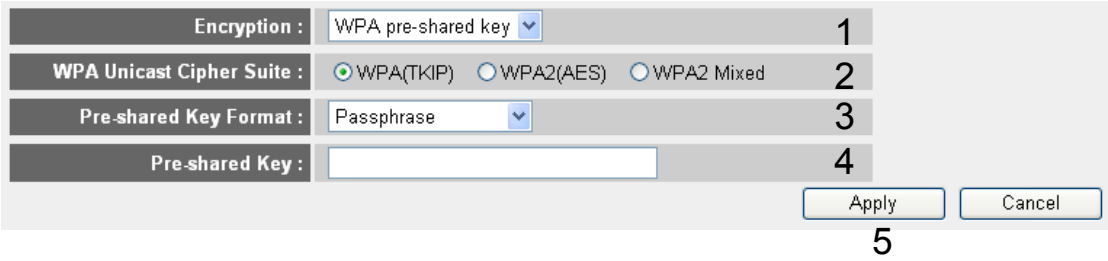
After you finish the WEP settings, click Apply (10). The following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

2-7-3-3 Wi-Fi Protected Access (WPA):

When you select this mode, the wireless router will use WPA encryption, and the following setup menu will be shown on your Web browser:

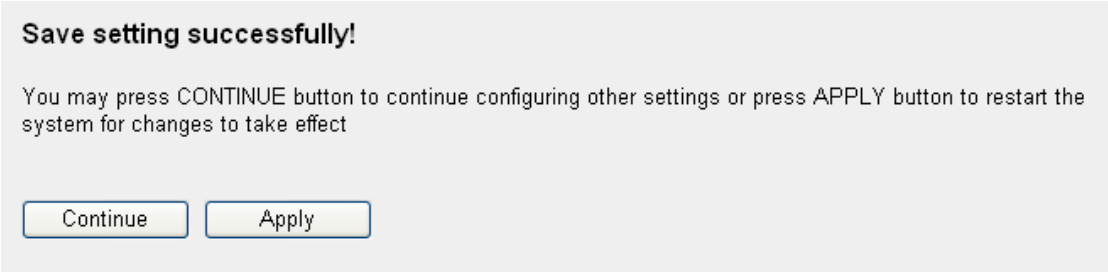


Here are descriptions of every setup item:

WPA Unicast Cipher Suite (2):	*Select a type of WPA cipher suite. Options are WPA (TKIP), WPA2 (AES) and WPA2 Mixed. You can select one of them, but you need to make sure your wireless client supports the cipher you select.*
Pre-shared	*Select the type of pre-shared key: Passphrase*

Key Format (3):	*(8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9, and a-f).*
Pre-shared Key (4):	*Input the WPA passphrase. For security, It's recommended that you not use a word that can be found in a dictionary.*

After you finish the WPA Pre-shared key settings, click Apply (5); the following message will be displayed on your Web browser:

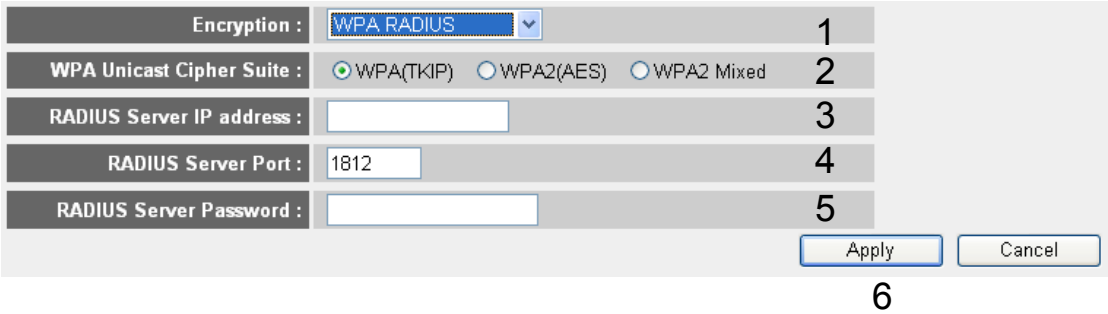


Click Continue to go back to the setup menu or to continue to router setup, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

NOTE: Some wireless clients (especially those manufactured before 2003) only support WEP or WPA (TKIP) ciphers. A driver upgrade would be needed for those clients to use WPA and WPA2 encryption.

2-7-3-4 WPA RADIUS:

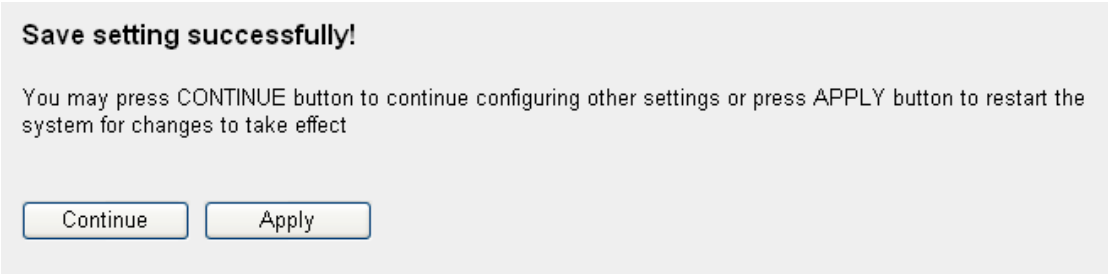
If you have a RADIUS server, this router can work with it and provide safer wireless authentication.



Here are descriptions of every setup item:

WPA Unicast Cipher Suite (2):	*Select a type of WPA cipher suite: WPA (TKIP), WPA2 (AES) or WPA2 Mixed. You can select one of them, but you need to make sure your wireless client supports the cipher you selected.*
RADIUS Server IP address (3):	*Input the IP address of your RADIUS authentication server.*
RADIUS Server Port (4):	*Input the port number of your RADIUS authentication server.* ***Default setting is 1812.***
RADIUS Server Password (5):	*Input the password of your RADIUS authentication server.*

After you finish with all settings, click Apply”(6); the following message will be displayed on your Web browser:

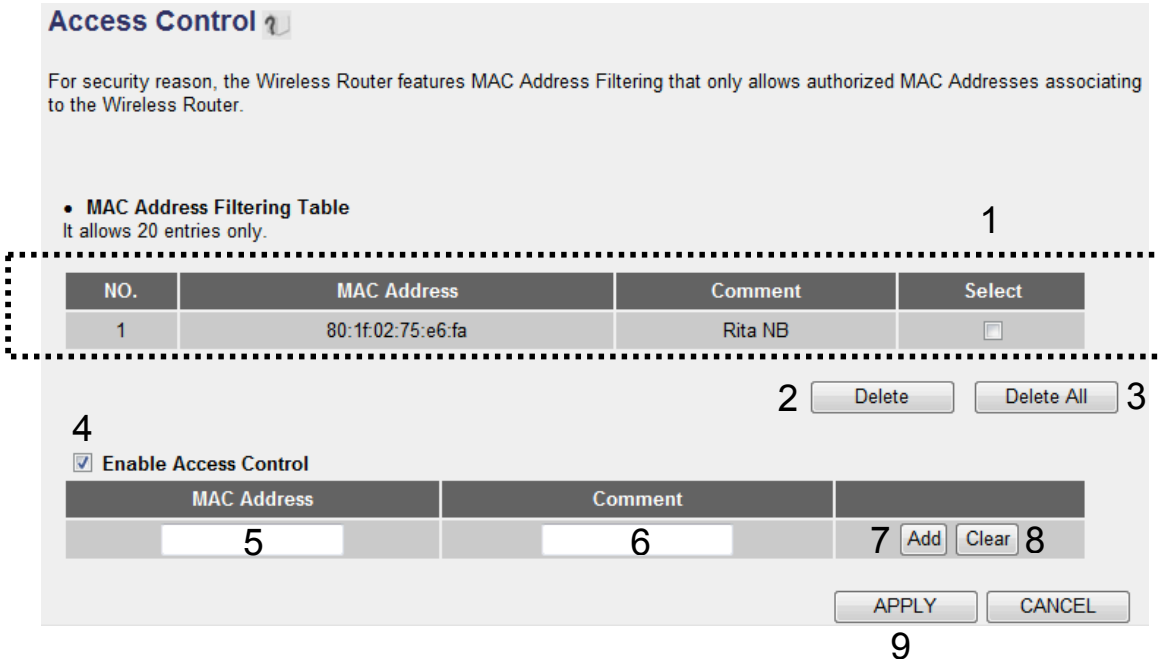


Click Continue to go back to the setup menu or to continue to router setup, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

2-7-4 Wireless Access Control

This function will help you prevent unauthorized users from connecting to your wireless router; only those wireless devices that have the MAC address you assign here can gain access to your wireless router. You can use this function with other security measures described in previous sections to create an even safer wireless environment.

Up to 20 MAC addresses can be assigned by using this function. Click “2.4GHz Wireless” or “5GHz Wireless” on the left side of the Web management interface, then click “Access Control.” The following message will be displayed on your Web browser:



All allowed MAC addresses will be displayed in the MAC Address Filtering Table (1).

Here are descriptions of every setup item:

Delete Selected (2):	*To delete a specific MAC address entry, check the Select box of the MAC address you want to delete, then click Delete Selected. (You can select more than one MAC address.)*
Delete All (3):	*If you decide to delete all MAC addresses listed here, click Delete All.*
Enable Access Control (4):	*To enforce MAC address filtering, you need to check “Enable Wireless Access Control.” When this item is unchecked, the wireless router will not enforce MAC address filtering.*

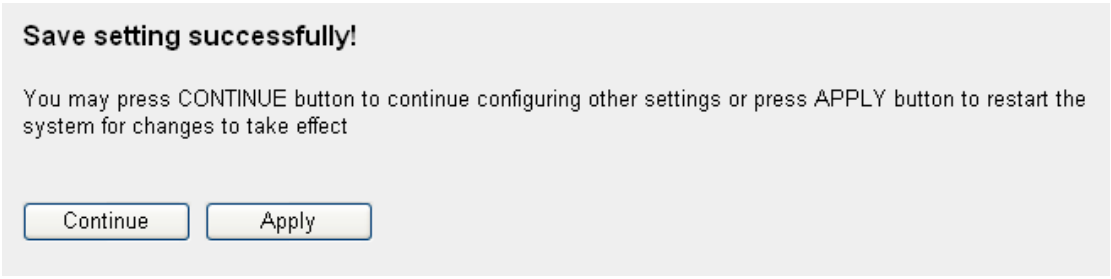
MAC Address (5): *Input the MAC address of your wireless devices. Note: dashes (-) and colons (:) are not required; i.e., if the MAC address label of your wireless device reads "aa-bb-cc-dd-ee-ff" or "aa:bb:cc:dd:ee:ff," just input "aabbccddeeff."*

Comment (6): *You can input any text here to comment on or define this MAC address, such as "AndyS." You can input up to 16 alphanumerical characters. This is optional and you can leave it blank; however, it's recommended you use this field to write a comment for every MAC address as a memory aid.*

Add (7): *Click Add to add the MAC address and any associated comment to the MAC address filtering table.*

Clear (8): *Click Clear to remove the value you entered in the MAC address and comment field.*

After you finish with all settings, click Apply (9); the following message will be displayed on your Web browser:



Click Continue to go back to the setup menu or to continue to router setup, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

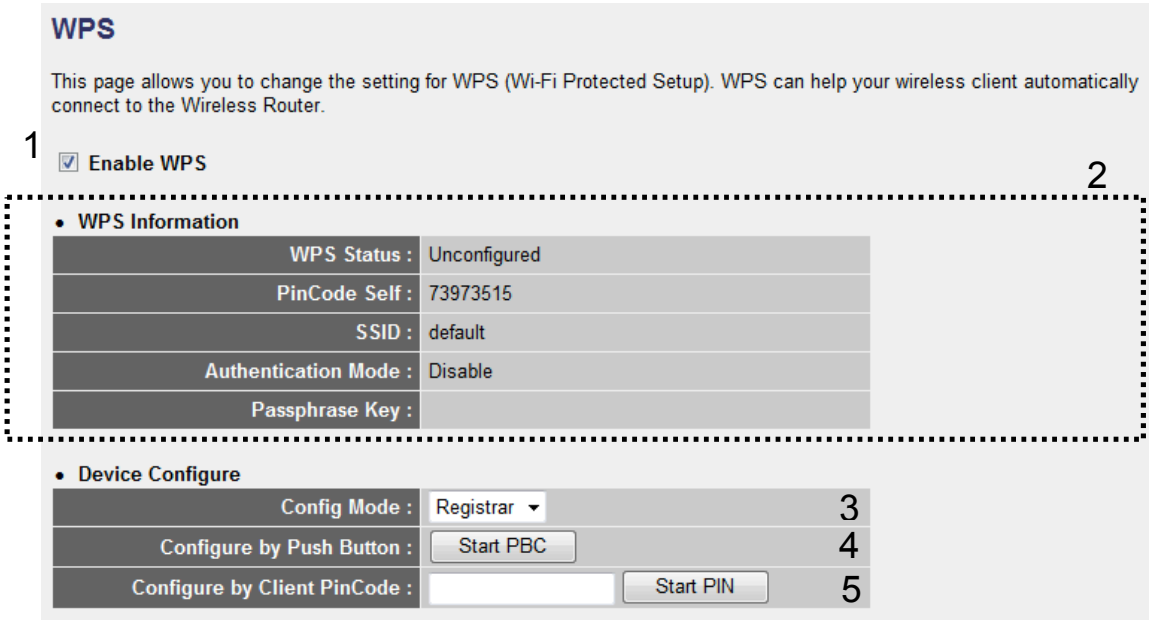
To reset all settings on this screen back to previously saved values, click Cancel.

2-7-5 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is the simplest way to build a connection between wireless network clients and this wireless router. You don't have to select an encryption mode or input a long encryption passphrase every time you need to set up a wireless client; you only have to press a button on the wireless client and this wireless router, and WPS will do the rest for you.

This wireless router supports two types of WPS: Push-Button Configuration (PBC) and PIN Code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode and switch this wireless router to WPS mode, too. You can push the Reset/WPS button of this wireless router, or click "Start PBC" in the Web management interface to do this; if you want to use PIN Code, you have to know the PIN code of the wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you want to connect to this wireless router. The detailed instructions follow.

Click 2.4GHz Wireless or 5GHz Wireless on the left side of the Web management interface, then click WPS; the following message will be displayed on your Web browser:



Here are descriptions of every setup item:

Enable WPS (1): *Check this box to enable the WPS function; uncheck it to disable WPS.*

WPS Information (2): *WPS-related system information will be displayed here:*

WPS Status: If the wireless security (encryption) function of this wireless router is properly set, you'll see a "Configured" message here. If the wireless security function has not been set, you'll see "unConfigured."

PinCode Self: This is the WPS PIN code of this wireless router. This code is useful when you need to build a wireless connection by WPS with other WPS-enabled wireless devices.

SSID: The SSID of this wireless router will be displayed here.

Authentication Mode: The wireless security authentication mode of this wireless router will be displayed here. If you don't enablethe security function of the wireless router before WPS is activated, the router will auto-set the security to WPA (AES) and generate a set of passphrase keys for WPS connection.

Passphrase Key: The wireless security key of the router will be displayed here.

Config Mode (3): *There are Registrar and Enrollee modes for the WPS connection. When Registrar is enabled, the wireless clients will follow the router's wireless settings for WPS connection. When*

	Enrollee mode is enabled, the router will follow the wireless settings of the wireless client for WPS connection.
Configure by Push-Button (4):	*Click Start PBC to start the Push-Button type of WPS setup. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The WLAN LED on the wireless router will light for 2 minutes when this wireless router is waiting for incoming WPS requests.*
Configure by Client Pin Code (5):	*Input the PIN code of the wireless client you wanth to connect to, and click Start PIN. The WLAN LED on the wireless router will light when this wireless router is waiting for incoming WPS requests.*

2-7-6 Security Tips for the Wireless Network

Here are some quick tips to help you improve the security level of your wireless network:

1. Never use simple words (like school, apple and computer) for WEP encryption or WPA passphrases.

2. A complicated (combination of numbers, letters or symbols and long) WEP key and WPA passphrase are much safer than simple and short ones. Remember that the wireless client is capable of keeping the key or passphrase for you, so you only need to input the complicated key or passphrase once. It’s not too much trouble, and will greatly improve the security level.

3. You can hide the ESSID of this router by setting the Broadcast ESSID option to Disable. Your wireless router will not be found by other people in proximity if they’re just using the AP scanning function of their wireless device, and this can reduce the chance of being hacked.

4. Use the Access Control function described in section 2-7-4 so those people who are not on your list will not be able to connect to your network.

Chapter III Advanced Functions

3-1 Quality of Service (QoS)

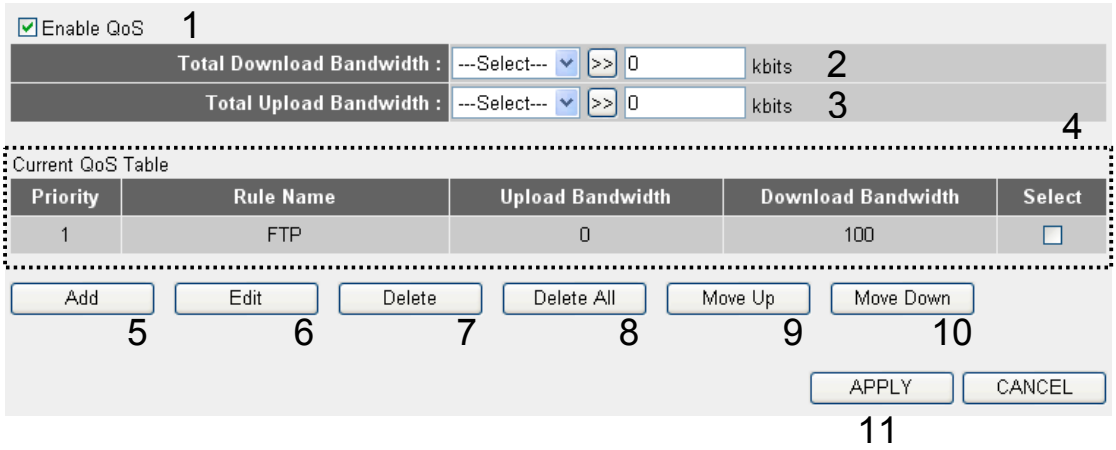
Quality of service provides an efficient way for computers on the network to share the Internet bandwidth with a promised quality of Internet service. Without QoS, all computers and devices on the network will compete with each other for Internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephones) will be affected, resulting, for example, in the interruption of video/audio transfer.

With this function, you can limit the maximum bandwidth or give a guaranteed bandwidth for a specific computer to avoid such problems.

3-1-1 Basic QoS Settings

To set QoS parameters:

Click QoS on the left side of the Web management interface; the following message will be displayed on your Web browser:



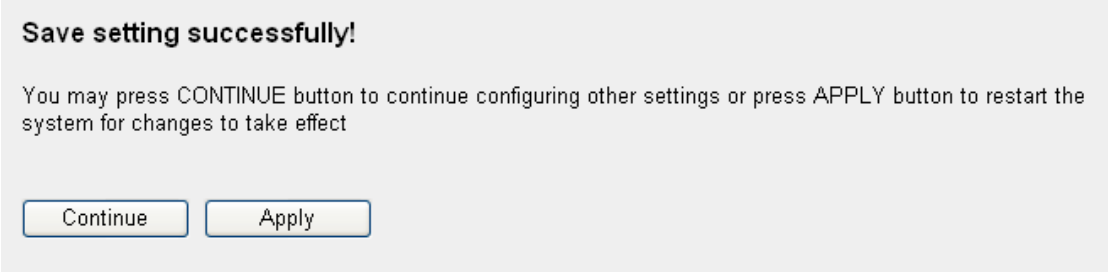
Here are descriptions of every setting:

Enable QoS (1):	*Check this box to enable the QoS function; unselect this box if you don't want to enforce QoS bandwidth limitations.*
Total Download Bandwidth (2):	*You can set the limit of the total download bandwidth in kbits. To disable the download bandwidth limitation, input "0" here.*
Total Upload Bandwidth (3):	*You can set the limit of the total upload bandwidth in kbits. To disable the upload bandwidth limitation, input "0" here.*
Current QoS Table (4):	*All existing QoS rules will be displayed here.*
Add (5):	*Click Add to add a new QoS rule (see section 3-1-2 Add a New QoS Rule).*
Edit (6):	*To modify the content of a specific rule, check the "Select" box of the rule you want to edit, then click Edit.* ***Only one rule should be selected t aa time!*** *If you didn't select a rule before clicking Edit, you'll be prompted to add a new rule.*
Delete (7):	*You can delete selected rules by clicking Delete. You can select one or more rules to delete by checking the Select box of the rule(s) you want to delete.* ***If the QoS table is empty, this button will be grayed out and can not be clicked.***
Delete All (8):	*By clicking Delete All, you can delete all rules currently in the QoS table.* ***If the QoS table is empty, this button will be grayed out and can not be clicked.***

Move Up (9): *You can pull up the priority of the QoS rule you selected by clicking this button.*

Move Down (10): *You can lower the priority of the QoS rule you selected by clicking this button.*

After you finish with all settings, click Apply (11); the following message will be displayed on your Web browser:

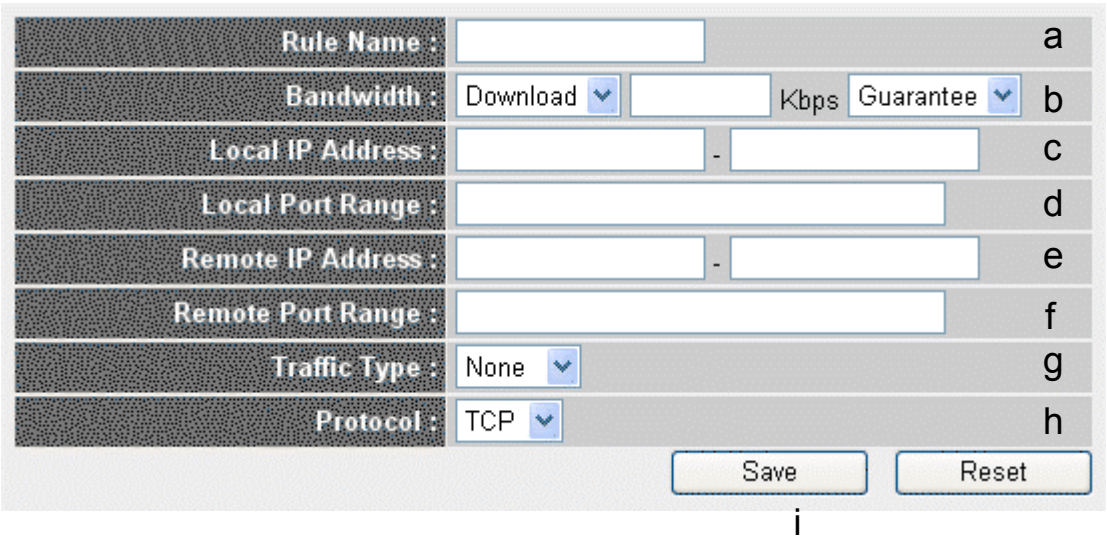


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

If you want to reset all settings on this screen back to previously saved values, click Cancel.

3-1-2 Add a new QoS rule

After you click Add in the QoS menu, the following message will appear:



Here are descriptions of every setup item:

Rule Name (a): *Assign a name to this QoS rule (up to 15 alphanumerical characters).*

Bandwidth (b): *Set the bandwidth limitation of this QoS rule. You have to select the data direction of this rule (Upload or Download) and the speed of the bandwidth limitation in kbps, then select the type of QoS: 'guarantee' (guaranteed usable bandwidth for this rule) or 'max' (set the maximum bandwidth for the application allowed by this rule).*

Local IP Address (c): *Specify the local (source) IP address that will affected by this rule. Input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.*

Local Port Range (d): *Input the range of the local (source) port numbers that will be affected by this rule. If you want to apply this rule on Ports 80 to 90 input "80-90"; to apply this rule to a single port, just input the port number, like "80."*

Remote IP Address: (e):	*Specify the remote (destination) IP address that will be affected by this rule. Input the starting IP address in the left field and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.*
Remote Port Range (f):	*Input the range of remote (destination) port numbers that will be affected by this rule. If you want to apply this rule on Ports 80 to 90, input "80-90"; to apply this rule on a single port, just input the port number, like "80." If the remote (destination) IP address and /or port number is universal, just leave this blank.*
Traffic Type (g):	*Select the traffic type of this rule: None, SMTP, HTTP, POP3 and FTP. You can select a specific traffic type for this rule: If you want to make this rule an IP address-based rule (apply the limitation on all traffic to/from the specified IP address / port number), select None.*
Protocol (h):	*Select the protocol type for this rule: TCP or UDP. If you don't know what protocol your application uses, try TCP first, and switch to UDP if this rule doesn't seem to work.*

After you finish with all settings, click Save (i). You'll be brought back to the previous menu, and the rule you just set will appear in the current QoS table. If any settings were incorrect, you'll get an error message when you click Save: Correct your input per the instructions given by the error message.

If you decide to erase all values you just entered, click Reset.

3-2 Network Address Translation (NAT)

Network address translations solve the problem of sharing a single IP address to multiple computers. Without NAT, all computers must be assigned a valid Internet IP address to get connected to the Internet, but Internet service providers provide very few IP addresses to each user. Therefore, it's necessary to use NAT technology to share a single Internet IP address among multiple computers on a local network,so everyone can get connected to the Internet.

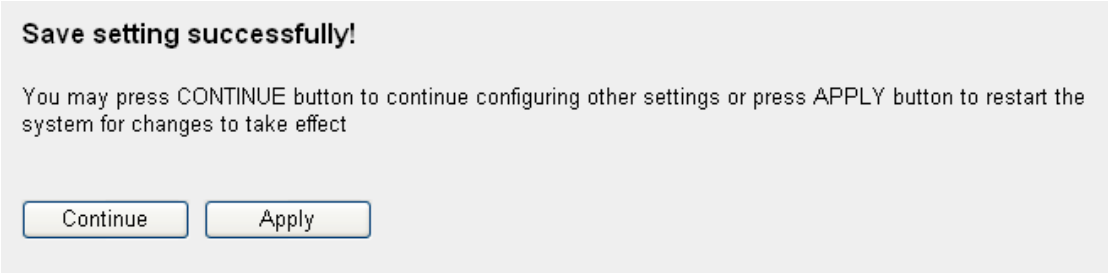
To set NAT parameters:

3-2-1 Basic NAT Settings (Enable or disable NAT function)

Click NAT on the left side of the Web management interface; the following message will be displayed on your Web browser:

To enable the NAT function, select "Enable" for "Enable NAT module function" (1); to disable, select "Disable."

After you make the selection, click Apply (2); the following message will be displayed on your Web browser:

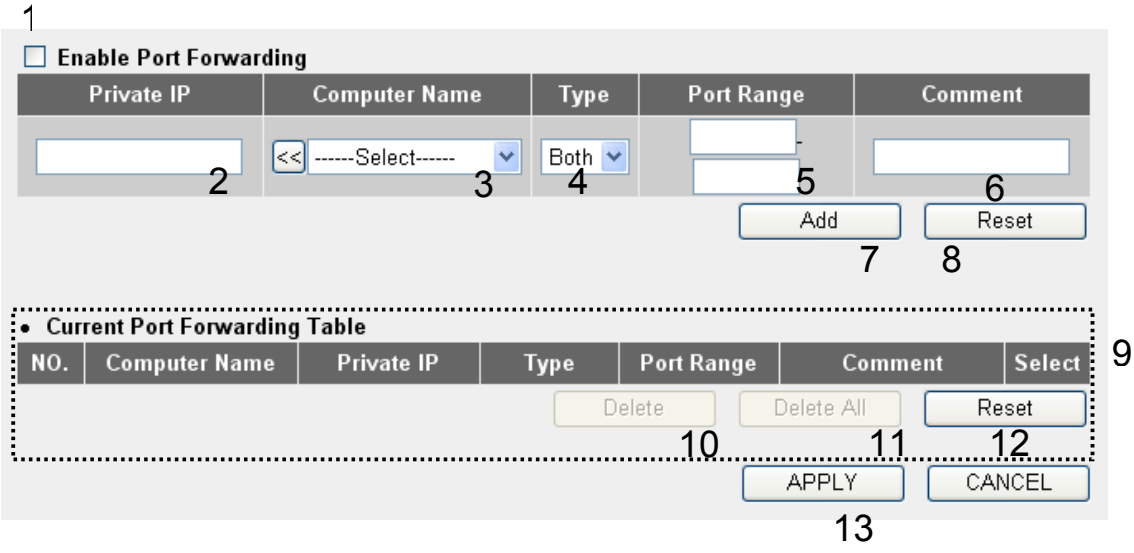


Click Continue to go back to the setup menu or to continue to other setup procedures, or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while router is rebooting).

3-2-2 Port Forwarding

This function allows you to redirect a single port or consecutive ports of an Internet IP address to the same port of the IP address on a local network. The port number(s) of an Internet IP address and private IP address (the IP address on a local network) must be the same. If the port numbers of an Internet IP address and private IP address are different, use the Virtual Server function, described in next section.

Click NAT on the left side of the Web management interface, then click Port Forwarding; the following message will be displayed on your Web browser:

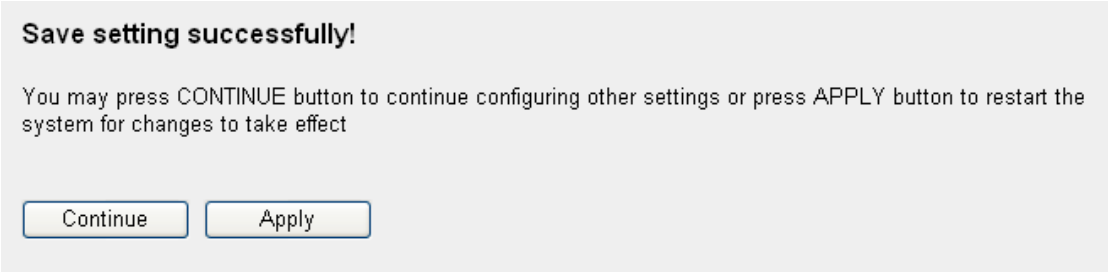


Here are descriptions of every setup item:

Enable Port Forwarding (1):	*Check this box to enable port mapping; uncheck this box to disable port mapping.*
Private IP (2):	*Input the IP address of the computer on the local network that provides Internet service.*
Computer Name (3):	*Pull down the menu and all the computers connected to the router will be listed here. You can easily select the computer name without checking the IP address of the computer.*
Type (4):	*Select the type of connection: TCP or UDP. If you're not sure, select "Both."*
Port Range (5):	*Input the starting port number in the left field, and input the ending port number in the right field. To redirect a single port number, just enter the port number in the left field.*
Comment (6):	*Input any text to describe this mapping, up to 16 alphanumerical characters.*
Add (7):	*Add the mapping to the Port Forwarding table.*
Reset (8):	*Remove all inputted values.*
Port Forwarding Table (9):	*All existing port forwarding mappings will be displayed here.*
Delete (10):	*Select a port forwarding mapping by checking the "Select" box of the mappin option, then click Delete Selected to remove the mapping. If there's no existing mapping, this option will be grayed out.*
Delete All (11):	*Delete all mappings the in Virtual Server table.*

Reset (12): *Unselect all mappings.*

After you finish with all settings, click Apply (13); the following message will be displayed on your Web browser:



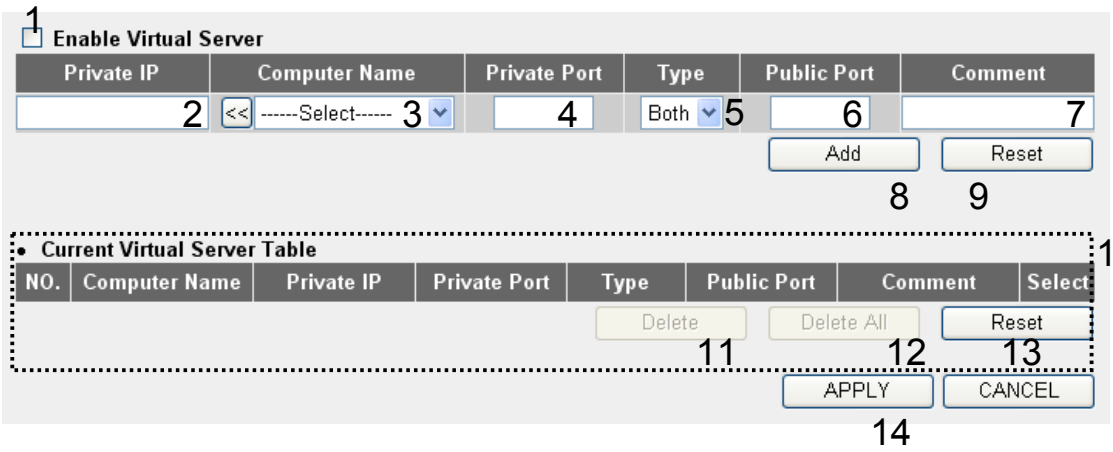
Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-2-3 Virtual Server

This function allows you to redirect a port of the Internet IP address (on WAN port) to a specified port of an IP address on the local network, so you can set up an Internet service on the computer on the local network without exposing it on the Internet directly. You can also build many sets of port redirection to provide many different Internet services on different local computers via a single Internet IP address.

Click NAT on the left side of the Web management interface, then click Virtual Server; the following message will be displayed on your Web browser:

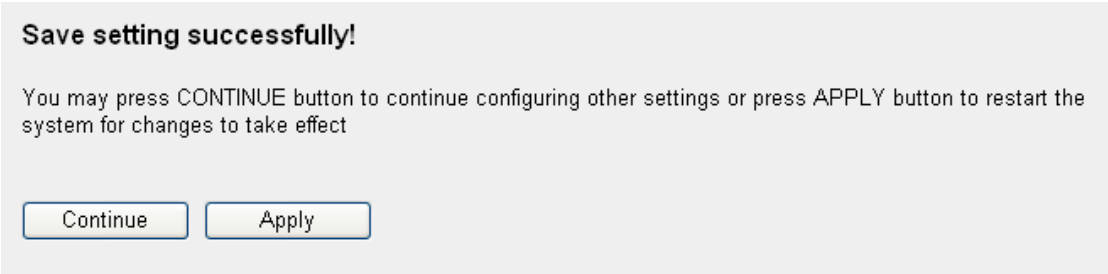


Here are descriptions of every setup item:

Enable Virtual Server (1):	*Check this box to enable the virtual server uncheck to disable the virtual server.*
Private IP (2):	*Input the IP address of the computer that provides Internet service.*
Computer Name (3):	*Pull down the menu and all the computers connected to the router will be listed here. You can easily select the computer name without checking the IP address of the computer.*
Private Port (4):	*Input the port number of the IP address that provides Internet service.*
Type (5):	*Select the type of connection: TCP or UDP. If you're not sure, select "Both."*
Public Port (6):	*Select the port number of the Internet IP address that will be redirected to the port number of the local IP address defined above.*
Comment (7):	*Input any text to describe this mapping, up to 16 alphanumerical characters.*
Add (8):	*Add the mapping to the Virtual Server table.*

Reset (9):	*Remove all inputted values.*
Virtual Server Table (10):	*All existing virtual server mappings will be displayed here.*
Delete (11):	*Select a virtual server mapping by clicking the "Select" box of the mapping, then click Delete Selected to remove the mapping. If there's no existing mapping, this option will be grayed out.*
Delete All (12):	*Delete all mappings in the Virtual Server table.*
Reset (13):	*Unselect all mappings.*

After you finish with all the settings, click Apply (14); the following message will be displayed on your Web browser:

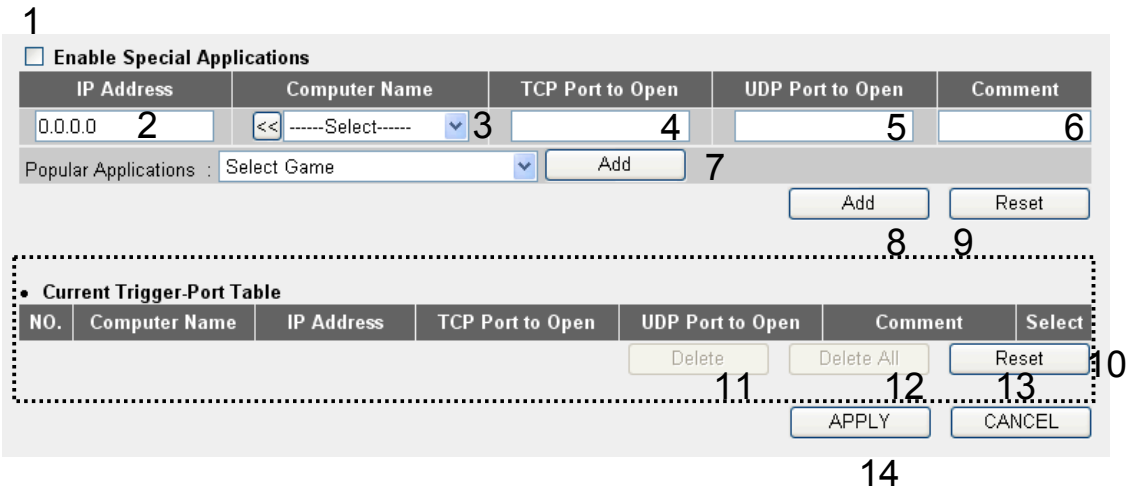


Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-2-4 Port Mapping for Special Applications

Some applications require more than one connection at a time; these applications won't work with simple NAT rules. In order to make these applications work, you can use this function to let these applications work.



Here are descriptions of every setup item:

Enable (1): *Check this box to enable special applications; uncheck to disable the virtual server.*

IP Address (2): *Input the IP address of the computer which you want to open the ports.*

Computer Name (3): *Pull down the menu and all the computers connected to the router will be listed here. You can easily select the computer name without checking the IP address of the computer.*

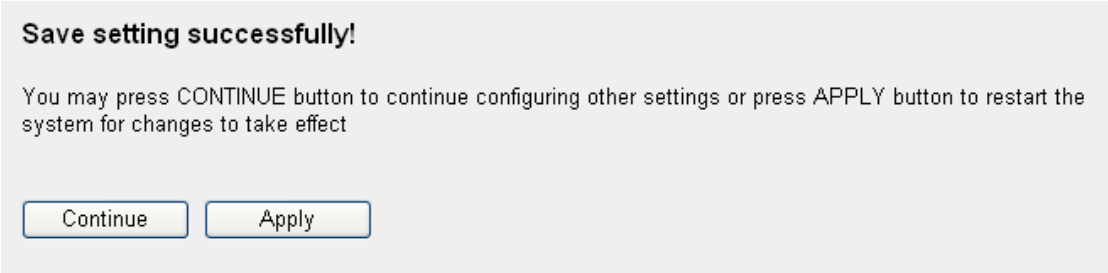
TCP Port to Open (4): *This is the outgoing (Outbound) range of TCP port numbers for this particular application.*

UDP Port to Open (5): *This is the outgoing (Outbound) range of UDP port numbers for this particular application.*

Comment (6):	*The description of this setting.*
Popular Applications (7):	*This section lists the more popular applications that require multiple connections. Select an application and click Add to save the setting to the Current Trigger-Port Table.*
Add (8):	*Add the setting to the Current Trigger-Port Table.*
Reset (9):	*Click Reset to clear all above settings (and can set agai, if needed).*
Current Trigger-Port (10):	*All the settings for the special applications will be listed here. If you want to remove some Special Application settings from the Current Trigger-Port Table, select the Special Application settings you want to remove in the table and click Delete Selected. To remove all Special Application settings from the table, just click Delete All. Click Reset to clear your current selections.*
Delete (11):	*Select a special application by clicking the "Select" box of the mapping, then click Delete Selected to remove the setting. If there's no setting here, this option will be grayed out.*
Delete All (12):	*Delete all settings existed in trigger port table.*
Reset (13):	*Unselect all settings.*

Note: Only one LAN client can use a particular special application at a time.

After you finish with all settings, click Apply (14); the following message will be displayed on your Web browser:



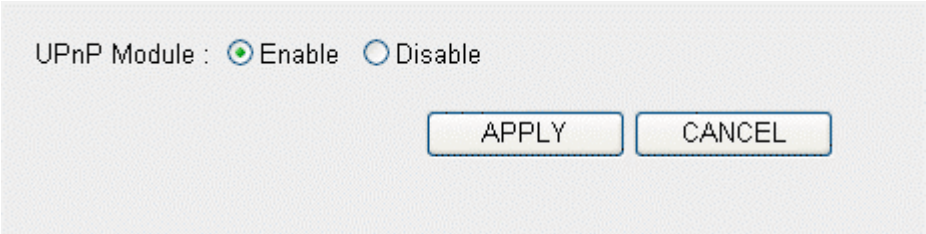
Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

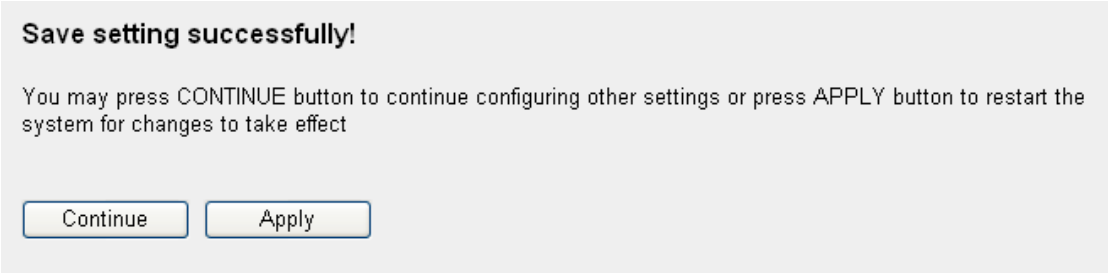
3-2-5 UPnP Setting

This function enables network auto-configuration for peer-to-peer communications. Network devices will be able to communicate with other devices directly and “learn” about other devices. Many network devices and applications rely on the UPnP function.

Click NAT on the left side of the Web management interface, then click UPnP; the following message will be displayed on your Web browser:



There is only one option on this screen: Select “Enable” or “Disable” to enable or disable UPnP function, then click Apply; the following message will be displayed on your Web browser:



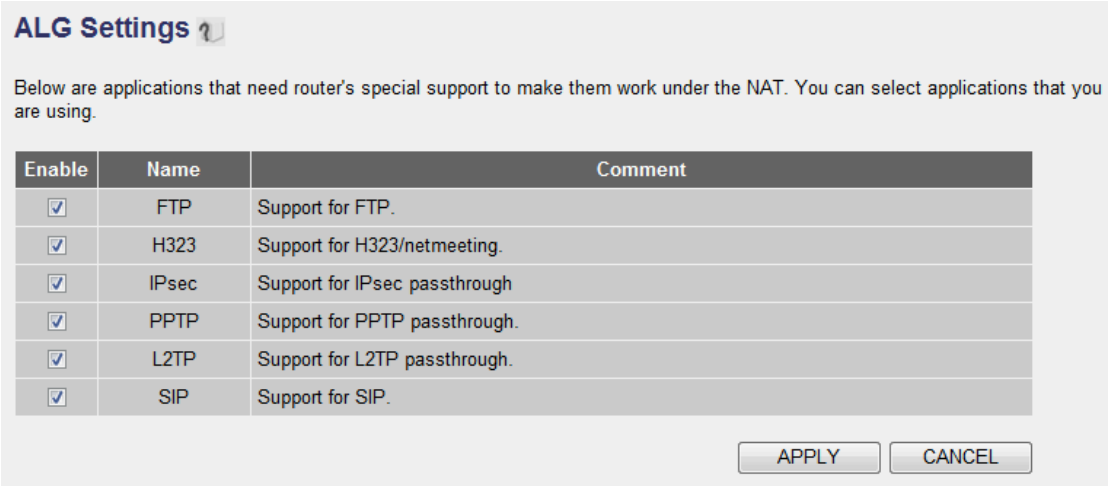
Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-2-6 ALG Settings

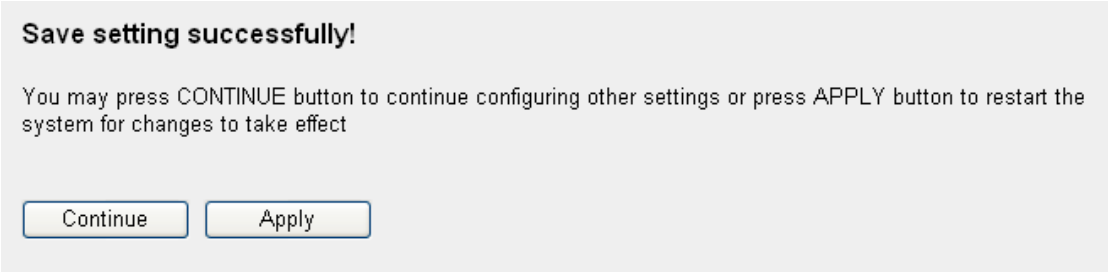
Application Layer Gateway (ALG) is a special function of this router. It includes many preset routing rules for numerous applications that require special support. With these supports, those applications will be able to work with NAT architecture.

Click NAT on the left side of the Web management interface, then click ALG Settings; the following message will be displayed on your Web browser:



There are many applications listed here. Check the box of the

special support for applications you need, then click Apply; the following message will be displayed on your Web browser:



Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

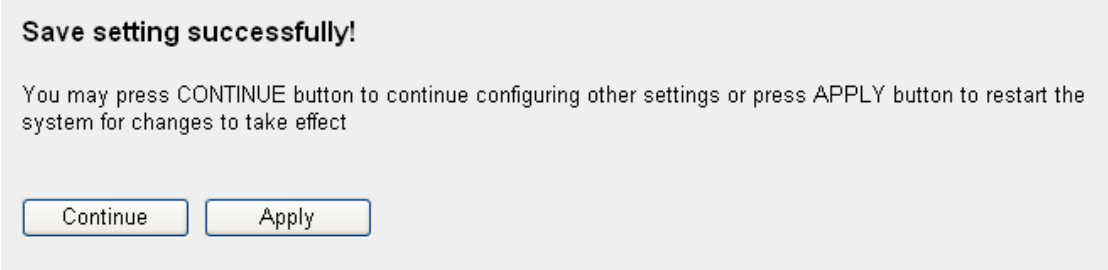
If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-3 Firewall

This router also provides a firewall function to block malicious intruders from accessing your computers on the local network. These functions include inbound attack prevention and blocking outbound traffic (like blocking URLs with pre-defined keywords).

Click Firewall on the left side of the Web management interface; the following message will be displayed on your Web browser:

Select “Enable” or “Disable” to enable or disable the firewall function. Then click Apply; the following message will be displayed on your Web browser:

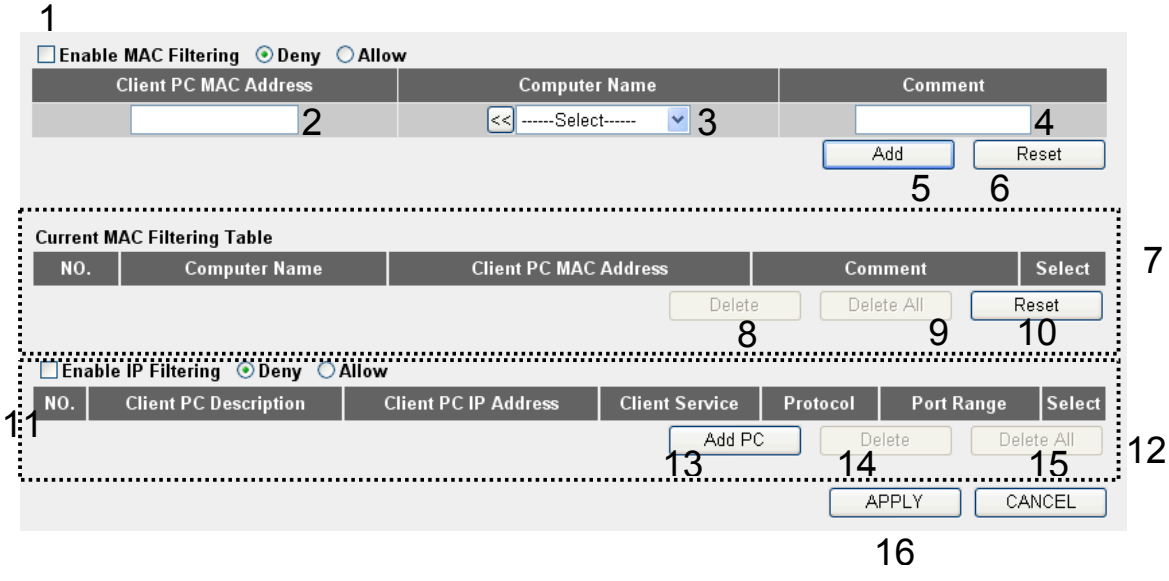


Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

3-3-1 Access Control

This function allows or denies computers with specific MAC address from connecting to the network. It can also allow or deny computers with specific IP addresses, protocols or ports.

Click Firewall on the left side of the Web management interface, then click Access Control; the following message will be displayed on your Web browser:



Here are descriptions of every setup item:

Enable MAC Filtering (1):	*Check this box to enable MAC address-based filtering, and select "Deny" or "Allow" to decide the behavior of the MAC filtering table. If you select "Deny," all MAC addresses listed in the filtering table will be prevented from connecting to the network; if you select "Allow," only MAC addresses listed in the filtering table will be able to connect to the network, rejecting all other network devices.*
Client PC MAC address (2):	*Input the MAC address of computer or network devices here. Dashes (-) and colons (:) are not required (i.e., if the MAC address label of your wireless device indicates "aa-bb-cc-dd-ee-ff" or "aa:bb:cc:dd:ee:ff," just input "aabbccddeeff."*
Computer Name (3):	*Pull down the menu and all the computers connected to the router will be listed here. You can select the computer name without checking the IP address of the computer.*
Comment (4):	*You can input any text here as to comment on this MAC address, like "ROOM 2A Computer." You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank; however, it's recommended that you use this field to write a comment for every MAC addresses as a memory aid.*
Add (5):	*Click "Add" to add the MAC address and associated comment to the MAC address filtering table.*

Reset (6): *Remove all inputted values.*

Current MAC Filtering Table (7): *All existing MAC addresses in the filtering table will be listed here.*

Delete (8): *If you want to delete a specific MAC address entry, check the "select" box of the MAC address you want to delete, then click "Delete Selected." (You can select more than one MAC address.)*

Delete All (9): *If you want to delete all MAC addresses listed here, click "Delete All."*

Reset (10): *You can also click "Reset" to unselect all MAC addresses.*

Enable IP Filtering (11): *Check this box to enable IP address-based filtering, and select "Deny" or "Allow" to determine the behavior of the IP filtering table. If you select "Deny," all IP addresses listed in the filtering table will be prevented from connecting to the network; if you select "Allow," only IP addresses listed in the filtering table will be able to connect to the network, rejecting all other network devices.*

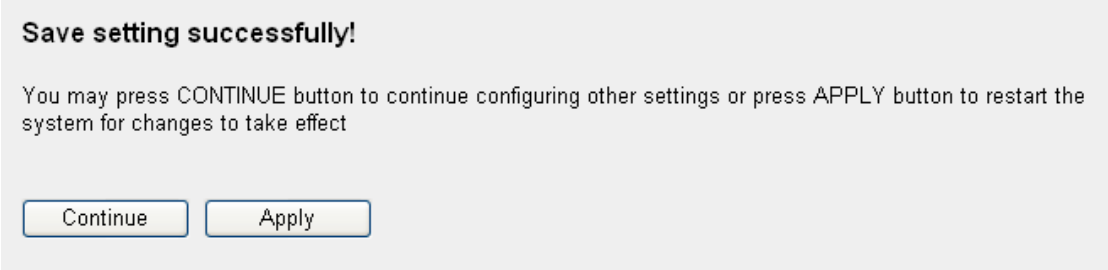
IP Filtering Table (12): *All existing IP addresses in the filtering table will be listed here.*

Add PC (13): *Click to add a new IP address to the IP filtering table. Up to 20 IP addresses can be added. Refer to section 3-3-1-1 "Add PC" below.*

Delete (14): *If you want to delete a specific IP address entry, check the "Select" box of the IP address you want to delete, then click "Delete Selected." (You can select more than one IP address.)*

Delete All (15): *If you want to delete all IP addresses listed here, click "Delete All."*

After you finish with all settings, click Apply (16); the following message will be displayed on your Web browser:

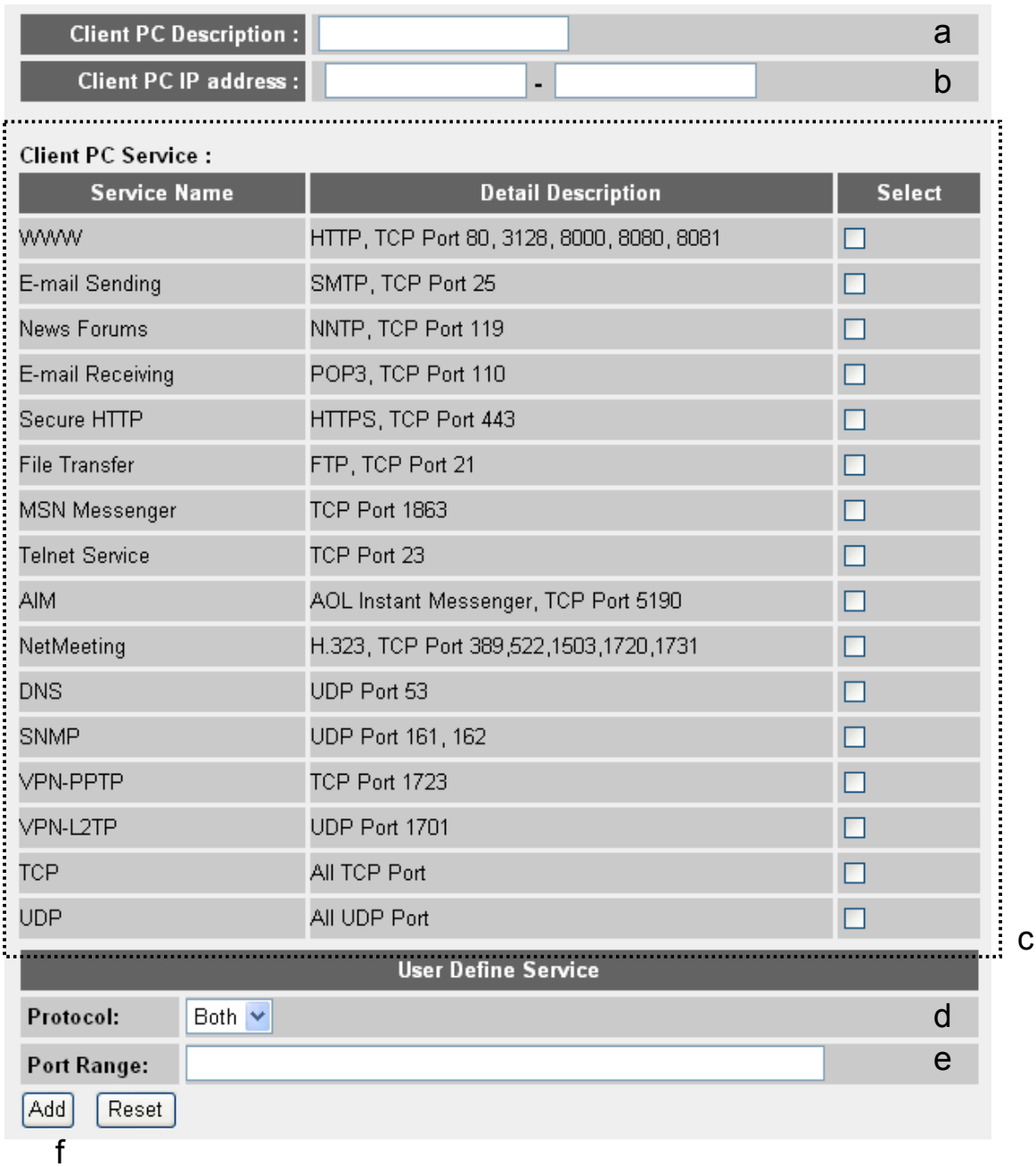


Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-3-1-1 Add PC

After this is clicked, the following message will be displayed on your Web browser:



Here are descriptions of every setup item:

Client PC Description (a):	*Input any text to describe this IP address, up to 16 alphanumerical characters. Input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.*
Client PC IP address (b):	

Client PC Service (c):	*Check all the services you want to allow or deny this IP address to use. You can check multiple services.*
Protocol (d):	*If the service you need is not listed above, you can create a new service on your own. Select "TCP" or "UDP." If you're not sure, select "Both."*
Port Range (e):	*Input the port range of the new service here. If you want to specify Ports 80 to 90, input "80-90"; if you want to apply this rule on a single port, just input the port number, like "80."*
Add (f):	*When you finish with all settings, click Add to save the settings. You'll be brought back to the previous menu, and the rule you just set will appear in the current IP filtering table.*

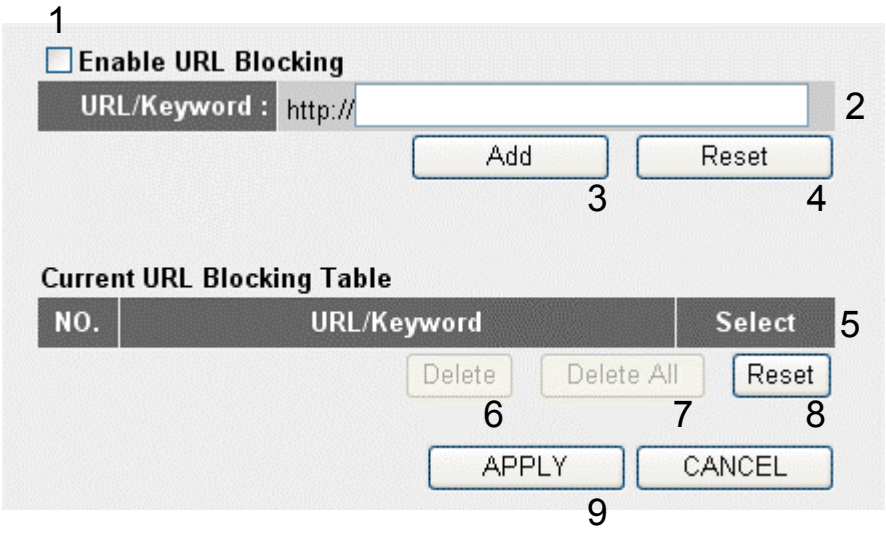
If you want to remove all settings on this screen, click "Reset."

3-3-2 URL Blocking

If you want to prevent computers in local network from accessing certain websites (like pornography, violence or anything you want to block), you can use this function to stop computers in the local network from accessing the sites you define here.

This function is useful for parents and company managers.

Click Firewall on the left side of th Web management interface, then click URL Blocking; the following message will be displayed on your Web browser:



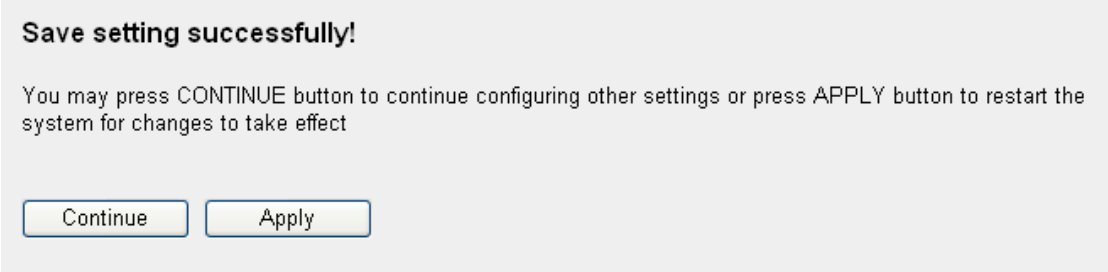
Here are descriptions of every setup item:

Enable URL Blocking (1):	*Check this box to enforce URL Blocking; uncheck it to disable URL Blocking.*
URL/Keyword (2):	*Input the URL (host name or IP address of website, like http://www.blocked-site.com or http://11.22.33.44), or the keyword which is contained in the URL (like pornography, cartoon, stock or anything).*
Add (3):	*Click Add to add the URL / keyword to the URL / Keyword filtering table.*
Reset (4):	*Click Reset to remove the value you inputted in the URL/Keyword field.*
Current URL Blocking Table (5):	*All existing URL/Keywords in the filtering table will be listed here.*
Delete (6):	*If you want to delete a specific URL/Keyword entry, check the "Select" box of the MAC address you want to delete, then click Delete Selected. (You can select more than one MAC address.)*

Delete All (7): *If you want to delete all URLs/Keywords listed here, click Delete All.*

Reset (8): *You can also click Reset to unselect all URLs/Keywords.*

After you finish with all settings, click Apply (9); the following message will be displayed on your Web browser:



Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

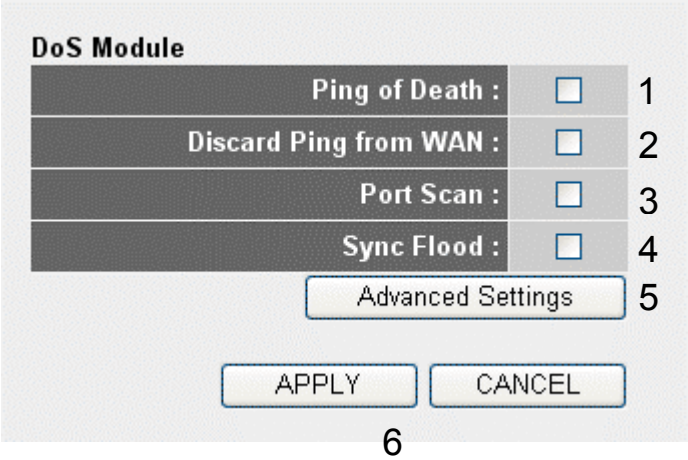
If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-3-3 DoS Attack Prevention

Denial of Service (DoS) is a common attack measure: If someone were to transmit a great amount of data or requests to your Internet IP address and server, the Internet connection will become very slow, and the server may stop responding because it is not able to handle that much traffic.

This router has a built-in DoS attack prevention mechanism: When you activate it, the router will stop the DoS attack for you.

Click Firewall on the left side of the Web management interface, then click DoS; the following message will be displayed on your Web browser:



Here are descriptions of every setup item:

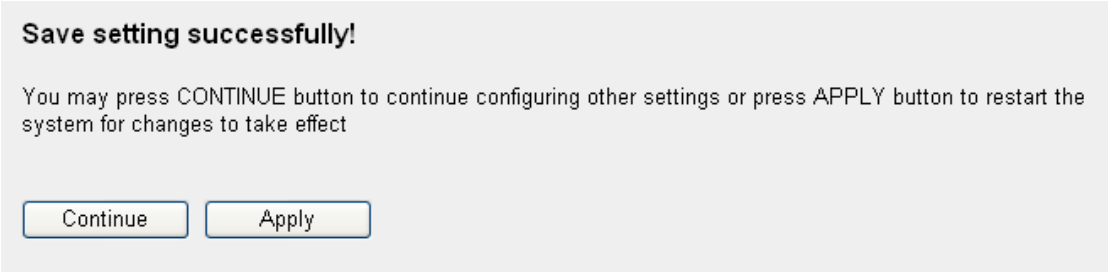
Ping of Death (1): *Ping of Death is a special packet, and it will cause certain computers to stop responding. Check this box and the router will filter this kind of packet out.*

Discard Ping From WAN (2): *Ping is a common and useful tool to find out the connection status of a specified remote network device, but some malicious intruder could try to fill your network bandwidth with a lot of Ping-request data packets to make your Internet connection become very slow, even unusable. Check this box and the router will ignore all inbound Ping requests; but when you activate this function, you will not be able to ping your own router from the Internet.*

Port Scan (3): *Some malicious intruder could try to use a port scanner to learn how many ports of your Internet IP address are open, and they can collect a lot of valuable information by doing so. Check this box and the router will block all*

	traffic that is trying to scan your Internet IP address.
Sync Flood (4):	*This is another kind of attack. It uses a lot of fake connection requests to consume the memory of your server and make your server unusable. Check this box and the router will filter this kind of traffic out.*
Advanced Settings (5):	*Click this button and you can set advanced settings of the DoS prevention method listed above. See section 3-3-3-1 DoS – Advanced Settings below.*

After you finish with all settings, click Apply (6); the following message will be displayed on your Web browser:

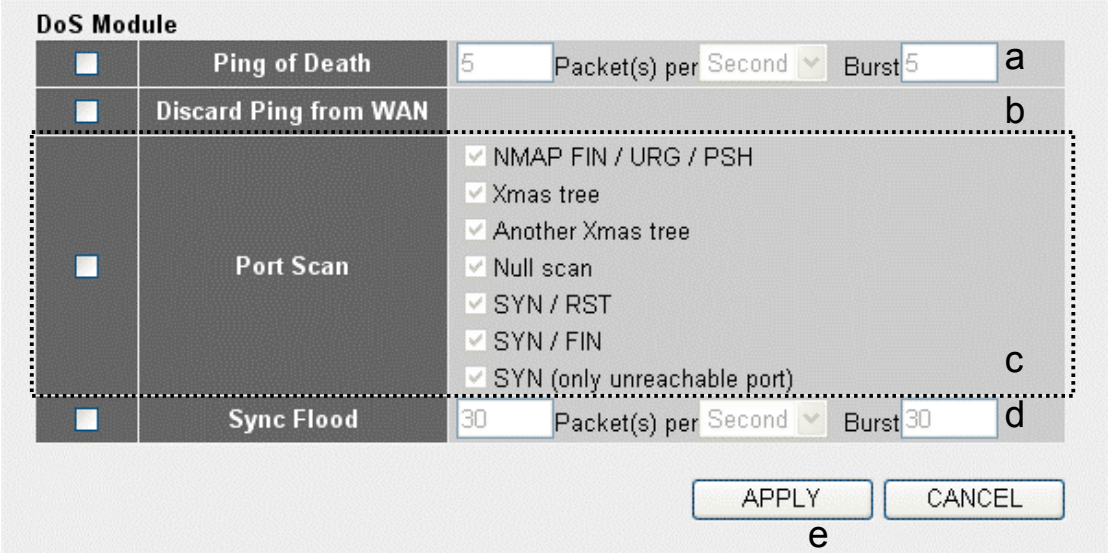


Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-3-3-1 DoS - Advanced Settings

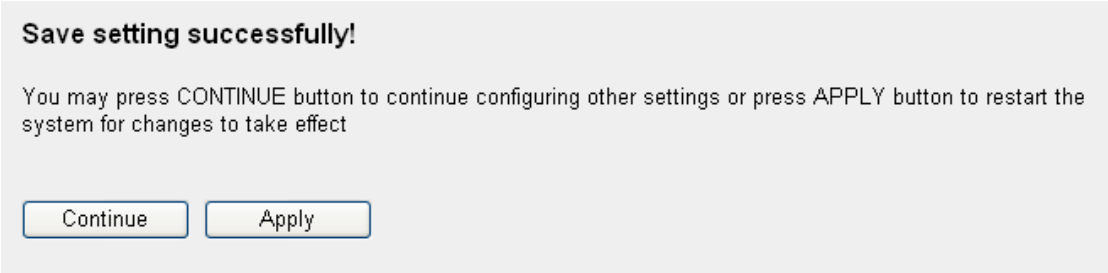
When you click Advanced in the DoS menu, the following message will be displayed on your Web browser:



Here are descriptions of every setup item:

Ping of Death (a):	*Set the threshold for when this DoS prevention mechanism will be activated. Check the box for Ping of Death, and input the frequency of the threshold (how many packets per second, minute or hour). You can also input the Burst value, which means when this number of Ping of Death packets is received in a very short time, this DoS prevention mechanism will be activated.*
Discard Ping From WAN (b):	*Check the box to activate this DoS prevention mechanism.*
Port Scan (c):	*Many kinds of port scan methods are listed here. Check one or more DoS attack methods you want to prevent.*
Sync Flood (d):	*Like Ping of Death, you can set the threshold for when this DoS prevention mechanism will be activated.*

After you finish with all settings, click Apply (e); the following message will be displayed on your Web browser:



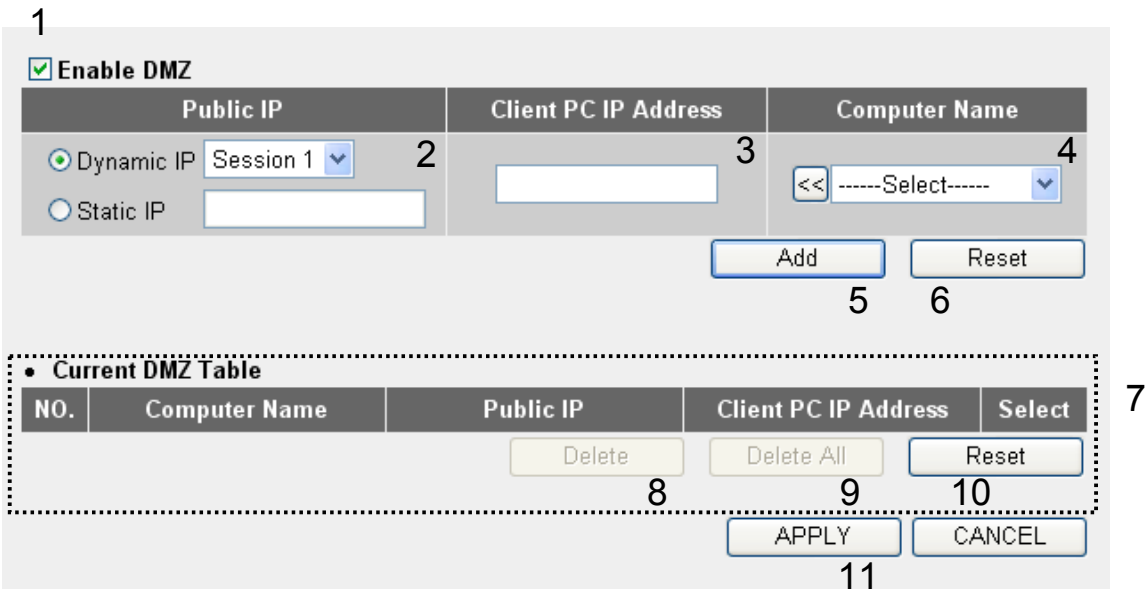
Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-3-4 Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ) refers to a special area in your local network. This area resides in the local network, and all computers in this area use private IP addresses, too. But these private IP addresses are mapped to a certain Internet IP address so other people on the Internet can fully access those computers in DMZ.

Click Firewall on the left side of the Web management interface, then click DMZ; the following message will be displayed on your Web browser:

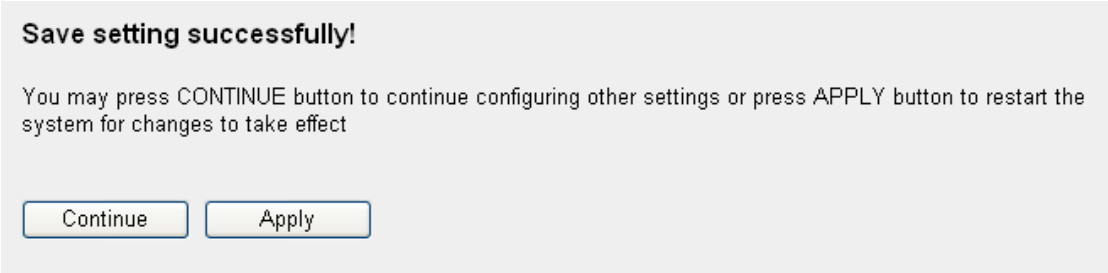


Here are descriptions of every setup item:

Enable DMZ (1):	*Check this box to enable the DMZ function; uncheck this box to disable DMZ function.*
Public IP address (2):	*You can select "Dynamic IP" or "Static IP" here. If you select "Dynamic IP," you have to select an Internet connection session from the drop-down menu; if you select "Static IP," input the IP address you want to map to a specific private IP address.*
Client PC IP address (3):	*Input the private IP address that the Internet IP address will be mapped to.*
Computer Name (4):	*Pull down the menu and all the computers connected to the router will be listed here. You can select the computer name without checking the IP address of the computer.*
Add (5):	*Click Add to add the public IP address and associated private IP address to the DMZ table.*
Reset (6):	*Click Clear to remove the value you inputted in the Public IP address and Client PC IP address*

	fields.
Current DMZ Table (7):	*All existing public IP address and private IP address mapping will be displayed here.*
Delete (8):	*If you want to delete a specific DMZ entry, check the "Select" box of the DMZ entry you want to delete, then click "Delete Selected." (You can select more than one DMZ entries.)*
Delete All (9):	*If you want to delete all DMZ entries listed here, click Delete All.*
Reset (10):	*You can also click Reset to unselect all DMZ entries.*

After you finish with all settings, click Apply (11); the following message will be displayed on your Web browser:



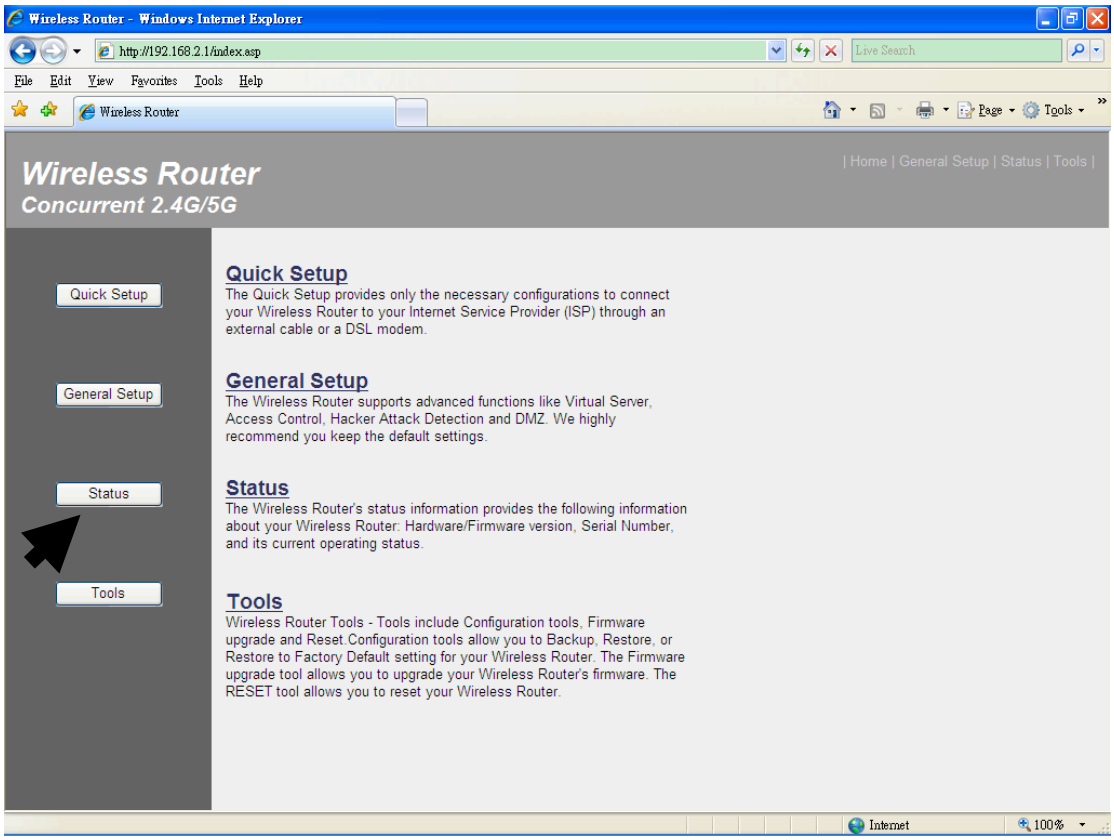
Click Continue to go back to the previous setup menu or to continue to other setup procedures; or click Apply to reboot the router so the settings will take effect (wait about 40 seconds while the router is rebooting).

If you decide to reset all the settings on this screen back to previously saved values, click Cancel.

3-4 System Status

The functions described here provide system-related information. To enter this menu, either click the Status link located at the upper-right corner of the Web management interface or click Status in the main menu.

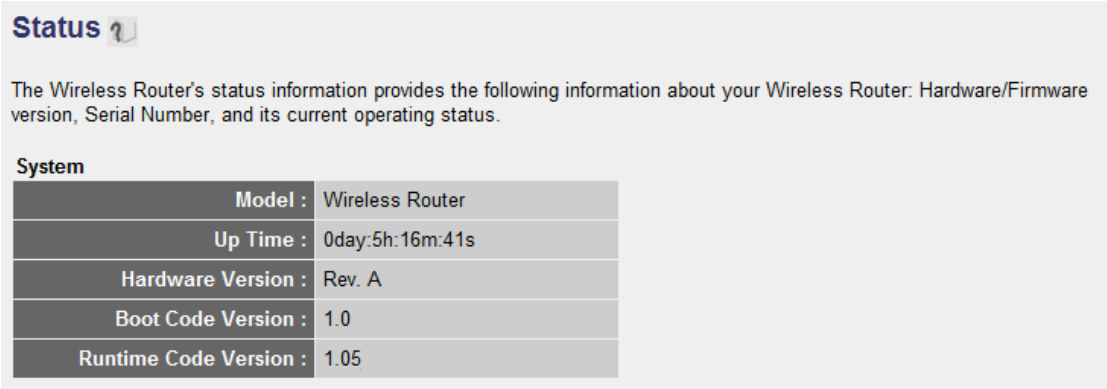
HERE!



3-4-1 System information and firmware version

You can use this function to learn about the system information and firmware version of this router.

Click the Status link located at the upper-right corner of the Web management interface, and the following message will be displayed on your Web browser.

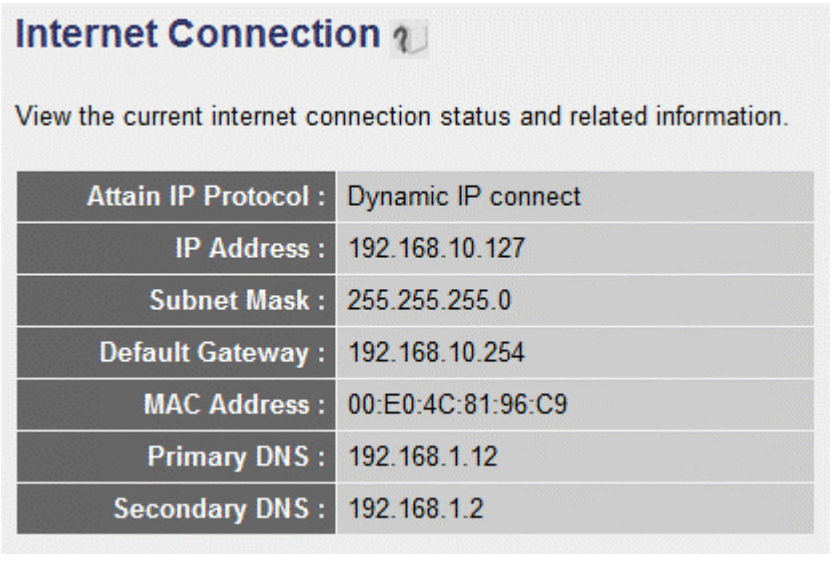


NOTE: Information displayed here may vary.

3-4-2 Internet Connection Status

You can use this function to see the status of current Internet connections.

Click Internet Connection on the left side of the Web management interface, and the following message will be displayed on your Web browser:

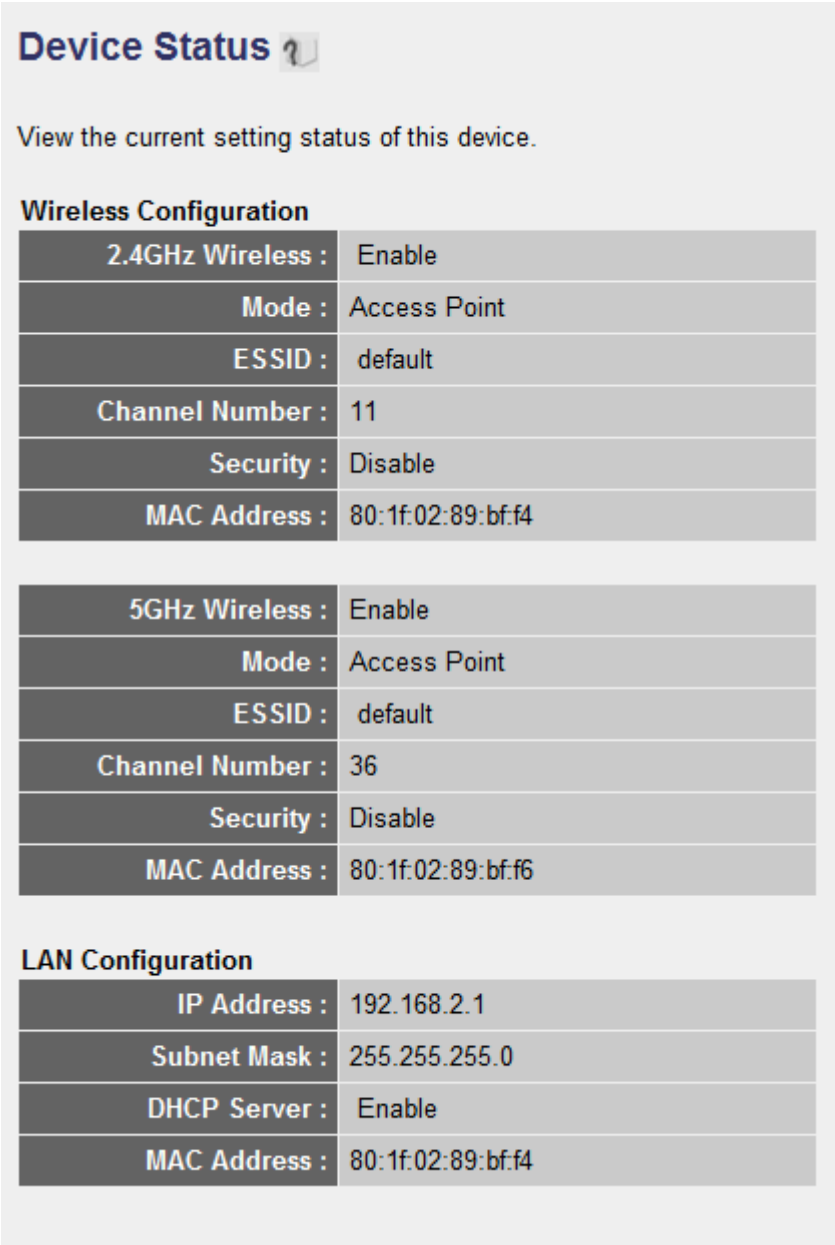


This information will vary depending on the connection status.

3-4-3 Device Status

You can use this function to see the status of your router.

Click Device Status on the left side of the Web management interface; the following message will be displayed on your Web browser:

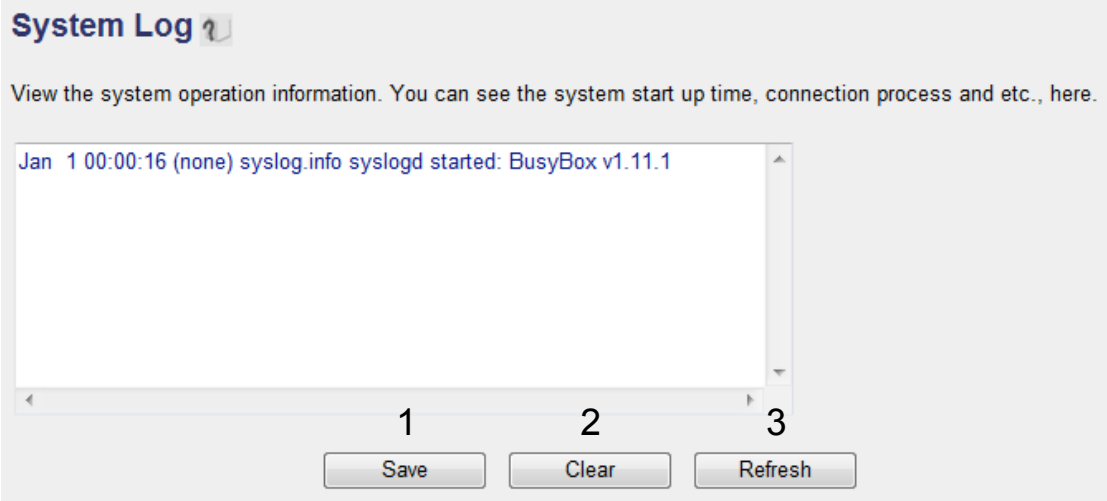


This information will vary depending on the device status.

3-4-4 System Log

All important system events are logged. You can use this function to check the event log of your router.

Click System Log on the left of side of the Web management interface; the following message will be displayed on your Web browser:



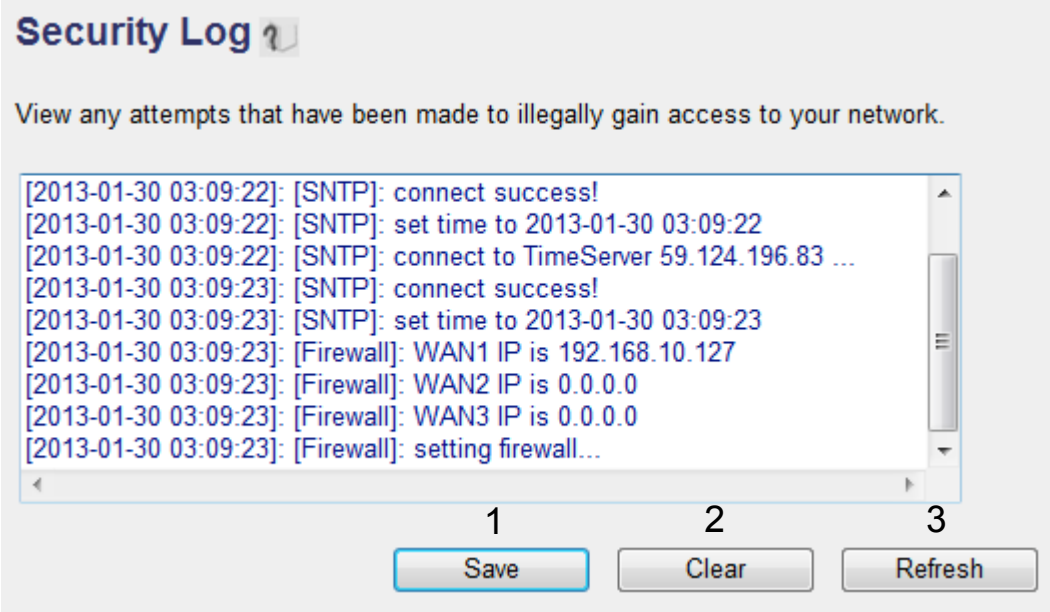
The system events will be displayed on this screen. Here are descriptions of the buttons:

Save (1):	*Save current event log to a text file.*
Clear (2):	*Delete all event logs displayed here.*
Refresh (3):	*Refresh the event log display.*

3-4-5 Security Log

All information about network and system security is kept here, and you can use this function to check the security event log of your router.

Click Security Log on the left side of the Web management interface; the following message will be displayed on your Web browser:



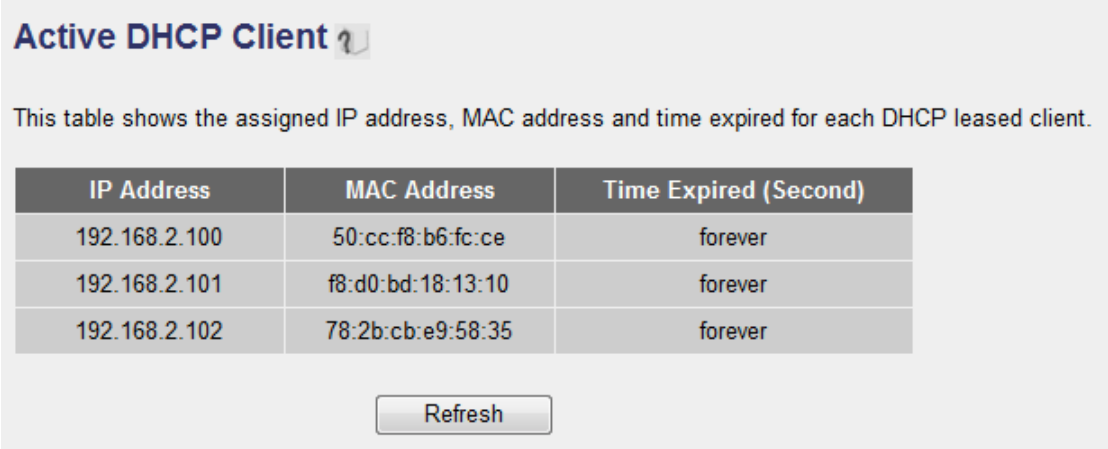
The system events will be displayed on this screen/ Jere are descriptions of the buttons:

Save (1):	*Save current event log to a text file.*
Clear (2):	*Delete all event logs displayed here.*
Refresh (3):	*Refresh the event log display.*

3-4-6 Active DHCP client list

If you're using the DHCP server function of this router, you can use this function to check all active DHCP leases issued by this router.

Click Active DHCP Client on the left side of the Web management interface; the following message will be displayed on your Web browser:

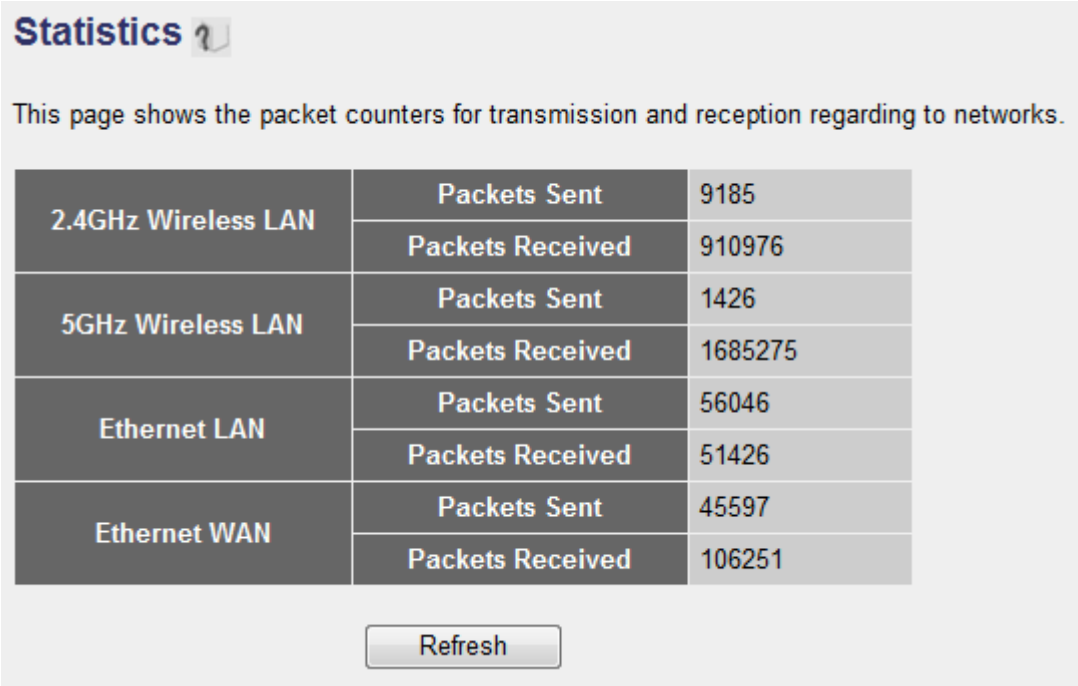


All information about active DHCP leases issued by this router will be displayed here. You can click Refresh to display the latest information.

3-4-7 Statistics

You can use this function to check the statistics of the wireless, LAN and WAN interfaces of this router.

Click Statistics on the left side of the Web management interface; the following message will be displayed on your Web browser:

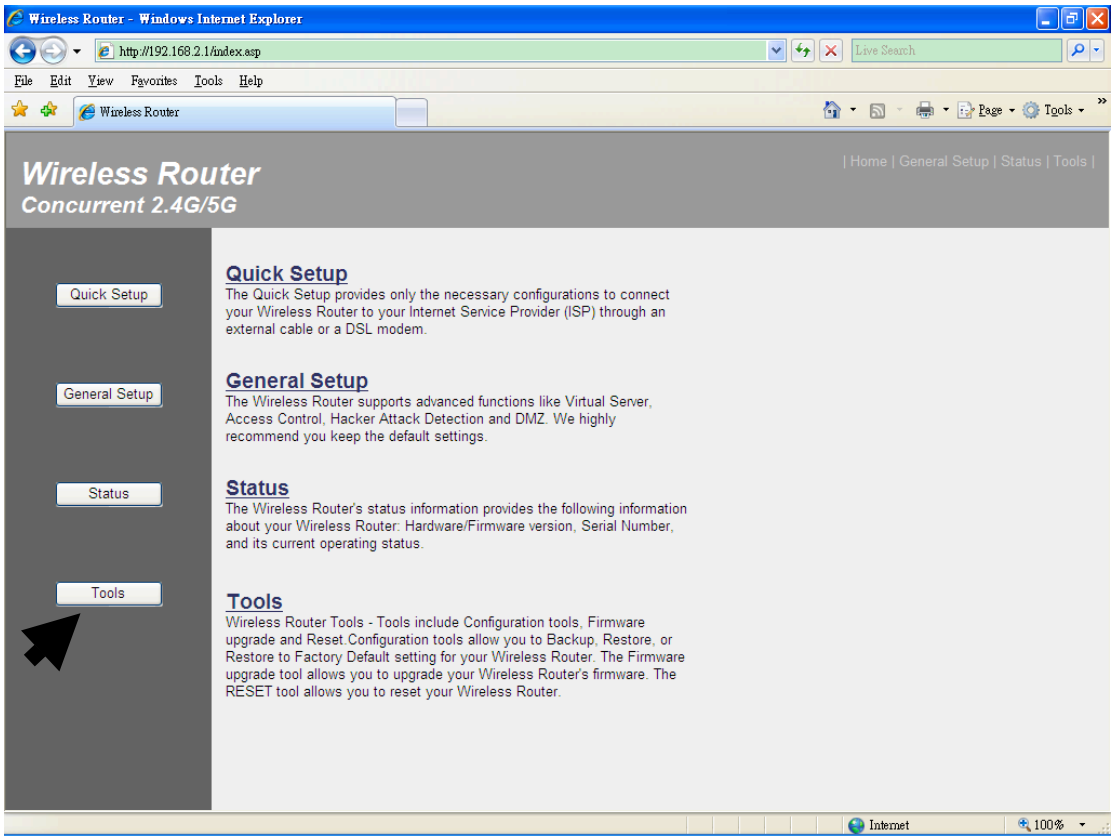


You can click Refresh to display latest information.

3-5 System Tools

The functions described here will provide you system tools for the all the settings backup/restore, firmware upgrade and resetting the router to default settings. To enter system status menu, either click the Tools link located at the upper-right corner of the Web management interface or click Tools in main menu.

HERE!



3-5-1 Configuration Backup and Restore

You can back up all configurations of this router to a file, so you can make several copies of router configuration for security.

Click Tool located at the upper-right corner of the Web management interface, then click Configuration Tools on the left side of the Web management interface; the following message will be displayed on your Web browser:

Here are descriptions of every button:

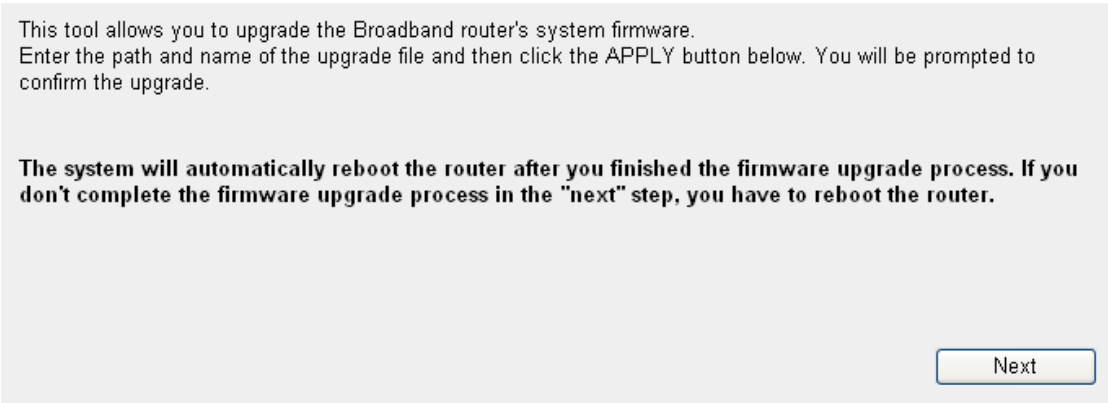
Backup Settings (1):	*Press Save and you'll be prompted to download the configuration as a file. The default*

	filename is “config.bin.” You can save it as another filename for different versions and keep it in a safe place.
Restore Settings (2):	*Press Browse… to pick a previously saved configuration file from your computer, and then click Upload to transfer the configuration file to the router. After the configuration is uploaded, the router’s configuration will be replaced by the file you just uploaded.*
Restore to Factory Default (3):	*Click to remove all settings you’ve made and restore the configuration to factory default settings.*

3-5-2 Firmware Upgrade

The system software used by this router is called firmware. Just like any applications on your computer, when you replace the old application with a new one, your computer will be equipped with the new function. You can also use this firmware upgrade function to add new functions to your router, and even fix bugs in this router.

Click Tool at the upper-right corner of the Web management interface, then click Firmware Upgrade on the left side of the Web management interface; the following message will be displayed on your Web browser:



Click Next and the following message will be displayed:

Click Browse… first. You'll be prompted to provide the filename of the firmware upgrade. Download the latest firmware file from our website and use it to upgrade your router.

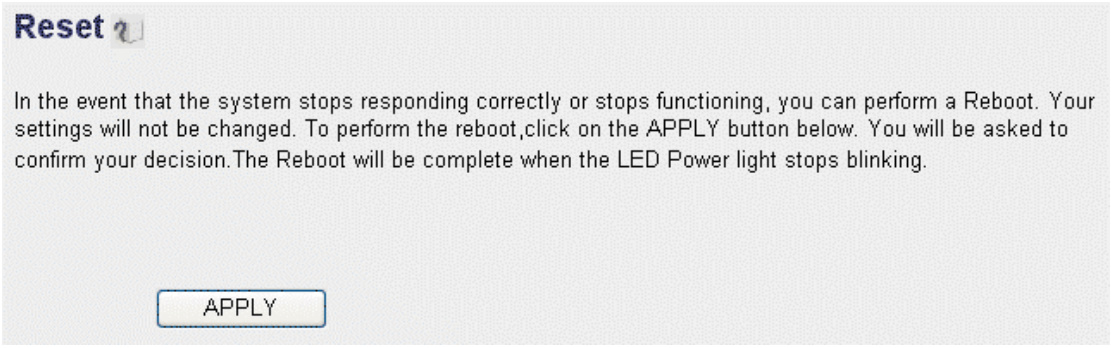
After a firmware upgrade file is selected, click Apply; the router will start the firmware upgrade procedure automatically. The procedure may take several minutes.

NOTE: Never interrupt the upgrade procedure by closing the Web browser or physically disconnecting your computer from the router. If the firmware you upload is corrupt, the firmware upgrade will fail, and you may have to return this router to the dealer of purchase to ask for help. (Warranty voids if you interrupted the upgrade.)

3-5-3 System Reset

If you think the network performance is bad, or you find the behavior of the router is strange, you can perform a router reset. Sometimes it will solve the problem.

Click Tool at the upper-right corner of the Web management interface, then click Reset on the left side of the Web management interface; the following message will be displayed on your Web browser:



Click Apply to reset your router. It will be available again after a few minutes.

Chapter IV: Appendix

4-1 For Specifications, refer to the datasheet at manhattan-products.com.

4-2 Troubleshooting

If you found the router is working improperly or stop responding to you, don't panic! Before you contact your dealer of purchase for help, read this. Some problems can be solved by you in a very short time!

Scenario	Solution
Router is not responding to me when I want to access it by web browser	a. Please check the connection of power cord and network cable of this router. All cords and cables should be correctly and firmly inserted to the router. b. If all LEDs on this router are off, please check the status of A/C power adapter, and make sure it's correctly powered. c. You must use the same IP address section which router uses. d. Are you using MAC or IP address filter? Try to connect the router by another computer and see if it works; if not, please restore your router to factory default settings (pressing 'reset' button for over 10 seconds). e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can get an IP address. f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help. g. If all above solutions don't work, contact the dealer of purchase for help.
Can't get connected to Internet	a. Go to 'Status' -> 'Internet Connection' menu, and check Internet connection status. b. Please be patient, sometime Internet is just that slow. c. If you connect a computer to Internet

	directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password again. e. Call your Internet service provide and check if there's something wrong with their service. f. If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter. g. Try to reset the router and try again later. h. Reset the device provided by your Internet service provider too. i. Try to use IP address instead of hostname. If you can use IP address to communicate with a remote server, but can't use hostname, please check DNS setting.
I can't locate my router by my wireless client	a. 'Broadcast ESSID' set to off? b. All two antennas are properly secured. c. Are you too far from your router? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File download is very slow or breaks frequently	a. Are you using QoS function? Try to disable it and try again. b. Internet is slow sometimes, being patient. c. Try to reset the router and see if it's better after that. d. Try to know what computers do on your local network. If someone's transferring

	big files, other people will think Internet is really slow. e. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log onto web management interface: password is wrong	a. Make sure you're connecting to the correct IP address of the router! b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
Router become hot	a. This is not a malfunction, if you can keep your hand on the router's case. b. If you smell something wrong or see the smoke coming out from router or A/C power adapter, please disconnect the router and A/C power adapter from utility power (make sure it's safe before you're doing this!), and call your dealer of purchase for help.

4-3 Glossary

Default Gateway (Router): Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandrouter.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four

cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading
1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000
It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband router's

NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.