WIRELESS N
3G ROUTER
USER MANUAL
MODELS 524681 & 524940

INTELLINET

NETWORK SOLUTIONS
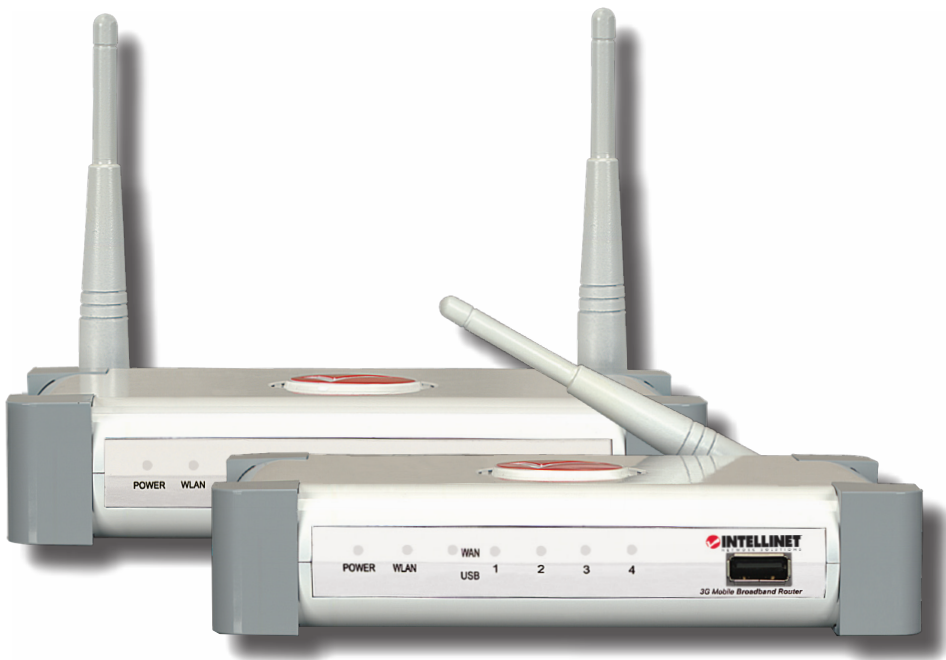
Federal Communications Commission Interference Statement

FCC Part 15

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.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions, and a minimum of 20 cm of space (approx. 8 inches) must be provided between any computer-mounted antenna and a person's body (excluding hands, wrists and feet) during wireless modes of operation.

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate the equipment.

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 channels 1-11 only.

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).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

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 manufacturer 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.

Table of Contents

CHAPTER I: PRODUCT INFORMATION

CHAPTER II: SYSTEM AND NETWORK SETUP

CHAPTER III: ADVANCED FUNCTIONS

CHAPTER IV: APPENDIX

Chapter I: Product Information

1-1 Introduction and Safety Information

Thank you for purchasing this INTELLINET NETWORK SOLUTIONS™ Wireless 300N 3G Router, Model 524681, or Wireless 150N 3G Router, Model 524940.

This high-speed wireless 3G broadband router supports both UMTS/ HSDPA and EVDO networks. When connecting a 3G / 3.5G USB modem* to the router, all network (wired/wireless) users can share the 3G / 3.5G Internet connection. The router can support 3G / 3.5G speed up to 7.2 Mbps.

Other features of this access point include:
• Supports UMTS/HSDPA and EVDO 3G networks
• Up to 300 Mbps network link speed (150 Mbps for Model 524940)
• Complies with 2.4 GHz Draft IEEE 802.11n standard and is
   backward compatible with IEEE 802.11g/b standards
• 2T2R MIMO technology for enhanced throughput and coverage
   (Model 524681 only)
• Supports WMM function to meet the multimedia data bandwidth
   requirement
• Supports Wi-Fi Protected Setup (WPS)
• Supports WAN connection auto fail-over
• Supports WEP and WPA/WPA2 (TKIP and AES) data encryption
• DHCP server supports static lease management
• Supports virtual server, port forwarding and DMZ
• Supports DDNS (dynamic DNS)
• Supports UPnP (Universal Plug and Play)
• Integrated anti-DOS firewall
• QoS (Quality of Service) bandwidth management
• VPN Passthrough (PPTP/IPSec)
• Integrated USB 2.0 port for UMTS/HSDPA and EVDO 3G
   modems
• Easy installation through Web-based user interface

* For a complete list of compatible 3G USB modems, visit www.intellinet-network.com.

1-2 Safety Information

To maintain the safety of users and property, follow these safety instructions:

1. This device is designed for indoor use only; DO NOT place this device outdoors.

2. DO NOT put this device in or near hot or humid places, like a kitchen or bathroom. Also, do not leave this device in your car in hot weather.

3. DO NOT pull any connected cable with force; disconnect it from the device first.

4. If you want to place this device at any significant height or hang it on a wall, make sure it's firmly secured. Falling from any height would damage the device and its accessories.

5. Accessories of this device, like the antennas and power supply, are dangers to small children under 3 years of age. They may put the small parts in their nose or mouth, possibly causing injury. KEEP THIS DEVICE OUT THE REACH OF CHILDREN!

6. The device will become hot when in use for long time. ***This is normal and is not a malfunction.*** DO NOT put this device on paper, cloth or other flammable materials.

7. There's no user-serviceable part inside the device. If the device is not working properly, contact your dealer and ask for help. DO NOT disassemble the device.

8. If the device 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 electrical technician for help.

9. If you smell something strange or even see some smoke coming from the device or power supply, remove the power supply or switch the electrical power off immediately and call the dealer for help.

1-3 System Requirements

• Internet connection, provided by xDSL or cable modem or 3G modem.
• Computer or network devices with wired or wireless network interface card.
• Web browser (Firefox, Microsoft Internet Explorer 4.0 or above, Netscape Navigator 4.7 or above, Opera Web browser or Safari Web browser)
• Available AC power socket (100 – 240 V, 50/60 Hz)

1-4 Package Contents

Before you start to use this router, check to see if there's anything missing in the package. If so, contact your dealer of purchase.

• Wireless 300N or 150N 3G Router
• Quick installation guide
• User manual on CD
• A/C power adapter

1-5 Connections and Indicators

Front Panel
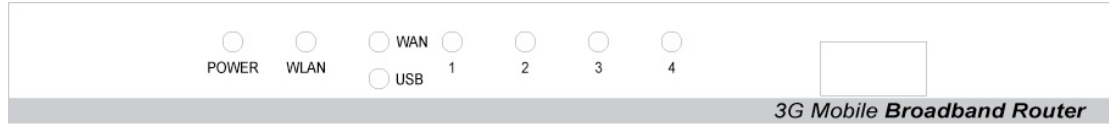
LED Name	Light Status	Description
POWER	On	Router is switched on and correctly powered.
WLAN	On	Wireless WPS function is enabled.
	Off	Wireless network is switched off.
	Flashing	Wireless LAN activity (transferring or receiving data).
WAN LNK/ACT	On	WAN port is connected.
	Off	WAN port is not connected.
	Flashing	WAN activity (transferring or receiving data).
USB LNK/ACT	On	USB modem is connected.
	Off	USB modem is not connected.
	Flashing	USB modem 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
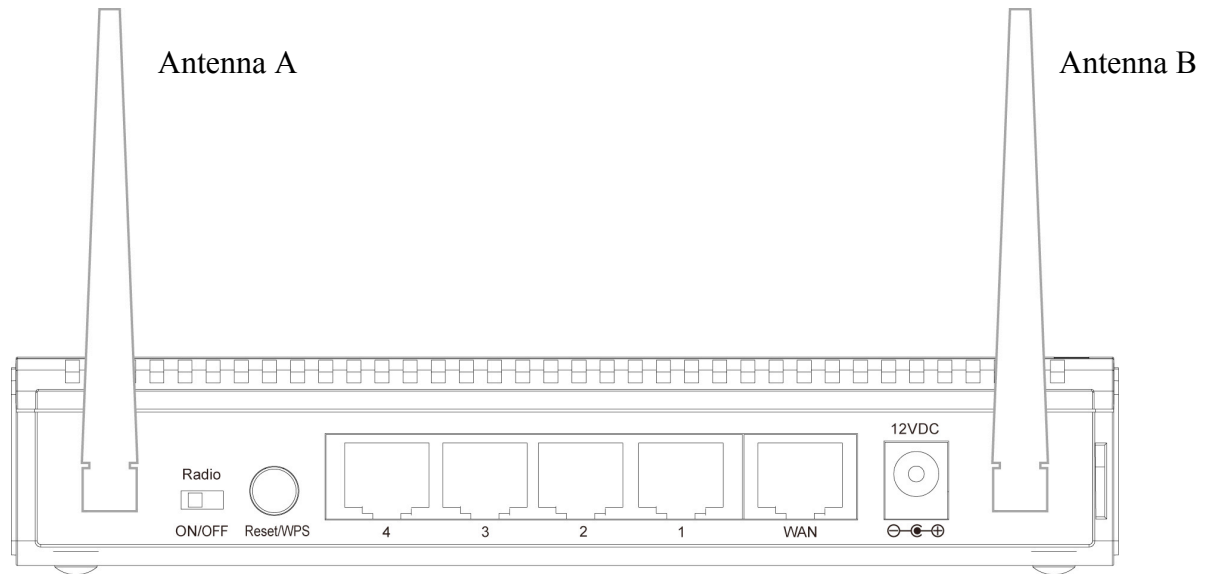
Item Name	Description
Antenna A/B*	These antennas are 3dBi dipole antennas.
Radio ON/OFF	Switch the button to activate or deactivate the wireless functions.
Reset / WPS	Reset the router to factory default settings (clear all settings) or start WPS function. Press this button and hold for 10 seconds to restore all settings to factory defaults, and press this button for less than 5 seconds to start WPS function.
1 – 4	Local Area Network (LAN) ports 1 to 4.
WAN	Wide Area Network (WAN / Internet) port.
Power	Power connector, connects to A/C power adapter.

* Only one antenna for Model 524940

Chapter II: System and Network Setup

2-1 Network Connections

1. Connect your USB modem to the USB port located on the front panel of the router.
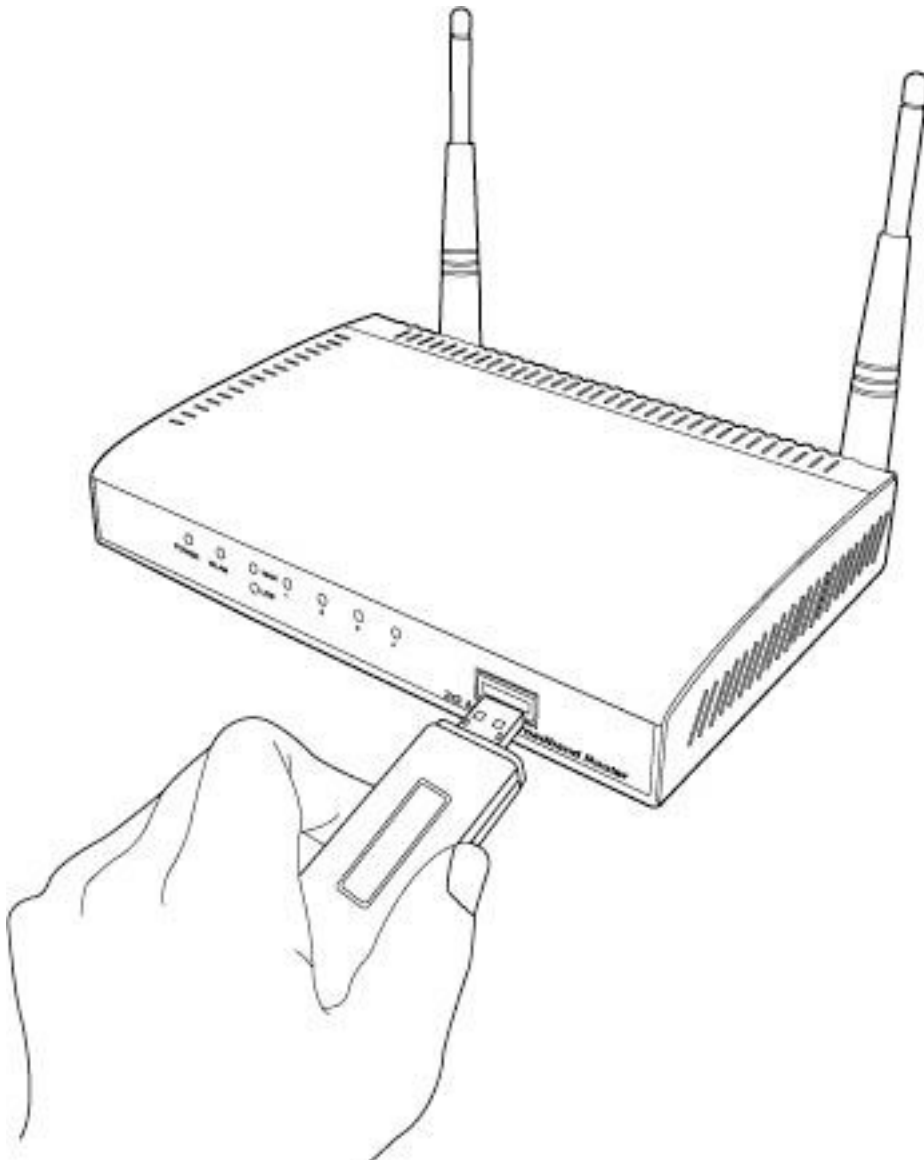
2. Connect your xDSL / cable modem to the WAN port of router by Ethernet cable. ***NOTE:*** Go to Section 3-4 Fail Over to assign the WAN connection priority if you have subscribed to both 3G and xDSL/Cable Modem services.
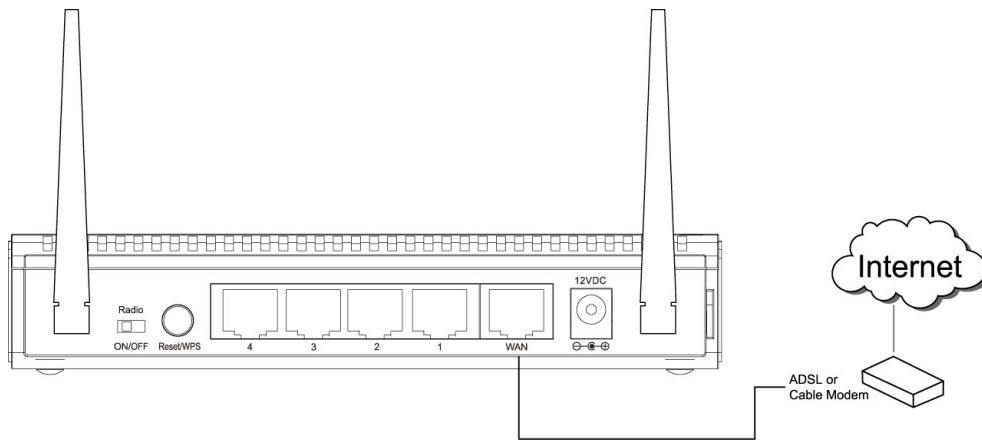
3. Connect all your computers, network devices (network-enabled consumer devices other than computers, like game consoles or switches/hubs) to the LAN port of the router.
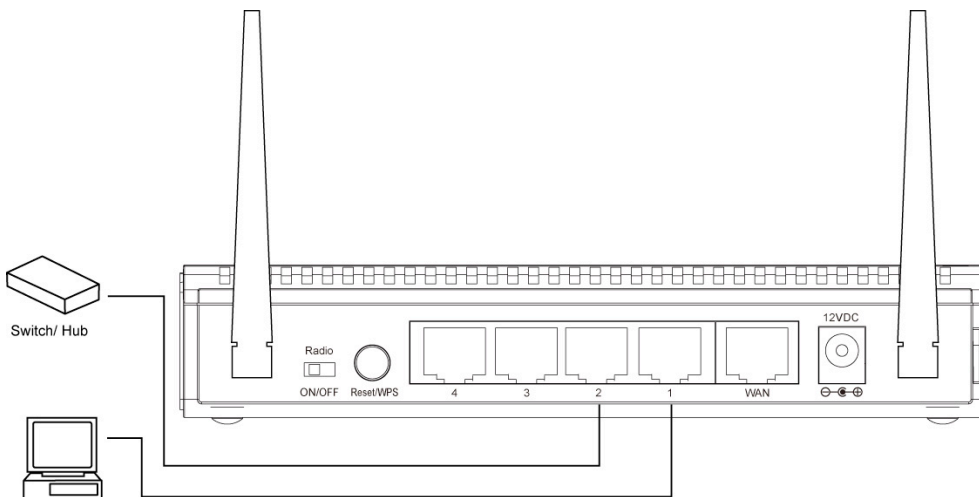
4. Connect the AC power adapter to the wall socket, then connect it to the Power socket of the router.
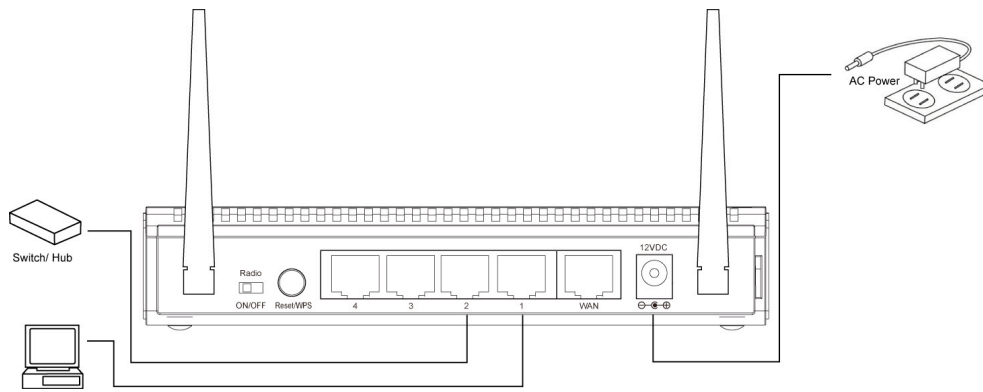
5. Check all LEDs on the front panel. The Power LED should be on; the WAN, LAN and USB LEDs should be on if the computer / network device connected to the respective ports of the router are powered on and correctly connected. If the Power LED is not on, or if any LED you expected to be on isn't, re-check the cabling or refer to **4-2 Troubleshooting** for possible causes and solutions.

2-2 Connecting to the Router via Web Browser

After the network connection is established, 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 obtain an IP address automatically (use dynamic IP address). If it's set to use a static IP address, or if you're unsure, follow the instructions below to configure your computer to use a dynamic IP address:

If the operating system of your computer is

Windows 95/98/Me	- go to section 2-2-1
Windows 2000	- go to section 2-2-2
Windows XP	- go to section 2-2-3
Windows Vista/7	- go to section 2-2-4

2-2-1 Windows 95/98/Me IP Address Setup

1. Click Start (at the lower-left corner of your desktop), then click Control Panel. Double-click the **Network** icon and the **Network** window will appear. Select "TCP/IP," then click "Properties."
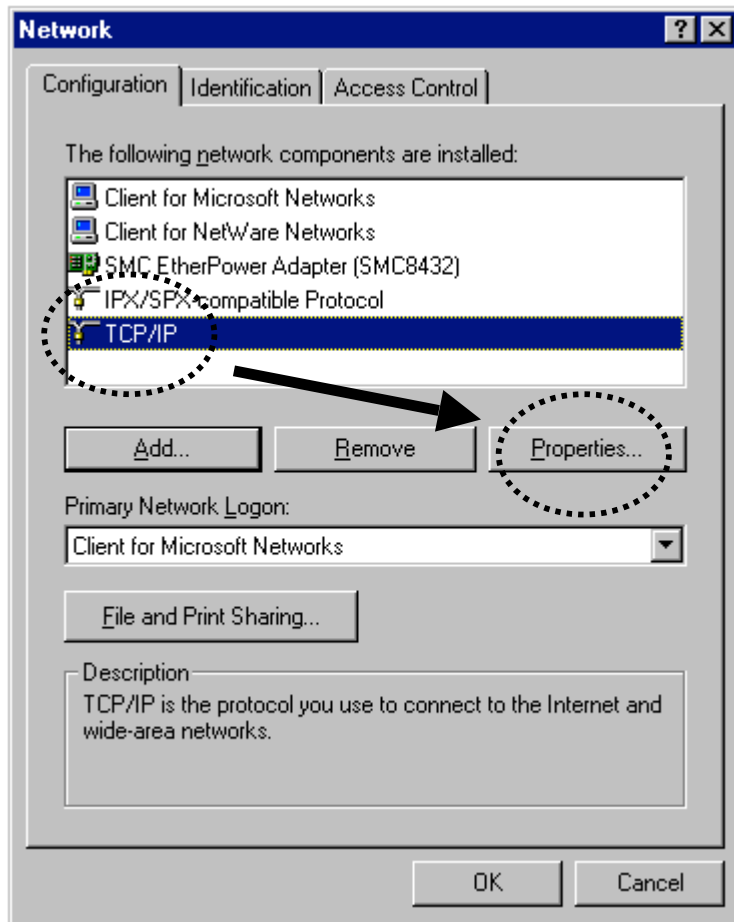
2. Select "Obtain an IP address from a DHCP server" and then click "OK."
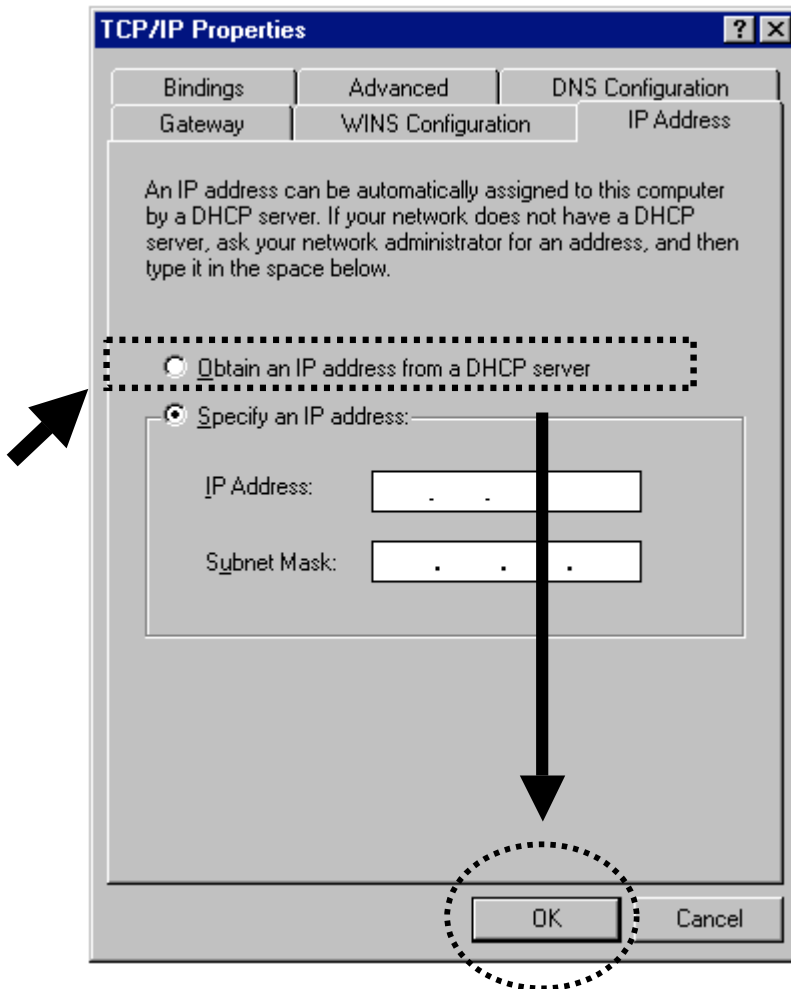
2-2-2 Windows 2000 IP Address Setup

1. Click Start (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."
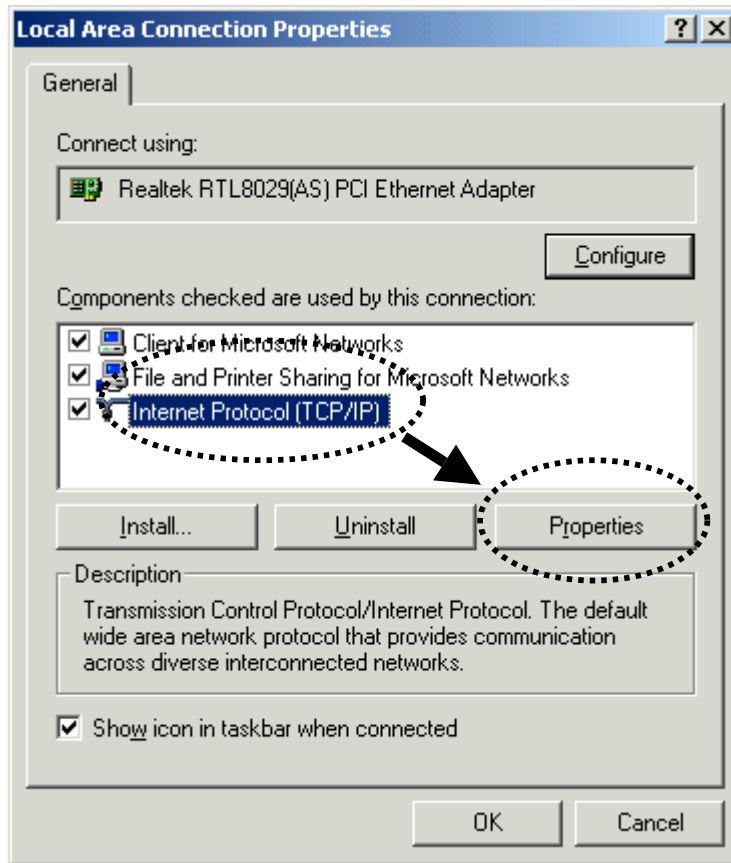
2. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically," then click "OK."
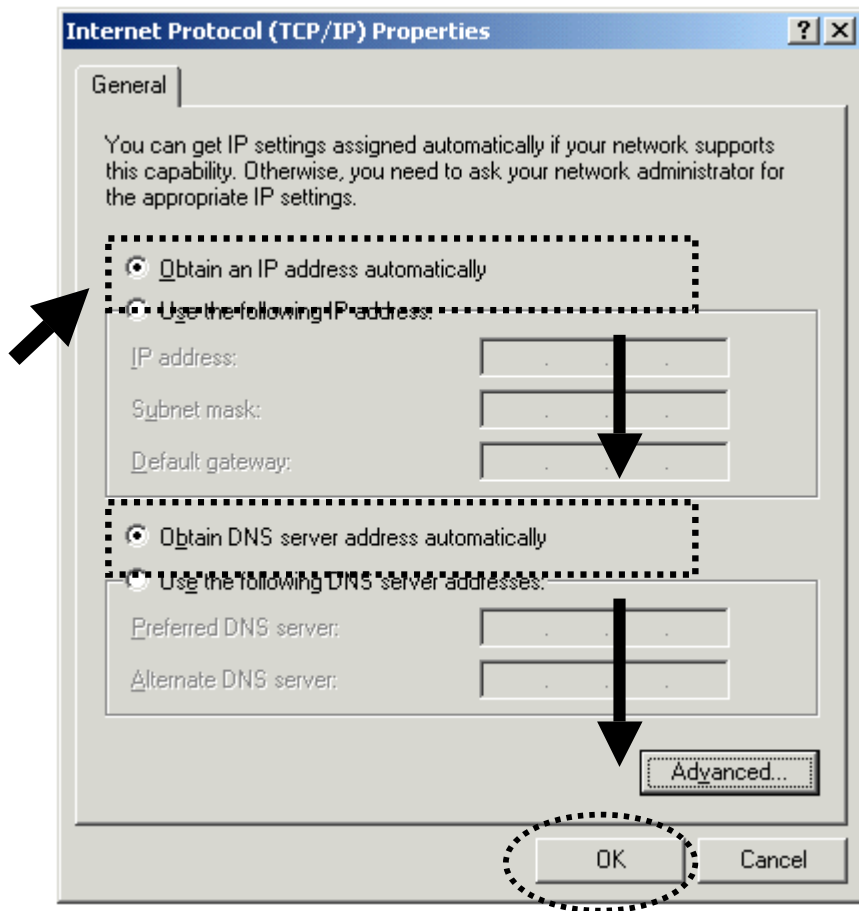
2-2-3 Windows XP IP Address Setup

1. Click Start (at the lower-left corner of your desktop), then click Control Panel. Double-click the **Network and Internet Connections** icon, click **Network Connections,** then double-click **Local Area Connection**; the **Local Area Connection Status** window will appear. Click "Properties."
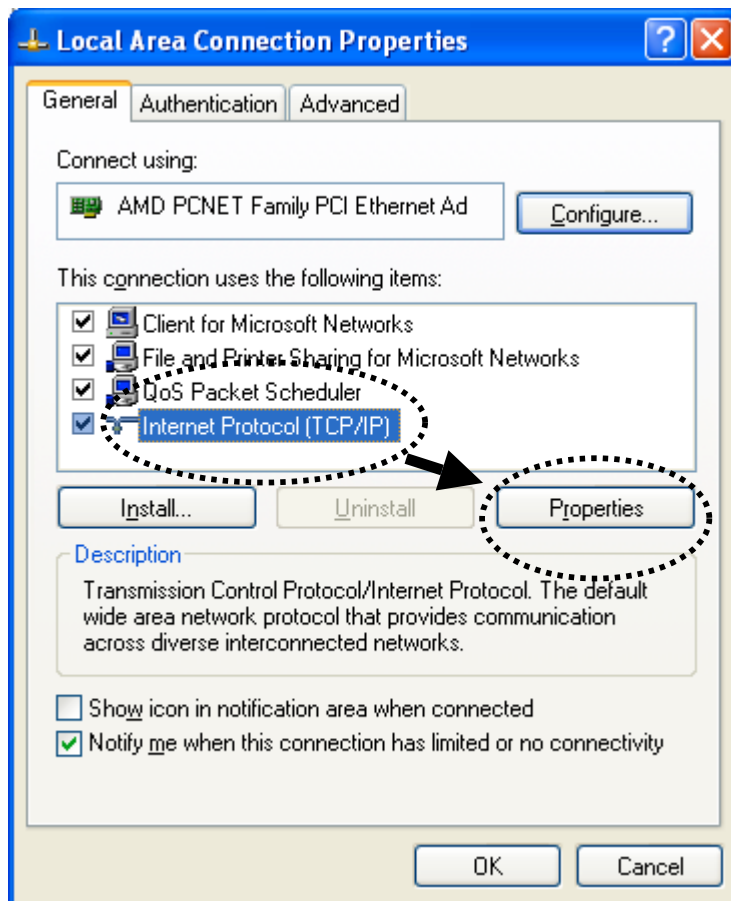
2. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically," then click "OK."
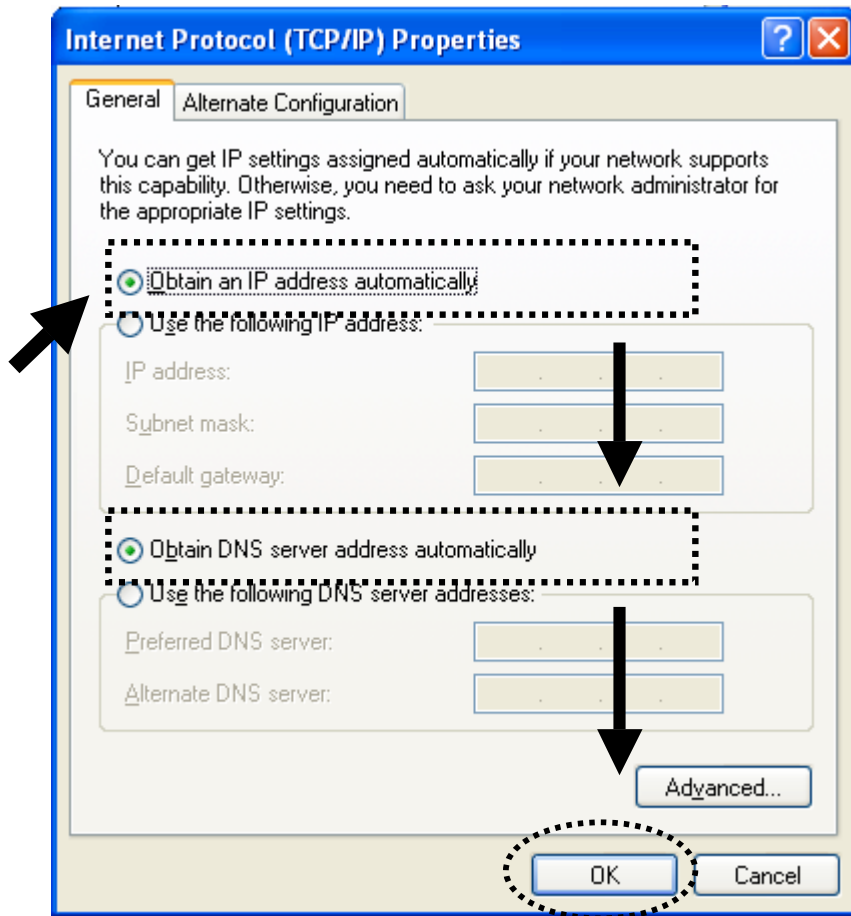
2-2-4 Windows Vista/7 IP Address Setup

1. Click Start (at the lower-left corner of your desktop), then click Control Panel. Click **View Network Status and Tasks**, and then click **Manage Network Connections.** Right-click **Local Area Network**, then select **"Properties."** The **Local Area Connection Properties** window will appear. Select "Internet Protocol Version 4 (TCP / IPv4)," and then click "Properties."
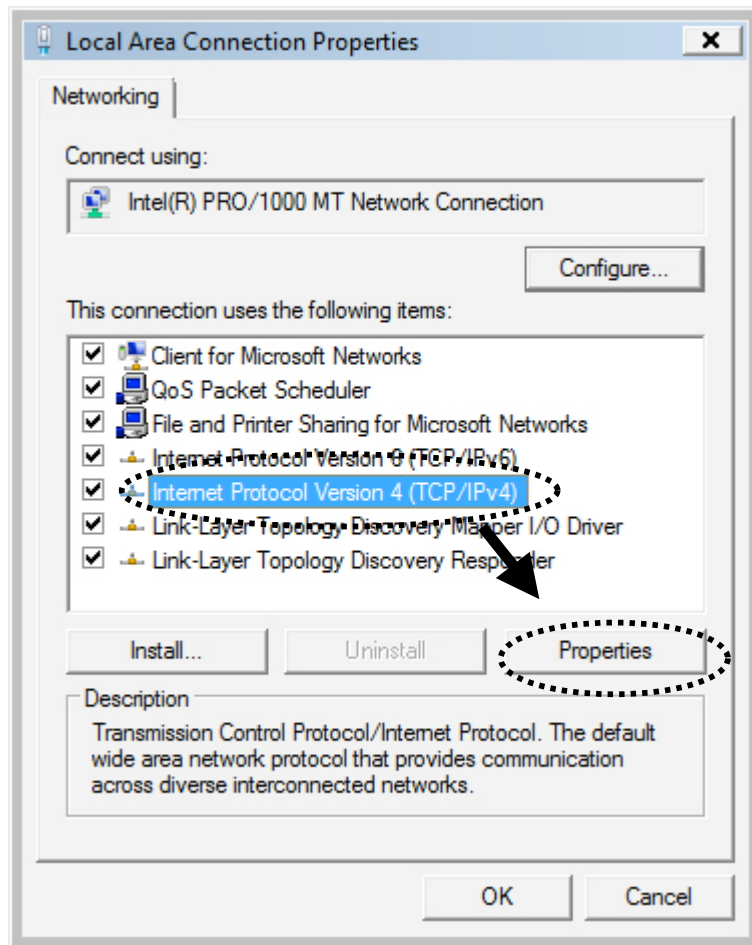
2. Select "Obtain an IP address automatically" and "Obtain DNS server address automatically," then click "OK."
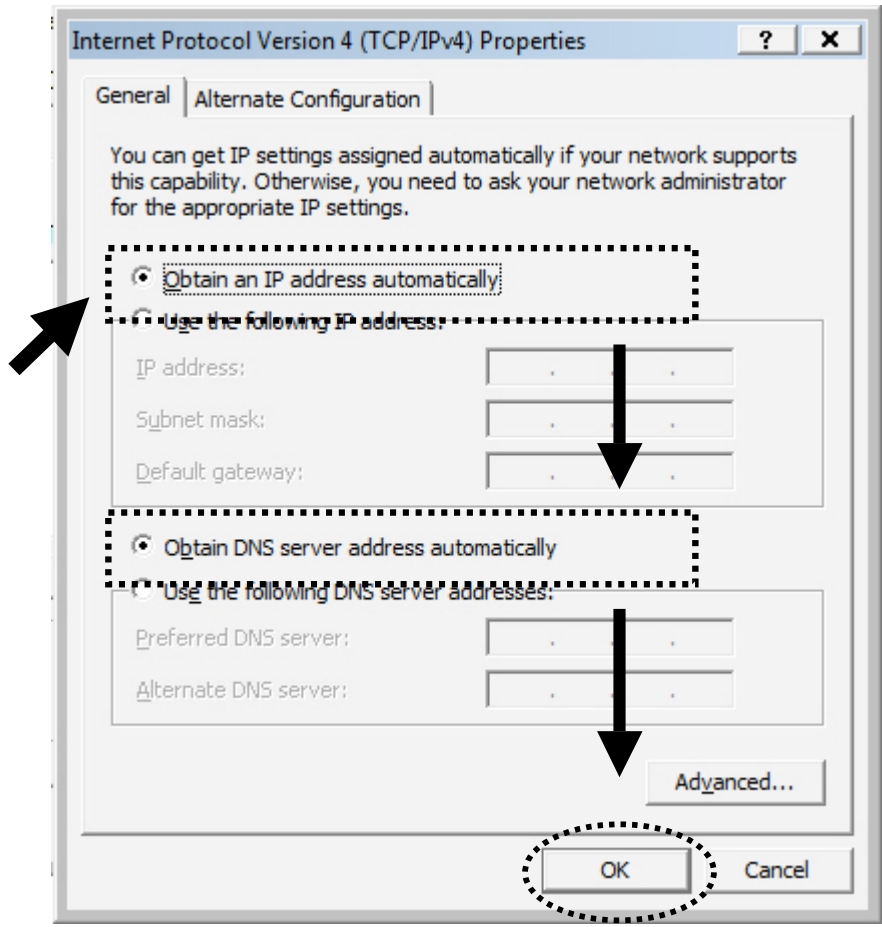
2-2-5 Router IP Address Lookup

After the IP address setup is complete, go to Start, then Run at the bottom-lower corner of your desktop:
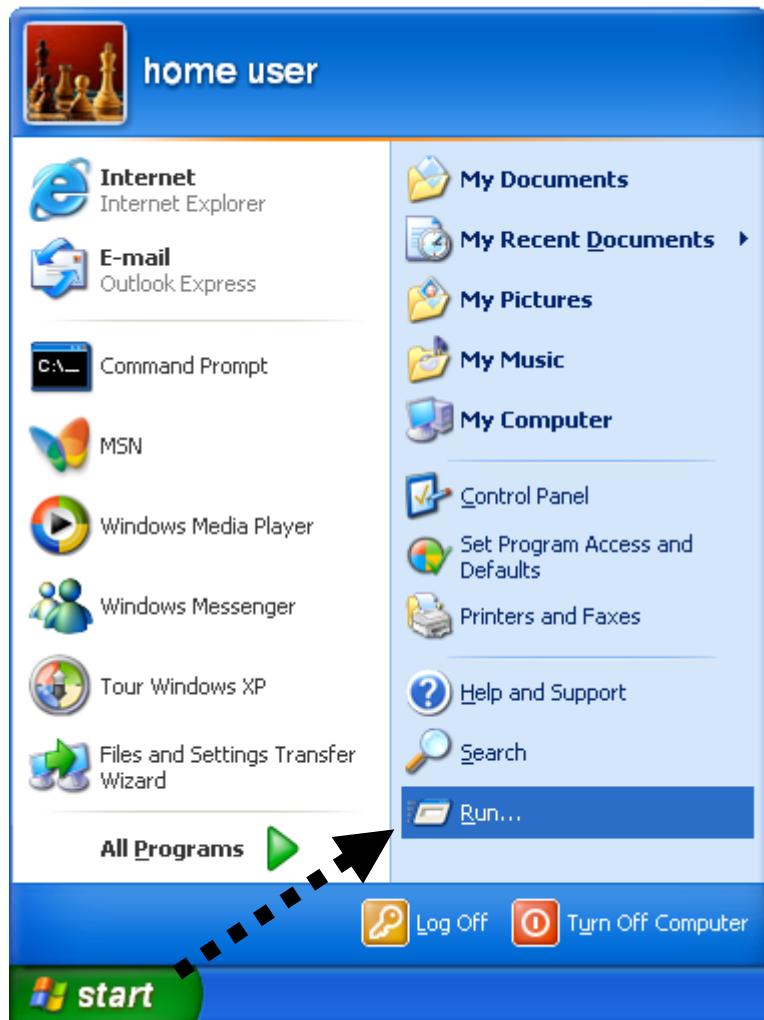
Input "cmd," then click "OK."
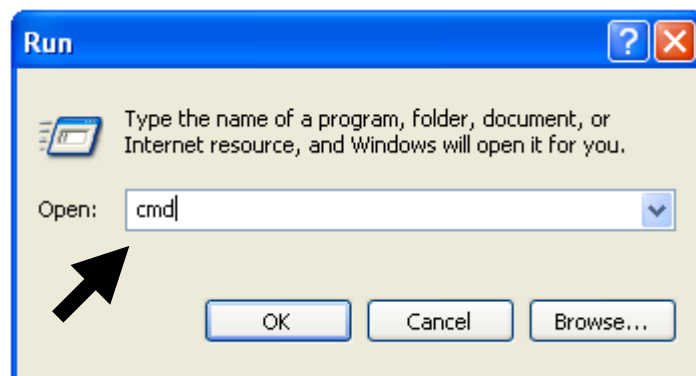
Input "ipconfig," then press <Enter>. Check the IP address followed by the default gateway (in this example, the IP address of the router is 192.168.2.1).
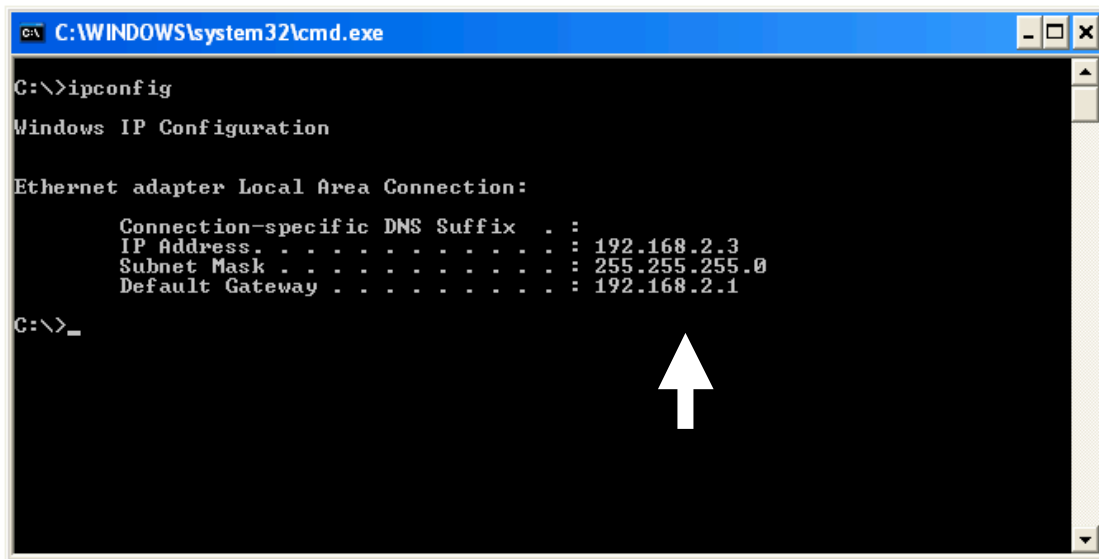
NOTE: If the IP address of the default gateway is not displayed, or if the address following "IP Address" begins with "169," re-check the network connection between your computer and router, and/or go to the beginning of this chapter to re-check each step of the network setup procedure.

3. Connect the router's management interface by Web browser

After your computer obtains an IP address from the router, start your Web browser and input the IP address of the router in the address bar. The following window should display.
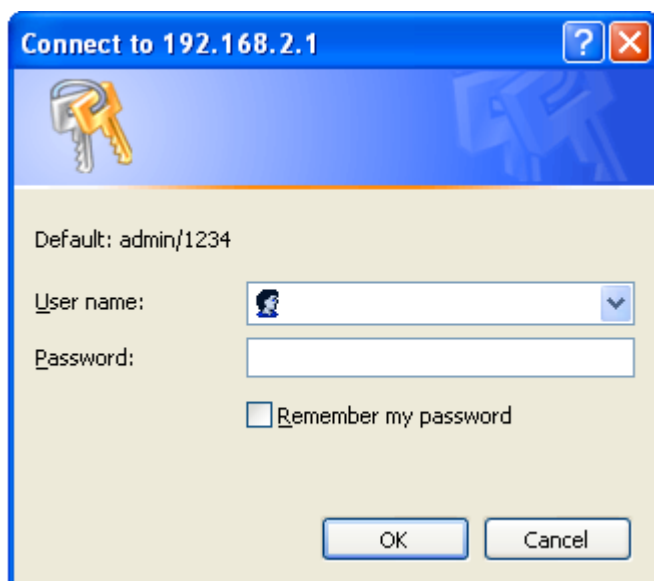
Enter a user name and password in their respective fields (default user name is "admin"; default password is "1234"). Click "OK" band you can see the Web management interface of the router.
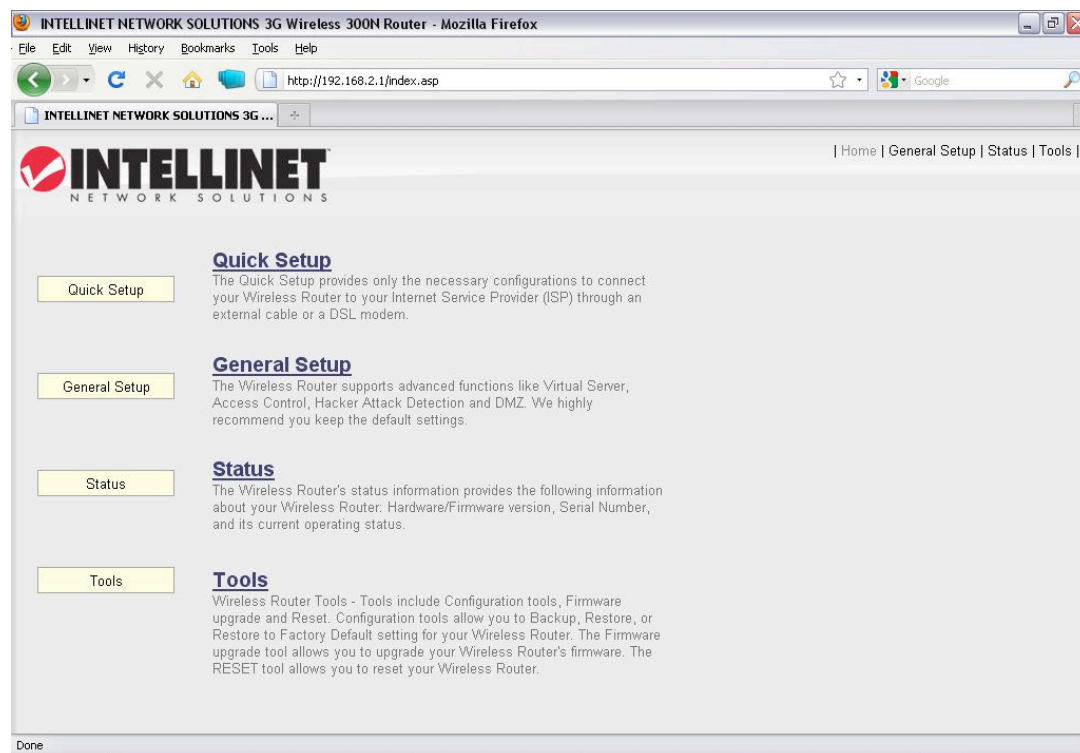
NOTE: If you can't see the Web management interface and you're being prompted to input the user name and password again, it means you didn't input the user name and password correctly: Re-enter the user name and password. If you're certain the user name and password you entered are correct, refer to 4-2 Troubleshooting to perform a factory reset to set the password back to its default value.

TIP: This page shows the four major menus: Quick Setup, General Setup, Status and Tools. The shortcuts to these menus are at the upper-right corner of every page so you don't have to go back to the first page.

2-3 Using Quick Setup

Quick Setup lets you complete all the required settings you need in order to access the Internet very quickly.

Click "Quick Setup" on the left-hand navigation panel.

The following message will be displayed:

1. Set Time Zone

Below are descriptions of each option:

Set Time Zone (1):	*Click ⌄ and a drop-down list will be shown. Choose the time zone for your location.*

Time Server Address (2):	*Input the IP address / host name of time server here.*
Daylight Savings (3):	*If the country you live in uses Daylight Saving, check "Enable Function" and choose the duration of Daylight Saving.*

After you finish the settings, click "Next" (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 the time on the router is incorrect, try another time server.

---

2. Broadband Type
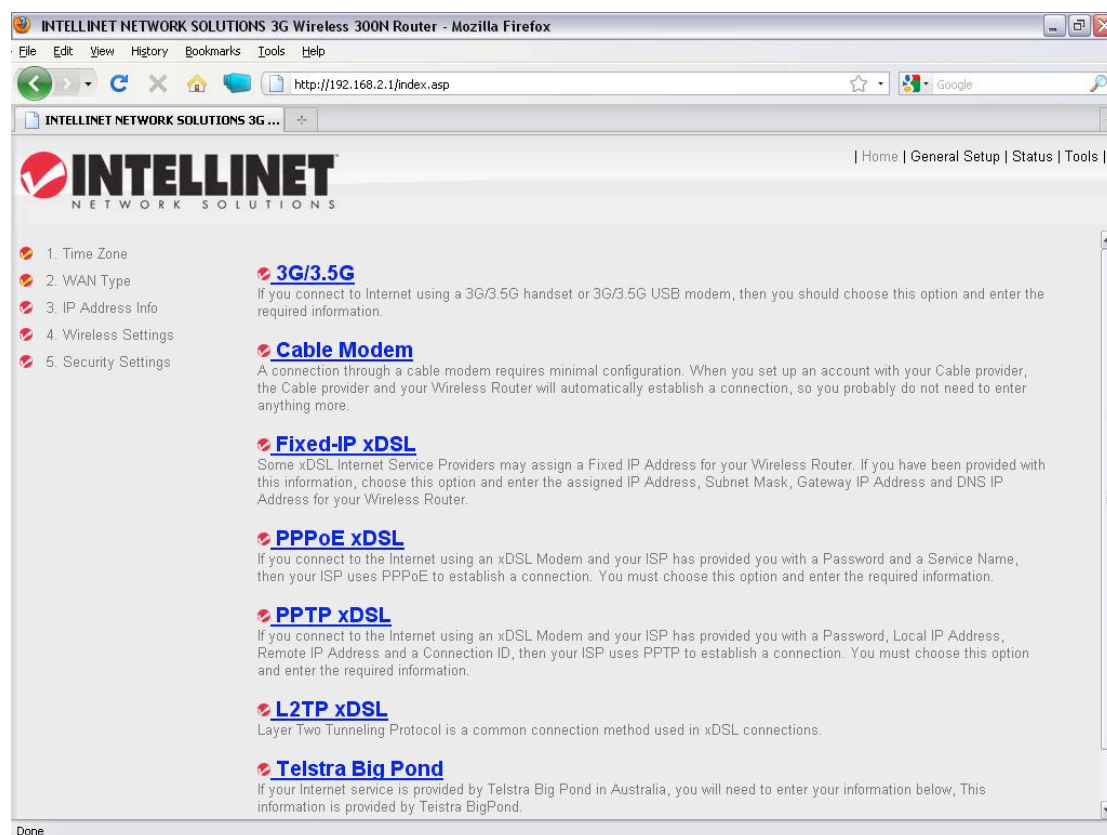
Choose the broadband (Internet connection) type you're using.
There are seven types of Internet connections:

3G/3.5G	- go to section 2-3-1
Cable Modem	- go to section 2-3-2
Fixed-IP xDSL	- go to section 2-3-3
PPPoE xDSL	- go to section 2-3-4
PPTP xDSL	- go to section 2-3-5
L2TP xDSL	- go to section 2-3-6
Telstra BigPond	- go to section 2-3-7

If you're not sure which to use, 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 to a previous step, click "Back" at the bottom of the
page.

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 you're using another connection type, like xDSL. Also, some cable modems use PPPoE, so you can choose PPPoE xDSL for such a connection even if you're using a cable modem.

3. Basic Settings

Below are descriptions of each option:

Wireless Module (1): Click "Enable" to start using the wireless function of this router, or select "Disable" to close the wireless interface of this router.

Band (2): *Select a band type from the drop-down list. It allows you to set the router at 802.11b or 802.11g or 802.11n mode. You also can select B+G or B+G+N mode to allow the router to select an 802.11b, 802.11g or 802.11n connection automatically.*

SSID (3): *This is the name of the wireless router. You can enter any alphanumerical characters here*

(maximum 32 characters). SSID is used to identify your own wireless router from others when there are other wireless routers in the area. Default SSID is "INTELLINET"; it's recommended to change the default SSID name to one that is easily recognizable, such as "my home," "office_room1," etc.

Channel Number (4): Select a channel from the drop-down list. Available channel numbers are 1 to 13 for European countries; 1 to 11 for the U.S. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use. Some wireless clients support manual channel number select, and this would help in certain scenarios where there is a radio communication problem.

Associated Clients (5): Click "Show Active Clients" and 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.

After you finish the settings, click "Next" (6); to go back to a previous menu, click "Back."

4. Security Settings

5. Security Settings

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption : Disable

☐ Enable 802.1x Authentication

BACK   OK

Choose the Encryption type you're using from the drop-down list. There are three types of Encryption:

WEP   - go to section 2-7-3-2
WPA pre-shared key   - go to section 2-7-3-3
WPA RADIUS   - go to section 2-7-3-4

To go back to a previous step, click "Back" at the bottom of the page.

2-3-1 Setup Procedure for 3G/3.5G

3G/3.5G

Enter the User Name, Password, APN, PIN Code and Dialed Number provided to you by your service provider in the appropriate fields.

● **3G/3.5G Settings :**

PIN Code :		1
APN :	internet	2
User Name :		3
Password :		4
Verify Password :		5
Service :	3G/3.5G Only (UMTS/HSPA/HSDPA)	6
AT Dial Script :	*99#	7

Back   NEXT

8

Below are descriptions of each option:

PIN Code (1):   *Enter a Pin Code for your UMTS or HSDPA or EVDO connection. This is optional, and is only required if your service provider asks you to do so.*

APN (2):   *Enter the APN code assigned by your Internet service provider here.*

User Name (3):   *Enter the user name assigned by your Internet service provider here.*

Password (4):   *Enter the password assigned by your Internet service provider here.*

Verify Password (5): Enter the password again for confirmation.

Service (6):   *Select your card type from the drop-down menu.*

AT Dial Script (7):   *Enter the dialed number for your UMTS or HSDPA connection. The default is *99#. This field should not be altered except when required by your service provider.*

After you finish the settings, click "Next" (8); to go back to a previous menu, click "Back."

2-3-2 Setup Procedure for Cable Modem

Below are descriptions of each option:

Host Name (1):	*Enter 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):	*Enter the MAC address of your computer here if your service provider only permits computers 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 click "Clone Mac address" to fill the MAC address field with the MAC address of your computer.*

After you finish the settings, click "Next" (3); to go back to a previous menu, click "Back."

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

Below are descriptions of the options:

IP address (1):	*Enter the IP address assigned by your service provider.*
Subnet Mask (2):	*Enter the subnet mask assigned by your service provider.*
DNS Address (3):	*Enter the IP address of the DNS server provided by your service provider.*
Default Gateway (4):	*Enter the IP address of the default 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 the settings, click "Next" (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 you're not using DHCP or PPPoE protocols.**

PPPoE

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.

User Name :		1
Password :		2
Service Name :		3
MTU :	1392 (512<=MTU<=1492)	4
Connection Type :	Continuous ⌄ Connect Disconnect	5
Idle Time Out :	10 (1-1000 Minute)	6
	BACK NEXT	7

Below are descriptions of each option:

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

Password (2):   Enter the password assigned by your Internet service provider here.

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

MTU (4):   Enter the MTU value of your network connection here. If you don't know, contact your ISP.

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

Idle Time Out (6):   Enter the idle time out (detailed explanation listed below).

When you finish the settings, click "Next" (7); to go back to a previous menu, click "Back."

MTU - If you don't know what it is, ask your service provider for a proper value.

Connection Type - There are 3 options: "Continuous" keeps the Internet connection alive (doesn't disconnect); "Connect on Demand" only connects to the Internet when there's a connection attempt; "Manual" only connects to the Internet when "Connect" is clicked, and disconnects when "Disconnect" is clicked.

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

2-3-5 Setup Procedure for PPTP xDSL

PPTP xDSL requires two kinds of settings: WAN Interface Settings (setup IP address) and PPTP Settings (PPTP user name and password). First, WAN Interface Settings:

Select how 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., a 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 how you should fill in these fields.

Next, PPTP Settings:

Below are descriptions of each option:

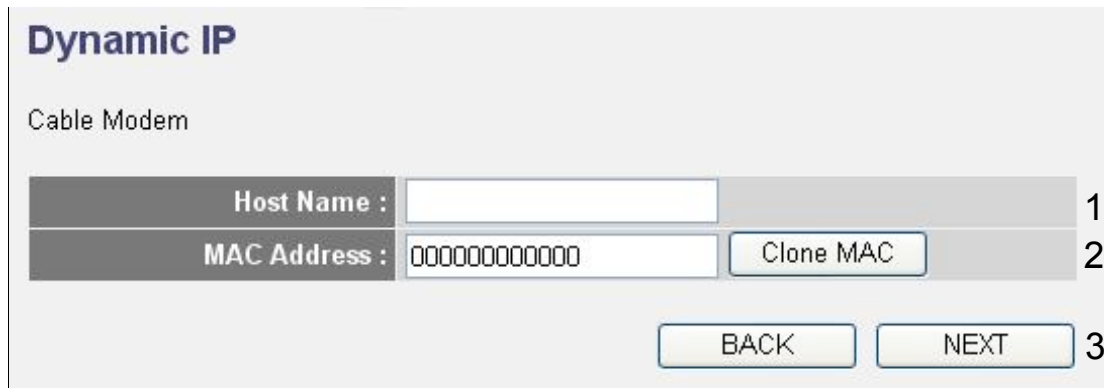|	
User Name (1):	*Enter the user name assigned by your Internet service provider here.*
Password (2):	*Enter the password assigned by your Internet service provider here.*
PPTP Gateway (3):	*Enter the IP address of the PPTP gateway assigned by your Internet service provider here.*
Connection ID (4):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

Connection Type: Select the connection type of Internet
(7)   connection you want to use (refer to the last
*   section for detailed descriptions).*

Idle Time Out (8): Enter the idle time out of the Internet
*   connection you want to use (refer to the last*
*   section for detailed descriptions).*

When you finish the settings, click "Next" (9); to go back to a previous menu, click "Back."

2-3-6 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 PPTP connection.

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

Select how 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., a 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 how you should fill in these fields.

Next, L2TP Settings:

Below are descriptions of each option:

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

When you finish the settings, click "Next" (7); to go back to a previous menu, click "Back."

2-3-7 Setup Procedure for Telstra BigPond

This setting only works when you're using Telstra BigPond's network service in Australia.

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

When you finish the settings, click "Next" (5); to go back to a previous menu, click "Back."

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

Save setting successfully!

Please press APPLY button to restart the system for changes to take effect.

Apply

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

System Restarting! Please wait for a while !

OK!

Wait for about 30 seconds, then click "OK!" You'll be back to the router management interface, and the router is ready with new settings.

2-4 Basic Setup

In this chapter, you'll see 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 screen).
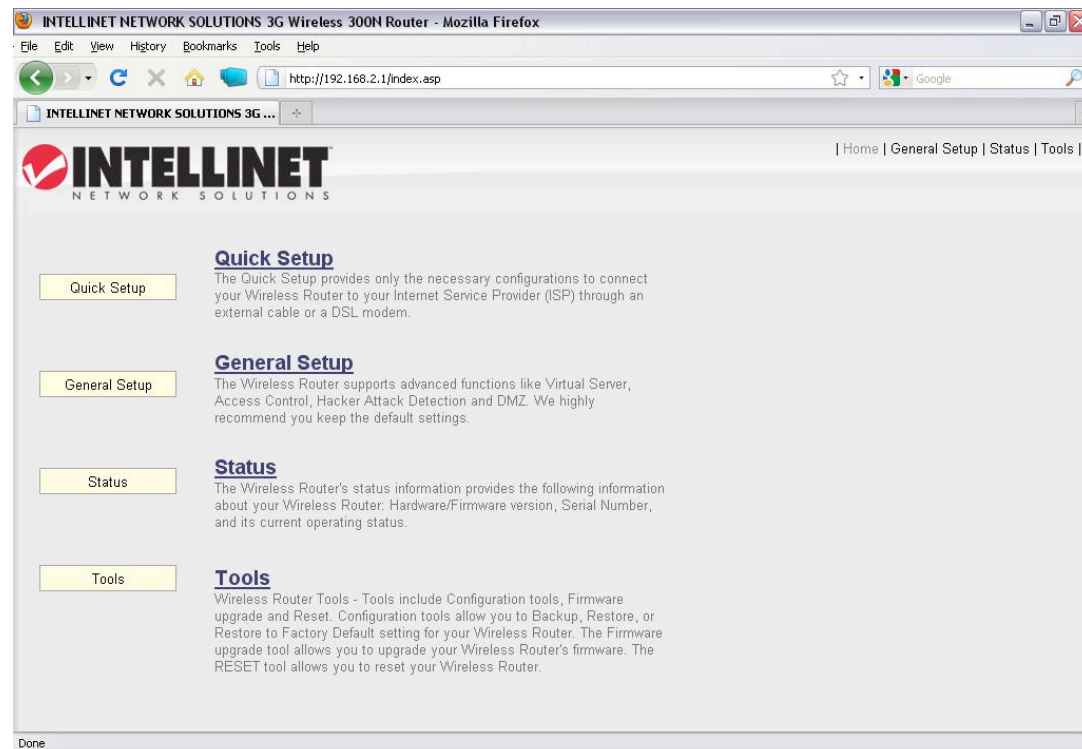
2-4-1 Time Zone and Time Auto-Synchronization

In the General Setup menu, click "System" on the left side of the Web management interface, then click "Time Zone." The following message will be displayed on your Web browser:

Set the time zone of the Wireless Router. This information is used for log entries and firewall settings.

Time Zone :	(GMT+00:00)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ∨
Time Server Address :	192.43.244.18
Daylight Savings :	☐ Enable Time From January ∨ 1 ∨ To January ∨ 1 ∨

APPLY   CANCEL

Below are descriptions of each option:

Time Zone (1):	*Select a time zone from the drop-down list.*
Time Server Address (2):	*Enter the IP address or host name of the time server here.*
Daylight Saving (3):	*Check the "Enable" box and set the duration of Daylight Saving.*

When you finish, click "Apply." You'll see the following message displayed on the Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
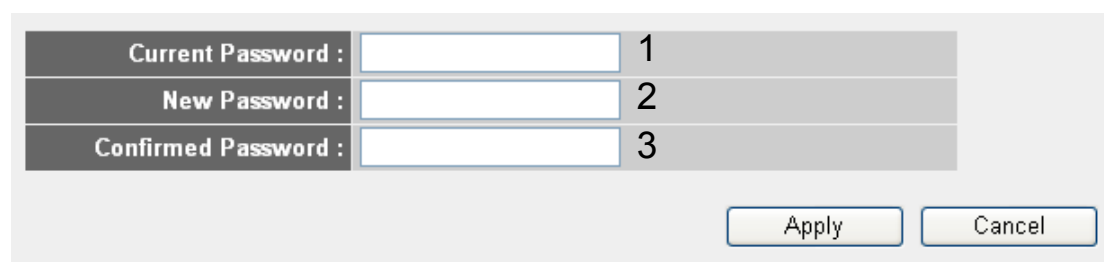
Continue   Apply

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: You can refer to the instructions given in last chapter, Using Quick Setup, for detailed descriptions on time zone settings.

2-4-2 Changing the Management Password

The default password of this router is 1234, and it's displayed on the login prompt when accessed from the 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." The following message will be displayed on your Web browser:

Current Password :		1
New Password :		2
Confirmed Password :		3

Apply   Cancel

Below are descriptions of each option:

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

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

If the password you entered in the "New Password" (2) and "Confirmed Password" (3) fields aren't the same, you'll see the following message:
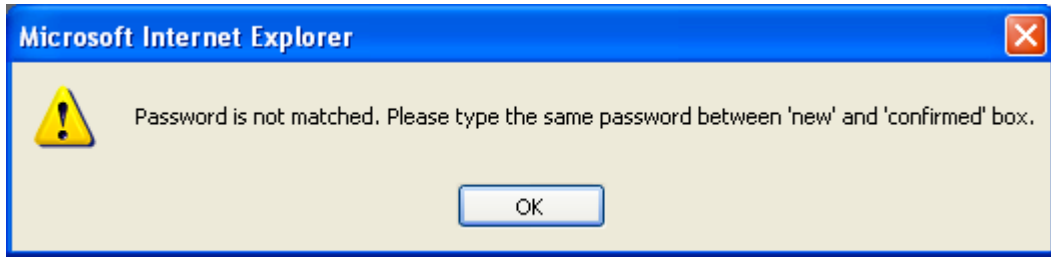
Re-enter the new password if you see above message.

If you see the *following* message, the content in the "Current Password" field is wrong. Click "OK" to go back to the previous menu, and try to enter the current password again.
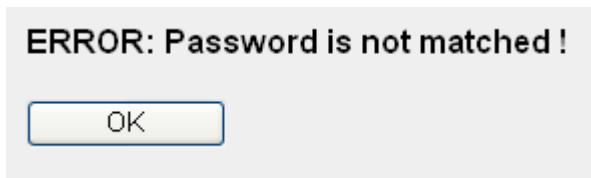
If the current and new passwords are correctly entered, after you click "Apply" you'll be prompted to enter your new password:
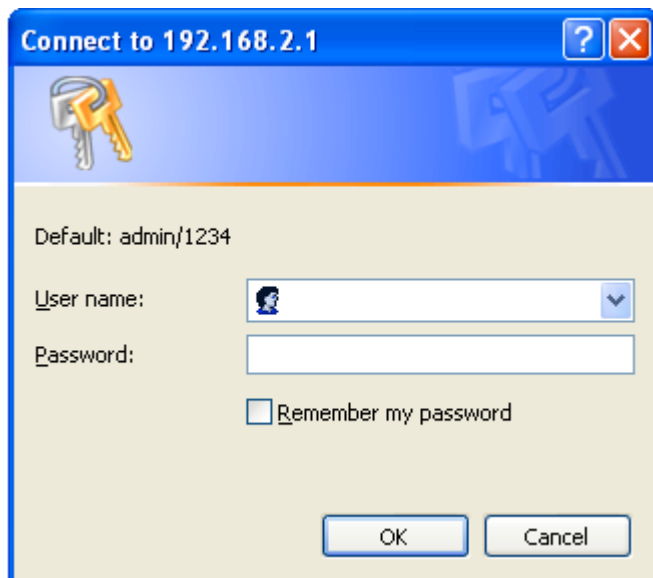
Use the new password to enter the Web management interface again, and you should be able to log in with new password.

2-4-3 Remote Management

This router does not allow management access from the Internet to prevent possible security risks (as when a too-simple password is used or when the default password isn't changed). However, you can still management 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." The following message will be displayed on your Web browser:

Host address		Port		Enabled	
0.0.0.0	1	8080	2	☐	3

Below are descriptions of each option:

Host Address (1):	*Input the IP address of the remote host for which you want to initiate management access.*
Port (2):	*You can define the port number through which the router should 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).*
Enabled (3):	*Select the field to start the configuration.*

When you finish the settings, click "Apply" and you'll see the following message displayed on the Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue]   [Apply]

Click "Continue" to save the settings and go back to the Web management interface; click "Apply" to save the settings 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 dynamic IP to host name mapping services like DDNS. Refer to section 2-5-8 DDNS Client for details.

NOTE: The default port number 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 Setting Up the Internet Connection (WAN)

Internet connection setup can be done by using Quick Setup as described in Section 2-3. However, you can also set up WAN connections up 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, and the screen below will be displayed on your Web browser.

Select an Internet connection method based on 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.
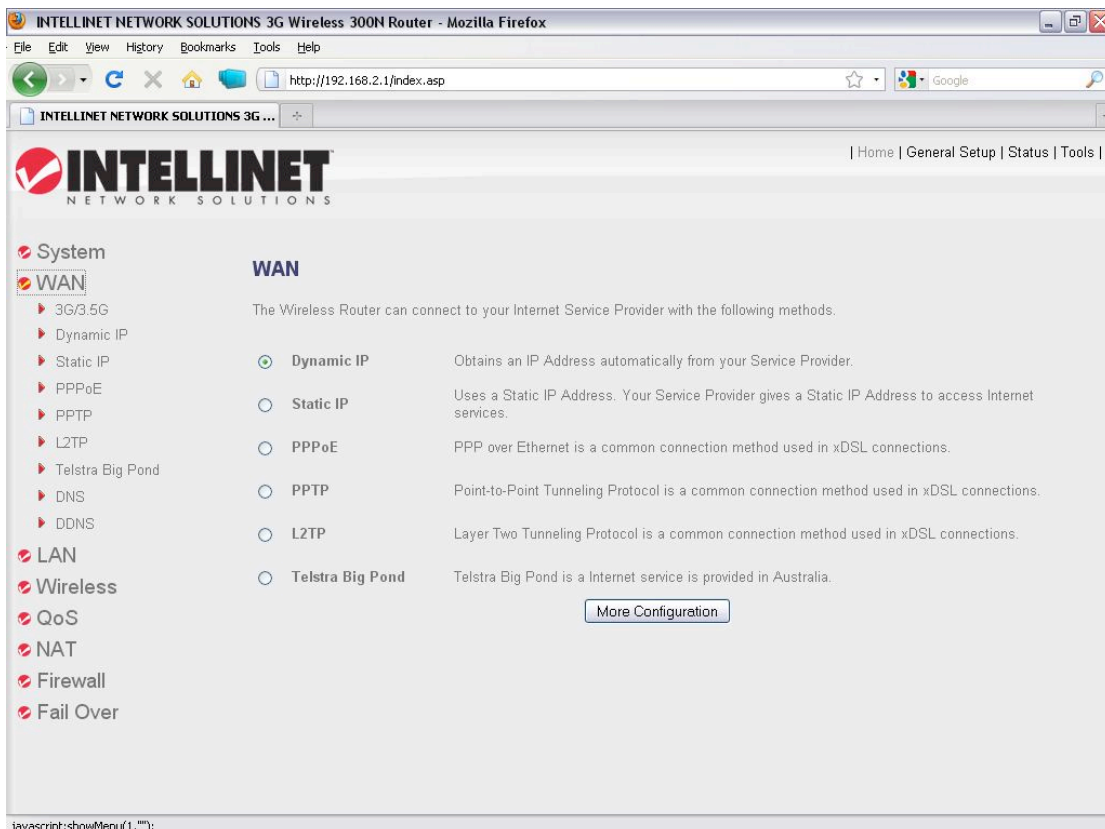
3G / 3.5G	- go to section 2-5-1
Dynamic IP	- go to section 2-5-2
Static IP	- go to section 2-5-3
PPPoE	- go to section 2-5-4

PPTP   - go to section 2-5-5
L2TP   - go to section 2-5-6
Telstra BigPond - go to section 2-5-7
DNS   - go to section 2-5-8
DDNS   - go to section 2-5-9

2-5-1 Setup Procedure for 3G / 3.5G

8

Below are descriptions of each option:

PIN Code (1):   *Enter the Pin Code for your UMTS or HSDPA connection. This is optional, and is required only if your service provider asks you to do so.*

APN (2):   *Enter the access point name.*

User Name (3):   *Enter the user name assigned by your Internet service provider here.*

Password (4):   *Enter the password assigned by your Internet service provider here.*

Verify Password (5): Enter the password again for confirmation.

Service (6):   Select your card type from the drop-down menu.

AT Dial Script (7): Enter the dialed number for your UMTS or HSDPA connection. The default is *99#. This field should not be altered except when required by your service provider.

After you finish the settings, click "Apply" (8); to remove any value you entered, click "Cancel."

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while router is rebooting.)

2-5-2 Setup Procedure for Dynamic IP

Dynamic IP

The Host Name is optional, but may be required by some Service Providers. The default MAC Address is set to the WAN physical interface on the Wireless Router. If required by your Service Provider, you can use the 'Clone MAC Address' button to copy the MAC Address of the Network Interface Card installed in your PC and replace the WAN MAC Address with this MAC Address.

Host Name :	1
MAC Address :	000000000000 2 [Clone MAC]

[APPLY] [CANCEL]
3

Below are descriptions of each option:

Host Name (1):	*Enter 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):	*Enter the MAC address of your computer if your service provider only permits computers with certain MAC addresses Internet access. If you're using a computer that's 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 the 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" to go back and continue with the router setup, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

2-5-3 Setup Procedure for Static IP

Below are descriptions of each option:

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

After you finish the settings, click "Apply" (4) and the following

message will be displayed on your Web browser:

Click "Continue" to go back and continue with the router setup, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-5-4 Setup Procedure for PPPoE

Below are descriptions of each option:

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

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

Service Name (3): *Enter a name for this Internet service. (This is optional.)*

MTU (4): *Enter the MTU value of your network connection here. If you don't know it, contact your ISP.*

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

Continuous – The connection will be kept on. If the connection is interrupted, the router will re-connect automatically.

Connect On-Demand – Only connects 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 the "Connect" button and "Disconnect" button. 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 the settings, click "Apply" (7) and the following message will be displayed on your Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue] [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-5-5 Setup Procedure for PPTP

PPTP requires two kinds of settings: WAN Interface Settings (set up an IP address) and PPTP Settings (PPTP user name and password). First, the WAN Interface Settings:

- **WAN Interface Settings**
  - ⊙ Obtain an IP Address Automatically
    - Host Name : [   ]
    - MAC Address : [000000000000] [Clone MAC]
  - ○ Use The Following IP Address
    - IP Address : [0.0.0.0]
    - Subnet Mask : [0.0.0.0]
    - Default Gateway : [0.0.0.0]

Select how you obtain an IP address from your service provider here. You can choose "Obtain an IP address Automatically" (equal to DHCP; refer to the Cable Modem section above), or "Use the Following IP Address" (i.e., static IP address).

WAN interface settings must be correctly set, or the Internet connection will fail even if the PPTP settings are correct. Contact

your Internet service provider if you don't know how you should fill in these fields.

Next, PPTP Settings:

Below are descriptions of each option:

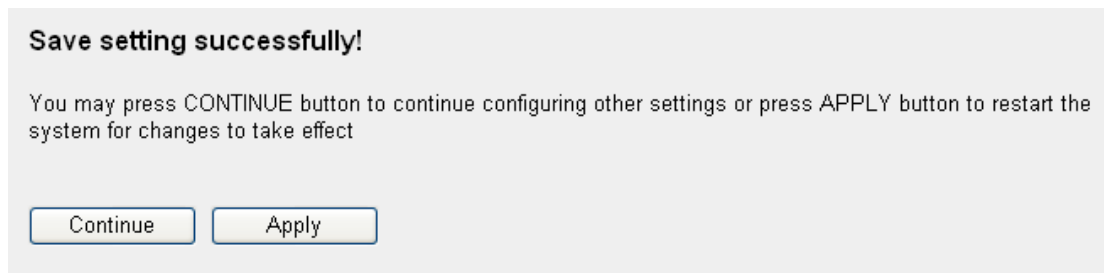|	
User Name (1):	*Enter the user name assigned by your Internet service provider here.*
Password (2):	*Enter the password assigned by your Internet service provider here.*
PPTP Gateway (3):	*Enter the IP address of PPTP gateway assigned by your Internet service provider here.*
Connection ID (4):	*Enter the connection ID here. (This is optional: You can leave it blank.)*
MTU (5):	*Enter the MTU value of your network connection here. If you don't know it, contact your ISP.*
BEZEQ-ISRAEL (6):	*If you are connecting to the BEZEQ network in Israel, enable this function.*

Connection Type (7):   *Select the connection type of the Internet connection you want to use. (Refer to section 2-5-3 for detailed descriptions.)*

Idle Time Out (8):   *Enter the idle time out of the Internet connection you want to use. (Refer to section 2-5-3 for detailed descriptions.)*

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
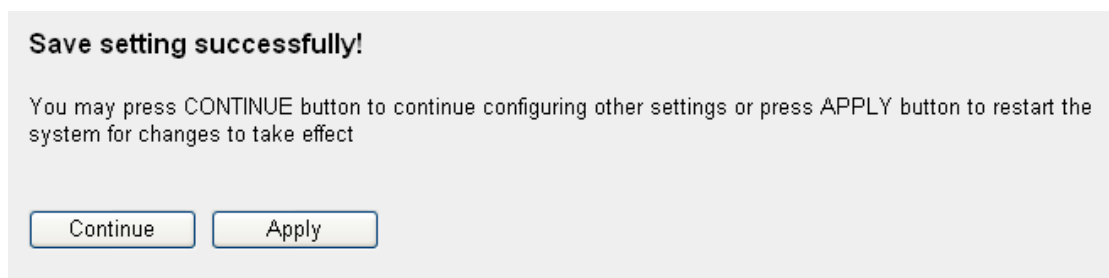
Continue   Apply

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-5-6 Setup Procedure for L2TP

- **L2TP Settings**

User Name :		1
Password :		2
L2TP Gateway :		3
MTU :	1392 (512<=MTU<=1492)	4
Connection Type :	Continuous Connect Disconnect	5
Idle Time Out :	10 (1-1000 Minute)	6

APPLY   CANCEL

7

Below are descriptions of each option:

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

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
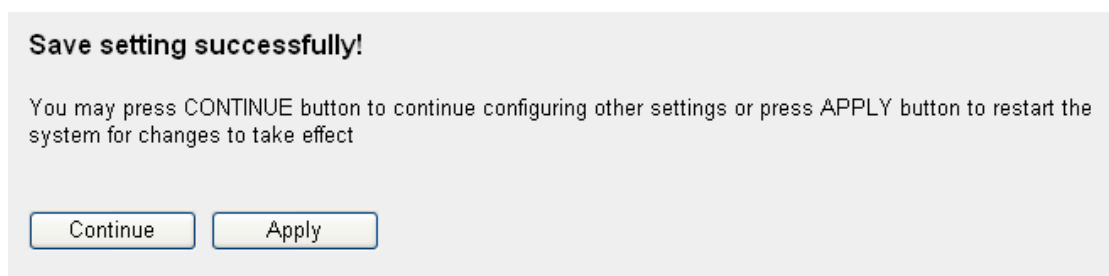
[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-5-7 Setup Procedure for Telstra BigPond

These settings only work when you're using Telstra BigPond's network service in Australia.

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

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue   Apply

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-5-8 Setup Procedure for DNS

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

DNS

A DNS (Domain Name System) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.

Primary DNS : _____ 1
Secondary DNS : _____ 2

3 APPLY   CANCEL

Below are descriptions of each option:

Primary DNS (1):	*Enter the IP address of the DNS server provided by your service provider.*
Secondary DNS (2):	*Enter the IP address of another DNS server provided by your service provider (this is optional).*

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

10.20.30.40………………………………………………………………… Correct

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-5-9 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 such a user wants to provide services to other users on the Internet because their IP address will vary every time they connect to the Internet, and other users will not be able to know the IP address they're using at a certain time.

This router supports the DDNS service of several service providers; for example:

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

Go to one of the DDNS service provider's Web site listed above, and get a free DDNS account using the instructions they provide.

Below are descriptions of each option:

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

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

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

Account / *Enter account or e-mail of DDNS registration.*
E-Mail (4):

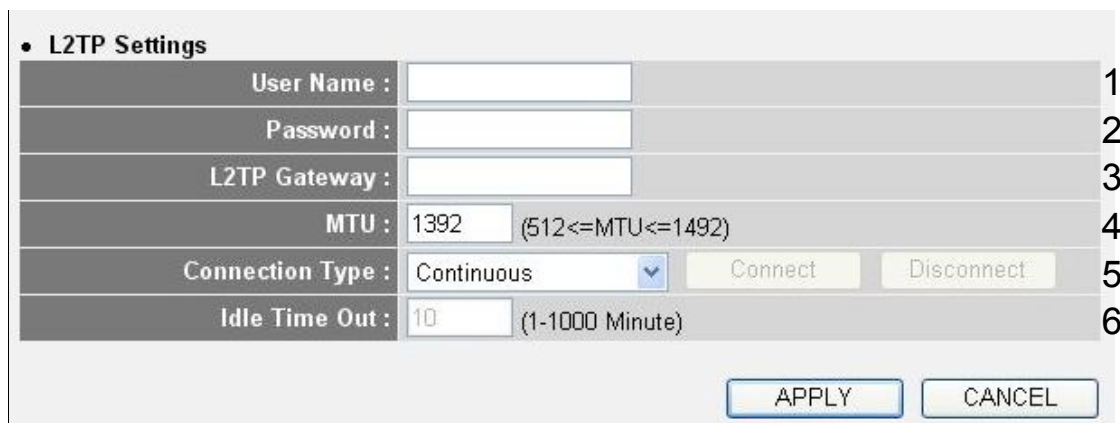*Password / Key (5):* *Enter the DDNS service password or key.*

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

Click "Continue" to go back and continue with the router setup

procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

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

2-6 Wired LAN Configurations

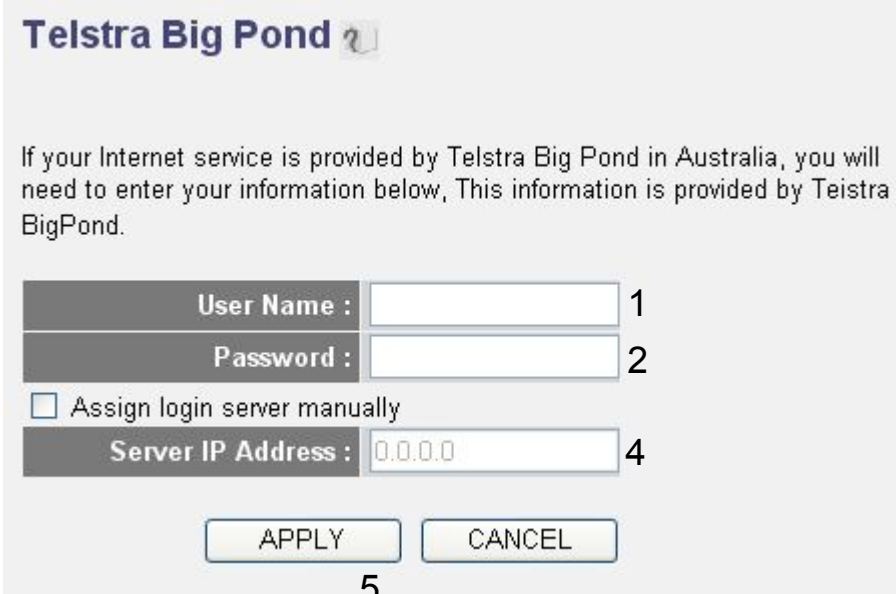Before all computers using wired Ethernet connections (i.e., those computers connect to this router's LAN ports 1 to 4 by Ethernet cable) can communicate with each other and access the Internet, they each must have a valid IP address.

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 addresses of computers will be assigned by the router automatically). It's recommended that most of the computers 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 that will provide services to other computers and users that come from the Internet, a static IP address should be used so other computers can locate the server.

Suggestions for a IP address numbering plan:

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 company users, it's suggested to use 192.168.c.d, where c is an integer between 0 and 254, and d is an integer between 1 and 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 between 1 and 254), and pick a number between 0 and 254 for field "c."**
2. **In most cases, you should use 255.255.255.0 for the subnet mask, which allows up to 253 clients (this also matches the router's ability to work with up to 253 clients).**
3. **For all servers and network devices that will provide services to other people (like Internet service, print service and file service), they should use a static IP address. Give each of them a unique number between 1 and 253, and maintain a list so everyone can locate those servers easily.**
4. **For computers that are not dedicated to providing specific service to others, they should use a dynamic IP address.**

If you don't really understand the descriptions listed above, don't worry! We will provide recommended setup values below.

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."

2-6-1 LAN IP

Below are descriptions of the options:

IP address (1):   Enter the IP address of this router.

Subnet Mask (2):   Enter the subnet mask for this network.

802.1d   If you want to activate the 802.1d Spanning Spanning Tree (3): Tree function, select "Enabled."

DHCP Server (4):   If you want to activate the DHCP server function of this router, select "Enabled."

> **Recommended values 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 "LAN IP" is enabled. Below are descriptions of the options:

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):   *Enter the start IP address of the IP range.*

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

Domain Name (4): If you wish, you can also optionally input the domain name for your network.

Recommended values 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)
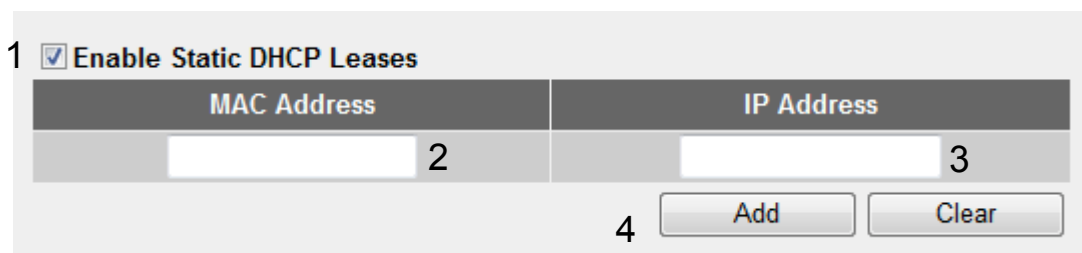
NOTE:

1. **The number of the last field (the "d" field) of "End IP" must be greater than "Start IP" and can't be the same as the router's IP address.**
2. **The first three fields of the IP address of "Start IP," "End IP" and "IP Address" of "LAN IP" ("a," "b" and "c") should be the same.**
3. **These settings will affect wireless clients, too.**

2-6-3 Static DHCP Leases Table

This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, but can still enjoy the benefit of using DHCP server. A maximum of 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 this way).

Below are descriptions of the options:

Enable Static DHCP Leases (1):	*Check this box to enable this function; otherwise uncheck it to disable this function.*
MAC Address (2):	*Input the MAC address of the computer or network device (total 12 characters, with characters from 0 to 9, and from a to f, such as "001122aabbcc").*
IP Address (3):	*Input the IP address you want to assign to this computer or network devic.e*
Add (4):	*After you enter the MAC address and IP address pair, click this button to add the pair to the static DHCP leases table.*

To remove all characters you just entered, click "Clear."

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

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

After you finish all LAN settings, click "Apply" at the bottom of this page. After you click "Apply," the following message will be displayed on your Web browser:

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the 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 let them 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 malicious intruders.

Click Wireless on the left side of the Web management interface, and the message below will be displayed on your Web browser. You must enable the wireless function of this router; otherwise, the wireless interface of this router will not function. Select "Enable" (1), then click "Apply" (2).

To disable the wireless function, select "Disable" (3), then click "Apply" (2).

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

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

2-7-1 Basic Wireless Settings

Click Wireless on the left side of the Web management interface, then click "Basic Settings." The following message will be displayed on your Web browser:

Below are descriptions of the options:

Band (1):   Select the radio band you want to use from the drop down menu. The following information will be displayed:

2.4 GHz (B)	*2.4GHz band only allows 802.11b wireless network clients to connect to this router (maximum transfer rate 11 Mbps).*
2.4 GHz (N)	*2.4GHz band only allows 802.11n wireless network clients to connect to this router (maximum transfer rate 150 Mbps).*
2.4 GHz (B+G)	*2.4GHz band only allows 802.11b and 802.11g wireless network clienst to connect to this router (maximum transfer rate 11 Mbps for 802.11b clients; 54 Mbps for 802.11g clients).*
2.4 GHz (G)	*2.4GHz band only allows 802.11g wireless network clienst to connect to this router (maximum transfer rate 54 Mbps).*
2.4 GHz (B+G+N)	*2.4GHz band allows 802.11b, 802.11g and 802.11n wireless network clients to connect to this router (maximum transfer rate 11 Mbps for 802.11b clients; 54 Mbps for 802.11g clients; 150 Mbps for 802.11n clients).*

NOTE: For 802.11b and 802.11g mode, the signals can be transmitted only by antenna 1 (the antenna on the right side of the rear panel).

For 802.11n mode: The router is operating in a 2T2R Spatial Multiplexing MIMO configuration. 2 antennas are for signal transmitting and 2 antennas are for signal receiving.

SSID (2):   *This is the name of the wireless router. You can type any alphanumerical characters here (maximum of 32 characters). ESSID is used to identify your own wireless router from others when there are other wireless routers in the same area. The default SSID is "INTELLINET";*

it's recommended to change default ESSID name to one that is meaningful to you, such as "myhome," "office_room1," etc.

Channel Number (3):	*Select a channel from the drop-down list. Available channel numbers are 1 to 13 for European countries; 1 to 11 for the U.S. You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use. Some wireless clients support manual channel number select, which would help in certain scenarios where there is some radio communication problem.*
Associated Clients (4):	*Click "Show Active Clients" and an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the router.*

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

TIPS: You can try changing 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.

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

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router is rebooting.)

2-7-2 Advanced Wireless Settings

This router provides some advanced control of wireless parameters. Click Wireless on the left side of the Web management interface, then click "Advanced Settings" and the following message will be displayed on your Web browser:

Below are descriptions of the options:

Fragment Threshold (1):   Set the threshold of the wireless radio. **Do not modify the default value if you don't know what it does (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 does (default value is 2347).**

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

Data Rate (5):   Set the wireless data transfer rate to a certain value. 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 clients.

Channel Width (7): Set the channel width. **Do not modify the default value if you don't know what it does (default setting is "Auto 20/40 MHz").**

Preamble Type (8): Set the type of preamble. **Do not modify the default value if you don't know what it does (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 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 wireless router in a really big space, you may not have to set output power to 100%. **This will enhance security (distant malicious/unknown users won't be able to reach your wireless router).**

WMM (12): Wi-Fi MultiMedia will enhance the data transfer performance of multimedia content when it's being transferred over the 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" (though the default is "Disable").**

After you finish these wireless settings, click "Apply" (13) and the following message will be displayed on your Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
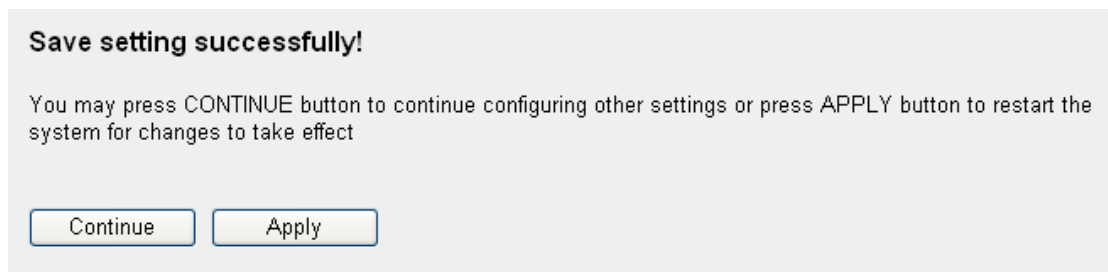
Continue   Apply

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

2-7-3 Wireless Security

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

Click Wireless on the left side of the Web management interface, then click "Security Settings."

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 or disabling ESSID broadcast).

Only use this option when you really want to allow everyone to use your wireless router and you don't care if someone reads 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:

Encryption :	WEP ▼	1
Key Length :	64-bit ▼	2
Key Format :	Hex (10 Characters) ▼	3
Default Tx Key :	Key 1 ▼	4
Encryption Key 1 :	**********	5
Encryption Key 2 :	**********	6
Encryption Key 3 :	**********	7
Encryption Key 4 :	**********	8

9 ☐ **Enable 802.1x Authentication**

10 [APPLY] [CANCEL]

Below are descriptions of the options:

Key Length (2): *There are two types of WEP key length: 64-bit and 128-bit. "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 the key will be displayed. For example, if you select "64-bit" as the key lengt, 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 unsure, select "Key 1."***

Encryption Key 1 to 4 (5-8): *Input WEP key characters here. 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; if you enter multiple WEP keys, they should all be different.

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 users by IEEE 802.1x, but it does not encrypt the data during communication. If there is a RADIUS server in your environment, enable this function. Check this box and another sub-menu will appear:*

☑ Enable 802.1x Authentication		
RADIUS Server IP Address :		11
RADIUS Server Port :	1812	12
RADIUS Server Password :		13

RADIUS Server IP Address (11):   *Enter the IP address of the RADIUS server here.*

RADIUS Server Port (12):   *Enter the port number the RADIUS server here.*

RADIUS Server Password (13):   *Enter the RADIUS server password here.*

TIPS: Some examples of WEP keys (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 found in a dictionary or which are too easy to remember! ("pilot" and "phone" are examples of bad choices). Wireless clients will remember the WEP key, so you only have to input the WEP key for a wireless client once.

After you finish the WEP settings, click "Apply" (10) and the following will be displayed on your Web browser:
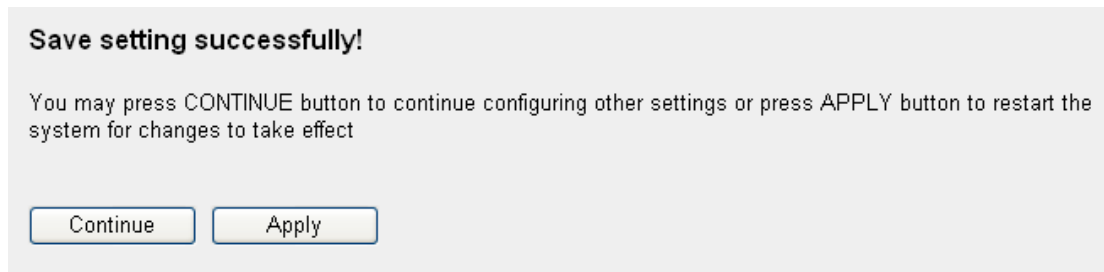
Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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:

Below are descriptions of the options:

_____

WPA Unicast   *Select a type of WPA cipher suite.*
Cipher Suite (2):   *Options are "WPA (TKIP)," "WPA2 (AES)" and "WPA2 Mixed." You can select any one of them, but you have to make sure your wireless client supports the cipher you select.*

Pre-shared Key Format (3):	*Select the type of pre-shared key. You can select Passphrase (8 or more alphanumerical characters, up to 63), or Hex (64 characters of 0-9 and a-f).*
Pre-shared Key (4):	*Enter the WPA passphrase here.* ***It's not recommended to use a word that can be found in a dictionary due to security reasons.***

After you finish the WPA Pre-shared Key settings, click "Apply" (5) and the following will be displayed on your Web browser:
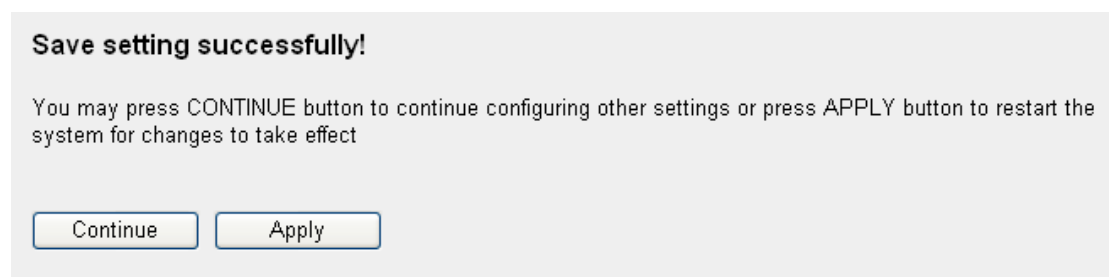
Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

NOTE: Some wireless clients (especially those manufactured before year 2003) only support WEP or WPA (TKIP) cipher. 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.

Encryption :	WPA RADIUS ▼	1
WPA Unicast Cipher Suite :	⊙ WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed	2
RADIUS Server IP Address :		3
RADIUS Server Port :	1812	4
RADIUS Server Password :		5
	APPLY CANCEL	

6

Below are descriptions of the options:

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

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

| Continue | Apply |

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

2-7-4 Wireless Access Control

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

Up to 20 MAC addresses can be assigned by using this function. Click 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 "MAC Address Filtering Table" (1).

Below are descriptions of the options:

Delete (2):	*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." (You can select more than one MAC address).*
Delete All (3):	*If you want to delete all the MAC addresses listed here, click "Delete All."*

Enable Wireless   *To enforce MAC address filtering, check*
Access Control (4): *"Enable Wireless Access Control." When this*
     item is unchecked, the router will not enforce
     MAC address filtering of wireless clients.

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

Comment (6):   *You can input any text here as a comment about*
     this MAC address, like "Room 2A Computer."
     Enter up to 16 alphanumerical characters here.
     This is optional and you can leave it blank.

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

Clear (8):   *Click "Clear" to remove the value you entered in*
     "MAC Address" and "Comment" fields.

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
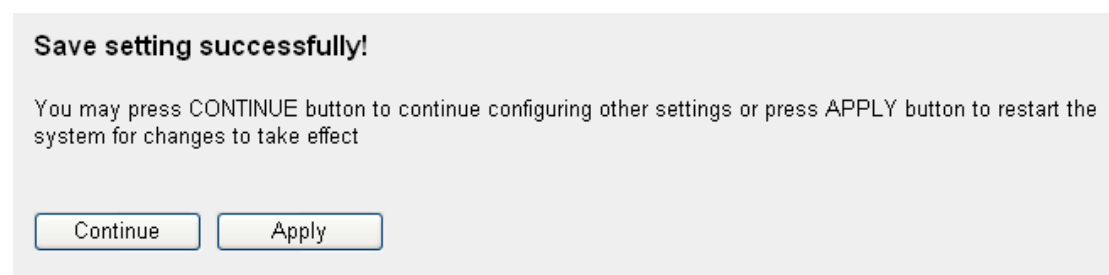
[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

If you want to reset all settings on this page 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 need to press a button on the wireless client and this wireless router, and the 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 need 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 on this wireless router or click "Start PBC" on the Web configuration interface to do this; if you want to use PIN Code, you need 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.

Click Wireless on the left side of the Web management interface, then click "WPS." The following message will be displayed on your Web browser:

Below are descriptions of the options:

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

Wi-Fi Protected Setup 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 "Configured" here. If the function has not been set, you'll see "unConfigured."

Self PIN code: This is the WPS PIN code of this wireless router. This code is useful when you need to build a wireless connection using 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 enable the security function of the wireless router before WPS is activated, the router will auto-set the security to WPA2 Mixed 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 selected, wireless clients will follow the router's wireless settings for WPS connection. When "Enrollee" is selected, the router will follow the settings of the wireless client for WPS connection.

Configure by Push Button (4):	*Click "Start PBC" to start Push Button-style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The WLAN LED on the wireless router will be lit for 2 minutes when this wireless router is waiting for incoming WPS requests.*
Configure by Client PinCode (5):	*Enter the PIN code of the wireless client you want to connect to, and click "Start PIN." The WLAN LED on the wireless router will be lit when this wireless router is waiting for incoming WPS requests.*

2-7-6 Security Tips for 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) as WEP encryption or WPA passphrases.

2. A complicated (lengthy combination of numbers, letters and even symbols) WEP key and WPA passphrase is much safer than a simple and short one. Remember that the wireless client is able to keep the key or passphrase for you, so you only have to input the complicated key or passphrase once. It's not too much trouble, and it will greatly improve your security level.

3. You can hide the ESSID of this router by setting "Broadcast ESSID" 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 client, and this can reduce the chance of being hacked.

4. Use Access Control described in Section 2-7-4 so those 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 to get Internet bandwidth, and some applications which require guaranteed bandwidth (like video streaming and network telephone) will be affected, possibly resulting 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 this and other problems.

3-1-1 Basic QoS Settings

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

Below are descriptions of the options:

Enable QoS (1):	*Check this box to enable the QoS function; de-select this box if you don't want to enforce QoS bandwidth limitations.*
Total Download Bandwidth (2):	*You can set the limit of total download bandwidth in kbits. To disable the download bandwidth limitation, enter "0" here.*
Total Upload Bandwidth (3):	*You can set the limit of total upload bandwidth in kbits. To disable the upload bandwidth limitation enter "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 below).*
Edit (6):	*If you want 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 a time!** If you didn't select a rule before clicking "Edit," you'll be prompted to add a new rule.*
Delete Selected (7):	*You can delete selected rules by clicking this button. You can select one or more rules to delete by checking the "Select" boxes 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 this button, 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 the settings, click "Apply" (11) and the following message will be displayed on your Web browser:
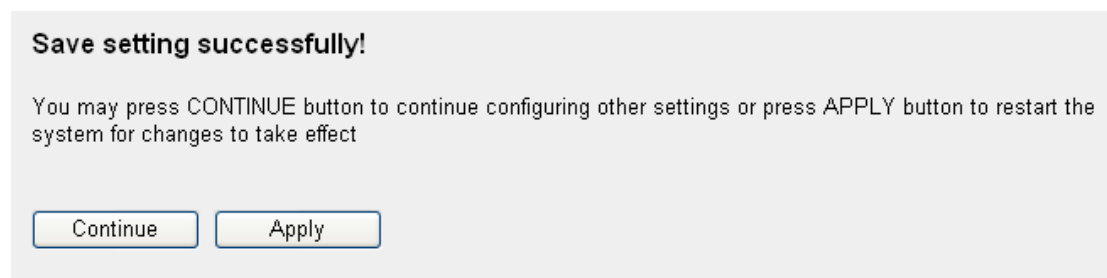
Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-1-2 Adding a New QoS Rule

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

Rule Name :		a
Bandwidth :	Download ▼ Kbps Guarantee ▼	b
Local IP Address :	-	c
Local Port Range :		d
Remote IP Address :	-	e
Remote Port Range :		f
Traffic Type :	None ▼	g
Protocol :	TCP ▼	h
	Save Reset	

i

Below are descriptions of the options:

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

Bandwidth (b):   *Set the bandwidth limitation of this QoS rule. You need to select the data direction of this rule (Upload or Download), and the speed of 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 be affected by this rule. Enter the starting IP address in the left field and enter the end IP address in the right field to define a range of IP addresses, or just enter the IP address in the left field to define a single IP address.*

Local Port Range (d):   *Enter 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, enter "80-90"; if you want to apply this rule on a single port, just enter the port number, such as "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 number that will be affected by this rule. If you want to apply this rule on ports 80 to 90, input "80-90"; if you want to apply this rule on a single port, just input the port number, such as "80." If the remote (destination) IP address and/or port number is universal, just leave it blank.*
Traffic Type (g):	*Select the traffic type of this rule. Options are "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 traffics from/to the specified IP address/port number), select "None."*
Protocol (h):	*Select the protocol type of this rule. Options are "TCP" and "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 the 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 you did anything wrong, you'll get an error message when you click "Save." Correct your entry as instructed by the error message.

If you want to erase all the values you just entered, click "Reset."

3-2 Network Address Translation (NAT)

Network address translations solve the problem of sharing a single IP address on 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 only a very few IP addresses to each user. Therefore, it's necessary to use NAT technology to share a single Internet IP address on multiple computers on a local network so everyone can get connected to the Internet.

3-2-1 Basic NAT Settings

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

To enable the NAT function, select "Enable"; to disable, select "Disable."

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue   Apply

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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 the Internet IP address and private IP address (the IP address on the local network) must be the same. If the port numbers of the Internet IP address and private IP address are different, use the Virtual Server function described in the 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:

Below are descriptions of the options:

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 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. If you only want 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 entered values.*
Port Forwarding Table (9):	*All existing port forwarding mappings will be displayed here.*
Delete (10):	*Select a port forwarding mapping by clicking the "Select" box of the mapping, then click "Delete Selected" to remove the mapping. If there's no existing mapping, this button will be grayed out.*
Delete All (11):	*Delete all mappings in the virtual server table.*

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
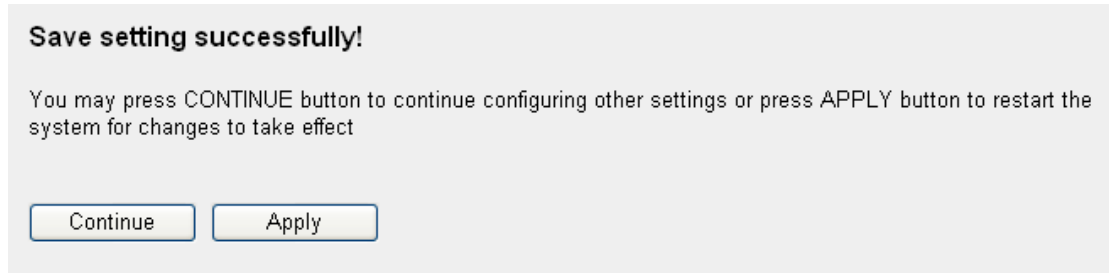
[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-2-3 Virtual Server

This function allows you to redirect a port on the Internet IP address (on a 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:

Below are descriptions of the options:

Enable Virtual Server (1):	*Check this box to enable the virtual server; uncheck this box to disable it.*
Private IP (2):	*Input the IP address of the computer which provides Internet service.*
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.*
Private Port (4):	*Input the port number of the IP address which 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 entered values.*

Virtual Server　　*All existing virtual server mappings will be*
Table (10):　　　　*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 button will be grayed out.

Delete All (12):　　*Delete all mappings in the virtual server table.*

Reset (13):　　　　*Unselect all mappings.*

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


```
Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the
system for changes to take effect

  [ Continue ]   [ Apply ]
```
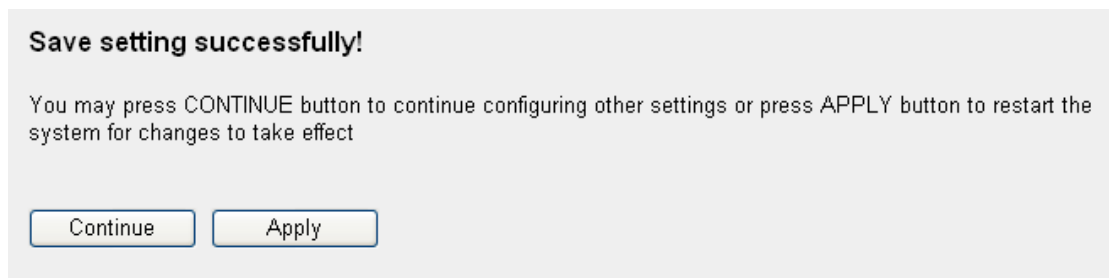
Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-2-4 Port Mapping for Special Applications

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

Below are descriptions of the options:

Enable (1):	*Check this box to enable special applications; uncheck this box to disable the virtual server.*
IP Address (2):	*Input the IP address of the computer 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 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):	*Enter a description of this setting.*

Popular Applications (7):	*This section lists the more popular applications that require multiple connections. Select an application from the "Popular Applications" section and click "Add" to save the setting to "Current Trigger-Port Table."*
Add (8):	*Add the setting to the "Current Trigger-Port Table."*
Reset (9):	*Click to clear all the above settings.*
Current Trigger - Port Table (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 then click "Delete Selected." If you want 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 button will be grayed out.*
Delete All (12):	*Delete all settings in the 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 the settings, click "Apply" (14) and the following message will be displayed on your Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue   Apply

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-2-5 UPnP Settings

This function enables network auto-configuration for peer-to-peer communications. With this function, network devices will be able to communicate with other devices directly and learn about them. Many network device and applications rely on the UPnP function nowadays.

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

UPnP Module : ○ Enable ◉ Disable

APPLY   CANCEL

There is only one option on this page: Select "Enable" or "Disable" to enable or disable the UPnP function, then click "Apply." The following message will be displayed on your Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue] [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

If you want to reset all settings on this page 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, allowing them to work with the 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:

Enable	Name	Comment
☑	Amanda	Support for Amanda backup tool protocol.
☑	Egg	Support for eggdrop bot networks.
☑	FTP	Support for FTP.
☑	H323	Support for H323/netmeeting.
☑	IRC	Allows DCC to work though NAT and connection tracking.
☑	MMS	Support for Microsoft Streaming Media Services protocol.
☑	Quake3	Support for Quake III Arena connection tracking and nat.
☑	Talk	Allows netfilter to track talk connections.
☑	TFTP	Support for TFTP.
☑	IPsec	Support for IPsec passthrough
☐	Starcraft	Support for Starcraft/Battle.net game protocol.
☐	MSN	Support for MSN file tranfer.
☑	PPTP Pass Through	Support for PPTP passthrough.

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:
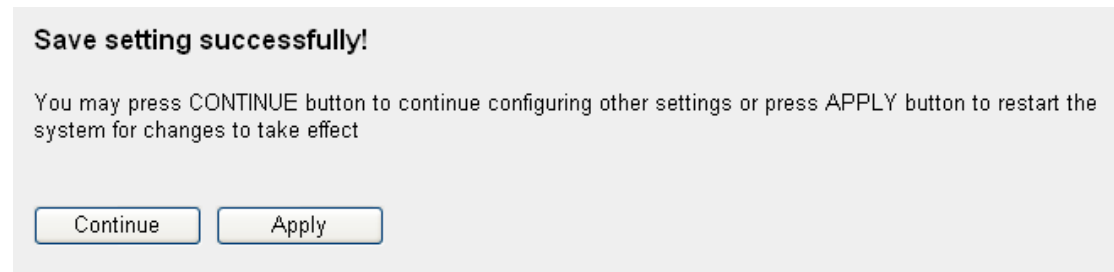
Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

| Continue | Apply |

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-3 Firewall

In addition to NAT, this router provides firewall functions to block malicious intruders from accessing your computers on your local network. These functions include inbound attack prevention and blocking of outbound traffic, such as blocking URLs that have pre-defined keywords.

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

Firewall

The Wireless Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Firewall Module :   ○ Enable   ● Disable
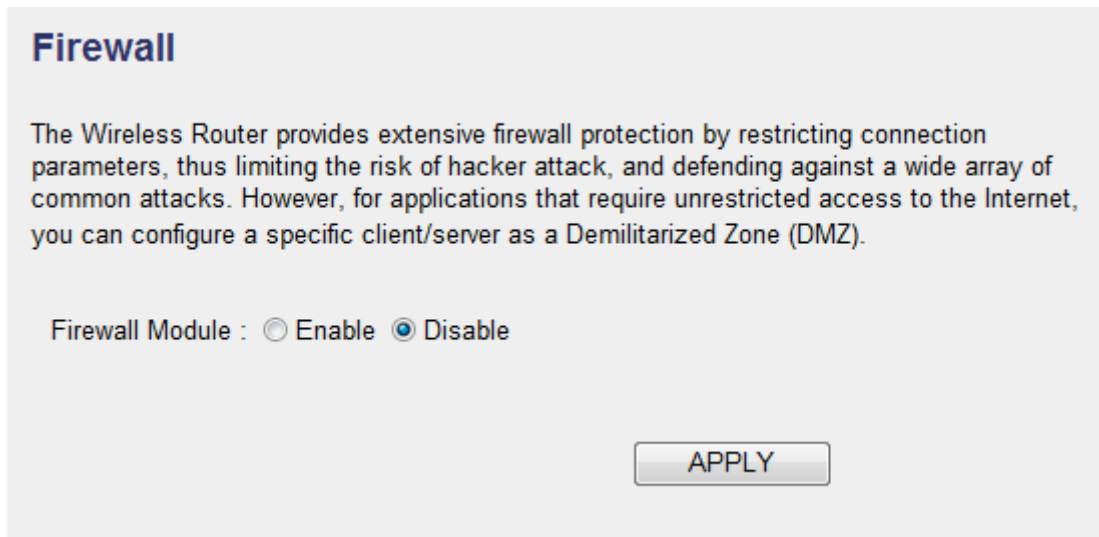
APPLY

Select "Enable" or "Disable" to enable or disable the firewall functions of this router, then click "Apply." The following message will be displayed on your Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

Continue   Apply

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

3-3-1 Access Control

This function allows or denies computers with specific MAC addresses access to the network; it can also allow or deny computers with a specific IP address, protocol or port.

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:

Below are descriptions of the options:

Enable MAC Filtering (1):	*Check this box to enable MAC address based filtering, and select "Deny" or "Allow" to determine the behavior of the MAC filtering table. If you select "Deny," all MAC addresses listed in filtering table will be denied 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, and all other network devices will be rejected.*
Client PC MAC address (2):	*Enter the MAC address of the computer or network device here. Dashes (-) and colons (:) are not required; i.e., if the MAC address label of your wireless device is "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 a comment about this MAC address, such as "ROOM 2A Computer." Enter up to 16 alphanumerical characters. This is optional and you can leave it blank.*
Add (5):	*Click to add the MAC address and associated comments to the MAC address filtering table.*
Reset (6):	*Remove all entered values.*
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 Table (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 filtering table will be denied 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, and all other network devices will be rejected.

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 Selected (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 the settings, click "Apply" (16) and the following message will be displayed on your Web browser:
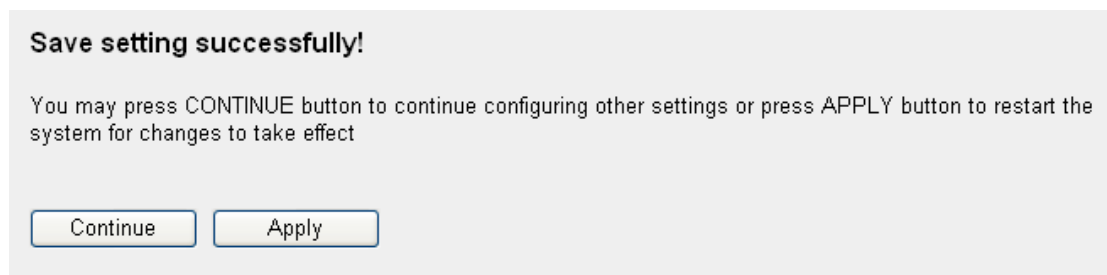
Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect

[Continue]　[Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

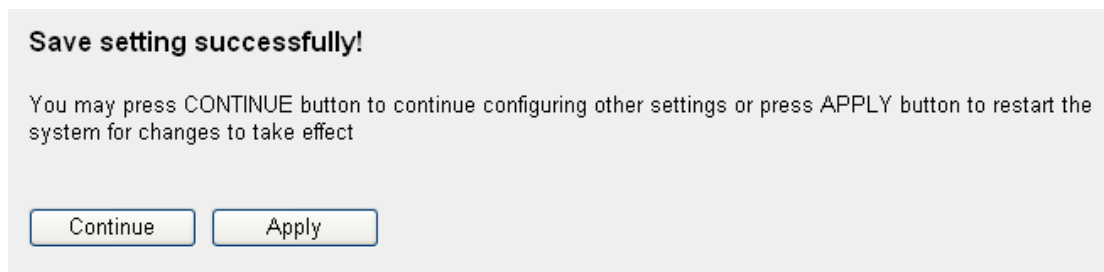If you want to reset all settings on this page back to previously saved values, click "Cancel."

3-3-1-1 Add PC

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

Client PC Description :		a
Client PC IP address :	-	b

Client PC Service :

Service Name	Detail Description	Select
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	☐
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☐
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☐
NetMeeting	H.323, TCP Port 389,522,1503,1720,1731	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐
VPN-PPTP	TCP Port 1723	☐
VPN-L2TP	UDP Port 1701	☐
TCP	All TCP Port	☐
UDP	All UDP Port	☐

c

User Define Service		
Protocol:	Both ⌄	d
Port Range:		e

[Add] [Reset]

f

Below are descriptions of the options:

Client PC Description (a):	*Enter any text to describe this IP address. (Up to 16 alphanumerical characters.)*
Client PC IP	*Input the starting IP address in the left*

address (b):	*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 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 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, such as "80."*
Add (f):	*When you finish with the 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 page, click "Reset."

3-3-2 URL Blocking

If you want to prevent computers on the local network from accessing certain Web sites (like pornography, violence or anything else you want to block), you can use this function, which is popular among parents and company managers.

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

Below are descriptions of the options:

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 the Web site, like http://www.blocked-site.com or http://11.22.33.44), or the keyword that is contained in the URL (like pornography, cartoon, stock or anything).*
Add (3):	*Click to add the UR /keyword to the URL/ Keyword filtering table.*
Reset (4):	*Click to remove the entry you entered in the URL/Keyword field.*
Current URL Blocking Table (5):	*All existing URL/Keywords in the filtering table will be listed here.*
Delete Selected (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 URL/Keyword entries listed here, click "Delete All."*

Reset (8):   *You can also click "Reset" to unselect all URL/Keyword entries.*

After you finish the settings, click "Apply" (9) and the following message will be displayed on your Web browser:
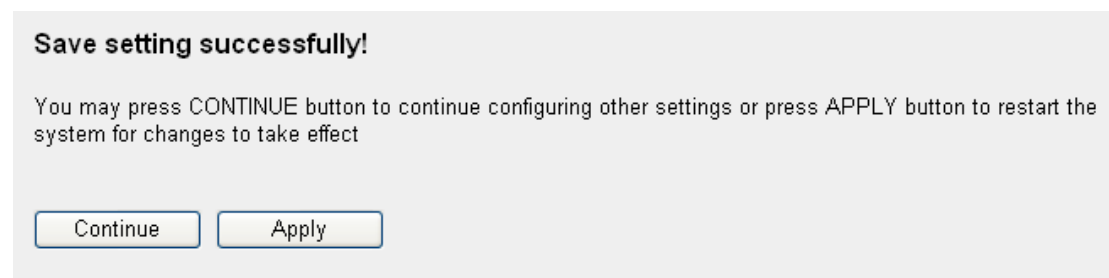
Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-3-3 DoS Attack Prevention

Denial of Service (DoS) is a common attack measure that works by transmitting 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 the 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:
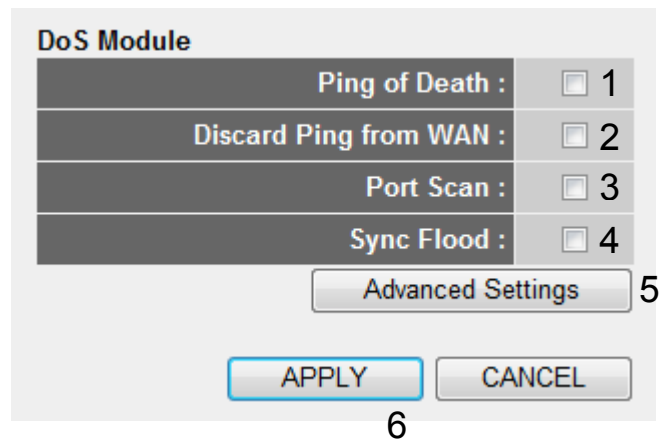
Below are descriptions of the options:

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 for learning
the connection status of a specified remote
network device. A malicious intruder may 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. When you activate this
function, however, you will not be able to ping
your own router from the Internet.*

Port Scan (3):   *A malicious intruder may try to use a port
scanner to learn how many ports of your
Internet IP address are open. 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 that uses a lot of
fake connection requests to consume the
memory of your server, trying to make your*

server become 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 the settings, click "Apply" (9) and the following message will be displayed on your Web browser:

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
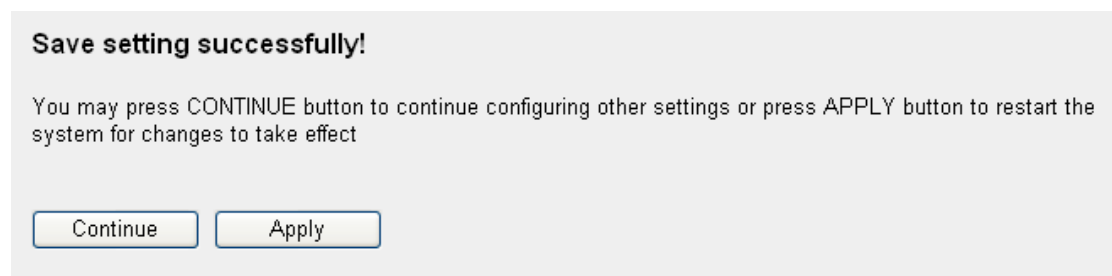
[Continue]   [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-3-3-1 DoS - Advanced Settings

Click "Advanced" in the DoS menu and the following message will be displayed on your Web browser:

Below are descriptions of the options:

Ping of Death (a):	*Set the threshold for when this DoS prevention mechanism will be activated. Check the box of 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 of the 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 the settings, click "Apply" (e) and the following message will be displayed on your Web browser:

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

If you want to reset all settings on this page 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 in which all computers use private IP addresses that are mapped to a certain Internet IP address so other people on the Internet can fully access those computers in the 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:

Below are descriptions of the options:

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

Public IP address (2):   *You can select "Dynamic IP" or "Static IP" here. If you select "Dynamic IP," you need to select an Internet connection session from the drop-down menu; if you select "Static IP," input the IP address that 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 to add the public IP address and associated private IP address to the DMZ table.*

Reset (6):   *Click "Reset" to remove the value you entered in the "Public IP" 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 entry.)*

Delete All (9):   *Click to delete all DMZ entries listed here.*

Reset (10):　　　　　*You can also click "Reset" to unselect all DMZ entries.*

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
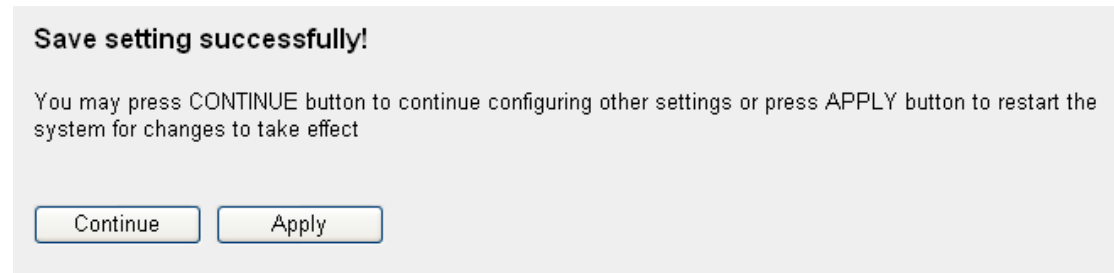
[Continue]　[Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

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

3-4 FailOver

WAN failure detection works by detecting the presence of traffic on the 3G modem link. If the link is idle for too long, the router will attempt to ping a target IP address. If the ping does not reply, the router assumes the link is down and attempts to fail over to an Ethernet WAN link.

Configure the priority of existing WAN connections and the rule for WAN fail over.

WAN FailOver :	○ Enable ⦿ Disable	1
WAN Priority :	3G/3.5G ▾	2
Idle Timeout Detect :	0 sec.	3
Ping Target IP :	0.0.0.0	4
E-Mail Notification :	○ Enable ⦿ Disable	5
SMTP Server :		6
Mail Address From :		7
Mail Address To :		8

APPLY 9

Below are descriptions of the options:

WAN FailOver (1): Check this box to enable the function.

WAN Priority (2):   *Select the WAN connection priority from the drop-down menu.*

Idle Timeout   *Input the idle time for detecting the Internet*
Detect (3):   *connection. If the major Internet connection is idle for this amount of time, then the router will send a ping to the target IP address you have assigned. If the ping gets a reply, the router will restart the idle timer; otherwise, it will fail over to the second-priority WAN connection.*

Note: The router will not connect back to the first-priority Internet connection once it has already failed over to another one.

Ping Target IP (4): Input the target IP address you want to ping out. If the major Internet connection is idle for too long, the router will attempt to ping the target IP address.

E-Mail Notification (5): If you enable the E-Mail Notification function, when the WAN connection fails the router will automatically attempt to connect to the second-priority WAN connection and mail a notification to you.

SMTP Server (6): Input the SMTP server you want to use.

Mail Address From (7): Input the mail address you would like to use as an alarm.

Mail Address To (8): Input the mail address you would like to notify.

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

Save setting successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system for changes to take effect
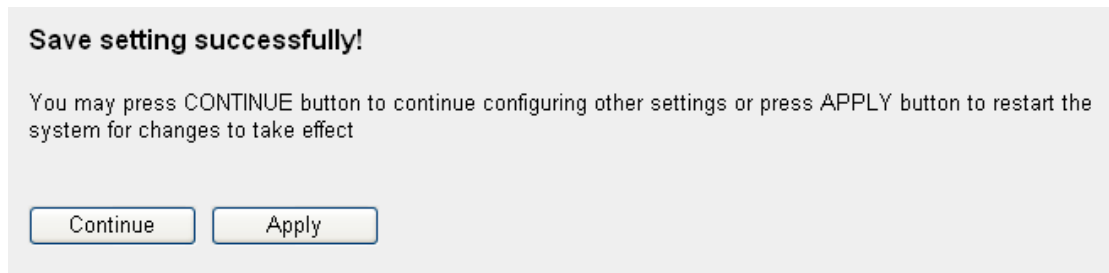
[Continue] [Apply]

Click "Continue" to go back and continue with the router setup procedure, or click "Apply" to reboot the router so the settings will take effect. (Wait for about 30 seconds while the router reboots.)

3-5 System Status

The functions described here will provide you with system-related information. To enter the System Status menu, either click the "Status" link in the upper-right corner of the Web management interface or click "Status" in the main menu.

3-5-1 System Information and Firmware Version

Click "Status," and the following message will be displayed on your Web browser.

System	
Model :	Wireless 3G Router
Up Time :	0day:6h:14m:2s
Hardware Version :	Rev. A
Boot Code Version :	1.0
Runtime Code Version :	2.06

NOTE: Information displayed here may vary.

3-5-2 Internet Connection Status

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.

3-5-3 Device Status

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

116

This information will vary depending on the device status.

3-5-4 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 side of the Web management interface, and the following message will be displayed on your Web browser:


```
Jan  3 08:24:41 (none) syslog.info syslogd started: BusyBox v1.00-pre2 (200
```

Save	Clear	Refresh
1	2	3

Below are descriptions of the options:

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

3-5-5 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, and the following message will be displayed on your Web
browser:


```
[2000-01-01 00:00:08]: start Static IP
[2000-01-01 00:00:09]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2000-01-01 00:00:09]: [FIREWALL]: WAN IP is 192.168.1.10 setting firewall.
[2000-01-01 00:00:19]: [SNTP]: connect fail!!
[2000-01-01 00:22:43]: [DNS]: dns restart ...
[2000-01-01 00:22:48]: start Static IP
[2000-01-01 00:22:49]: [SNTP]: connect to TimeServer 192.43.244.18 ...
[2000-01-01 00:22:49]: [FIREWALL]: WAN IP is 192.168.1.10 setting firewall.
[2000-01-01 00:22:59]: [SNTP]: connect fail!!
```

| Save | Clear | Refresh |
| 1 | 2 | 3 |
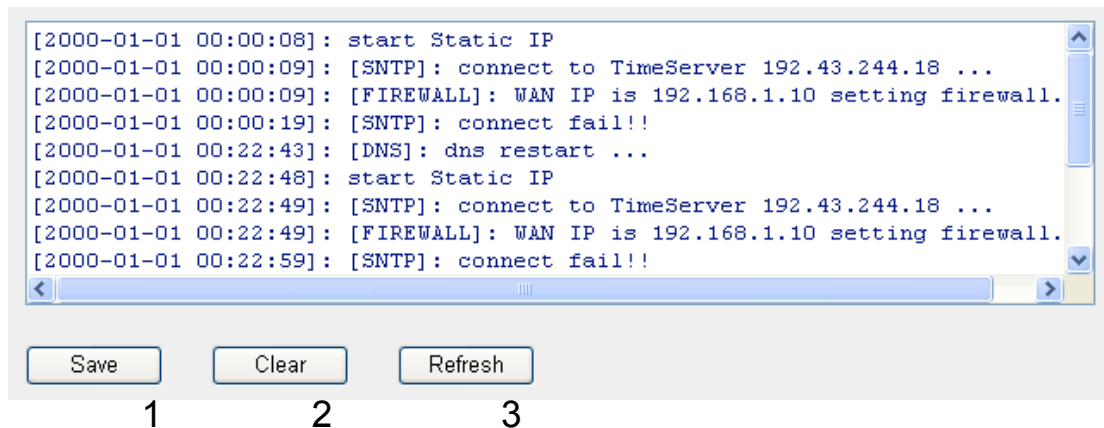
Below are descriptions of the options:

Save (1):   *Save the current event log to a text file.*

Clear (2):   *Delete all event logs displayed here.*

Refresh (3):   *Refresh the event log display.*

3-5-6 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, and the following message will be displayed on your Web
browser:

IP Address	MAC Address	Time Expired(s)
192.168.2.240	00:10:60:db:52:9d	58

| Refresh |

All information about active DHCP leases issued by this router will be displayed here. Click "Refresh' to display the latest information.

3-5-7 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, and the following message will be displayed on your Web browser:

Wireless LAN	Packets Sent	11281
	Packets Received	650086
Ethernet LAN	Packets Sent	15042
	Packets Received	4409
Ethernet WAN	Packets Sent	2337
	Packets Received	0

Refresh

Click "Refresh" to display the latest information.

3-5-8 Modem Info

You can use this function to check the information of the 3G modem card.

Click "Modem" Info on the left side of the Web management interface, and the following message will be displayed on your Web browser:
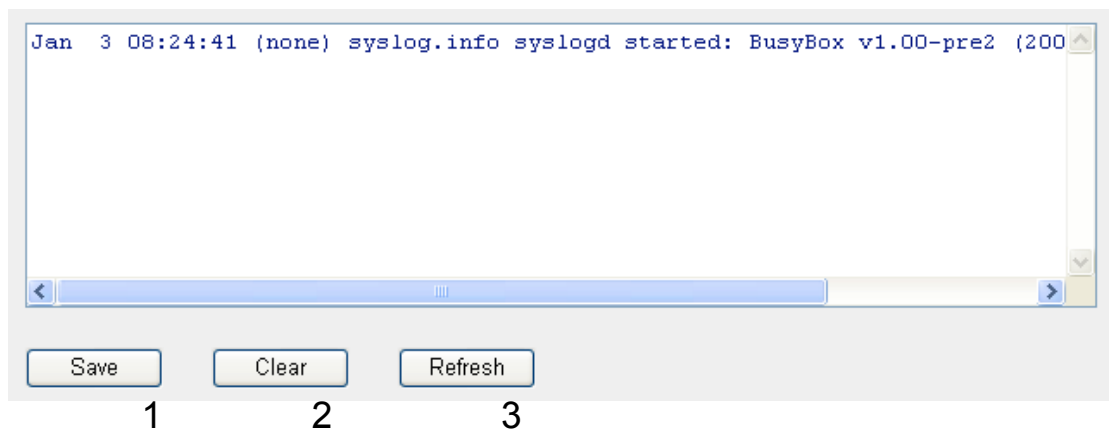
Diagnostic 3G/3.5G modem information.

Manufacturer:	N/A
Product:	N/A
IMEI:	N/A
Signal:	N/A

3-6 Configuration Backup and Restore

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

Click "Tools" 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:

Backup Settings : [Save...] 1

Restore Settings : [_____] [Browse...] 2
[Upload]

Restore to Factory Default : [Reset] 3

Below are descriptions of the options:

Backup Settings (1):	Click "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):	Click "Browse…" to pick a previously saved configuration file from your computer, then click "Upload" to transfer the file to the router. After the configuration is uploaded, the router's

120

Restore to Factory Default (3):	*Click to remove all settings you made and restore the configuration of this router back to factory default settings.*

3-7 Firmware Upgrade

The system software used by the router is referred to as "firmware," just like applications on your computer. When you replace an older 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 (even fix bugs).

Click "Tools" lat the upper-right corner of the Web management interface, then click Firmware Upgrade on the left side. The following message will be displayed on your Web browser:

This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.

Next

Click "Next" and the following message will be displayed:

Firmware Upgrade

This tool allows you to upgrade the Broadband router's system firmware.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

[Browse...]

[Apply]   [Cancel]

Click "Browse" first and you'll be prompted to provide the filename of the firmware upgrade file. Download the latest firmware file from www.intellinet-network.com and use it to upgrade your router. After a firmware upgrade file is selected, click "Apply" and 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 uploaded is corrupt, the firmware upgrade will fail, and you may have to return this router to the dealer of purchase to ask for help.**

3-8 System Reset

If you feel that the network performance is poor, or if you find the behavior of the router to be abnormal, you can perform a router reset as a possible solution to the problem.

Click "Tools" located at the upper-right corner of the Web management interface, then click Reset on the left side. The following message will be displayed on your Web browser:

Reset

In the event that the system stops responding correctly or stops functioning, you can perform a Reboot. Your settings will not be changed. To perform the reboot,click on the APPLY button below. You will be asked to confirm your decision.The Reboot will be complete when the LED Power light stops blinking.

[APPLY]

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

Chapter IV: Appendix

4-1 Specifications

Standards
- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.11b (11 Mbps Wireless LAN)
- IEEE 802.11g (54 Mbps Wireless LAN)
- IEEE 802.11n Draft 2.0 (300 Mbps Wireless LAN)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)

General
- LAN ports: 4 RJ45 10/100 Mbps data ports
- LAN ports with Auto MDI/MDI-X
- WAN port: 10/100 Mbps RJ45 connector
- USB 2.0 port: 3G/3.5G USB modem
- Flash: 4 MB
- Memory: 16 MB SDRAM
- Certifications: FCC Class B, CE
- For a complete list of compatible 3G USB modems, visit
  www.intellinet-network.com

Router
- Supported WAN connection types:
    - 3G / 3.5G
    - Dynamic IP
    - Static IP
    - PPPoE
    - PPTP
    - L2TP
    - Telstra BigPond
- Protocols:
    - CSMA/CA
    - CSMA/CD
    - TCP/IP
    - UDP

- ICMP

- PPPoE

- NTP

- NAT

- DHCP

- DNS

• NAT:

- Virtual server

- Port forwarding

- Special applications (port trigger)

• Firewall:

- Access control based on MAC address

- URL filter

- DMZ (demilitarized zone)

• Supports UPnP (Universal Plug and Play)

• Supports DHCP (client/server)

• Supports WPS (WiFi Protected Setup)

• VPN passthrough: PPTP, IPSec protocol

Wireless

• Chipset: Ralink RT3052 (Model 524681); Ralink RT 3050 (Model 524940)

• Wireless frequency range: 2.400 – 2.483 GHz

• Modulation technologies:

- 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK

- 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM

- 802.11n: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM

• Channels:

- USA & Canada: 11 channels

- Europe: 13 channels

- Japan: 14 channels

• Data rates:

- IEEE 802.11b (11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps)

- IEEE 802.11g (54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, 6 Mbps)

- IEEE 802.11n (MCS0-07: up to 150 Mbps)

- IEEE 802.11n (MCS0-15: up to 300 Mbps)
• Output power:
   - OFDM: 15 dBm +/- 1 dBm (300 Mbps, 40 mW max.)
   - OFDM: 15 dBm +/- 1 dBm (54 Mbps, 40 mW max.)
   - CCK: 17 dBm +/- 1 dBm (11 Mbps, 63 mW max.)
• Receiver sensitivity:
   - 11n (150 Mbps) MCS0-07: 20 MHz: -73 dBm; 40 MHz: -68 dBm
   - 11n (300 Mbps) MCS0-15: 20 MHz: -73 dBm; 40 MHz: -68 dBm
   - 11g (54 Mbps) OFDM: -78 dBm
   - 11b (11 Mbps) CCK: -91 dBm
• Maximum coverage distance: 100 m / 328 ft. (indoors); 300 m / 980 ft.
 (outdoors)
• Wireless security:
   - WEP encryption (64/128 bit)
   - WPA TKIP
   - WPA2 AES
   - WPA2 mixed
   - WPA RADIUS
   - Client access control through media access control (MAC) filter
• Antennas, Model 524681:
   - 2 fixed dipole antennas with 3 dBi gain each
   - 2T2R MIMO mode (2 transmitters, 2 receivers)
• Antenna, Model 524940:
   - 1 fixed dipole antenna with 3 dBi gain

LEDs
• Power
• WLAN Link/Act
• LAN 1-4 Link/Act
• USB

Environmental
• Dimensions: 157 (W) x 127 (L) x 30 (H) mm (6.2 x 5.0 x 1.2 in.)
• Weight: 0.215 kg (7.58 oz.)
• Operating temperature: 10 – 40°C (50 – 104°F)
• Operating humidity: 10 – 90% RH, non-condensing
• Storage temperature: -20 – 60°C (4 – 149°F)

Power

• External power adapter: 12 V DC, 1.0 A

• Power consumption: 5 W max., Model 524681; 3.5 W max., Model 524940

Package Contents

• Wireless 3G Router (150N or 300N)

• User manual on CD, plus quick install guide

• Power adapter

• Ethernet Cat5 RJ45 cable: 1.0 m (3 ft.)

• USB extension cable: 1.0 m (3 ft.)

4-2 Troubleshooting

If you find the router is working improperly or has stopped responding, see if a possible solution appears in this section before you contact your dealer of purchase for help.

Scenario	Solution
Router is not responding when I try to access it by Web browser.	a. Check the router's power cord and network cable connections. All cords and cables should be correctly and firmly inserted into the router. b. If all LEDs on the router are off, check the AC power adapter to make sure the router is correctly powered. c. You must use the same IP address the 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, restore your router to factory default settings (pressing the Reset button for more than 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 the above solutions don't work, contact your dealer of purchase for help.
Can't get connected to the Internet.	a. Go to Status then Internet Connection and check the Internet connection status. b. Wait long enough to be sure it's not just that the Internet is slow. c. If you connected a computer to the Internet directly before, try to do that again, and check if you can get

	connected to the Internet with your computer directly attached to the device provided by your Internet service provider. d. Check the PPPoE / L2TP / PPTP user ID and password again. e. Call your Internet service provider and check if there's something wrong with their service. f. If you just can't connect to one or more Web sites but you can still use other Internet services, check the URL/ Keyword filter. g. Try to reset the router and try again later. h. Reset the device provided by your Internet service provider. 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, check the DNS setting.
I can't locate my router by my wireless client.	a. Check if Broadcast ESSID is set to off? b. Confirm that the antennas are secured. c. Try operating closer to the router. d. Make sure you've input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File download is very slow or breaks frequently.	a. Are you using the QoS function? Try to disable it and try again. j. Wait long enough to be sure it's not just that the Internet is slow. b. Try to reset the router and see if it's better after that. c. See what the computers on your LAN are doing. If someone's transferring big files, others will think the Internet is really slow.

	d. If this never happened before, call your Internet service provider to see if there is something wrong with their network.
I can't log on to the Web management interface; the password is wrong.	a. Make sure you're connecting to the correct IP address of the router. b. The password is case-sensitive. Make sure the Caps Lock light isn't illuminated. c. If you forget the password, do a hard reset.
Router becomes hot.	a. This is not a malfunction if you can keep your hand on the router's case. b. If you smell something odd or see smoke coming from the router or AC power adapter, disconnect the router and AC power adapter from utility power (make sure it's safe before doing this!), and call your dealer of purchase for help.
The date and time of all event logs are wrong.	a. Adjust the internal clock of the router.

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 toward 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.