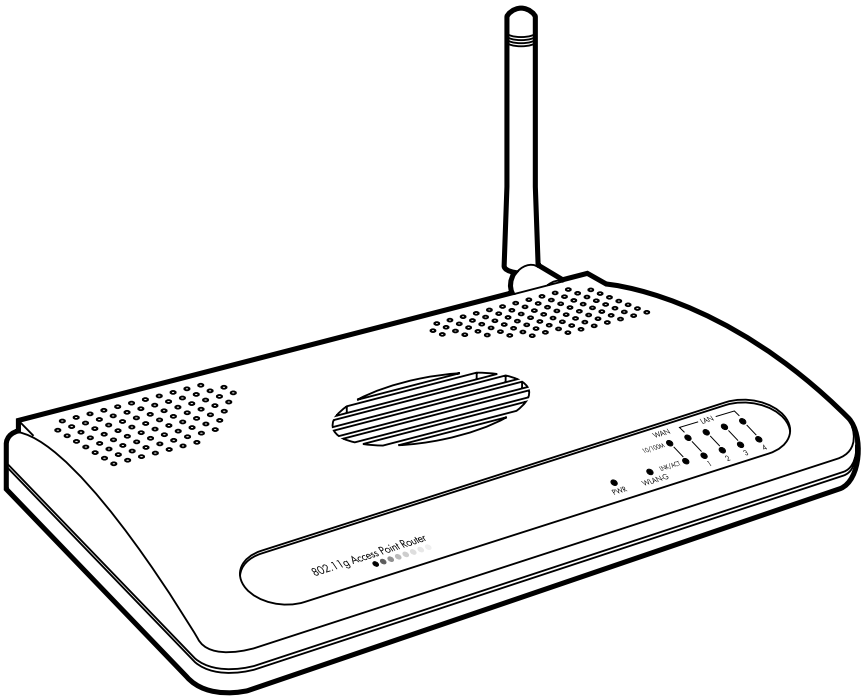
1000 Park Drive • Lawrence, PA 15055-1018 • 724-746-5500 • Fax 724-746-0746

BLACK BOX®
NETWORK SERVICES

AUGUST 2004
LW6005A
LW6005A-EU
LW6005A-UK

Pure Networking 802.11g Wireless Router Users' Guide



CUSTOMER SUPPORT INFORMATION

Order **toll-free** in the U.S.: Call **877-877-BBOX** (outside U.S. call **724-746-5500**)
FREE technical support 24 hours a day, 7 days a week: Call **724-746-5500** or fax **724-746-0746**
Mailing address: **Black Box Corporation**, 1000 Park Drive, Lawrence, PA 15055-1018
Web site: **www.blackbox.com** • E-mail: **info@blackbox.com**

FEDERAL COMMUNICATIONS COMMISSION and INDUSTRY CANADA RADIO FREQUENCY INTERFERENCE STATEMENTS

Class B Digital Device. This equipment has been tested and found to comply with the limits for a Class B computing device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular 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. If this equipment does cause harmful interference to radio or telephone reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To meet FCC requirements, shielded cables and power cords are required to connect this device to a personal computer or other Class B certified device.

This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of Industry Canada.

NORMAS OFICIALES MEXICANAS (NOM)
ELECTRICAL SAFETY STATEMENT

INSTRUCCIONES DE SEGURIDAD

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc..
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.

12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.

13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.

14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.

15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.

16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.

17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.

18. Servicio por personal calificado deberá ser provisto cuando:

    A: El cable de poder o el contacto ha sido dañado; u

    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o

    C: El aparato ha sido expuesto a la lluvia; o

    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o

    E: El aparato ha sido tirado o su cubierta ha sido dañada.

TRADEMARKS USED IN THIS MANUAL

Macintosh is a registered trademark of Apple Computer, Inc.

pcANYWHERE is a registered trademark of Dynamic Microprocessor Associates, Inc.

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

Sun is a registered trademark of Sun Microsystems, Inc.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Contents

Chapter **Page**

Contents (continued)

Chapter **Page**

1. Specifications

Standards: 802.11g, PPPoE, PPTP, L2TP, IEEE 802.3 (10 Mbps), IEEE 802.3u (100 Mbps), WEP, WPA, WES

CPU: ADMtek 6120 (175-MHz MIPS R4000)

Memory: Flash: 2 MB NOR; RAM: 16 MB DRAM

Speed: (1) WAN and (4) LAN ports: 10 or 100 Mbps, autosensing

Internet Access Throughput: Up to 50 Mbps

Users Supported: Up to 253

Connectors: (5) RJ-45: (4) LAN, (1) WAN

Indicators: (12) LEDs: (1) PWR, (1) WAN 10/100 M, (1) WAN LNK/ACT, (4) LAN 10/100 M, (4) LAN LNK/ACT, (1) WLAN-G

Temperature Tolerance: 50 to 113°F (10 to 45°C)

Humidity: Up to 90%, noncondensing

Size: 1.2"H x 7.4"W x 3.9"D (3 x 18.8 x 9.9 cm)

2. Introduction

2.1 Overview

The Pure Networking 802.11g Wireless Router is a cost-effective IP sharing router that enables multiple users to share the Internet through an ADSL or cable modem. Simply configure your router's Internet connection settings, plug your PC into the LAN port, and you're ready to share files and access the Internet. As your network grows, you can connect other hubs or switches to the router's LAN ports, allowing you to easily expand your network.

This router has high Internet access throughput (up to 50 Mbps). It supports up to 253 users. You can also access private LAN servers from the public network. The router includes four 10-/100-Mbps LAN ports and one 10-/100-Mbps WAN port.

The router is embedded with an IEEE 802.11g/b access point that allows you to build up a wireless LAN. It's perfect for the Small and Medium-sized Business (SMB) and the Small Office/Home Office (SOHO) markets, giving you an instant network today, and the flexibility to handle tomorrow's expansion and speed.

For easy setup, the router supports DHCP (Server/Client). It also supports advanced features such as special applications, DMZ, virtual servers, access control, firewall, and bridge mode. Monitor the router's status via DHCP client log, security log, and device/connection status. You can even configure the router remotely via its Web-based Graphical User Interface (GUI).

2.2 Minimum Requirements

- (1) External xDSL (ADSL) or cable modem with an Ethernet port (RJ-45).
- (1) Network interface card (NIC) for each PC.
- PCs with a Web browser (Internet Explorer 4.0 or higher, or Netscape Navigator® 4.7 or higher).

2.3 What's Included

- (1) Pure Networking 802.11g Wireless Router
- (1) Quick Installation Guide
- (1) CD-ROM containing a users' manual in PDF format

- (1) power adapter
- (1) 2.2-dBm dipole antenna

2.4 The Router Illustrated

2.4.1 Back Panel

Figure 2-1 shows the router's back panel. Numbers 1–5 in Figure 2-1 correspond to Numbers 1–5 in the text following Figure 2-1.

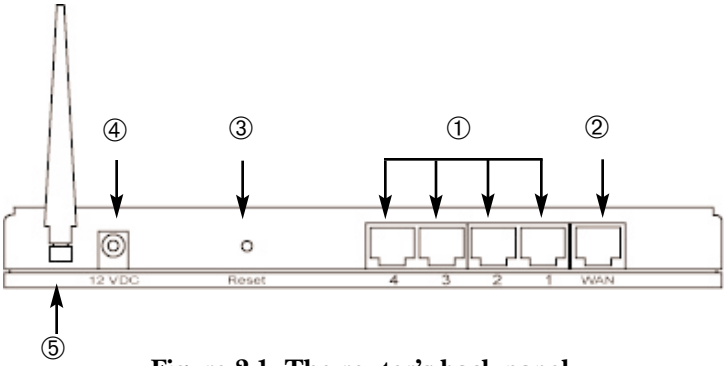


Figure 2-1. The router's back panel.

① Local Area Network (LAN): The router's four LAN ports are where you connect your LAN's PCs, printer servers, hubs, switches, etc.

② Wide Area Network (WAN): The WAN port is the segment connected to your xDSL or cable modem; it's linked to the Internet.

③ Reset: The Reset button allows you to do one of two things.

1. If problems occur with your router, press the Reset button with a pencil tip (for less than 4 seconds). The router will reboot itself, keeping your original configurations.

2. If problems persist, if you experience extreme problems, or if you forgot your password, press the Reset button for more than 4 seconds. The router will reset itself to the factory-default settings.

④ Power connector.

⑤ Antenna connector.

2.4.2 Front Panel

On the router's front panel are LED lights that inform you of the router's current status. Table 2-1 and Figure 2-2 describe these LEDs. Numbers 1–6 in Figure 2-2 correspond to numbers 1–6 in Table 2-1.

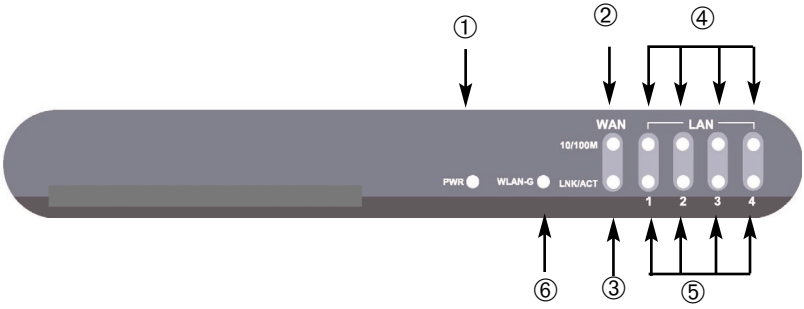


Figure 2-2. The router's front panel.

Table 2-1. Front-panel LEDs and their functions.

LED	Status	Description
① PWR	On	Router's power supply is on.
② WAN 10/100M	On	WAN port 100 Mbps is connected.
	Off	WAN port 10 Mbps is connected.
③ WAN LNK/ACT	On	WAN is connected.
	Off	No WAN connection.
	Flashing	WAN port has activity (ACT), data is being sent.
④ LAN 10/100M (Ports 1–4)	On	LAN port 100 Mbps is connected.
	Off	LAN port 10 Mbps is connected.
⑤ LAN LNK/ACT (Ports 1-4)	On	LAN is connected.
	Off	No LAN connection.
	Flashing	LAN port has activity (ACT), data is being sent.
⑥ WLAN-G	On	Wireless LAN has been activated.
	Off	Wireless LAN is disabled.
	Flashing	Wireless LAN has activity (ACT), data is being sent.

3. Installation

This chapter contains step-by-step instructions for how to set up the router and get connected to the Internet.

1. Set up your network as shown in Figure 3-1.

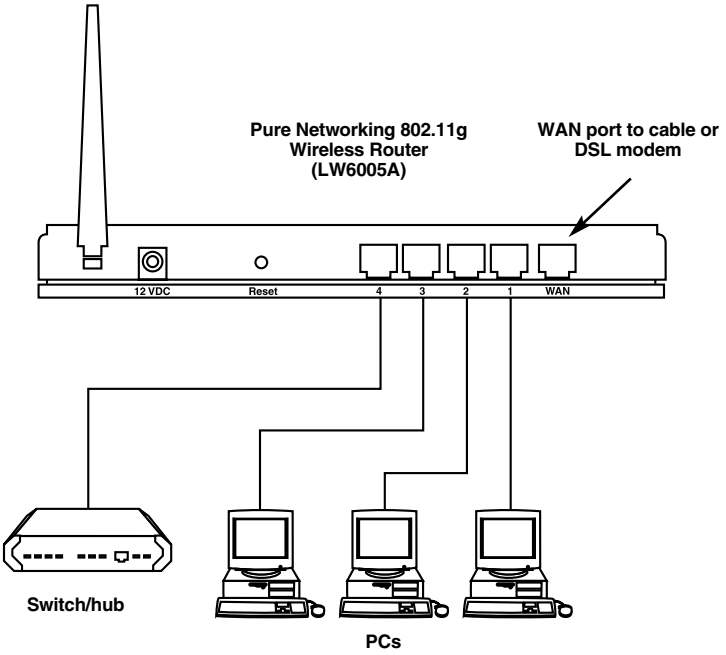


Figure 3-1. Typical application.

2. Set your LAN PC client so that it can obtain an IP address automatically.

   All LAN clients require an IP address. Just like an address, it allows LAN clients to find one another. (If you have already configured your PC to obtain an IP address automatically, proceed to step 3 on page 20.)

Configure your PC to obtain an IP address automatically

Because the router's DHCP is on, you only have to configure your PC to obtain an IP address automatically. Once you've configured your PC to obtain an IP address automatically, the router obtains its IP address automatically. Step 2 will show you how to configure your PC so that it can obtain an IP address automatically for either Windows® 95/98/Me (step 2a), Windows XP (step 2b), Windows 2000 (step 2c), or Windows NT® (step 2d) operating systems. For other operating systems (Macintosh®, Sun®, etc.), follow the manufacturer's instructions.

2a) Windows 95/98/Me

1. Click on the **Start** button and select **Settings**, then click on **Control Panel**. The Control Panel window will appear.

2. Double-click on the **Network** icon. The Network window will appear.

3. Check your list of network components. If TCP/IP is not installed, click on the **Add** button to install it now. If TCP/IP is installed, go to step 6 below.

4. In the Network Component Type dialog box, select **Protocol** and click on the **Add** button.

5. In the Select Network Protocol dialog box, select **Microsoft and TCP/IP**, then click on the **OK** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

6. After installing TCP/IP, go back to the Network dialog box. Select **TCP/IP** from the list of network components, then click on the **Properties** button. Figure 3-2 appears.

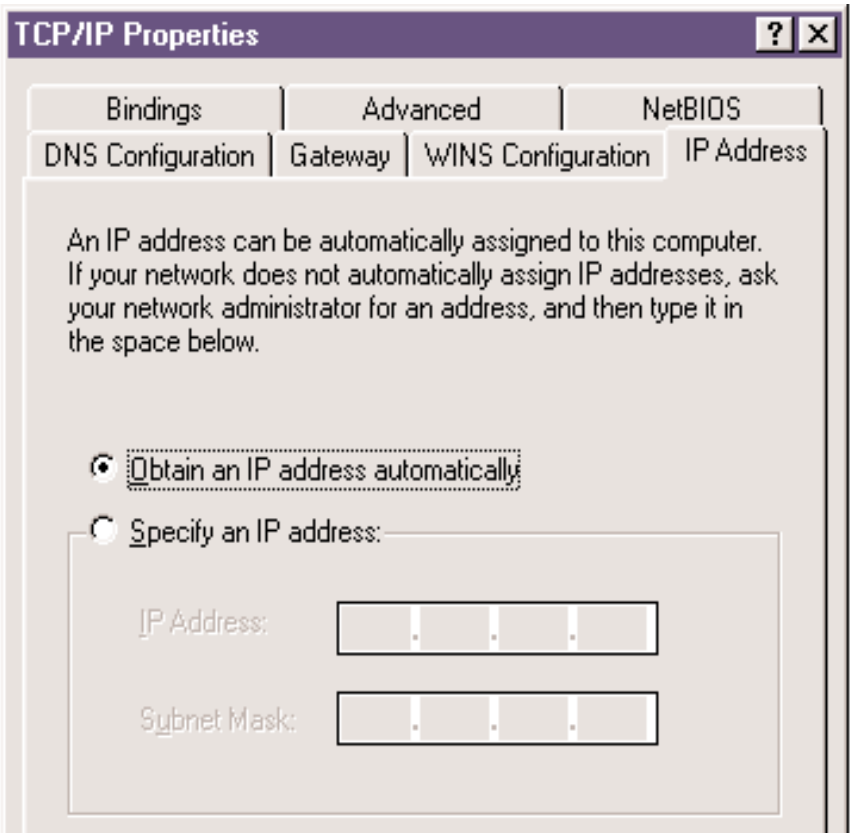


Figure 3-2. TCP/IP Properties screen, IP Address tab.

7. Check each of the tabs and verify the following settings:

   - Bindings: Check **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks**.
   - Advanced: Select the router's configuration.
   - NetBIOS: Select this tab.
   - DNS Configuration: Select **Disable DNS**.
   - Gateway: All fields are blank.
   - WINS Configuration: Select **Disable WINS Resolution**.

- IP Address: Select **Obtain IP address automatically**.

8. Reboot the PC. Your PC will now obtain an IP address automatically from your router's DHCP server.

NOTE

Please make sure that the router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, proceed to step 3 on page 20.

2b) Windows XP

1. Click on the **Start** button and select **Settings**, then click on **Network Connections**. The Network Connections window will appear.

2. Double-click on the **Local Area Connection** icon. The Local Area Connection window will appear.

3. Check your list of Network Components. You should see **Internet Protocol [TCP/IP]** on your list. Select it, and click on the **Properties** button. Figure 3-3 appears.

4. In the Internet Protocol (TCP/IP) Properties window, select **Obtain an IP address automatically** and **Obtain DNS server address automatically** as shown in Figure 3-3.

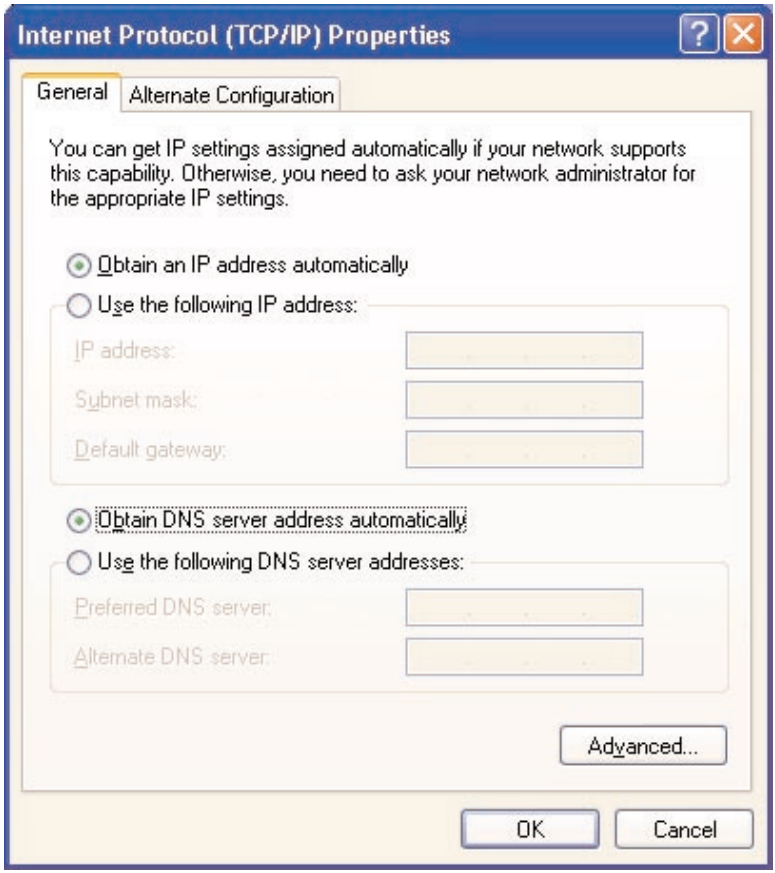


Figure 3-3. Internet Protocol (TCP/IP) Properties screen, General tab.

5. Click on the **OK** button to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

NOTE

Make sure that the router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, proceed to step 3 on page 20.

2c) Windows 2000

1. Click on the **Start** button and select **Settings**, then click on **Control Panel**. The Control Panel window will appear.

2. Double-click on the **Network and Dial-up Connections** icon. In the Network and Dial-up Connection window, double-click on the **Local Area Connection** icon. The Local Area Connection window will appear.

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

4. Check your list of Network Components (this screen is not shown here). You should see **Internet Protocol [TCP/IP]** on your list. Select it, and click on the **Properties** button.

5. In the Internet Protocol (TCP/IP) Properties window, select **Obtain an IP address automatically** and **Obtain DNS server address automatically** as shown in Figure 3-4.

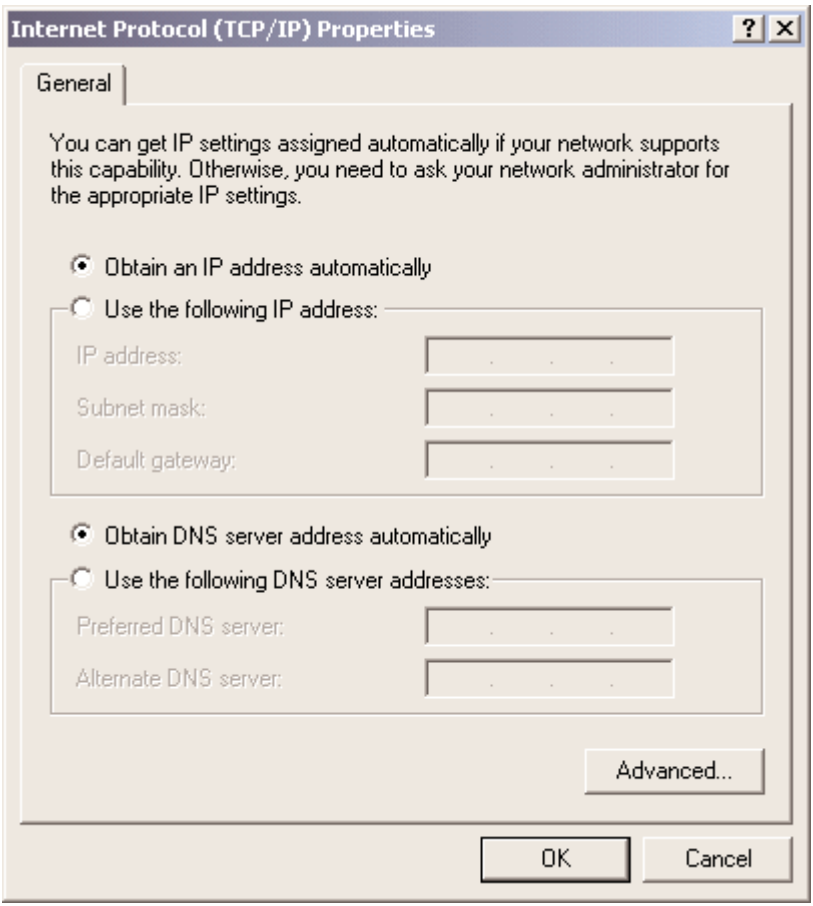


Figure 3-4. Internet Protocol (TCP/IP) Properties screen, General tab.

6. Click on the **OK** button to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

NOTE

Make sure that the router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, proceed to step 3 on page 20.

2d) Windows NT

1. Click on the **Start** button and select **Settings**, then click on **Control Panel**. The Control Panel window will appear.

2. Double-click on the **Network** icon. The Network window will appear. Select the **Protocol** tab from the Network window.

3. Check to see if the **TCP/IP Protocol** is on your list of Network Protocols. If TCP/IP is not installed, click on the **Add** button to install it now. If TCP/IP is installed, go to step 5 below.

4. In the Select Network Protocol window, select the **TCP/IP Protocol** and click on the **OK** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

5. After you install TCP/IP, go back to the Network window. Select **TCP/IP** from the list of Network Protocols, then click on the **Properties** button. Figure 3-5 appears.

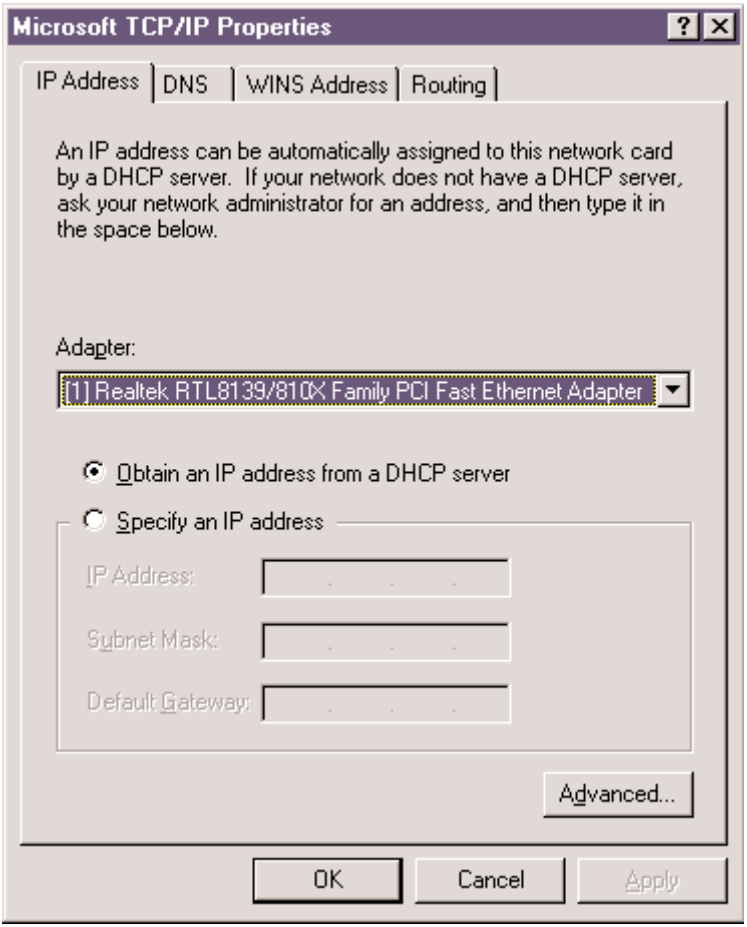


Figure 3-5. Microsoft TCP/IP Properties screen, IP Address tab.

6. Check each of the tabs and verify the following settings:

   - IP Address: Select **Obtain an IP address from a DHCP server**.
   - DNS: Leave all fields blank.
   - WINS Address: Leave all fields blank.
   - Routing: Leave all fields blank.

7. Click on the **OK** button to confirm the setting. Your PC will now obtain an IP address automatically from your router's DHCP server.

NOTE

Make sure that the router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, proceed to step 3 (below).

3. Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give your LAN clients an IP address. By default, the router's DHCP server is enabled so that you can obtain an IP address automatically. To see if you have obtained an IP address, refer to the **Appendix**.

NOTE

Make sure that the router's DHCP server is the only DHCP server available on your LAN. If there is another DHCP server on your network, then you'll need to switch one of the DHCP servers off. (To disable the router's DHCP server, see the previous page.)

4. Once your PC has obtained an IP address from your router, enter the default IP address `192.168.2.1` (router's IP address) into your PC's Web browser and press **Enter**. See Figure 3-6.

Figure 3-6. Enter the default IP address.

5. The login screen shown in Figure 3-7 will appear. Enter the user name and password; then click on **OK** to log in.

NOTE

By default, the user name is admin and the password is 1234. For security reasons, we recommend that you change the password as soon as possible (in General setup/system/password; see Section 5.1.2 for details).

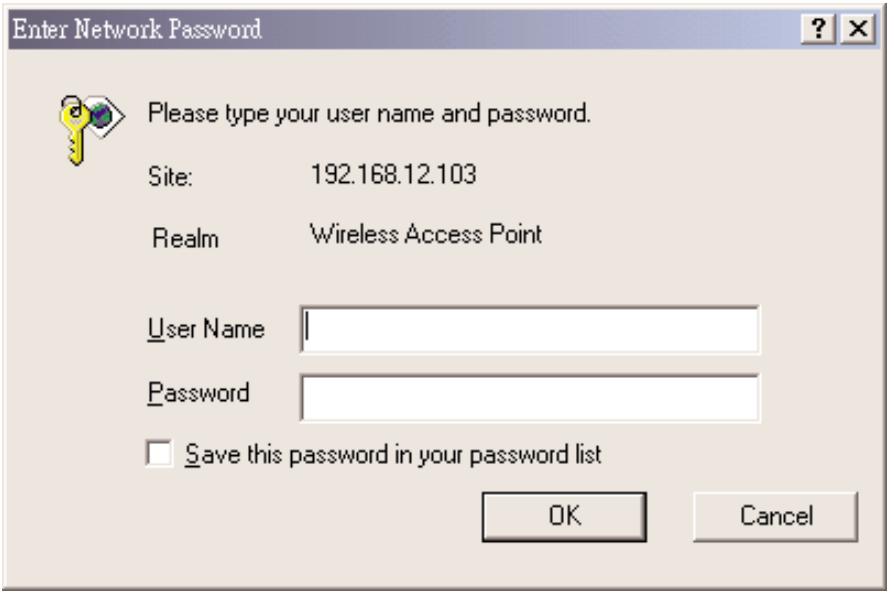


Figure 3-7. Enter the password and user name.

6. The Home screen (shown in Figure 3-8) will appear. The Home screen is divided into four sections: Quick Setup Wizard, General Setup, Status Information, and Tools. Table 3-1 also describes these sections.

   - Quick Setup Wizard: If you want to start using the router as an Internet access device only, then you need to configure the screens in the Quick Setup Wizard section only.

   - General Setup: If you want to use the router's more advanced features, you'll need to configure the Quick Setup Wizard *and* the General Setup section. Or, you can just configure the General Setup section since the General Setup and the Quick Setup Wizard contain the same configurations.

   - Status Information: The Status Information section allows you only to monitor the router's current status information.

   - Tools: If you want to reset the router (because of problems), save your configurations, or upgrade the firmware, the Tools section is the place to do this.

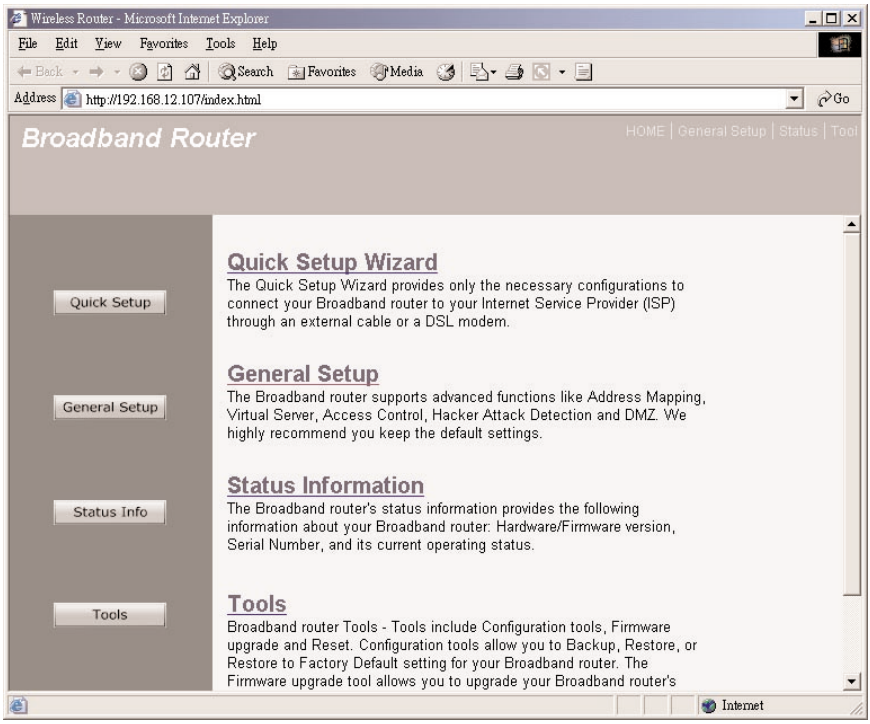


Figure 3-8. Home screen.

Table 3-1. Home screen options.

Menu	Description
Quick Setup Wizard	Select your Internet connection type, then type in the configurations needed to connect to your Internet Service Provider (ISP). See **Chapter 4**.

Table 3-1 (continued). Home screen options.

Menu	Description
General Setup	This section contains configurations for the router's advanced functions such as bridge, address mapping, virtual server, access control, hacker attack prevention, DMZ, special applications, and other functions to meet your LAN requirements. See **Chapter 5**.
Status Information	In this section you can see the router's system information, Internet connection, device status, security log, and DHCP client log information. See **Chapter 6**.
Tools	This section contains the router's tools. These include configuration tools, firmware upgrade, and reset. Configuration tools allow you to backup (save), restore, or restore to the factory-default configuration. The firmware upgrade tool allows you to upgrade your router's firmware. The reset tool allows you to reset your router. See **Chapter 7**.
Logout	Selecting Logout (scroll down to see this option) will return you to the Enter Network Password page (see Figure 3-7).

7. Click on Quick Setup Wizard to start configuring settings required by your ISP so that you can access the Internet. The other sections (General Setup, Status Information, and Tools) do not need to be configured unless you wish to implement or monitor more advanced features or information.

Select the section (Quick Setup Wizard, General Setup, Status Information, or Tools) you wish to configure and proceed to the corresponding chapter (listed in Table 3-1). Use the selections on the Home screen's top right-hand page (see Figure 3-9) to navigate around the Web-based management user interface.

Figure 3-9. Select the Home screen options.

4. Quick Setup Wizard

The Quick Setup Wizard is designed to get you using the router as quickly as possible. You're required to fill in only the information necessary to access the Internet. Once you click on the Quick Setup Wizard in the Home screen (see Figure 3-8), Figure 4-1 should appear.

4.1 Time Zone

The Time Zone allows your router to base its time on the settings configured here; this will affect functions such as log entries and firewall settings. Figure 4-1 shows the Time Zone screen.

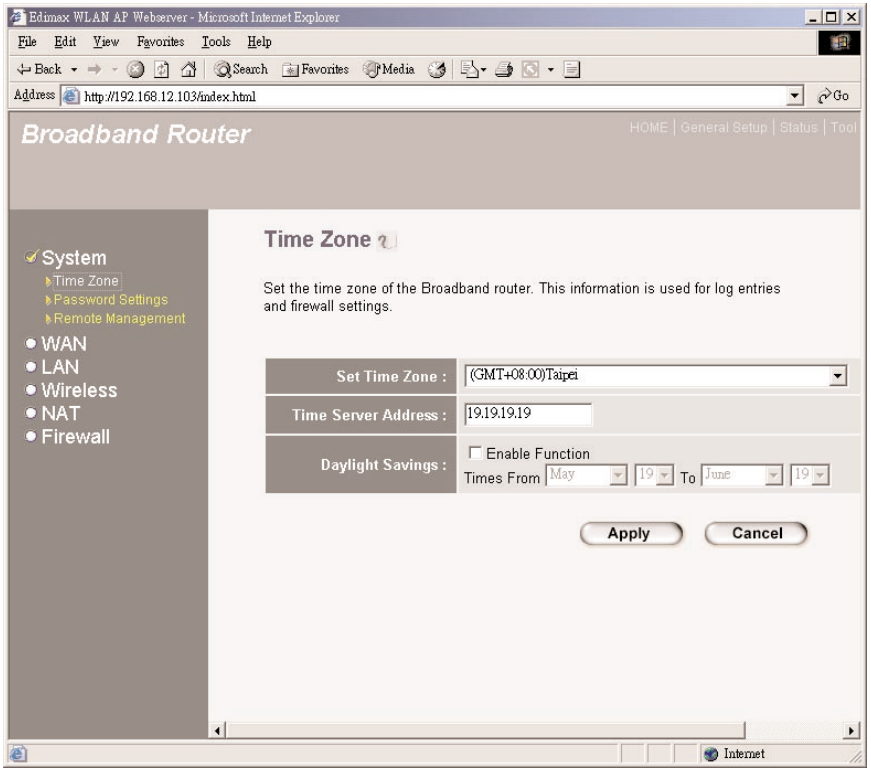


Figure 4-1. Setting the time zone.

Table 4-1 lists the router's time zone options that you can select in Figure 4-1.

Table 4-1. Time zone parameters.

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	You can manually assign the time server's address if the default time server does not work.
Daylight Savings Enable Function	The router can also take Daylight Savings into account. If you wish to use this function, you must check the Enable Function box to enable the Daylight Savings configuration (below).
Start Daylight Savings Time	Select the day you want to start Daylight Savings Time.
End Daylight Savings Time	Select the day you want to end Daylight Savings Time.
Apply	Click on this button to save your changes.
Cancel	Click on this button to cancel your changes.

Click on **Apply** to proceed to the next screen, Broadband Type.

4.2 Broadband Type

In this screen, you'll select one of four types of connections you'll use to connect your router's WAN port to your ISP (see Figure 4-2).

NOTE

Different Internet Service Providers (ISPs) require different methods of connecting to the Internet. Please check with your ISP for the type of connection it requires.

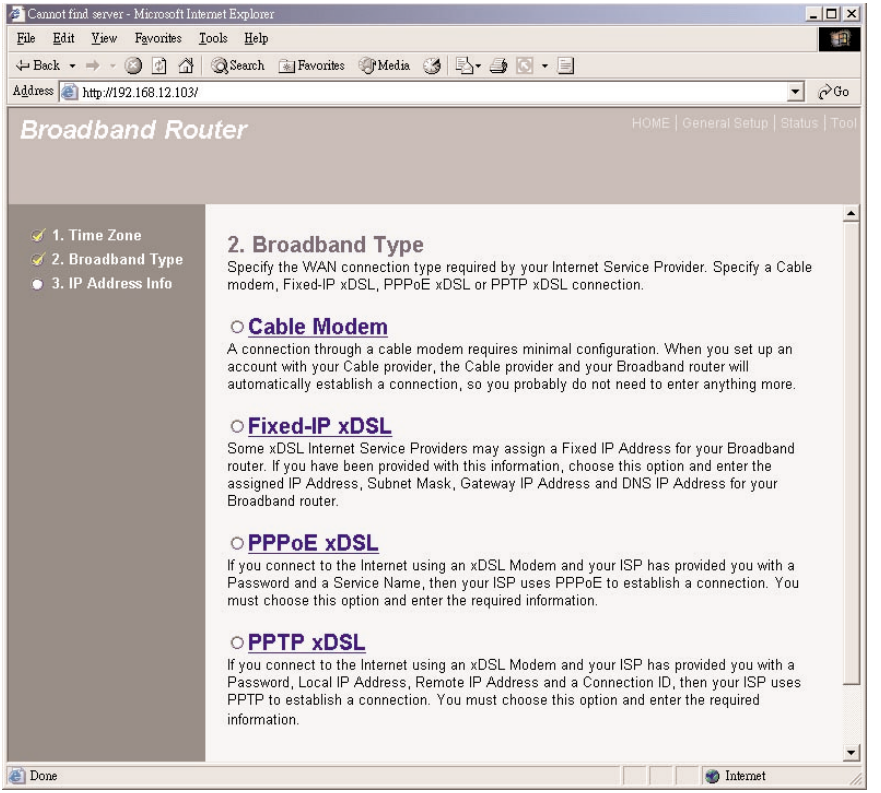


Figure 4-2. Setting the broadband type.

Table 4-2 lists the router's broadband type options, including ISP requirements.

Table 4-2. Broadband type parameters.

Parameter	Description
Cable Modem	Your ISP will automatically give you an IP address.
Fixed-IP xDSL	Your ISP has given you an IP address already.
PPPoE xDSL	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.
PPTP xDSL	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.

Click on one of the broadband types and click on **OK**, then proceed to the manual's relevant sub-section (**4.2.1**, **4.2.2**, **4.2.3**, or **4.2.4**). Click on **Back** (Figure 4-2; scroll down to see this button) to return to the previous screen.

4.2.1 Cable Modem

Choose Cable Modem if your ISP will automatically give you an IP address. Some ISPs may also require that you fill in additional information such as Host Name and MAC address (see Figure 4-3).

NOTE

The Host Name and MAC Address section is optional. You can skip this section if your ISP does not require these settings for you to connect to the Internet.

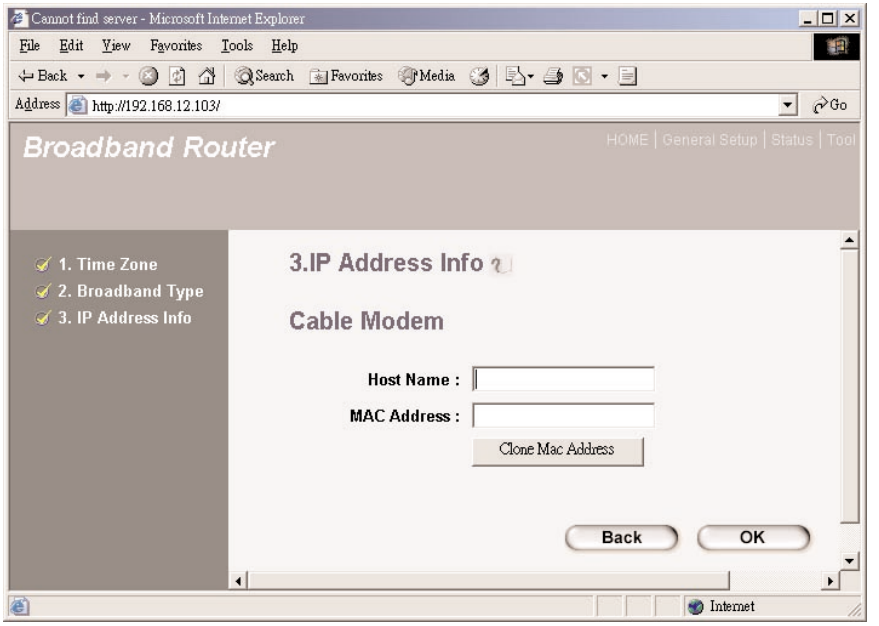


Figure 4-3. Selecting the cable modem.

Table 4-3 lists the router's cable modem's host name and MAC address options.

Table 4-3. Cable modem parameters.

Parameters	Description
Host Name	If your ISP requires a host name, type in the host name provided by your ISP; otherwise, leave it blank if your ISP does not require a host name.
MAC Address	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in the MAC address in this section.
Clone MAC Address button	Or, use the **Clone MAC Address** button to replace the WAN MAC address with the MAC address of the PC you are currently using. To find out what the PC's MAC address is, see the **Appendix**. (See the **Glossary** for an explanation of MAC address.)
Back	Click on this button to go back to the previous screen.
OK	Click on this button to save your changes.

Click on the **OK** button when you have finished the configuration. The configuration for the cable modem connection is now complete. Start using the router now, or, if you wish to use some of the advanced features supported by this router, see **Chapters 5**, **6**, and **7**.

4.2.2 FIXED-IP xDSL

Select Fixed-IP xDSL (see Figure 4-4) if your ISP has given you a specific IP address to use. Your ISP should provide all the information required.

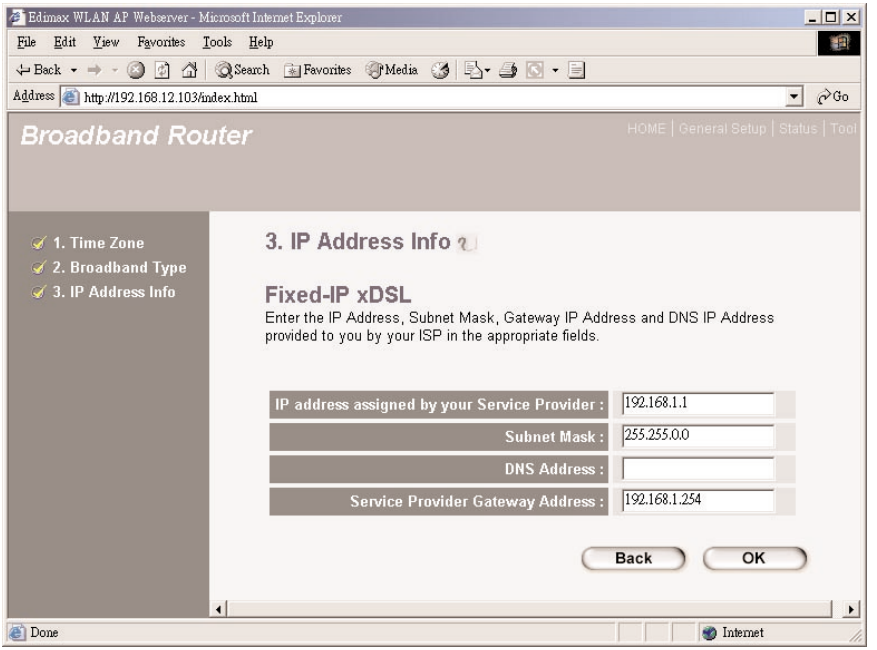


Figure 4-4. Fixed-IP xDSL.

Table 4-4 lists the router's Fixed-IP xDSL options.

Table 4-4. Fixed-IP xDSL parameters.

Parameters	Description
IP address assigned by your Service Provider	This is the IP address that your ISP has given you.
Subnet Mask	Enter the subnet mask provided by your ISP (for example, 255.255.255.0).
DNS Address	This is the ISP's DNS server IP address.
Service Provider Gateway Address	This is the ISP's IP address gateway.

Table 4-4 (continued). Fixed-IP xDSL parameters.

Parameters	Description
Back	Click on this button to return to the previous screen.
OK	Click on this button to save your changes.

Click on the **OK** button. The configuration for the Fixed-IP xDSL connection is complete. Start using the router now, or, if you wish to use some of the advanced features supported by this router, see **Chapters 5**, **6**, and **7**.

4.2.3 PPPoE xDSL

Select PPPoE xDSL if your ISP requires the PPPoE protocol to connect to the Internet. Your ISP should provide all the information required in this section (see Figure 4-5).

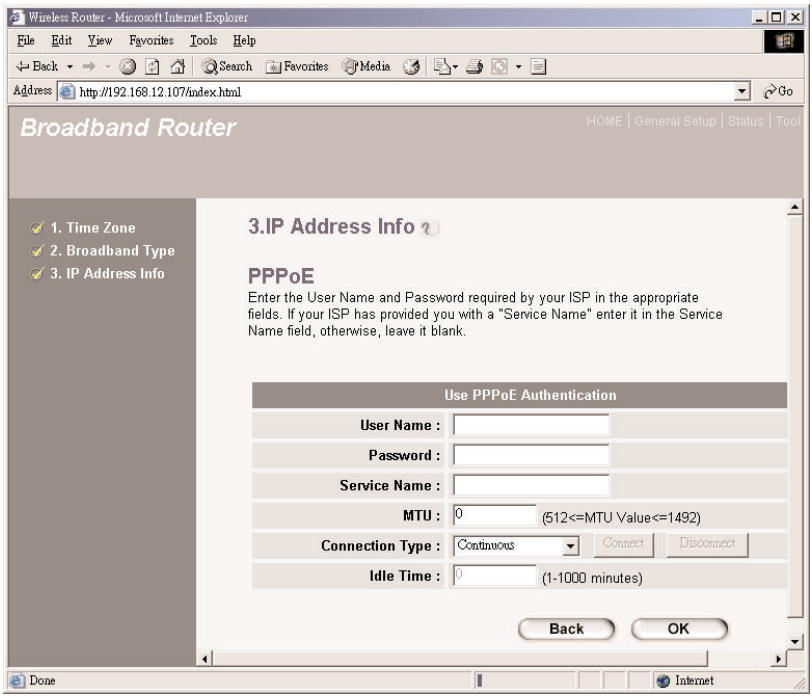


Figure 4-5. PPPoE xDSL.

Table 4-5 lists the router's PPPoE xDSL options.

Table 4-5. PPPoE xDSL parameters.

Parameter	Description
User Name	Enter the user name provided by your ISP for the PPPoE connection.
Password	Enter the password provided by your ISP for the PPPoE connection
Service Name	(This is optional.) Enter the service name if your ISP requires it; otherwise, leave it blank.
MTU	(This is optional.) You can specify the maximum size of your transmission packet to the Internet. Leave it as is if you do not wish to set a maximum packet size.
Connection Type	If you select **Continuous**, the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select **Connect On Demand**, the router will auto-connect to the ISP when someone wants to use the Internet and will stay connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the Idle Time. If you select **Manual**, the router will connect to the ISP only when you click on **Connect** manually from the Web user interface. The WAN connection will not disconnect because of the idle timeout. If the WAN line breaks down and later links again, the router will not auto-connect to the ISP.

Table 4-5 (continued). PPPoE xDSL parameters.

Parameter	Description
Connect button	Click on this button to connect to the Internet via PPPoE.
Disconnect button	Click on this button to disconnect from the Internet via PPoE.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means that if no packets have been sent (no one is using the Internet) during this specified period, the router will automatically disconnect your ISP's connection.
Back button	Click on this button to go back to the previous screen.
OK button	Click on this button to save your changes.

NOTE

This idle timeout function may not work because of some network application software's abnormal activities, computer virus, or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. Turn off your computer when you are not using it. This function also may not work with some ISPs. Make sure this function can work properly when you use it for the first time, especially if your ISP charges you by time used.

Click on the **OK** button when you have finished the configuration above. The configuration for the PPPoE connection is complete. Start using the router now, or, if you want to use some of the advanced features supported by this router see **Chapters 5**, **6**, and **7**.

4.2.4 PPTP xDSL

Select PPTP xDSL if your ISP requires the PPTP protocol for connecting to the Internet. Your ISP should provide all the information required in this section (see Figure 4-6).

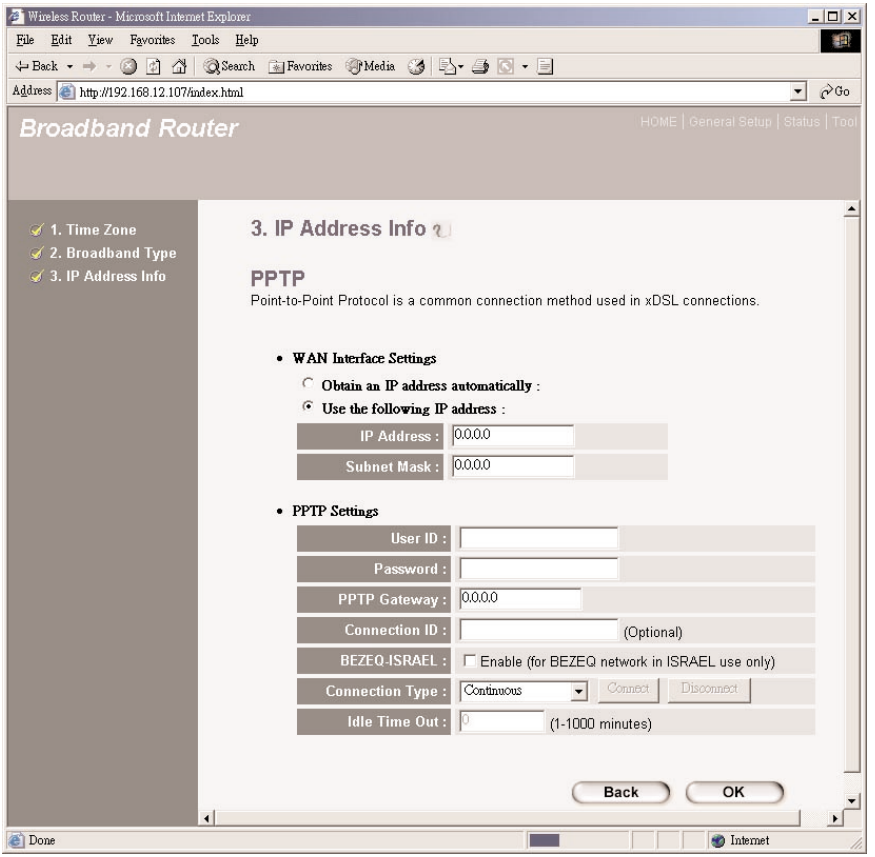


Figure 4-6. PPTP xDSL.

Table 4-6 lists the router's PPTP options shown in Figure 4-6.

Table 4-6. PPTP xDSL parameters.

Parameter	Description
Obtain an IP address automatically	The ISP requires you to obtain an IP address by DHCP automatically before connecting to the PPTP server.
Use the following IP address	The ISP gives you a static IP to be used to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the subnet mask provided by your ISP (for example, 255.255.255.0).
User ID	Enter the user name provided by your ISP for the PPTP connection. This is sometimes called a connection ID.
Password	Enter the password provided by your ISP for the PPTP connection.
PPTP Gateway	If your LAN has a PPTP gateway, enter that PPTP gateway IP address here. If you do not have a PPTP gateway, enter the ISP's gateway IP address above.
Connection ID	(This is optional.) This is the ID given by your ISP.
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.

Table 4-6 (continued). PPTP xDSL parameters.

Parameter	Description
Connection Type	If you select **Continuous** from the drop-down menu, the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP. If you select **Connect On Demand** from the drop-down menu, the router will auto-connect to the ISP when someone wants to use the Internet and will stay connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the idle time. If you select **Manual** from the drop-down menu, the router will connect to the ISP only when you click on **Connect** manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and later links again, the router will not auto-connect to the ISP.
Connect button	Click on this button to connect to the ISP.
Disconnect button	Click on this button to disconnect from the ISP.
Idle Time Out	You can specify an idle time threshold (minutes) for the WAN port. This means that if no packets have been sent (no one is using the Internet) throughout this specified period, then the router will automatically end the connection with your ISP.
Back button	Click on this button to return to the previous screen.
OK button	Click on this button to save your changes.

NOTE

This idle timeout function may not work because of some network application software's abnormal activities, computer virus, or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. Turn off your computer when you are not using it. This function also may not work with some ISPs. Make sure this function can work properly when you use it for the first time, especially if your ISP charges you by time used.

Click on the **OK** button when you have finished the configuration. The configuration for the PPTP connection is complete. Start using the router now, or, if you want to use some of the advanced features supported by this router, see **Chapters 5**, **6**, and **7**.

5. General Setup

Once you click on the General Setup button from the Home screen, the screen in Figure 5-1 appears.

If you have already configured the Quick Setup Wizard (**Chapter 4**), you do *not* need to configure anything in the General Setup screen for you to start using the Internet.

The General Setup option contains advanced features that allow you to configure the router to meet your network's needs, such as wireless, bridge, address mapping, virtual server, access control, hacker attack prevention, special applications, DMZ, and other functions.

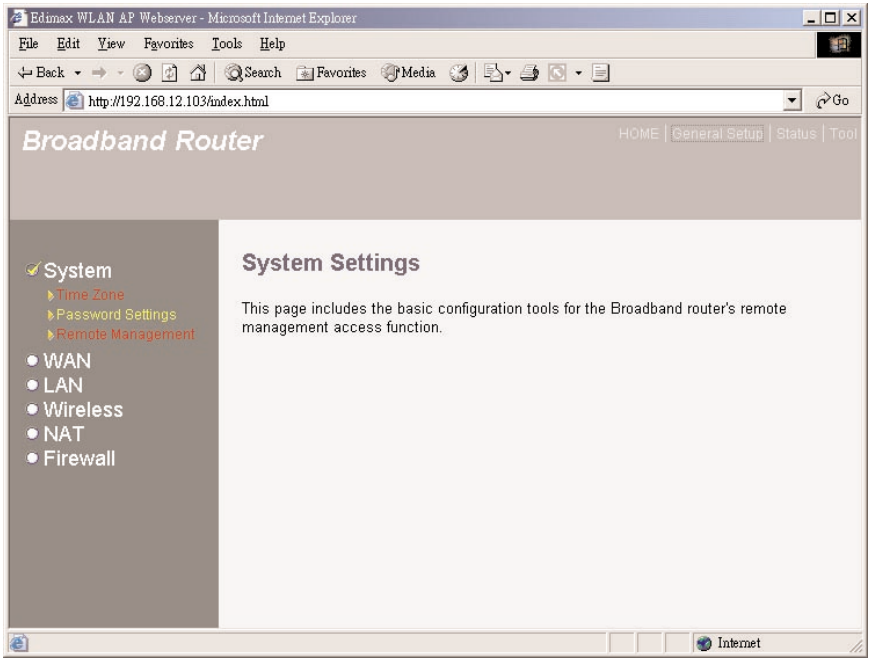


Figure 5-1. General Setup menu (at left of screen).

Table 5-1 provides a general description of what advanced functions are available for this router.

Table 5-1. General Setup options.

Menu	Description
System	This section allows you to set the router's system time zone, password, and remote management administrator.
WAN	This section allows you to select the connection method in order to establish a connection with your ISP (same as the Quick Setup Wizard, **Chapter 4**).
LAN	Specify the LAN segment's IP address, subnet mask, enable/disable DHCP, and select an IP range for your LAN.
Wireless	Set up the wireless LAN's SSID, WEP key, and MAC filtering.
NAT	Configure the address mapping, virtual server, and special applications functions in this section.
Firewall	The firewall section allows you to configure access control, hacker prevention, and DMZ.

Select one of the above six General Setup selections and proceed to the manual's relevant sub-section (**Sections 5.1** through **5.6**).

5.1 System

The system screen (see Figure 5-2) allows you to specify a time zone, to change the system password, and to specify a remote management user for the router.

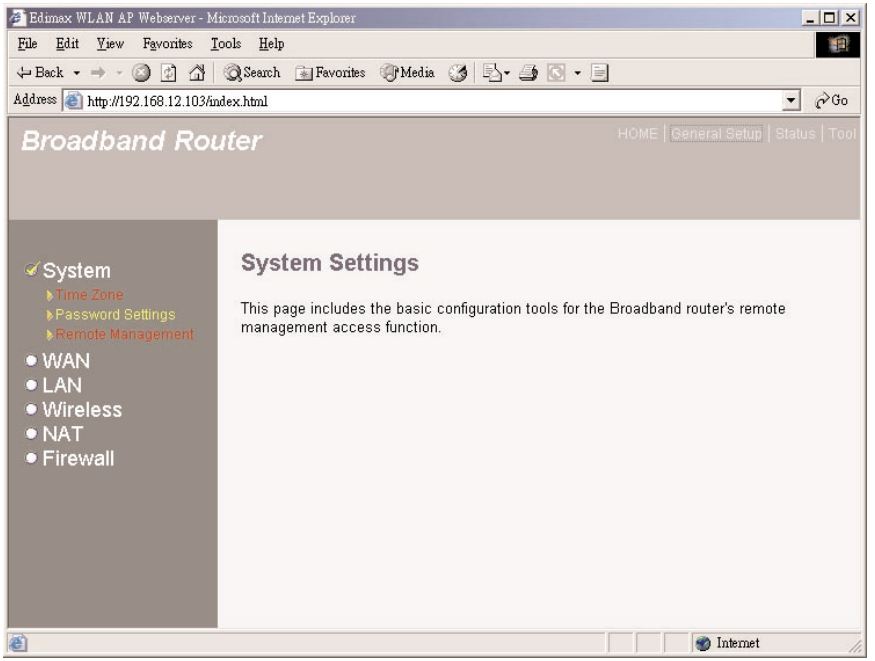


Figure 5-2. System settings screen.

Table 5-2 lists the router's system settings options.

Table 5-2. System settings parameters.

Parameters	Description
Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Password Settings	Allows you to select a password in order to access the Web-based management Web site.
Remote Management	You can specify a Host IP address that can perform remote management functions.

Select one of the previous three system settings selections and proceed to the manual's relevant sub-section (**Section 5.1.1**, **5.1.2**, or **5.1.3**).

5.1.1 Time Zone

The Time Zone (see Figure 5-3) allows your router to base its time on the settings configured here. This will affect functions such as log entries and firewall settings.

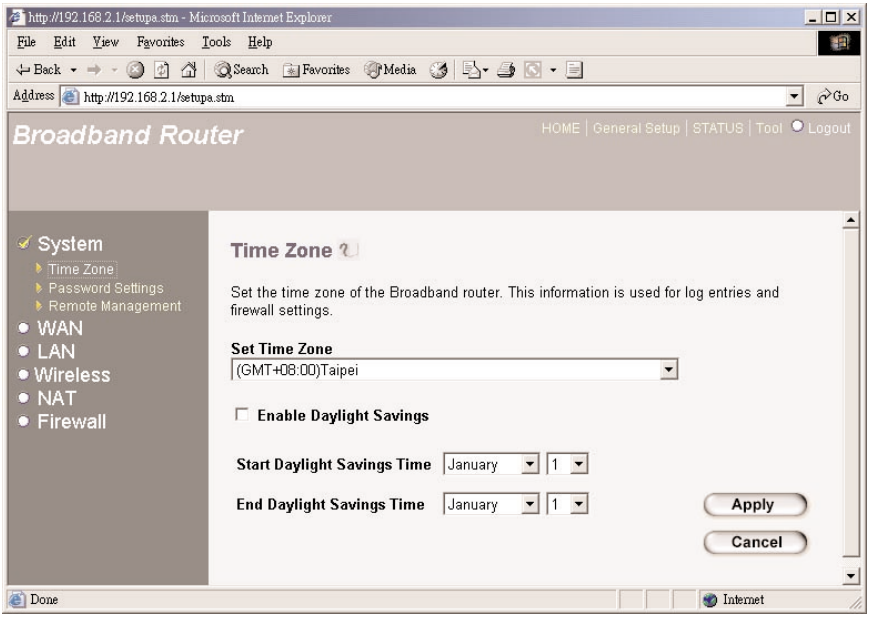


Figure 5-3. Time zone screen.

Table 5-3 lists the router's time zone options.

Table 5-3. Time zone parameters.

Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Enable Daylight Savings	The router can also take Daylight Savings into account. If you wish to use this function, you must check the Enable Daylight Savings box.

Table 5-3 (continued). Time Zone parameters.

Parameter	Description
Start Daylight Savings Time	Select the day you want to start Daylight Savings Time.
End Daylight Savings Time	Select the day you want to end Daylight Savings Time.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advance settings in place).

5.1.2 Password Settings

You can change the password (see Figure 5-4) required to log into the router's system Web-based management. By default, there is no password. Assign a password to the administrator as soon as possible and store it in a safe place. Passwords can contain up to 12 alphanumeric characters and are case-sensitive.

Figure 5-4. Password settings screen.

Table 5-4 lists the router's password settings options.

Table 5-4. Password settings parameters.

Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your router.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification purposes.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

NOTE

By default there is no password.

NOTE

If you forget your password, you'll have to reset the router to the factory default (no password) with the reset button (see Figure 2-1).

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.1.3 Remote Management

The remote management function (see Figure 5-5) gives an Internet host the ability to configure the router from a remote site. Enter the designated host IP address in the Host Address field.

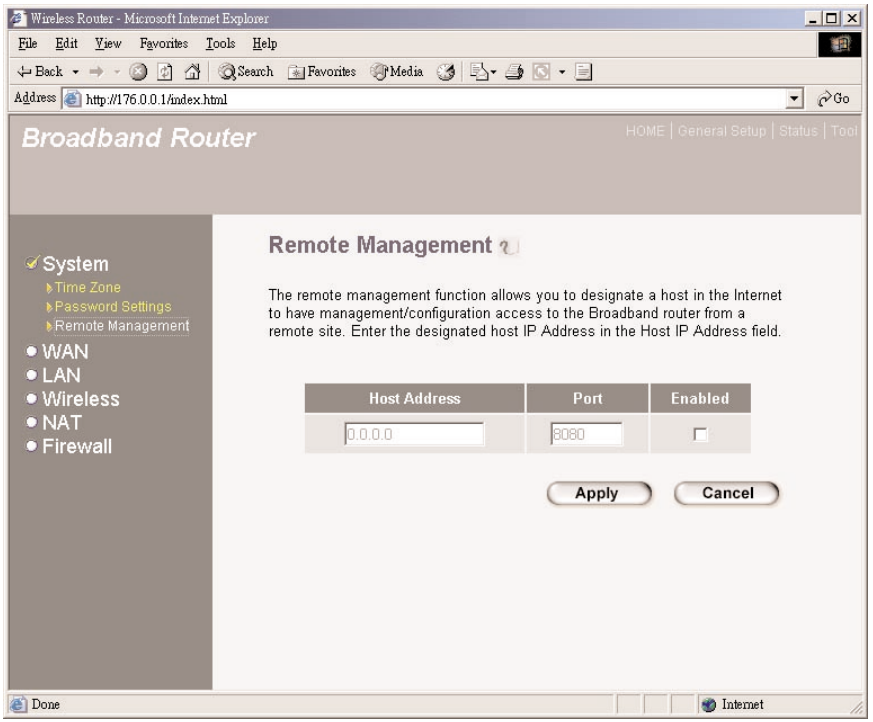


Figure 5-5. Remote management screen.

Table 5-5 lists the router's remote management options.

Table 5-5. Remote management parameters.

Parameters	Description
Host Address	This is the host's IP address in the Internet (not the local IP address) that will have management/configuration access to the router from a remote site. If you are at home and your home IP address has been designated as the router's remote management host IP address (located in your company office), then you are able to configure the router from your home. If the Host Address is left as 0.0.0.0, anyone can access the router's Web-based configuration from a remote location, providing they know the password.
Port	The port number of remote management Web interface.
Enabled	Select Enabled to enable the remote management function.
Apply button	Click on this button to apply your changes.
Cancel button	Click on this button to cancel your changes.

NOTE

When you want to access the Web-based management from a remote site, you must enter the router's WAN IP address (for example, 10.0.0.1) into your Web browser, followed by port number 8080. For example, enter 10.0.0.1:8080 (see Figure 5-6). You'll also need to know the password set in the Password Setting screen in order to access the router's Web-based management.

Figure 5-6. WAN IP address.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.2 WAN

Use the WAN Settings screen (Figure 5-7) if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows you to specify the type of WAN port connection you want to establish with your ISP. The WAN settings offer the following selections for the router's WAN port: dynamic IP, static IP address, PPPoE, PPTP, L2TP, and Telstra Big Pond.

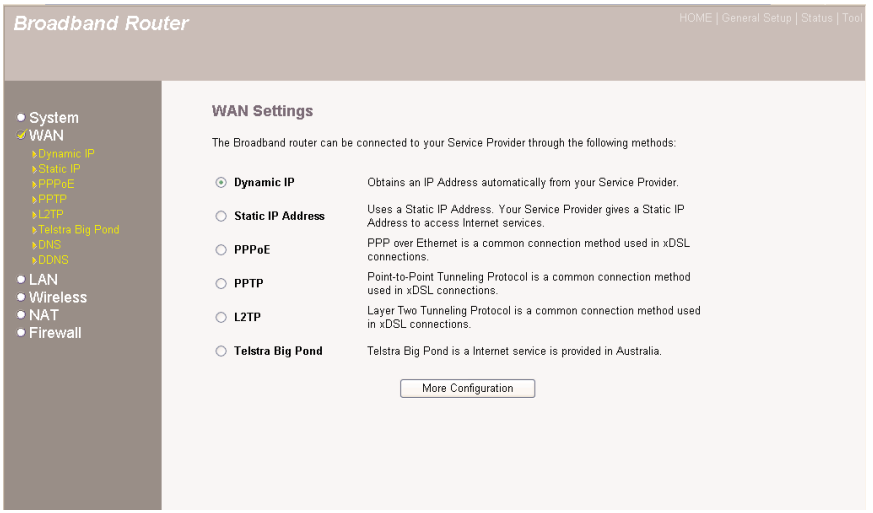


Figure 5-7. WAN settings screen.

Table 5-6 lists the router's WAN settings options.

Table 5-6. WAN settings parameters.

Parameters	Description
Dynamic IP	Your ISP will automatically give you an IP address.

Table 5-6 (continued). WAN settings parameters.

Parameters	Description
Static IP address	Your ISP has given you an IP address already.
PPPoE	Your ISP requires you to use a PPPoE connection.
PPTP	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
L2TP	Your ISP requires an L2TP connection.
Telstra Big Pond	Your ISP requires a Telstra Big Pond connection.
More Configuration button	Click on this button to further configure the selected option.

Once you have made a selection, click on **More Configuration** at the bottom of the screen and proceed to the manual's relevant sub-section (**Section 5.2.1** through **5.2.8**).

5.2.1 Dynamic IP

Choose the Dynamic IP selection if your ISP will automatically give you an IP address. Some ISPs may also require that you fill in additional information such as host name, domain name, and MAC address (see **4.2.1**, Cable Modem, for more details).

5.2.2 Static IP Address

Select Static IP Address if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section. (See **Section 4.2.2**, Fixed-IP xDSL, for more details.)

5.2.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol for connecting to the Internet. Your ISP should provide all the information required in this section. (See **Section 4.2.3**, PPPoE xDSL, for more details.)

5.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol for connecting to the Internet. Your ISP should provide all the information required in this section. (See **Section 4.2.4**, PPTP xDSL, for more details.)

5.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol for connecting to the Internet. Your ISP should provide all the information required in this section.

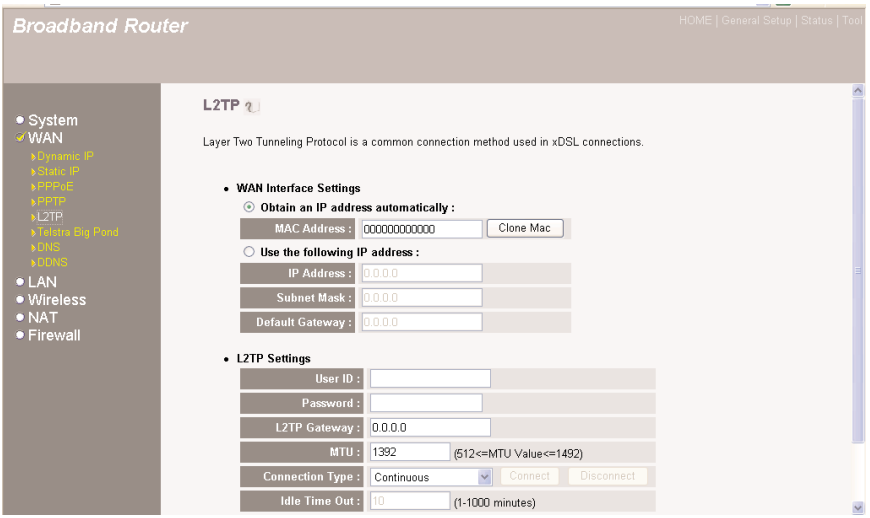


Figure 5-8. L2TP screen.

Table 5-7 lists the router's L2TP options.

Table 5-7. L2TP parameters.

Parameter	Description
Obtain an IP address automatically	The ISP requires you to obtain an IP address by DHCP before connecting to the L2TP server.
Clone MAC button	Press this button to use the MAC address.

Table 5-7 (continued). L2TP parameters.

Parameter	Description
Use the following IP address	The ISP give you a static IP to be used to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish an L2TP connection.
Subnet Mask	Enter the subnet mask provided by your ISP (for example, 255.255.255.0).
Default Gateway	Enter the ISP gateway's IP address.
User ID	Enter the PPTP connection's user name provided by your ISP. This is sometimes called a connection ID.
Password	Enter the password provided by your ISP for the PPTP connection.
L2TP Gateway	If your LAN has an L2TP gateway, enter that L2TP gateway IP address here. If you do not have an L2TP gateway, enter the ISP's gateway IP address.
MTU	(This is optional.) Type in the maximum size of your transmission packet to the Internet. Leave it as is if you don't want to set a maximum packet size.
Connection Type	If you select **Continuous**, the router will always connect to the ISP. If the WAN line breaks down and links again, the router will auto-reconnect to the ISP.

Table 5-7 (continued). L2TP parameters.

Parameter	Description
Connection Type (continued)	If you select **Connect On Demand**, the router will auto-connect to the ISP when someone wants to use the Internet and stay connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the idle time. If you select **Manual**, the router will connect to the ISP only when you click on **Connect** manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and later links again, the router will not auto-connect to the ISP.
Connect button	Click on this button to connect to the Internet via L2TP.
Disconnect button	Click on this button to disconnect from the Internet via L2TP.
Idle Time Out	You can specify an idle time threshold (minutes) for the WAN port. This means that if no packets have been sent (no one is using the Internet) throughout this specified period, then the router will automatically disconnect from your ISP.
OK button	Click on this button (not shown in Figure 5-8) to save your changes.

NOTE

This idle timeout function may not work because of some network application software's abnormal activities, computer virus, or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. Turn off your computer when you are not using it. This function also may not work with some ISPs. Make sure this function can work properly when you use it for the first time, especially if your ISP charges you by time used.

Click on **OK** when you have finished the configuration above. You have completed the configuration for the L2TP connection. Start using the router now, or if you wish to use some of the advanced features supported by this router see **Chapters 6** and **7**.

5.2.6 Telstra Big Pond

Select Telstra Big Pond (see Figure 5-9) if your ISP requires the Telstra Big Pond protocol for connecting to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia.

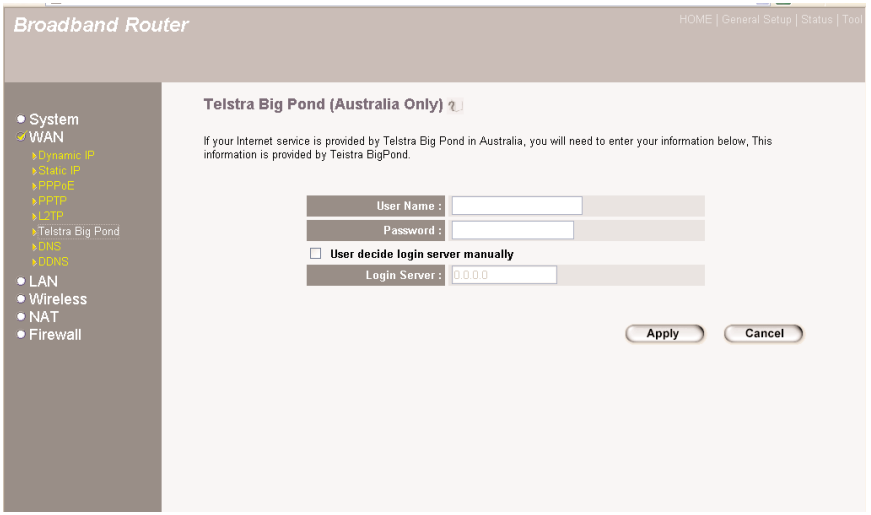


Figure 5-9. Telstra Big Pond screen.

Table 5-8 lists the router's Telstra Big Pond options.

Table 5-8. Telstra Big Pond parameters.

Parameter	Description
User Name	Enter the user name provided by your ISP for the Telstra Big Pond connection.
Password	Enter the password provided by your ISP for the Telstra Big Pond connection.
User decide login server manually	Check this box if you want to assign the IP of Telstra Big Pond's login server manually.
Login Server	The login server's IP address.
Apply button	Click on this button to apply your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** when you have finished the configuration. The configuration for the Telstra Big Pond connection is complete. Start using the router now, or if you want to use some of the advanced features supported by this router see **Chapters 6** and **7**.

5.2.7 DNS

A Domain Name System (DNS) server (see Figure 5-10) is like an index of IP addresses and Web addresses. To get to this screen, click on DNS from the menu on the left side of the screen shown in Figure 5-7. If you type a Web address into your browser, such as *www.router.com*, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your service provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify the IP address of that DNS server here.

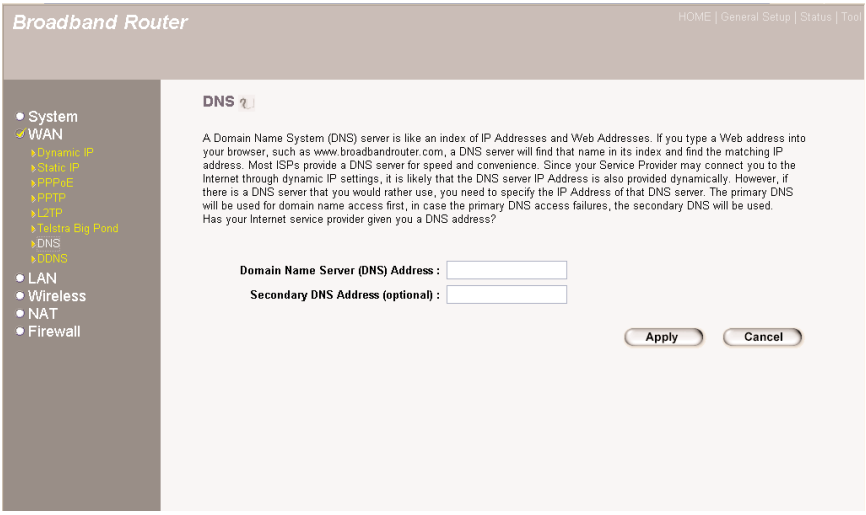


Figure 5-10. DNS screen.

Table 5-9 lists the router's DNS options.

Table 5-9. DNS parameters.

Parameters	Description
Domain Name Server (DNS) Address	This is the ISP's DNS server IP address provided, or specify your own preferred DNS server IP address.
Secondary DNS Address (optional)	(This is optional.) You can enter another DNS server's IP address as a backup. The secondary DNS will be used if the primary DNS fails.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. Configure other advanced sections or start using the router (with the advanced settings in place).

5.2.8 DDNS

DDNS (see Figure 5-11) allows you to map the static domain name to a dynamic IP address. To get to this screen, click on DDNS from the menu on the left side of the screen shown in Figure 5-7. You must get an account, password, and your static domain name from the DDNS service providers. This router supports DynDNS and TZO.

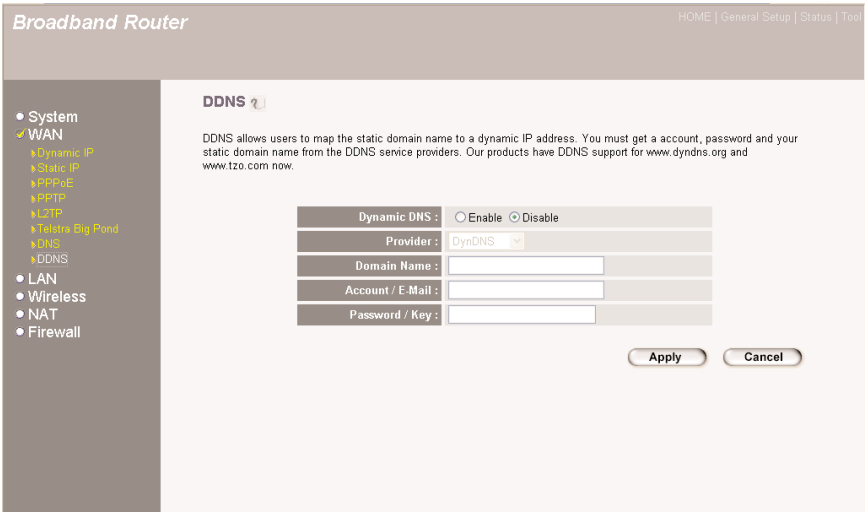


Figure 5-11. DDNS screen.

Table 5-10 lists the router's DDNS options.

Table 5-10. DDNS parameters.

Parameters	Description
Dynamic DNS Enable/Disable	Enable/disable the router's DDNS function. Default is Disable.
Provider	Select a DDNS service provider.
Domain name	Your static domain name that uses DDNS.

Table 5-10 (continued). DDNS parameters.

Parameters	Description
Account/E-mail	The account that your DDNS service provider assigned to you.
Password/Key	The password you set for the DDNS service account above.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.3 LAN

The LAN Settings screen (see Figure 5-12) allows you to specify your router's LAN port's private IP address as well as your LAN segment's subnet mask.

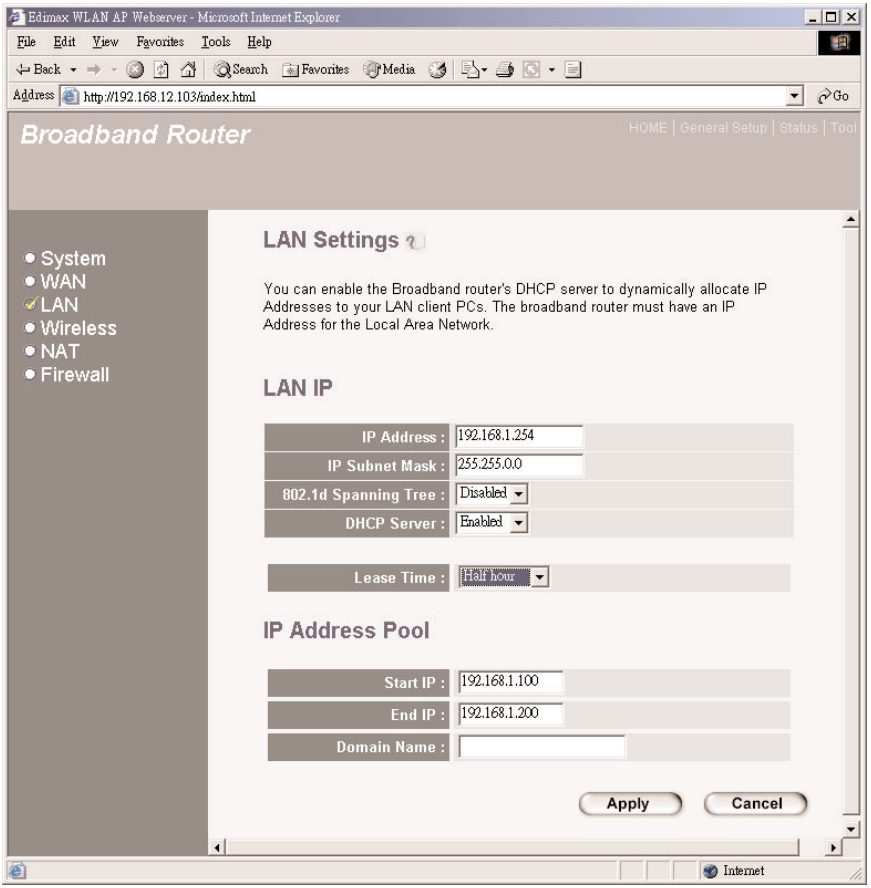


Figure 5-12. LAN settings screen.

Table 5-11 lists the router's LAN settings options.

Table 5-11. LAN settings parameters.

Parameters	Default	Description
LAN IP IP address	192.168.2.1	This is the router's LAN port IP address (your LAN client's default gateway IP address).
IP Subnet Mask	255.255.255.0	Specify a subnet mask for your LAN segment.
802.1d Spanning Tree	Disabled	If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent network loops in the LAN ports.
DHCP Server	Enabled	Enable or disable the DHCP server. When DHCP is enabled, the router will automatically give your LAN clients an IP address. If the DHCP is not enabled, you'll have to manually set your LAN client's IP addresses. Make sure the LAN client is in the same subnet as the router if you want the router to be your LAN client's default gateway.
Lease Time		The DHCP, when enabled, will temporarily give your LAN clients an IP address. In the lease time setting, you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.

Table 5-11 (continued). LAN settings parameters.

Parameters	Default	Description
IP Address Pool Start IP End IP	 192.168.1.100 192.168.1.200	Select a particular IP address range for your DHCP server to issue IP addresses to your LAN clients.
Domain Name	None	Specify a domain name for your LAN.
Apply button	—	Click on this button to save your changes.
Cancel button	—	Click on this button to cancel your changes.

NOTE

By default, the IP range is a Start IP of 192.168.2.100 and an End IP of 192.168.2.199. If you want your PC to have a static/fixed IP address, you'll have to choose an IP address outside this IP address pool.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.4 Wireless

The router has a built-in IEEE 802.11g/b wireless access point. It incorporates a wireless LAN that enables all PCs equipped with an IEEE 802.11g or 802.11b wireless network adapter to connect to your Intranet. The access point supports WEP encryption to enhance the security of your wireless network. Wireless access point menu options are listed on the left side of the screen shown in Figure 5-13.

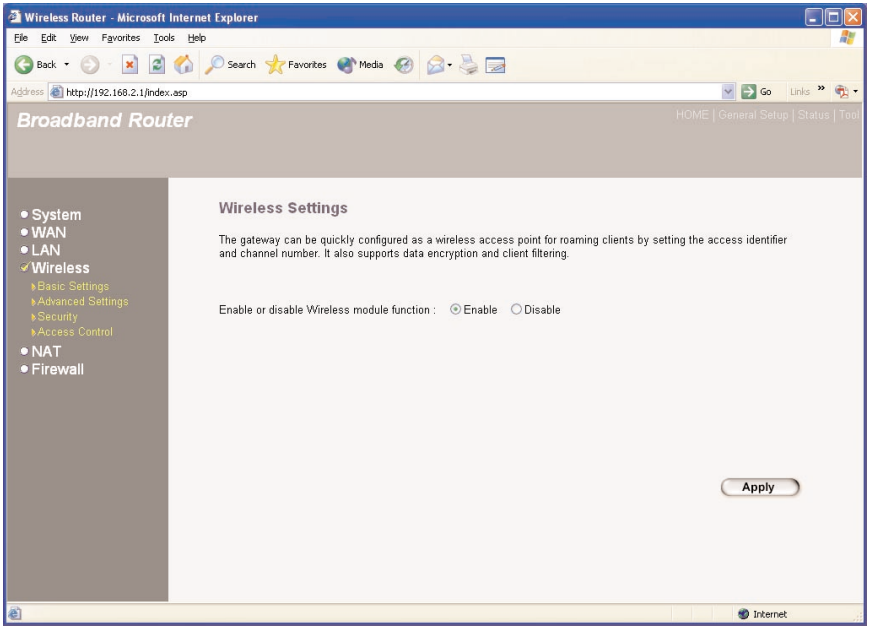


Figure 5-13. Wireless settings screen.

Table 5-12 describes the router's access point's wireless settings options.

Table 5-12. Wireless settings parameters.

Parameters	Default	Description
Enable or disable wireless module	Enable	Enable or disable the router's wireless access point module.
Apply button	—	Click on this button to save your changes.

Select the menu option from the four options under the Wireless menu on the left side of Figure 5-13, then click on **Apply** at the bottom of the screen to go to the selected menu. Depending on the menu option you selected, one of the screens shown in Figure 5-14, 5-20, 5-21, or 5-27 will appear. Refer to the appropriate section (**Sections 5.4.1**, **5.4.2**, **5.4.3**, or **5.4.4**). You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.4.1 Basic Settings

To get to the Basic Settings screen (see Figure 5-14), click on **Basic Settings** in the menu on the left in Figure 5-13. From the Basic Settings screen, you can set the wireless router to AP, bridge, and AP bridge-WDS, AP bridge point-to-point, or AP bridge point-to-multipoint modes. AP mode provides pure access point function. The simplest way to build up a wireless LAN is to use AP mode. Bridge mode bridges more than two wired Ethernet networks together by wireless LAN. Use two access points or wireless routers with AP bridge-point to point mode (see Figure 5-15) to bridge two wired Ethernet networks together.

To bridge more than two wired Ethernet networks together, you must use enough access points or wireless routers with AP bridge-point to multipoint mode (see Figure 5-16). A wireless router with AP bridge-point to point mode or AP bridge-point to multipoint mode can only be used to bridge wired Ethernet networks together. It can't accept connections from other wireless stations at the same time.

If you want a wireless router to bridge wired Ethernet networks and provide connection service for other wireless stations at the same time, you have to set the wireless router to AP bridge-WDS mode (see Figure 5-17). Simply speaking, the AP bridge-WDS mode function is the combination of AP mode and AP bridge-point to multipoint mode.

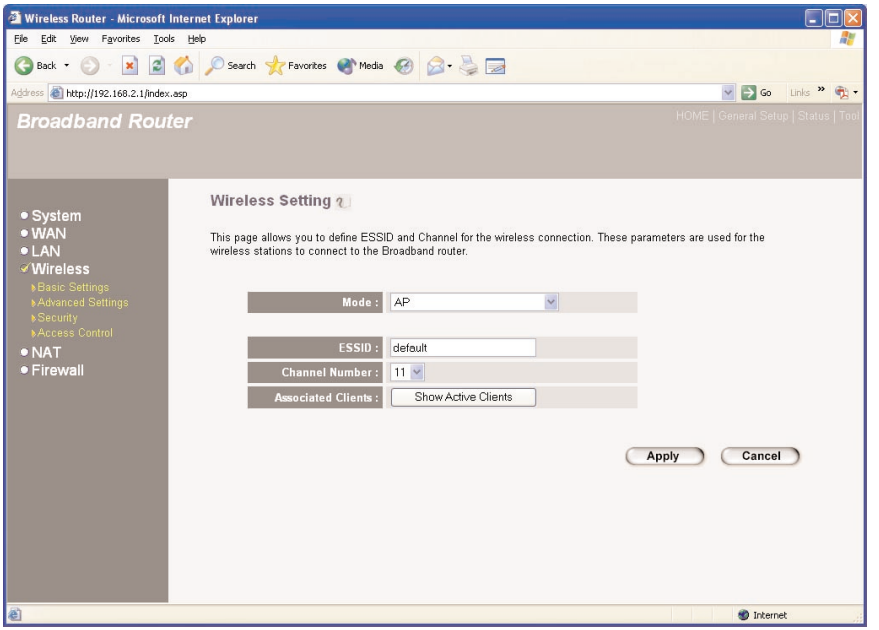


Figure 5-14. Basic settings screen.

Table 5-13 lists the router's basic settings options.

Table 5-13. Basic settings parameters.

Parameters	Default	Description
Mode	—	Select from AP, bridge, AP bridge-WDS, AP bridge point-to-point, or AP bridge point-to-multipoint.
ESSID	default	This is the name of the wireless LAN. All the devices in the same wireless LAN should have the same ESSID.
Channel Number	11	The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.
Associated Clients	None	Click on the **Show Active Clients** button, then an Active Wireless Client Table will pop up (see page 69). You can see the status of all active wireless stations that are connecting to the access point.
Apply button	—	Click on this button to save your changes.
Cancel	—	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

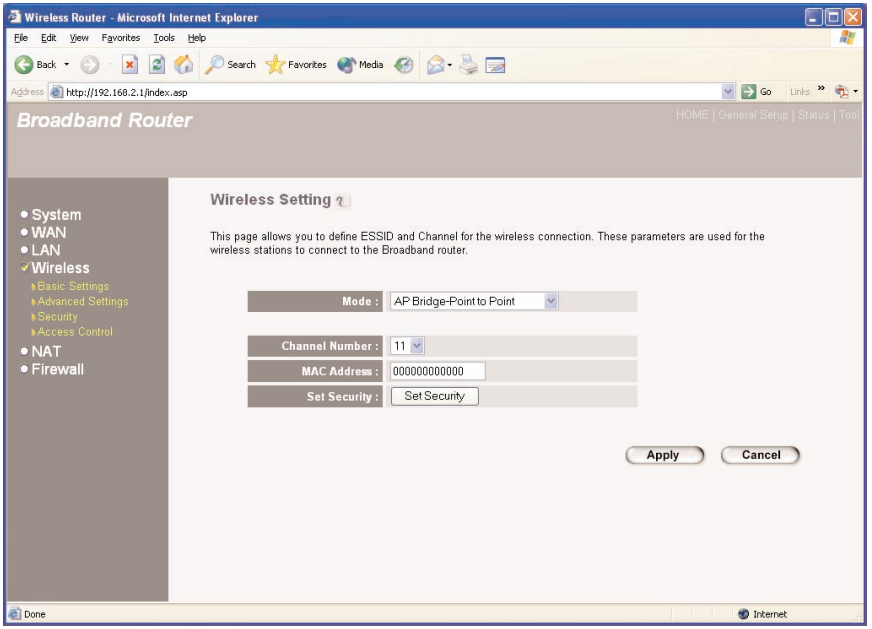


Figure 5-15. AP bridge-point to point mode settings page.

Table 5-14 lists the router's AP bridge-point to point or multipoint options.

Table 5-14. AP bridge-point to point or multipoint mode parameters.

Parameter	Description
Mode	Select from AP, bridge, AP bridge-WDS, AP bridge point-to-point, or AP bridge point-to-multipoint.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1–11 (North America) Channel 1–14 (Japan) Channel 1–13 (Europe) Assign an alias name in AP mode, station-ad hoc mode, AP bridge-point to point mode, AP bridge-point to multi-point mode, and AP bridge-WDS mode.

Table 5-14 (continued). AP bridge-point to point or multipoint mode parameters.

Parameter	Description
MAC Address	If you want to bridge more than one wired Ethernet network together with a wireless LAN, set this access point to AP bridge-point-to-point mode, AP bridge-point-to-multipoint mode, or AP bridge-WDS mode. Enter the MAC addresses of other access points that join the bridging work.
Set Security	Enable or disable the security option.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

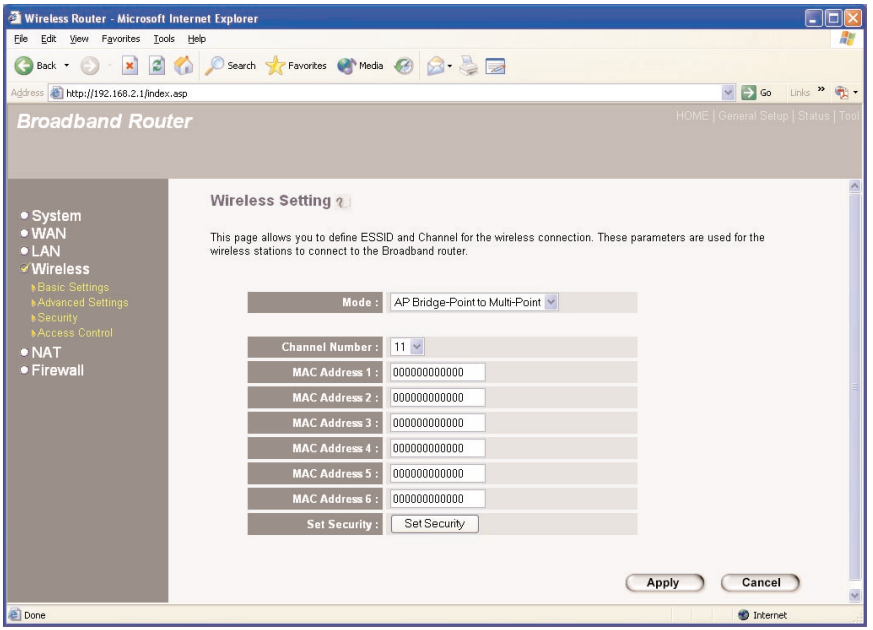


Figure 5-16. AP bridge-point to multipoint mode setting screen.

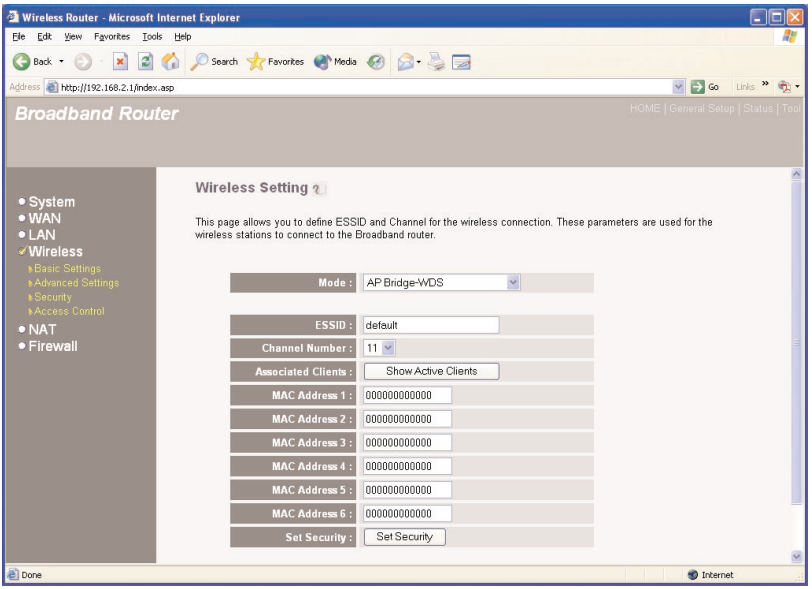


Figure 5-17. AP bridge-WDS mode settings page.

Table 5-15 lists the router's AP bridge-WDS mode options.

Table 5-15. AP bridge-WDS mode settings parameters.

Parameter	Description
Mode	Select from AP, bridge, AP bridge-WDS, AP bridge point-to-point, or AP bridge point-to-multipoint.
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Make sure that the ESSID of all stations in the same WLAN network are the same. The default ESSID is **default**. Assign an alias name in AP mode, station-ad hoc mode, station-infrastructure mode, and AP bridge-WDS mode.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. There are 14 channels available. Channel 1–11 (North America) Channel 1–14 (Japan) Channel 1–13 (Europe)

Table 5-15 (continued). AP bridge-WDS mode settings parameters.

Parameter	Description
Associated Clients	Click on the **Show Active Clients** button, then the Active Wireless Client Table (see Figure 5-19) will appear. You can see the status of all active wireless stations that are connecting to the access point.
MAC Address	If you want to bridge more than one wired Ethernet network together with a wireless LAN, you must set this access point to AP bridge-point to point mode, AP bridge-point to multipoint mode, or AP bridge-WDS mode. Enter the MAC addresses of other access points that join the bridging work.
Set Security	Click on **Set Security** in Figure 5-17 to set up the WEP encryption. The paragraph entitled "Set Security" below provides more information about this parameter.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the access point.

Set Security

While you are in the AP bridge-WDS mode settings screen (Figure 5-17), you can set up the WEP encryption used for the communication between all current or future access points or wireless routers that join the bridging job. Doing this ensures that security will be enabled for all wireless APs or routers in the network. Click on the Set Security button in Figure 5-17, and Figure 5-18 appears. The WEP setting here is not used to protect the communication between the wireless stations and this wireless router.

Figure 5-18. WDS security setup screen.

Table 5-16 lists the router's security options.

Table 5-16. Security parameters.

Parameters	Description
Enable WEP Security	Check this box to enable the WEP encryption between wireless routers and access points that join the bridging job.
Key Length	Select either the 64-bit or the 128-bit key to encrypt transmitted data. A larger key length will provide a higher level of security, but the throughput will be lower. You also can select disable to transmit data without encryption.
Key Format	Select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the WEP Key.

Table 5-16 (continued). Security parameters.

Parameters	Description
Key Format (continued)	For example: ASCII characters: guest Hexadecimal digits: 12345abcde
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select in the default key will take effect.
Encryption Keys 1–4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: Type in 10-digit Hex values (in the A–F, a–f, and 0–9 range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: Type in 26-digit Hex values (in the A–F, a–f, and 0–9 range) or 10-digit ASCII characters as the encryption keys.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router.

Active Wireless Client Table

Click on **Associated Clients** from the Basic Settings screen (Figure 5-14). Select **Show Active Clients** from the drop-down menu, then click on **Apply**. Figure 5-19 appears.

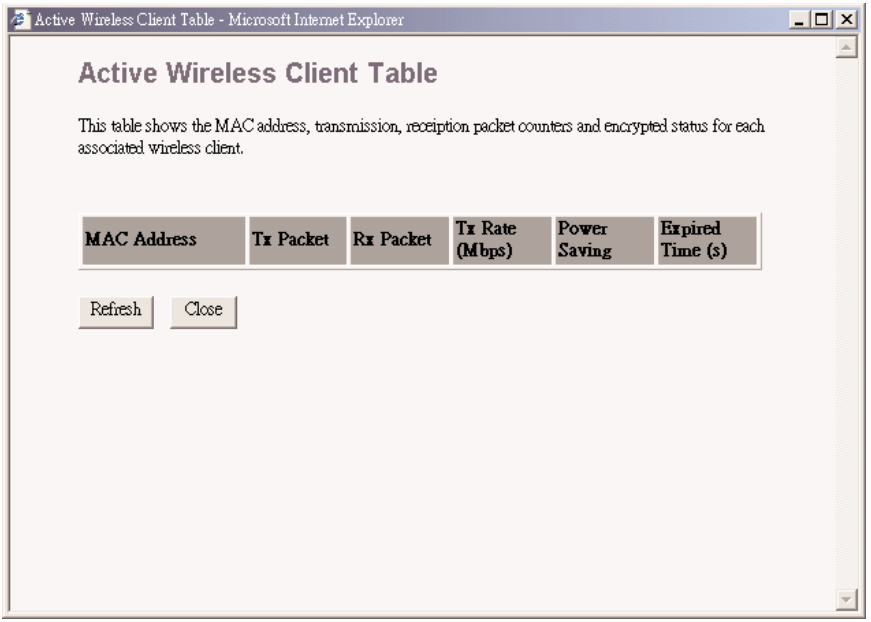


Figure 5-19. Active wireless client table screen.

Table 5-17 lists the active wireless client's options.

Table 5-17. Active wireless client table parameters.

Parameters	Description
MAC Address	MAC address of this active wireless station.
Tx Packet	The number of transmitted packets that are sent out from this active wireless station.
Rx Packet	The number of received packets that are received by this active wireless station.
TX Rate (Mbps)	The transmission rate in Mbps.
Power Saving	Shows if the wireless client is in power saving mode.

Table 5-17 (continued). Active wireless client table parameters.

Parameters	Description
Expired Time	This is the time in seconds before dissociation. If the wireless device stays idle longer than the expired time, this wireless router will dissociate it. The wireless client station has to associate again when it becomes active.
Refresh	Refresh the Active Wireless Client Table.
Close	Close the Active Wireless Client Table.

5.4.2 Advanced Settings

You can set the advanced wireless router LAN parameters. Select **Advanced Settings** from the Wireless Setting screen (see Figure 5-13). Figure 5-20 appears. Do not change any parameters unless you know what effect the changes will have on this router.

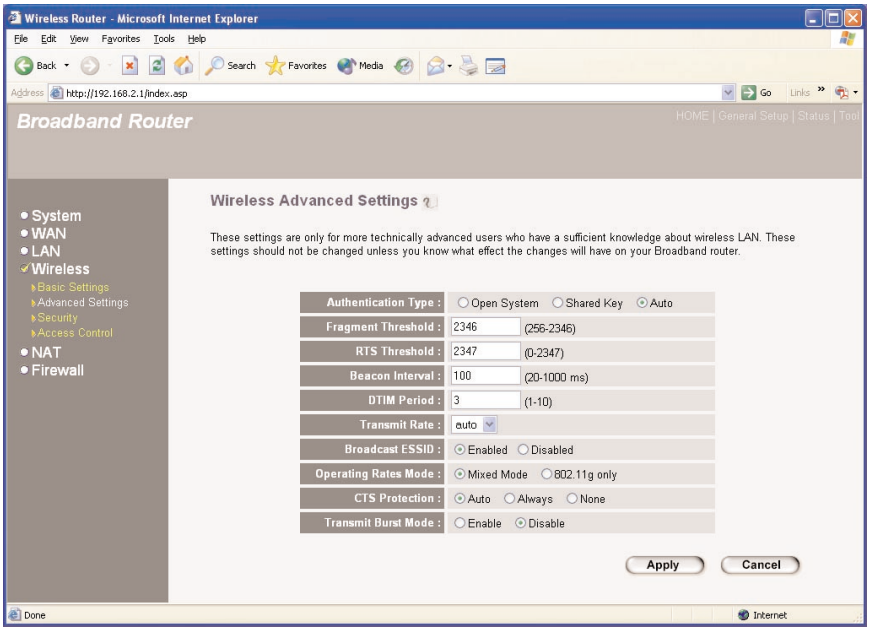


Figure 5-20. Wireless advanced settings screen.

Table 5-18 lists the wireless advanced settings options.

Table 5-18. Wireless advanced settings parameters.

Parameters	Description
Authentication Type	There are three authentication types: open system, shared key, and auto. When you select open system, wireless stations can associate with this wireless router without WEP encryption. When you select shared key, you should also set up WEP key in the encryption page, and wireless stations should use WEP encryption in the authentication phase to associate with this wireless router. If you select both, the wireless client can associate with this wireless router by using any one of these two authentication types. When you select Auto, the router will automatically select open system or shared key.
Fragment Threshold	Fragment threshold specifies the maximum size of packets during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	This is the interval of time that this wireless router broadcasts a beacon. A beacon is used to synchronize the wireless network.
DTM Period	Period of time that clients have to listen to broadcasts.
Transmit Rate	The data rate is the rate this router uses to transmit data packets. The router will use the highest possible selected transmission rate.

Table 5-18 (continued). Wireless advanced settings parameters.

Parameters	Description
Broadcast ESSID	If you enable broadcast ESSID, every wireless station located within this router's coverage can discover the access point easily. If you are building a public wireless network, enable this feature. Disabling broadcast ESSID can provide better security.
Operating Rates Mode	Operates in a pure 802.11g (54 Mbps) environment or a mix of 11-Mbps (802.11b) and 54-Mbps devices.
CTS Protection	Locks out access so that 802.11b frames and 802.11g frames are not mixed up.
Transmit Burst Mode	Provides short-lived bursts of data to 54-Mbps devices.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router.

5.4.3 Security

By using encryption, the data will be transmitted securely over the wireless network. You have to set up the same encryption key both on your router and wireless client devices. Select **Security** from the Wireless Setting screen (see Figure 5-13). Figure 5-21 appears.

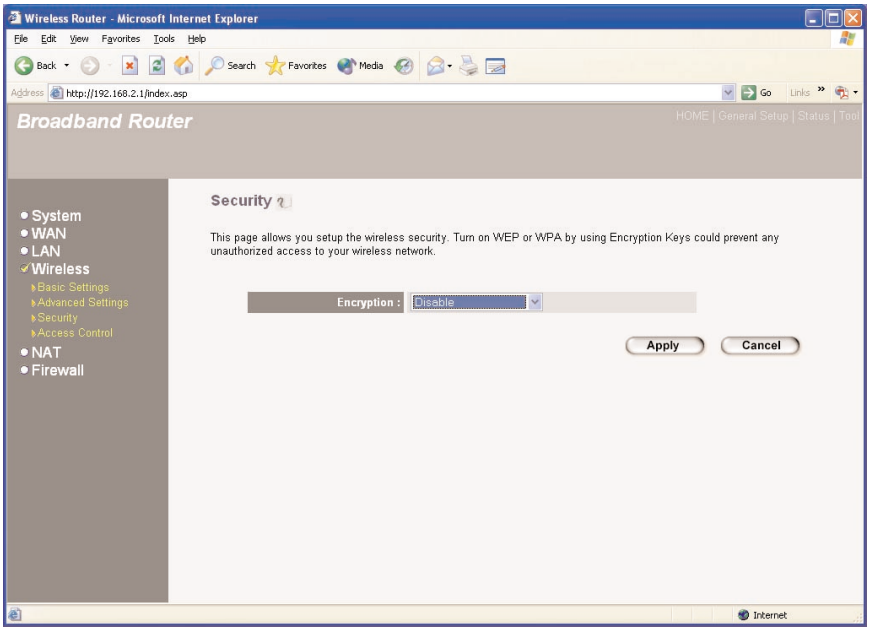


Figure 5-21. Security screen.

Table 5-19 lists the router's security options.

Table 5-19. Security parameters.

Parameters	Description
Encryption	Select the WEP key length for encryption (64-bit, 128-bit, or 152-bit). A larger WEP key length will provide a higher level of security, but the throughput will be lower. You also can select Disabled to transmit data without encryption. The default value is Disabled.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

When you select the 64-bit, 128-bit, or 152-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You also can enter a pass phrase and let the router generate the WEP key for you. In the 64-bit WEP mode, you can enter four WEP keys and select one of them as the default key.

Then the router can receive any packets encrypted by one of the four keys.

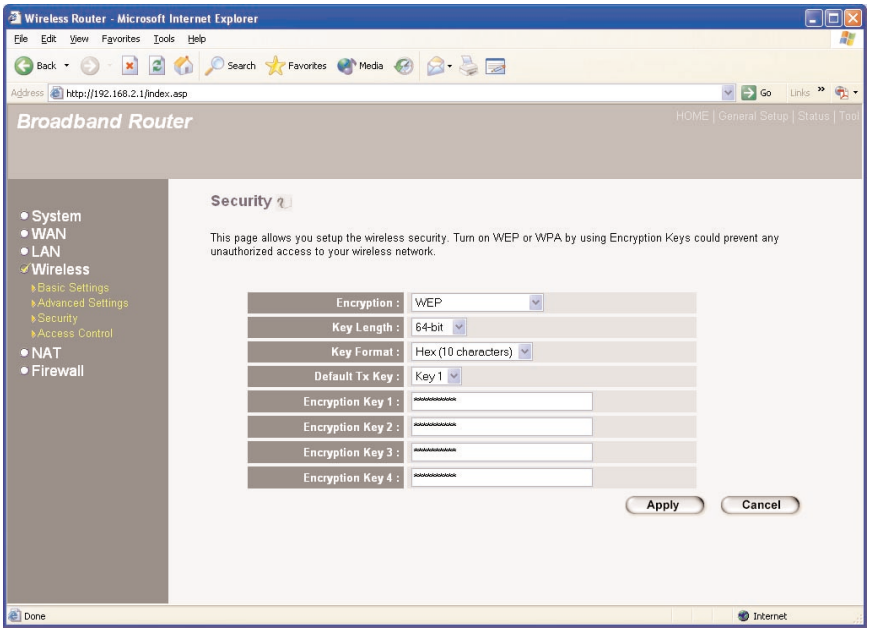


Figure 5-22. WEP encryption key security screen.

Table 5-20 lists the router's encryption options.

Table 5-20. Encryption parameters.

Parameters	Description
Encryption	Select **WEP** from the drop-down menu.
Key Length	Select the 64-, 128-, or 152-bit key to encrypt transmitted data. A larger WEP key length will provide a higher level of security, but the throughput will be lower. You can also select Disable to transmit data without encryption.

Table 5-20 (continued). Encryption parameters.

Parameters	Description
Key Format	Select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the WEP Key. For example: ASCII characters: guest Hexadecimal digits: 12345abcde
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select as the default key will take effect.
Encryption Key 1 – Key 4	The encryption keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: Type in 10-digit hex values (in the A–F, a–f, and 0–9 range) or 5-digit ASCII characters as the encryption keys. 128-bit WEP: Type in 26-digit hex values (in the A–F, a–f, or 0–9 range) or 10-digit ASCII characters as the encryption keys.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

802.1x

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to the router before accessing the wireless LAN. The authentication is processed by a RADIUS server. You can use an external RADIUS server or use the RADIUS server built into the router. This mode only authenticates users by IEEE 802.1x, but it does not encrypt the data during communication. Select IEEE 802.1x from the Wireless Settings screen (Figure 5-13). The IEEE 802.1x screen (Figure 5-23) appears.

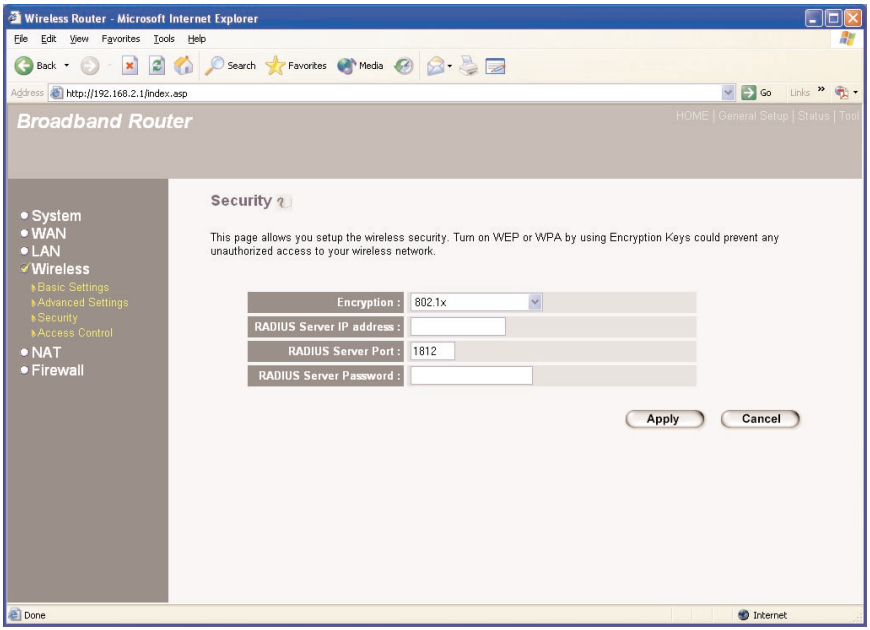


Figure 5-23. 802.1x screen.

Table 5-21 lists the router's 802.1x options.

Table 5-21. 802.1x parameters.

Parameter	Description
Encryption	Select **802.1x** from the drop-down menu.
RADIUS Server IP address	The external RADIUS server's IP address.

Table 5-21 (continued). 802.1x parameters.

Parameter	Description
RADIUS Server Port	The external RADIUS server's service port.
RADIUS Server Password	The password used by the external RADIUS server.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router.

802.1x WEP Static Key

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this router before accessing the wireless LAN. The authentication is processed by a RADIUS server. You can use an external RADIUS server or use the RADIUS server built into the router. This mode also uses WEP to encrypt the data during communication. To get to the IEEE 802.1x WEP static key screen, select WEP Static Key from the Security screen (Figure 5-21). Figure 5-24 appears.

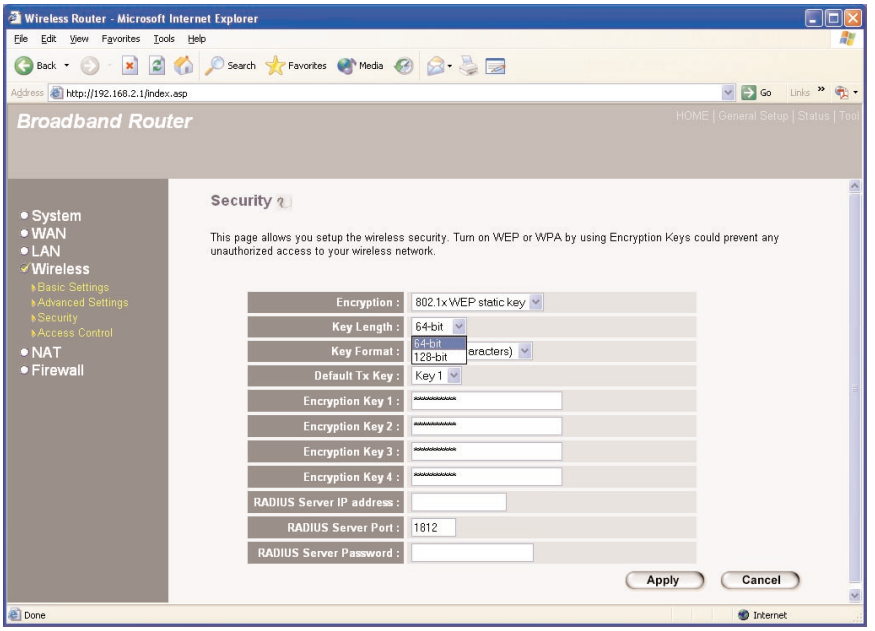


Figure 5-24. 802.1x WEP static key screen.

Table 5-22 lists the router's 802.1x WEP static key options.

Table 5-22. 802.1x WEP static key parameters.

Parameter	Description
Encryption	Select **802.1x WEP static key** from the drop-down menu.
Key Length	You may select 64-bit or 128-bit to encrypt transmitted data. A larger key length will provide a higher level of security, but the throughput will be lower.
Key Format	Select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal digits: 12345abcde

Table 5-22 (continued). 802.1x WEP static key parameters.

Parameter	Description
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select as the default key will take effect.
Encryption Key 1–4	The keys are used to encrypt data transmitted in the wireless network. Fill the text box, keeping in mind the points listed below. • 64-bit—Type in 10-digit Hex values (in the A–F, a–f, and 0–9 range) as the encryption keys. For example, "0123456aef". • 128-bit—Type in 26-digit Hex values (in the A–F, a–f, and 0–9 range) as the encryption keys. For example, "01234567890123456789abcdef".
RADIUS Server IP Address	The external RADIUS server's IP address.
RADIUS Server Port	The external RADIUS server's service port.
RADIUS Server Password	The password used by external RADIUS server.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router.

WPA pre-shared key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP to change the encryption key frequently. This can improve security. Select **WPA Pre-Shared Key** from the Security screen (Figure 5-21). Figure 5-25 appears.

NOTE

This router does not provide the AES encryption method.

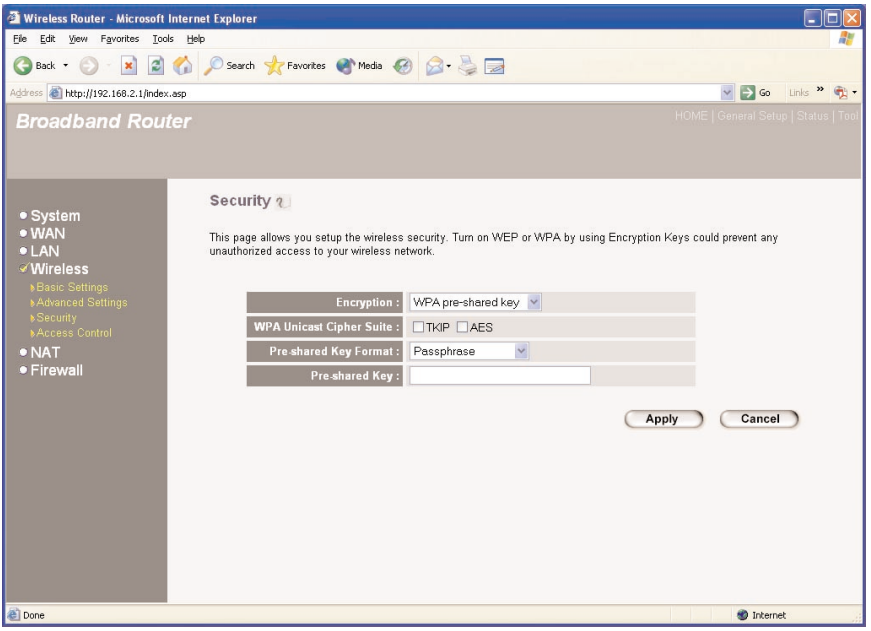


Figure 5-25. WPA pre-shared key screen.

Table 5-23 lists the router's pre-shared key options.

Table 5-23. WPA pre-shared key parameters.

Parameter	Description
Encryption	Select WPA Pre-Shared Key from the drop-down menu.
WPA Unicast Cipher Suite	Check the TKIP box to change the encryption key frequently to enhance the wireless LAN's security. Check the AES box for an efficient and highly secure encryption algorithm that can enhance the wireless LAN's security.
Pre-shared Key Format	From the drop-down menu, select ASCII characters (alphanumeric format) or hexadecimal digits (in the A–F, a–f, and 0–9 range) to be the pre-shared key. For example: ASCII Characters: iamguest Hexadecimal digits: 12345abcde
Pre-shared Key	The pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex WEP: Type in 64-digit hex values (in the A–F, a–f, and 0–9 range) or at least an 8-character pass phrase for the pre-shared keys.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router.

WPA RADIUS

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP to change the encryption key frequently. This can improve security. To get to this screen, select **WPA** from the Security screen (see Figure 5-21). The WPA RADIUS setup screen appears (see Figure 5-26).

NOTES

This router does not provide AES encryption method.

WPA cannot use the internal RADIUS server for authentication.

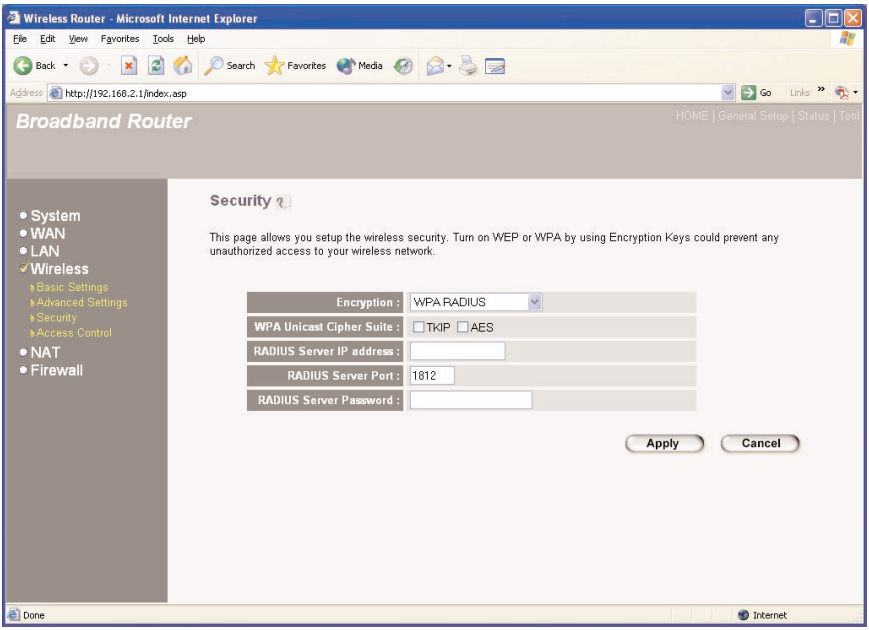


Figure 5-26. WPA RADIUS setup screen.

Table 5-24 lists the router's WPA RADIUS setup options.

Table 5-24. WPA RADIUS setup screen parameters.

Parameter	Description
Encryption	Select **WPA radius** from the drop-down menu.
WPA Unicast Cipher Suite	Check the TKIP box to change the encryption key frequently to enhance the wireless LAN security. The AES option is not available.
RADIUS Server IP Address	The external RADIUS server's IP address.
RADIUS Server Port	The external RADIUS server's service port.
RADIUS Server Password	The external RADIUS server's password.
Apply button	Click on this button to save your changes.
Cancel button	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router.

5.4.4 Access Control

This wireless router provides MAC access control, which prevents unauthorized MAC addresses from accessing your wireless network. To get to this screen, select **Access Control** from the Wireless Settings screen (Figure 5-13). The Wireless access control screen appears (see Figure 5-27).

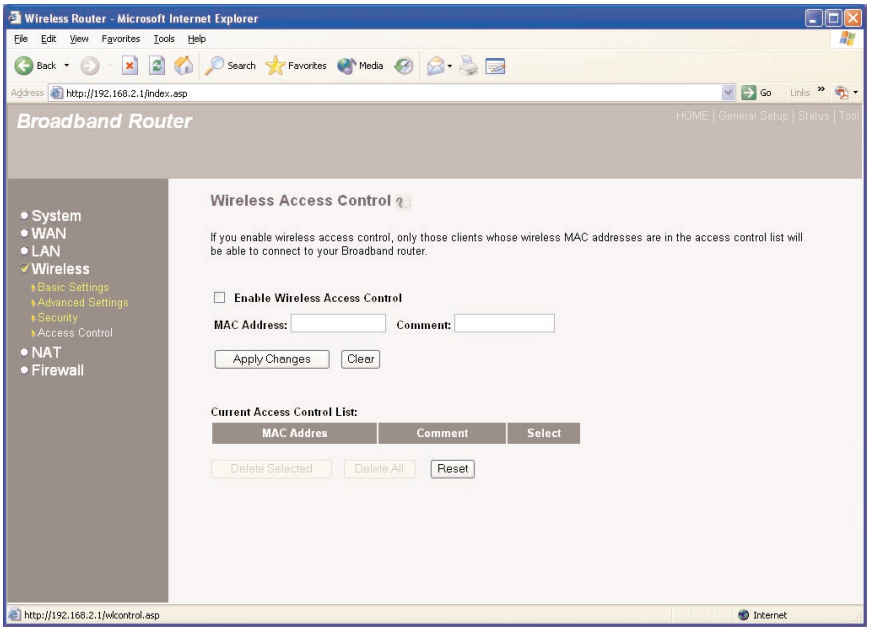


Figure 5-27. Wireless access control screen.

Table 5-25 lists the router's wireless access control options.

Table 5-25. Wireless access control parameters.

Parameters	Description
Enable Wireless Access Control	Check this box to enable wireless access control.
MAC Address	Type in the MAC address for the wireless station to be added.
Comment	Type in a comment for the wireless station to be added.
Apply Changes	Click on this button to add the wireless station to the Current Access Control List.

Table 5-25 (continued). Wireless access control parameters.

Parameters	Description
Clear	If you make a typing error before clicking on **Apply Changes** and want to retype it, click on the **Clear** button. Both the MAC Address and Comment fields will be cleared.
Delete Selected	If you want to remove some MAC addresses from the Current Access Control List, select the MAC addresses you want to remove, then click on this button.
Delete All	If you want remove all MAC addresses from the table, click on this button.
Reset	Click on this button to clear your current selections.

Click on **Apply Changes** to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.5 NAT

Network Address Translation (NAT) (see Figure 5-28) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT provides firewall protection from hacker attacks and has the flexibility to allow you to map private IP addresses to public IP addresses for key services such as Web sites and FTP.

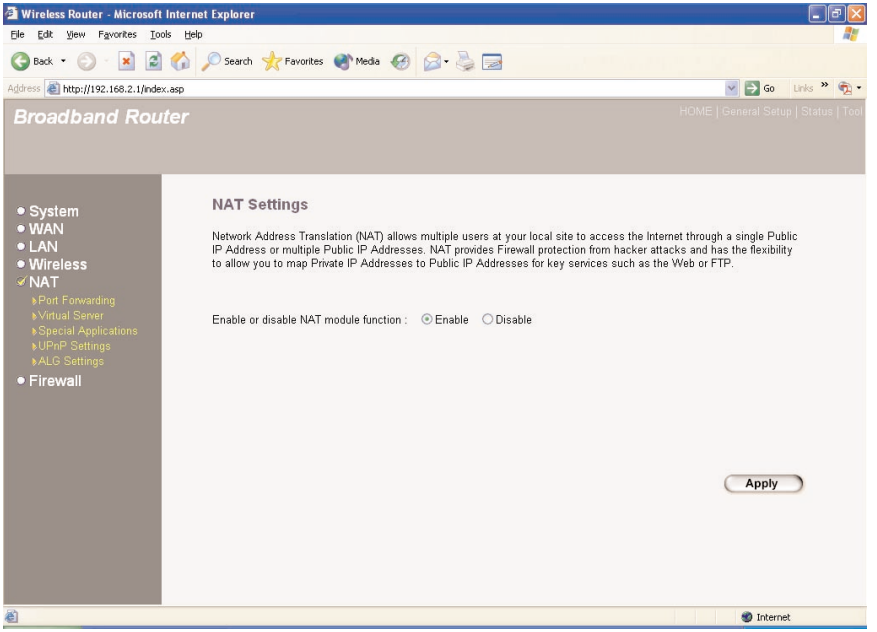


Figure 5-28. NAT settings screen.

Table 5-26 lists the router's NAT settings options.

Table 5-26. NAT settings parameters.

Parameter	Description
Port Forwarding	Different services (for example, email, FTP, Web, etc.) can apply to different service servers/clients in your LAN. Select the port forwarding option from the vertical menu on the left side of the screen to allow you to redirect a particular range of service port numbers (from the Internet/WAN ports) to a particular LAN IP address.

Table 5-26 (continued). NAT settings parameters.

Parameter	Description
Virtual Server	Different services (for example, email, FTP, Web, etc.) can apply to different service servers/clients in your LAN. The virtual server option allows you to redirect a particular service port number (from the Internet/WAN port) to a particular LAN IP address and its service port number.
Special Applications	Some applications require multiple connections, such as Internet games, videoconferencing, Internet telephony, and others. In the Special Applications section, you can configure the router to support these types of applications.
UPnP Settings	UPnP is more than just a simple extension of the plug-and-play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for device categories from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices—all automatically, truly enabling zero configuration networks. Devices can subsequently communicate with each other directly, further enabling peer-to-peer networking.
ALG Settings	You can select special applications for gateways operating at the ISO's Application layer.
Enable button	Once you select an option from the vertical menu on the left side of Figure 5-28, click on this button (in the middle of the screen) to go to the option's screen.
Disable button	Click on this button to disconnect from an option's screen.
Apply button	Click on this button to go on to the next screen.

Click on one of the NAT selections and proceed to the manual's relevant sub-section (**5.5.1**, **5.5.2**, **5.5.3**, **5.5.4**, or **5.5.5**).

5.5.1 Port Forwarding

The Port Forwarding screen (see Figure 5-29) allows you to redirect a particular range of service port numbers (from the Internet/WAN ports) to a particular LAN IP address. It helps you host some servers behind the router NAT firewall.

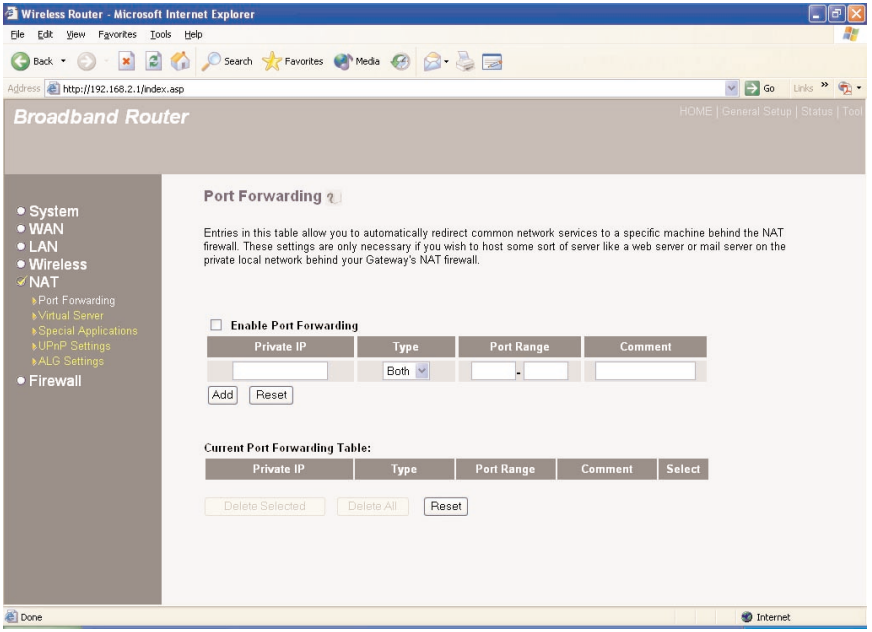


Figure 5-29. Port forwarding screen.

Table 5-27 lists the router's port forwarding options.

Table 5-27. Port forwarding parameters.

Parameter	Description
Enable Port Forwarding	Check this box to enable port forwarding.
Private IP	This is the private IP of the server behind the NAT firewall.

Table 5-27 (continued). Port forwarding parameters.

Parameter	Description
Type	This is the protocol type to be forwarded. You can choose to forward either TCP or UDP packets or both.
Port Range	The range of ports to be forwarded to the private IP.
Comment	The description of the port range setting.
Add	Type in the private IP, type, port range, and comment of the setting to be added, then click on this button.This port forwarding setting will be added to the screen's Current Port Forwarding Table.
Reset	If you make a mistake and haven't pressed **Add** yet, click on this button to clear the fields.
Delete Selected	If you want to remove some port forwarding settings from the Current Port Forwarding Table, select them and click on this button.
Delete All	If you want remove all port forwarding settings from the table, click on this button.
Reset	Click on this button to clear your current selections.

NOTE

Give your LAN PC clients a fixed/static IP address for port forwarding to work properly.

Click on **Add** to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.5.2 Virtual Server

Use the Virtual Server function (see Figure 5-30) when you want different servers/clients in your LAN to handle different services/applications from the Internet (for example, email, FTP, Web server, etc.). Computers use port numbers to recognize a particular service/Internet application. The virtual server allows you to redirect a particular service port number (from the Internet/WAN port) to a particular LAN private IP address and its service port number. (See the **Glossary** for an explanation of port number.)

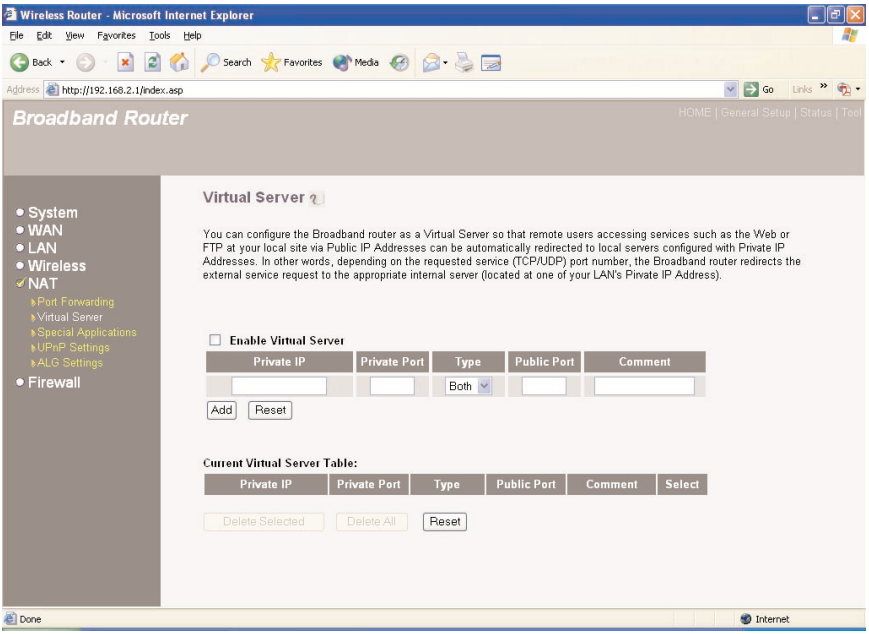


Figure 5-30. Virtual server screen.

Table 5-28 lists the router's virtual server options.

Table 5-28. Virtual server parameters.

Parameters	Description
Enable Virtual Server	Check this box to enable the virtual server.
Private IP	This is the LAN client/host IP address that the public port number packet will be sent to.

Table 5-28 (continued). Virtual server parameters.

Parameters	Description
Private Port	This is the port number (of the previously mentioned private IP host) that the public port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).
Type	Select the port number protocol type (TCP, UDP, or Both). If you are unsure, leave it as the default (Both).
Public Port	Enter the service port number from the Internet that will be redirected to the previously mentioned Private IP address host in your LAN.
Comment	The description of this setting.
Add	Type in the private IP, private port, type, public port, and comment for the setting to be added, then click on this button. This virtual server setting will be added to the Current Virtual Server table.
Reset	If you make a mistake and have not yet pressed the **Add** button, click on **Reset** and the fields will be cleared.
Delete Selected	If you want to remove some virtual server settings from the Current Virtual Server table, select them, then click on this button.
Delete All	If you want remove all virtual server settings from the table, press this button.
Reset	Clears the current selections.

NOTE

You need to give your LAN PC clients a fixed/static IP address for the virtual server to work properly.

NOTE

The virtual server function will have priority over the DMZ function if there is a conflict between the virtual server and the DMZ settings.

Once you've entered the parameters listed in Table 5-28 in the screen shown in the top half of Figure 5-30, click on **Add** to add a new virtual server. You can now configure other advanced sections or start using the router (with the advanced settings in place).

Figure 5-31 demonstrates one of the ways you can use the virtual server function. Use the virtual server when you want the Web server located in your private LAN to be accessible to Internet users. The configuration in the bottom half of Figure 5-30 means that any request coming from the Internet to access your Web server will be translated to your LAN's Web server (192.168.2.2).

NOTE

For the virtual server to work properly, Internet/remote users must know your global IP address. (For Web sites, you will need to have a fixed/static global/public IP address.)

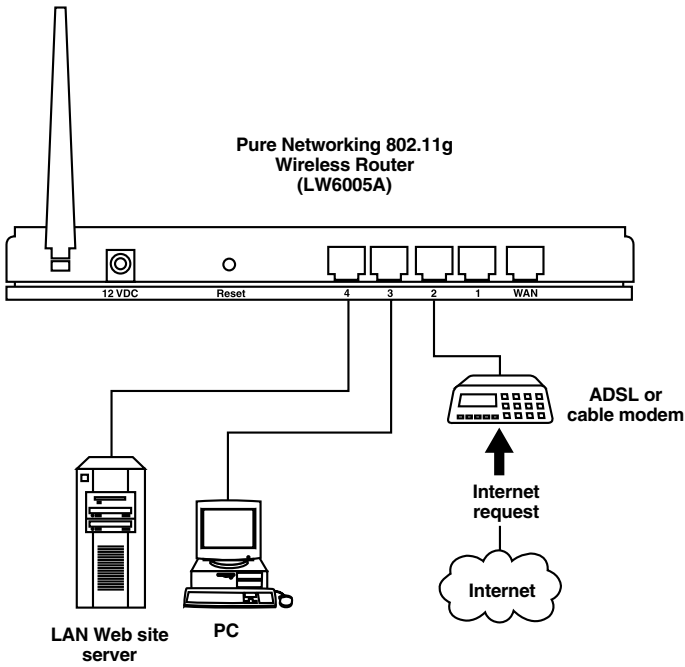


Figure 5-31. Maintain security while allowing limited access to specified servers.

5.5.3 Special Applications

Some applications (such as Internet games, videoconferencing, and Internet telephony) require multiple connections. In this section, you can configure the router to support multiple connections for these types of applications.

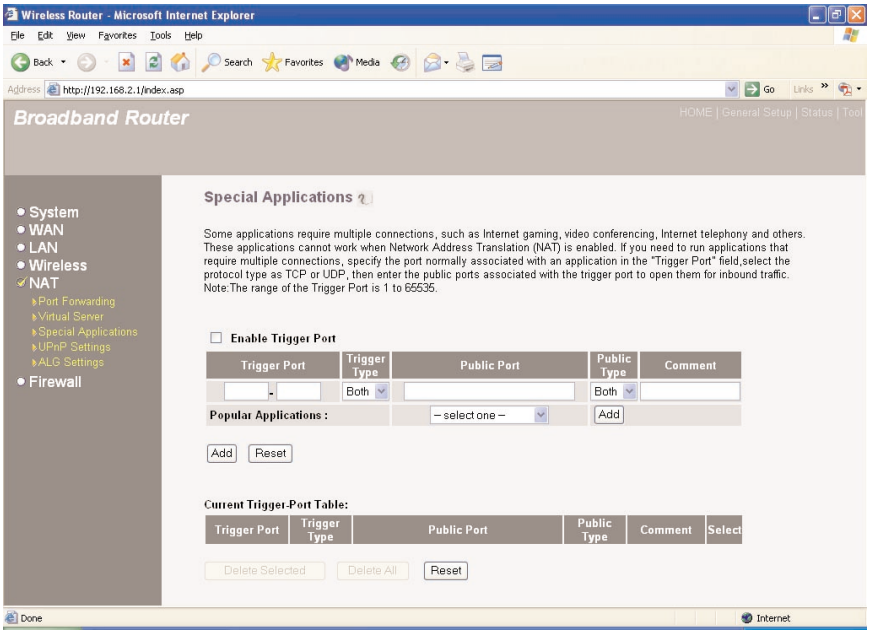


Figure 5-32. Special Applications screen.

Table 5-29 lists the router's special applications options.

Table 5-29. Special Applications parameters.

Parameters	Description
Enable Trigger Port	Check this box to enable the special application function.
Trigger Port	This is the outgoing (outbound) range of port numbers for this particular application.
Trigger Type	Select whether the outbound port protocol is TCP, UDP, or Both.

NOTE

Individual port numbers are separated by a comma (for example, 47624, 5775, 6541, etc.). Type in a port range, and use a dash to separate the port number range (for example, 2300–2400).

Table 5-29 (continued). Special Applications parameters.

Parameters	Description
Public Port	Enter the incoming (inbound) port or port range for this type of application (for example, 2300–2400, 47624).
Public Type	Select the inbound port protocol type: TCP, UDP, or Both.
Add button	Click on this button to add the port described in the top half of the screen shown in Figure 5-32.
Comment	The description of this setting.
Popular Applications	This section lists the more popular applications that require multiple connections. Select an application from the popular applications section. Once you have selected an application, select a location (1–10) in the drop-down selection box, then click on the **Add** button. This will automatically list the public ports required for this popular application in the location (1–10) you'd specified.
Add button	Fill in the trigger port, trigger type, public port, public type, and comment of the setting to be added. Click on this button. This special application setting will be added to the Current Trigger Port Table. If you want to add a popular application, select it and click on **Add**.
Reset button	If you make a mistake before pressing the **Add** button, click **Reset** to clear the fields.
Delete Selected	If you want to remove some special application settings from the Current Trigger Port Table, select them and click on this button.

Table 5-29 (continued). Special Applications parameters.

Parameters	Description
Delete All	If you want to remove all special application settings from the table, press this button.
Reset	Clears your current selections.

Click on the **Add** button to save the configuration described in the top half of Figure 5-32. You can now configure other advanced sections or start using the router (with the advanced settings in place).

A special applications example is shown below.

Suppose you need to run applications that require multiple connections. Specify the port (outbound) normally associated with that application in the Trigger Port field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Table 5-30. Special applications example.

ID	Trigger Port	Trigger Type	Public Port	Public Type	Application Name
1	28800	UDP	2300–2400, 47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In Table 3-30, when a user triggers port 28800 (outbound) for MSN Game Zone, the router will allow incoming packets for ports 2300–2400 and 47624 to be directed to that user.

NOTE

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

5.5.4 UPnP Settings

Selecting UPnP (see Figure 5-33) enables plug-and-play operation.

With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices—all automatically when you plug in the device.

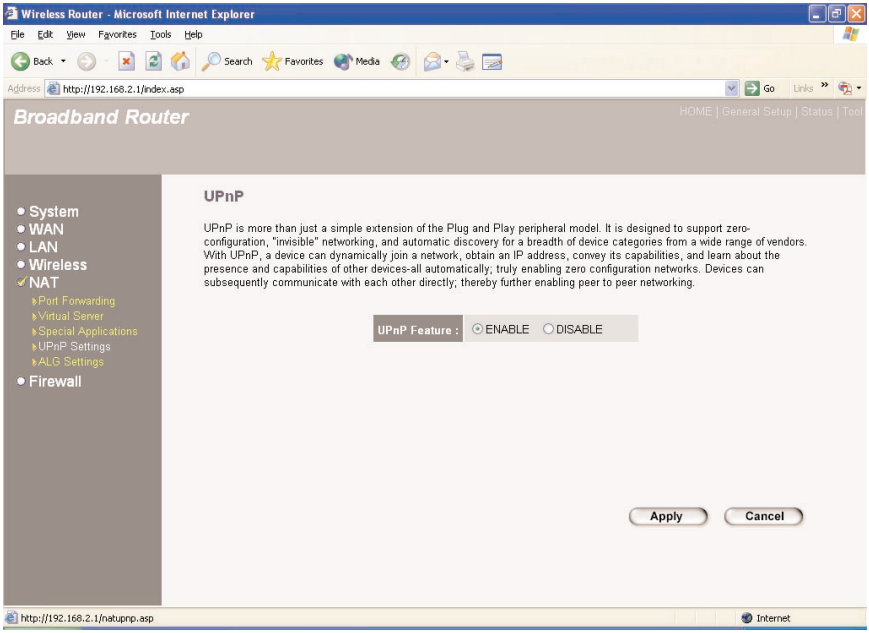


Figure 5-33. UPnP screen.

Table 5-31 lists the UPnP options for automatic configuration.

Table 5-31. UPnP parameters.

Parameters	Description
Enable	Check this box to enable the UPnP function.
Disable	Check this box to disable the UPnP function.

Table 5-31 (continued). UPnP parameters.

Parameters	Description
Apply	Click on this button to save your changes.
Cancel	Click on this button to cancel your changes.

Click on the **Apply** button at the bottom of the screen to save the above configurations. The router will pop up on the network for configuring.

5.5.5 ALG Settings

Select applications for gateways operating at the ISO's Application layer. Table 5-32 tells you how to enable or disable Application Layer Gateway (ALG). From the NAT settings screen (Figure 5-28), select ALG. Figure 5-34 appears.

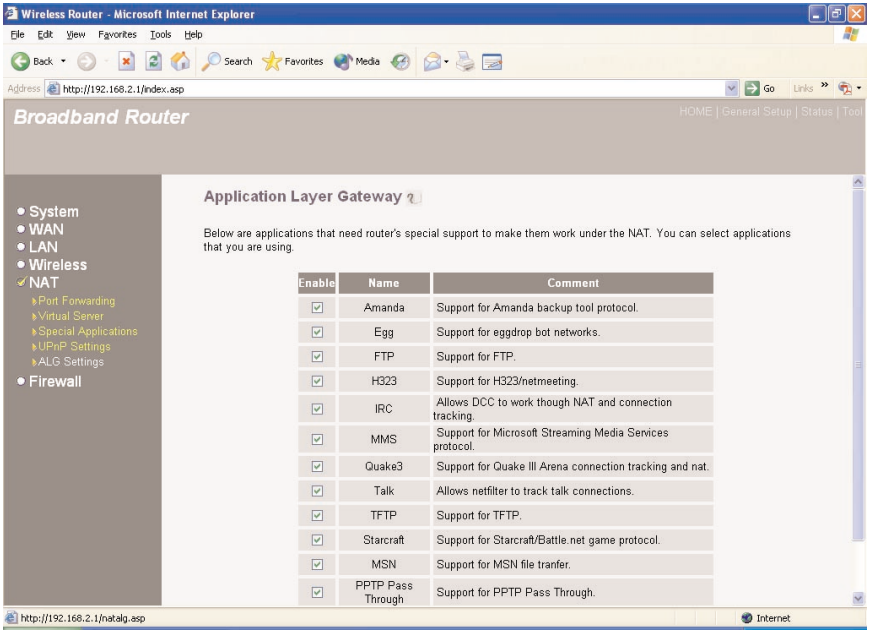


Figure 5-34. ALG screen.

Table 5-32 lists the router's ALG parameters. These are used to configure the router at the OSI's Application layer. Typical applications include FTP servers and IP phones.

Table 5-32. ALG parameters.

Parameters	Description
Enable	Check this box to enable Application Layer Gateway. The router will then let that application correctly pass though the NAT gateway.
Name	This is the supported application's name.
Comment	Type in a description for each supported application.
Apply button	Scroll down to see this button, then click on it to save the changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.6 Firewall

The router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ). From the security screen (Figure 5-21), click on **Firewall**. The screen shown in Figure 5-35 appears.

NOTE

To enable the firewall settings, select Enable and click on Apply.

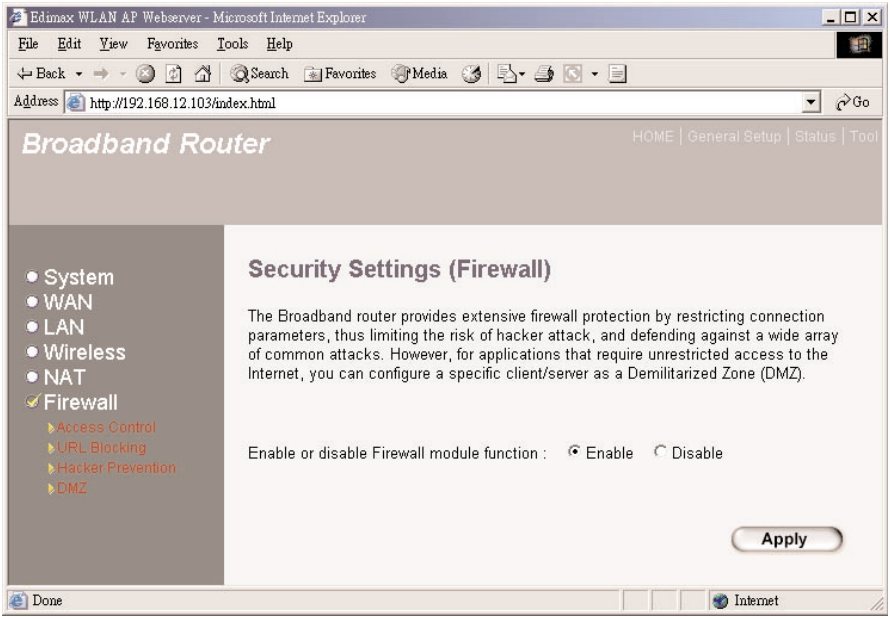


Figure 5-35. Firewall settings screen.

Table 5-33 lists the firewall menu options (not visible in Figure 5-35, but on your screen they will appear under the Firewall entry on the left side of the Security Settings [Firewall] screen [Figure 5-35]). Select a menu option, then click on **Enable** or **Disable**. Click on **Apply** to go to the selected sub-screen.

Table 5-33. Firewall options.

Parameters	Description
Access Control	Access control allows you to specify which host's users can or cannot have access to certain Internet applications.
URL Blocking	URL blocking allow you to specify which URLs can't be accessed by users.
Denial of Service (DoS)	The router's firewall can block common hacker attacks and log the attack activities.

Table 5-33 (continued). Firewall options.

Parameters	Description
DMZ	The DMZ function allows you to redirect all packets going to your WAN port IP address to a particular IP address in your LAN.

Click on one of the firewall selections (listed on the left side of the Firewall Settings screen) and proceed to the manual's relevant sub-section (**5.6.1**, **5.6.2**, **5.6.3**, or **5.6.4**). The firewall selections are not visible in Figure 5-35, but will appear on your screen when you are using the software.

5.6.1 Access Control

If you want to restrict users from accessing certain Internet applications/services (for example, Internet Web sites, email, FTP, etc.), then this is the place to set that configuration. Access control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services. From the Firewall Settings screen (see Figure 5-35), click on **Access Control**. This is the first option under Firewall in the Firewall Settings screen. Figure 5-36 appears.

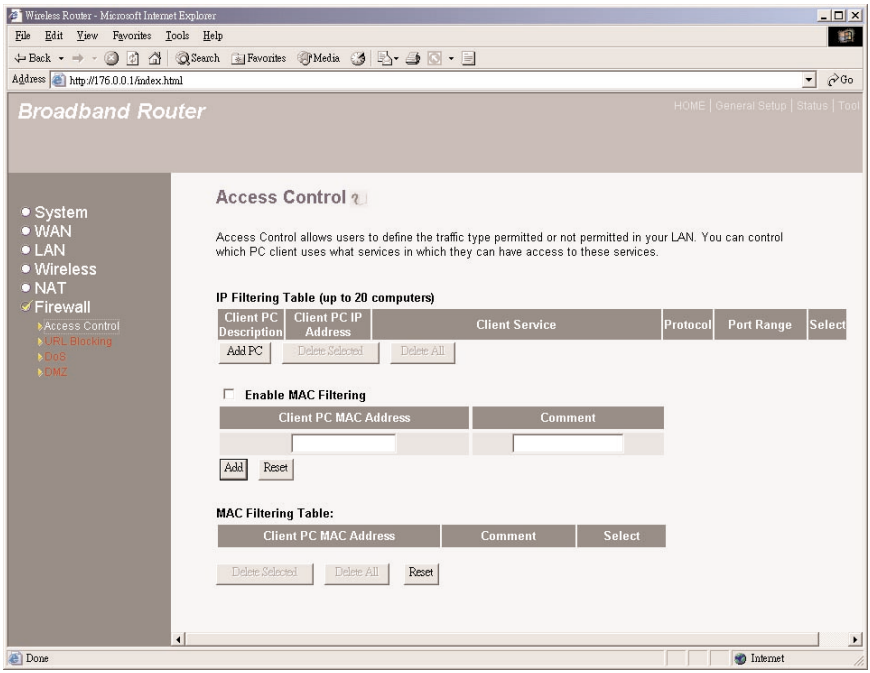


Figure 5-36. Access Control screen.

Table 5-34 lists the router's access control options.

Table 5-34. Access Control parameters.

Parameters	Description
Add PC	Click on this button to add an access control rule (this will restrict user access) via IP addresses.
Delete Selected	If you want to remove a PC from the IP Filtering Table, select the PC you want to remove, then click on this button.
Delete All	If you want to remove all PCs from the table, click on this button.
Enable MAC Filtering	Check this box to activate MAC filtering.
Add	Fill in the Client PC MAC Address and Comment fields to designate the PC that's allowed to access the Internet, then click on this button.
Reset button	If you make a mistake and haven't pressed **Add** yet, click on this button to clear the fields.
Deleted Selected	If you want to remove a PC from the MAC Filtering Table, select the PC and click on this button.
Delete All	If you want to remove all PCs from the table, click on this button.
Reset button	If you want to clear the selection and reselect again, click on this button.

You can now configure other advanced sections or start using the router (with the advanced settings in place).

Add PC screen

To get to the Add PC screen, from the Security Settings Firewall screen (see Figure 5-35), click on the **Access Control** option in the menu on the left of the screen. Figure 5-36 will appear. Then press the **Add PC** button and Figure 5-37 will appear.

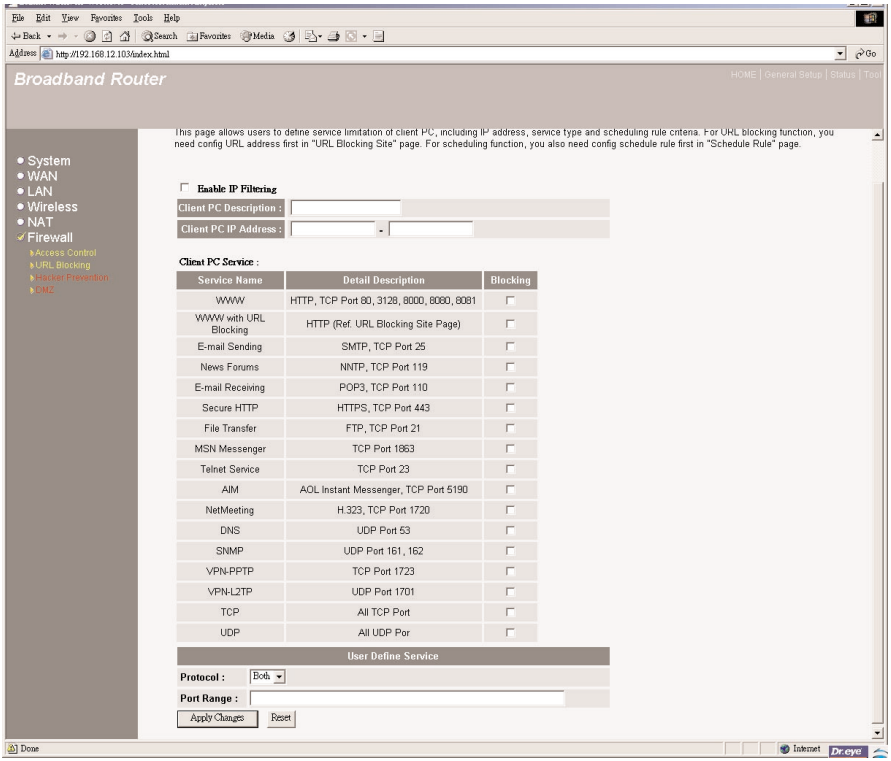


Figure 5-37. Add PC screen.

Table 5-35 lists the Add PC screen's options.

Table 5-35. Add PC parameters.

Parameters	Description
Enable IP Filtering	Check this box to activate IP filtering.
Client PC Description	The client PC's configured access rules. (Access rules restrict user access to Web sites via IP addresses.)
Client PC IP Address	The access control rule will allow/deny the PC's access to Internet Web sites.You can select a range of users simply by typing in the starting user's IP address and the last user's IP address in the appropriate boxes. If you want to select only one user, then type in the user's IP address in both boxes.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select UDP, TCP, or both protocol types that you want to block.
Port Range	Assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Apply Changes	Click on this button to save the settings.
Reset	Click on this button to clear all fields.

NOTE

You need to give your LAN PC clients a fixed/static IP address so that the access control rule will allow/deny the PC's access to Internet Web sites accurately.

Click on **Apply Changes** at the bottom of the screen to save the above configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place).

An example of access control is shown below. LAN client A can only access Web sites that use Port 80. However, LAN client B is able to access Web sites and any other service that uses ports between 80 and 999. See Figure 5-38.

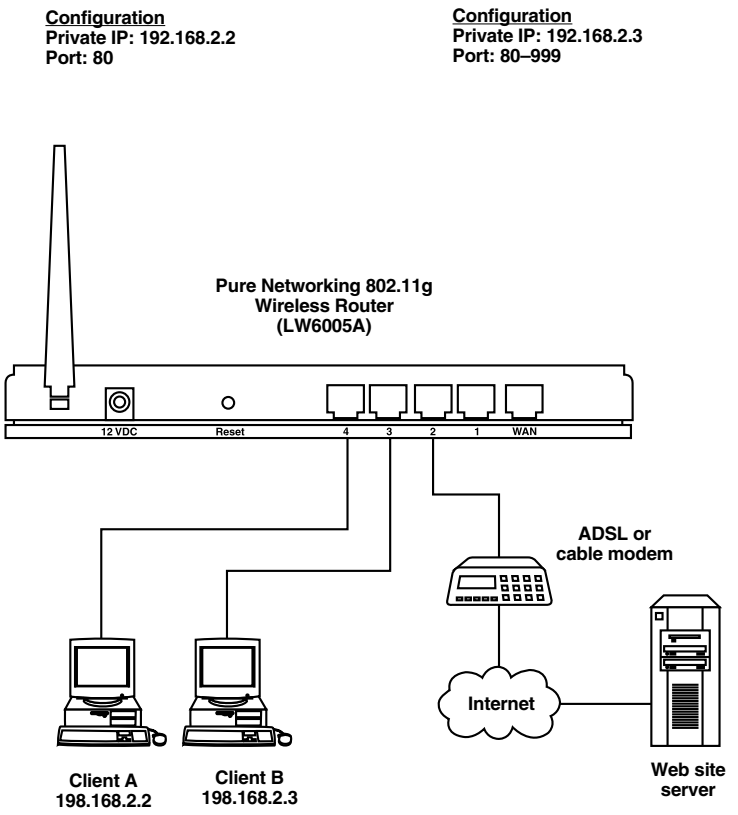


Figure 5-38. Each workstation's access to ports on the Web is controlled by the router's access control configuration.

5.6.2 URL Blocking

You can block access to some Web sites from particular PCs by entering a full URL address or just a keyword of the Web site.

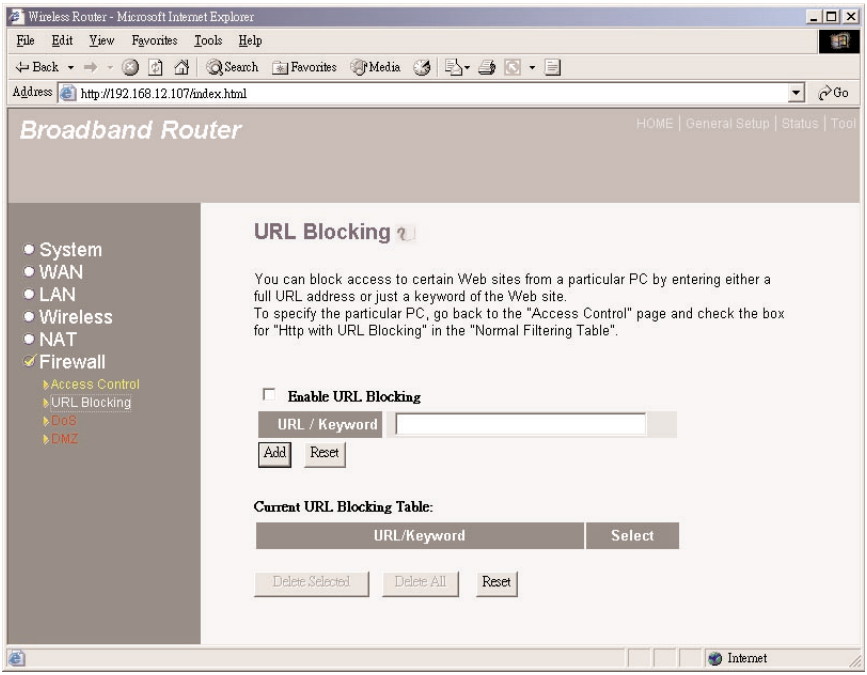


Figure 5-39. URL blocking screen.

Table 5-36 describes the URL blocking options.

Table 5-36. URL blocking parameters.

Parameters	Description
Enable URL Blocking	Check this box to enable/disable URL blocking.
Add button	Type in the URL/Keyword, then click on this button. You can enter the full URL address or the keyword of the Web site you want to block.
Reset button	If you make a typing mistake before pressing the **Add** button and want to retype it properly, click on this button. The field will be cleared.

Table 5-36 (continued). URL blocking parameters.

Parameters	Description
Delete Selected	If you want to remove a URL keyword from the Current URL Blocking Table, select the URL keyword, then click on this button.
Delete All	If you want remove all URL keywords from the table, click on this button.
Reset button	If you want to clear the selection and reselect again, click on this button.

You can now configure other advanced sections or start using the router (with the advanced settings in place).

5.6.3 Denial of Service (DoS)

The router's firewall can block common hacker attacks including denial of service, ping of death, port scan, and sync flood. If Internet attacks occur, the router can log the events. See Figure 5-40.

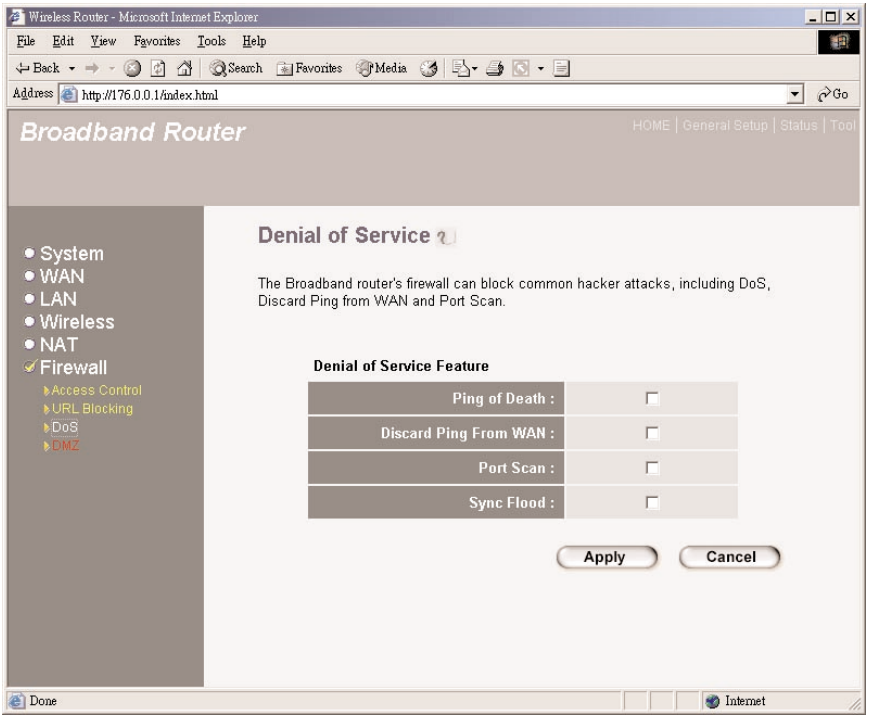


Figure 5-40. Denial of Service screen.

Table 5-37 describes options for DoS, which is one type of intrusion detection.

Table 5-37. Denial of Service parameters.

Parameters Denial of Service (DoS) Feature	Description
Ping of Death	Protects from Ping of Death attack.
Discard Ping From WAN	The router's WAN port will not respond to any ping requests.
Port Scan	Protects the router from Port Scan.
Sync Flood	Protects the router from Sync Flood attack.

Table 5-37 (continued). Denial of Service parameters.

Parameters	Description
Apply	Click on this button to save your changes.
Cancel	Click on this button to cancel your changes.

Click on **Apply** at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the router (with the advanced settings in place).

5.6.4 DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall (for example, Games), then you can open the client up to unrestricted two-way Internet access by defining a DMZ host (see Figure 5-41). The DMZ function allows you to redirect all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server redirects a particular service/Internet application (for example, FTP, Web sites) to a particular LAN client/server, whereas DMZ redirects all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

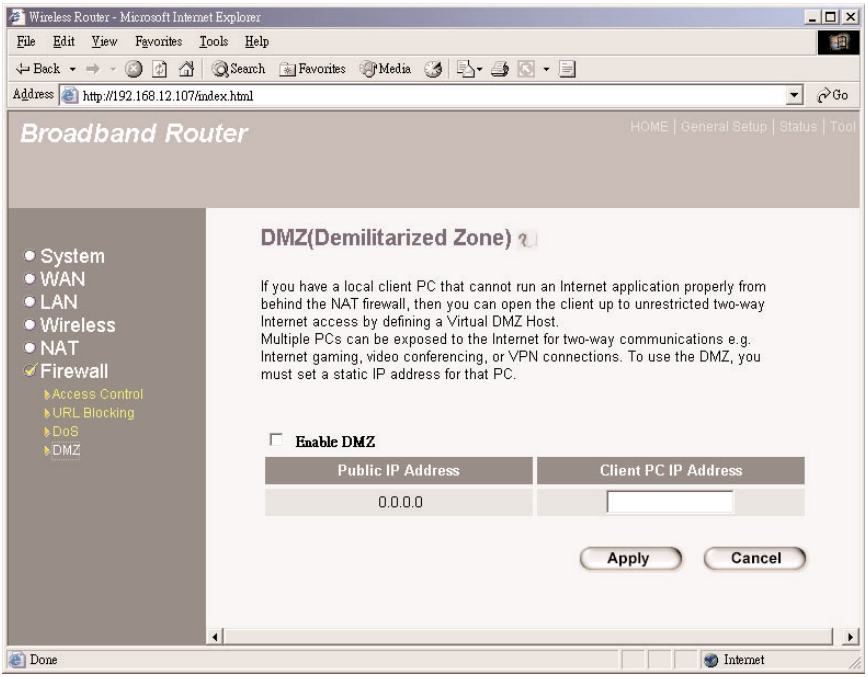


Figure 5-41. DMZ screen.

NOTE

If there is a conflict between the virtual server and the DMZ setting, the virtual server function will have priority over the DMZ function.

Table 5-38 explains the DMZ options.

Table 5-38. DMZ parameters.

Parameters	Description
Enable DMZ	Check this box to enable/disable DMZ.
Public IP Address	The WAN port's IP address or any other public IP addresses given to you by your ISP.

Table 5-38 (continued). DMZ parameters.

Parameters	Description
Client PC IP Address	Type in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/public IP address above.
Apply	Click on this button to save your changes.
Cancel	Click on this button to cancel your changes.

NOTE

You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

You can now configure other advanced sections or start using the router (with the advanced settings in place).

6. Status Information

The Status section allows you to monitor the current status of your router. You can use the Status screen to monitor the connection status of the router's WAN/LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

Table 6-1. Status parameters.

Parameters	Description
Status and Information	Shows the router's system information.
Internet Connection	View the router's current Internet connection status and other related information.
Device Status	View the router's current setting status.
Security Log	View any attempts that have been made to illegally gain access to your network.
Active DHCP Client Table	View your LAN client's information that is currently linked to the router's DHCP server.
Statistics	Shows the statistics.

Select one of the above six Status selections and proceed to the manual's relevant sub-section (**Section 6.1**, **6.2**, **6.3**, **6.4**, **6.5**, or **6.6**).

6.1 Status and Information

The status and information section (see Figure 6-1) allows you to view the router's system information.

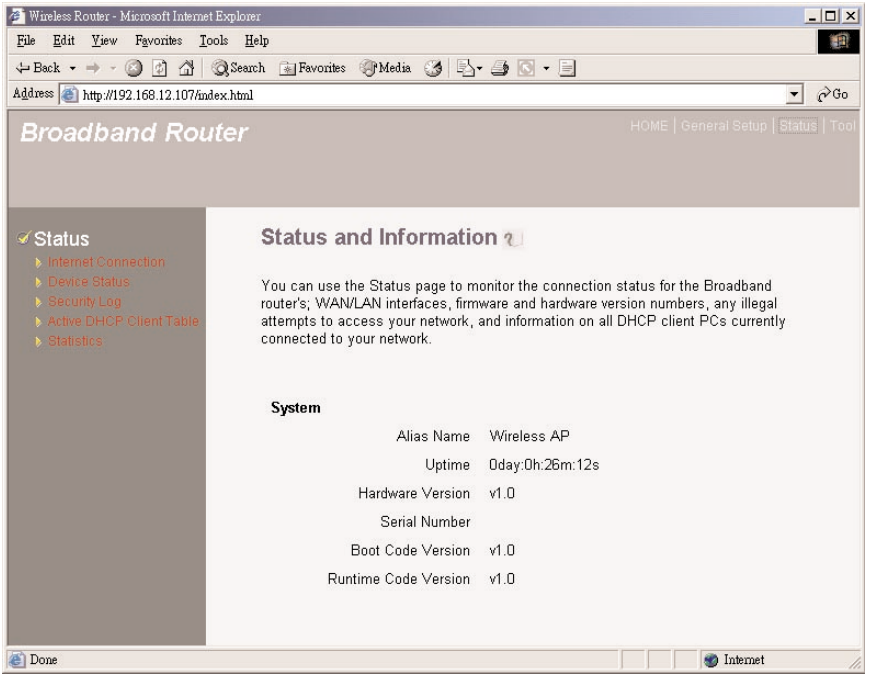


Figure 6-1. Status and information screen.

Table 6-2 lists the system information displayed in Figure 6-1.

Table 6-2. Status and information parameters.

Parameters	Description
Information	You can see the router's system information such as the alias name, uptime, hardware version, serial number, boot code version, and runtime code version.

6.2 Internet Connection

View the router's current Internet connection status and other related information. See Figure 6-2.

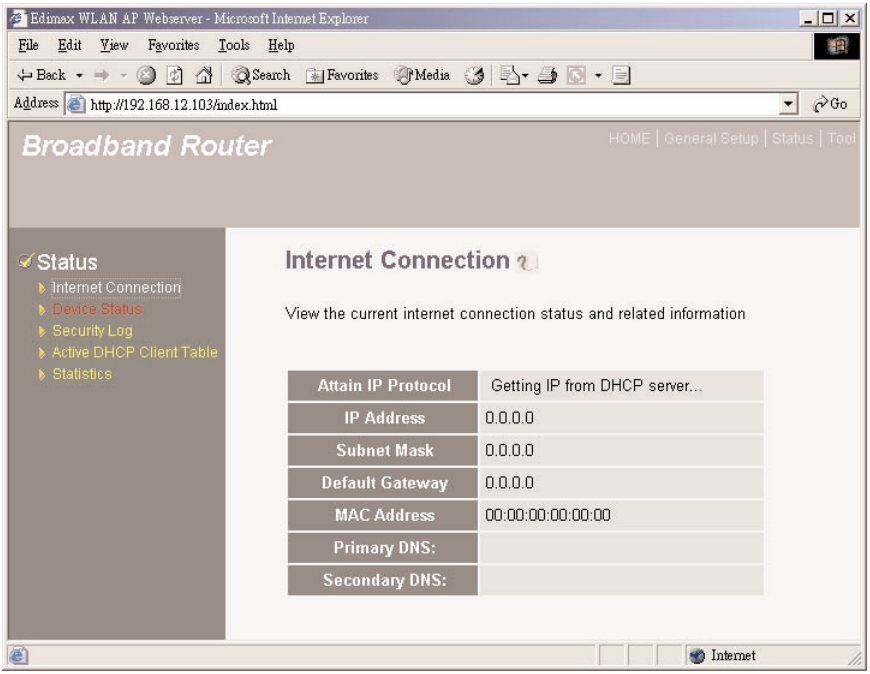


Figure 6-2. Internet connection screen.

Table 6-3 lists the options you can view in Figure 6-2.

Table 6-3. Internet connection parameters.

Parameter	Description
Internet Connection	This page displays how the router gets its IP protocol (Attain IP Protocol). It also displays the router's IP address, subnet mask, default gateway, and MAC address, as well as the primary DNS and secondary DNS being used.

6.3 Device Status

View the router's current configuration settings (see Figure 6-3). The Device Status screen displays the configuration settings you've configured in the Quick Setup Wizard/General Setup section.

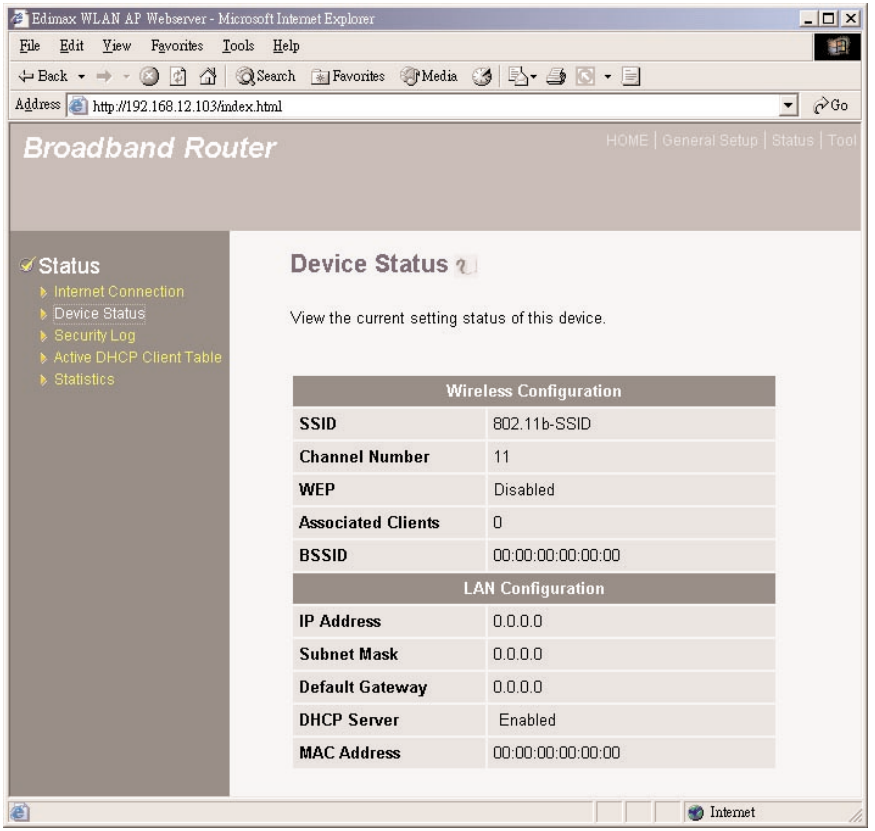


Figure 6-3. Device status screen.

Table 6-4 lists the device status options displayed in Figure 6-3.

Table 6-4. Device status parameters.

Parameters	Description
Device Status	This page shows the router's current device settings. It displays the router LAN port's current LAN IP address and subnet mask, as well as the default gateway. It also shows whether the DHCP server is enabled/disabled and lists the MAC address. For the wireless configuration, the screen displays values for SSID, channel number, WEP, associated clients, and BSSID.

6.4 Security Log

View any attempts that have been made to illegally gain access to your network. See Figure 6-4.

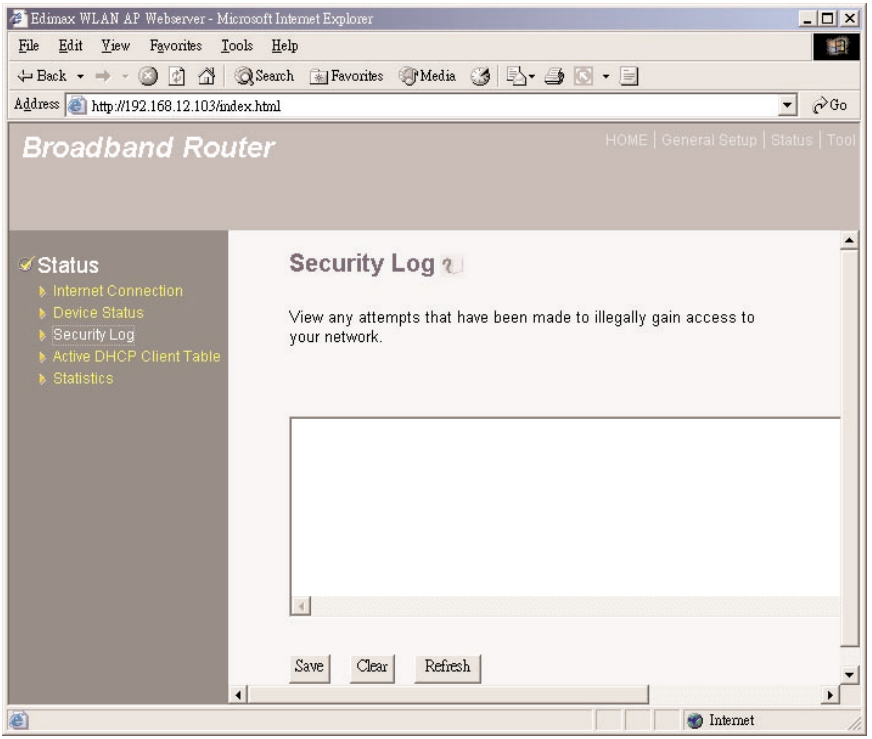


Figure 6-4. Security log screen.

Table 6-5 describes the security log options.

Table 6-5. Security log parameters.

Parameters	Description
Security Log	This page shows the router's current security log. It displays any illegal attempts to access your network. At the bottom of the page, click on **Save** to save the security log to a local file for further processing. Press **Clear** to clear the security log. Press **Refresh** to refresh the screen to get the most updated situation. When the system is powered down, the security log will disappear if it's not saved to a local file.

6.5 Active DHCP Client Table

View your LAN client's information that is currently linked to the router's DHCP server. See Figure 6-5.

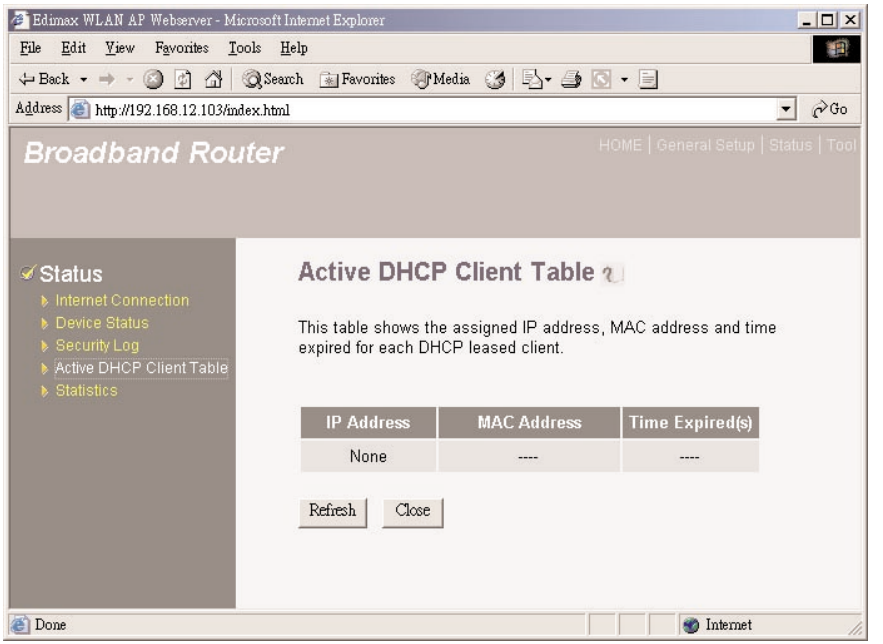


Figure 6-5. Active DHCP client table screen.

Table 6-6 describes the DHCP options shown in Figure 6-5.

Table 6-6. Active DHCP client table parameters.

Parameters	Description
Active DHCP Client Table	This screen shows all DHCP clients (LAN PCs) currently connected to your network. The Active DHCP Client Table displays the IP address, the MAC address, and the time expired for each LAN client.
Refresh	Use this button to get the most updated information.
Close	Closes this screen.

6.6 Statistics

View the statistics of packets sent and received on WAN, LAN, and wireless LAN. See Figure 6-6.

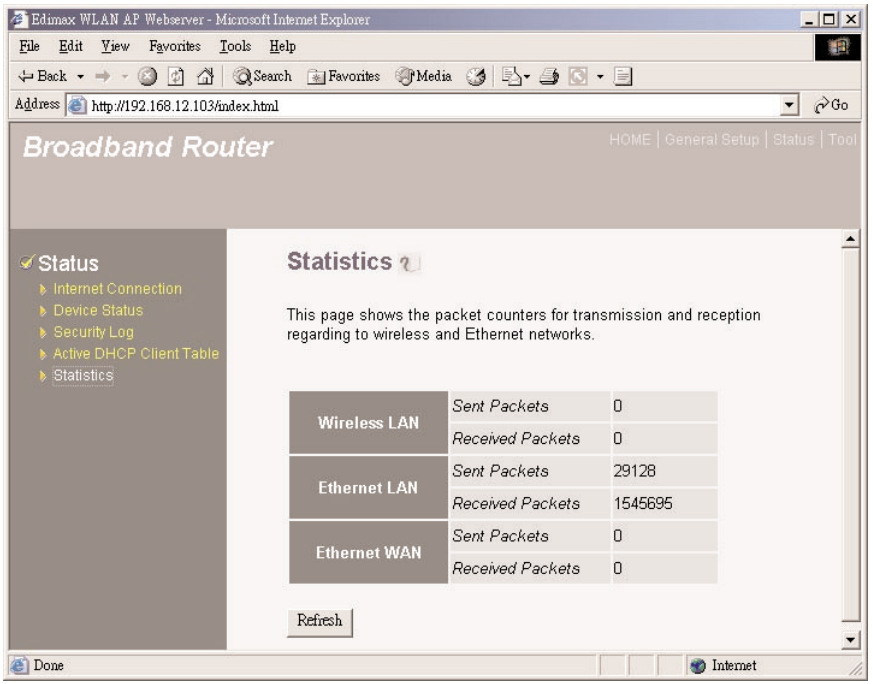


Figure 6-6. Statistics screen.

Table 6-7 explains the statistics values shown in Figure 6-6.

Table 6-7. Statistics parameters.

Parameter	Description
Statistics	Shows the number of packets sent and received on WAN, LAN, and wireless LAN.
Refresh	Click on this button to refresh the screen.

7. Tools

The Tools screen includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware), and Reset. See Figure 7-1.

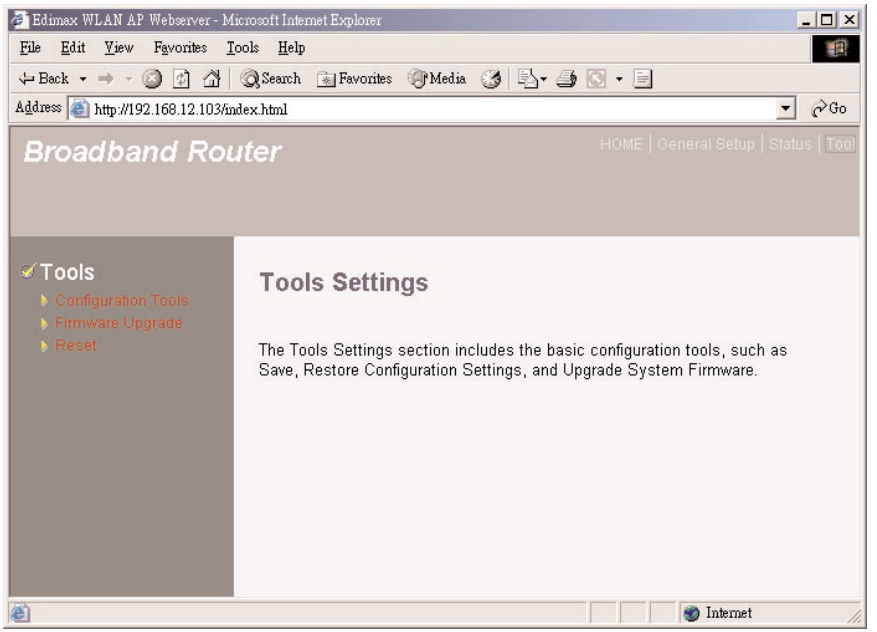


Figure 7-1. Tools screen.

Table 7-1 lists the available Tools options.

Table 7-1. Tools screen parameters.

Parameters	Description
Configuration Tools	You can save the router's current configuration, restore the router's saved configuration files, and restore the router's factory-default settings
Firmware Upgrade	This page allows you to upgrade the router's firmware.
Reset	You can reset the router's system if any problem exists.

Select one of the three Tools settings and proceed to the relevant text (**Section 7.1**, **7.2**, or **7.3**).

7.1 Configuration Tools

The Configuration Tools screen (see Figure 7-2) allows you to save (backup) the router's current configuration setting. Saving the configuration settings provides an added protection and convenience if problems occur with the router and you have to reset it to factory default. When you save the configuration setting, you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur, you can use the Restore to Factory Default selection; this will set all configurations to the original default settings (for example, when you first purchased the router).

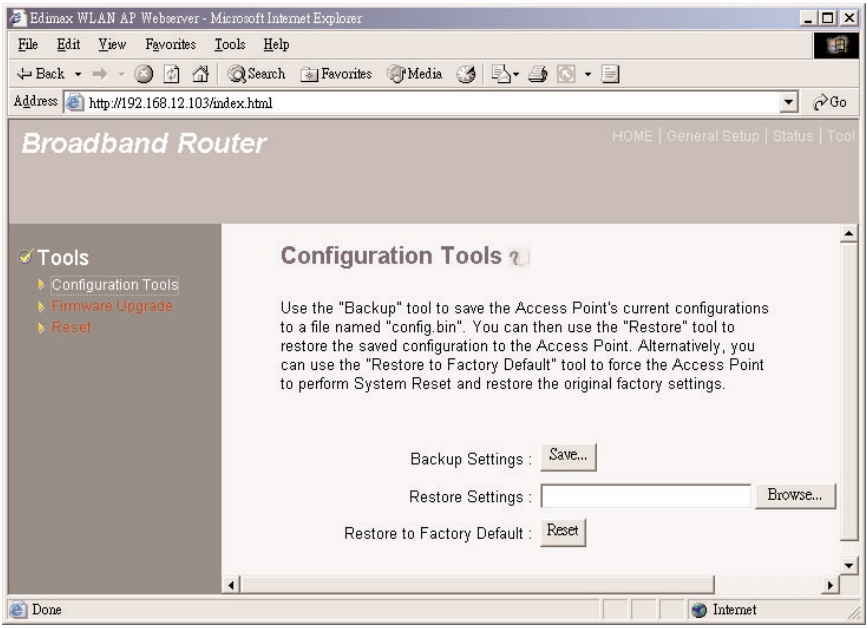


Figure 7-2. Configuration Tools screen.

Table 7-2 describes the options shown in Figure 7-2.

Table 7-2. Configuration Tools parameters.

Parameters	Description
Backup Settings	Use the Backup tool to save the router's current configuration to a file named **config.bin** on your PC.
Save	Click on this button to save your changes.
Restore Settings	Use the Restore tool to restore the saved configuration to the router.
Browse	Use this button to browse through existing settings.
Restore to Factory Default	Use this tool to force the router to perform a power reset and restore the original factory settings.
Reset	Click on this button to clear the changes.

7.2 Firmware Upgrade

This screen allows you to upgrade the router's firmware. See Figure 7-3.

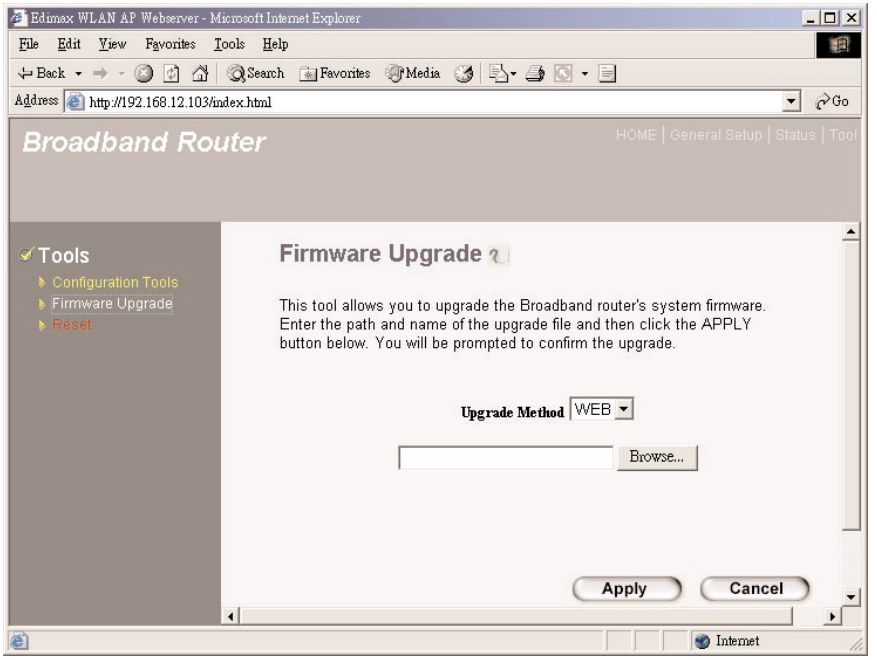


Figure 7-3. Firmware upgrade screen.

Table 7-3 describes the options shown in Figure 7-3.

Table 7-3. Firmware upgrade parameters.

Parameters	Description
Upgrade Method	This tool allows you to upgrade the router's system firmware. To upgrade your router's firmware, download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page.
Browse button	Use this button to find the firmware file on your PC.

Table 7-3 (continued). Firmware upgrade parameters.

Parameters	Description
Apply	Click on this button to save your changes.
Cancel	Click on this button to cancel your changes.

Once you've selected the new firmware file, click on the **Apply** button to start the upgrade process. (You may have to wait a few minutes for the upgrade to finish.) Once the upgrade is complete, you can start using the router.

7.3 Reset

If the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. The reset function (see Figure 7-4) essentially reboots your router's system.

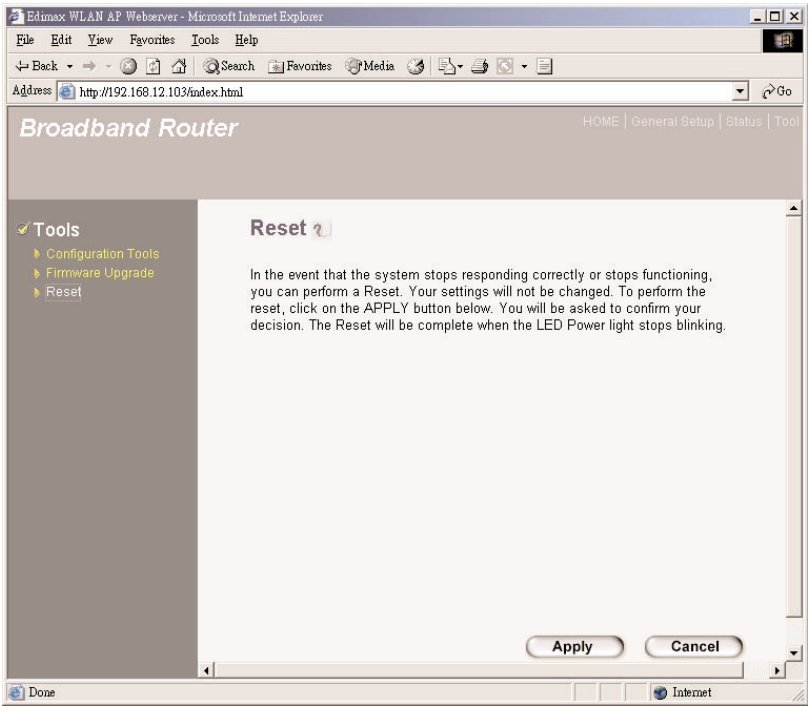


Figure 7-4. Reset screen.

Table 7-4 describes the buttons in the router's Reset screen.

Table 7-4. Reset parameters.

Parameters	Description
Apply	To perform the reset, click on this button. You will be asked to confirm your decision. The reset is finished when the power light stops blinking. Once the reset process is complete, you may start using the router again.
Cancel	To cancel the reset, click on this button.

8. Troubleshooting

8.1 Calling Black Box

If you determine that your Pure Networking 802.11g Wireless Router is malfunctioning, do not attempt to alter or repair the unit. It contains no user-serviceable parts. Contact Black Box at 724-746-5500.

Before you do, make a record of the history of the problem. We will be able to provide more efficient and accurate assistance if you have a complete description, including:

- the nature and duration of the problem.
- when the problem occurs.
- the components involved in the problem.
- any particular application that, when used, appears to create the problem or make it worse.

8.2 Shipping and Packaging

If you need to transport or ship your Pure Networking 802.11g Wireless Router:

- Package it carefully. We recommend that you use the original container.
- If you are shipping the router for repair, make sure you include everything that came in the original package. Before you ship, contact Black Box to get a Return Authorization (RA) number.

Appendix. How to Manually Find Your PC's IP and MAC Address

1. In Windows, open the Command Prompt program. See Figure A-1.

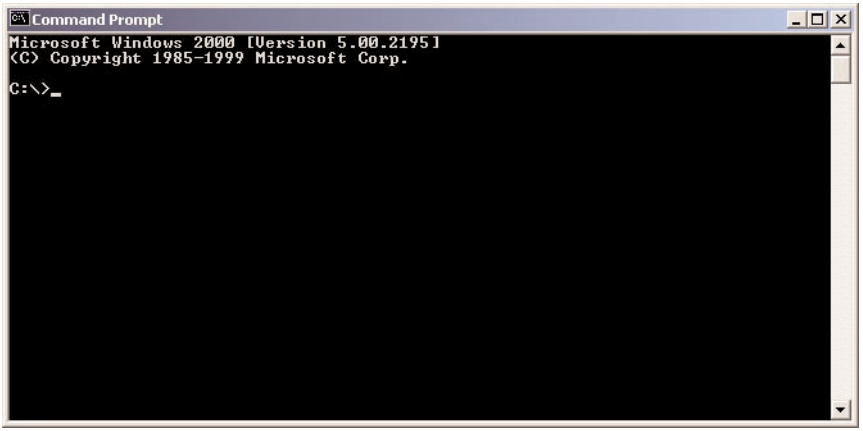


Figure A-1. Command prompt screen.

2. Type `Ipconfig /all` and press **Enter**. Figure A-2 will appear.

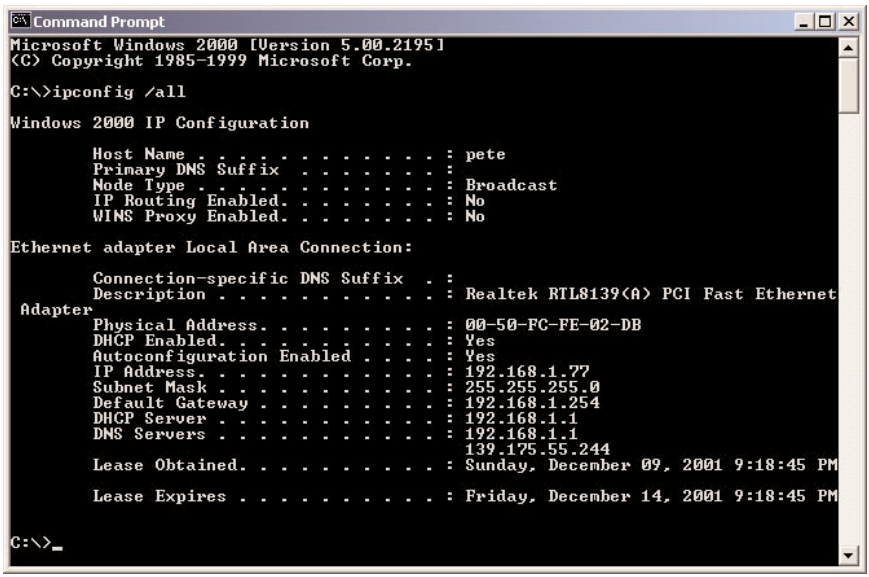


Figure A-2. Configuration screen.

Your PC's IP address is the one entitled IP Address (192.168.1.77).

The router's IP address is the one entitled Default Gateway (192.168.1.254).

Your PC's MAC address is the one entitled Physical Address (00-50-FC-FE-02-DB).

Glossary

Bridge: A bridge is an intelligent internetworking device that forwards or filters packets between different networks based on Data Link layer (MAC) address information.

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. This allows Internet servers to have a domain name (such as *www.router.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 (for example, typing `router.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 they move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle timeout is designed so that after there's 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 that identifies a single, unique Internet computer host in an IP network (for example, 192.168.2.1). It consists of two portions: the IP network address and the host ID.

The IP address is a 32-bit binary pattern that can be represented as four cascaded decimal numbers separated by a period. For example, aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by a period: bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern. It consists of consecutive leading 1's followed by consecutive trailing 0's (for example, 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, then 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: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

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

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 correspond 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 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
pcANYWHERE®	TCP	5631
pcANYWHERE	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dialup 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 (for example, 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 protocols. 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 (for example, different buildings, cities, or 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 Netscape Navigator or Microsoft® Internet Explorer to control, configure, or monitor the device being managed.