# Setting up filters

The *Advanced (Filter)* page lets you set a variety of overall Internet Access Policies for your entire network or specific policies for selected computers on your network.

Each policy you establish can deny or allow access (to the Internet or to inbound traffic) to the network clients (computers) you specify. You can also allow or deny this access based on the time of day, day of the week, service type, domain name, or a keyword you designate.

## To establish Internet Access Policies:

1 Open your Internet browser and go to the Gateway Wireless Router Setup utility. For more information, see "Contacting the router" on page 17.

2 Click **Advanced** on the left side of the window. The *Advanced (Data)* page opens.

3 Click the **Filter** tab at the top of the page to open the *Advanced (Filters)* page.
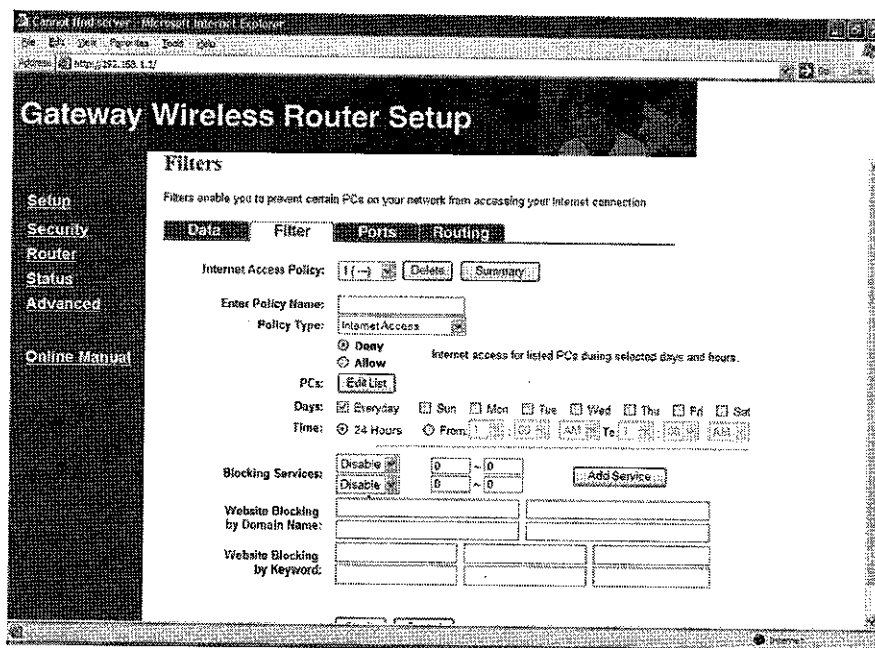


4 Click the arrow to open the **Internet Access Policy** list, then click a policy number (1 to 10).

5 In the **Enter Policy Name** field, type a unique, alphanumeric name.

**6** Click the arrow to open the **Policy Type** list, then click one of the following:

- **Internet Access** - to control access to the Internet by computers on your network

- **Inbound Traffic** - to control access to your internal network by computers outside your network.

**7** Click to select the **Deny** check box (to deny access to specific computers during the times and days specified).

- OR -

Click to select the **Allow** check box (to give access to specific computers during the times and days specified).

**8** Click **Edit List**. A *List of PCs* or *List of Internet PCs* page opens (depending on the Policy Type selected).

**a** Enter the MAC addresses, the IP addresses, or the Range of IP addresses of the computers which are affected by this policy.

**b** Click **Apply** to save your changes

-OR-

Click **Cancel** to remove your entries.

**c** Click **Close** to return to the *Advanced (Filters)* page.

**9** Click to select the **Days** you want to control access for.

**10** Click to select either **24 Hours** or **From** (requires you to enter a time interval). If you selected From, click the arrows to open the time lists, then click the time.

**11** If you selected the Internet Access policy type, click the arrow to open the **Blocking Services** list, then click the type of services you want blocked. If you click a service to block, the type of service and port range appear in the **Blocking Services** boxes. To add or edit a service, do the following:

**a** Click **Add Service**. The *Add Services* window opens.
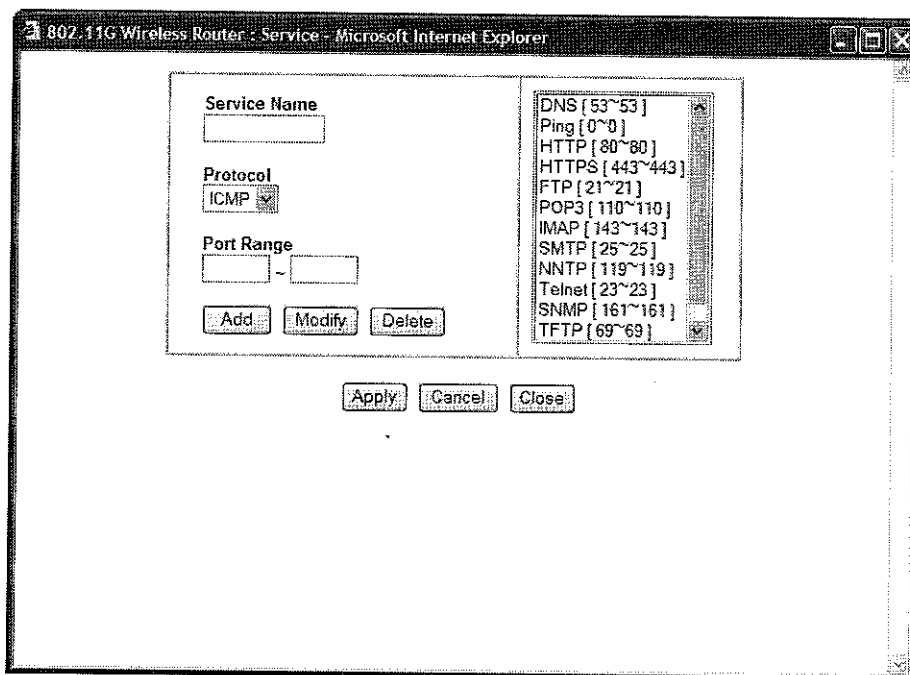


**b** To add a new service, type the name of the service in the **Service Name** box, click the arrow to open the **Protocol** list, then click the Protocol Type in the range of ports for the service in the **Port Range** boxes. Click **Add** when you finish. The service is added to the list.

**c** To modify a service and port range, click the service on the list at the right of the window. Click the arrow to open the **Protocol** list, then click a new protocol, or change the port ranges in the **Port Range** boxes. Click **Modify.** The service parameters change.

**d** To delete a service, select the service from the list at the right of the window, then click **Delete.** The service is removed from the list.

**e** To remove your entries or your changes, click **Cancel.**

**f** When you are finished, click **Close** to return to the *Advanced (Filters)* page.

**12** If you selected the Internet Access policy type, type the URL addresses (as many as four) in the **Website Blocking by Domain Name** boxes for any Web sites that you want to permanently block access to.

**13** If you selected the Internet Access policy type, type the URL addresses (as many as six) in the **Website Blocking by Keyword** boxes for any Web sites that you want to permanently block access to.

**14** To create additional policies, repeat Step 4 through Step 13 (blocked services and Web sites remain blocked at all times).

**15** To delete an access policy, click the arrow to open the **Internet Access Policy** list, then click the policy number. Click the **Delete** button.

**16** For a summary of all access policies in effect, and a description of each policy, click **Summary** to open the *Internet Policy Summary* window.

**17** When you are finished making changes, click **Apply** to save your changes.

-OR-

Click **Cancel** to return the router's filter settings to the defaults.

# Setting up port forwarding

The *Advanced (Ports)* page lets you set up a variety of public services on your network. These services can include Web servers, ftp servers, mail servers, and other, more specialized functions such as gaming or video conferencing.

Up to ten customized applications can be configured to allow access to specific ports on individual computers. Applications can be set up and enabled immediately, or set up and enabled as needed.

| Important | To facilitate port forwarding to a computer, the DHCP client function must be disabled on the computer and a static IP address assigned (see "Setting a static IP address" on page 55). |
|---|---|

## To set up customized applications:

1 Open your Internet browser and go to the Gateway Wireless Router Setup utility. For more information, see "Contacting the router" on page 17.)

2 Click **Advanced** on the left side of the window. The *Advanced (Data)* page opens.

3 Click the **Ports** tab at the top of the page to open the *Advanced (Ports)* page.
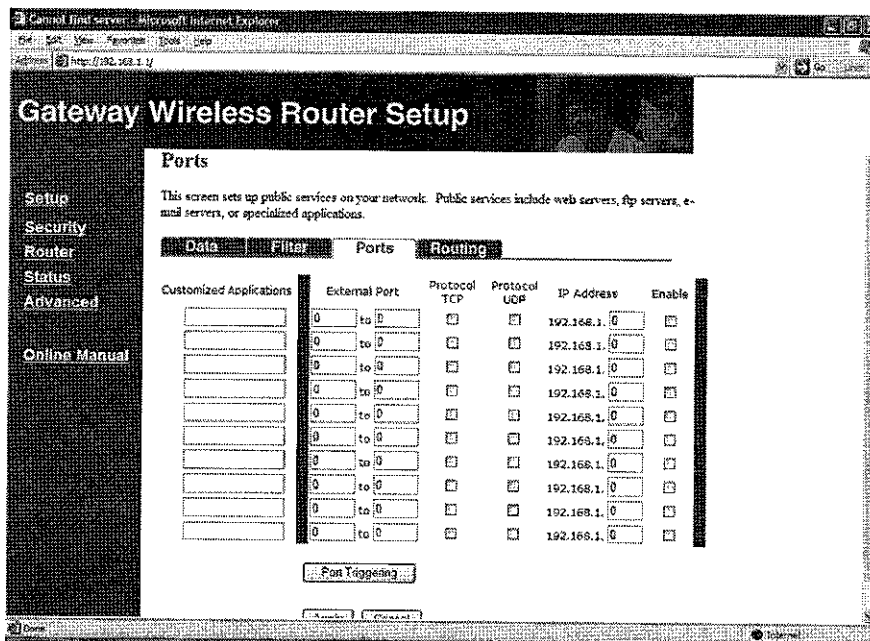


4 In the first available **Customized Applications** box, type the name of the service or application you are setting up.

5 On the same line, in the **External Port** boxes, type the port range that the service uses.

6 On the same line, click to select a check box under the **Protocol** required by the application.

■ **TCP** - Transmission Control Protocol (allows data streaming)

■ **UDP** - User Datagram Protocol (used primarily for broadcasting messages over a network)

**7** On the same line, enter the static **IP Address** of the computer that runs the application or provides the service.

**8** On the same line, click to select the **Enable** check box to turn on access to the application or service.

**9** For special applications where the computer sends data out from a different port than it receives data from, click **Port Triggering** to set up the router to monitor outgoing data for specific port numbers so the router can direct the requested incoming data to the same computer. The *Port Trigger List* window opens.



**a** On the first available line, type the Application Name in the **Application Name** box.

**b** On the same line, under **Trigger Port Range**, type the outgoing port range used by the application or service.

**c** On the same line, under **Incoming Port Range**, type the incoming port range used by the application or service.

**d** Click **Apply** to save your entries.

-OR-

Click **Cancel** to delete your entries.

**e** Click **Close** to close the window and return to the *Advanced (Ports)* page.

**10** To set up additional services or applications, repeat Step 4 through Step 9 (blocked services and Web sites remain blocked at all times).

**11** When you are finished making changes, click **Apply** to save your changes.

-OR-

Click **Cancel** to delete your entries.

# Setting up the routing mode

The *Advanced (Routing)* page lets you set the operating mode and configuration of the router.

If the router is used to host your network's connection to the Internet, you should set it to **Gateway** mode. If your router is part of a network with other routers, you should set it to **Router** mode.

## To set the routing mode:

**1** Open your Internet browser and go to the Gateway Wireless Router Setup utility. For more information, see "Contacting the router" on page 17.)

**2** Click **Advanced** on the left side of the window. The *Advanced (Data)* page opens.

**3** Click the **Routing** tab at the top of the page to open the *Advanced (Routing)* page.
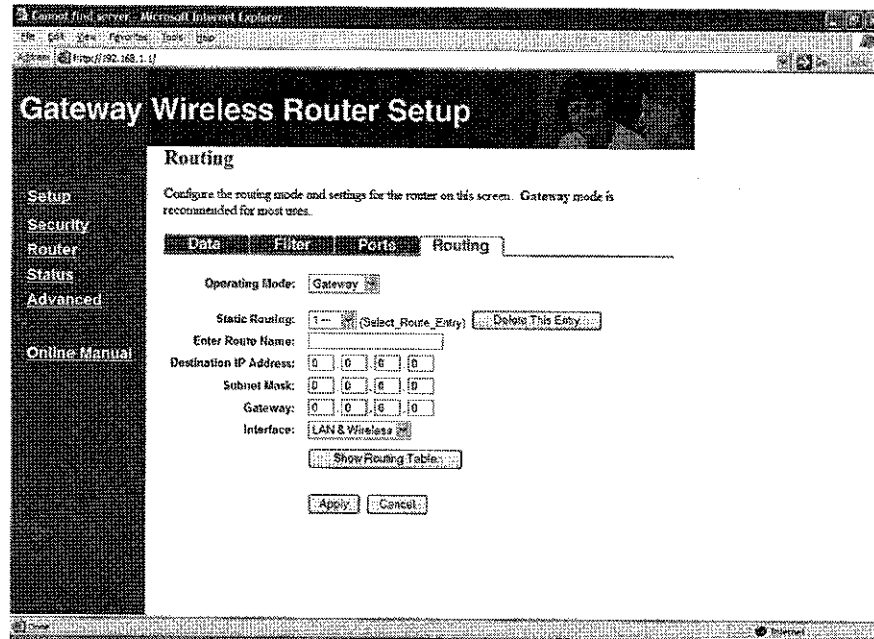


**4** Click the arrow to open the **Operating Mode** list, then click **Gateway** or **Router.**

■ **Gateway** - If the router is used to host your network's connection to the Internet

■ **Router** - If your router is part of a network with other routers

**5** If you selected Router mode and you want to use dynamic routing, click the arrow to open the **Dynamic Routing (RIP)** list, then click **Enable.**

Dynamic routing lets your router automatically adjust to changes in your network's layout and exchange routing tables with other routers on your network.

**6** When you are finished making changes, click **Apply** to save your changes

-OR-

Click **Cancel** to delete your entries.

# Setting up static routes

The *Advanced (Routing)* page also lets you set up static routes (preset pathways) between your router and other specific hosts or networks.
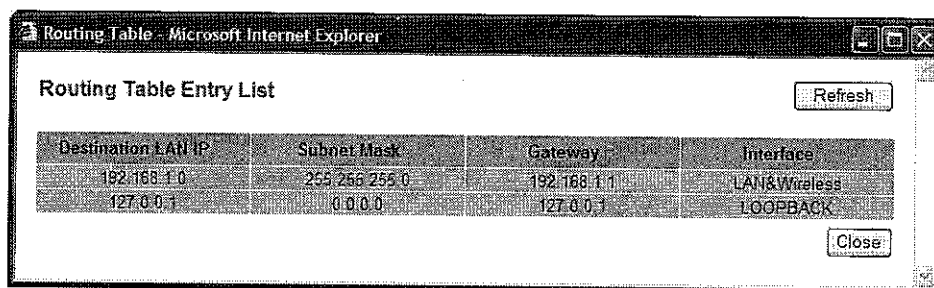
### To set up a static route:

1 Open your Internet browser and go to the Gateway Wireless Router Setup utility. For more information, see "Contacting the router" on page 17.)

2 Click the **Advanced** heading on the left side of the window. The *Advanced (Data)* page opens.

3 Click the **Routing** tab at the top of the page to open the *Advanced (Routing)* page.

4 Click the arrow to open the **Static Routing** list, then click a route number.

5 Type a descriptive name in the **Enter Route Name** box.

6 Type the IP address of the network or host to which the static route is directed in the **Destination IP Address** box.

7 Type the subnet mask of the network or host to which the static route is directed in the **Subnet Mask** box.

8 Type the IP address of the gateway device permitting contact with the network or host to which the static route is directed in the **Gateway** box.

9 Click the arrow to open the **Interface** list, then click **LAN & Wireless** or **Internet**, depending on where the destination IP address is located.

10 Click **Show Routing Table** to see a table that shows all of the valid static routes in use by the router. The *Routing Table Entry List* window opens and shows the Destination LAN IP, the Subnet Mask, the Gateway, and the Interface type on all established static routes.

| Destination LAN IP | Subnet Mask | Gateway | Interface |
|---|---|---|---|
| 192.168.1.0 | 255.255.255.0 | 192.168.1.1 | LAN&Wireless |
| 127.0.0.1 | 0.0.0.0 | 127.0.0.1 | LOOPBACK |

11 To set up additional static routes, repeat Step 3 through Step 9.

**12** To delete an active static route from the router, click the arrow to open the **Static Routing** list, click the static route you want to delete, then click **Delete This Entry**. The settings for that static route are deleted.

**13** When you are finished making changes, click **Apply** to save your changes.

-OR-

Click **Cancel** to delete your current entries.

# Chapter 6

## Troubleshooting

- Ping utility
- Setting a static IP address
- Problem resolution
- Contact information

# Ping utility

You can use the ping utility to help determine whether a connection has been established on a network or to determine a numerical IP address (xxx.xxx.xxx.xxx) based on an alphanumeric Internet or Web address such as www.gateway.com.

Also, your router may have difficulty sending and receiving e-mail or connecting to the Internet if your ISP's mail and server addresses are configured with single words, such as *mail*, *home*, or *pop3*. The router has no way to resolve these abbreviated addresses to the actual IP and Web addresses required for connection. The ping utility can help you find out the required addresses.

## To use the ping utility to obtain an IP address:

1 Turn on your computer, the router, and the DSL or cable modem.

2 Click **Start**, then click **Run**. Type **command** in the *Open* box, then click **OK**.

3 At the command prompt, type **ping** followed by the single word or verbal address you want resolved (for example **ping mail**), then press **ENTER**.

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1998-2001.

C:\DOCUME~2\DEFAULT>ping mail

Pinging mail.adelphia.net [64.8.50.100] with 32 bytes of data:

Reply from 64.8.50.100: bytes=32 time=157ms TTL=53
Reply from 64.8.50.100: bytes=32 time=149ms TTL=53
Reply from 64.8.50.100: bytes=32 time=147ms TTL=53
Reply from 64.8.50.100: bytes=32 time=146ms TTL=53

Ping statistics for 64.8.50.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 146ms, Maximum = 157ms, Average = 149ms

C:\DOCUME~2\DEFAULT>_
```

4 The ping utility returns the actual IP address of the *mail* server (in this case 64.8.50.100). Write down this number.

This number works as the IP address of your ISP's e-mail server. Unfortunately, this number may change at some point, so it may be necessary to further resolve the number to determine the actual Web address of the server (which will not change).

In the above example, note the line that states **Pinging mail.adelphia.net [64.8.50.100] with 32 bytes of data**. In this case **mail.adelphia.net** is the actual Web address of the mail server and does not need to be resolved. Write down this Web address and use it to replace your ISP's one word mail server address (in your Web browser or e-mail program).

However, if the ping utility returned only the IP address, you will need to determine the Web address.

## To resolve an IP address:

1 With the ping utility still active, type **ping -a 64.8.50.100**, (64.8.50.100 is the IP address returned from pinging *mail*), then press ENTER.

2 The ping utility returns several lines of information, including one that states **Pinging mail.adelphia.net [64.8.50.100] with 32 bytes of data**. In this case **mail.adelphia.net** is the actual Web address of the mail server. Write down this Web address and use it to replace your ISP's one word mail server address (in your Web browser or e-mail program).

# Setting a static IP address

Typically, the computers on your network are to obtain an IP address dynamically (using the DHCP server function of the router) whenever they contact your local network. However, in certain cases, such as DMZ hosting or port forwarding, you are required to assign a static IP address to a computer so that it's address remains constant and it can be contacted at the same address over time.

## To set a static IP address using Windows XP:

1 Click **Start**, then **Control Panel**. If your Control Panel is in Category View, click **Network and Internet Connections**.

2 Click/Double-click **Network Connections**.

3 Right-click the **Local Area Connection** that is associated with your network adapter card, then click **Properties**.

4 In the **This connection uses the following items list**, click **Internet Protocol (TCP/IP)**, then click **Properties**.

5 In the **IP Address** box, type a unique IP address that will not be used by any other computer on your network. You can use IP addresses between 192.168.1.2 and 192.168.1.99 (IP address 192.168.1.1 is assigned to the router and the router's DHCP server assigns addresses from 192.168.1.100 up to 192.168.1.254).

6 In the **Subnet Mask** box, type 255.255.255.0.

7 In the **Default Gateway** box, type 192.168.1.1.

**8** At the bottom of the window, click **Use the following DNS server addresses** and type the **Preferred DNS Server and Alternative DNS Server** (contact your ISP if you do not have this information).

**9** Click **OK** to close the *Internet Protocol (TCP/IP) Properties* window.

**10** Click **OK** to close the *Local Area Connection Properties* window.

## To set a static IP address using Windows 2000:

**1** Click **Start, Settings**, then click **Control Panel.**

**2** Double-click **Network and Dial-Up Connections,** right-click the **Local Area Connection** that is associated with your network adapter card, then click **Properties.**

**3** In the **Components checked are used by this connection** list, click **Internet Protocol (TCP/IP),** then click **Properties.**

**4** Click **Use the following IP address.**

**5** In the **IP Address** box, type a unique IP address that will not be used by any other computer on your network. You can use IP addresses between 192.168.1.2 and 192.168.1.99 (IP address 192.168.1.1 is assigned to the router and the router's DHCP server assigns addresses from 192.168.1.100 up to 192.168.1.254).

**6** In the **Subnet Mask** box, type 255.255.255.0.

**7** In the **Default Gateway** box, type 192.168.1.1.

**8** At the bottom of the window, click **Use the following DNS server addresses,** then type the **Preferred DNS Server** and **Alternative DNS Server** (contact your ISP if you do not have this information).

**9** Click **OK** to close the *Internet Protocol (TCP/IP) Properties* window.

**10** Click **OK** to close the *Local Area Connection Properties* window. If you are prompted, restart your computer.

## To set a static IP address using Windows 98SE and Windows Me:

**1** Click **Start, Settings**, then click **Control Panel.** The *Control Panel* window opens.

**2** Double-click the **Network** icon. The *Network* window opens.

**3** In **The following network components are installed** list, click the TCP/IP line associated with your computer's network adapter (if there is only one TCP/IP line, click it), then click **Properties.** The *TCP/IP Properties* window for your network adapter opens.

4 Click the **IP Address** tab, then click **Specify an IP address.**

5 In the **IP Address** box, type a unique IP address that will not be used by any other computer on your network. You can use IP addresses between 192.168.1.2 and 192.168.1.99 (IP address 192.168.1.1 is assigned to the router and the router's DHCP server assigns addresses from 192.168.1.100 up to 192.168.1.254).

6 In the **Subnet Mask** box, type 255.255.255.0.

7 Click the **Gateway** tab. In the **New Gateway** box, type 192.168.1.1, then click **Add.**

8 Click the **DNS Configuration** tab, then click **Enable DNS.**

9 Type any **Host** and **Domain** names, then type the DNS IP address provided by your ISP (contact your ISP if you do not have this information).

10 Click **OK** to close the *TCP/IP Properties* window.

11 Click **OK** to close the *Network* window. If you are prompted, restart your computer.

# Problem resolution

## Your wireless router will not turn on (no LEDs)

■ Make sure that the AC adapter is plugged in and connected to the router.

| **Warning** | Use only the power cord and AC adapter provided with the router. Use of an unauthorized power cord or AC adapter may cause damage to your router and void your warranty. |
|---|---|

■ Make sure that the power strip, surge protector, or UPS (uninterruptable power supply) is operating correctly.

## You have forgotten your password

Press the **Reset** button on the back of the router for approximately 10 seconds to reset the router to the defaults, then use the default User Name and Password (admin and admin) to access the Gateway Wireless Router Setup utility. Change the password (see "Establishing a router security scheme" on page 36) and write it down.

## You are having problems connecting to the Internet

**1** Turn off the computer, the router, and the DSL or cable modem.

**2** Turn on the DSL or cable modem and wait several minutes until the modem has established communication with you ISP.

**3** Turn on the router, then turn on the computer.

If you still cannot connect, open the Gateway Wireless Router Setup utility and make sure that the settings are all correct (see "Configuring the router" on page 19). You may need to enter additional information, for example your ISP may require a specific MAC address setting on your router (see "Changing default router settings" on page 32).

## You receive a time-out message when you try to enter a URL or address in your browser

- Check the other computers on your network to see if they have the same problem or if the problem is isolated to one specific computer.

- If the problem is isolated:

  - Make sure that the configuration settings are correct (DHCP setting, IP address, subnet mask, default gateway, and DNS), then restart the computer.

  - If the problem is general:

    - Make sure that the router is on and configured correctly (see "Configuring the router" on page 19).

    - Make sure that the DSL or cable modem is on and operating correctly (check the LEDs on the front to make sure it is receiving power and is not on standby).

    - Check with your ISP for outage or cable problems.

    - Try connecting a single computer to the DSL or cable modem to see if connection is possible.

    - If you are connected to a remote server using a VPN, try disconnecting the VPN.

    - Make sure that your browser is set to connect directly to the Internet and not to use a dial-up connection.

## You cannot access your wireless router

- Make sure that your router is turned on (check the power LED).

- Make sure that the SSIDs (wireless) or workgroup name on both the router and the computer are the same (see "Configuring the router" on page 19, and see the documentation that came with your wireless network card).

- Make sure that the router has the same subnet mask as the computer.

■ If you assigned IP addresses to the computers, make sure that all computers have different IP addresses. For home networks, IP addresses should be 192.168.1.N where N is a number you assign between 100 and 254. The N should be different for all computers on your network.

■ Press and hold the RESET button on the back of the router for 10 seconds to reset the router to the default settings.

## You cannot see the other computers on your network

■ Make sure that all computers are plugged into a powered electrical outlet and turned on.

■ Make sure that all computers on your network have the same workgroup name.

■ Make sure that all computers are using the same subnet mask.

■ If you are using DHCP though the router, make sure that the other computers are set to obtain IP addresses from DHCP.

■ If you assigned IP addresses to the computers, make sure that all computers have different IP addresses. For home networks, IP addresses should be 192.168.N.N where N is a number you assign between 0 and 254. The first N should be the same for all computers on your network and the second N should be different for all computers on your network.

■ If you are operating in wireless mode, make sure that the router and each wireless network adapter have the same settings for Mode, SSID, channel, and encryption type.

■ Check the signal strength of your wireless network. For more information, see "Your wireless Ethernet network is running slower than you expect" on page 59.

## Your wireless Ethernet network is running slower than you expect

■ If your wireless Ethernet network is running slower than you expect, you should check your network signal strength. If you find the signal strength is low, try moving to a new location to increase the signal strength.
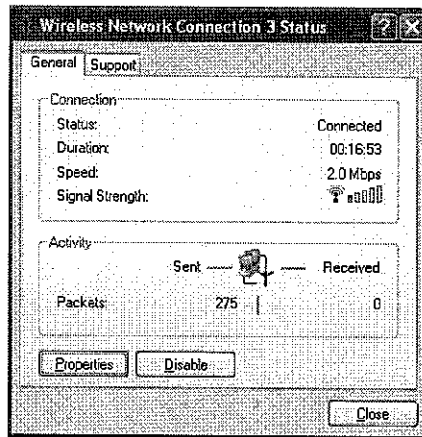
> **Important**
>
> Signal strength is affected by the distance between your wireless network devices, by radio interference, and by interference from natural obstructions such as walls, floors, and doors.

**To check the signal strength of your wireless Ethernet network in Windows XP:**

1 Click **Start**, then click **Control Panel**. The *Control Panel* window opens. If your Control Panel is in Category View, click **Network and Internet Connections**. The *Network and Internet Connections* window opens.

2 Click/Double-click **Network Connections**. The *Network Connections* dialog box opens.

3 Right-click **Wireless Network Connection**, then click **Status**. The *Wireless Network Connection Status* dialog box opens. The meter shows the signal strength for wireless Ethernet networking on your computer if other computers with the same network name are within range of your computer.
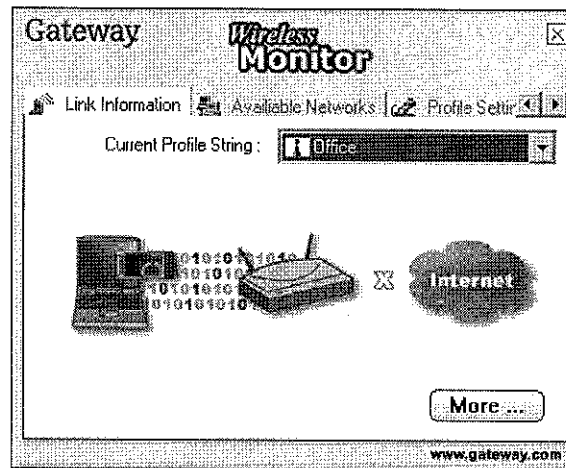


To check the signal strength of your wireless Ethernet network in Windows 2000, Windows Me, or Windows 98SE using the Gateway Wireless Monitor:
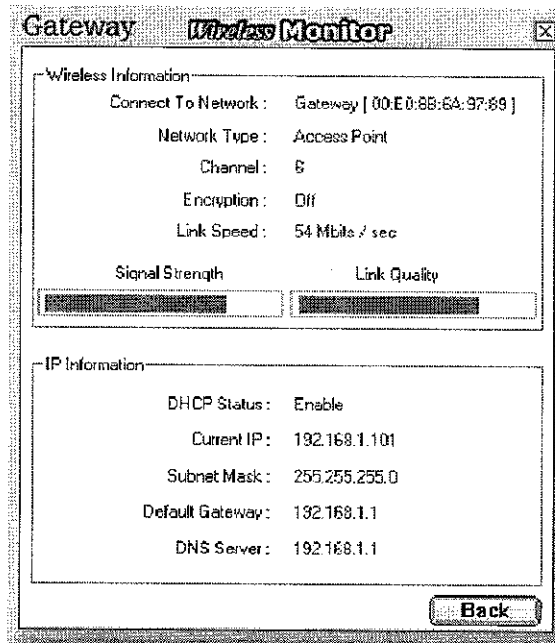
**Important**  If your Windows 2000, Windows Me, or Windows 98SE computer uses a client manager other than the Gateway Wireless Monitor, see the instructions that came with your wireless networking hardware for instructions on checking the signal strength.

**60**

**1** Double-click the Gateway Wireless Monitor icon 🖼 on the taskbar. The Gateway Wireless Monitor program opens.



**2** Click the **Available Networks** tab and make sure that you are connected to the network.

**3** Click the **Link Information** tab.

4 Click **More**. The following screen opens. The meter shows the signal strength for wireless Ethernet networking on your computer if other computers with the same network name are within range of your computer.

```
Gateway    Wireless Monitor                        [X]
┌─Wireless Information───────────────────────────────
         Connect To Network :   Gateway [ 00:E0:8B:6A:97:69 ]
            Network Type :   Access Point
                 Channel :   6
              Encryption :   Off
              Link Speed :   54 Mbits / sec

         Signal Strength              Link Quality
       [▓▓▓▓▓▓▓▓▓▓▓    ]          [▓▓▓▓▓▓▓▓▓▓▓▓▓ ]

┌─IP Information─────────────────────────────────────
             DHCP Status :   Enable
              Current IP :   192.168.1.101
             Subnet Mask :   255.255.255.0
          Default Gateway :   192.168.1.1
              DNS Server :   192.168.1.1

                                      [  Back  ]
```

# Technical Support

Gateway offers a wide range of customer service, technical support, and information services.

## Automated troubleshooting system

| Service description | How to reach |
|---|---|
| Use an automated menu system and your telephone keypad to find answers to common problems. | 800-846-2118 (US)<br>877-709-2945 (Canada) |

## Telephone numbers

You can access the following services through your telephone to get answers to your questions:

| Resource | Service description | How to reach |
|---|---|---|
| Fax on demand support | Order a catalog of documents on common problems, then order documents by document numbers. The documents will be faxed to you. | 800-846-4526 (US)<br>877-709-2951 (Canada) |
| Gateway's fee-based software tutorial service | Get tutorial assistance for software issues billed by the minute. | 800-229-1103 (charged to your credit card)<br>900-555-4695 (charged to your telephone bill) |
| Gateway Technical Support | Talk to a Gateway Technical Support representative about a non-tutorial technical support question.)<br><br>TDD Technical Support (for hearing impaired) is available:<br>Weekdays 6:00 a.m. - 8:00 p.m. Central Time<br>Weekends 6:00 a.m. - 5:00 p.m. Central Time | 800-846-2301 (US)<br>800-846-3609 (Canada and Puerto Rico)<br>605-232-2191 (all other countries)<br><br>800-846-1778 (TDD) |
| Sales, accounting, and warranty | Get information about available systems, pricing, orders, billing statements, warranty service, or other non-technical issues. | 800-846-2000 (US)<br>888-888-2037 (Canada) |

*Chapter 6: Troubleshooting*

# Appendix A

## Glossary

# Terms you should know

**adapter (network)** - A circuit board that plugs into a computer to let the computer connect to a network.

**beacon interval** - A beacon is a periodic broadcast by the router to keep the network synchronized. The interval indicates how often the router broadcasts the beacon.

**broadband** - When multiple signals or channels (such as voice, data, and video) share the bandwidth of a single medium.

**browser** - A program running on a computer which makes it possible to view and interact with the Internet.

**cable modem** - A broadband device that uses a coaxial cable to connect to an ISP to access the Internet.

**CAT 5** - The minimum standard of twisted-pair cable suitable for data transmission over a computer network.

**data packet** - A unit of transmitted data. For more information, see *packet*.

**default gateway** - A routing device that forwards data over a local network.

**DHCP (Dynamic Host Configuration Protocol)** - DHCP lets a router or access point router temporarily assign an IP address to a computer on the network.

**DMZ (demilitarized zone)** - DMZ hosting lets a single computer on your LAN expose all of its ports to the Internet. When you set up DMZ hosting on a computer, you bypass the security provided by a router. Consider *port forwarding* as an alternative to DMZ hosting.

**DNS** - A database that translates and stores domain and host names as IP addresses.

**domain** - A set of IP addresses usually *owned* by a company. For example, in an e-mail address the name of the domain comes after the @ symbol.

**DSL (Digital Subscriber Line)** - A broadband Internet connection that uses an ordinary telephone line to provide a fast, *always on* connection to the Internet.

**DTIM (Delivery Traffic Indication Message)** - A message sent by the router to a wireless network device to indicate when the next broadcast or multicast message will be sent. This parameter is necessary to accommodate devices using power save mode.

**dynamic IP address** - An IP address that is temporarily assigned by a DHCP server. Many ISPs use dynamic IP addresses. When a computer connects the Internet, an ISP provides an IP address. When the computer disconnects from the Internet, the ISP reassigns the dynamic IP address to another computer requesting Internet access.

**dynamic routing** - In dynamic routing, a router is configured to automatically generate routing information and share the information with neighboring routers.

**encryption** - The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have the encryption key (code) associated with the encrypted data. Encryption is especially useful when you are using a wireless network because it prevents outsiders from accessing data. Each computer on a wireless network must use the same encryption code.

**Ethernet** - Ethernet is a common technology used to create computer networks. Wired Ethernet uses cables to link computers, hubs, switches, and routers. Wireless Ethernet uses radio waves to create links.

**firmware** - Firmware is programming that is inserted into programmable read-only memory (programmable ROM), thus becoming a permanent part of a computing device. Firmware cannot be modified by a user. Updating firmware requires a special program usually provided by the hardware manufacturer.

**fragmentation** - The process of breaking data into small segments for transmitting. When the segments are received, the data is defragmented and returned to its original format.

**FTP (File Transfer Protocol)** - A simple method of transferring files from one computer to another.

**Gateway** - A system that joins two networks together.

**hardware** - Physical equipment as opposed to software. A router is a hardware device.

**HTTP (HyperText Transport Protocol)** - A system that lets Web browsers and Web servers communicate.

**hub** - A hardware device that joins multiple computers to create a network.

**IP address** - A number that uniquely identifies a computer on the network.

**IPSec (Internet Protocol Security)** - A standard method for providing data confidentiality, integrity, and the authentication between participating hosts.

**ISP (Internet service provider)** - A company that provides access to the Internet. Most ISPs also provide e-mail addresses.

**LAN (local area network)** - A LAN uses network hardware, such as network adapters, hubs, cables, and wireless devices, to link multiple computers for sharing resources, such as files, printers, and an Internet connection.

**MAC (Media Access Control) Address** - A unique number assigned to networking hardware, such as routers, hubs, and network interface cards by the manufacturer.

**Mbps (MegaBits Per Second)** - Transfer speed of 1 million bits per second.

**network** - Two or more computers linked together for the purpose of sharing resources, such as files, printers, or an Internet connection. Routers are often used to link the device, especially if the network includes more than two computers.

**packet** - A unit of transmitted data. When a server sends information, such as e-mail messages and files, through the Internet, the server divides the information into *packets* that contains identifying information called *headers* and *footers*. The system receiving the information uses the headers and footers to reassemble the information.

**passphrase** - Similar to a password, a passphrase is a sequence of characters used by the router to create encryption keys.

**ping (Packet INternet Groper)** - A network utility that determines if a remote device, such as a server, can be reached on the network. For more information, see "Ping utility" on page 54.

**plug-and-play** - If a device is a *plug-and-play* device, a computer can automatically detect and configure the device and install the appropriate software called a device driver.

**port** - A computer program using TCP/IP sends information to another computer through a *port*. Ports are assigned numbers that come after a standard IP address. Many programs hide these port numbers to reduce the complexity of TCP/IP.

**port forwarding** - Port forwarding, unlike DMZ hosting, lets a single computer on your LAN expose only one of its ports to the Internet. This type of port exposure has more security than DMZ hosting.

**PPPoE (Point-to-Point Protocol over Ethernet)** - A communications protocol that combines the Ethernet and Point-to-Point Protocol (PPP) standards. PPPoE is sometimes used with broadband modems.

**PPTP (Point-to-Point Tunneling Protocol)** - A protocol that lets a private network connect securely to another private network through private *tunnels* over the public Internet. This kind of interconnection is known as a virtual private network (VPN).

**protocol** - A set of communication rules. When two computers or networks use the same protocol, they can communicate with each other.

**RIP (Routing Information Protocol)** - A protocol used by a router to maintain routing tables of configuration information to filter incoming and outgoing traffic based on the IP addresses of the senders and receivers.

**RJ-45** - RJ-45 jacks connect a computer to a router. In a wired network, one end of a network cable is plugged into the RJ45 jack on a computer. The other end of the cable is plugged into an RJ45 jack on a router. Data is passed to and from the computer and router through the RJ45 jacks.

**router** - A hardware device that connects devices in a network. A router can also provide Internet access to the networked devices.

**RTS (Request To Send)** - A signal sent by a receiving device, like a router, that tells the sending device to begin transmission.

**server** - A computer that provides shared network service to a network. For example, a server can provide file and printer sharing between networked computers.

**SSID (Service Set IDentifier)** - In a wireless network, the SSID identifies a network. All computers in the network must use the same SSID.

**static IP address** - An IP address that is permanently assigned to a device.

**static routing** - The routing of network information through a single, set path.

**subnet mask** - This number identifies what subnetwork the computer is located on. This number is the same on all computers on a home network.

**switch** - Like a hub, a switch is a hardware device that links computers to create a network. A switch provides better data routing than a hub.

**TCP (Transmission Control Protocol)** - A protocol used in connection with Internet Protocol (IP) to let computers communicate over the Internet.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** - A combination of two protocols (TCP and IP) that lets computers communicate with Web servers.

**UDP (User Datagram Protocol)** - UDP is a simpler, faster protocol than TCP. UDP is used with IP. Unlike TCP, UDP drops packets without retries and packets are received in a different order than they were sent. UDP is often used in videoconferencing applications or games where speed is preferred over guaranteed message delivery.

**upgrade** - An addition or update to a program that provides additional features or *fixes*.

**URL (Uniform Resource Locator)** - A standard method of specifying a Web location, for example the URL for Gateway is www.gateway.com. Also called a *Web address*.

**VPN (Virtual Private Network)** - A private network link that lets a computer communicate with another network over the Internet. VPNs usually use encryption to provide secure communication.

**WAN (Wide Area Network)** - A network that provides data communications to a large number of independent users spread over a large geographic area. A WAN often links several networks. The Internet is a WAN.

**WEP (Wired Equivalent Privacy)** - A protocol that adds security to wireless local area networks (WLANs). WEP uses encryption to provide security.

# Appendix B

## Specifications

# Specifications

Specifications are subject to change without notice or obligation.

| | |
|---|---|
| **Dimensions** | 7.32 x 6.89 x 1.89 in. (186 x 175 x 48 mm) |
| **Weight** | 17 oz. (0.482 Kg) |
| **Color** | Graphite and Platinum |
| **Power consumption** | 50 mW to 200 mW |
| **Power supply** | Input 100-240V AC ~ .4A Output 5V DC 2.5A |
| **Operating temperature** | 320° to 40°C (32° to 104°F) |
| **Operating humidity** | 10% to 85% non-condensing |
| **Non-operating temperature** | -20° to 70°C (-4° to 158°F) |
| **Non-operating humidity** | 5% to 90% con-condensing |
| **MTBF** | 500,000 hours |
| **Operating range (indoors)** | As much as 30 m (100 ft) @ 54 Mbps |
| | As much as 50 m (165 ft) @ 24 Mbps |
| | As much as 70 m (230 ft) @ 12 Mbps |
| | As much as 91 m (300 ft) @ 6 Mbps |

# Appendix C

## Safety, Regulatory, and Legal Information

# Regulatory compliance statements

## Wireless Guidance

The WGR-250 802.11G wireless LAN, (low power Radio Frequency, RF, transmitting device), operates in the 2400 - 2483.5 MHz band. The following section is a general overview of considerations while operating the wireless LAN.

Limitations, cautions, and concerns are listed below and in the specific country sections (or country group sections). This wireless device is only qualified for use in the countries identified by the Radio Approval Marks on the device rating label. If the country you will be using the wireless device in is not listed, please contact that countries local Radio Approval agency for requirements prior to operation. Wireless devices are closely regulated and use may not be allowed.

The power output of the WGR-250 wireless LAN device is well below the RF exposure limits as known at this time. Because this wireless device emits less energy than is allowed in radio frequency safety standards and recommendations, Gateway believes these devices are safe for use. Regardless of the power levels, care should be taken to minimize human contact during normal operation.

Measurements have been performed to show that the RF exposure is below what is considered safe limits; however care should be taken to make sure the user or bystanders keep the transmitter away from their body when the wireless device is transmitting. The transmitting antenna should be installed and used in a manner to maintain 20cm (8 inches) from user's or bystander's bodies.

This wireless device is intended to be used indoors. In some areas, use of this device outdoors is prohibited.

Some circumstances require restrictions on using wireless devices. Examples of common restrictions are listed below:

| Warning | In environments where the risk of interference to other devices or services is harmful or perceived as harmful, the option to use a wireless device may be restricted or eliminated. Airports, Hospitals, and Oxygen or flammable gas laden atmospheres are limited examples where use of wireless devices may be restricted or eliminated. When in environments where you are uncertain of the sanction to use wireless devices, ask the applicable authority for authorization prior to use or turning on the wireless device. |
|---|---|
| Warning | Every country has different restrictions on the use of wireless devices. Since your router is equipped with a wireless device, when traveling between countries with your system, check with the local Radio Approval authorities prior to any move or trip for any restrictions on the use of a wireless device in the destination country. |
| Warning | Do not operate the wireless device unless all covers and shields are in place and the device is fully assembled. |

| **Warning** | Wireless devices are not user serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact Gateway for service. |
|---|---|

| **Warning** | Only use drivers approved for the country in which the device will be used. See the Gateway System Restoration Kit, or contact Gateway Technical Support for additional information. |
|---|---|

# United States of America

**Federal Communications Commission (FCC)**
**Intentional emitter per FCC Part 15**

The power output of the WGR -250 wireless LAN device is well below the RF exposure limits as known at this time. Because this wireless device emits less energy than is allowed in radio frequency safety standards and recommendations, Gateway believes these devices are safe for use. Regardless of the power levels, care should be taken to minimize human contact during normal operation.

Measurements have been performed to show that the RF exposure is below what is considered safe limits; however care should be taken to make sure the user or bystanders keep the transmitter away from their body when the wireless device is transmitting. The transmitting antenna should be installed and used in a manner to maintain 20cm (8 inches) from user's or bystander's bodies.

This wireless device is intended to be used indoors. In some areas, use of this device outdoors is prohibited.

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

| **Warning** | Wireless devices are not user serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact Gateway for service. |
|---|---|

| **Warning** | In order to comply with FCC requirements this transmitter must not be operated (or co-located) in conjunction with any other transmitter or antenna. |
|---|---|

**Unintentional emitter per FCC Part 15**

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

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

Compliance Accessories: These accessories are required to be used in order to ensure compliance with FCC rules: The AC Adapter supplied with the device.

**FCC declaration of conformity**

Responsible party:

Gateway Companies, Inc.
610 Gateway Drive, North Sioux City, SD 57049
(605) 232-2000   Fax: (605) 232-2023

Product:

- Gateway WGR-250

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

| **Warning** | Changes or modifications not expressly approved by Gateway could void the FCC compliance and negate your authority to operate the product. |
|---|---|

# California Proposition 65 Warning

| **Warning** | This product contains chemicals, including lead, known to the State of California to cause cancer, birth defects, or reproductive harm. |
|---|---|

# Notices

# Index

## A
ActiveX filter
    turning on 37
adapter (network)
    definition 66
add service
    blocking 44
Advanced (Data) page
    filters 42
    ports 46
    routing 48, 50
    using 38
advanced settings 38
authentication
    auto 40
    open system 40
    type 40
auto authentication
    setting 40
automated troubleshooting system
    using 63
automatic configuration
    DHCP 19

## B
basic rates
    setting 41
beacon interval
    definition 66
    setting 41
blocking services
    setting 44
broadband
    definition 66
browser
    definition 66

## C
cable modem
    connecting 8, 14
    definition 66
Cat-5
    connecting 8, 14

    definition 66
    purchasing 3
CD 3
channel
    setting 20
client lease time
    setting 25
configuring
    PCs 15
    router 9, 17, 29, 35
connections
    power 5
cookies filter
    setting 37
CTS protection mode
    setting 41
currently assigned
    checking DHCP clients 25
customized applications
    setting 46

## D
data packet
    definition 66
data transmission settings
    changing 38
default gateway
    definition 66
    obtaining from ISP 8, 14
DHCP (Dynamic Host Configuration
        Protocol)
    definition 66
    server 25
    setting maximum users 25
disable
    wireless mode 20
DMZ (Demilitarized Zone)
    definition 66
    turning on 37
DNS
    definition 66
domain
    definition 66

DSL (Digital Subscriber Line)
    connecting modem 8
    definition 66
    modem 8, 14
DTIM (Delivery Traffic Indication Message)
    definition 66
    setting interval 41
dynamic IP address
    definition 66
dynamic routing
    definition 66

E
encryption
    definition 67
Ethernet
    cable 3
    definition 67
external port
    setting 46

F
filters
    cookies 37
    setting up 42
firmware
    definition 67
    upgrading 31
fragmentation
    definition 67
    setting threshold 41
FTP (File Transfer Protocol)
    definition 67

G
gateway
    definition 67
G-Only mode 20

H
hardware
    definition 67
HTTP (HyperText Transport Protocol)
    definition 67
hub
    definition 67

I
incoming port range
    setting 47
Internet interface 50
IP address 8, 14
    definition 67
    resolving 55
IPSec (Internet Protocol Security)
    definition 67
ISP (Internet service provider)
    definition 67

J
Java filter
    turning on 37

L
L2TP (Layer-2 Tunneling Protocol)
    setting 37
LAN (local area network)
    connections 5
    definition 67
    interface 50
    LEDs 4
List of Internet PCs 43
List of PCs 43

M
MAC (Media Access Control) address
    cloning 32
    definition 67
    setting filter list 40
Mbps
    definition 67
mixed mode
    setting 20
MTU (Maximum Transmission Unit)
    setting 33

N
network
    definition 67

O
open system authentication 40
operating mode

setting 25
static IP address
    definition 69
    setting 19, 55
static routes
    setting up 50
static routing
    definition 69
subnet mask
    definition 69
    obtaining from ISP 8, 14
summary
    Internet policy summary 45
switch
    definition 69

## T

TCP (Transmission Control Protocol)
    definition 69
    using protocol 46
TCP/IP
    definition 69
Technical Support 63
telephone numbers 63
threshold
    fragmentation 41
    RTS 41
transmission rate
    setting 41

## U

UDP (User Datagram Protocol)
    definition 69
    using protocol 46
upgrade
    definition 69
    firmware 31
UPnP 33
URL (Uniform Resource Locator)
    definition 69
user guide 3

## V

VPN (Virtual Private Network)
    definition 69
    pass-through 37

## W

WAN (Wide Area Network)
    connection 5
    definition 69
    LED 4
Web filters
    setting 37
Website Blocking
    by Domain Name 45
    by Keyword 45
WEP (Wired Equivalent Privacy)
    definition 69
    setting 21
WINS 25
wireless
    interface 50
    LED 4
    MAC filter 40
wizard
    using 9

MAN 802.11G ROUTER GDE R1 02/04

8509687