Wireless-G Router

User's Manual

CE Declaration of Conformity

This equipment complies with the specifications relating to electromagnetic compatibility EN 55022/A1 Class B and EN 50082-1. This meets the reasonable protection requirements set out in the European Council Directive on the approximation of the laws of the member states relating to Electromagnetic Compatibility Directive (89/336/EEC).

Manufacturer's Disclaimer

The information in this document is subject to change without notice and does not represent a commitment on the part of the vendor. No warranty or representation, either expressed or implied, is made with respect to the quality, accuracy, or fitness for any particular purpose of this document. The manufacturer reserves the right to make changes to the content of this document and/or the products associated with it at any time without obligation to notify any person or organization. In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use this product or documentation, even if advised of the possibility of such damages.

Copyright Notice

Packing List

Below are the items that should be included in your Wireless-G Router package.

- One Wireless-G router
- One AC power adapter (12V, 0.5A)
- One 1.5 meter (4 ft. 11 in.) category 5 Ethernet cable
- One CD-ROM containing the quick setup guide and user's manual in PDF form

Before installing the system, examine the contents of the package carefully. If anything appears to be damaged or missing, contact the supplier as soon as possible.

FCC Statement

This product is designed and manufactured to comply with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful radio-frequency interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found 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 or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Contents

Introduction

Congratulations on purchasing a sophisticated, high-quality networking product. Your Wireless-G router is many devices in one, and was designed and manufactured to the highest standards. Still, like any digital electronic product, it requires proper setup and care. Follow the instructions in this manual carefully to ensure that your Wireless-G router will give you many years of trouble-free service.

Overview of the Router

Not long ago, to get all the functionality provided by your Wireless-G router, you would have had to buy three separate devices: a router (which at the time would have been *just* a router), a wireless access point (AP), and an Ethernet switching hub (now called an Ethernet switch or simply a switch).

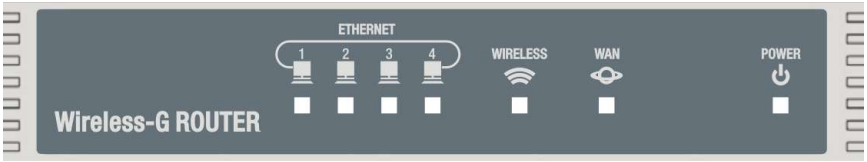
(Why is it called a switch? Because it can switch each transmission to the port the destination machine is connected to. Early Ethernet hubs sent all transmissions out on all ports.)

You would have connected the router, the AP, and your computers together through the switch to form your local-area network (LAN). Then you would have connected the router to your modem for access to the wide-area network (WAN), that is, your ISP's network, and through it, the Internet.

With your Wireless-G router, everything is in one box, and the AP and router are connected internally to the switch. You only have to connect your computers to the **LAN** ports and your modem to the **WAN** port.

For the most part in this manual, we will refer to the combination of router, AP, and switch as a unit. Terms like "the router" and "your router" should be understood to include the built-in AP and switch.

The Parts of the Router: The router has seven light-emitting diode (LED) indicators on its front panel. These are described briefly below.



- **ETHERNET indicators:** Each of these corresponds to a **LAN** port on the back of the router. When a good but idle link is detected on the port, the indicator shines steadily; when there is activity on the link, the indicator blinks off and on.

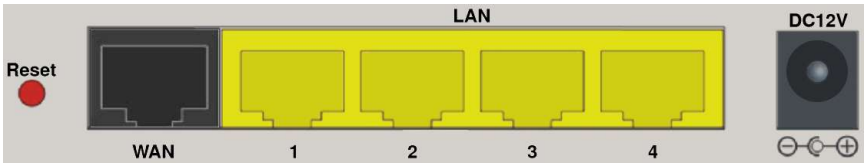
- **WIRELESS indicator:** This indicator shines steadily when wireless networking is enabled but the router is not actively transmitting or receiving; blinks off and on

when there is wireless activity; and stays off when wireless networking is disabled.

- **WAN indicator:** This indicator shines steadily when a good but idle link is detected on the **WAN** port, and blinks off and on when there is activity on the WAN link.

- **POWER indicator:** This indicator flashes on and off during the router's power-on self-test, and shines steadily when the router is ready for operation.

The router has a button, five Ethernet ports, and a power receptacle on its back panel. These are described briefly below.



- **Reset button:** Press this button briefly to restart the router. The router will go through its power-on self-test and then resume operation. Press **Reset** for at least five seconds to restore the router's factory settings.

  NOTE: Restoring the factory settings may cause your Internet and/or wireless links to go down.

- **WAN port:** This is for the Ethernet connection to your DSL or cable modem.

- **LAN ports:** These are for Ethernet connections to computers and other devices on the LAN. These connections can be indirect: you can connect a hub or switch to a **LAN** port, and then connect machines to the remaining Ethernet ports of the hub or switch.

- **DC12V receptacle:** This is for connecting the AC power adapter included with the router.

  WARNING: Use only the AC power adapter that came with the router. Connecting any other power adapter may damage the router and cause a fire hazard.

Major Non-routing Functions: Besides performing the functions of a pure router, AP, and switch, your Wireless-G router provides many other capabilities, some of which are provided on some networks by special-purpose devices or powerful servers. A few of the important ones are listed below.

- **Login:** Your ISP (especially if you use ADSL, VDSL, etc.) may have given you software for connecting to and disconnecting from the Internet. Such software is often called a *login client*. After the router is set up, you will no longer use any login client — the router will automatically log on for you.

(The router can connect automatically whenever you access the Internet, or it can stay connected all the time. The choice is yours.)

- **DHCP:** This stands for Dynamic Host Configuration Protocol. To communicate on the Internet, a machine needs Internet Protocol (IP) settings such as an IP address. The router is set at the factory to be a DHCP server, that is, to give machines on the LAN IP settings if they request them. Most computers are set by default to be DHCP clients, that is, to request IP settings from a DHCP server.

- **NAT:** This stands for Network Address Translation. The router uses one IP address on the LAN and another on the WAN. When a machine on the LAN sends a request to the Internet, the router changes the source IP address to its own WAN IP address. Any reply, therefore, is addressed to the router. The router changes the reply's destination IP address to that of the local machine originating the exchange, and places it on the LAN so that machine can receive it.

- **Firewall:** NAT helps protect your computers by hiding their IP addresses from the WAN. The router also has a firewall that performs "stateful packet inspection," monitoring each connection for abnormal activity. By default, the router blocks common denial-of-service (DoS) attacks. In fact, it blocks all attempts to connect from the Internet, but you can set it to accept connection types that you need.

The above list is far from complete. The router's other functions will be explained in the chapters on setup.

Care of the Router: Observe the following precautions to ensure that the router has a long service life:

- Never block the air vents on the bottom and sides of the router.

- Use only the 12-volt, 0.5-ampere AC power adapter that came with the router.

- Keep the router away from liquids and moisture. Clean it only with a slightly damp cloth.

- Never open the router. For reasons of electrical safety, the router may only be opened by an authorized service technician.

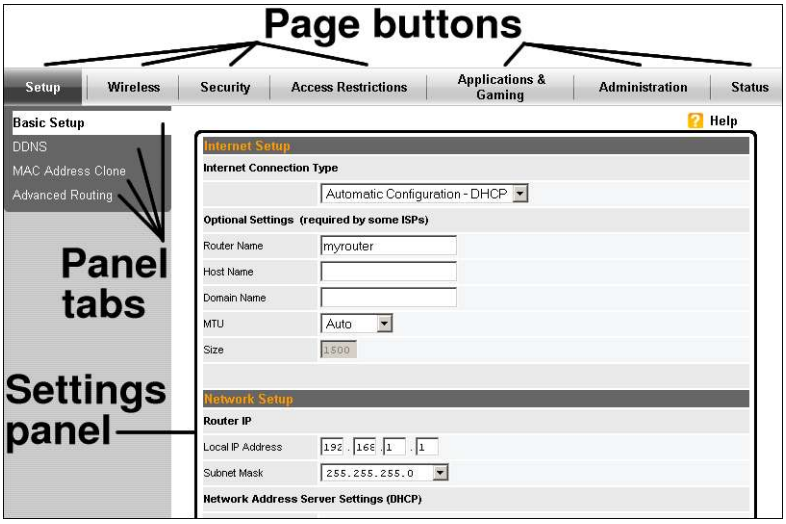
About this Manual

A large part of this manual explains the router's setup utility — the user interface that the router displays to let you change router settings. In this section we explain the terminology we use to describe the setup utility. This will also help you understand the setup utility's organization and manner of operation.

The setup utility is coded, and served to your computer, in exactly the same way as a World Wide Web site, and you will view it with your Web browser, so some of our terminology comes from the language of the World Wide Web.

Many Web sites have links at the top of each page for displaying other pages on the site. Similarly, at the top of the setup utility are seven buttons that we call *page buttons*. Each takes you to a different page of the setup utility.

Most pages are made up of several *panels*. Panels contain the *controls* for setting the router. To change panels, you click *panel tabs* on the left.



Shown above is the **Setup** page's **Basic Setup** panel. It has two *sections*, named **Internet Setup** and **Network Setup**, and the **Internet Setup** section has two *subsections*, named **Internet Connection Type** and **Optional Settings (required by some ISPs)**. The first control in the **Optional Settings (required by some ISPs)** subsection is the **Router Name** control, and its default (factory) *setting* is **myrouter**. This is the terminology we will use in this manual.

Important Concepts

If you are new to networking, you may encounter many unfamiliar terms when setting up the router. Those that appear most frequently and are most basic for understanding router settings are explained below.

IP Address: We have already touched on IP addresses without explaining them. A thorough explanation would require a separate chapter, and is quite beyond the scope of this manual. A short explanation of IP addressing as it applies to your router, however, is necessary.

"IP" stands for "Internet Protocol," and IP addresses are the means by which networks and individual machines are identified on the Internet (and now on most LANs as well). An IP address is usually written in "dotted quad" notation — four numbers separated by "dots" (periods). Your Wireless-G router's default LAN-side IP address, for example, is 192.168.1.1. (It has no default WAN-side IP address; its "WAN IP" must be set manually or sent to the router by your ISP.)

Each number in an IP address takes up an octet — eight bits — of computer storage space, so its range is 0–255. Certain numbers, however, have special significance in certain positions. No machine's IP address can end in 0 or 255, for example.

Subnet Mask: Each machine on an IP network must have an IP address that is unique on that network. All the machines, however, must share a set of values called a *subnet mask*. The router's default LAN-side subnet mask is 255.255.255.0. Combined with the router's default LAN-side IP address of 192.168.1.1, this tells us (and all machines getting their IP settings from the router) —

- The first three numbers of the IP address — 192.168.1 — are the *network portion* of the address, shared by all machines on the LAN, and the fourth number is the *host portion*, unique to each machine.

- The machines on the LAN (including the router) can have.IP addresses from 192.168.1.1 to 192.168.1.254. Machines with addresses in this range are *local*, and can be reached directly.

- Machines with IP addresses outside this range can only be reached through a *gateway* such as the router.

DNS: We prefer names to IP addresses. The name www.bigcompany.com is likely to identify a Web server in the domain of servers run by bigcompany, which is part of the domain of commercial enterprises on the Internet. To reach this server, we need its IP address. Our Internet software gets the address by contacting a Domain Name System (DNS) server, also called a name server. If one DNS server doesn't have a particular IP address in its tables, it can get it from a DNS server that does.

The IP address of at least one DNS server is a required setting for any machine that will access the Internet. On most types of Internet connections, the router can get at least one DNS server's IP address from your ISP, and it passes the address(es) to machines on the LAN that get their IP settings from the router.

MAC Address: Ethernet was developed separately from the Internet and has a very different system of addressing. In Ethernet, each device is identified by its *medium* (or *media*) *access control* (MAC) address. This is a value that is assigned at the factory and usually cannot be changed. The Institute of Electrical and Electronics Engineers (IEEE) administers a system that ensures that no two Ethernet devices in the world have the same MAC address.

A device's MAC address is usually printed on a sticker placed on the back or bottom of the device. Various formats are used, but the address is always in hexadecimal (base 16) notation and always consists of twelve hexadecimal digits. Two common formats are 12:34:56:78:9A:BC and 123456:789ABC .

Chapter 1: Required Setup

The router always requires some setup. There are several reasons:

- It works with six different kinds of Internet connection. Even if the default setting is the kind of connection you have, some setup may be required to get it working.

- Wireless networking is enabled by default. If you don't change some settings, your network will be open to possibly malevolent intruders.

- The router's setup utility is password-protected, but the default password is easy to find out. Unless you change the router password, anyone with access to your network can change router settings (and cut you off from your own network!).

Information You Need

Internet Connection Type: You will need information from your ISP, starting with the type of Internet connection you have. That will be one of the following:

- Automatic Configuration – DHCP (the Dynamic Host Configuration Protocol)
- Static IP (fixed IP settings)
- PPPoE (the Point-to-point Protocol over Ethernet)
- PPTP (the Point-to-point Tunneling Protocol)
- L2TP (the Layer 2 Tunneling Protocol)
- Telstra Cable (BigPond broadband cable service)

Depending on which of these you use, other information may be required. It must be obtained from your ISP.

Wireless Environment: It is important to know in advance what kinds of wireless stations will access the router: Wireless-G (802.11g), Wireless-B (802.11b), or both. If you are adding the router to an existing wireless network, you will need to know how that network is set up. You should also find out if other wireless equipment is operating nearby, so you can pick a channel that minimizes interference.

Preparation for Setup

Making Connections: It is assumed here that you have a computer connected to your modem through an Ethernet cable, and that the computer has a Javascript-enabled Web browser installed. It is best to use this computer to set up the router.

(If your Internet connection type is Static IP or PPTP, this computer might have fixed IP settings. The computer that you use to set up the router must be set to obtain IP settings automatically. For information on checking and changing the setting, look up "automatic addressing" or "DHCP" with the operating system's Help function.)

Make connections for setup as follows:

1. **Power down the modem.**

   Some modems are designed to stop working if they detect a change in the MAC address of the device connected to them.

2. **Disconnect the Ethernet cable from the modem.**

3. **Plug the Ethernet cable into any one of the router's four LAN ports.**

   The Ethernet cable that led from the computer to the modem should now lead from the computer to the router.

4. **Plug in and connect the router's AC power adapter.**

The router will be ready for setup shortly after its **POWER** indicator stops flashing and starts shining steadily.

If you need to restore the router's factory defaults, press its **Reset** button for at least five seconds and wait until it is again ready.

You can connect the router's **WAN** port to the modem with an Ethernet cable and turn the modem on now, if you wish. From the point of view of security, however, it is better to do this after setup is complete.

Accessing the Setup Utility: If all has gone well, the computer will now have IP settings (received from the router) that let you conveniently browse to the router's setup utility. Access the setup utility as follows:

1. **Start up the Web browser.**

   If it tries to go to a start page on the Internet, click its Stop button or press **Esc**.

2. **Type http://192.168.1.1/ into the browser's address bar and then press Enter.**

   You will be prompted for a user name and password.

3. **Leave the User Name box blank, type admin into the Password box, and press Enter (or click OK).**

   The **Basic Setup** panel of the setup utility's **Setup** page will appear.

Later, after the router and your LAN are fully set up and in operation, you will still be able to access the router's setup utility in this way: start up a browser on any computer networked to the router, type **http://** plus the router's IP address into the address bar, press **Enter**, and supply the correct password when prompted (that password will be something other than **admin** if you follow our recommendations during initial setup).

Setup Utility Basics: Note the following characteristics of the setup utility:

- Each settings panel has a **Save Settings** button. After changing settings, you must click **Save Settings** to have the changes applied on the router.

- Switching panels cancels unsaved changes. Finish up in one panel before going to another.

- Many controls appear only when certain settings are selected. If you don't see a certain control at first, you will see it when you select a setting that makes it necessary.

- Although you log on to the setup utility by supplying a password, there is no procedure for logging off. After you save all your settings, you can simply close your browser or browse to other pages.

Setup for Internet Access

Internet Connection Type: To begin setup for Internet access, open the **Internet Connection Type** list and select your connection type.

- For almost all connection types, **User Name** and **Password** boxes will appear. If they do, be sure to click in these boxes and type in the strings required by your ISP.

  NOTE: Your ISP may refer to the user name as a user ID, account name, or "login."

- For almost all connection types, you can select either **Connect on Demand** or **Keep Alive**. Click the option you want and set the time period you want; this is not decided by your ISP.

  Connect on Demand means automatically connecting to your ISP when Internet access is needed, and then disconnecting when there has been no activity for a given number of minutes (the **Max Idle Time** setting).

  Keep Alive means never breaking the connection, and automatically trying to restore it if it goes down for a given number of seconds (the **Redial Period** setting).

Find your connection type below and follow the additional instructions given. When finished, go to "Optional Settings (required by some ISPs)," below.

- **Automatic Configuration – DHCP:** This is the most common connection type for cable ISPs. The router will receive its WAN-side IP settings from a DHCP server on your ISP's network. Your ISP may require that you connect from a registered MAC address; in that case you must either (*a*) register the router's WAN-side MAC address with your ISP (this address is shown in the **Status**

page's **Router** panel), or (*b*) use the **MAC Address Clone** panel to change the router's WAN-port MAC address.

- **Static IP:** Use this setting if you have purchased a fixed IP address from your ISP and you are not using PPTP. All IP settings must be input manually: **Internet IP Address**, **Subnet Mask**, **Gateway**, and at least one **Static DNS** server address. All values must be obtained from your ISP.

- **PPPoE:** This is the most common connection type for DSL ISPs. You must input the **User Name** and **Password** settings required by your ISP. WAN-side IP settings will be received over the wire from your ISP when the router connects.

- **PPTP:** This is used by a minority of ISPs. You must input the **User Name** and **Password** settings required by your ISP. If you have received fixed IP settings from your ISP, you must input them in the **Internet IP Address**, **Subnet Mask**, and **Gateway** boxes. If these settings are assigned dynamically (over the wire), leave the Internet IP address set to 0.0.0.0.

- **L2TP:** This is used by a minority of ISPs. You must input the **User Name**, **Password**, and **L2TP Server** IP address settings required by your ISP. WAN-side IP settings will be received over the wire when the router connects.

- **Telstra Cable:** This is used on Telstra BigPond broadband cable connections in Australia. You must input the **User Name** and **Password** settings required by BigPond. Input the name of a heartbeat server if Telstra BigPond indicates that this is necessary on your connection; otherwise leave the **Heart Beat Server** box blank.

Optional Settings (required by some ISPs): Some of the settings in this group are required on some Internet accounts. Your ISP can tell you which ones you need to set, if any.

- **Router Name:** This is not required by any ISP. It is for your reference, and does not affect operation. You can set this to any string you like, as long as it does not contain spaces and is no more than 39 characters long.

- **Host Name and Domain Name:** One or (more often) both of these may be required. Enter the strings your ISP has instructed you to use. Usually, a host name has no dots (www is a common host name), while a domain name has at least one dot (bigcompany.com, for example).

- **MTU and Size:** Information is sent over a network in chunks called packets. Packet size is measured in octets (also called bytes) of eight bits (1s and 0s) each. MTU stands for Maximum Transmission Unit. MTU size is the greatest allowable packet size on a given connection.

  With the **MTU** control set to **Auto**, the router adjusts MTU size according to connection type (1500 for Ethernet, 1492 for PPPoE, 1436 for PPTP, and so on).

In very rare cases, an ISP may require an unusual MTU size. Where this is the case, set **MTU** to **Manual** and enter the value in the **Size** box.

This completes adjustment of settings in the **Basic Setup** panel's **Internet Setup** section. Some controls in the **Network Setup** section, however, are related to the Internet. Below are a few things you can do before you click **Save Settings**.

- If (1) you will use the router as a DHCP server for machines on the LAN, and (2) your ISP has given you the IP addresses of any DNS servers, you can enter those addresses in the **Static DNS 1**, **2**, and **3** boxes. (For a connection type of Static IP, however, these addresses are entered not here but in the **Internet Setup** section.)

  WINS stands for Windows Internet Name Service. If the router will be a DHCP server and you have been given the IP address of a WINS server, you can enter that address in the **WINS** boxes.

- You can select your time zone from the **Time Zone** list, and if Daylight Saving Time is not used in your area, you can uncheck **Automatically adjust clock for daylight saving changes**.

  The router will set its clock by obtaining Universal Coordinated Time readings from servers on the Internet and adding or subtracting the number of hours required for your time zone. This makes it possible for you to specify when particular machines can and cannot access the Internet.

Unless you are very knowledgeable about networking, we recommend not changing any other settings in the **Network Setup** section at this time.

Finishing Up: Click **Save Settings** to save and apply your settings on the router. After a short wait, a success message and a **Continue** button will appear. Click **Continue** to return to the **Basic Setup** panel.

Testing the Connection: If you wish to test the connection, we recommend making the test brief for security reasons. Setup for Internet access may be complete, but required setup is not.

You will need a second Ethernet cable. Test the connection as follows:

1. **Power up the modem.**

2. **Connect the router's WAN port to the modem with an Ethernet cable.**

3. **Point the browser *directly* at an Internet Web site.**

   Simply choose a site from your bookmarks or favorites. Do not run any program your ISP gave you for connecting and disconnecting. The router will do that for you from now on.

4. **Return to the setup utility and turn the modem off.**

If your settings are correct and you still cannot connect, the most likely cause is that your ISP requires the machine connected to the modem to have a particular MAC address. One solution is to register the MAC address of the router's **WAN** port with your ISP. You can find this MAC address by clicking the **Status** button.

Another solution is to use the **MAC Address Clone** function.

MAC Address Clone: If you can find out the MAC address that your ISP requires, or it is the MAC address of the computer you are using to set up the router, you can "clone" the address to the router's **WAN** port. Do this as follows:

1. **On the setup utility's Setup page, click the MAC Address Clone tab.**

2. **Click Enable.**

3. **Do *one* of the following:**

   If the address is not *that of the computer being used to set up the router*, enter the address in the **User Defined Entry** boxes.

   If the address is *that of the computer being used to set up the router*, click **Clone Your PC's MAC**.

4. **Click Save Settings.**

Setup for Wireless Networking

The router acts as a wireless *access point* (AP, also called a base station). Wireless *clients* (computers with wireless interfaces, also called wireless stations) connect to the wired network, the Internet, and each other through the AP portion of the router.

- *If you will not use wireless networking*, click the **Wireless** page button, open the **Wireless Network Mode** list, click **Disabled**, and click **Save Settings**. Then go to "Setup for Router Security," below.

If you have a wireless client, we suggest starting up the client's wireless connection software and clicking **Site Survey** while the router is on.

The router will be detected (its default SSID, or wireless network name, is **mySSID**), and you will be able to join the network (this is usually done by double-clicking the displayed SSID). Anyone else in the vicinity with a wireless client can do this also. Setup is required to make the wireless network secure against intrusion.

While the Site Survey results are displayed, take note of the wireless channels used by any other APs or wireless networks operating in the vicinity.

Basic Wireless Settings: Start setup for wireless networking by clicking the **Wireless** page button. The **Basic Wireless Settings** panel will appear. The controls in this panel are explained below.

- **Wireless Network Mode:** Set this control according to the kind(s) of wireless client(s) that will join the network. Use **Mixed** if both Wireless-B (IEEE 802.11b) and Wireless-G (IEEE 802.11g) clients will join; **B-Only** if only Wireless-B clients will join; and **G-Only** if only Wireless-G clients will join. This is important for network performance.

  Any Wireless-G clients will have a similar control, and must use the same setting as the router.

- **Wireless Network Name (SSID):** This is a string by which the router and all its wireless clients identify themselves as belonging to the same network. It can be up to 32 characters long. All typable characters, including spaces, are allowed. The setting is case-sensitive. A long, hard-to-guess SSID that is not broadcast can help prevent casual intrusion, but is less convenient for authorized clients.

  Do not use the factory-set SSID. This is very important for security.

- **Wireless Channel:** Open this list to see the numbers and center frequencies of the wireless channels the router can use. Each channel is a cluster of frequencies. Closely spaced channels share some frequencies, which can cause interference and impair performance. Networks (or APs on the same network) with overlapping coverage areas should be set at least 5 channels apart. If channel 6 is being used by another device near the router, for example, set the router to channel 1 or channel 11.

  Wireless clients will automatically find the channel used by the router.

- **Wireless SSID Broadcast:** Use the default setting, **Enable**, to allow the SSID to show up in wireless clients' Site Survey results. This saves users the trouble of typing the SSID in by hand on each client. Click **Disable** to prevent the SSID from appearing in Site Survey results.

Click **Save Settings** when finished making changes in the **Basic Wireless Settings** panel.

Wireless Security: To make wireless links secure, you must use encryption. This means scrambling wireless transmissions using a string of characters or values called a key.

The router offers six encryption options. They are described below in order of increasing security. Assuming that you will use encryption, you must select an option that all of your wireless clients can use.

- **WEP** (Wired Equivalent Privacy) is the least secure option, but is supported by all Wireless-B and Wireless-G clients. One reason it is relatively insecure is that it does not automatically change keys.

- **RADIUS** (Remote Authentication Dial-in User Service) can be used together with WEP to provide authentication and periodically change keys. This requires a RADIUS server, which can be expensive and difficult to administer.

- **WPA Personal** is Wi-Fi Protected Access–Personal, also known as WPA-PSK (WPA Pre-shared Key). This uses the Temporal Key Integrity Protocol (TKIP) to periodically change keys. Newer WPA Personal clients can use AES (see next).

- **WPA2 Personal** uses the more powerful Advanced Encryption Standard (AES), and can also use AES and TKIP concurrently so that both WPA2 Personal and older WPA Personal clients can connect.

- **WPA Enterprise** is similar to WPA Personal but adds RADIUS authentication, requiring a RADIUS server.

- **WPA2 Enterprise** is similar to WPA2 Personal but adds RADIUS authentication, requiring a RADIUS server.

Setting the Encryption Option: Check your wireless clients to find the most secure encryption option they can all use (keeping in mind whether or not a RADIUS server is available). Then click the **Wireless** page's **Wireless Security** tab, open the **Security Mode** list, and select the option you will use.

Controls for setting up the selected encryption method will appear. Follow the instructions below for that method.

- **WPA Personal Step 1; WPA Enterprise Step 1:**

  Check, and if necessary change, the WPA Algorithms setting.

  Leave this control set to **TKIP** if you have clients that can only use TKIP. Set this control to **AES** if all your clients can use AES and you want stronger encryption.

- **WPA2 Personal Step 1; WPA2 Enterprise Step 1:**

  Check, and if necessary change, the WPA Algorithms setting.

  If only WPA2 clients will connect, use **AES**. If both WPA2 and WPA clients will connect, use **TKIP+AES**.

- **WPA Personal Step 2; WPA2 Personal Step 2:**

  (a) Input the WPA shared key.

The WPA shared key (also called the WPA pre-shared key) must contain 8 to 63 characters. All characters found on a U.S.-type keyboard, including spaces, are valid. A string of 14 to 22 randomly chosen characters is recommended. The setting is case-sensitive. All clients must use exactly the same string as the router.

(In some client setup utilities, the WPA shared key is called a passphrase. It is not in fact used directly as an encryption key; it is used to generate encryption keys that change periodically.)

(b) Check, and if desired change, the Group Key Renewal setting.

Group Key Renewal controls how frequently the router changes the key for broadcast and multicast traffic (this key is generated automatically). Most broadcast traffic is for network control; most multicast (partial broadcast) traffic is for audio/video applications.

A client can leave the network and then continue to monitor broadcast and multicast traffic until the group key changes. Input a lower value here if the possibility of such monitoring is a concern. The default value is 3600 seconds (1 hour); the allowable range is 600 (10 minutes) to 7200 (2 hours).

(c) Click Save Settings and go to "Setup for Router Security.".

- **WPA Enterprise Step 2; WPA2 Enterprise Step 2:**

(a) Input the RADIUS server address.

(b) Check, and if necessary change, the RADIUS Port setting.

One machine can provide many different services. "Port" here is a number specifying a particular service. The standard port number for RADIUS is 1812. If your network's RADIUS server uses a non-standard port number, enter that number here.

(c) Input the shared key (also called the RADIUS secret or RADIUS shared secret).

This is a string shared by the router and the RADIUS server. Input the string specified by the administrator of your RADIUS server.

(b) Check, and if desired change, the Key Renewal Timeout setting.

Key Renewal Timeout controls how frequently the key for broadcast and multicast traffic is changed (this key is generated automatically). Most broadcast traffic is for network control; most multicast (partial broadcast) traffic is for audio/video applications.

A client can leave the network and then continue to monitor broadcast and multicast traffic until the group key changes. Input a lower value here if the

possibility of such monitoring is a concern. The default value is 3600 seconds (1 hour); the allowable range is 600 (10 minutes) to 7200 (2 hours).

(c) Click Save Settings and go to "Setup for Router Security."

- **RADIUS Step 1:**

(a) Input the RADIUS server address.

(b) Check, and if necessary change, the RADIUS Port setting.

One machine can provide many different services. "Port" here is a number specifying a particular service. The standard port number for RADIUS is 1812. If your network's RADIUS server uses a non-standard port number, enter that number here.

(c) Input the shared key (also called the RADIUS secret or RADIUS shared secret).

This is a string shared by the router and the RADIUS server. Input the string specified by the administrator of your RADIUS server.

- **RADIUS Step 2; WEP:**

(a) If you will use 64-bit WEP, set Default Transmit Key to 1, 2, 3, or 4.

In 64-bit WEP, four short keys are used. Each device can use any one of these keys as its default transmit key, and uses the other three keys only for decryption. In 128-bit WEP, a single long key is used by all devices for both encryption and decryption. It must appear as key 1, and **Default Transmit Key** must be set to **1**.

(b) Set WEP Encryption to 64 bits 10 hex digits or 128 bits 26 hex digits.

64-bit WEP is also known as 40-bit WEP (24 bits are generated automatically). WEP keys are generated or input in hexadecimal (base 16) numeric notation. In "hex," the numerals *0–9* and the letters *A–F* (or *a–f*; case does not matter) are used as digits. Your wireless clients must use the same setting as the router.

(c) Either input a passphrase and click Generate, or input the key(s) manually.

The passphrase can contain up to 16 characters. All typable characters, including spaces, are valid; the generated keys will contain only hex digits.

Your wireless clients' setup utilities may also let you generate the key(s) from a passphrase. Unfortunately, different manufacturers' setup utilities generate different keys from the same passphrase. Carefully copy the key(s) down for input on your wireless clients.

(d) Click Save Settings and go to "Setup for Router Security."

Setup for Router Security

You accessed the router's setup utility using a simple, easily discovered password, **admin**. If you do not change the password, anyone using your network — even wirelessly — can do the same, and cause considerable trouble for you. We consider changing the router password a required part of setup.

Change the router password as follows:

1. **Click the Administration page button.**

   The **Management** panel will appear.

2. **Clear the Password box and type the new password.**

   The password can be up to 32 characters long, and must not contain any spaces.

3. **Clear the Re-enter to confirm box and type the new password again.**

4. **If you do not expect to access the router's setup utility from a wireless client, set Wireless Access Web to Disable.**

3. **Click Save Settings and wait to be returned to the Management panel.**

Chapter 2: Setup Utility Reference

After completing required setup, you may wish to further adjust router settings, or use some of the router's advanced features. This chapter provides a complete reference covering each panel of each page of the router's setup utility.

Accessing the Setup Utility: To access the setup utility, start up a Web browser on your computer and enter the router's default IP address, 192.168.1.1, in the address bar. Then press **Enter**.

You will be prompted for a user name and password. Leave the **User Name** box blank. The first time you open the setup utility, use the default password **admin**. (You can set a new password using the **Administration** page's **Management** panel.) Click **OK** to continue.

Setup Page – Basic Setup Panel

The first panel that appears is the **Basic Setup** panel. This allows you to change settings related to Internet access and LAN operation.

The **Internet Setup** section lets you configure the router for your Internet connection. Most of the information you need can be obtained from your ISP.

Internet Connection Type: Open this list and select the type of Internet connection your ISP provides. The available types are:

- Automatic Configuration – DHCP (the Dynamic Host Configuration Protocol)
- Static IP (fixed IP settings)
- PPPoE (the Point-to-point Protocol over Ethernet)
- PPTP (the Point-to-point Tunneling Protocol)
- L2TP (the Layer 2 Tunneling Protocol)
- Telstra Cable (BigPond broadband cable service)

- **Automatic Configuration - DHCP:** By default, Internet Connection Type is set to Automatic Configuration - DHCP. Use this setting only if your ISP provides you with a dynamic IP address via DHCP. (This option usually applies to cable connections.)

- **Static IP:** If you use a permanently fixed IP address to connect to the Internet, select Static IP. To use this option, you must input the settings listed below.

  Internet IP Address: This is the router's IP address, as seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

  Subnet Mask: This is the subnet mask used by the router on your ISP's network. Your ISP will provide you with the subnet mask.

Gateway: Your ISP will provide you with the gateway address, which is the IP address of a router on your ISP's network.

DNS: Your ISP will provide you with at least one DNS (Domain Name System) server IP address.

- **PPPoE:** Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable PPPoE.

  User Name and Password: Enter the user name and password provided by your ISP.

  Connect on Demand: Max Idle Time: You can configure the router to disconnect from the Internet after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically reconnect when you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time box, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes.

  Keep Alive: Redial Period: If you select this option, the router will periodically check your Internet connection. If you are disconnected, the router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period box, specify how often you want the router to check the Internet connection. The default Redial Period is 30 seconds.

- **PPTP:** The Point-to-Point Tunneling Protocol (PPTP) is a connection method used mostly in European countries.

  Internet IP Address: This is the router's IP address as seen from the Internet. Your ISP will provide you with the IP address you need to specify here.

  Subnet Mask: This is the subnet mask used by the router on your ISP's network. Your ISP will provide you with the subnet mask.

  Gateway: Your ISP will provide you with the gateway address.

  User Name and **Password:** Enter the user name and password provided by your ISP.

  Connect on Demand: Max Idle Time: You can configure the router to disconnect from the Internet after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically reconnect when you attempt to access the Internet again. To use this option, select Connect

on Demand. In the Max Idle Time box, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes.

Keep Alive: Redial Period: If you select this option, the router will periodically check your Internet connection. If you are disconnected, the router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period box, specify how often you want the router to check the Internet connection. The default Redial Period is 30 seconds.

- **L2TP:** The Layer Two Tunneling Protocol is a connection method used mostly in Israel.

  User Name and **Password:** Enter the user name and password provided by your ISP.

  L2TP Server: This is the IP address of the L2TP server. Your ISP will provide you with the IP address you need to specify here.

  Connect on Demand: Max Idle Time: You can configure the router to disconnect from the Internet after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically reconnect when you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time box, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes.

  Keep Alive: Redial Period: If you select this option, the router will periodically check your Internet connection. If you are disconnected, the router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period box, specify how often you want the router to check the Internet connection. The default Redial Period is 30 seconds.

- **Telstra Cable:** Telstra Cable is a connection method used in Australia only. If you use Telstra BigPond cable service, then select Telstra.

  User Name and **Password:** Enter the user name and password provided by your ISP.

  Heart Beat Server: This is the name or IP address of the heartbeat server. Your ISP will provide you with the string or address you need to specify here. If no heartbeat server is used on your connection, then leave this box blank.

  Connect on Demand: Max Idle Time: You can configure the router to disconnect from the Internet after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the router to automatically reconnect

when you attempt to access the Internet again. To use this option, select Connect on Demand. In the Max Idle Time box, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is 5 minutes.

Keep Alive: Redial Period: If you select this option, the router will periodically check your Internet connection. If you are disconnected, the router will automatically re-establish your connection. To use this option, select Keep Alive. In the Redial Period box, specify how often you want the router to check the Internet connection. The default Redial Period is 30 seconds.

Optional Settings: Some of these settings may be required by your ISP. Verify with your ISP before making any changes.

- **Router Name:** In this box, you can enter a name of up to 39 characters to represent the router.

- Host Name/Domain Name: These boxes let you supply a host and domain name for the router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your Internet service has been configured with a host and domain name. In most cases, leaving these boxes blank will work.

- **MTU:** MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the router select the best MTU for your Internet connection, keep the default setting, Auto.

- **Size:** When **Manual** is selected as the **MTU** setting, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet connection type: DHCP, Static IP, or Telstra — 1500; PPPoE — 1492; PPTP or L2TP — 1460.

Network Setup: The Network Setup section changes the settings on the network connected to the router's Ethernet ports. Wireless setup is performed through the Wireless page.

- **Router IP:** This presents both the router's IP address and subnet mask as seen by your network.

- **Network Address Server Settings (DHCP):** These controls let you configure the router's Dynamic Host Configuration Protocol (DHCP) server function. The router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the router's DHCP server option, make sure there is no other DHCP server on your network.

  DHCP Server: DHCP is enabled by factory default. If you already have a DHCP

server on your network, or you don't want a DHCP server, then select Disable (no other DHCP features will be available).

Starting IP Address: Enter a value for the DHCP server to start with when issuing IP addresses. Because the router's default IP address is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.255. The default starting IP address is 192.168.1.100.

Maximum Number of DHCP Users: Enter the maximum number of machines that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is 50.

Client Lease Time: The client lease time is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is 0 minutes, which means one day.

Static DNS (**1**-**3**): The Domain Name System (DNS) is how the Internet translates domain or Web site names into IP addresses. Your ISP will provide you with at least one DNS server IP address. If you wish to use another, enter that IP address in one of these groups of boxes. You can enter up to three DNS server IP addresses here. The router will use these for quicker access to functioning DNS servers.

WINS: The Windows Internet Naming Service (WINS) manages Windows PCs' interaction with the Internet. If you use a WINS server, enter that server's IP address here. Otherwise, leave this blank.

Time Setting: Select from this list the time zone in which your network functions. (You can even automatically adjust for daylight saving time.)

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Setup Page – DDNS Panel

The router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you have a fixed host and domain name without having a fixed Internet IP address. If the router's Internet IP address is dynamically assigned and you wish to host a Web site, FTP site, or other service, you must use DDNS so the Domain Name System is automatically updated when the router's Internet IP address changes.

Before you can use this feature, you need to sign up for DDNS service with DDNS provider Dynamic Network Services, Inc., also known as DynDNS (http://www.dyndns.org/). If you do not want to use this feature, keep the default setting, **Disable**.

DDNS Service: If you have signed up for DDNS service with DynDNS, open the DDNS Service list and select **DynDNS.org**.

- **User Name:** Enter the User Name for your DDNS account.
- **Password:** Enter the Password for your DDNS account.
- **Host Name:** This is the host name assigned by the DDNS service. It is a fully qualified domain name (FQDN) in the format name.dyndns.org.
- **Internet IP Address:** The router's Internet IP address is displayed here. Because it is dynamic, it will change.
- **Status:** The status of the DDNS service is displayed here.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Setup Page – MAC Address Clone Panel

Enable/Disable: To clone a MAC address to the router's WAN port, select **Enable**.

User Defined Entry: If the MAC address you wish to clone is not that of computer you are using to access the router's setup utility, enter that MAC address here.

Clone Your PC's MAC: Clicking this button will clone the MAC address of the computer you are using to access the router's setup utility.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Setup Page – Advanced Routing Panel

This panel is used to configure advanced routing functions. The router can operate as a gateway with or without static (fixed) routes through other routers on your LAN. It can also operate as a full router, even using the Routing Information Protocol (RIP) to discover routes through communication with other routers.

Operating Mode: Select the mode in which the router will function. If the router is hosting your network's connection to the Internet, select Gateway. If another router exists on your network, select Router. When Router is chosen, dynamic routing will be available as an option.

Dynamic Routing: This section appears only when Operating Mode is set to Router.

- **RIP:** This feature enables the router to automatically adjust to physical changes in

network layout and exchange routing tables with other routers. This feature is disabled by default. From the drop-down list, you can select LAN & Wireless, which performs dynamic routing over your Ethernet and wireless links. Alternatively, you can select WAN (Internet), which performs dynamic routing on the link to your ISP. Finally, selecting Both enables dynamic routing on all links.

Static Routing: A static route is a predetermined pathway that network information must travel to reach a specific host or network.

- **Select set number:** You can have up to 20 static routes. Each has a number and a name. Select from this list the static route you wish to be displayed.
- **Delete This Entry:** Click here to delete the displayed route.
- **Enter Route Name:** Enter a name for the route here. The name can contain up to 25 alphanumeric characters.
- **Destination LAN IP:** The destination LAN IP is the address of the remote network or host to which you want to assign a static route.
- **Subnet Mask:** The subnet mask determines which portion of a destination LAN IP address is the network portion, and which portion is the host portion.
- **Default Gateway:** This is the IP address of the gateway device that provides contact between the router and the remote network or host.
- **Interface:** This setting tells the router whether the destination IP address is on the LAN & Wireless (Ethernet and wireless networks) or the WAN (Internet).
- **Show Routing Table:** Click this button to open a window displaying how data is routed through your local network. For each route, the destination LAN IP address, subnet mask, gateway, and interface are displayed. Click **Refresh** to update the information. Click **Close** to exit this window.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Wireless Page – Basic Wireless Settings Panel

The basic settings for wireless networking are set in this panel.

Wireless Network Mode: From this drop-down list, you can select the wireless standards running on your network. If you have both 802.11g and 802.11b devices on your network, keep the default setting, Mixed. If you have only 802.11g devices, select G-Only. If you have only 802.11b devices, select B-Only. If you do not have any 802.11g or 802.11b devices on your network, select Disable.

Wireless Network Name (SSID): The SSID is the network name shared among all

devices on a wireless network. The SSID must be identical for all devices on the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all devices on your wireless network. For added security, you should replace the default SSID (mySSID) with a unique name.

Wireless Channel: Select the channel from the list provided to correspond with your network settings. Devices that connect to the router wirelessly will automatically discover the channel it is set to.

Wireless SSID Broadcast: When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the router. To broadcast the router's SSID, keep the default setting, Enable. If you do not want to broadcast the router's SSID, then select Disable.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Wireless Page – Wireless Security Panel

This panel lets you protect your wireless network against eavesdropping and intrusion. There are six wireless security options: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. These are briefly discussed here. For detailed instructions on configuring wireless security for the router, see "Setup for Wireless Security" in Chapter 1.

To be able to join the network, wireless devices must all use the same security method and wireless encryption key or keys.

Security Mode: Select the security method for your wireless network. If you do not want to use wireless security, keep the default, Disabled.

- **WPA Personal:** WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption.

  WPA Algorithms: WPA supports two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES. (AES is a stronger encryption method than TKIP.)

  WPA Shared Key: Enter the key shared by the router and your other network devices. It must have 8–63 characters.

  Group Key Renewal: Enter a key renewal period, which tells the router how often it should change the group (broadcast/multicast) encryption key. The default group key renewal period is 3600 seconds.

- **WPA Enterprise:** This version of WPA requires a RADIUS authentication server on the network. It is designed for large corporate networks.

WPA Algorithms: WPA supports two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES. (AES is a stronger encryption method than TKIP.)

RADIUS Server Address: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared by the router and the RADIUS server.

Key Renewal Timeout: Enter a key renewal period, which tells the router how often it should change the group (broadcast/multicast) encryption key. The default key renewal timeout is 3600 seconds.

- **WPA2 Personal:** WPA2 is a more advanced, more secure version of WPA.

  WPA Algorithms: WPA2 supports two encryption methods, TKIP and AES. Select the type of algorithm, AES, or TKIP+AES. The default selection is AES. Select TKIP+AES to allow connection by both WPA and WPA2 devices.

  WPA Shared Key: Enter the key shared by the router and your other network devices. It must have 8–63 characters.

  Group Key Renewal: Enter a key renewal period, which tells the router how often it should change the group (broadcast/multicast) encryption key. The default group key renewal period is 3600 seconds.

- **WPA2 Enterprise:** This version of WPA2 requires a RADIUS authentication server on the network. It is designed for large corporate networks.

  WPA Algorithms: WPA2 supports two encryption methods, TKIP and AES. Select the type of algorithm, AES, or TKIP+AES. The default selection is AES. Select TKIP+AES to allow connection by both WPA and WPA2 devices.

  RADIUS Server Address: Enter the IP address of the RADIUS server.

  RADIUS Port: Enter the port number of the RADIUS server. The default value is 1812.

  Shared Key: Enter the key shared by the router and the RADIUS server.

  Key Renewal Timeout: Enter a key renewal period, which tells the router how often it should change the group (broadcast/multicast) encryption key. The default key renewal timeout is 3600 seconds.

- **RADIUS:** RADIUS stands for Remote Authentication Dial-in User Service. As a

wireless security method, RADIUS means WEP used in combination with a RADIUS server.

RADIUS Server Address: Enter the IP address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server. The default value is 1812.

Shared Key: Enter the key shared by the router and the RADIUS server.

Default Transmit Key: If you will use 64-bit WEP, choose which key the router should use when transmitting. The default is **1**.

WEP Encryption: Select a level of WEP encryption, 64 bits (where the four keys must each be 10 hex digits long) or 128 bits (where the single key must be 26 hex digits long). The default is **64 bits 10 hex digits**.

Passphrase: If you wish to have keys automatically generated for you, enter a string of 1–16 characters here and then click **Generate**.

Key 1–4: If you did not enter a passphrase, enter the WEP key(s) manually.

- **WEP:** WEP stands for Wired Equivalent Privacy. This is a very early and relatively less secure wireless encryption method.

  Default Transmit Key: If you will use 64-bit WEP, choose which key the router should use when transmitting. The default is **1**.

  WEP Encryption: Select a level of WEP encryption, 64 bits (where the four keys must each be 10 hex digits long) or 128 bits (where the single key must be 26 hex digits long). The default is **64 bits 10 hex digits**.

  Passphrase: If you wish to have keys automatically generated for you, enter a string of 1–16 characters here and then click **Generate**.

  Key 1–4: If you did not enter a passphrase, enter the WEP key(s) manually.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Wireless Page – Wireless MAC Filter Panel

Wireless access can be controlled by filtering machines according to their MAC addresses.

Wireless MAC Filter: To filter wireless users by MAC address, either permitting or blocking access, click **Enable**. If you do not wish to filter users by MAC address, keep the default setting, **Disable**.

Prevent: Select this to block wireless access by MAC address. This button is selected by default.

Permit Only: Select this to allow wireless access by MAC address. This button is not selected by default.

Edit MAC Filter List: Click this to open the **MAC Address Filter List** window. In this window, you can list users, by MAC address, to whom you wish to provide or block access. For easy reference, click **Wireless Client MAC List** to display a list of current wireless network users by MAC address.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Wireless Page – Advanced Wireless Settings Panel

This panel is used to set up the router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Authentication Type: The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With Open System authentication, the sender and the recipient do NOT use a WEP key for authentication. With Shared Key authentication, the sender and recipient use a WEP key for authentication.

Basic Rate: The Basic Rate setting is not actually one rate of transmission but a series of rates at which the router can transmit. The router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the router can transmit at all standard wireless rates from 1 to 54 Mbps. Other options are **1-2 Mbps**, for use with older wireless technology, and **All**, when the router can transmit at all wireless rates. The Basic Rate is not the actual rate of data transmission. If you want to specify the router's rate of data transmission, configure the **Transmission Rate** setting.

Transmission Rate: The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the router automatically use the fastest possible data rate, with auto-fallback. Auto-fallback will negotiate the best possible connection speed between the router and a wireless client. The default value is **Auto**.

CTS Protection Mode: CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your Wireless-G products not being able to transmit to the router in an environment with heavy 802.11b traffic. This function boosts the router's ability to catch all Wireless-G transmissions but will severely decrease performance.

Frame Burst: Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To turn on the Frame Burst option, select **Enable**. The default is **Disable**.

Beacon Interval: The default value is 100. Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network.

DTIM Interval: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.

Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.

RTS Threshold: Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.

AP Isolation: This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the router but not with each other. To use this function, select **On**. AP Isolation is turned off by default.

Secure Easy Setup: On versions of the router with the SecureEasySetup feature, this control lets you enable or disable that feature.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Security Page – Firewall Panel

This panel is used to configure a firewall that can filter out various types of unwanted traffic.

Block Anonymous Internet Requests: This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default.

Deselect the feature to allow anonymous Internet requests.

Filter Multicast: Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the router will allow IP multicast packets to be forwarded to the appropriate computers. This feature is selected by default. Deselect this feature to disable it.

Filter Internet NAT Redirection: This feature uses port forwarding to block access to local servers from local networked computers. Select Filter Internet NAT Redirection to filter Internet NAT redirection. This feature is not selected by default.

Filter IDENT (Port 113): This feature keeps port 113 from being scanned by devices outside your local network. This feature is selected by default. Deselect this feature to disable it.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Security Page – VPN Passthrough Panel

This panel lets you allow or not allow Virtual Private Network tunnels using the IPSec, PPTP, or L2TP protocol to pass through the router's firewall.

IPSec Passthrough: Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the router, keep the default, **Enable**.

PPTP Passthrough: Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the router, keep the default, **Enable**.

L2TP Passthrough: Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the router, keep the default, **Enable**.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Access Restrictions Page – Internet Access Panel

This panel lets you block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and Web sites during specific days and times.

Internet Access Policy: Access is managed by policies. You can have up to 10 Internet access policies. Each has a number and a name. All the settings in the **Internet Access** panel are saved as one policy when you click **Save Settings**. After you have created some policies, use this drop-down list to select the policy you want

displayed. To delete a policy, display that policy and click **Delete**. To view all your policies, click **Summary**. Policies can be deleted using the **Internet Policy** Summary window by selecting them and clicking **Delete**. To return to the **Internet Access** panel, click **Close**.

Status: Policies are disabled by default. To enable a policy, display that policy and select **Enable**.

To create an Internet access policy:

1. **Select a number from the Internet Access Policy drop-down list.**
2. **To enable this policy, click Enable.**
3. **Enter a name in the Enter Policy Name box.**
4. **Click Edit List of PCs to select which PCs will be affected by the policy.**

   The **List of PCs** window will appear. You can identify a PC by its MAC address or IP address. You can also enter a range of IP addresses if you want this policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.

5. **Select the appropriate option, Deny or Allow, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs window.**
6. **Decide which days and what times you want this policy to be enforced.**

   Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.

7. **Input any Blocked Services and Website Blocking settings you wish to use.**
8. **Click Save Settings to save the policy's settings, or click Cancel Changes to cancel the policy's settings.**

Blocked Services: You can filter access to various services accessed over the Internet, such as FTP or Telnet, by selecting services from the drop-down lists next to **Blocked Services**. (You can block up to 20 services.) Then enter the range of ports you want to filter.

Add/Edit Service: If the service you want to block is not listed or you want to edit a service's settings, then click **Add/Edit Service**. The **Port Services** window will appear.

To add a service, enter the service's name in the **Service Name** box. Select its protocol from the **Protocol** drop-down list, and enter its range in the **Port Range**

boxes. Then click **Add**.

To modify a service, select it from the list on the right. Change its name, protocol setting, or port range. Then click **Modify**.

To delete a service, select it from the list on the right. Then click **Delete**.

When you are finished making changes in the **Port Services** window, click **Apply** to save the changes. If you want to cancel your changes, click **Cancel**. To close the **Port Services** window and return to the **Access Restrictions** panel, click **Close**.

Website Blocking by URL Address: If you want to block Web sites with specific URL addresses, enter each URL in a separate box next to **Website Blocking by URL address**.

Website Blocking by Keyword: If you want to block Web sites using specific keywords, enter each keyword in a separate box next to **Website Blocking by Keyword**.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Applications and Gaming Page – Port Range Forward Panel

This panel allows you to set up public services on your network, such as Web servers, FTP servers, e-mail servers, or other Internet applications. When a request for a particular service (indicated by the port number in the request) is received from the Internet, the router will forward it to the local machine specified here. Any machine to which you do port forwarding must have a fixed IP address (it cannot be a DHCP client).

Application: In this box, enter the name of the service or application. This is for your own reference only. Each name can contain up to 12 characters.

Start/End: This is the port range. Enter the number that starts the port range in the **Start** column and the number that ends the range in the **End** column. These two numbers can be the same.

Protocol: Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

IP Address: For each application, enter the IP address of the PC running the specific application.

Enable: Select Enable to enable port forwarding for the relevant application.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Applications & Gaming Page – Port Triggering Panel

This panel lets you set the router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the router, so that when the requested data returns through the router, the data is sent to the proper computer by way of IP address and port mapping rules.

Application: Enter the name of the application for which you will do port triggering. This name is for your own reference only.

Triggered Range: For each application, list the outgoing triggered port range. Check the application's documentation for the port number(s) needed.

Start Port: Enter the starting port number of the triggered range.

End Port: Enter the ending port number of the triggered range. This can be the same as the starting port.

Forwarded Range: For each application, list the incoming forwarded port range. Check the application's documentation for the port number(s) needed.

Start Port: Enter the starting port number of the forwarded range.

End Port: Enter the ending port number of the forwarded range. This can be the same as the starting port.

Enable: Select **Enable** to enable port triggering for the indicated application.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Applications and Gaming Page – DMZ Panel

The DMZ feature allows one local computer to be exposed to the Internet for use of a special-purpose application such as Internet gaming or videoconferencing. All incoming requests for services not handled by the port forwarding feature will be directed to this computer. This computer should have its own firewall for security. It also must have a fixed IP address (it cannot be a DHCP client).

To expose one PC, select **Enable**. Then, enter the computer's IP address in the **DMZ Host IP Address** box. This feature is disabled by default.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Applications and Gaming Page – QoS Panel

Quality of Service (QoS) assigns priority levels to improve the performance of high-bandwidth, latency-sensitive applications such as VoIP and videoconferencing. You can specify priority levels for particular machines, LAN ports, and applications, and you can enable/disable special QoS options for wireless links.

QoS: This section contains controls not specifically related to wireless QoS.

Enable/Disable: To enable QoS, select **Enable**. Otherwise, select **Disable**. QoS is disabled by default.

Upstream Bandwidth: In this box you can specify the maximum outgoing bandwidth that applications can utilize.

- **Device Priority:** Here you can assign priority to particular machines on your LAN. Enter a name (this is for your own reference only), enter the machine's MAC address, and then select its priority from the drop-down list.

- **Ethernet Port Priority:** These controls allow you to assign priority levels to the router's four LAN ports. For each port, select the priority and flow control setting.

  Priority: Select **High** or **Low** in the **Priority** column. All four LAN ports have been assigned low priority by default.

  Flow Control: If you want the router to control the transmission of data between network devices, select **Enabled**. To disable this feature, select **Disabled**.

- **Application Priority:** Applications are identified by their port (service) numbers, so they can be given the desired priority throughout their passage between the LAN and the WAN.

  Optimize Gaming Applications: Select this to automatically allow common game application ports to have a higher priority. These games include, but are not limited to: Counter-Strike, Half-Life, Age of Empires, Everquest, Quake2/Quake3, and Diablo II. The default setting is unselected.

  Application Name: Enter a name for the application in the Application Name box. This is for your reference only.

  Priority: Select **Low**, **Medium**, **High**, or **Highest** to assign a priority to the application. The default selection is **Low**.

  Specific Port #: Enter the port number for the application.

Wireless QoS: This section contains controls specific to wireless QoS.

WMM Support: Wi-Fi Multimedia (WMM), formerly known as Wireless Multimedia Extensions (WME), is a Wi-Fi Alliance certified feature, based on the IEEE 802.11e standard. This feature provides QoS to wireless networks. It is especially suitable for

voice, music, and video applications, for example,Voice over IP (VoIP), video streaming, and interactive gaming. If you have other devices on your wireless network that support WMM, select **Enabled**. Otherwise, keep the default, **Disabled**.

No Acknowledgement: This feature prevents the router from re-sending data if an error occurs. To use this feature, select **Enabled**. Otherwise, keep the default setting, **Disabled**.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Administration Page – Management Panel

The Administration page's Management panel lets you manage specific router functions for access and security.

- **Router Password:** This section controls access to the router's setup utility.

  Local Router Access: This lets you change the setup utility password.

  Router Password: Enter a new password for the setup utility.

  Re-enter to confirm: Enter the Password again to confirm.

- **Web Access:** These controls concern security and wireless access.

  Access Server: HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secure Sockets Layer) to encrypt data transmitted for higher security. Select **HTTP** or **HTTPS**. The default selection is **HTTP**.

  Wireless Access Web: If you are using the router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the router's setup utility. You will only be able to access the setup utility via a wired connection if you select **Disable**. Keep the default, **Enable**, to enable wireless access to the router's setup utility, or select **Disable** to disable wireless access to the utility.

- **Remote Router Access:** These controls concern access to the setup utility from the Internet.

  Remote Management: To be able to access the router remotely, from outside the network, select **Enable**. You will need to enter the router's password when accessing the router this way, as usual.

  Management Port: Enter the port number that will be open to outside access.

  Use https: To require the use of HTTPS for remote access, select this feature.

UPnP: UPnP is Universal Plug-and-Play. Some devices and applications use UPnP to change router settings so that information that would normally be blocked by the firewall or NAT can pass through.

UPnP: Keep the default, **Enable**, to enable the UPnP feature; otherwise, select **Disable**.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Administration Page – Log Panel

The router can keep logs of all traffic on your Internet connection.

Log: To disable the Log function, keep the default setting, **Disable**. To monitor traffic between the network and the Internet, select **Enable**.

When you wish to view the logs, click **Incoming Log** or **Outgoing Log**, depending on which you wish to view.

Click **Save Settings** to apply the new settings, or click **Cancel Changes** to cancel any unsaved changes.

Administration Page – Diagnostics Panel

The diagnostic tests (Ping and Traceroute) allow you to check the connections of your network components.

Ping: The Ping test checks the status of a connection. Click **Ping** to open the **Ping Test** window. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click **Ping**. The **Ping Test** window will show if the test was successful. To stop the test, click **Stop**. Click **Clear Log** to clear the displayed results. Click **Close** to return to the **Diagnostics** panel.

Traceroute: To test the performance of a connection, click **Traceroute** to open the **Traceroute Test** window. Enter the address of the PC whose connection you wish to test and click **Traceroute**. The **Traceroute Test** window will show if the test was successful. To stop the test, click **Stop**. Click **Clear Log** to clear the displayed results. Click **Close** to return to the **Diagnostics** panel.

Administration Page – Factory Defaults Panel

This panel lets you restore the router's factory default settings.

Restore Factory Defaults: To reset the router's settings to the default values, select **Yes**, and then click **Save Settings**. Any settings you have saved will be lost when the

default settings are restored.

Administration Page – Upgrade Firmware Panel

This panel lets you upgrade the router's firmware. Do not upgrade the firmware unless you are experiencing problems with the router or the new firmware has a feature you want to use.

Before upgrading the firmware, find out from your network equipment supplier how to obtain a router firmware file. Then obtain and extract the file.

Please select a file to upgrade: Click **Browse** and select the extracted firmware file. Then click **Upgrade** and follow the on-screen instructions.

Administration Page – Config Management Panel

Use this panel when you want to save a configuration file containing all of the router's current settings, and when you want to send a configuration file to the router to restore the settings in it.

Backup: To create a configuration file, click **Backup**. Then follow the on-screen instructions.

Please select a file to restore: Click **Browse** and select a configuration file. Then click **Restore** to send the file to the router.

Status Page – Language Panel

In multilingual versions of the router, this panel is used to select the interface language and to upgrade the language file held in the router. In the current version of the router, only English is available as an interface language.

Status Page – Router Panel

This panel displays information about the router's firmware and about router operation on the WAN.

Firmware Version: This is the version number of the router's current firmware.

Current Time: This shows the time, if the router is in contact with a time server.

MAC Address: This is the MAC address of the router's WAN port.

Router Name: This is the router name currently set in the **Basic Setup** panel.

Host Name: This is the host name, if any, currently set in the **Basic Setup** panel.

Domain Name: This is the domain name, if any, currently set in the **Basic Settings** panel.

Internet: The information shown in this section depends on the Internet connection type selected in the **Basic Setup** panel.

Click **Refresh** to update the on-screen information. When the router is set to obtain IP settings from your ISP by DHCP, there are also buttons to release and renew the router's DHCP lease.

Status Page – Local Network Panel

This panel displays information about router operation on the wired LAN.

MAC Address: This is the router's MAC address, as seen on your local Ethernet network.

IP Address: This shows the router's IP address, as it appears on your local Ethernet network.

Subnet Mask: This shows the subnet mask that the router is set to use on your local network.

DHCP Server: This shows whether the router's DHCP server function is currently enabled or disabled.

Start IP Address: This is the lowest IP address that the router will assign by DHCP on the local network.

End IP Address: This is the highest IP address that the router will assign by DHCP on the local network.

DHCP Clients Table: Clicking this button will open a window to show you which PCs are utilizing the router as a DHCP server. You can delete PCs from that list, and sever their connections, by checking a Delete box and clicking the **Delete** button.

Click **Refresh** to update the on-screen information.

Status Page – Wireless Panel

This panel displays information about router operation on your wireless network.

MAC Address: This is the router's MAC address, as seen on your local wireless network.

Mode: This shows whether the router's wireless interface is disabled, set for a Wireless-B/Wireless-G mixed environment, or set for Wireless-B only or Wireless-G

only.

SSID: This is the wireless network name currently set in the **Basic Wireless Settings** panel.

DHCP Server: This shows whether the router is acting as a DHCP server for wireless clients.

Channel: This is the wireless channel currently set in the **Basic Wireless Settings** panel.

Encryption Function: This shows the security mode currently selected in the **Wireless** page's **Wireless Security** panel.

Click **Refresh** to update the on-screen information.

Appendix A: Troubleshooting

You cannot connect to the Internet.

- Make sure the router is powered on. The POWER indicator should be shining a steady green and not flashing.
- If the POWER indicator is flashing, then power off all of your network devices, including the modem, router, and computers. Then power on each device in the following order: (1) Cable or DSL modem, (2) router, (3) computer.
- Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the router, and the modem must be connected to the Internet port on the router.

The modem does not have an Ethernet port.

It is is a dial-up modem. To use the router, you need a cable or DSL modem and a high-speed Internet connection.

The software you formerly ran to connect to your DSL service no longer works.

After you set up the router, it will automatically connect to your ISP, so you no longer need to connect with software from your ISP.

The DSL telephone line does not fit into the router's Internet port.

The router does not have a built-in modem. You still need your DSL modem in order to use the router. Connect the telephone line to the DSL modem and follow the instructions in Chapter 1.

When you start up your Web browser, you are prompted for a user name and password. If you want to get rid of the prompt, follow these instructions.

Launch the Web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

1. Open the **Tools** menu and choose **Internet Options**.
2. Click the **Connections** tab.
3. Select **Never dial a connection**.
4. Click **OK**.

The router does not have a coaxial port for the cable connection.

The router does not have a built-in modem. You still need your cable modem in order to use the router. Connect your cable to the cable modem and then follow the instructions in Chapter 1.

The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the router.

You need to modify the settings on the router.

Open the Web browser (for example, Internet Explorer or Firefox), and enter the router's IP address in the address bar (the default IP address is 192.168.1.1). When prompted, leave the **User Name** box blank and enter the password to the router (the default is **admin**). Click the appropriate tab to change the settings.

Appendix B: Specifications

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b
Channels	11 Channels (US, Canada) 13 Channels (Europe) 14 Channels (Japan)
Ports	WAN: One 10/100 RJ-45 Port LAN: Four 10/100 RJ-45 Switched Ports One Power Receptacle
Buttons	Reset
Cabling Type	Category 5 Shielded/Unshielded Twisted-pair
LEDs	Ethernet (1-4), Wireless, WAN, Power
UPnP able/cert.	Able
Security Features	Stateful Packet Inspection (SPI) Firewall, Internet AccessPolicies
Wireless Security	Wi-Fi Protected Access™ 2 (WPA2), WEP, Wireless MAC Filtering
Power Supply	External, 12V DC, 0.5A
Certifications	FCC, IC-03, CE, Wi-Fi (802.11b, 802.11g), WPA2, WMM
Operating Temp.	32° to 104° F (0° to 40° C)
Storage Temp.	-4° to 158° F (-20° to 70° C)
Operating Humidity	10% to 85%, Noncondensing
Storage Humidity	5% to 90%, Noncondensing

Appendix C: Warranty Information

Limited Warranty

The manufacturer warrants to You that, for a period of one year (the "Warranty Period"), the Product will be substantially free of defects in materials and workmanship under normal use. Your exclusive remedy and the manufacturer's entire liability under this warranty will be for the manufacturer at its option to repair or replace the Product or refund Your purchase price less any rebates. This limited warranty extends only to the original purchaser.

If the Product proves defective during the Warranty Period contact your network equipment supplier for assistance in obtaining a Return Authorization Number, if applicable. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND. If You are requested to return the Product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective Products to the manufacturer. The manufacturer pays for UPS Ground shipping from its facilities back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

This warranty does not apply if the Product (a) has been altered, except by the manufacturer, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by the manufacturer, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident. In addition, due to the continual development of new techniques for intruding upon and attacking networks, the manufacturer does not warrant that the Product will be free of vulnerability to intrusion or attack.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL THE MANUFACTURER BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF THE MANUFACTURER HAS BEEN ADVISED OF THE POSSIBILITY

OF SUCH DAMAGES. IN NO EVENT WILL THE MANUFACTURER'S LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT.

The foregoing limitations will apply even if any warranty or remedy provided under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.