Actiontec™

Wireless–Ready DSL Gateway

User Manual

Table of Contents

Introduction **1**
- Package Contents 1
- Minimum System Requirements 1
- Technical Support 2

Connecting the Gateway **3**
- Connecting the Power and DSL Cable 3
- Connecting to a Computer 5
- Connecting the Phone Filters 7
- Connecting Network Computers 8

Configuring the Gateway **11**

Using Qwest DSL **15**
- Connecting to the Internet 15
- Disconnecting from the Internet 15

Basic Setup **17**
- Basic Setup 17
- Gateway Features 19

Advanced Setup **23**
- Accessing Advanced Setup 23
- WAN IP Address 24
- Wireless Settings 27
- LAN IP Address 29
- DHCP Server 30
- Services Blocking 31
- Website Blocking 32
- VPN Pass Through 32
- Remote Management 33
- Port Forwarding 34
- DMZ Hosting 34
- MAC Address Cloning 35
- Status 35

Utilities **37**
- Web Activity Log 37
- DSL Settings 38
- Restore Default Settings 38
- Upgrade Firmware 38

Troubleshooting **41**

Reference **43**

Locating Computer Information 43
Locating Windows Operating System Files 44
Wiring Information 46
Computer Security 49
Securing the Gateway and Computer 49
Specifications 53
General 53
Wireless Operating Range 54
LED Indicators 54
Environmental 55
Glossary 57
Notices 61
Regulatory Compliance Notices 61
Modifications 61
Limited Warranty 63

Introduction 1

Thank you for purchasing the *Action*tec Wireless-Ready Gateway. The Gateway is the simplest way to connect a multiple number of computers to a single high-speed broadband connection. This easy-to-use product is perfect for the home office or small business. If you want to take your computing to the next level, the *Action*tec Wireless-Ready DSL Gateway is one of the keys to your success.

Package Contents

- Four-port Actiontec Wireless-Ready DSL Gateway
- Power adapter
- Ethernet cable
- USB cable
- Installation CD
- User guide and quick start guide
- Warranty and registration card

Minimum System Requirements

- Active DSL service
- Computer with an 10 Mbps or 10/100 Mbps Ethernet connection
- Microsoft Windows 95, Windows 98, Windows 98 Second Edition (SE), Windows Millennium Edition (Me), Windows NT 4.0, Windows 2000, Windows XP, Mac OS 7.1+, Mac OS 8.0+, Mac OS 9.0+, or Mac OS X+

☞ ***Note***: USB LAN port is not supported with Microsoft Windows 95, Windows NT 4.0, and Mac OS

- Internet Explorer 4.0 or higher (5.x recommended) or Netscape Navigator 4.0 or higher (4.7 recommended)
- TCP/IP network protocol installed on each computer

Technical Support

*Action*tec Electronics prides itself on making high-quality, durable, high-performance products. If you need assistance, the *Action*tec Technical Support Department is available every day from 6 A.M. to 11 P.M. (MST) to provide professional support.

_Action_tec Electronics, Inc.

760 N. Mary Avenue
Sunnyvale, CA 94085

Technical Support

Phone: 719-884-8300
E-mail: techsupp@actiontec.com
Internet: www.actiontec.com/support

Connecting the Gateway

4

The instructions that follow parallel closely with the steps contained in the Installation Buddy, which provides a visual guide to setting up the Gateway. It is recommended that the user run the Installation Buddy first, before attempting any other procedures.

To set up the Gateway, the user must first connect it to a computer via USB or Ethernet cable. After connecting this first computer, other computers can be added to the home network via USB, Ethernet, or wirelessly (see "Connecting Additional Computers on page xx).

Connecting the Power and DSL Cable

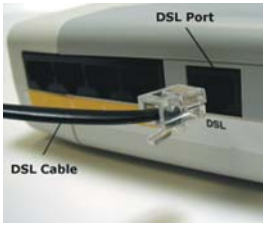
1. Get the **DSL Gateway** from your DSL Quick Start Kit and take it out of the bag.

2. Get the **Power Cord** out of the **Black Bag** and plug the smaller end of the Power Cord into the **Black Port** located on the back of the DSL Gateway.

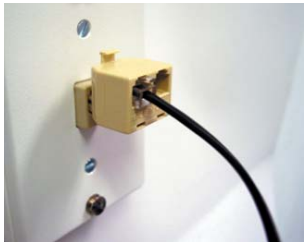
3. Confirm that the **Power Light** on the DSL Gateway is green.

4. Get the **Phone Line Splitter** out of the **Black Bag**.and plug the thin, rectangular end of the Splitter into the Phone Jack closest to your computer

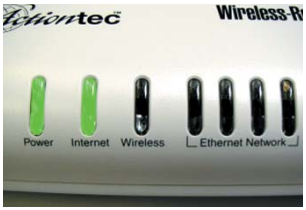
5. Get the **Black DSL Cable** out of the **Black Bag**. and plug one end of the DSL Cable into the **DSL Port** located on the back of the DSL Gateway.



6. Plug the other end of the **DSL Cable** into one of the two ports on the **Splitter** plugged into the **Phone Jack** closest to your computer.



7. Confirm that the **Power** and **Internet Lights** on the DSL Gateway are solid green.



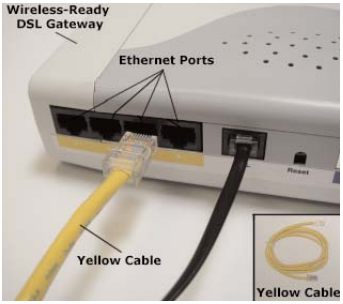
Note: If the Internet Light continues to blink, confirm you have received notification from your DSL Service Provider that your DSL service is on. Otherwise, contact your DSL Service Provider immediately.

Connecting to a Computer

There are two ways to connect the Gateway to a computer: Ethernet or USB cable.

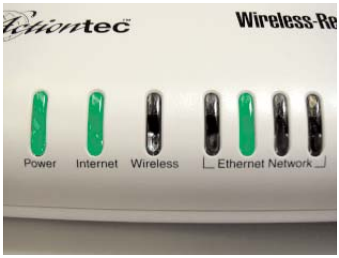
Ethernet

1. Get the **Yellow Cable** from the **Yellow Bag**, and plug one end of the Yellow Cable into one of the **Yellow Ports** on the back of the DSL Gateway. The Yellow Cable can be plugged into any of the Yellow Ports.



2. Plug the loose end of the **Yellow Cable** into the **Ethernet Port** on the back of the computer.

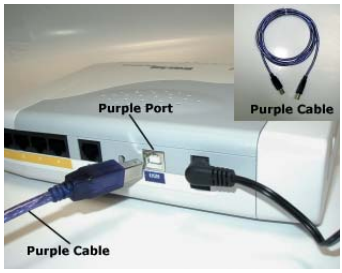
3. Confirm that one of the four **Ethernet Network Lights** on the DSL Gateway is green (this may take a few moments).



Note: If none of the Ethernet Network Lights glows green, check the Yellow Cable and ensure it has been connected properly.

USB

1. Get the **Purple Cable** from the **Purple Bag** and plug one end of the Purple Cable into the **Purple Port** on the back of the Gateway.



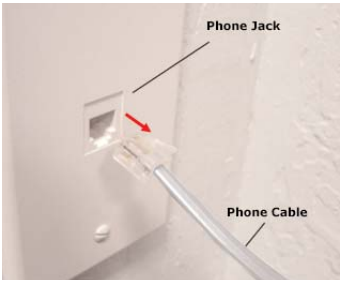
2. Plug the loose end of the **Purple Cable** into the **USB Port** on the front or back of your computer.

Connecting the Phone Filters

Phone filters separate the DSL signal from the voice signal on the phone line to allow the user to talk on the phone and be online at the same time. All devices using the same phone line (the same phone number) as the DSL connection require phone filters, including telephones, fax machines, caller ID boxes, and answering machines.

To install a phone filter:

1. Unplug the device (telephone, answering machine, etc.) from the phone jack.

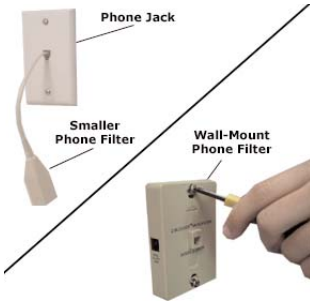


Caution: DO NOT unplug the black DSL Line from the phone jack near your computer.

2. Open the **Clear Bag** and remove the **phone filters**. The bag should contain four small phone filters and one wall-mount phone filter**.**

If a wall-mount telephone needs a phone filter, use the wall mount phone filter. Take the telephone off of the wall and install the wall-mount phone filter in the phone jack, securing it with the screws (see the figure on the next page, after Step 3). For other devices that need phone filters, use the small phone filters.

3. Plug a **phone filter** into the **phone jack**.



4. Plug one end of the **phone cable** into the **phone jack** and keep the other end attached to the device.

5. Repeat steps 1-4 for every other device that shares a phone line with the DSL connection.

Connecting Network Computers

Other computers can be connected to the Gateway to form a network. The network computers can be connected to the Gateway in three ways: Ethernet, USB, or wirelessly.

Ethernet

Use the procedure for connecting the first computer to the Gateway via Ethernet (see "Ethernet" on page xx) to connect network computers, substituting a standard, straight-through Ethernet cable for the yellow cable. Up to four network computers can be connected to the Gateway via Ethernet.

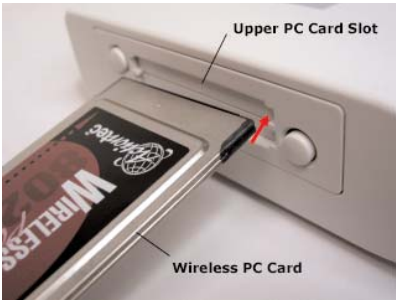
USB

Use the procedure for connecting the first computer to the Gateway via USB (see "USB" on page xx) to connect network computers, substituting a standard, USB cable for the purple cable. Only one computer can be connected to the Gateway via USB.

Wireless

Note: Computers to be added to the network wirelessly must have wireless capabilities (PCI wireless adapter, USB wireless adapter, etc.).

1. Insert an *Action*tec Wireless Adapter PC Card into the upper slot of the Gateway's PC Card slots.



2. Confirm the **Wireless LED** is glowing solid green.

3. To connect your wireless client (computer with wireless capabilities) to the Gateway, enter the following in the wireless client's settings:

   Network name (SSID): ACTIONTEC

   Encryption: None, or disabled

   Refer to the documentation that came with the wireless adapter for more information on how to set the Network name (SSID) and encryption.

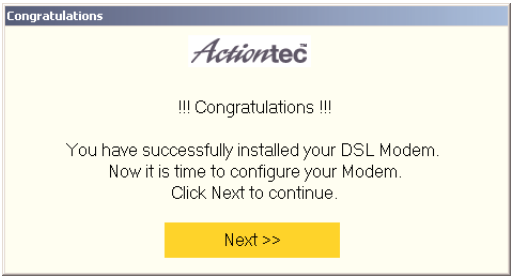
The computer is now connected to the network wirelessly.

Configuring the Gateway

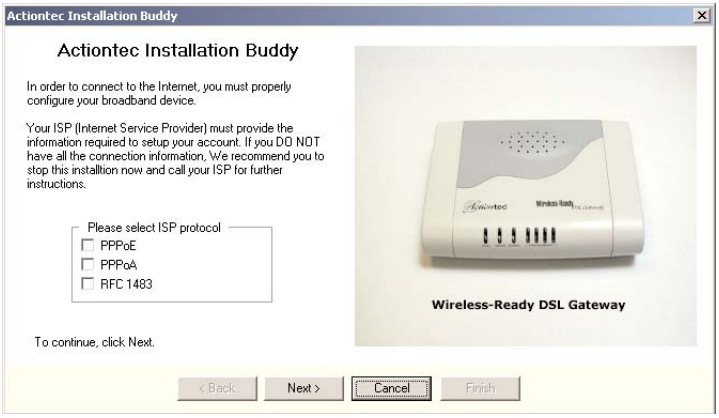
3

Once the Gateway has been connected to a computer, it must be configured. Use the following procedure.

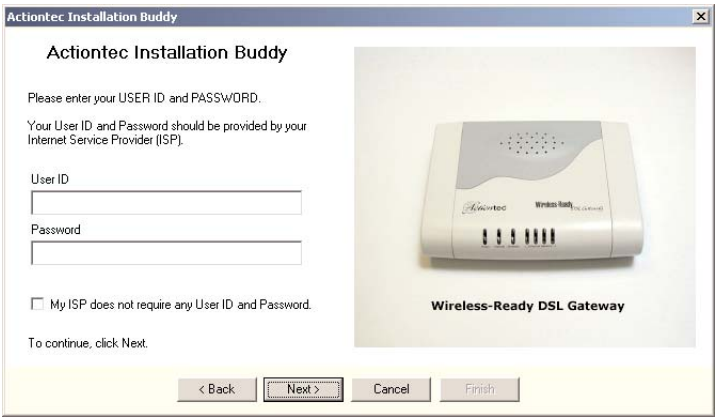
1. If you connected the DSL Gateway correctly, a "Congratulations" window appears. Click **Next**.



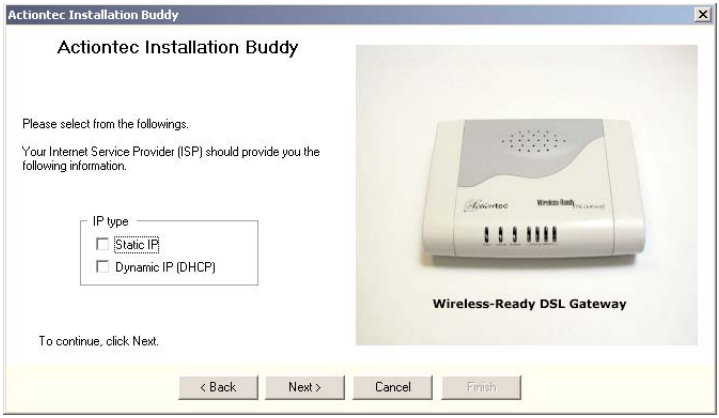
2. The first "Actiontec Installation Buddy" window appears. Read the instructions onscreen, select the type of **ISP protocol**, then click **Next**. (If you chose "RFC 1483," go to Step 4.)



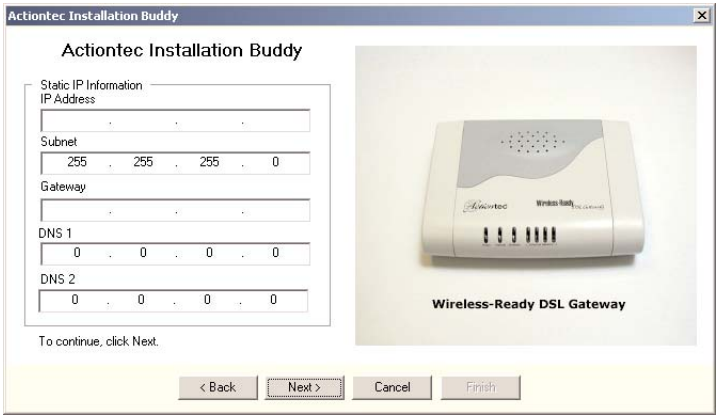
3. In the next window, type in the **User ID** and **Password**. If the ISP doesn't require this information, check the appropriate box. Click **Next**.



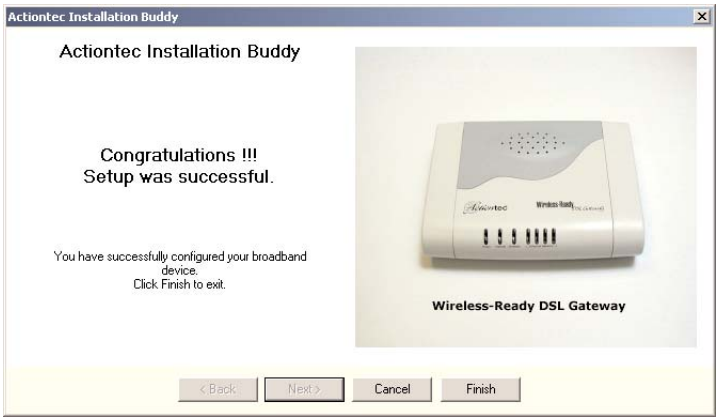
4. In the next window, select the type of Internet protocol your ISP connection uses (Static IP or Dynamic IP [DHCP]), then click **Next**. (If "Dynamic IP" was chosen, go to Step 6.)



5. In the next window, type in the **IP Address**, **Subnet**, **Gateway**, **DNS 1**, and **DNS 2** addresses in their respective text boxes. Depending on your connection, you may not have to type an address in every text box.



6. The last window appears. Click **Finish** to exit the Installation Buddy.



The installation of the DSL Gateway is complete.

Using Qwest DSL 4

Qwest DSL operates over home or business phone lines equipped with Qwest DSL service. For this reason, the Qwest DSL connection is not portable; it can't be accessed while away from home or business. To connect while traveling, ask the ISP about a dial-up account. Most Qwest DSL ISPs provide a dial-up account for free, while others charge a minimal fee.

Qwest DSL is a highly reliable service, but it is possible to have a dial-up connection in the unlikely event that problems arise with the DSL service. Most Qwest DSL ISPs provide a dial-up account for free. If not, there are a number of free Internet providers whose products make great backup Internet access in the unlikely event they are ever needed.

Connecting to the Internet

Whether connecting via Point-to-Point Protocol (PPPoE, PPPoA) or Bridging Mode (RFC 1483), after connecting and configuring the Gateway, the Internet connection is always on. Therefore, to connect or reconnect to the Internet, simply turn on your computer, open the Web browser and go to the Web site of your choice. No further set up is needed.

Disconnecting from the Internet

To disconnect from the Internet, close the Web browser. To completly disengage, turn off the computer.

Basic Setup

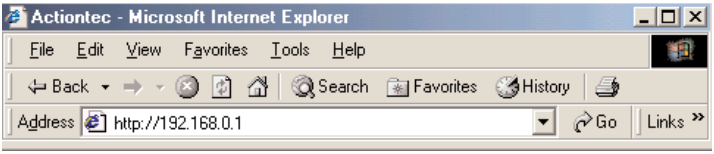
5

This section is a guide through a basic configuration of the Gateway, including how to connect the Gateway to the ISP.

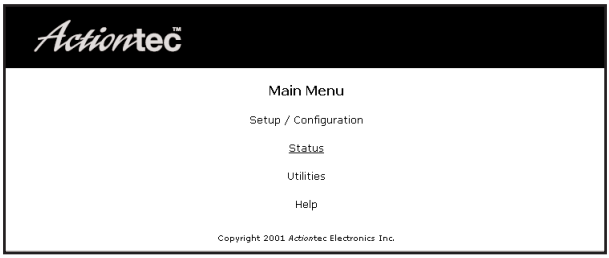
Basic Setup

To configure the gateway for basic operation:

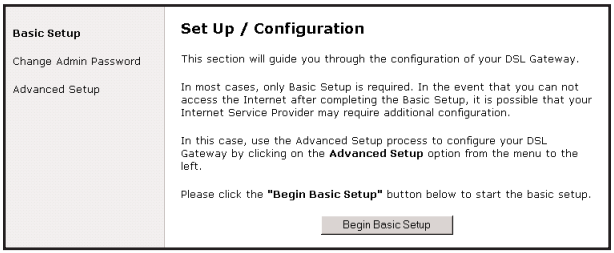
1. Open the Web browser. In the address bar, enter
   `http://192.168.0.1`
   then press **Enter** on the keyboard.



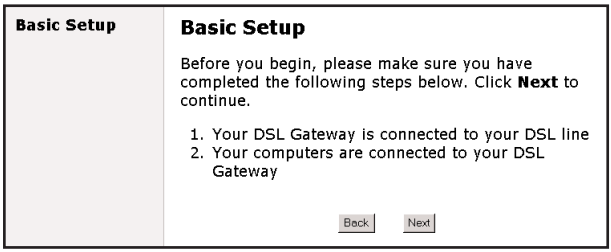
2. The "Main Menu" screen appears. Select **Setup/Configuration**.



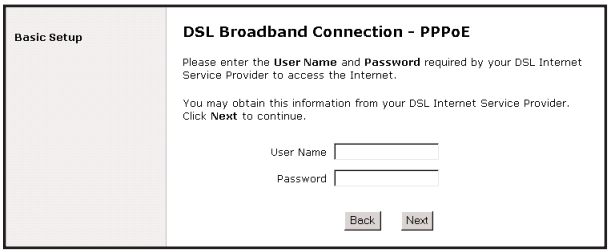
3. Follow the instructions in the "Set Up/Configuration" screen, then click **Begin Basic Setup**.



4. Complete the two steps listed in the "Basic Setup" screen, then click **Next**.



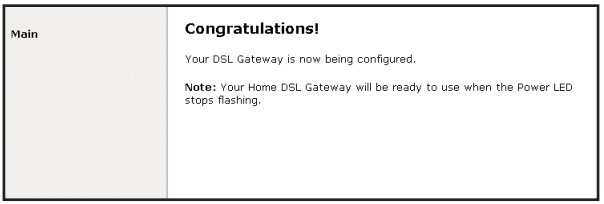
6. Enter the **User Name** and **Password** provided by the ISP in the "DSL Broadband Connection - PPPoE" screen. Click **Next**.



☞ ***Note***: If the ISP uses a connection method other than PPPoE (DHCP or Static IP, for example) see "Advanced Setup" to connect the Gateway.

7. Click **Save and Restart** in the "Save and Restart" screen.

8. The "Congratulations" screen appears. The Gateway is successfully configured.



The power LED flashes rapidly while the Gateway restarts, then glows steadily green when fully operational. The Gateway is now configured and users can start surfing the Web.
If an error stating the Web browser was unable to connect to the Internet appears, check the configuration settings. Ensure all the information required by the ISP is entered correctly.

Gateway Features

This section contains a quick description of the Gateway's LEDs and switches.

Power LED - The Power LED displays the Gateway's current status. If the Power LED glows steadily green, the Gateway is receiving power and fully operational. When the Power LED is rapidly flashing, the Gateway is initializing. If the Power LED is not illuminated when the power adapter is plugged in, the Gateway has suffered a critical error and technical support should be contacted.

Internet LED - When the Internet LED glows steadily, the Gateway is connected to the ISP.

Wireless LED - When the Wireless LED glows steadily, the Gateway is ready for wireless networking.

Ethernet Network LED - The Ethernet Network LEDs glow when a network link is established with a computer. A flashing LED signifies network traffic across the specific Ethernet connection.

Reset Switch - Depressing the reset switch for one or two seconds will reset the Gateway. To restore the Gateway's factory default settings, depress and hold the Reset Switch for approximately 10 seconds.

Advanced Setup

6

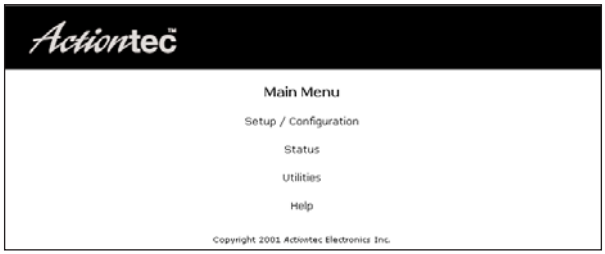
This section contains information concerning advanced configuration, such as wireless settings, remote management, and Web site blocking.

Accessing Advanced Setup

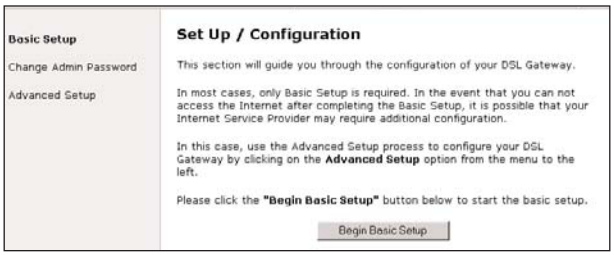
To access the Advanced Setup configuration screens, follow these instructions:

1. Open the Web browser. In the address bar enter:
   `http://192.168.0.1`
   then press **Enter** on the keyboard.

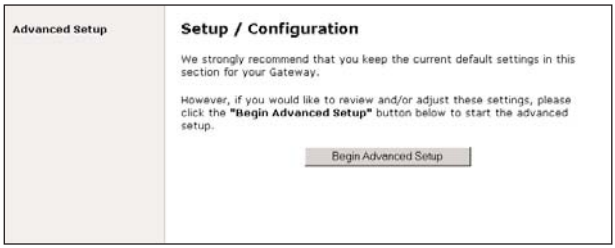
2. The "Main Menu" screen appears. Select **Setup/Configuration**.



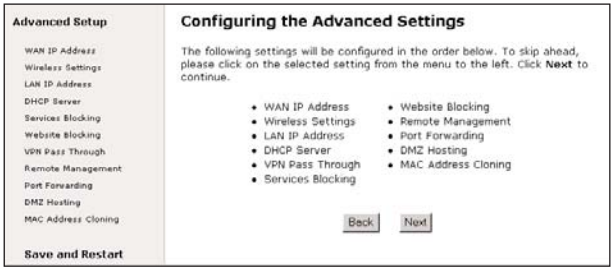
3. In the "Set Up/Configuration" screen, read the instructions, then select **Advanced Setup** from the menu on the left side.



4. In the next screen, read the recommendations. To perform an advanced setup on the Gateway, click **Begin Advanced Setup**.



5. The "Configuring the Advanced Settings" screen appears. To check all the settings, or if unsure of which settings to modify, select **Next**. To modify a specific configuration, click on its name in the menu bar on the left.



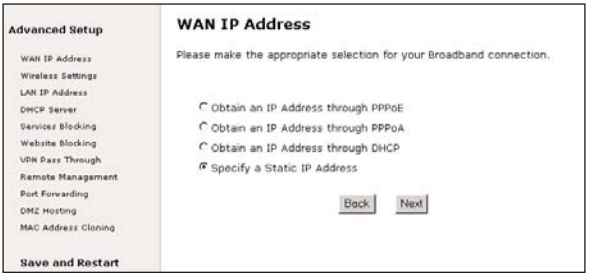
Note: Click **Save and Restart** on the bottom left-hand side of the screen after finishing the configuration of one or more of the Advanced Setup settings.

WAN IP Address

Selecting **WAN IP Address** in the "Advanced Configuration" screen generates the "WAN IP Address" screen. WAN IP Address allows manual set up of the IP address of the Gateway. There are three ways to do this: **Obtain an IP Address through PPPoE**, **Obtain an IP Address Through DHCP**, and **Specify a Static IP Address**.

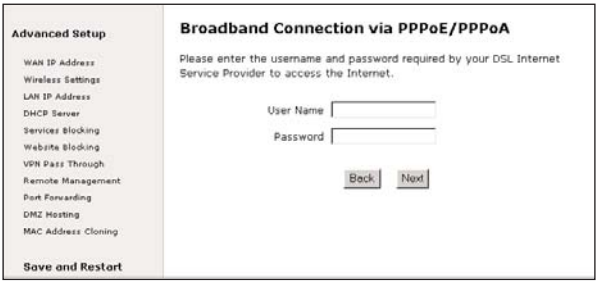
Note: Some DSL providers use PPPoE to establish communication with an end user, while others use static IP. Cable modem providers and other types of broadband Internet connections (such as fixed point wireless) may use either DHCP or Static IP address. If unsure about which connection is present, check with the ISP before continuing.

After selecting a connection type, click **Next** to continue configuring the connection.



Obtain an IP Address through PPPoE or PPPoA

Select this option to allow the Gateway to use the Point-to-Point over Ethernet (PPPoE) or Point-to-Point over ATM (PPPoA) protocol.

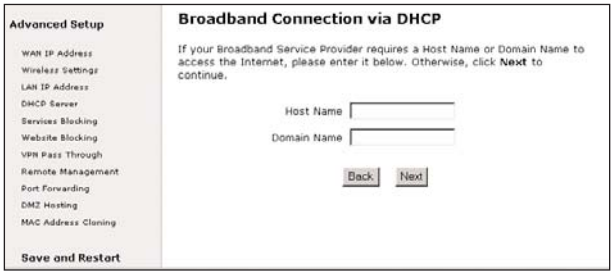


If a **User Name** and **Password** was entered during Basic Setup, it should be displayed in the "Broadband Connection via PPPoE/PPPoA" screen. If not, enter the information now. If the information is unavailable, contact the ISP.

Obtain an IP Through DHCP

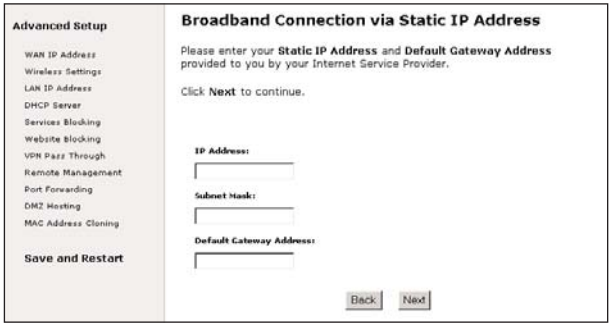
Select this option (used for cable modem configurations without a Static IP assigned by an ISP) to allow the modem to query the ISP and receive IP address and routing information. Some ISPs need to authenticate their end users with a **Host Name** and/or **Domain Name**. If this is the case, check with the ISP for a host name and domain name and enter them in the "Broadband Connection via DHCP" screen. If the ISP does not require these settings, leave the text boxes blank.

☞ ***Note***: Host and domain name information may also be accessed from the computer originally connected to the cable modem.



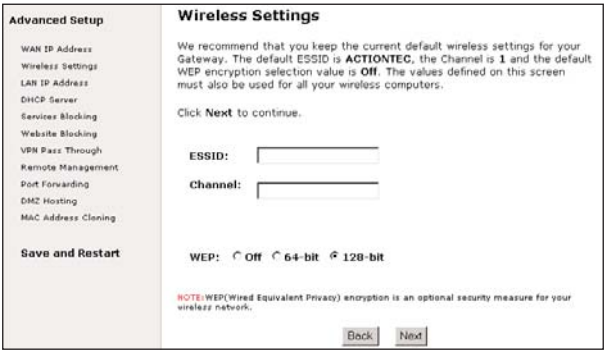
Specify a Static IP Address

Select this option if assigned a static (specific) IP Address by the ISP. Enter the **IP Address**, along with the **Subnet Mask** and **Default Gateway Address** (also provided by the ISP), in the "Broadband Connection via Static IP Address" screen. If required to provide a **Host Name** and **Domain Name**, enter them here as well.



Wireless Settings

Selecting **Wireless Settings** in the "Advanced Configuration" screen generates the "Wireless Settings" screen. Modify the wireless capabilities of the Gateway here.



ESSID

ESSID is the network name assigned to the wireless network. The factory default setting is "ACTIONTEC." Although *Action*tec recommends keeping the default value intact, the ESSID value can be modified, using any combination of alphanumeric characters (i.e., A-Z, a-z, 0-9). All wireless-capable computers included on the Gateway's wireless network must have this same ESSID value. (For the *Action*tec 802.11b Wireless PC Card, the ESSID value must be the same as the SSID value.)

Channel

Channel assigns the frequency band at which the Gateway communicates. In the United States, use channels 1-11. (The factory default value is set to 1.)

Wireless Equivalent Privacy

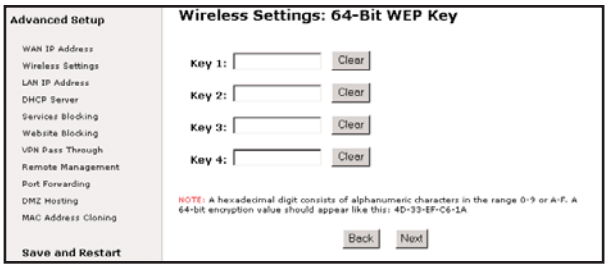
Wireless Equivalent Privacy (WEP) is an encryption method used with the 802.11b standard to ensure data security over wireless networks. The Gateway offers three levels of WEP: Off, 64-bit, and 128-bit. If encryption is not required, *Action*tec recommends selecting **Off** (the factory default setting). Encryption is not required for wireless operation, and can reduce network performance. If selecting **64-bit** or **128-bit** encryption, click **Next** to continue WEP configuration.

Off

Selecting **Off** disables encryption. Selecting this option allows any computer with wireless capability and the correct ESSID value to join the wireless network.

64-bit WEP

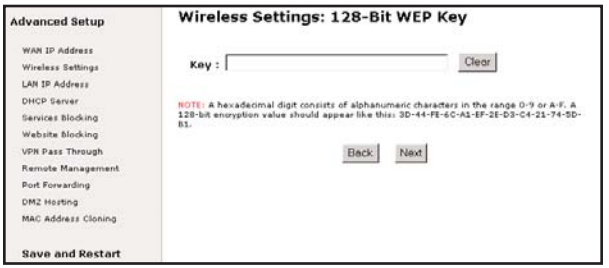
64-bit WEP requires four separate keys. Each key comprises five hexadecimal digit pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 64-bit WEP key is: 4E-A3-3D-68-72. To create a set of 64-bit WEP keys, enter five hexadecimal digit pairs in each **Key** text box (**Key 1**, **Key 2**, **Key 3**, **Key 4**). After activating 64-bit WEP on the Gateway, a computer with wireless capability can join the network only if these same keys are entered in the computer's wireless encryption scheme.



128-bit WEP

128-bit WEP requires one key of 13 hexadecimal pairs. A hexadecimal digit consists of alphanumeric characters ranging from 0-9 or A-F. An example of a 128-bit WEP key is: 3D-44-FE-6C-A1-EF-2E-D3-C4-21-74-5D-B1. To create a 128-bit WEP key, enter 13 hexadecimal digit pairs in the **Key** text box. After activating 128-bit WEP on the Gateway, a computer with wireless capability can join the network only if this key is entered in the computer's wireless encryption scheme.

Note: Not all wireless PC Cards support 128-bit WEP. Ensure that all PC Cards installed in the networked computers support 128-bit WEP before activating.



LAN IP Address

Selecting **LAN IP Address** in the "Advanced Configuration" screen generates the "LAN IP Address" screen. The value in the **LAN IP Address** text box is the IP address of the Gateway as seen on the network.
The LAN IP address of the Gateway can be modified, but *Action*tec recommends keeping the default factory setting (192.168.0.1).

Note: If the Gateway's LAN IP Address is modified, verify the DHCP Server range is within the same subnet. For more information, see "DHCP Server Configuration."

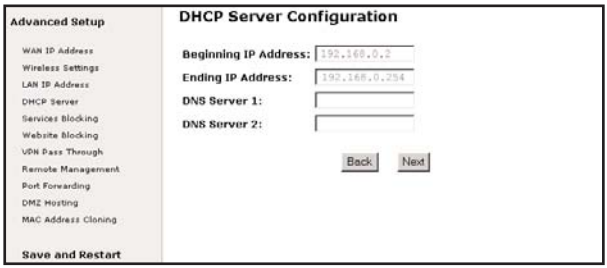
DHCP Server

Selecting **DHCP Server** in the "Advanced Configuration" screen generates the "DHCP Server" screen. The Gateway has a built-in DHCP (Dynamic Host Configuration Protocol) server that automatically assigns a different IP address to each computer on the network, eliminating IP address conflicts.
The factory default setting is **On**. To disable the DHCP Server, select **Off**.

*Action*tec strongly recommends leaving the DHCP Server option **On**. If the DHCP Server option is **Off**, ensure the IP addresses of the networked computers are on the same subnet as the IP address of the Gateway. For more information, see "DHCP Server Configuration."

DHCP Server Configuration

Clicking **Next** in the "DHCP Server" screen generates the "DHCP Server Configuration" screen. Change IP address range and DNS server information here.



Beginning IP Address - the IP address at which the DHCP server starts assigning IP addresses. *Action*tec recommends keeping the factory default setting (192.168.0.2).

Ending IP Address - the IP Address at which the DHCP Server stops assigning IP addresses. *Action*tec recommends keeping the factory default settings (192.168.0.254).

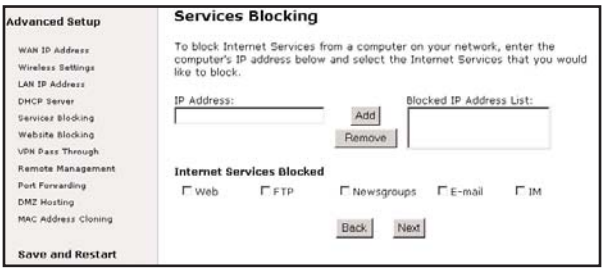
The beginning and ending IP addresses define the IP address range of the Gateway. If the default values are left intact, the Gateway supplies a unique IP address between 192.168.0.2 and 192.168.0.254 to each computer on the network. Note that the first three groups of numbers of the addresses are identical; this means they are on the same subnet. The IP address of the Gateway must be on the same subnet as the IP address range it generates. For instance, if the Gateway's IP address is changed to 111.33.222.1, set the beginning IP address to 111.33.222.2, and the ending IP address to 111.33.222.254.

DNS Server 1 - the primary DNS server provided by the ISP. If the ISP provided DNS server information, enter it here. If not, leave the text box intact.

DNS Server 2 - the secondary DNS provided by the ISP. If the ISP provided secondary DNS server information, enter it here. If not, leave the text box intact.

Services Blocking

Selecting **Services Blocking** in the "Advanced Configuration" screen generates the "Services Blocking" screen.

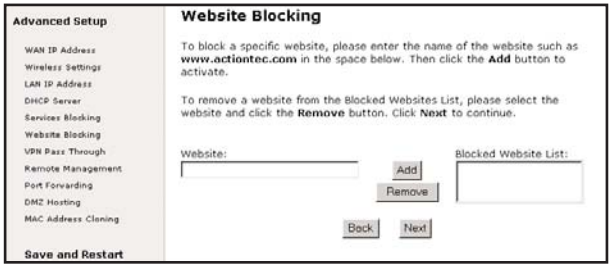


To modify Internet privileges (Web, FTP, Newsgroups, etc.) for the computers on the network:

1. Enter the computer's IP address in the **Enter IP Address:** text box.
2. At the bottom of the screen, select the Internet service(s) to be blocked.
3. Click **Add** to enter the computer's IP address in the "Blocked IP Address List" text box.
4. To remove blocked services, select the computer's IP address in the "Blocked IP Address List" text box and click **Remove**.

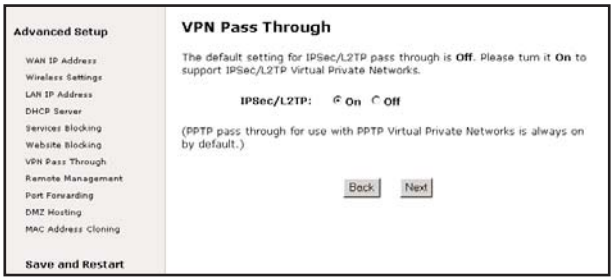
Website Blocking

Selecting **Website Blocking** in the "Advanced Configuration" screen generates the "Website Blocking" screen. This feature enables the Gateway to block Web sites to all computers on the network. To block a Web site, enter the address of the Web site in the "Website" text box and click **Add**. The blocked Web site address will be displayed in the "Blocked Website List" text box, and will not be available to computers on the network. To remove a blocked Web site, click on it in the "Blocked Website List," then click **Remove**.



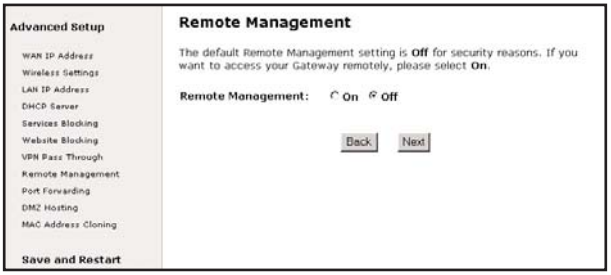
VPN Pass Through

Selecting **VPN Pass Through** in the "Advanced Configuration" screen generates the "VPN Pass Through" screen. To set up Virtual Private Networking (VPN) using IPSec/L2TP (which allows multiple, client-initiated VPN pass-through sessions), select **On**. Note that VPN via PPTP pass through is always active.



Remote Management

Selecting **Remote Management** in the "Advanced Configuration" screen generates the "Remote Management" screen. Remote Management allows access to the Gateway through the Internet via another computer. *Action*tec recommends leaving the Remote Management **Off** (the factory default setting).

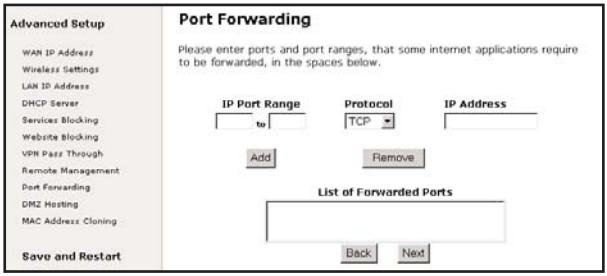


To access the Gateway from the Internet, activate Remote Management by selecting **On** and writing down the WAN IP address of the Gateway (see "WAN IP Address"). On a computer outside of the network, open a Web browser and enter the Gateway's WAN IP address in the address text box. The Gateway's Main Menu (or a password prompt, if a password has been set) appears in the browser window.

Port Forwarding

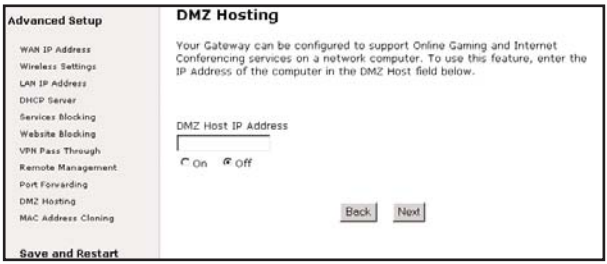
Selecting **Port Forwarding** in the "Advanced Configuration" screen generates the "Port Forwarding" screen. Port forwarding allows certain programs to bypass the Gateway's built-in firewall, allowing access to parts of the network (for hosting a Web or ftp server, for example). To use port forwarding, enter the IP port range in the "IP Port Range" text boxes. (If more than 10 ports are needed, *Action*tec recommends using DMZ Hosting. See "DMZ Hosting," below, for more information.) Choose the protocol type from the "Protocol" list box, then enter the IP address of the computer on the network to be used as a host. Click **Add**. The forwarded ports appear in the "List of Forwarded Ports" text box. For a list of programs that use port forwarding, as well as port numbers used, see "Appendix C - Program and Port List."

To remove forwarded ports, highlight them, then click **Remove**.



DMZ Hosting

Selecting **DMZ Hosting** in the "Advanced Configuration" screen generates the "DMZ Hosting" screen. To use DMZ hosting, enter the IP address of the computer on the network to be used as a DMZ host in the "DMZ Host IP Address" text box, then click **On**.



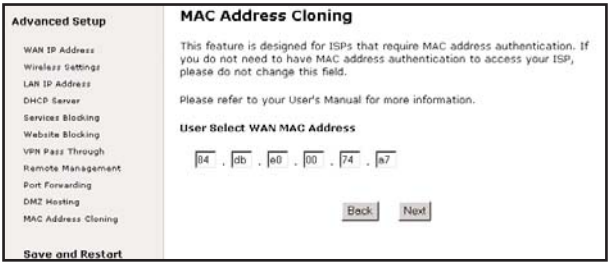
DMZ hosting is used to support online gaming and Internet conferencing services. These programs usually require multiple open ports, making the network accessi-

ble from the Internet. DMZ hosting symbolically places the DMZ host computer outside of the Gateway's network. Access to the network resources while DMZ hosting is active is blocked. *Action*tec recommends activating DMZ hosting only as long as necessary.

Warning: The DMZ Host computer will be vulnerable to computer hackers on the Internet while in DMZ mode.

MAC Address Cloning

Selecting **MAC Address Cloning** in the "Advanced Configuration" screen generates the "MAC Address Cloning" screen. A MAC (media access control) address is an identifier unique to every networkable device. Some ISPs require a MAC address to validate a computer's permission to be on their network. If the ISP requires this information, obtain the MAC address of the computer originally configured for the ISP (see Appendix D for instructions to determine the computer's MAC address). Enter the MAC address in the "User Select WAN MAC Address" text boxes in the "MAC Address Cloning" screen.



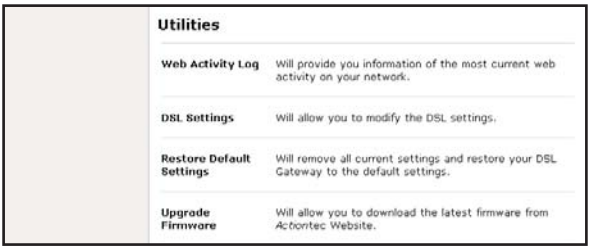
Status

After configuring the Gateway, settings can be viewed by selecting **Status** in the Main Menu. The "Current Status" screen appears, displaying many of the Gateway's settings. No settings (other than connecting or disconnecting from the Internet) can be changed from the Current Status screen.

Utilities

7

To access the Gateway's utilities select **Utilities** from the "Main Menu" screen. The "Utilities" screen appears.



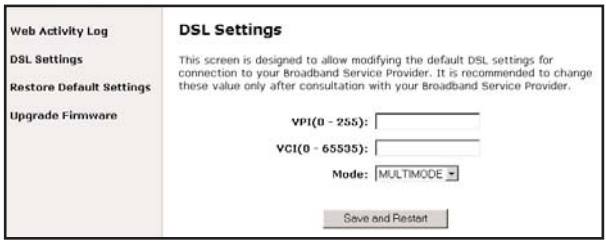
From here, the Web activity log can be viewed, the DSL settings changed, the Gateway's factory default settings restored, and the Gateway's firmware upgraded.

Web Activity Log

The Web Activity Log provides information about the Web sites each computer on the Gateway's network has visited. To access the Web Activity Log, select **Web Activity Log** from the "Utilities" screen.

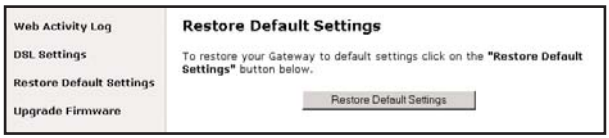
DSL Settings

To access DSL Settings, select **DSL Settings** from the "Utilities" screen. The Gateway's VPI, VCI, and Mode settings can be changed from here. *Action*tec recommends not changing these values without consulting the ISP.



Restore Default Settings

To restore the Gateway to its factory default settings, select **Restore Default Settings** from the "Utilities" screen. When the "Restore Default Settings" screen appears, click **Restore Default Settings**. Any changes made to the Gateway's settings will be lost and the factory default settings will be restored. During this process, the Gateway's power LED flashes and the Gateway is disabled. When the power LED stops flashing and glows steadily green, the Gateway is fully operational.



Upgrade Firmware

Selecting **Upgrade Firmware** in the "Utilities" screen generates the "Upgrade Firmware" screen. *Action*tec periodically posts firmware upgrades to enhance the Gateway's capabilities.

To upgrade the Gateway's firmware:

1. Click the link in the "Upgrade Firmware" window and download the upgrade files to the hard drive of the computer.
2. Double-click on the upgrade file, named "upgrade.exe."
3. Enter the IP address of the Gateway and click **Start**. The upgrade process begins.
4. After the upgrade is complete, unplug the power adapter from the Gateway, then plug it back in again.
5. When the power LED stops flashing and glows steadily green, the Gateway is fully operational.
6. Reconfigure the Gateway settings.

Troubleshooting 8

This chapter contains a list of problems that may be encountered while using the Gateway, and solutions to overcome the problem.

LAN Connection Failure

- Ensure the Gateway is properly installed, the LAN connections are correct, and the power is on.
- Confirm the computer and Gateway are on the same network segment. If unsure, let the computer get the IP address automatically by initiating the DHCP function (see "DHCP Server"), then verify the computer is using an IP address within the default range (192.168.1.2 through 198.168.1.254). If the computer is not using an IP address within the range, it will not connect to the Gateway.
- Ensure the Subnet Mask address is set to 255.255.255.0 by clicking **Status** in the "Main Menu" screen.

Cannot Connect to the Internet

- Ensure both ends of the power adapter and network cables are properly connected and the status LEDs on the front panel are working properly.
- If running Windows 98, check the computer's TCP/IP settings. Select **Start**, **Run**, enter

  `winpcfg`

  in the"Open" text box, then press **Enter** on the keyboard. The computer should have an IP address in the default range (192.168.1.2 through 198.168.1.254).
- Ensure the Subnet Mask address is set to 255.255.255.0 by clicking **Status** in the "Main Menu" screen.
- Verify the Gateway's settings are the same as the computer by clicking **Status** in the "Main Menu" screen.

Time out error occurs when entering a URL or IP Address

- Verify all the computers are working properly.
- Ensure the IP settings are correct.
- Ensure the Gateway is on and connected properly.
- Verify the Gateway's settings are the same as the computer by clicking **Status** in the "Main Menu" screen.
- Check the cable/DSL modem by attempting to connect to the Internet.

Reference

A

This appendix contains information about various topics, including accessing information about your Windows computer and wiring under special circumstances.

Locating Computer Information

The following procedure is valid for Windows 98, 98 SE, Me, NT 4.0, 2000 and XP.

1. From the desktop, right-click on **My Computer**.
2. Select **Properties** from the menu that appears.
3. When the "System Properties" window appears, select **General**.
   The version of the operating system, processor type, and amount of RAM installed in the computer are listed here.
4. Close the System Properties window.
5. From the desktop, double-click on **My Computer**.
6. Right-click the icon representing your hard disk. For example: Local Disk (C:).
   Some computers have multiple hard disks.
7. From the menu that appears, select **Properties**.
8. When the window appears, select **General**.
9. The Free space value is the available space on the hard disk.
10. Close all windows.

Locating Windows Operating System Files

If the operating system files reside on the hard drive of the computer, follow the instructions below to locate them. If the files are not on the hard drive, they must be loaded from the installation disks.

Windows 98, 98 SE

1. From the desktop, click **Start**.
2. When the menu appears, select **Find,** then **Files or Folders**.
3. When the "Find: All Files" window appears, select **Name & Location**.
4. In the "Named" text box, enter:
   `*.cab`
5. Click the **down arrow** next to the "Look In" text box and select **My Computer** from the list that appears.
6. Click **Find Now**.
7. When the search is complete, note the directory path that appears most often in the "In Folder" column. For example: C:\WINDOWS \SYSTEM.
8. The Windows operating system files are located in this directory. Write down the directory path for future reference.
9. Close the Find: All Files window.

Windows Me, 2000

1. From the desktop, click **Start**.
2. Select **Search**, then **For Files and Folders**.

3a. ***Windows Me***: The "Search Results" window appears. In the "Search for files or folders named" text box, enter:
`*.cab`

3b. ***Windows 2000***: The "Search Results" window appears. In the "Search for files or folders named" text box, enter:
`i386`

4. Click the **down arrow** next to the "Look in" text box and select **My Computer** from the list that appears.

5. Click **Search Now**.

6a. ***Windows Me***: When the search is complete, note the directory path that appears most often in the "In Folder" column. For example: C:\WINDOWS \OPTIONS\INSTALL.

6b. ***Windows 2000***: When the search is complete, note the directory path that appears most often in the "In Folder" column. For example: C:\WINNT \Driver Cache.

7. The Windows operating system files are located in this directory. Write down the directory path for future reference.

8. Close the Search Results window.

Windows NT 4.0

1. From the desktop, click **Start**.

2. When the menu appears, select **Find,** then **Files or Folders**.

3. When the "Find: All Files" window appears, select **Name & Location**.

4. In the "Named" text box, enter:

```
i386
```

5. Click the **down arrow** next to the "Look In" text box and select **My Computer** from the list that appears.

6. Click **Find Now**.

7. When the search is complete, note the directory path that appears most often in the "In Folder" column. For example: C:\.

8. The Windows operating system files are located in this directory. Write down the directory path (followed by "i386") for future reference.

9. Close the Find: All Files window.

Windows Me, 2000

1. From the desktop, click **Start**.
2. Select **Search**, then **For Files and Folders**.
3. The "Search Results" window appears. In the panel at left titled "What do you want to search for?", click **All files and folders**.
4. Another panel, titled "Search by any or all of the criteria below" appears. In the "Look in" text box, click the **down arrow** and select **My Computer** from the menu that appears.
5. In the "All or part of the file name" text box, enter:
   i386
6. Click **Search**.
7. When the search is complete, note the directory path that appears most often in the "In Folder" column. For example: C:\WINDOWS \Driver Cache\.
8. The Windows operating system files are located in this directory. Write down the directory path (followed by "\i386") for future reference.
9. Close the Search Results window.

Wiring Information

This section contains information about how to connect the Gateway to a two-line phone, a security alarm system, an automatic water meter, and a PBX or key phone system sharing a line with Qwest DSL.

Two-Line Phone

If Qwest DSL is connected in a location with two phone lines using two separate phone numbers, the DSL phone filters must be installed on the correct phone line.

In most two-line phone setups, the red and green lines connect Line 1, while the yellow and black lines connect Line 2. If a phone filter is installed between a two-line phone jack and a telephone with two-line capability, only Line 1 will be filtered and operational (because the phone filter connects the red and green wires only), while Line 2 will be completely disconnected.

The solution is twofold: 1) the phone filter must be installed to filter the line with Qwest DSL; and 2) the second line must be wired to bypass the phone filter. The

easiest way to do this is to purchase a pair of two-line modular adapters, a line-cord coupler, and some short lengths of phone cable, available at any telephone supply retailer.

☞ ***Note***: Do not purchase a 1-line modular adapter or line splitter. Installing either of these items results in two phone jacks on Line 1, and no access to Line 2.

1. Disconnect the telephone from the two-line phone jack.
2. Install one of the two-line modular adapters (modular adapter #1) in the phone jack
3. If Qwest DSL is on Line 1, install the phone filter in the Line 1 jack of modular adapter #1.
4. Install a short length of phone cable between the phone filter and the Line 1 jack of the other two-line modular adapter (modular adapter #2).
5. Install a short length of phone cable between the Line 2 jacks of modular adapters #1 and #2.
6. Connect the line-cord coupler to 2-line modular adapter #2.
7. Install a short length of phone cable between the line-cord coupler and the telephone.

If Qwest DSL is on Line 2, use the same procedure, but install the phone filter on Line 2.

Security Alarm System

If the user plans to connect Qwest DSL at a location that has two phone lines, Qwest DSL must be installed on the phone line that does not service the alarm system.

If the alarm system and Qwest DSL must share the same phone line, contact Qwest Sales to order a technical install. Special wiring needs are required when Qwest DSL and the alarm system share the same phone line. Qwest Sales telephone numbers are listed at the back of this manual.

Automatic Water Meter

If an automatic water meter and Qwest DSL share a phone line, a DSL phone filter must be installed on the water meter. If needed, contact the water company for assistance in connecting the phone filter.

PBX or Key System

To share Qwest DSL with telephone line in an office PBX or key system:

1. In the building's phone closet, splice (into two lines) the telephone line on which Qwest DSL is installed.
2. On one of the spliced lines, connect the Gateway. The Gateway should be connected as close as possible to the telephone network to assure a strong signal.
3. Connect the Gateway to a computer or LAN hub via Ethernet cable.
4. On the other spliced line, install the DSL phone filter, then wire normally through the PBX or key system unit to the telephone.

Computer Security

B

The Internet is a giant network of computers all over the world. When a computer is connected to the Internet, it can exchange information with any other computer on the Internet. This lets the user send e-mail, surf the World Wide Web, download files, and buy products and services online, but it also makes the computer vulnerable to attack from persons intent on doing malicious mischief. Unless access to the computer is controlled, someone on the Internet can access the information on the computer, and they can damage or destroy that information.

Securing the Gateway and Computer

The Qwest DSL web site explains how to secure your computer and modem from attack. Go to

http://www.qwest.com/dsl/

then click **Security**.

The topics featured include:

- Modem security
- Computer operating system security
- Physical system security

The following sections briefly discuss some major security concerns and explain the risks involved. Please go to the Qwest DSL web site for full explanations and instructions.

Comparing DSL Service with a Dial-Up Modem

With a dial-up modem, a computer user makes an Internet connection by dialing a telephone number, surfs the Internet for a period of time (maybe a few minutes, maybe all day), and then disconnects the dial-up modem. No one on the Internet can access a computer that is not connected to the Internet.

Unlike a dial-up modem, DSL service is "always on." The connection is always available – there is no need to dial a phone number to access the Internet. The computer can be connected to the Internet all the time.

With both types of Internet connections, access to the computer must be controlled to make sure someone on the Internet doesn't access the information on the computer. The longer the computer is connected to the Internet, the easier it is for someone on the Internet to find the computer and attempt to access it without permission. DSL service also provides fast Internet connections. This not only improves Internet performance, it also improves Internet performance for anyone attempting to access the computer.

Gateway Security

If connecting to the ISP through Point-to-Point Protocol (PPP), be sure to provide the Gateway an password. If a password is not set, someone on the Internet can access the Gateway and change its configuration or steal your PPP login name and password. For instructions on setting the password, see the "Advanced Setup chapter.

If connecting to the ISP through bridging mode, the Gateway is safe from unwarranted and illegal intrusion.

Computer Security

To protect the valuable information on the computer, review the following topics. These topics cover software programs and operating system features affecting the security of the computer's data.

Anti-Virus Programs

The computer should have an anti-virus program, and the virus definitions should be updated on a regular basis – at least once a month.

E-Mail Attachments

Never run a program received as an attachment to an e-mail message unless the program is known to be safe. A program from an unknown source can delete all the files on the computer's hard disk or install a "backdoor" software application that lets people on the Internet gain access to the computer without permission.

Internet Browsers

Always exit the Internet browser (for example, Internet Explorer or Netscape Navigator). Never "minimize" the browser or leave it open in the background. Breaking into a computer is easy when an Internet browser is running.

Network Applications

Network applications (such as software programs) that allow remote access to the computer also make the computer vulnerable to access from other people on the Internet. If using a network application that allows remote access, install a firewall.

Electronic Security

Here are two methods to secure your computer electronically.

Network Address Translation

If a local area network and a PPP connection to the ISP using dynamic IP addresses through a DHCP server are being used, Network Address Translation (NAT) is being used. NAT provides a very basic level of security. See the Qwest DSL LAN book for more information about NAT.

Firewalls

The safest way to prevent attacks on the computer is through a firewall – a hardware device or software program that protects the computer from unauthorized access by controlling who can access your computer and by monitoring the transmissions between the computer and the Internet

Windows XP has a built-in firewall. For more information, select **Help and Support Center** from the Help menu. Search for **Internet Connection Firewall**.

If Windows 98, 98 SE, Me, NT 4.0, or 2000, 98, or NT 4.0 is running on the computer, consider installing a firewall. Hardware and software firewall products are changing rapidly as more homes and businesses establish high-speed digital connections between their local area networks and the Internet.

For more information about firewalls,including vendors who sell firewall products, go to the Qwest DSL web site and click the Security topic. Firewall products are available from computer and networking equipment retailers.

Specifications

C

General

Model Number

GS204AD9-01 (Four-Port Wireless-Ready DSL Gateway

Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX)
IEEE 802.11b (Wireless)
G.dmt
G.lite
t1.413
RFC 1483, 2364, 2516

Protocol

CSMA/CD

WAN

Full-rate DSL modem

LAN

GS204AD9-01

10/100 RJ-45 switched ports (4)
USB port (1)

GS404AD9-01

10/100 RJ-45 port (1)
USB port (1)

Expansion

PCMCIA expansion slot (2)

Speed

LAN Ethernet: 10/100Mbps
Wireless: See "Wireless Operating Range" (if used)

Cabling Type

10BaseT: UTP/STP Category 3 or 5
100BaseTX: UTP/STP Category 5
USB

Wireless Operating Range

If used:

Indoors

Up to 30M (100 ft.) @ 11 Mbps
Up to 50M (165 ft.) @ 5.5 Mbps
Up to 70M (230 ft.) @ 2 Mbps
Up to 91M (300 ft.) @ 1 Mbps

Outdoors

Up to 152M (500 ft.) @ 11 Mbps
Up to 270M (885 ft.) @ 5.5 Mbps
Up to 396 (1300 ft.) @ 2 Mbps
Up to 457M (1500 ft.) @ 1 Mbps

Topology

Star (Ethernet)

LED Indicators

4-port: Power, Internet, Wireless, LAN, USB
1-port: Power, Internet, Wireless, Ethernet Network

Environmental

Power Input

External, 12V DC, 1.2 A

Certifications

FCC Class B
FCC Class C (part 15, 68)
CE Mark Commercial
UL

Operating Temperature

0° C to 40° C (32°F to 104°F)

Storage Temperature

-20°C to 70°C (-4°F to 158°F)

Operating Humidity

10% to 85% non-condensing

Storage Humidity

5% to 90% non-condensing

Glossary

Access Point

A device that allows wireless clients to connect to one another. An access point can also act as a bridge between wireless clients and a "wired" network, such as an Ethernet network. Wireless clients can be moved anywhere within the coverage area of the access point and remain connected to the network. If connected to an Ethernet network, the access point monitors Ethernet traffic and forwards appropriate Ethernet messages to the wireless network, while also monitoring wireless traffic and forwarding wireless client messages to the Ethernet network.

Client

A desktop or mobile computer connected to a network.

DHCP (Dynamic Host Configuration Protocol)

A protocol designed to automatically assign an IP address to every computer on a network.

DNS (Domain Name System) Server Address

Allows Internet host computers to have a domain name and one or more IP addresses. A DNS server keeps a database of host computers and their respective domain names and IP addresses so that when a user enters a domain name into a Web browser, the user is sent to the proper IP address. The DNS server address used by computers on the home network corresponds to the location of the DNS server the ISP has assigned.

DSL (Digital Subscriber Line) Modem

A modem that uses existing phone lines to transmit data at high speeds.

Encryption

Provides security for wireless data transmissions.

ESSID (Extended Service Set Identifier)

A unique identifier for a wireless network.

Ethernet Network

A standard wired network configuration using cables and hubs.

Firewall

Prevents users outside the network from accessing and/or damaging files or computers on the network.

Gateway

A device that manages the data traffic of a network, as well as data traffic to and from the Internet.

IP (Internet Protocol) Address

A series of four numbers separated by periods identifying a unique Internet computer host.

ISP Gateway Address

An IP address for the Internet gateway. This address is only required when using a cable or DSL modem.

ISP (Internet Service Provider)

A business that connects individuals or businesses to the Internet.

LAN (Local Area Network)

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

MAC (Media Access Control) Address

The hardware address of a device connected to a network.

NAT (Network Address Translation)

Allows all computers on a network to use one IP address, enabling access to the Internet from any computer on the the network without purchasing more IP addresses from an ISP.

PC Card

An Ethernet adapter connected to the PCMCIA slot in a computer, enabling the communication with the Gateway.

PPPoE (Point-to-Point Protocol over Ethernet)

A method of secure data transmission.

Subnet Mask

A set of four numbers configured like an IP address used to create IP address numbers used within a particular network only.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The standard protocol for data transmission over the Internet.

WAN (Wide Area Network)

A network connecting computers located in separate areas, (i.e., different buildings, cities, countries). The Internet is a WAN.

WECA (Wireless Ethernet Compatibility Alliance)

An industry group that certifies cross-vender interoperability and compatibility of IEEE 802.11b wireless networking products and promotes the standard for enterprise, small business, and home environments.

WLAN (Wireless Local Area Network)

A group of computers and other devices connected wirelessly in a small area.

Notices

Regulatory Compliance Notices

Class B Equipment

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

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

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by A*ction*tec Electronics, Inc., may void the user's authority to operate the equipment.

Declaration of conformity for products marked with the FCC logo – United States only.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference;

2. This device must accept any interference received, including interference that may cause unwanted operation.

☞ ***Note***: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

For questions regarding your product or the FCC declaration, contact:

*Action*tec Electronics, Inc.
760 North Mary Ave.
Sunnyvale, CA 94086
United States
Tel: (408) 752-7700
Fax: (408) 541-9005

Limited Warranty

Hardware: *Action*tec Electronics, Inc., warrants to the end user ("Customer") that this hardware product will be free from defects in workmanship and materials, under normal use and service, for twelve (12) months from the date of purchase from *Action*tec Electronics or its authorized reseller.

*Action*tec Electronics' sole obligation under this express warranty shall be, at *Action*tec's option and expense, to repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or if neither of the two foregoing options is reasonably available, *Action*tec Electronics may, in its sole discretion, refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of *Action*tec Electronics, Inc. Replacement products may be new or reconditioned. *Action*tec Electronics warrants any replaced or repaired product or part for ninety (90) days from shipment, or the remainder of the initial warranty period, whichever is longer.

Software: *Action*tec Electronics warrants to Customer that each software program licensed from it will perform in substantial conformance to its program specifications, for a period of ninety (90) days from the date of purchase from *Action*tec Electronics or its authorized reseller. *Action*tec Electronics warrants the media containing software against failure during the warranty period. The only updates that will be provided are at the sole discretion of *Action*tec Electronics and will only be available for download at the *Action*tec Web site, www.actiontec.com. *Action*tec Electronics' sole obligation under this express warranty shall be, at *Action*tec Electronics' option and expense, to refund the purchase price paid by Customer for any defective software product, or to replace any defective media with software which substantially conforms to applicable *Action*tec Electronics published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. *Action*tec Electronics makes no warranty or representation that its software products will meet Customer's requirements or work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the *Action*tec Electronics software product documentation or specifications as being compatible, *Action*tec Electronics will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product or from use of the software product not in accordance with *Action*tec Electronics published specifications or user guide.

THIS *ACTION*TEC ELECTRONICS PRODUCT MAY INCLUDE OR BE BUNDLED WITH THIRD-PARTY SOFTWARE, THE USE OF WHICH IS GOVERNED BY A SEPARATE END-USER LICENSE AGREEMENT.

THIS *ACTION*TEC ELECTRONICS WARRANTY DOES NOT APPLY TO SUCH THIRD-PARTY SOFTWARE. FOR THE APPLICABLE WARRANTY, PLEASE REFER TO THE END-USER LICENSE AGREEMENT GOVERNING THE USE OF SUCH SOFTWARE.

Obtaining Warranty Service: Customer may contact *Action*tec Electronics Technical Support Center within the applicable warranty period to obtain warranty service authorization. Dated proof of purchase from *Action*tec Electronics or its authorized reseller may be required. Products returned to *Action*tec Electronics must be pre-authorized by *Action*tec Electronics with a Return Merchandise Authorization (RMA) number marked on the outside of the package, and sent prepaid and packaged appropriately for safe shipment, and it is recommended that they be insured or sent by a method that provides for tracking of the package. The repaired or replaced item will be shipped to Customer, at *Action*tec Electronics' expense, not later than thirty (30) days after *Action*tec Electronics receives the defective product.

Return the product to:
(In the United States)
*Action*tec Electronics, Inc.
760 North Mary Avenue
Sunnyvale, CA 94085

*Action*tec Electronics shall not be responsible for any software, firmware, information, memory data, or Customer data contained in, stored on, or integrated with any products returned to *Action*tec Electronics for repair, whether under warranty or not.

WARRANTIES EXCLUSIVE: IF AN *ACTION*TEC ELECTRONICS' PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT *ACTION*TEC ELECTRONICS' OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. *ACTION*TEC ELECTRONICS

NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

*ACTION*TEC ELECTRONICS SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPT TO OPEN, REPAIR OR MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OTHER HAZARDS, OR ACTS OF GOD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, *ACTION*TEC ELECTRONICS ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCT, EVEN IF *ACTION*TEC ELECTRONICS OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT,OR REFUND OF THE PURCHASE PRICE PAID, AT *ACTION*TEC ELECTRONICS' OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Disclaimer: Some countries, states or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety, they will be limited to the duration of the applicable written warranty. This warranty gives you specific legal rights which may vary depending on local law.

Dispute Resolution: The customer may contact the Director of Technical Support in the event the Customer is not satisfied with *Action*tec Electronics' response to the complaint. In the event that the Customer is still not satisfied with the response of the Director of Technical Support, the Customer is instructed to contact the Director of Marketing. In the event that the Customer is still not satisfied with the response of the Director of Marketing, the Customer is instructed to contact the Chief Financial Officer and/or President.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California, U.S.A., excluding its conflicts of laws and principles, and excluding the United Nations Convention on Contracts for the International Sale of Goods.