Wireless DSL Gateway

GT704WG

User's Manual

Table of Contents

1 Introduction 1
Minimum System Requirements 1
Features 2
Getting to Know the Gateway 3
2 Performing a Quick Setup 7
Accessing Quick Setup Screens 7
Changing the Password 10
3 Viewing the Gateway's Status 13
Broadband Connection Status 13
Network Status 16
4 Configuring Wireless Settings 17
Accessing Wireless Setup 17
Basic Wireless Setup 20
Wireless Advanced Settings 20
Wireless Status 25
5 Configuring Advanced Settings 27
Accessing Advanced Setup Screens 27
DSL Settings 30
DHCP Settings 30
LAN IP Address 32
WAN IP Address 33
QoS Settings Upstream 35
QoS Settings Downstream 38
QoS Status 39
Remote Management/Telnet 39
Telnet Timeout Setting 40
Dynamic Routing 41
Static Routing 41
UPnP (Universal Plug and Play) 42
USB Port Detection 42
Time Zone 43
Remote Syslog Capture 43

6 Configuring Security Settings 45
Accessing Wired Security Screens 45
Admin User Name and Password 46
Firewall 47
Applications 50
DMZ Hosting 51
NAT (Network Address Translation) 52
Port Mapping 52
7 Configuring Parental Controls 53
Accessing Parental Control Screens 53
Services Blocking 54
Website Blocking 55
Schedule Rules 56
8 Configuring the Gateway's Utilities 59
Accessing the Utilities Screens 59
Restore Default Settings 61
Upgrade Firmware 61
Multiple PVC 62
Web Activity Log 62
System Log 63
OAM Ping Test 64
Ping Test 65
Reboot 65
9 Troubleshooting 67
Troubleshooting 67
Frequently Asked Questions 69
A Reference 75
Locating Computer Information 75
Locating Windows Operating System Files 76
B Switching to Static IP on the Computer 79
Windows 98 SE 79
Windows Me 82
Windows 2000 85
Windows XP 89
C Computer Security 93
Comparing DSL Service with a Dial-Up Modem 93
Gateway Security 94
Computer Security 94
Electronic Security 95

D Specifications **97**
General 97
Wireless Operating Range 98
LED Indicators 98
Environmental 98
E Glossary **99**
F Service Acronyms **103**
Service Acronym Definitions 103

This page left intentionally blank.

Introduction 1

Thank you for purchasing the Wireless DSL Gateway. The Gateway is the simplest way to connect computers to a 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 Wireless DSL Gateway is sure to be one of the keys to your success.

Minimum System Requirements

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

☞ ***Note***: USB LAN port is not supported with Microsoft Windows NT 4.0, Windows Vista 64-bit, or 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

Features

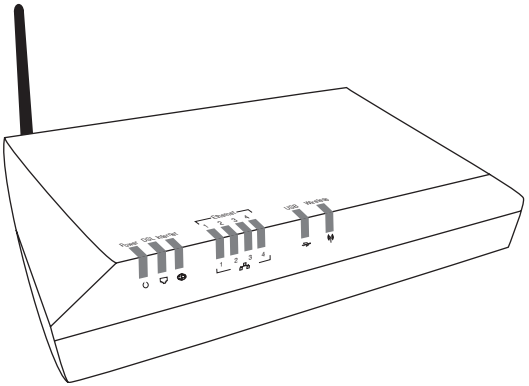
- Plug-and-Play installation support for computers running Windows operating systems (98SE, Me, 2000, XP, and Vista)
- ADSL WAN port (RJ-11)
- Full-rate ANSI T1.413 Issue 2, ITU G.992.1(G.dmt) and G.992.2(G.lite) standard compliance
- Auto-handshake for different ADSL flavors
- USB 1.1 device specification compliance
- 12 Mbps USB data rate (full speed) support
- Bridged Ethernet over ATM, PPP over ATM, PPP over Ethernet
- Precise ATM traffic shaping
- IP packet routing and transparent bridge
- RIP-1, RIP-2, and static routing protocol support
- Built-in NAT, DHCP server
- DNS relay support
- PAP/CHAP authentication, administrative passwords through Telnet
- 64-, 128-, and 256-bit WEP/WPA wireless LAN security
- IEEE 802.3 Ethernet standard compliance
- 10/100 Base-T Ethernet ports (4)
- Fast Ethernet flow control support
- Web-based configuration setup
- FTP firmware upgradeable
- Web download support
- 802.11b/g support

Getting to Know the Gateway

This section contains a quick description of the Gateway's lights, ports, etc. The Gateway has several indicator lights (LEDs) on its front panel and a series of ports on its rear panel.

Front Panel

The front panel of the Gateway features nine lights: Power, DSL, Internet, Ethernet (4), USB, and Wireless.



Power Light

The Power light displays the Gateway's current status. If the Power light glows steadily green, the Gateway is receiving power and fully operational. When the Power light is rapidly flashing, the Gateway is initializing. If the Power light is glows red when the Power cord is plugged in, the Gateway has suffered a critical error and technical support should be contacted.

DSL Light

The DSL light illuminates when the Gateway is connected to a DSL line.

Internet Light

When the Internet light glows steadily, the Gateway is connected to the DSL provider. When it flashes, the Gateway's built-in DSL modem is training for the DSL service.

Ethernet Lights

The Ethernet lights illuminate when the Gateway is connected to one or more of its yellow Ethernet ports.

USB Light

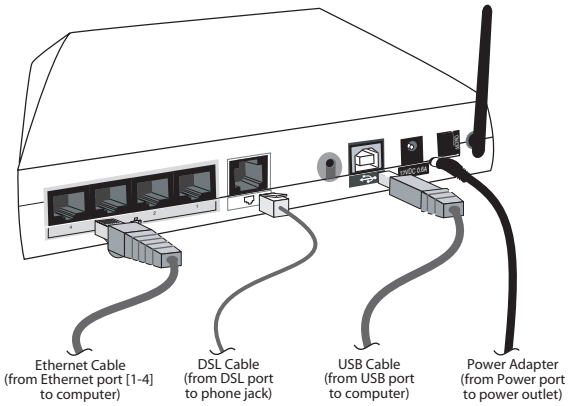
The USB light illuminates when the Gateway is connected via its USB port.

Wireless Light

The Wireless light illuminates when the Gateway is connected wirelessly (if the Gateway's Wireless feature is turned on).

Rear Panel

The rear panel of the Gateway contains seven ports (Ethernet [4], Phone, USB, and Power), as well as Reset and Power switches.



Ethernet Ports

The Ethernet ports are used to connect computers to the Gateway via Ethernet cable. The Ethernet ports are 10/100 Mbps auto-sensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

DSL Port

The DSL port is used to connect the Gateway to a DSL (Digital Subcriber Line) connection.

Reset Switch

Depressing the Reset switch for one second will restore the Gateway's factory default settings. To reset the Gateway, depress and hold the Reset switch for approximately one second. The reset process will start after releasing the switch.

USB Port

The USB port is used to connect a computer to the Gateway via USB cable.

Power Port

The Power port is used to connect the Power cord to the Gateway.

Warning: Do not unplug the Power cord from the Gateway during the reset process. Doing so may result in permanent damage to the Gateway.

Power Switch

The Power switch is used to power the Gateway on and off.

This page left intentionally blank.

Performing a Quick Setup

2

This chapter is a guide through a quick set up of the Gateway, including how to connect the Gateway to the ISP.

To complete the quick setup, have the Welcome Letter or ISP Worksheet handy. If the document is not available, contact the ISP immediately.

Accessing Quick Setup Screens

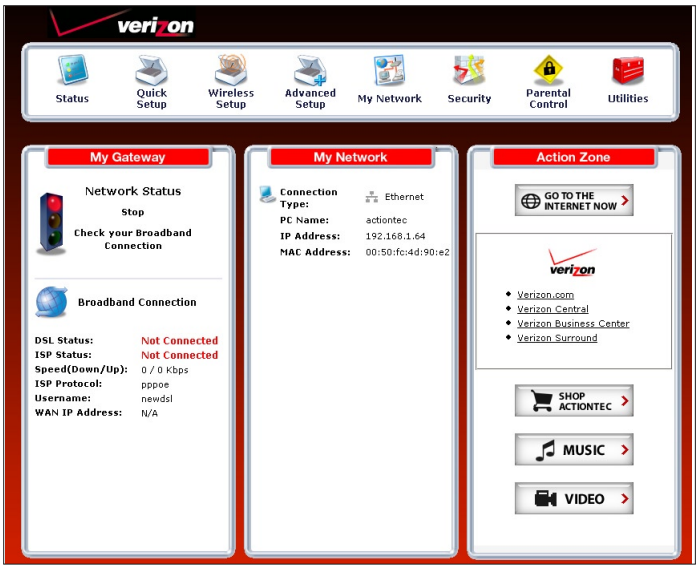
To access the Quick Setup screens:

1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.1.1`

   then press **Enter** on the keyboard.

2. The "Home" screen appears. Click **Quick Setup**.

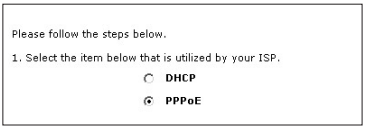


3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

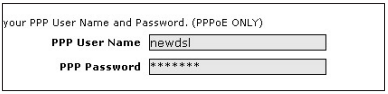
☞ ***Note:*** The default user name is "admin." The default password is "password."

4. Follow the instructions in the "Welcome to the Quick Setup" screen, then click **Next**.

5. At the top of the next window, select **PPPoE** or **DHCP**.

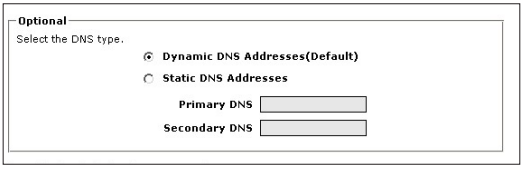


5a. If PPPoE was selected in step 5, the default user name and password are entered in the appropriate text boxes.
If "DHCP" was selected, go to step 6.



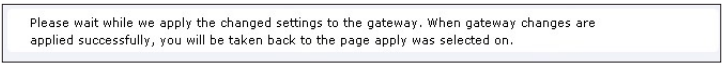
5b. If PPPoE was selected in step 5, select the IP type ("Dynamic IP-DHCP [Default]" or "Single Static IP Address"). If Single Static IP Address was selected, enter the address in the appropriate text box.

6. **Optional** - Select the DNS type ("Dynamic DNS Addresses [Default]" or "Static DNS Addresses"). If Static DNS Addresses was selected, enter the primary and secondary DNS addresses in the appropriate text boxes. If unsure what to enter in this section, contact the ISP.



7. Click **Apply** at the bottom of the screen.

8. Read the instructions on the next screen. The Gateway is successfully configured.



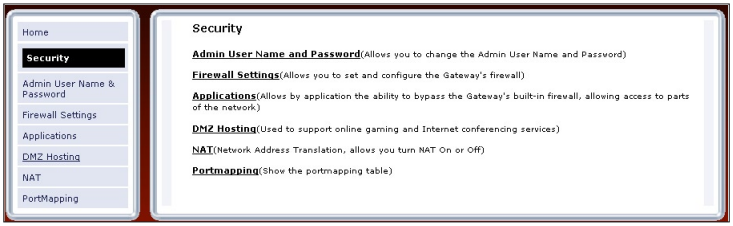
The Power light flashes rapidly while the Gateway restarts, then glows steadily green when fully operational. The Internet light will also glow steadily green. The Gateway is now configured and users can start surfing the Internet.
If an error appears, stating the Web browser was unable to connect to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

Changing the Password

To create or change the password allowing access to the Gateway's Web Configuration screens, follow these instructions:

1. From the "Home" screen, select **Security**.

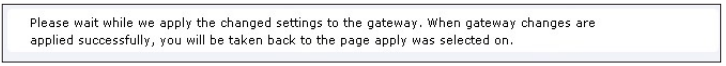
2. The "Security" screen appears. Select "Admin User Name and Password."



3. The "Change Admin Username/Password" screen appears. Enter a new Username in the "Admin User Name" text boxt, then enter a new password in the "Admin Password" text box. Make sure to write down the user name and password and keep it in a secure location. They will be needed to access the Gateway's Web Configuration screens in the future.

4. Click **Apply** at the bottom of the screen.

5. Read the instructions on the next screen. The user name and password are successfully changed.



Once the Gateway has rebooted, the new user name and password are active. To access the Gateway's Web Configuration screens, the new user name and password must be entered.

This page left intentionally blank.

Viewing the Gateway's Status

3

After configuring the Gateway, the Gateway's connection and network status can be viewed. The Internet connection status is viewed in the "Broadband Connection Status" screen, while the network status is viewed in the "My Network" screen.

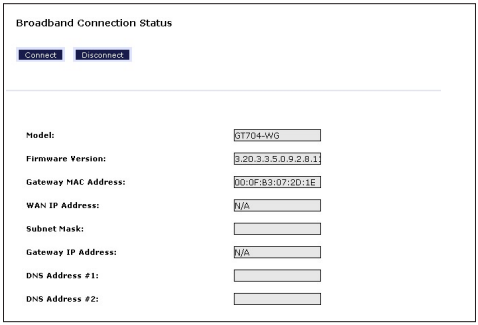
Broadband Connection Status

To view the Gateway's connection statistics, select **Status** in the Home screen. The "Broadband Connection Status" screen appears. There are three sections in this screen: General Statistics, PPP Status, and DSL Status.

> ***Note:*** No settings (other than connecting or disconnecting from the Internet by clicking on **Connect** or **Disconnect**) can be changed from the Broadband Connection Status screen.

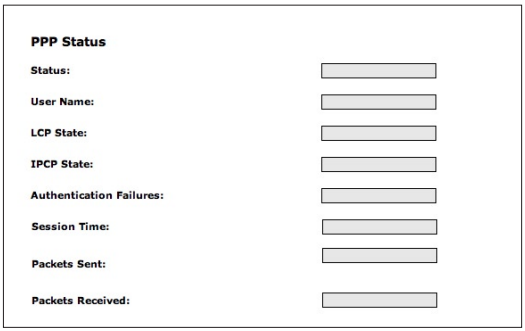
General Statistics

The top section of the Broadband Connection Status screen displays general statistics regarding the Gateway, including model number, firmware version, IP address, and gateway IP address.



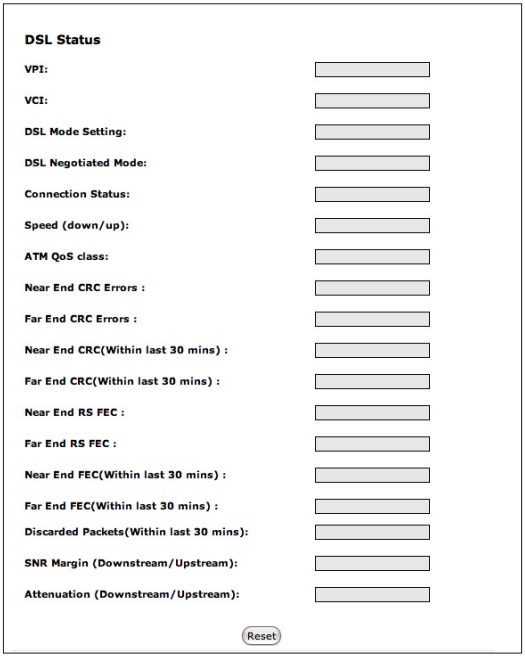
PPP Status

The middle section of the Broadband Connection Status screen displays the status of the Gateway's PPP connection, including user name, authentication failures, and packets sent and received.



DSL Status

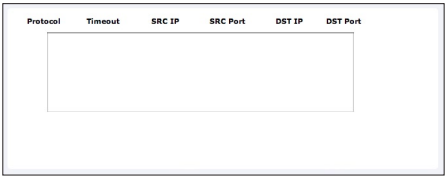
The bottom section of the Broadband Connection Status screen displays the status of the Gateway's DSL connection, including mode settings, connection status, and number of discarded packets. Click **Reset** to refresh all statistics on this screen



In the menu on the left side of the Broadband Connection Status screen, there are two other options available to view: **NAT Table** and **Routing Table**. Click to generate the option of choice.

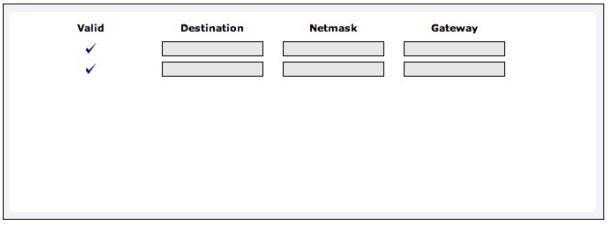
NAT Table

Selecting **NAT Table** generates the "NAT Table" screen. This screen displays an overview of the current list of open connections through NAT (Network Address Translation) the Gateway supports between the networked computers and the Internet.



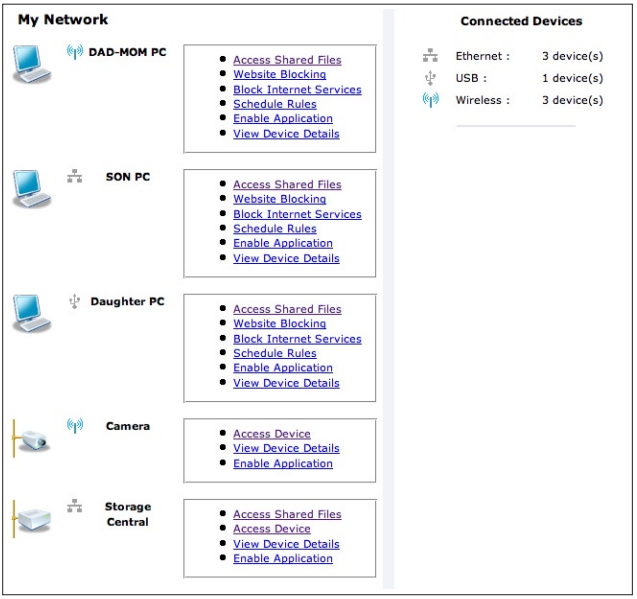
Routing Table

Selecting **Routing Table** generates the "Routing Table" screen. This screen displays the an overview of the Gateway's network routes.



Network Status

To view the Gateway's network status, select **My Network** in the "Home" screen. The "My Network" screen appears, listing all devices connected to the network. From this screen, various settings can be accessed, including Website blocking, Schedule Rules, and Enable Application.



To view the network status of a particular device, click **View Device Details** for the device. An overview of the device's network status appears.

Configuring Wireless Settings

4

This chapter explains how to set up the Gateway's wireless network capabilities, including setting up wireless security and viewing the wireless connection status.

Accessing Wireless Setup

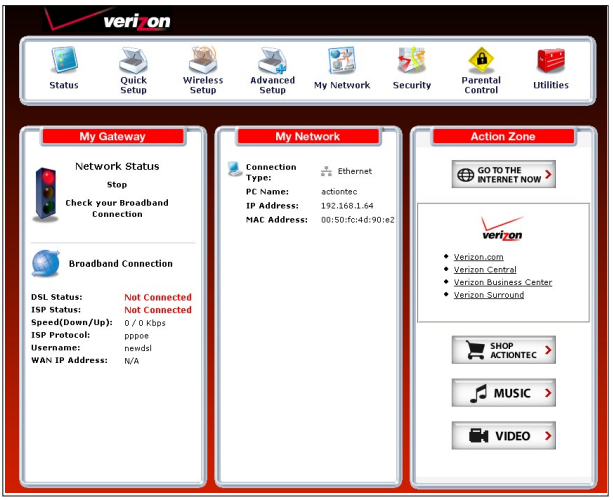
To access the Wireless Settings configuration screens, follow these instructions:

1. Open a Web browser. In the "Address" text box, type:

`http://192.168.1.1`

then press **Enter** on the keyboard.

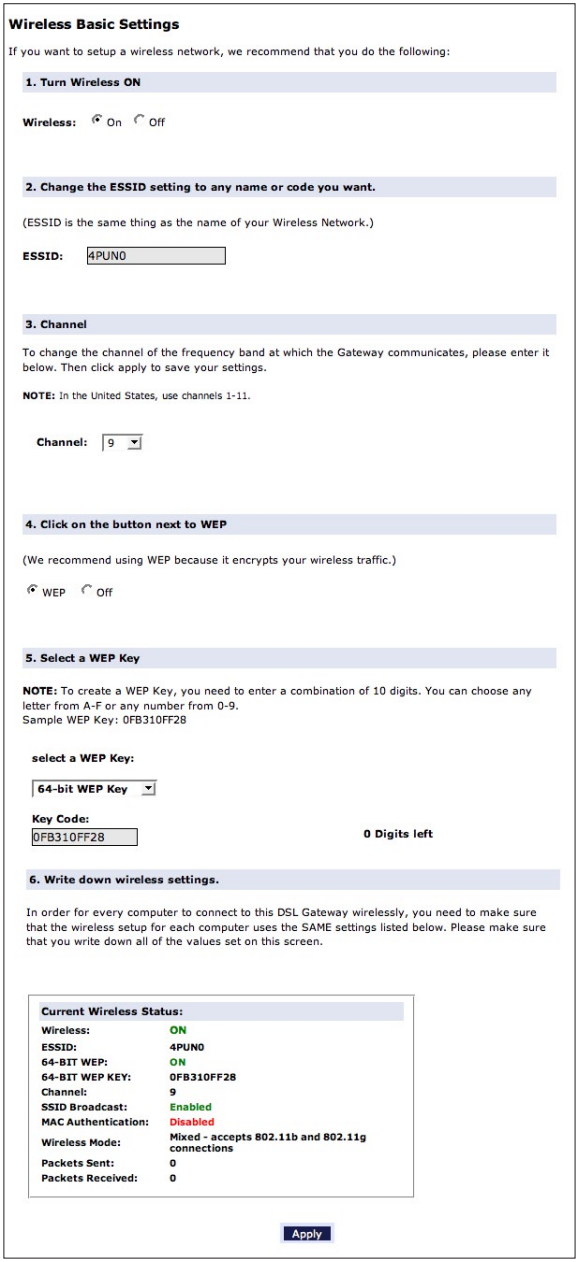
2. The "Home" screen appears. Click **Wireless Setup**.



3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Wireless Basic Settings" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.



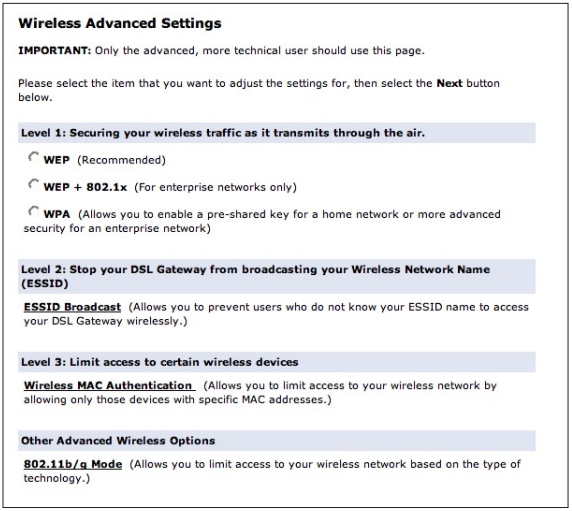
Basic Wireless Setup

To perform a basic setup of a wireless network using the Gateway:

1. In the "Wireless Basic Settings" screen, turn the Gateway's wireless radio on by selecting **On**.
2. Create a name for the wireless network and enter it in the "ESSID" text box.
3. Select a channel from the "Channel" drop-down menu. In the United States, use channels 1-11.
4. Activate WEP (Wired Equivalent Privacy) to secure the wireless network by selecting **WEP**.
5. Create a 64-bit WEP key by selecting **64-bit WEP Key** from the "select a WEP Key" drop-down menu, then entering a 10-digit key in the "Key Code" text box. The digits can be any letter from A-F, and any number from 0-9.
6. Write down the Gateway's wireless settings. To connect other devices to the wireless network, the devices' wireless settings must match the Gateway's wireless settings exactly. Check the "Current Wireless Status" box (available in any wireless setting screen) to view the Gateway's wireless status and settings.

Wireless Advanced Settings

To access the Gateway's wireless advanced settings screens, select **Advanced Settings** from the menu on the left side of the "Wireless Basic Settings" screen.



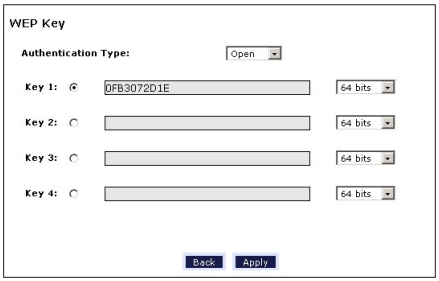
This generates the "Wireless Advanced Settings" screen. In this screen, the security of the wireless network can be activated and fortified.

Wireless Security

The first section of the Wireless Advanced Settings screen involves wireless security (securing wireless traffic as it transmits through the air). The Gateway offers three types of wireless security: WEP, WEP+802.1x, and WPA.

WEP

Selecting **WEP** in the Wireless Advanced Settings screen generates the "WEP Key" screen. Here, the authentication type, encryption level, and WEP keys are entered to activate WEP (Wired Equivalent Privacy) security encryption for the wireless network.



Authentication Type - There are three authentication types: Open, Shared, and Both. Open authenticaton allows any wireless-enabled device to recognize the network, even if the WEP key is invalid. Shared allows only wireless-enabled devices with the correct WEP key to recognize the network.

64-bit WEP - 64-bit WEP requires one or more keys, each key comprising five hexadecimal pairs. One key (Key 1) is automatically generated by the Gateway at startup, based on the Gateway's MAC address. This key is also displayed on a sticker on the bottom of the Gateway. 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 new set of 64-bit WEP keys, activate one or more keys by clicking in the appropriate circles, then enter five hexadecimal digit pairs in each activated **Key** text box (**Key 1-**, **Key 2-**, **Key 3-**, **Key 4-**). After activating 64-bit WEP, 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 or more keys, each key comprising 13 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character 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, activate **Key 1** by clicking in the appropriate circle, select "128 bit" from the drop-down list on the right, then enter 13 hexadecimal digit pairs in the **Key** text box. After activating 128-bit WEP, a computer with wireless capability can join the network only if this key is entered in the computer's wireless encryption scheme.

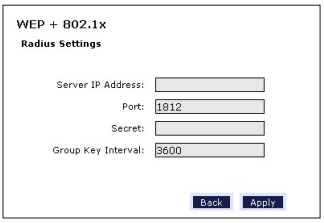
256-bit WEP - 256-bit WEP requires one or more keys, each key comprising 29 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. To create a 256-bit WEP key, activate **Key 1** by clicking in the appropriate circle, select "256 bit" from the drop-down list on the right, then enter 29 hexadecimal digit pairs in the **Key** text box. After activating 256-bit WEP, 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- or 256-bit WEP. Ensure all PC Cards installed in the networked computers support 128- or 256-bit WEP before activating.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

WEP+802.1x

Activating **WEP+802.1x** in the Wireless Advanced Settings screen generates the "WEP+802.1x" screen. This setting is for enterprise networks only, and should be accessed by an experienced information systems specialist.

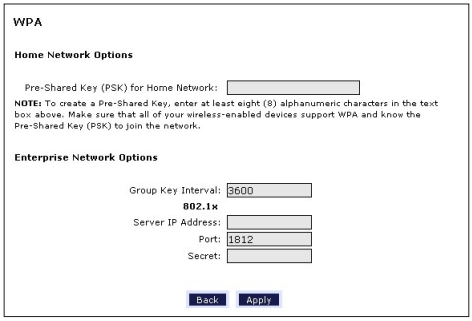


To set up WEP+802.1x security, enter the IP address of the RADIUS server in the "Server IP Address" text box, and the "Secret" key (for communication between the RADIUS server and the Gateway) in the "Secret" text box. The "Port" and "Group Key Interval" values should remain the same.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

WPA

Activating **WPA** (Wi-Fi Protected Access) in the Wireless Advanced Settings screen generates the "Wireless WPA Settings" screen.



There are two levels of WPA. "Pre-Shared Key (PSK) for Home Network" is for home network security. To set up a PSK (Pre-Shared Key), enter 8-63 alphanumeric characters in the text box. All wireless-enabled devices must support WPA and know the PSK to join the network.

The "Group Key Interval," "Server IP Address," "Port," and "Secret" text boxes are enterprise network specific, and should only be accessed by an information systems professional. See "WEP+802.1x" on the previous page for more information.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

ESSID Broadcast

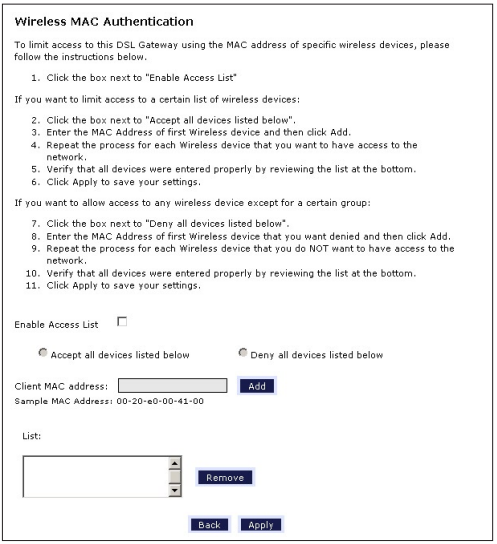
Selecting **ESSID Broadcast** in the Wireless Advanced Settings screen generates the "ESSID Broadcast" screen.

To prevent a unwanted computers from joining the Gateway's wireless network by using an ESSID of "Any," select **Disable** in the ESSID Broadcast screen. To broadcast the wireless network's ESSID, select **Enable**.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

Wireless MAC Authentication

Selecting **Wireless MAC Authentication** in the Wireless Advanced Settings screen generates the "Wireless MAC Authentication" screen.

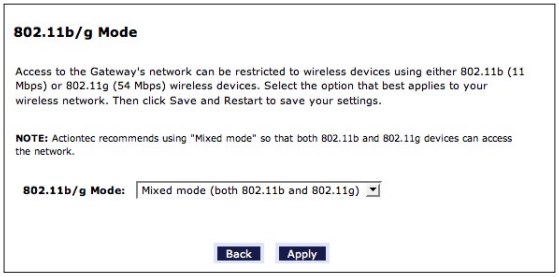


This feature allows the user to control the wireless LAN network by denying or allowing wireless access by specifying the MAC address of the wireless client(s) allowed or denied access on the wireless network. To do this, follow the instruction on-screen.

When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

802.11b/g Mode

Selecting **802.11b/g Mode** in the Wireless Advanced Settings screen generates the "802.11b/g Mode" screen.

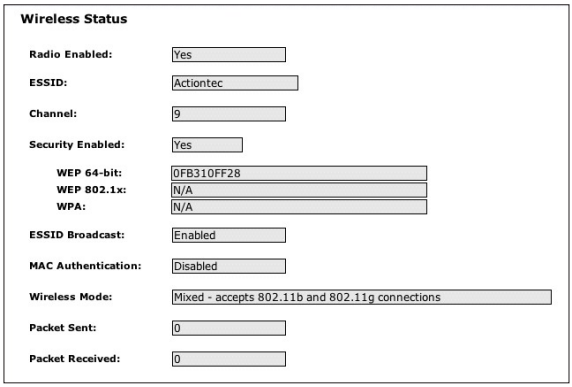


Access to the Gateway's network can be restricted to wireless clients using either the 802.11b or 802.11g wireless adapters. Click on the down arrow next to the drop-down menu and select the desired option. We recommend using the "Mixed" mode (the default option), which enables both 802.11b and 802.11g wireless clients to join the network.

When finished with this screen, click **Apply** to save all changes.

Wireless Status

To view the Gateway's wireless status and settings, select **Wireless Status** from the menu on the left side of the "Wireless Basic Settings" screen.



The "Wireless Status" screen appears, which displays all of the settings of the Gateway's wireless network settings.

This page left intentionally blank.

Configuring Advanced Settings

5

This chapter explains how to configure the Gateway's advanced settings, such as remote management, DHCP settings, and Quality of Service (QoS).

Accessing Advanced Setup Screens

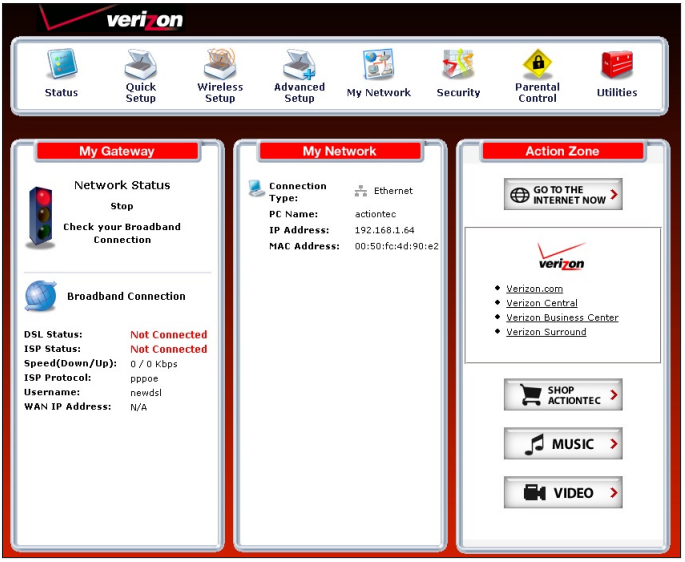
To access the Advanced Setup screens, follow these instructions:

1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.1.1`

   then press **Enter** on the keyboard.

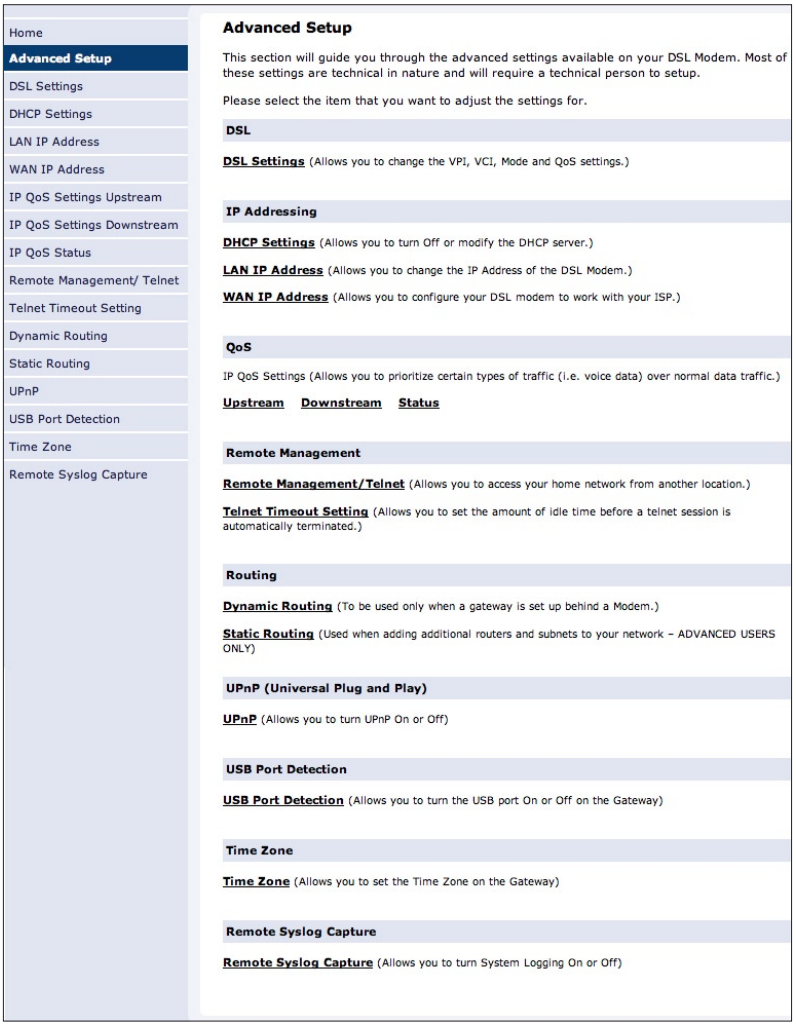
2. The "Home" screen appears. Click **Advanced Setup**.



3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

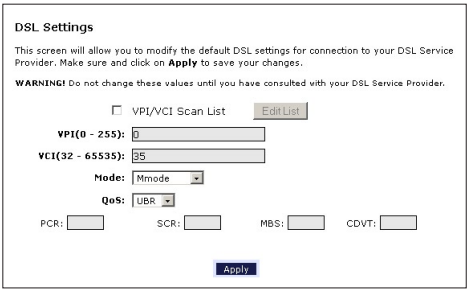
☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Advanced Setup" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.



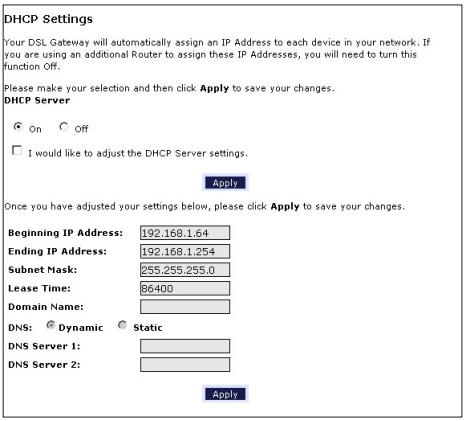
DSL Settings

To access DSL Settings, select **DSL Settings** from the "Advanced Setup" screen. The Gateway's VPI, VCI, Mode, and QoS (Quality of Service) settings can be changed from this screen, we recommend not changing these values without first consulting the ISP.



DHCP Settings

Selecting **DHCP Settings** in the "Advanced Setup" screen generates the "DHCP Settings" 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**, then click **Apply**.



We strongly recommend 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 in the check box labeled "I would like to adjust the DHCP server settings" activates the text boxes at the bottom of the DHCP Settings screen. Change the IP address range and DNS server information in these text boxes.

Beginning IP Address

This is the IP address at which the DHCP server starts assigning IP addresses. We recommend keeping the factory default setting (192.168.1.64).

Ending IP Address

This is the IP address at which the DHCP server stops assigning IP addresses. We recommend keeping the factory default settings (192.168.1.254).

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 192.168.1.64 and 192.168.1.254 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 10.33.222.1, set the beginning IP address to 10.33.222.2, and the ending IP address to 10.33.222.254.

Subnet Mask

Enter the IP address of the DHCP server's subnet mask here.

Lease Time

This value represents the amount of time (in seconds) the DHCP server holds onto a specific IP address.

Domain Name

This is the domain name provided by Verizon. If Verizon provided domain name information, enter it here. If not, leave the text box intact.

DNS (Dynamic or Static)

This is the type of DNS server provided by Verizon. If Verizon provided DNS server information, select the type here. If not, leave as is.

DNS Server 1

This is the primary DNS server provided by Verizon. If Verizon provided DNS server information, enter it here. If not, leave the text box intact.

DNS Server 2

This is the secondary DNS provided by Verizon. If Verizon provided secondary DNS server information, enter it here. If not, leave the text box intact.

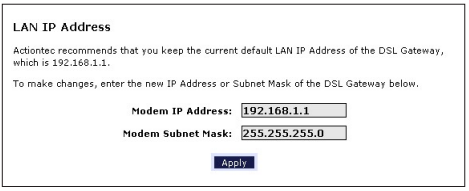
When finished in this screen, click **Apply** to activate any changes made.

LAN IP Address

Selecting **LAN IP Address** in the "Advanced Setup" screen causes a warning screen to appear.

Read the on-screen warning, then click **Yes** to continue.

The "LAN IP Address" screen appears.



The values in the "Modem IP Address" and "Modem Subnet Mask" text boxes are the IP and subnet mask address of the Gateway as seen on the network. These values can be modified for your LAN network, but we recommend keeping the default factory settings (IP address 192.168.1.1; subnet mask address 255.255.255.0).

☞ ***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."

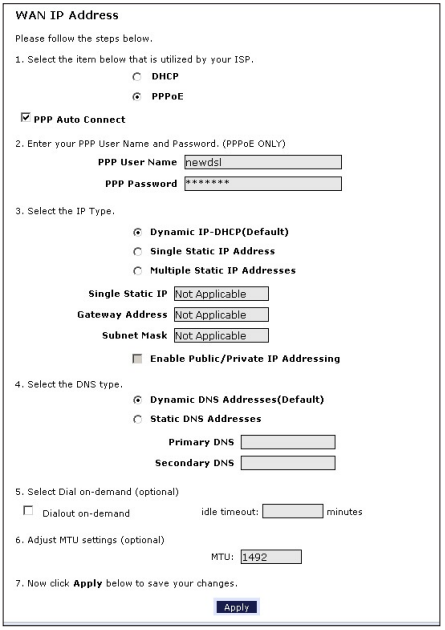
When finished in this screen, click **Apply** to activate any changes made.

WAN IP Address

Selecting **WAN IP Address** in the "Advanced Setup" screen causes a warning screen to appear.

Read the on-screen warning, then click **Yes** to continue.

The "WAN IP Address" screen appears.



WAN IP Address allows manual set up of the IP address of the Gateway. To do this:

> ***Note***: Some DSL providers use PPPoE to establish communication with an end user. Other types of broadband Internet connections (such as fixed point wireless) may use either DHCP or static IP address. If unsure which connection is present, check with Verizon before continuing.

1. Select "DHCP" or "PPPoE," depending on the type of connection the ISP uses. If PPP Auto Connect is being used, click in the appropriate check box.

2. If using PPPoE was selected in step 1, enter the user name and password in the appropriate text boxes.

3. Select the IP type. If "Single Static IP Address" was selected, enter the IP address in the "Single Static IP" text box. If "Multiple Static IP Addresses" was selected, enter the designated gateway IP address and subnet mask address in the "Gateway Address" and "Subnet Mask" text boxes, respectively.

4. Enable Public/Private IP Addressing. This feature is used in conjunction with Multiple Static IP Addresses. When selected, the Gateway uses NAT for private IP addressing for the LAN, allowing both public and private IP addressing to be configured to the LAN simultaneously, while the DHCP server is reserved for private IP addressing. All computers using public IP addresses must have the public IP addresses statically assigned.

5. Select the DNS type. If static DNS address was selected, enter the primary DNS address and, optionally, the secondary DNS address in the appropriate text boxes.

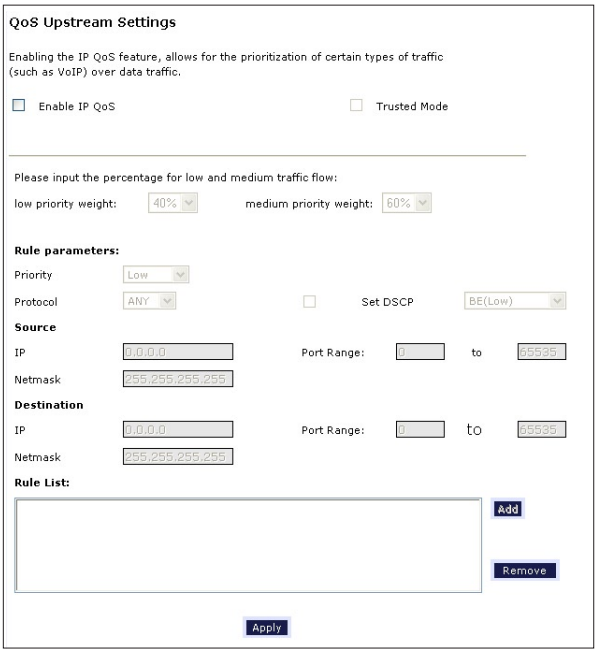
6. Select Dialout on-demand (optional). To have the Gateway automatically connect to the Internet whenever needed (when a Web browser is opened, for example), activate "Dialout on-demand" by clicking in the appropriate check box. When Dialout on-demand is activated, the user can also set the Gateway to disconnect from the Internet after a certain amount of idle time (no Internet activity). To do this, enter the number of idle time minutes (minimum 2 minutes) before disconnection occurs in the text box before "Minutes."

7. Adjust MTU settings (optional). Enter the maximum transmission unit (MTU) value (in bytes) in this text box. This value corresponds to the largest physical packet size the network is allowed to transmit. Packets larger than this size are divided into smaller packets. It is recommended to leave this value set at the default (1492).

When finished in this screen, click **Apply** to activate any changes made.

QoS Settings Upstream

Selecting **QoS Settings Upstream** from the "Advanced Setup" screen causes the "QoS Upstream Settings" screen to appear.



QoS (Quality of Service) allows the prioritization of certain types of data traffic (such as VoIP traffic) over other types of traffic (such as standard data). Both upstream (data coming into the network) and downstream (data going out of the network) traffic can be prioritzed using QoS.

Enable QoS

Clicking in this check box activates/deactivates QoS.

Trusted Mode

If "Trusted Mode" is activated, all data traffic set to an IP precedence level of 5 will be recognized as high priority traffic, regardless of IP or MAC address rule settings (used for VoIP only).

Total Available Bandwidth

Displays the total amount of available bandwidth (in kilobits per second).

High Priority Bandwidth

Enter the amount of high priority bandwidth to be used by the prioritized traffic type (cannot exceed total available bandwidth).

Priority

Always set to "High" and cannot be changed.

Protocol

Select the data type being configured. Options: TCP, UDP, ICMP.

Source

Identify the source device here, using the device's IP or MAC address, then enter appropriate value in text box. If IP is used, enter the netmask address, if applicable. A priority port range can also be defined, using the "Port Range" text boxes.

Destination

Identify the destination device here, using the device's IP address, then enter appropriate value in text box. Enter the netmask address, if applicable. A priority port range can also be defined, using the "Port Range" text boxes.

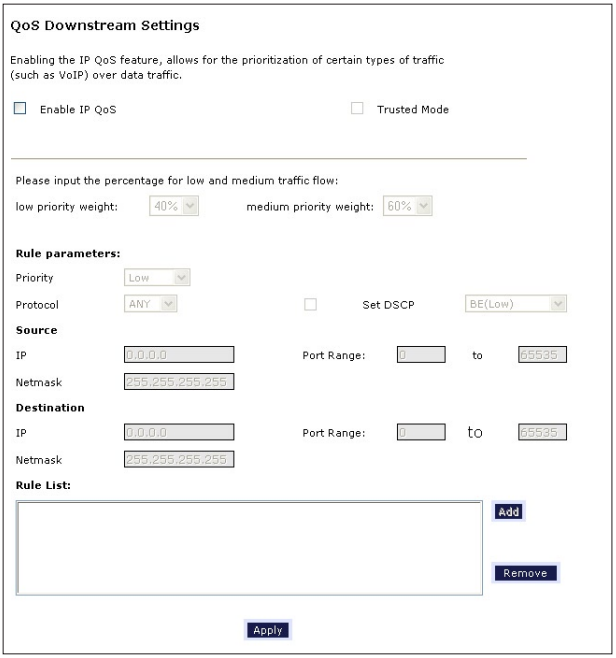
Rule List

After finishing the configuration of the QoS settings, click **Add** to save the settings in the Rule List menu box. This collection of QoS settings can then be reused at a future time. If deleting a QoS rule list, highlight it, then click **Remove**.

When finished in this screen, click **Apply** to activate any changes made.

QoS Settings Downstream

Selecting **QoS Settings Downstream** from the "Advanced Setup" screen causes the "QoS Downstream Settings" screen to appear.

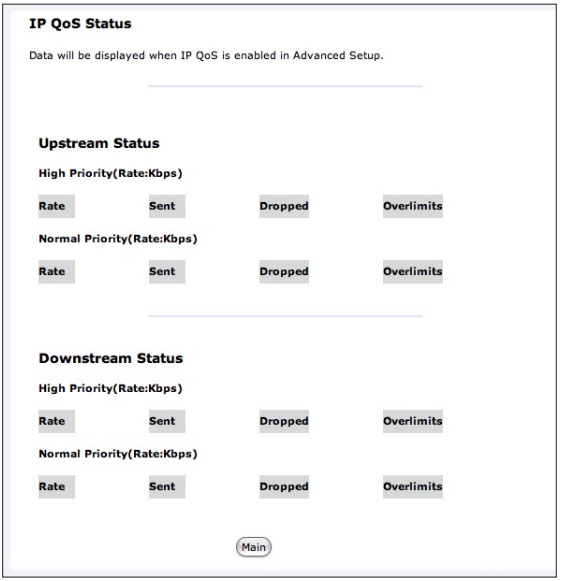


The "QoS Downstream Settings" screen is identical to the "QoS Upstream Settings" screen, with the exception of the "High Priority Bandwidth" option. Use this screen to configure QoS for data going out of the network.

When finished in this screen, click **Apply** to activate any changes made.

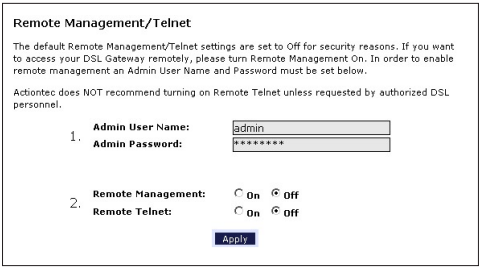
QoS Status

Selecting **QoS Status** from the "Advanced Setup" screen causes the "IP QoS Status" screen to appear. This screen displays the status of QoS upstream and downstream traffic, and differentiates both streams into high priority and normal priority traffic.



Remote Management/Telnet

Selecting **Remote Management** in the "Advanced Setup" screen generates the "Remote Management/Telent" screen. Remote management allows access to the Gateway through the Internet via another computer, while Telnet allows access to the Gateway using a computer running a Telnet program. we recommend leaving the Remote Management and Telnet **Off** (the factory default setting). The Gateway will be vulnerable to other users on the Internet if Remote Management or Telnet is activated.



Remote Management

To access the Gateway from the Internet, activate Remote Management by selecting the appropriate **On** radio button 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 Home screen (or a password prompt, if a password has been set) appears in the browser window.

Telnet

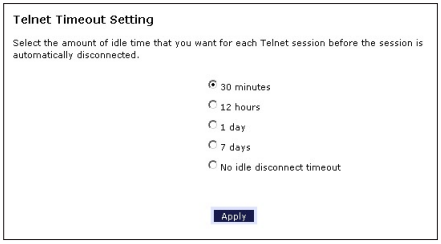
To access the Gateway via Telnet, activate Telnet by selecting the appropriate "On" radio button and writing down the WAN IP address of the Gateway (see "WAN IP Address"). On a computer outside the network running a Telnet program, enter the Gateway's WAN IP address to access the Gateway.

☞ ***Note***: Before remote management or Telnet can be activated, the administrator password must be set. To do this, go to the Home screen, click **Security**, then select **Admin User Name and Password**. Follow the instructions in the subsequent screens.

When finished in this screen, click **Apply** to activate any changes made.

Telnet Timeout Setting

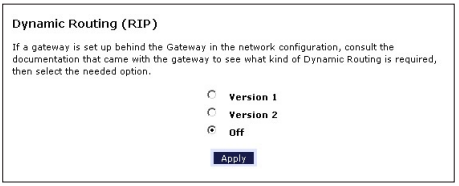
Selecting **Telnet Timeout Setting** in the "Advanced Setup" screen generates the "Telnet Timeout Setting" screen. Select a period of time from the choices available, and the Telnet session will automatically terminate at that time. If no automatic termination is needed, select "No idle disconnect timeout."



When finished in this screen, click **Apply** to activate any changes made.

Dynamic Routing

Selecting **Dynamic Routing** in the "Advanced Setup" screen generates the "Dynamic Routing" screen.

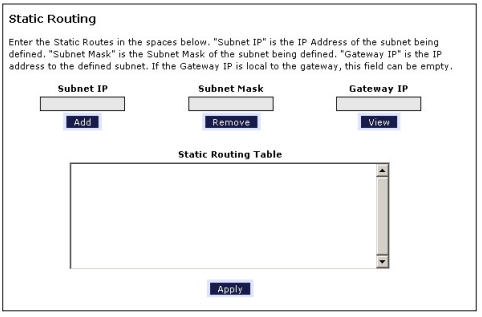


If another gateway or router is set up behind the Gateway in the network configuration, consult the documentation that came with the other gateway to see what kind of Dynamic Routing is required, then select the needed option.

When finished in this screen, click **Apply** to activate any changes made.

Static Routing

Selecting **Static Routing** in the "Advanced Setup" screen generates the "Static Routing" screen. Enter the static route addresses in their respective text boxes, then click **Add**. The address will appear in the "Static Routing Table." To remove an address, highlight it by clicking on it in the Static Routing Table, then click **Remove**.



When finished in this screen, click **Apply** to activate any changes made.

UPnP (Universal Plug and Play)

Selecting **UPnP** in the "Advanced Setup" screen generates the "UPnP" screen. In this screen, the Universal Plug and Play option is turned on or off by activating the appropriate circle.

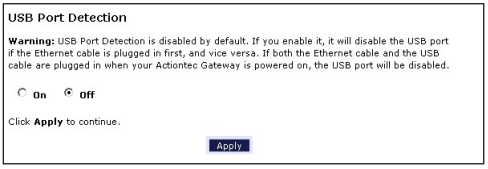
Universal Plug and Play is a zero-configuration networking protocol that allows hardware and software (such as Netmeeting) to operate more efficiently. If Netmeeting is not running properly, activate UPnP.

Note: Activating UPnP presents a slight security risk. After finishing with the hardware or software using UPnP, we recommend deactivating UPnP.

When finished in this screen, click **Apply** to activate any changes made.

USB Port Detection

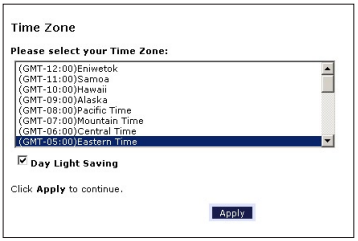
Selecting **USB Port Detection** in the "Advanced Setup" screen generates the "USB Port Detection" screen. In this screen, the USB port detection option is turned on or off by activating the appropriate circle (default is "Off"). If this option is turned on, the USB port will be disabled if an Ethernet cable is plugged into the Gateway first, or the Ethernet port will be disabled if the a USB cable is plugged into the Gateway first. If this option is turned on when both an Ethernet and a USB cable are plugged into the Gateway, the USB port will be disabled.



When finished in this screen, click **Apply** to activate any changes made.

Time Zone

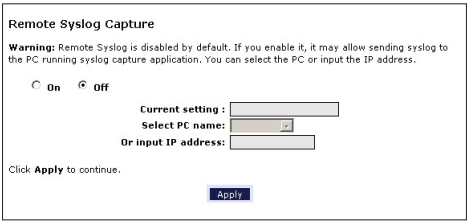
Selecting **Time Zone** in the "Configuring the Advanced Settings" screen generates the "Time Zone" screen. In this screen, select the time zone in which the Gateway is being used. Click in the "Day Light Saving" check box if Daylight Savings Time is currently in effect where the Gateway is being used.



When finished in this screen, click **Apply** to activate any changes made.

Remote Syslog Capture

Selecting **Remote Syslog Capture** in the "Advanced Setup" screen generates the "Remote Syslog Capture" screen. In this screen, the user can configure the Gateway to allow a remote computer to access the Gateway's system activity logs.



When finished in this screen, click **Apply** to activate any changes made.

This page left intentionally blank.

Configuring Security Settings

6

This chapter explains how to configure the Gateway's wired security capabilities, including firewall settings, DMZ hosting, and network address translation.

Accessing Wired Security Screens

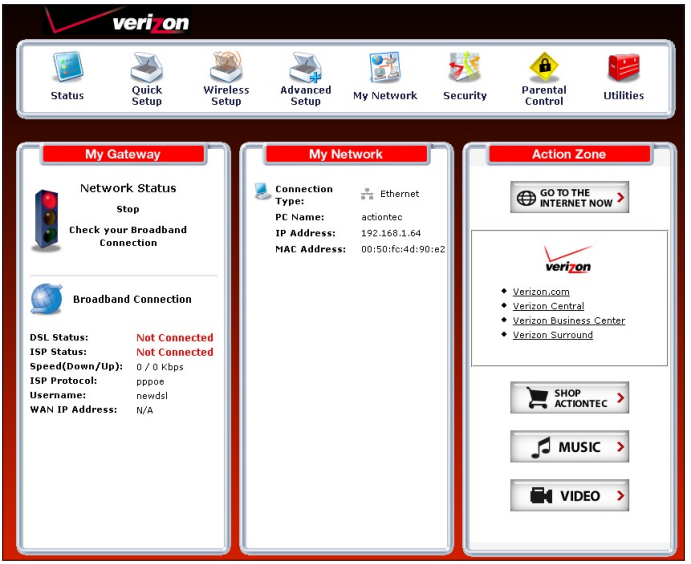
To access the Wired Security configuration screens, follow these instructions:

1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.1.1`

   then press **Enter** on the keyboard.

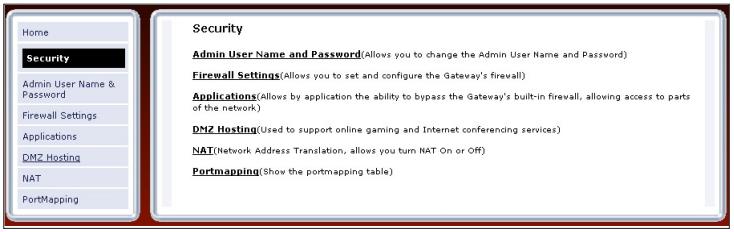
2. The "Home" screen appears. Click **Security**.



3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Security" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.



Admin User Name and Password

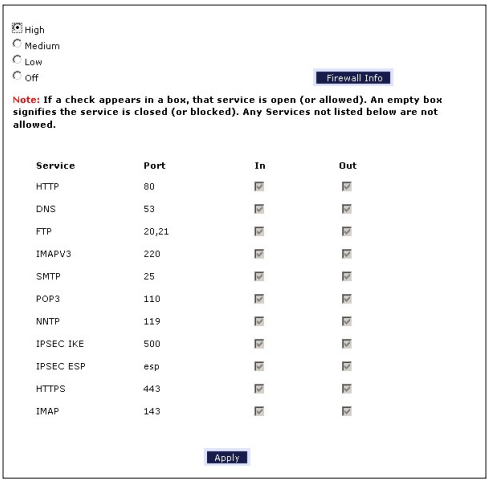
See "Changing the Password" on page 11.

Firewall

Selecting **Firewall** in the Security screen generates the "Firewall Settings" screen. Select the level of security needed for the network.

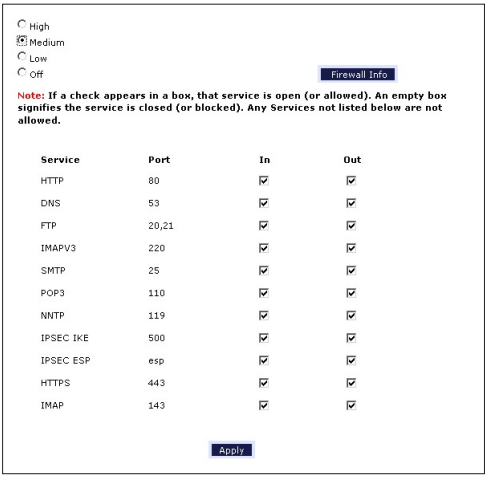
High

If **High** is selected in the "Firewall Security Level" screen, the services listed at the bottom of the screen (HTTP, DNS, FTP, IMAPv3, SMTP, POP3, NNTP, IPSEC IKE, IPSEC ESP, HTTPS, and IMAP) are the only ones allowed to pass through the firewall. All other services will be blocked. None of these settings can be changed from here.



Medium

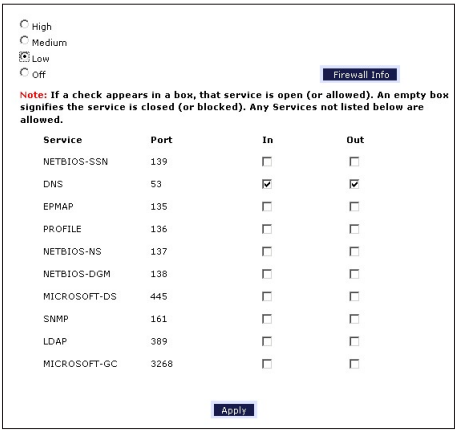
If **Medium** is selected in the "Firewall Security Level" screen, the services listed at the bottom of the screen (HTTP, DNS, FTP, IMAPv3, SMTP, POP3, NNTP, IPSEC IKE, IPSEC ESP, HTTPS, and IMAP) are the only ones allowed to pass through the firewall. All other services will be blocked. These settings can be modified to customize the firewall settings.



When finished with this screen, click **Apply** to save the changes.

Low

If **Low** is selected in the "Firewall Security Level" screen, the services listed at the bottom of the screen (NETBIOS-SSN, DNS, EPMAP, PROFILE, NETBIOS-NS, NETBIOS-DGM, MICROSOFT-DS, SNMP, LDAP, and MICROSOFT-GC,) can be denied access through the firewall. Click in the appropriate check box to allow or deny access for a particular service (check mark in the check box to deny; blank check box to allow). All services not listed are allowed access.



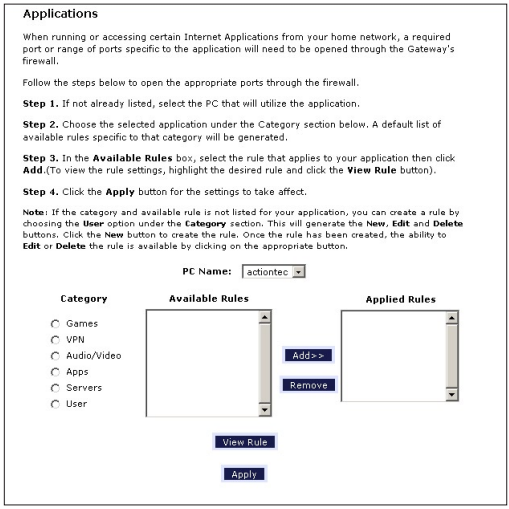
Off

If **Off** is selected in the "Firewall Security Level" screen, firewall filtering is based solely on the basic NAT firewall.

☞ ***Note***: See Appendix F, "Service Acronyms," for a description of the services listed in the Firewall Security Level screens.

Applications

Selecting **Applications** in the Security screen generates the "Applications" screen.



This screen 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, select the name of a computer on the network from the "PC Name" drop-down list, then click **Add**. Next, select a "Category" by clicking the appropriate radio button. In the "Available Rules" list box, select a game, application, server, etc., then click **Add**>>. The selected item appears in the "Applied Rules" list box. Repeat for each item needed

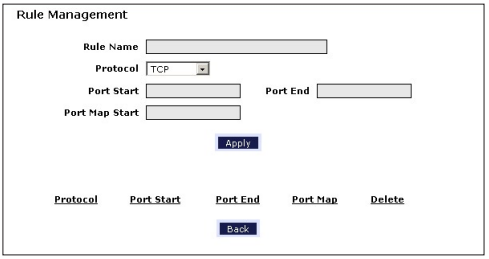
To remove an item from the Applied Rules list, highlight it, then click **Remove**.

To view an item's rules (forwarded ports, etc.), highlight it, then click **View Rule.**

When finished with this screen, click **Apply** to save the changes.

Rule Management

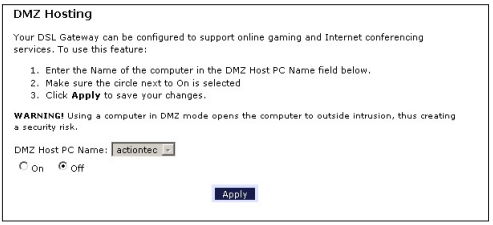
To create a custom set of rules, click the "User" radio button, then click **New**. The "Rule Management" screen appears.



In this screen, the user can create a custom set of rules for a game or application not listed in the Applications screen. Enter the "Rule Name," "Protocol," "Port Start," "Port End," and "Port Map" in the appropriate text boxes, then click **Apply**. The rules are summarized at the bottom of the screen, and the rule set will appear in the Applications screen after clicking **Back**.

DMZ Hosting

Selecting **DMZ Hosting** in the "Security" screen generates the "DMZ Hosting" screen. To use DMZ hosting, select the computer on the network to be used as a DMZ host in the "DMZ Host PC Name" drop-down menu, then click **On**.



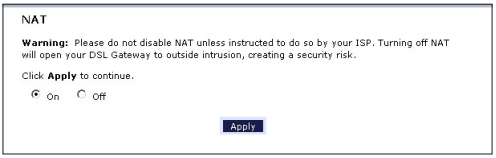
DMZ hosting is used to support online gaming and Internet conferencing services. These programs usually require multiple open ports, making the network accessible from the Internet. DMZ hosting symbolically places the DMZ host computer outside of the Gateway's network. We recommend activating DMZ hosting only as long as necessary.

When finished with this screen, click **Apply** to save the changes.

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

NAT (Network Address Translation)

Selecting **NAT** in the "Security" screen generates the "NAT" screen. The Gateway's basic firewall security is based on NAT. Disabling NAT allows the computers connected to the Gateway to be accessed by outside parties, and can cause the loss of Internet connectivity. Do not turn NAT off unless instructed to do so by Verizon.



When finished with this screen, click **Apply** to save the changes.

Port Mapping

Selecting **Port Mapping** in the "Security" screen generates the "TR-069 PortMapping Log" screen. This screen displays a log that lists port mapping changes made remotely by the service provider via the TR-069 protocol. This log is for information only, and should be consulted only if requested by the service provider or support technicians. No changes to the Gateway can be made from this screen.

Configuring Parental Controls

7

This chapter explains how to configure the parental control capabilities of the Gateway, such as services blocking, Web site blocking, and schedule rules.

Accessing Parental Control Screens

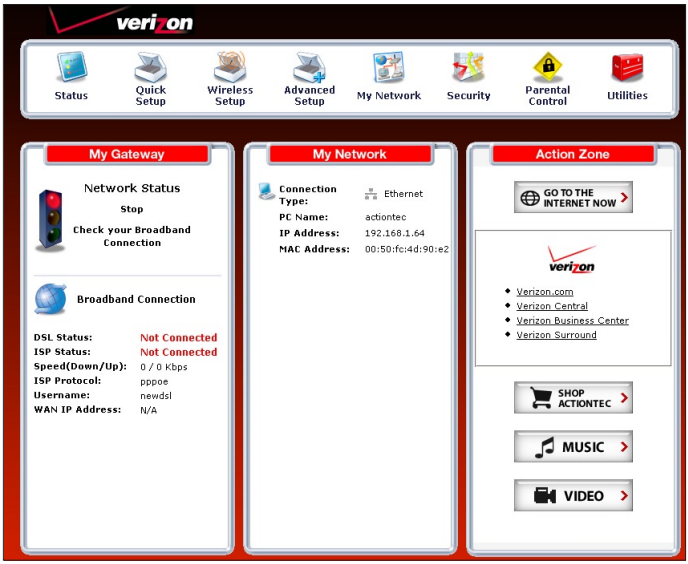
To access the Parental Control configuration screens, follow these instructions:

1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.1.1`

   then press **Enter** on the keyboard.

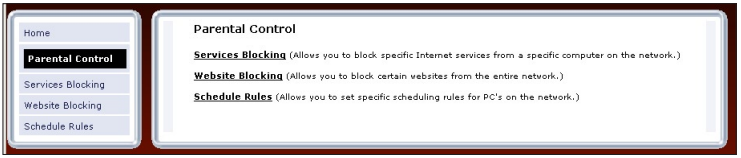
2. The "Home" screen appears. Click **Parental Control**.



3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

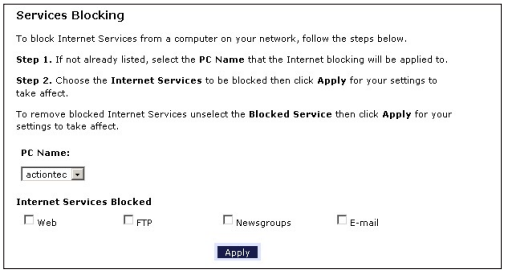
☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Parental Control" screen appears. To modify a specific setting, click on its name in the menu bar on the left, or from the list in the middle of the screen.



Services Blocking

Selecting **Services Blocking** in the Parental Control screen generates the "Services Blocking" screen.

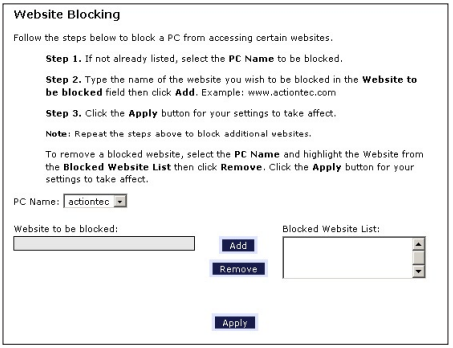


To modify Internet privileges (Web, FTP, Newsgroups, etc.) for the computers on the network:

1. Select the computer's network name from the "PC Name" drop-down menu.
2. Select the Internet service(s) to be blocked by clicking in the appropriate check box.
3. Click **Apply** to block the selected service from the selected computer.

Website Blocking

Selecting **Website Blocking** in the Parental Control screen generates the "Website Blocking" screen. This feature enables the Gateway to block Web sites to any or all computers on the network. To block a Web site, select the computer name from the "PC Name" drop-down menu. Then, enter the address of the Web site to be blocked 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 the selected computer on the network. To block the Web site from another computer on the network, repeat the process. To remove a blocked Web site, click on it in the "Blocked Website List," then click **Remove**. When finished, click **Apply**.



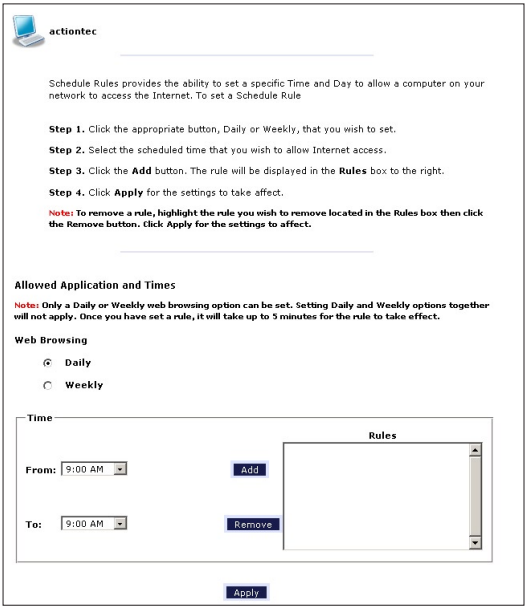
Schedule Rules

Selecting **Schedule Rules** in the Parental Control screen generates the "Schedule Rules" screen. Schedule rules allow computers on the network to access the Internet at scheduled times only.

To set up schedule rules for a computer on the network:

1. Select the computer's network name from the "PC Name" drop-down menu.

2. Click **View/Edit Access Details**. The computer's "Allowed Application and Times" screen appears.

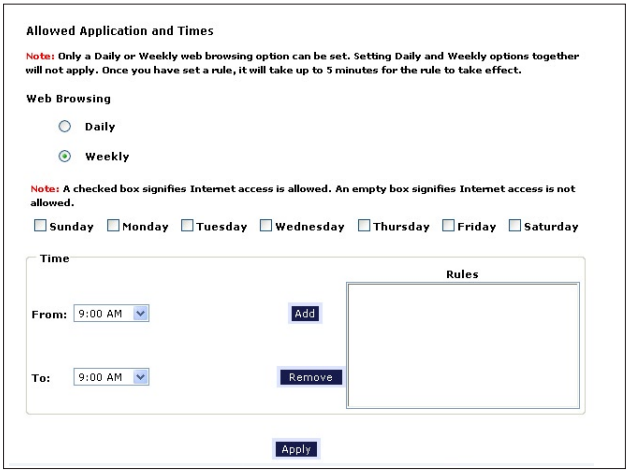


3. To schedule Internet access at the same time every day, select "Daily" by clicking the appropriate radio button. If creating different access schedules on a day-to-day basis, select "Weekly."

4a. If "Daily" was selected in step 3, create a period of Internet access (or rule) by selecting a beginning time (from the "From" drop-down menu) and ending time (from the "To" drop down menu). If allowing Internet access to a particular computer from 6 p.m. to 8 p.m., for example, select "18 (6 pm)" from the From drop-down menu, and "20 (8 pm)" from the To drop-down menu. Click **Add** to add the access period to the "Rules" list box. Additional access periods can be added by repeating this step (9 a.m. through 12 p.m., for example), and adding it to the Rules list box. Once the rules are applied in the Daily screen, Internet access will be granted every day at the times listed in the Rules list box.

☞ ***Note:*** When using "Daily" scheduling, an access period cannot include 12 a.m (midnight). To create an access period that includes midnight, create two access periods, one that ends at 12 a.m., and one that begins at 12 a.m.

4b. If "Weekly" was selected in step 3, periods of Internet access can be scheduled at different times on different days (6 p.m. to 8 p.m. on Friday, and 1 p.m. to 4 p.m. on Saturday, for example). To do this, select the day of the week by clicking in the appropriate check box, then create a access period (or rule), as explained in step 4a. Click **Add** for each separate time period. All access periods created will appear in the Rules list box. Once the rules are applied in the Weekly screen, Internet access will be granted to a particular computer at the days and times selected on a weekly basis.



☞ ***Note:*** When using "Weekly" scheduling, an access period cannot include 12 a.m (midnight). To create an access period that includes midnight, create two access periods, one that ends at 12 a.m. on one day, and one that begins at 12 a.m on the following day.

5. When finished with all scheduling, click **Apply** to save the changes to the Gateway.

Removing a Schedule Rule

To remove a scheduled rule, select it from the Rules list box, then click **Remove**. The schedule rule will disappear from the Rules list box.

Configuring the Gateway's Utilities

8

This chapter explains how to use the Gateway's utilities, including how to restore default settings, upgrade the Gateway's firmware, and perform a ping test.

Accessing the Utilities Screens

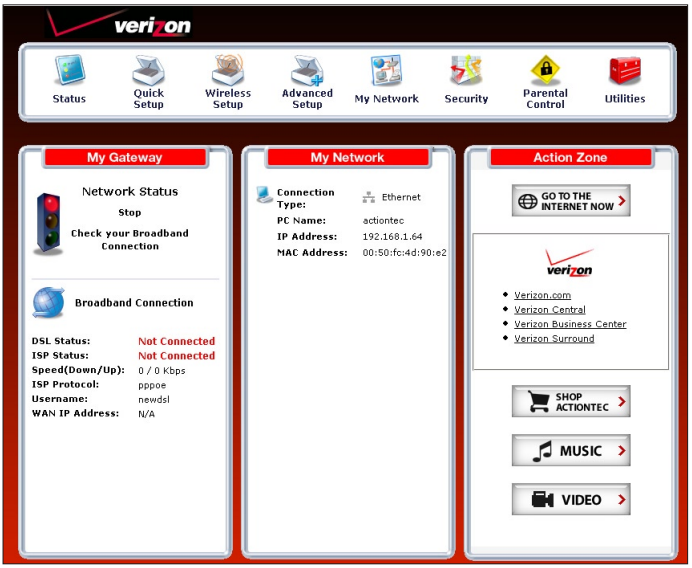
To access the Utilities configuration screens, follow these instructions:

1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.1.1`

   then press **Enter** on the keyboard.

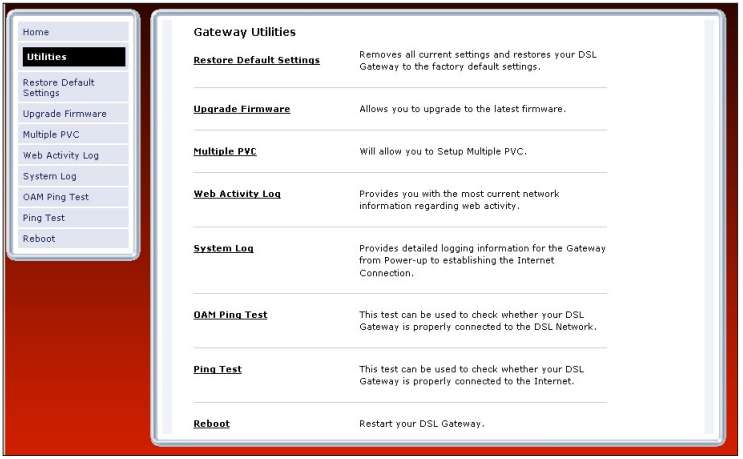
2. The "Home" screen appears. Click **Utilities**.



3. A login window appears. Enter the user name and password in the appropriate text boxes, then click **OK**.

☞ ***Note:*** The default user name is "admin." The default password is "password."

4. The "Utilities" screen appears. To modify a specific configuration, click on its name in the menu bar on the left, or from the list in the middle of the screen.



Restore Default Settings

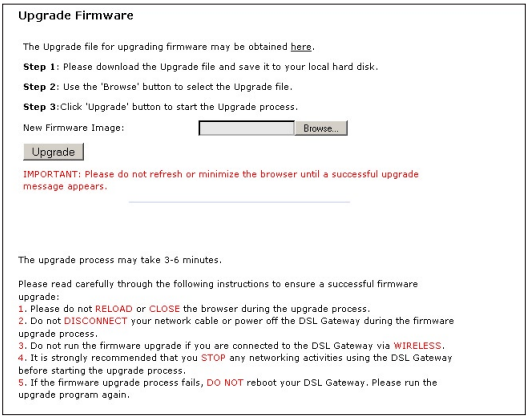
To restore the Gateway to its factory default settings, select **Restore Default Settings** from the Utilities screen. When the "Restore Default Settings" screen appears, click **Restore Default Settings**. Any changes made to the Gateway's settings will be lost and the factory default settings restored. During this process, the Gateway's Power light flashes and the Gateway is disabled.

Warning: Do not unplug the Power cord from the Gateway during the Restore Default Settings process. Doing so may result in permanent damage to the Gateway.

When the Power Light stops flashing and glows steadily green, the Gateway is fully operational.

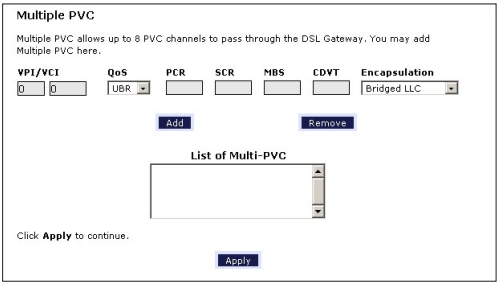
Upgrade Firmware

Selecting **Upgrade Firmware** in the Utilities screen generates the "Upgrade Firmware" screen. Firmware upgrades are periodically released to enhance the Gateway's capabilities. Follow the instructions on-screen to upgrade the Gateway's firmware.



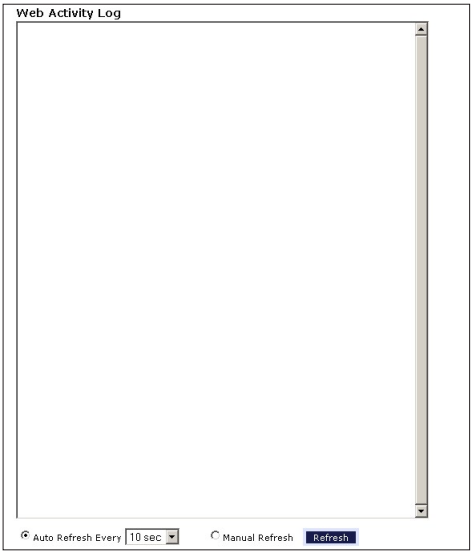
Multiple PVC

Selecting **Multiple PVC** in the Utilities screen generates the "Multiple PVC" screen, which allows the configuration of multiple PVCs.



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.



Auto Refresh

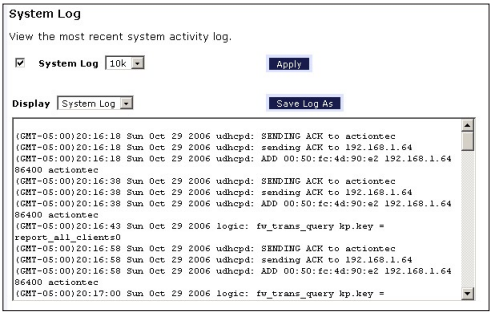
To set the Web Activity Log screen to automatically refresh at certain intervals, activate the circle next to "Auto Refresh Every" at the bottom of the Web Activity Log screen, then enter a time value (in seconds) in the text box, or click on the down arrow and select a time value from the menu that appears. The Web Activity Log will refresh at the selected interval.

Manual Refresh

To set the Web Activity Log screen to manually refresh, activate the circle next to "Manual Refresh" at the bottom of the Web Activity Log screen. To refresh the Web Activity Log screen, click **Refresh**.

System Log

The System Log provides information about the Gateway's activity. To access the System Log, select **System Log** from the Utilities screen.



System Log (Size)

Select the size of the system log displayed here. The smaller the size, the shorter the length of the system log saved.

Display

View other saved logs by selecting a log from this drop-down list.

Apply

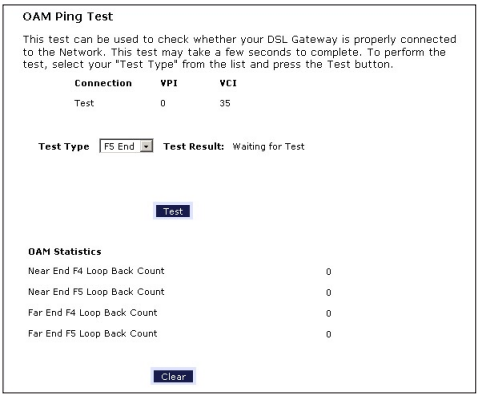
Pressing this button saves any changes to the System Log screen and causes the Save and Restart screen to appear.

Save Log As

Pressing this button allows the user to save a log as a file.

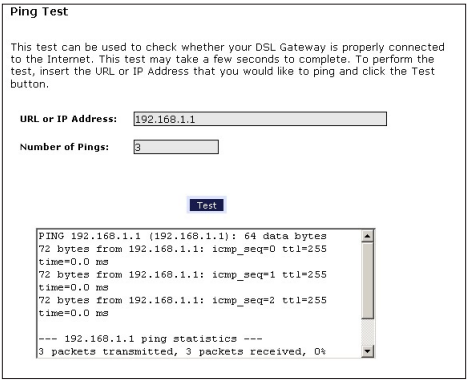
OAM Ping Test

Selecting **OAM Ping Test** from the Utilities screen generates the "OAM Ping Test" screen, which is used to check whether the Gateway is properly connected to the network. Follow the on-screen instructions to perform the test.



Ping Test

Selecting **Ping Test** from the Utilities screen generates the "Ping Test" screen, which is used to check whether the Gateway is properly connected to the Internet. Follow the on-screen instructions to perform the test.



Reboot

Selecting **Reboot** from the Utilities screen generates the "Reboot" screen. From this screen, the Gateway can be rebooted. To do this:

1. From the first Reboot screen, click **Reboot**.

2. A confirmation window appears. Click **OK**.

3. The Gateway reboots. Read the onscreen information in the screen that appears.

When the Gateway's Power light stops flashing, the Gateway has rebooted.

Troubleshooting 9

This chapter contains a list of problems that may be encountered while using the Gateway, and techniques to try and overcome the problem. Note that these techniques may not solve the problem. This chapter also include a list of frequently asked questions.

Troubleshooting

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" in chapter 3), 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 cord and all network cables are properly connected.
- 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.
- If running Windows 98 SE or Me, check the computer's TCP/IP settings. Select **Start**, **Run**, enter

  `winipcfg`

  in the "Open" text box, then press **OK**. The "IP Configuration" window appears. Ensure the text box at the top of the window contains the name of the Ethernet adapter installed in the computer. If not, click on the down arrow next to the

text box. When the list appears, click on the proper Ethernet adapter.
In the fields below, the Ethernet adapter's various addresses appear. There should be an entry for IP address, Subnet Mask, and Default Gateway. Additionally, the "IP Address" entry should be on the 192.168.1.x network (with "x" defining a range from 2 though 255).
If the Ethernet adapter is showing an incorrect IP address, click **Release**, which sets all values back to 0 (zero). Then, click **Renew** (this process may take a few seconds). The renewed IP address should be on the 192.168.1.x network.
If an error occurs, or the IP address renews with an address outside the 192.168.1.x network, contact the ISP immediately.

- If running Windows 98 SE, Me, 2000, or XP, check the computer's TCP/IP settings. Select **Start**, **Run**, enter

  CMD

  in the "Open" text box, then press **OK**. A "DOS" window appears, with a blinking cursor (prompt). Enter

  ipconfig

  at the cursor, then press **Enter** on the keyboard.
  The IP address of the Ethernet adapter should appear in the DOS window. Ensure the IP address in the 192.168.1.x network (with "x" defining a range from 2 though 255).
  If the Ethernet adapter is showing an incorrect IP address, enter

  ipconfig /release

  at the cursor, then press **Enter** on the keyboard, which sets all values back to 0 (zero). Next, enter

  ipconfig /renew

  at the cursor, then press **Enter** on the keyboard (this process may take a few seconds). The renewed IP address should be on the 192.168.1.x network.
  If an error occurs, or the IP address renews with an address outside the 192.168.1.x network, contact the ISP immediately

- Ensure the browser is not set to "Never dial a connection" and there are no previous LAN settings.
  To check this, go to **Start**, **Settings**, **Control Panel**. In the Control Panel, double-click **Internet Options**. When the "Internet Properties" window appears, ensure that the "Never dial a connection" option is not activated, then click **LAN Settings**. When the "Local Area Network (LAN) Settings" window appears, ensure that no settings are activated. If there are settings activated, deactivate them.

- Shutdown and restart the computer. After the computer restarts, unplug the power cord from the Gateway and plug it back in. When the lights glow solid green, try accessing the Internet.

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.

Frequently Asked Questions

This section includes a list of questions concerning the Gateway, and answers to those questions.

General

I have run out of Ethernet ports on my Gateway. How do I add more computers?

Plugging in an Ethernet hub or switch expands the number of ports on the Gateway. Run a standard Ethernet cable from the "Uplink" port of the new hub or switch to an Ethernet port on the Gateway.

Which protocols does the Gateway support?

The internal LAN connections support multiple protocols (e.g. TCP/IP, NetBEUI, IPX/SPX, and AppleTalk). The External WAN connection supports only TCP/IP.

Which connection speeds does the Gateway support?

The LAN connections on the Gateway support 10/100 Mbps. The WAN connection supports 8 Mbps, because of the physical restrictions placed on broadband connections. The 802.11g wireless connection supports up to 54 Mbps connection speeds (depending on signal quality, environmental factors, and physical distance).

Will my Xbox work with the Gateway?

Yes, the Gateway is compatible with the Xbox. You need to set a static IP on the Xbox in the Xbox live network settings, and forward ports 3074 (both UDP and TCP), 53 (both UDP and TCP), and 88 (UDP) if you run into DSL resolution errors.

Is the Gateway flash-upgradeable? How do I do it?

Yes, the firmware is upgradeable. You can find a link to the firmware site under "Utilities" in the Web-based configurator.

Does the Gateway function as a DSL modem?

Yes, the Gateway has a built-in DSL Modem.

Wireless

Can I use an 802.11b wireless card to connect to the Gateway?

Yes, the Gateway can handle 802.11b cards or 802.11g cards. The 802.11g standard is backward compatible with the 802.11b standard. The Gateway can be setup to handle just "g" wireless cards, just "b" wireless cards, or both.

If I install several Gateways in different locations in my building, will they be able to talk to each other? Will I be able to stay connected as I move between them?

The Gateway does not communicate with other access points, since it functions as a single access point system. If you installed several Gateway devices and were to move between coverage areas, your wireless device would have to reconnect to a separate network.

Which wireless cards will work with the Gateway?

The Gateway connects with any wireless card supporting the 802.11g/802.11b wireless standards.

Can my wireless signal pass through floors, walls, and glass?

The physical environment surrounding the Gateway can have a varying effect on signal strength and quality. Generally, the more dense the object (a concrete wall compared to a plaster wall, for example), the greater the interference. Concrete or metal-reinforced structures will experience a higher degree of signal loss than those made of wood, plaster, or glass.

I have an Apple computer that uses the Airport wireless device. Is this device compatible with the Gateway?

Yes, the Apple Airport system complies with the 802.11b standards. If you be use the WEP security feature, refer to the Apple Airport documentation for information on the proper method to enter the WEP key for compatibility with the Gateway's hexadecimal WEP entry.

Network

I use my laptop at work and at home. Is there something special I need to do to make it work in both places?

Yes. Reconfigure your network setting (Workgroup, Domain, Password, User name, IP addressing or any other specific settings used by your company). You may also use third party software like NetSwitcher to automatically switch between different configurations.

What is the valid IP range I can use for my home network?

The valid IP range for the Gateway is 192.168.1.64 to 192.168.1.254 by default.

How do I find out what IP address my computer is using?

Windows 95, 98, 98SE, and Me - Select **Start**, **Run**, and type "winipcfg." Press **Enter**. When the "Winipcfg" window appears, ensure your network device is selected.

Windows NT, 2000, and XP - Select **Start**, **Run** and type "cmd." Press **Enter**. When the command screen appears, type "ipconfig" and press **Enter**.

I used DHCP to configure my network. Do I need to restart my computer to refresh my IP address?

No. Follow these steps to refresh your IP address:

Windows 95, 98, 98SE, and Me - Select **Start**, **Run**, type "winipcfg," and press **Enter**. Ensure the Ethernet adapter is selected in the device box. Press the **Release_all** button, then press the **Renew_all** button.

Windows NT 4.0 and 2000 - Select **Start**, **Run**, type "cmd," and press **Enter**. At the DOS prompt, type "ipconfig /release," then type "ipconfig /renew."

Windows XP - Unplug the Ethernet cable or wireless card and plug it back in.

Can I run an application located on another computer over the network?

Yes, if the application is designed to run over a network.

Can I play games between computers on my network, or on the Internet?

Yes, if the games were designed for multi-player or LAN play. For specific information about whether a game is capable of Internet or LAN play, refer to the game documentation. Some games require ports to be forwarded to host or join games over the Internet.

I have an FTP or Web server on my network. How can I make it available to users on the Internet?

For a Web server, enable port forwarding for port 8088 to the IP address of the server and set up the Web server to receive on that port, as well. (Configuring the server to use a static IP address is recommended.)
For an FTP server, enable port forwarding for port 21 to the IP address of the server. (Configuring the server to use a static IP address is recommended.)

Connections

How many computers can be connected through the Gateway?

The Gateway is capable of 254 connections, but it is recommended to have no more than 45 connections. As you increase the number of connections, you decrease the available speed for each computer.

Security

What is the default username for the Gateway?

The default username for the router is "admin" and the default password is "password" (all lower case, no quotation marks). To activate the password to protect the Gateway, change the default password. Remote management will not be available on the Gateway until the default password is changed.

Does the Gateway function as a firewall?

Yes. The Gateway provides its security through the use of NAT firewall, which acts as a physical barrier between your network and the Internet.

What is NAT and how does it protect my network?

NAT (Network Address Translation) is a type of security that masks the private IP addresses of the computers on your network with a single public IP address. With NAT, the private IP address of the computers on your network is never transmitted over the Internet.

Which Virtual Private Networking (VPN) protocols are supported?

The Gateway supports pass-through for PPTP, L2TP, and IPSec.

This page left intentionally blank.

Reference

A

This appendix contains information about various topics, including accessing information about your Windows computer.

Locating Computer Information

The following procedure is valid for Windows 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 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 XP

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.

Switching to Static IP on the Computer

B

To communicate with the Gateway from a computer on the network (to access the Web Configuration screens, for example), the user may have to switch the IP address settings from DHCP-enabled to static IP, so that the computer and the Gateway are on the same subnet.

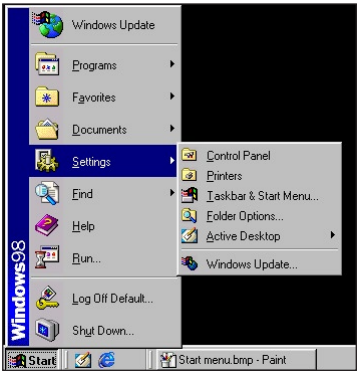
To set up static IP on a computer, select the operating system and follow the instructions.

☞ ***Note***: The following procedures are based on the Gateway's factory default IP address. If the Gateway's IP address has been changed, enter the new IP address when instructed to enter an IP address.

Windows 98 SE

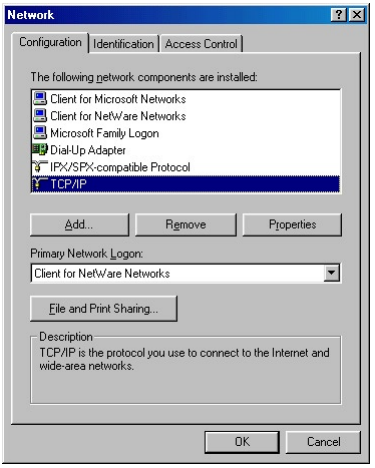
1. From the desktop, click **Start** in the lower left corner.
2. From the menu that appears, select **Settings**.

3. Another menu appears. Select **Control Panel**.

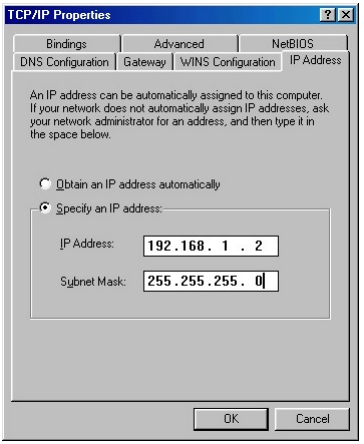


4. When the "Control Panel" window appears, double-click **Network**.

5. The "Network" window appears. In the "The following network components are installed" list box, locate and double-click **TCP/IP**.



6. The "TCP/IP Properties" window appears. Select **IP Address**.



7. In the IP Address tab, make sure the the circle next to "Specify an IP Address" is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.

8. Enter the following numbers in the "IP Address" text box:

`192.168.1.2`

Do not include the periods; they are automatically entered.

9. Enter the following numbers in the "Subnet mask" text box:

   `255.255.255.0`

   Do not include the periods; they are automatically entered.

10. Click **OK**. The TCP/IP Properties window disappears.

11. In the Network window, click **OK**. The Network window disappears.

12. The "System Settings Change" window appears, asking whether the computer should be restarted. Click **Yes**.

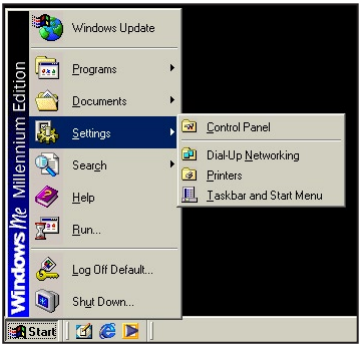
The computer restarts. It is now set up with a static IP address, allowing the user to access the Gateway's Web Configuration Utilities (Advanced Setup, Utilities, etc.).

Windows Me

1. From the desktop, click **Start** in the lower left corner.

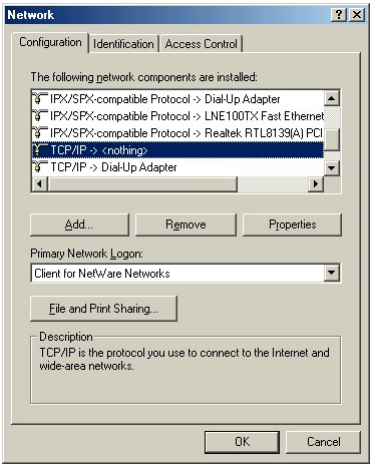
2. From the menu that appears, select **Settings**.

3. Another menu appears. Select **Control Panel**.

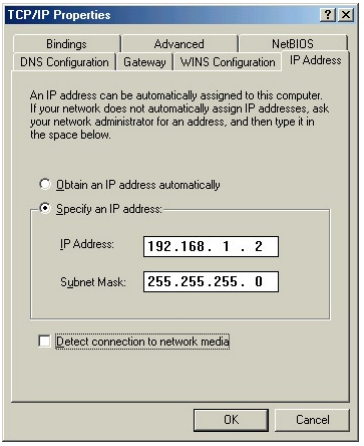


4. When the "Control Panel" window appears, double-click **Network**.

5. The "Network" window appears. In the "The following network components are installed" list box, locate and double-click **TCP/IP**.



6. The "TCP/IP Properties" window appears. Click **IP Address**.



7. In the "IP Address" tab, make sure the the circle next to "Specify an IP Address" is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.

8. Enter the following numbers in the "IP Address" text box:

`192.168.1.2`

Do not include the periods; they are automatically entered.

9. Enter the following numbers in the "Subnet mask" text box:

`255.255.255.0`

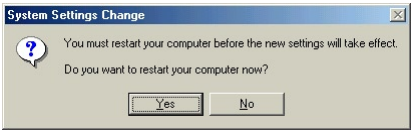
Do not include the periods; they are automatically entered.

10. Click **OK**. The TCP/IP Properties window disappears.

11. If there is a check in the box next to "Detect connection to network media," click on it to uncheck the box.

12. In the Network window, click **OK**. The Network window disappears.

13. The "System Settings Change" window appears, asking whether the computer should be restarted. Click **Yes**.



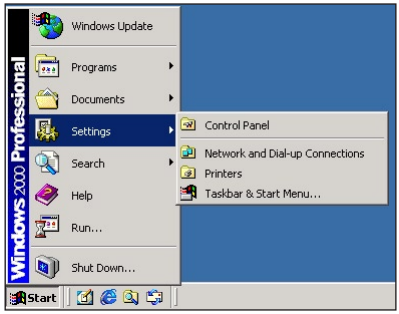
The computer restarts. It is now set up with a static IP address, allowing the user to access the Gateway's Web Configuration Utilities (Advanced Setup, Utilities, etc.).

Windows 2000

1. From the desktop, click **Start** in the lower left corner.

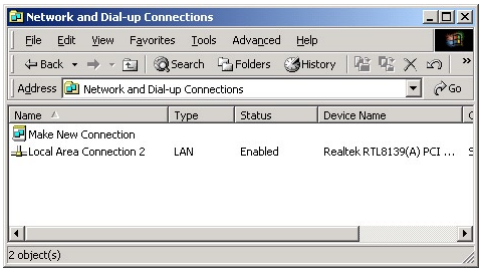
2. From the menu that appears, select **Settings**.

3. Another menu appears. Select **Control Panel**.

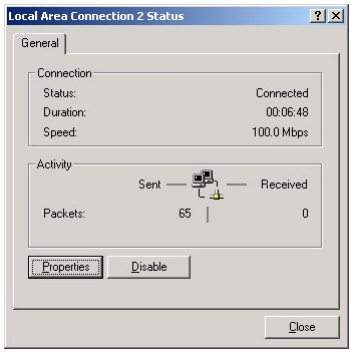


4. When the "Control Panel" window appears, double-click **Network and Dial-up Connections**.

5. In the "Network and Dial-up Connections" window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If there is more than one Local Area Connection listed, locate the one that corresponds to the network card installed in the computer by finding the name of the network card in the "Device Name" column.

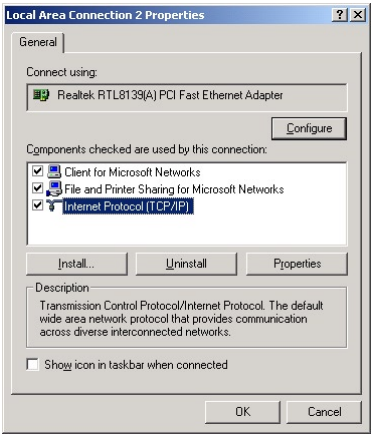


6. The "Local Area Connection Status" window appears. Select **General**, then click **Properties**.

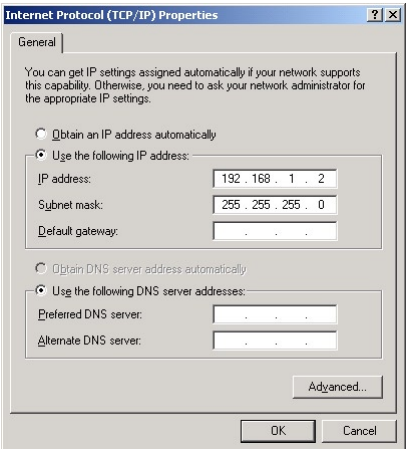


7. The "Local Area Connection Properties" window appears. Click **General**.

8. In the "Components checked are used by this connection" list box, double-click **Internet Protocol (TCP/IP)**.



9. The "Internet Protocol (TCP/IP) Properties" window appears.



10. In the "General" tab, make sure the the circle next to "Use the following IP Address " is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.

11. Enter the following numbers in the "IP Address" text box:

`192.168.1.2`

Do not include the periods; they are automatically entered.

12. Enter the following numbers in the "Subnet mask" text box:

`255.255.255.0`

Do not include the periods; they are automatically entered.

13. Click **OK**. The "Internet Protocol (TCP/IP) Properties" window disappears.

14 In the "Local Area Connection Properties" window, click **OK**. The Local Area Connection Properties window disappears.

15. Click **Close** in the Local Area Connection Status window. The window disappears.

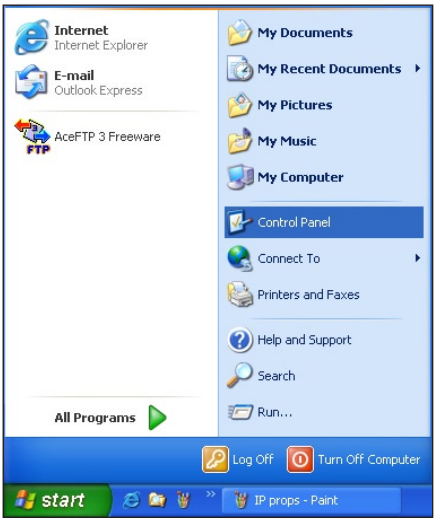
16. Close the Network and Dial-up Connections window by clicking on the "**x**" button at the upper right corner of the window.

The computer restarts. It is now set up with a static IP address, allowing the user to access the Gateway's Web Configuration Utilities (Advanced Setup, Utilities, etc.).

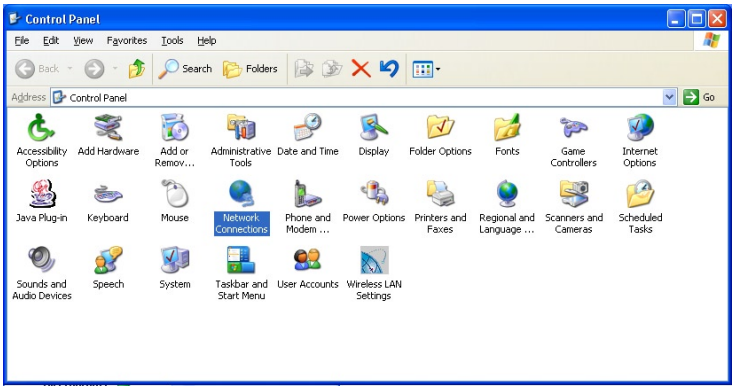
Windows XP

1. From the desktop, click **Start** button in the lower left corner.

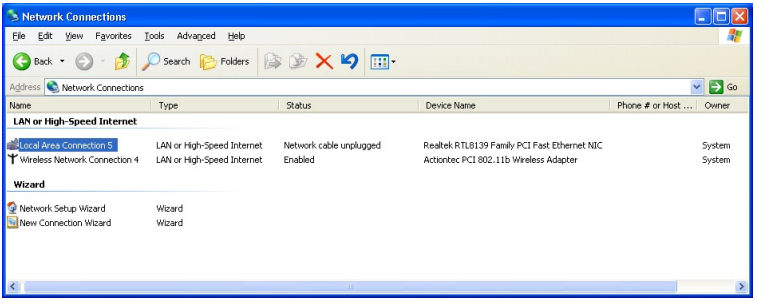
2. From the menu that appears, select **Control Panel**.



3. When the "Control Panel" window appears, double-click **Network Connections**.

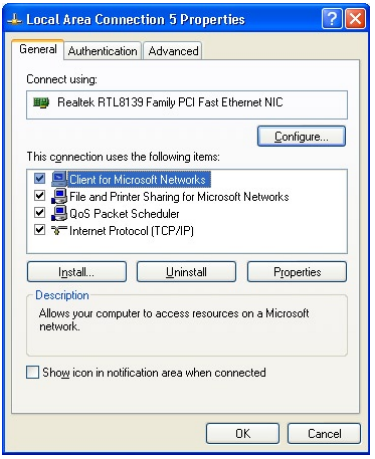


4. In the "Network Connections" window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If more than one Local Area Connection is listed, locate the one that corresponds to the network card installed in your computer by finding the name of the network card in the "Device Name" column.

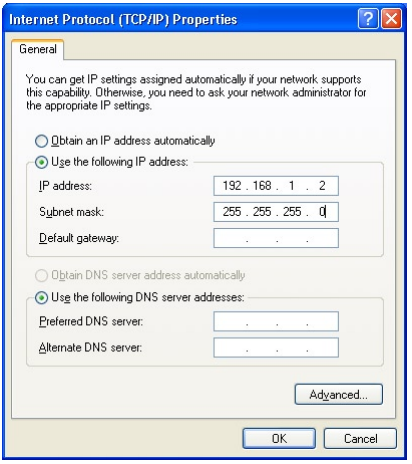


5. The "Local Area Connection Properties" window appears. Select **General**.

6. In the "This connection uses the following items" list box, double-click **Internet Protocol** (TCP/IP).



7. The "Internet Protocol (TCP/IP) Properties" window appears.



8. In the **General** tab, make sure the circle next to "Use the following IP Address" is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.

9. Enter the following address in the "IP Address" text box:
   `192.168.1.2`
   Enter the periods in the address by pressing the space bar on the keyboard.

10. Enter the following address in the "Subnet mask" text box:
    `255.255.255.0`
    Enter the periods in the address by pressing the space bar on the keyboard.

11. Click **OK**. The Internet Protocol (TCP/IP) Properties window disappears.

12 In the Local Area Connection Properties window, click **Close**. The Local Area Connection Properties window disappears.

13. Click **Close** in the Local Area Connection Status window. The window disappears.

14. Close the Network and Dial-up Connections window by clicking on the "**x**" button at the upper right corner of the window.

The computer restarts. It is now set up with a static IP address, allowing the user to access the Gateway's Web Configuration Utilities (Advanced Setup, Utilities, etc.).

Computer Security

The Internet is a giant network of computers located all over the world. When a computer is connected to the Internet, it can exchange information with any other computer on the Internet. This allows a computer user to 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, or worse. Unless access to the computer is controlled, someone on the Internet can access the information on the computer and damage or destroy that information.

We recommend securing your computer from unwanted intrusion. Security is ultimately the end user's responsibility. Please secure your computer, and don't be a victim.

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, 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 connected." 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 administrative 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 should be 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 (Internet Explorer or Netscape Navigator, for example). Never "minimize" the browser or leave it open in the background. Breaking into a computer is easier 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, consider installing 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.

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 SE, Me, NT 4.0, or 2000 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.

This page left intentionally blank.

Specifications

D

General

Model Number

GT704-WG (Wireless DSL Gateway)

Standards

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

Protocol

LAN - CSMA/CD
WAN - PPP, DHCP, Static IP

WAN

Full-rate ADSL Interface

LAN

10/100 RJ-45 switched port
USB port

Speed

LAN Ethernet: 10/100 Mbps auto-sensing
Wireless: 802.11g 54 Mbps optimal (see "Wireless Operating Range" for details)

Cabling Type

Ethernet 10BaseT: UTP/STP Category 3 or 5
Ethernet100BaseTX: UTP/STP Category 5
USB

Wireless Operating Range

Indoors

Up to 91M (300 ft.) @ 54 Mbps

Outdoors

Up to 457M (1500 ft.) @ 54Mbps

Topology

Star (Ethernet)

LED Indicators

Power, DSL, Internet, Ethernet (4), USB, Wireless

Environmental

Power

External, 12V DC, 600mA

Certifications

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

Operating Temperature

0º C to 40º C (32ºF to 104ºF)

Storage Temperature

-20ºC to 70ºC (-4ºF to 158ºF)

Operating Humidity

10% to 85% non-condensing

Storage Humidity

5% to 90% non-condensing

Glossary

E

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.

ATM (Asynchronous Transfer Mode)

A networking technology based on transferring data in fixed-size packets

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 your 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

A method to allow wireless data transmissions a level of security.

ESSID (Extended Service Set Identifier)

A unique identifier for a wireless network. Also known as "SSID."

Ethernet Network

A standard wired networking configuration using cables and hubs.

Firewall

A method preventing users outside the network from accessing and/or damaging files or computers on the network.

Gateway

A central device that manages the data traffic of your 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 router. This address is only required when using a cable or DSL modem.

ISP (Internet Service Provider)

A business that allows individuals or businesses to connect 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)

A method allowing all of the computers on a home network to use one IP address, enabling access to the Internet from any computer on the home network without having to purchase more IP addresses from the ISP.

PC Card

An adapter that inserts in the PCMCIA slot of a computer, enabling the communication with a device.

PPPoE (Point-To-Point Protocol over Ethernet)/
PPPoA (Point-To-Point Protocol over ATM)

Methods of secure data transmission.

Router

A central device that manages the data traffic of your network.

Subnet Mask

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

SSID

See "ESSID."

TCP/IP (Transmission Control Protocol/Internet Protocol)

The standard protocol for data transmission over the Internet.

WAN (Wide Area Network)

A network that connects 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.

Service Acronyms

F

The following information is related to the Firewall options (High, Medium, and Low) section in the "Advanced Setup" chapter of this manual. This appendix explains the meaning of the service acronyms included with the various levels of firewall security, and the UDP and TCP ports used by each service.

Service Acronym Definitions

DNS

Domain **N**ame **S**ystem. A data query system used to translate host names into Internet addresses (i.e., www.somewebsite.com translates to 888.999.000.111). Uses UDP 53 and TCP 53.

EPMAP

End**P**oint **Map**per. Uses UDP 135 and TCP 135.

FTP

File **T**ransfer **P**rotocol. A protocol used to transfer files over the Internet. Uses TCP 20 and 21.

HTTP

Hyper**T**ext **T**ransfer **P**rotocol. This protocol delivers information over the Internet, and is used when a computer connects to a Web site via an Internet browser. Uses TCP 80.

HTTPS

Hyper**T**ext **T**ransfer **P**rotocol using **S**ecure Socket Layer. A secure version of the protocol that delivers information over the Internet. Uses UDP 443 and TCP 443.

IMAP, IMAPv3

Internet **M**essage **A**ccess **P**rotocol. Protocols for retrieving E-mail messages. IMAP uses TCP 143; IMAPv3 uses TCP 220.

IPSEC IKE, IPSEC ESP

IP Security. Protocols which support the secure exchange of packets at the IP layer**.** Uses UDP 500.

LDAP

Lightweight **D**irectory **A**ccess **P**rotocol. A set of protocols for accessing information directories. Uses TCP 389.

MICROSOFT-DS, -GC

-DS uses UDP 445 and TCP 445; -GC uses TCP 3268.

NETBIOS-NS, -DGM, -SSN

Network **B**asic **I**nput **O**utput **S**ystem. Three types of DOS BIOS augmentation which add functions for local area networks (LANs). -NS uses UDP 137 and TCP 137; -DGM uses UDP 138; -SSN uses TCP 138.

NNTP

Network **N**ews **T**ransfer **P**rotocol. A protocol used to distribute and retrieve news articles over the Internet. Uses TCP 119.

POP3

Post **O**ffice **P**rotocol 3. Another protocol used to transfer E-mail between computers. Usually employs a pop3 server, and is used to receive mail only. Uses TCP 110.

PROFILE

Uses TCP 136.

SMTP

Simple **M**ail **T**ransfer **P**rotocol. A protocol used to transfer E-mail between computers over the Internet. Can be used to send and receive mail. Uses TCP 25.

SNMP

Simple **N**etwork **M**anagement **P**rotocol. A set of protocols for managing networks. Uses UDP 161.

This page left intentionally blank.