# Wireless DSL Gateway

## GT784WNV

# User Manual

# Contents

**Wireless DSL Gateway User Manual**

# Contents

**Wireless DSL Gateway User Manual (con't)**

# Contents

**Wireless DSL Gateway User Manual (con't)**

# 1



# Introduction

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 networking to the next level, the Wireless DSL Gateway is sure to be one of the keys to your success.

## 1.1 System Requirements

The Gateway must be used with the following systems and software:

- Active DSL service
- Computer with an 10 Mbps or 10/100 Mbps Ethernet connection
- Microsoft Windows XP, Vista, and 7; Mac OS OS X+
- Modern web browser
- TCP/IP network protocol installed on each computer

## 1.2 Features

The Gateway features:

- Plug-and-Play installation support for computers running Windows operating systems (XP, Vista, and 7)
- ADSL WAN port (RJ-14)
- 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
- 12 Mbps USB data rate (full speed) support
- Bridged Ethernet over ATM, PPP over ATM, PPP over Ethernet, Static IP mode
- 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- and 128-bit, WEP/WPA/WPA2 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
- Firmware upgradeable
- Web download support
- 802.11b/g/n support
- WPS support

## 1.3 Important Safety Instructions

When using telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electrical shock, and personal injury, including
the following:

- Do not use this product near water – for example, near a bathtub, kitchen sink, laundry tub, or swimming pool, or in a wet basement;
- Avoid using a telephone (other than a cordless type) during an electrical storm, as there may be a remote risk of electrical shock due to lightning;
- Do not use the telephone to report a gas leak in the vicinity of the leak;
- Use only the power cord and batteries indicated in this manual;
- Do not dispose of batteries in fire, as they may explode – check with local codes for possible special disposal instructions.

### 1.3a Telephone Line Cord Caution

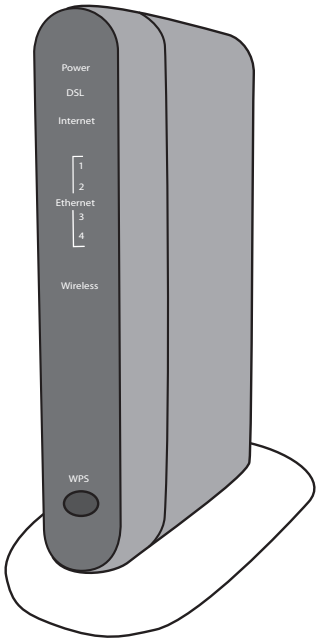
To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord.

## 1.4 Getting to Know the Gateway

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

### 1.4a Front Panel

The front panel of the Gateway features eight indicator LEDs: Power, DSL, Internet, Ethernet (4), and Wireless. It also features the WPS button.



### Power LED

The Power LED 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 LED

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

### Internet LED

When the Internet LED glows steadily, the Gateway is connected to the DSL provider. When it flashes, Internet traffic is moving through the Gateway.

### Ethernet LEDs

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

### Wireless Light

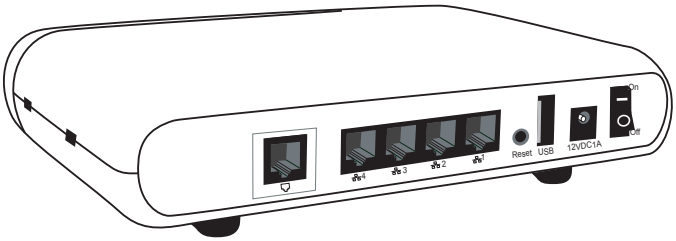
The Wireless light illuminates when the Gateway is connected wirelessly (if the Gateway's Wireless feature is turned on).

### WPS Button

The WPS button activates WPS (WiFi Protected Setup) on the Gateway. See chapter 4, "Configuring Wireless Settings," for more information about WPS.

## 1.4b Rear Panel

The rear panel of the Gateway contains six ports (Ethernet [4], Phone, and Power [12VDC1A]), as well as Reset and Power switches.




### Phone Port

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

### 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.

### 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 ten seconds. The reset process will start after releasing the switch.

## 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.

# 2



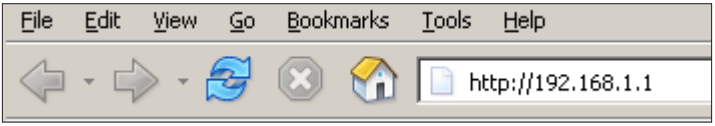
# Quick Setup

This chapter is a guide through a quick set up of the Gateway, including how to connect the Gateway to the ISP. Also included is an overview of the Gateway's Home screen.

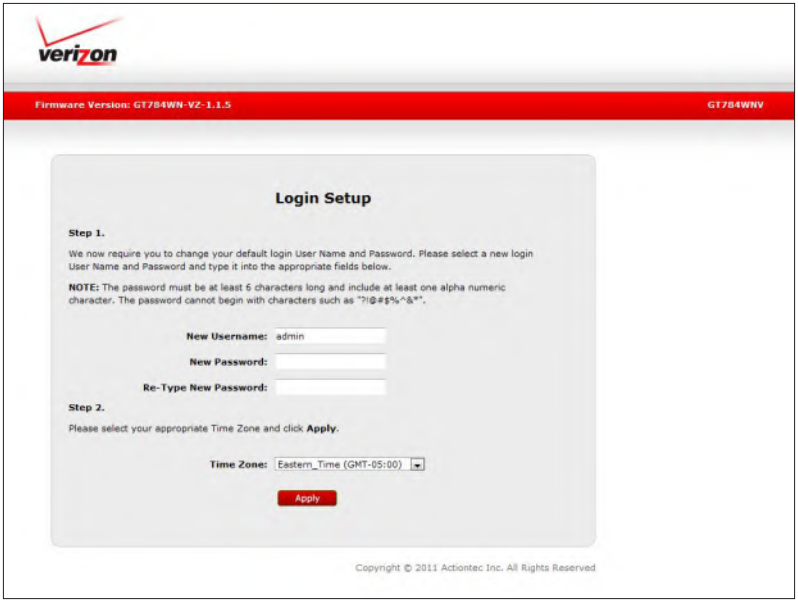
## 2.1 Performing a Quick Setup

To perform a quick setup on the Gateway, have the Welcome Letter or ISP Worksheet handy. If the document is not available, contact the ISP immediately. To access Quick Setup screens:

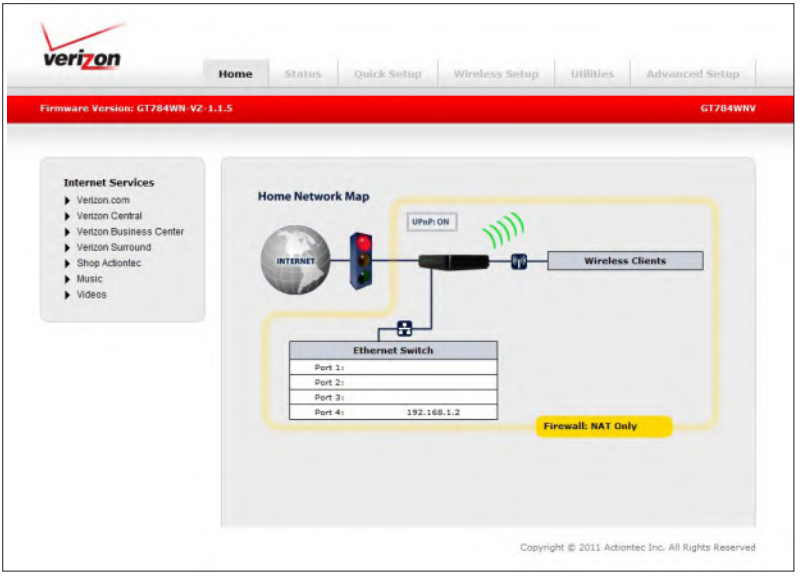
1. Open a Web browser. In the "Address" text box, type:
   **http://192.168.1.1**
   then press **Enter** on the keyboard.



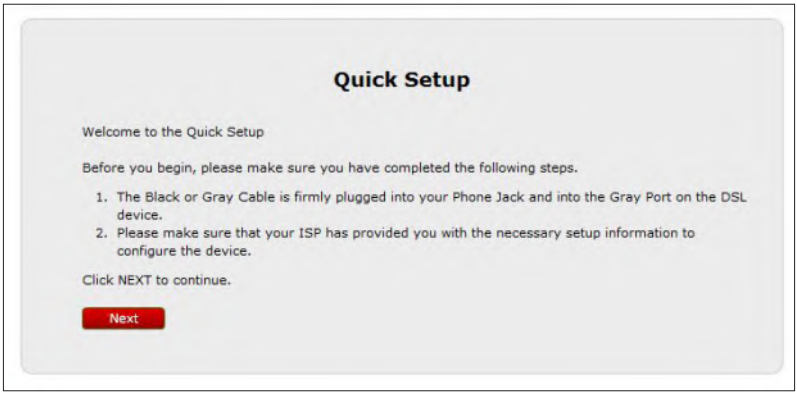

2. The "LogIn" screen appears. Enter a password in both the "New Password" and "Re-type New Password" text boxes. Make sure to write the password down on a piece of paper and keep it in a safe place for future reference, as you will need it to access the Gateway's firmware graphical user interface (GUI).



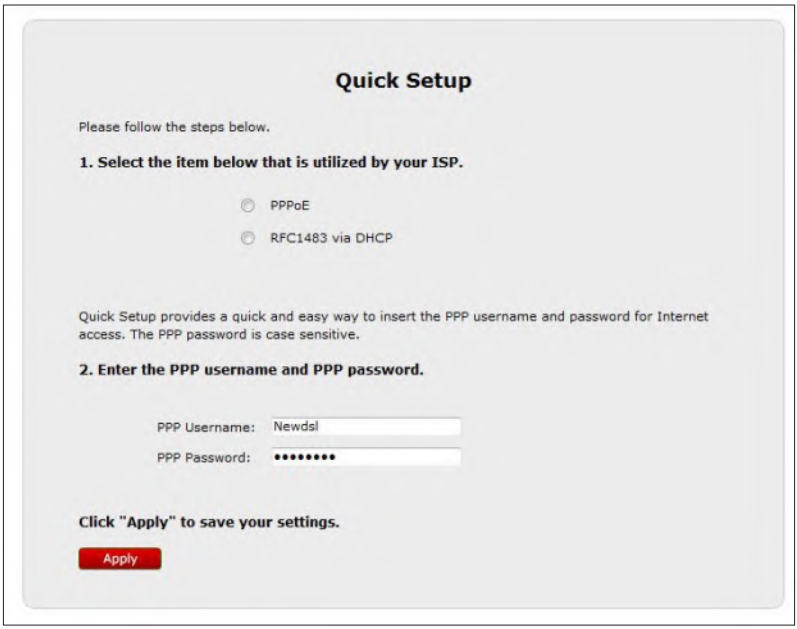
3. Select your local time zone from the "Time Zone" drop-down list.
4. Click **Apply**.
5. After the changes are applied, the Gateway's Home screen appears. Select **Quick Setup** from the row of button above the red bar.



**6.** The first "Quick Setup" screen appears. Read the onscreen instructions, and if you have performed all of the requirements, click **Next**.



7. The second Quick Setup screen appears. Select the network protocol used by your ISP. If you select PPPoE, you must enter the user name and password assigned to you by your ISP in the appropriate text boxes.

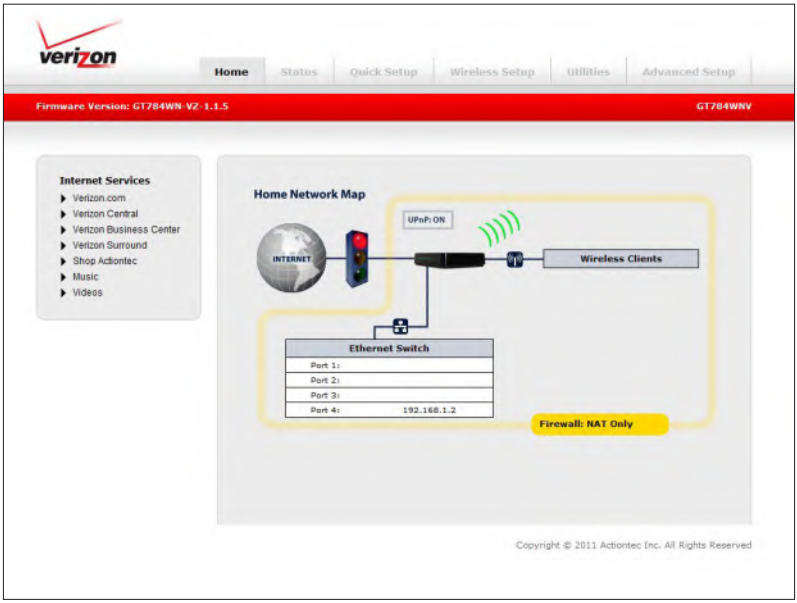



8. Click **Apply**.

The Gateway will reboot. After it does, you will be returned to the Home Screen.

## 2.2 Home Screen

The Gateway's firmware GUI Home screen is the first screen you will normally see after entering the user name and password. This section provides an overview of the Home screen's options.




### 2.2.1 Main Menu

At the top of the screen is the main menu, which contains the important configuration options accessible from the Home screen. **Status** (see chapter 3) contains information regarding the Gateway's connections and other vital statistics; **Quick Setup** (earlier in this chapter) includes a fast and simple procedure to connect to your ISP; **Wireless Setup** (chapter 4) allows you to modify the Gateway's wireless settings and perform other wireless tasks; **Utilities** (chapter 5) contains such items as Reboot, System Log, and Ping Test; and **Advanced Setup** (chapter 6) allows you to make highly technical changes to the Gateway (we recommend that you only make changes to the Advanced Setup settings only if requested to do so by your ISP, or if you are an experienced networking technician).

### 2.2.2 Internet Services

Internet Services is a list of links that will take you to various entertaining or helpful Verizon web sites, including our home page, Verizon Surround, and Verizon Business Center.

### 2.2.3 Home Network Map

The Home Network Map provides a graphical representation of the Gateway's network, both wired and wireless. Any clients connected to the Gateway will be shown, as well as the state of the Gateway's Internet connection, and the state of the Gateway's firewall.

# 3



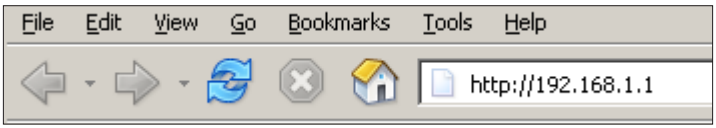
# Status

This chapter guides you through the Gateway's Status screens, including the state of its Internet connection, its firewall status, and a series of other parameters concerning the Gateway's operation.

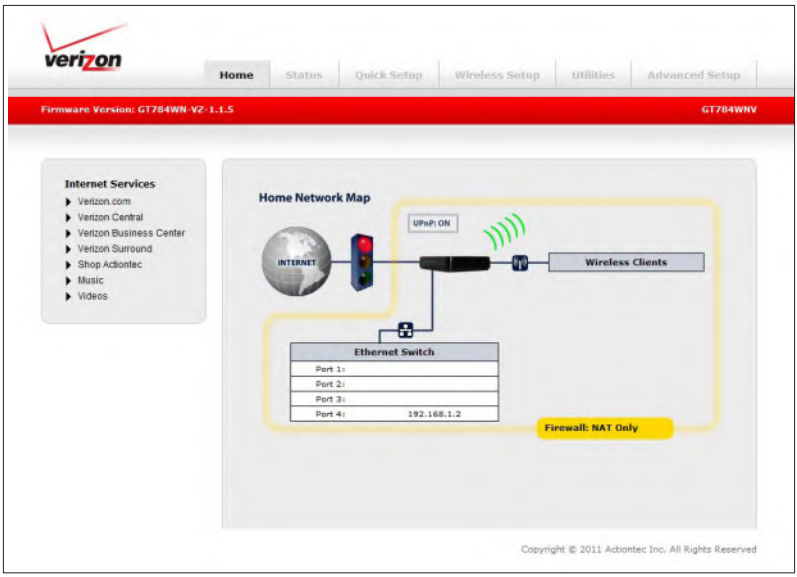
## 3.1 Accessing the Status Screens

To access the Gateway's Status screens:

1. Open a Web browser. In the "Address" text box, type:
   **http://192.168.1.1**
   then press **Enter** on the keyboard.



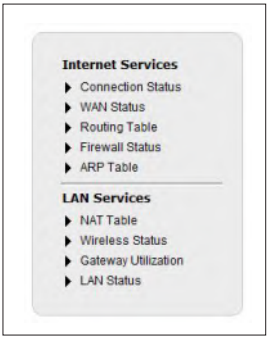

2. After entering your user name and password, the Gateway's Home screen appears. Select **Status** from the row of buttons above the red bar.




3. The first Status screen appears.

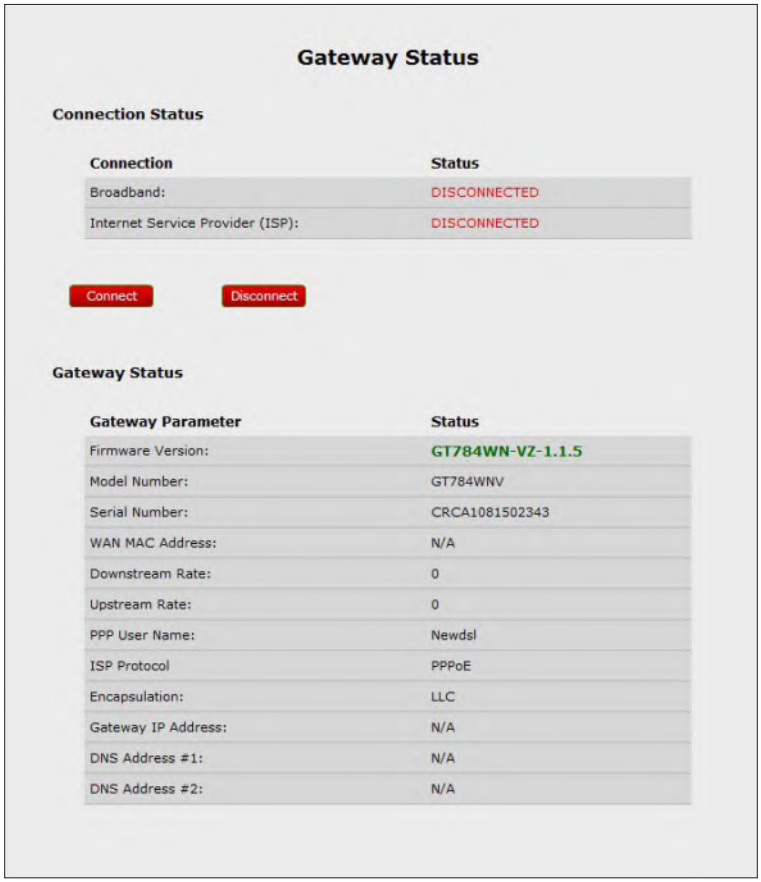
## 3.2 Status Screens

On the left hand side on the first Status screen (and every other Status screen) is the Status menu. Select any option from this menu and you will be taken to that Status screen.



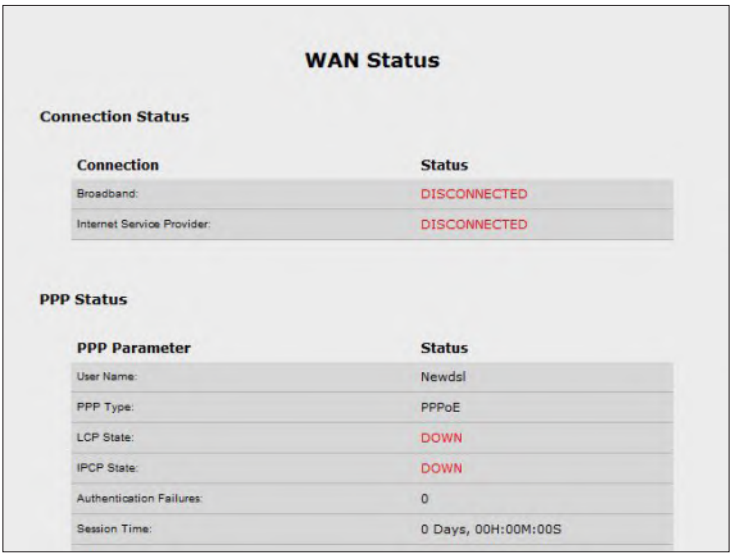
### 3.2.1 Connection Status

Selecting "Connection Status" from the Status menu generates the Connection Status screen. This screen displays various general parameters of the Gateway, including the state of the Gateway's connection, firmware version, model number, and DNS address. The only changes that can be made from the screen are connecting (by clicking **Connect**) or disconnecting (by clicking **Disconnect**) the Gateway from its Internet connection.

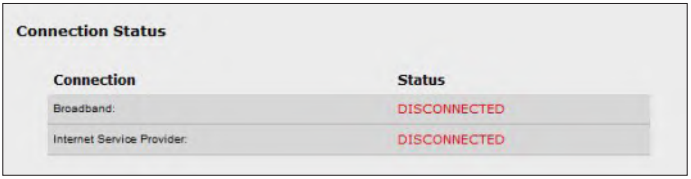


### 3.2.2 WAN Status

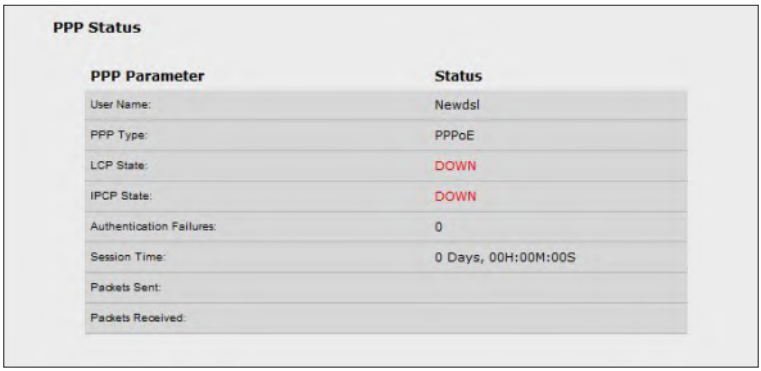
Selecting "WAN Status" from the Status menu generates the WAN (wide area network) Status screen. This screen displays the parameters of the Gateway's connection to the Internet via your service provider. No settings can be changed from here; it is for informational purposes only.




This screen provides an overview of several of the Gateway's connections. At the top is the Gateway's connection status.



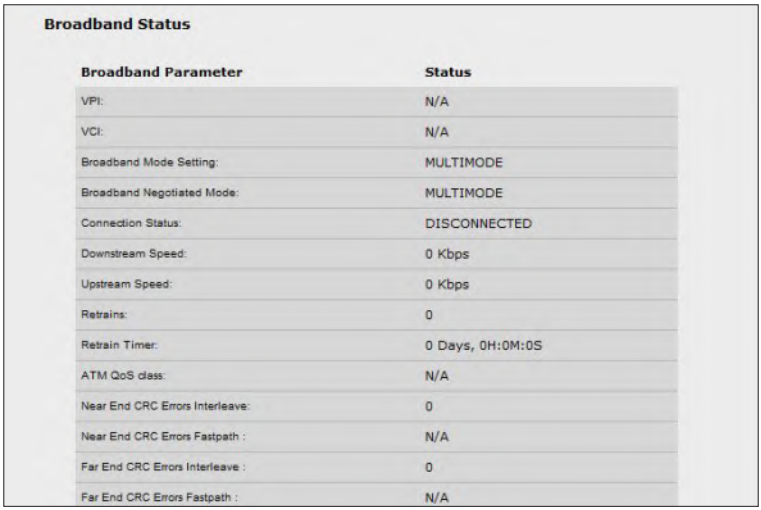
Next is the PPP Status, which displays PPP type, LCP State, and Session Time.



**PPP Status**

| PPP Parameter | Status |
|---|---|
| User Name: | Newdsl |
| PPP Type: | PPPoE |
| LCP State: | DOWN |
| IPCP State: | DOWN |
| Authentication Failures: | 0 |
| Session Time: | 0 Days, 00H:00M:00S |
| Packets Sent: | |
| Packets Received: | |

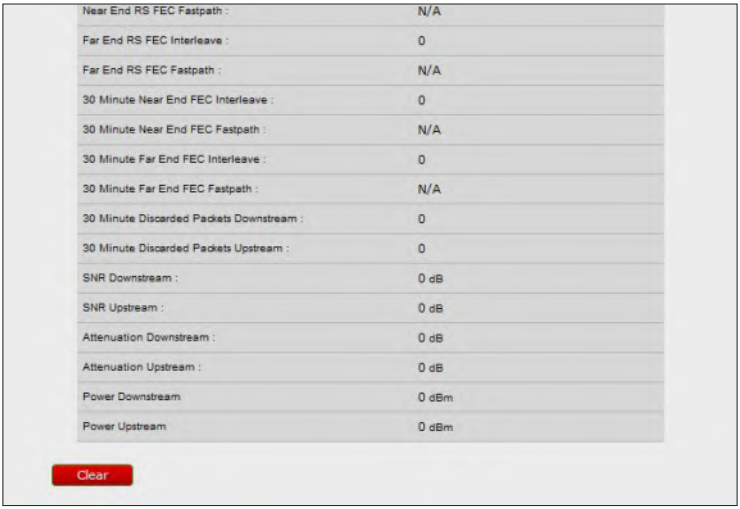
In the Broadband Status section, the VPI, VCI, Upstream Speed, and Retrain Timer, among other parameters, are displayed.



**Broadband Status**

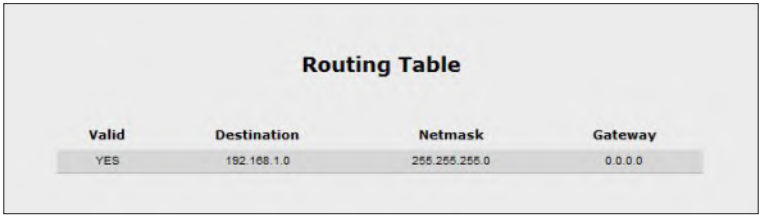
| Broadband Parameter | Status |
|---|---|
| VPI: | N/A |
| VCI: | N/A |
| Broadband Mode Setting: | MULTIMODE |
| Broadband Negotiated Mode: | MULTIMODE |
| Connection Status: | DISCONNECTED |
| Downstream Speed: | 0 Kbps |
| Upstream Speed: | 0 Kbps |
| Retrains: | 0 |
| Retrain Timer: | 0 Days, 0H:0M:0S |
| ATM QoS class: | N/A |
| Near End CRC Errors Interleave: | 0 |
| Near End CRC Errors Fastpath : | N/A |
| Far End CRC Errors Interleave : | 0 |
| Far End CRC Errors Fastpath : | N/A |

At the bottom of the screen, click **Clear** to clear all the values from the WAN Status screen and restart their counts.



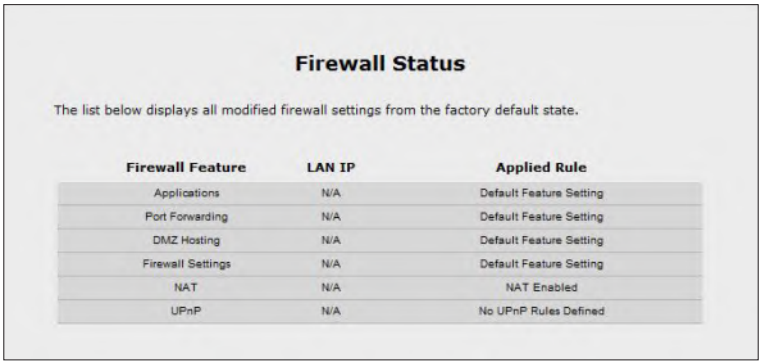

### 3.2.3 Routing Table

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



### 3.2.4 Firewall Status

Selecting **Firewall Status** generates the "Firewall Status" screen. This screen displays an overview of the Gateway's firewall, including port forwarding, DMZ hosting, and NAT parameters.



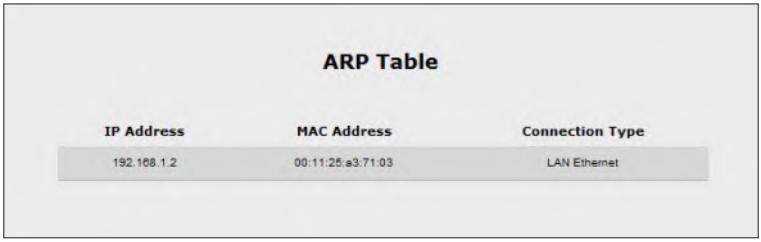
**Firewall Status**

The list below displays all modified firewall settings from the factory default state.

| Firewall Feature | LAN IP | Applied Rule |
|---|---|---|
| Applications | N/A | Default Feature Setting |
| Port Forwarding | N/A | Default Feature Setting |
| DMZ Hosting | N/A | Default Feature Setting |
| Firewall Settings | N/A | Default Feature Setting |
| NAT | N/A | NAT Enabled |
| UPnP | N/A | No UPnP Rules Defined |

### 3.2.5 ARP Table

Selecting **ARP Table** generates the "ARP Table" screen. This screen displays the Gateway's ARP (address resolution protocol) table.

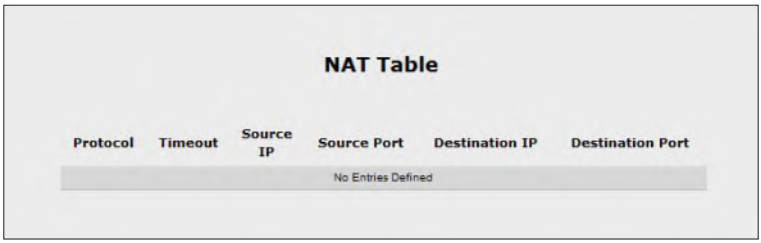


**ARP Table**

| IP Address | MAC Address | Connection Type |
|---|---|---|
| 192.168.1.2 | 00:11:25:a3:71:03 | LAN Ethernet |

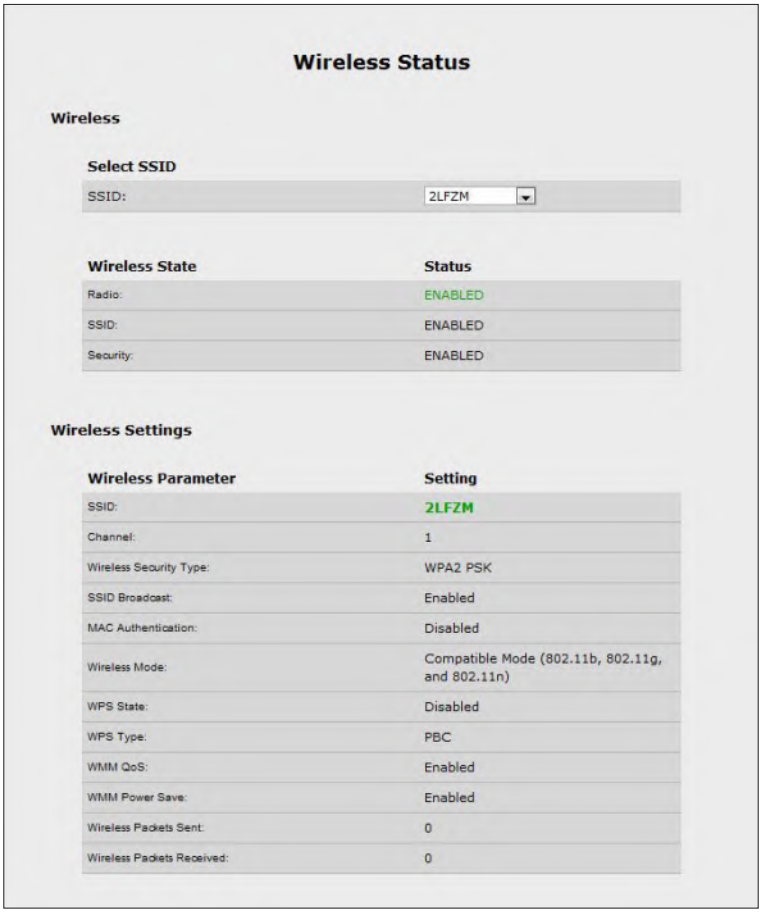
### 3.2.6 NAT Table

Selecting **NAT Table** generates the "NAT Table" screen. This screen displays the Gateway's NAT (network address translation) table.



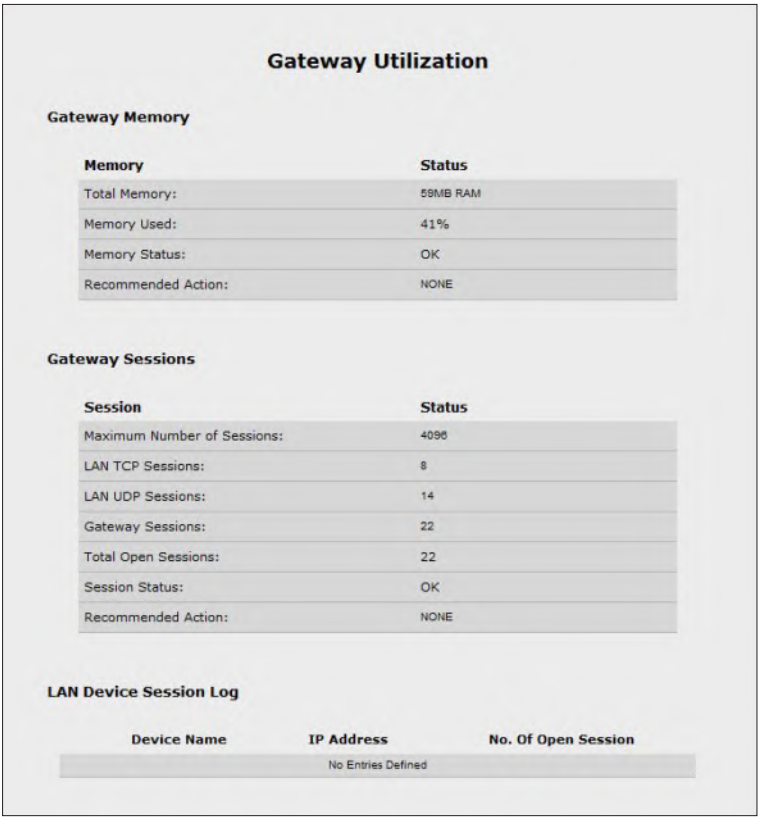
### 3.2.7 Wireless Status

Selecting **Wireless Status** generates the "Wireless Status" screen. This screen displays the Gateway's wireless network and connection status, including wireless security type, WPS state, and wireless packets sent. The only setting you can change from this screen is the name of the SSID (service set identifier), which operates as the name of the Gateway's wireless network as seen by other wireless devices.



### 3.2.8 Gateway Utilization

Selecting **Gateway Utilization** generates the "Gateway Utilization" screen. This screen displays the statistics regarding the Gateway's memory, sessions, and LAN device session log.



**Gateway Utilization**

**Gateway Memory**

| Memory | Status |
|---|---|
| Total Memory: | 59MB RAM |
| Memory Used: | 41% |
| Memory Status: | OK |
| Recommended Action: | NONE |

**Gateway Sessions**

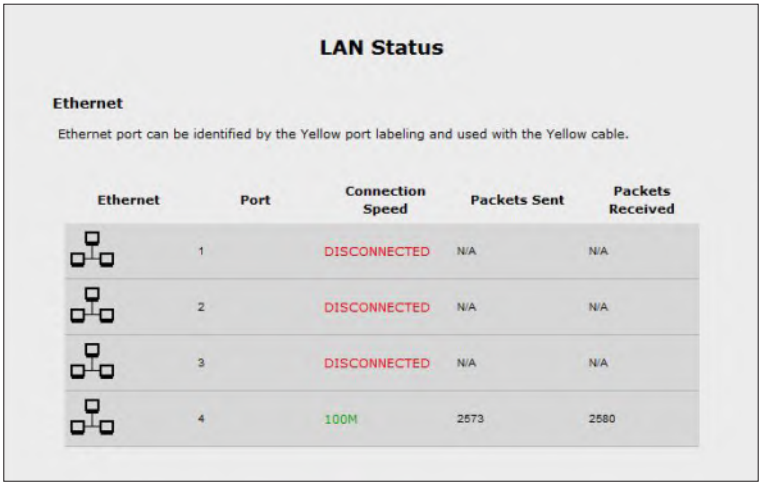
| Session | Status |
|---|---|
| Maximum Number of Sessions: | 4096 |
| LAN TCP Sessions: | 8 |
| LAN UDP Sessions: | 14 |
| Gateway Sessions: | 22 |
| Total Open Sessions: | 22 |
| Session Status: | OK |
| Recommended Action: | NONE |

**LAN Device Session Log**

| Device Name | IP Address | No. Of Open Session |
|---|---|---|
| No Entries Defined | | |

### 3.2.9 LAN Status

Selecting **LAN Status** generates the "LAN Status" screen. This screen displays the Gateway's LAN (local area network) status, which comprises the devices connected to the Gateway via its 4 Ethernet ports.



# 4



# Wireless Networking

This chapter explains how to set up the Gateway's wireless network capabilities, including creating a wireless network, enabling wireless security, and connecting a wireless client.

## 4.1 Overview

The Gateway provides the user with wireless connectivity over the 802.11b, g, and n standards (the most common wireless standards). 802.11b has a maximum data rate of 11 Mbps, 802.11g 54 Mbps, and 802.11n 144 Mbps. 802.11b, g, and n operate in the 2.4 GHz range

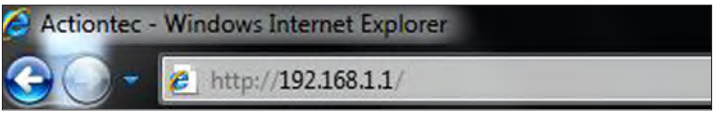
The Gateway's wireless feature is turned on, with wireless security activated, by default. The default security is WPA/WPA2 PSK, with a unique PSK (pre-shared key)already entered. This information is displayed on a sticker located on the bottom of the Gateway.

The Router integrates multiple layers of security. These include the IEEE 802.1x port-based authentication protocol, RADIUS client, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA/WPA2), and firewall and VPN applications.

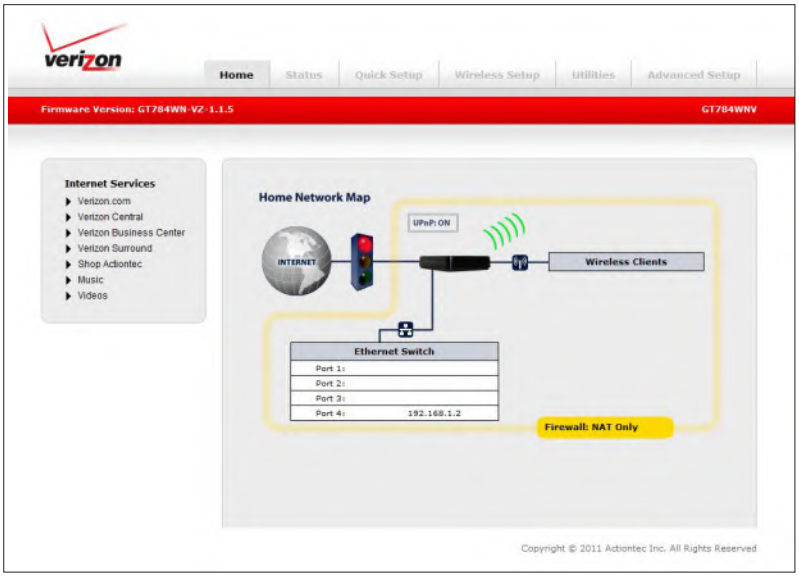
## 4.2 Accessing the Wireless Setup Screens

To set up a wireless network using the Gateway, or adjust the wireless network settings, you must access the Wireless Setup screens.
To access the Wireless 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. After entering your user name and password, the Gateway's Home screen appears. Select **Wireless Setup** from the row of buttons above the red bar.




3. The first Wireless Setup screen appears.

## 4.3 Connecting a Wireless Client

To connect a wireless client to the Gateway:

**Note:** The following procedure assumes the Gateway's default wireless settings are intact. If they have been changed, use the new SSID and wireless security settings.

1. In the wireless client's configuration interface, enter the Gateway's SSID (found on a sticker on the bottom of the Gateway's case) in the appropriate text box or field (this varies depending on the wireless client's manufacturer).

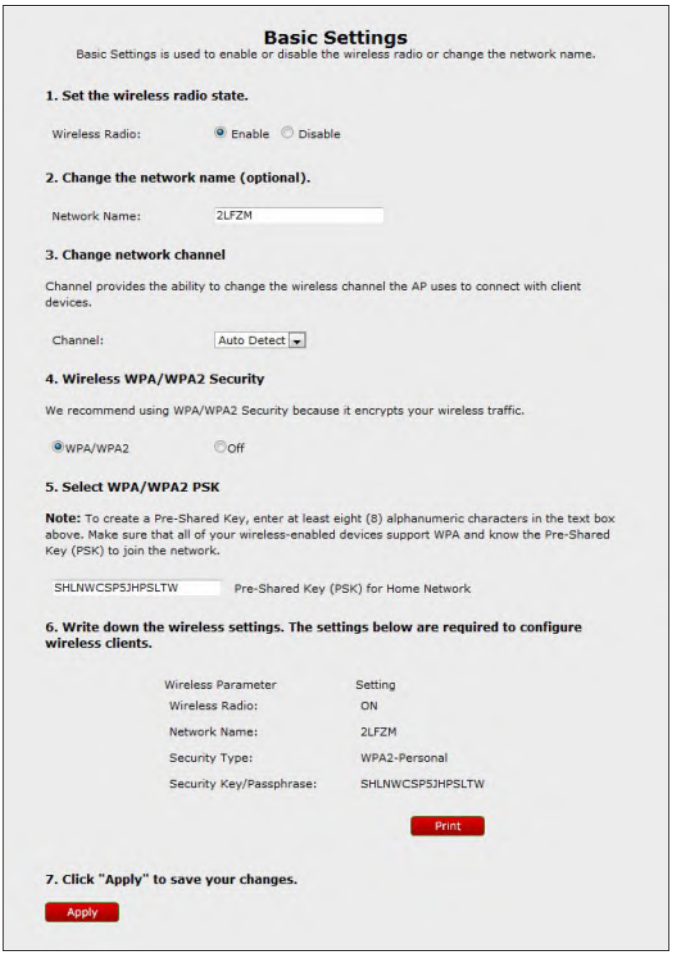
2. Enter the Gateway's WPA key (also found on the sticker on the bottom of the Router's case) in the wireless client's configuration interface.

3. Save the changes and exit the wireless client's configuration interface. The client should now detect and join the Gateway's wireless network. If not, check the wireless client's documentation, or contact its manufacturer.

## 4.4 Basic Wireless Setup

The first Wireless Setup screen is the "Basic Settings" screen. This screen takes you through a basic configuration of the Gateway's wireless network.

**Note**: These settings are already configured for the Gateway out of the box. Change them only if you want to change the wireless settings.



To set up your Gateway for wireless networking:

1. Click the "Enable" radio button to activate the Gateway's wireless radio.
2. Enter the name of the wireless network in the "Network Name" text box.
3. Select the channel at which the Gateway's wireless radio communicates by selecting it from the "Channel" drop-down list.
4. Click the "WPA/WPA2" radio button to activate WPA (Wi-Fi Protected Access) security on the wireless network.
5. Click **Apply** to save changes.
6. Print the wireless settings displayed at the bottom of the screen by clicking **Print**. Other wireless devices wishing to join the Gateway's wireless network must use these same settings when configuring the device's wireless networking scheme.

## 4.5 Wireless Setup Screens

On the left hand side on the first Wireless Setup screen (and every other Wireless Setup screen) is the Wireless Settings menu. Select any option from this menu and you will be taken to that Wireless Setup screen.

### 4.5.1 Wireless Security

Selecting "Wireless Security" from the Wireless Setup menu generates the Wireless Security screen. This screen displays various wireless security settings that can be changed for the Gateway's wireless network. Any or all of these settings can be changed independently of each other.


SSID

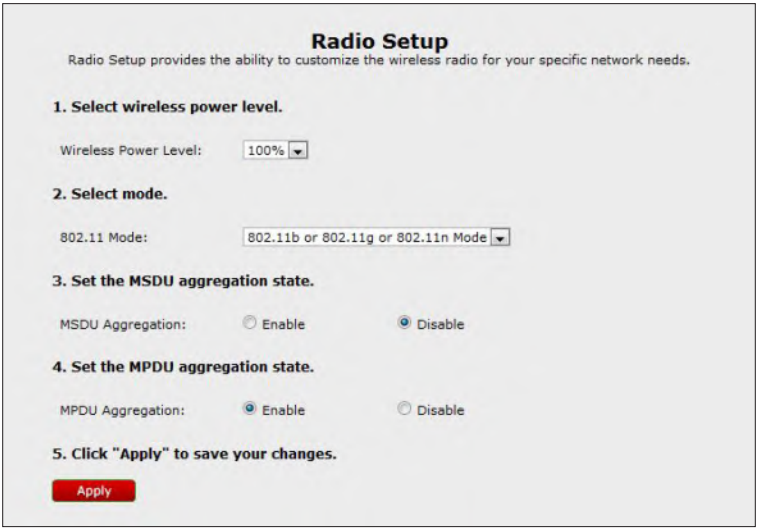
Select the new SSID (wireless network name) for the wireless network here.

### Security Type

Select a security type from the drop-down list. **WPA/WPA2-Personal** is the default wireless network security for the Gateway. You can change the passphrase required for joining the wireless network by clicking the "Use Custom Security Key/Passphrase" radio button, and then entering a new passphrase in the appropriate text box.
Another option is **WEP** (wired equivalent privacy). WEP is a weaker security protocol than WPA/WPA2, but may be needed for older wireless devices that do not support WPA/WPA2. To set up WEP, select it from the "Security Type" drop-down list. You can then use the default key, or enter your own key(s) in the appropriate text boxes. You can also choose between 64-bit and 128-bit security. The final choice is **No Security**. If you select this option, any wireless client within range of the Gateway's network will be able to join.

## 4.5.2 Radio Setup

Selecting **Radio Setup** from the Wireless Setup menu generates the "Radio Setup" screen. This screen displays various wireless radio settings that can be changed for the Gateway's wireless network. Any or all of these settings can be changed independently of each other.



### Power Level

Select a percentage power level from the drop-down list box.

### Mode

Select the mode in which the Gateway's wireless network will operate. You can select between various permutations among 802.11b (slowest), g (faster), and n (fastest). Be aware that selecting a lower speed network mode may slow the entire network down, but that older wireless devices may not support the faster speeds.

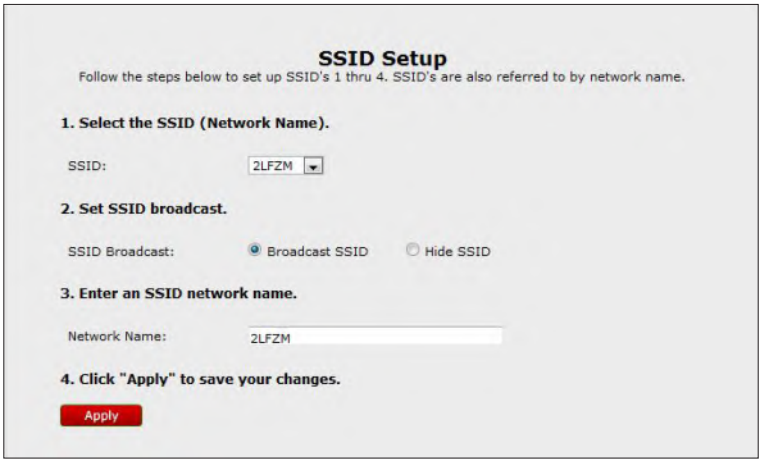
### MSDU, MPDU Aggregation States

Enable or disable these options. We recommend not changing these settings from their default states unless you are an experienced network technician.

After making changes in this screen, click **Apply** to save changes.

### 4.5.3 Multiple SSID

Selecting **Multiple SSID** from the Wireless Setup menu generates the "Multiple SSID" screen. This screen allows you to create multiple discrete wireless networks on the Gateway.

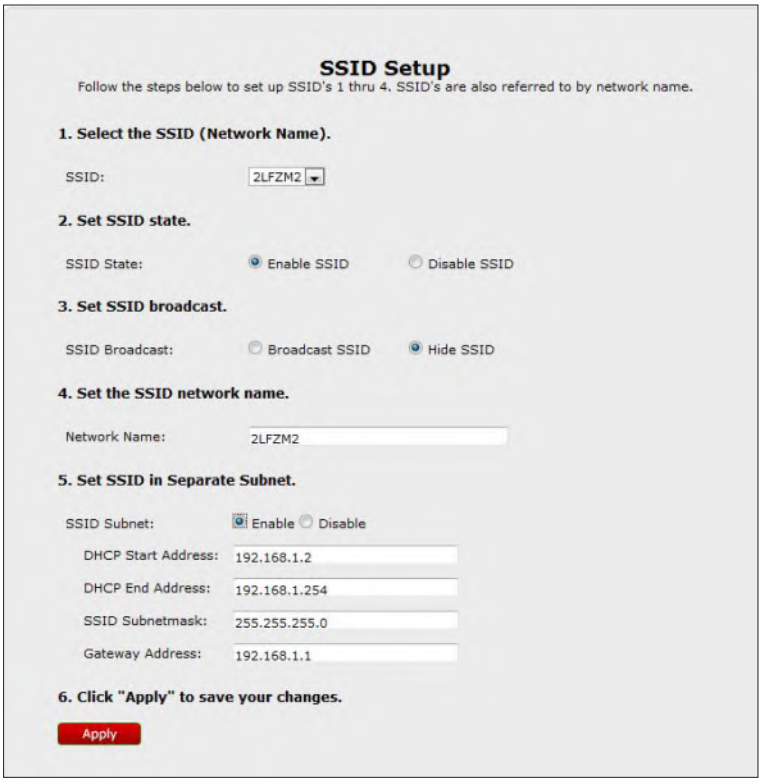



To create an additional SSID:

1. Select the SSID to change from the "SSID" drop-down list. The screen expands.
2. Enable the new SSID by clicking the "Enable SSID" radio button next to "SSID state."

3. Select whether to broadcast or hide the new SSID by clicking in the appropriate radio button.

4. Enter the new SSID in the "Network Name" text box.




5. If the new SSID needs its own subnet, click in the "SSID Subnet: Enable" radio button, then enter the address parameters for the subnet in the appropriate text boxes below.

6. Repeat steps 1-4 for additional SSID names.

7. Click **Apply** to save changes.

### 4.5.4 MAC Authentication

Selecting **MAC Authentication** generates the "MAC Authentication" screen. MAC authentication allows the user to allow or deny access to the Gateway's wireless network by a particular device's MAC address.


To set up wireless MAC authentication:

1. Select the SSID from the "SSID" drop-down list.
2. Click the "Enable" radio button.

3. Select either "Accept Device List" or "Deny Device List" by clicking the appropriate radio button. Selecting "Accept…" allows only the devices listed here by MAC address to join the Gateway's wireless network. Selecting "Deny…" prevents all listed devices here access to the network.

4. Enter the MAC address of a device in the "Manually Add MAC address" text box.

5. Click **Apply**.

6. Repeat steps 3, 4, and 5 to add more devices to the list.

To remove a MAC address, select it from the "MAC Authentication Device List," then click **Remove**.

### 4.5.5 WPS

Selecting **WPS** generates the "WPS (Wi-Fi Protected Setup)" screen. This screen allows you to activate the Gateway's WPS option, and configure its WPS settings.


To set up WPS:

1. Click the WPS button to activate WPS.

2. Select the WPS type. There are three options here: Push Button (PBC), AP PIN, or End Device Pin.

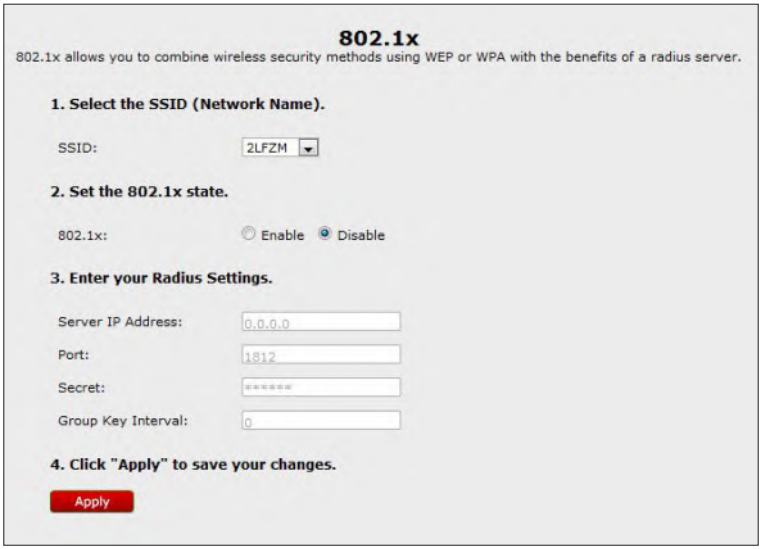
**Push Button**: click Connect, then press the WPS button on the wireless device within 2 minutes. The device will automatically connect to the Gateway's wireless network.
**AP PIN**: an AP PIN will be generated, which needs to entered into the device's wireless network interface.
**End Device PIN**: enter the PIN from the end device connected to the wireless network.

### 4.5.6 WMM

Selecting **WMM** generates the "WMM" screen. This screen displays the Gateway's WMM (Wi-Fi multimedia) , a traffic priority option than can keep the Gateway's wireless network running more smoothly. Both options in the screen are enabled by default, and we recommend not changing them unless suggested to do so by your service provider.

### 4.5.7 802.1x

Selecting **802.1x** generates the "802.1x" screen. This screen displays the Gateway's 802.1x options. This setting is for enterprise networks only, and should be accessed by an experienced network technician.




To set up 802.1x, select an SSID, then enable 802.1x by clicking the "Enable" radio button. Enter the Radius Settings in the appropriate text boxes, then click **Apply** to save changes.

# 5



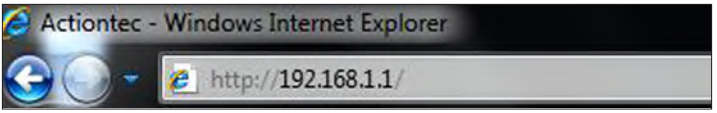
# Utilities

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.

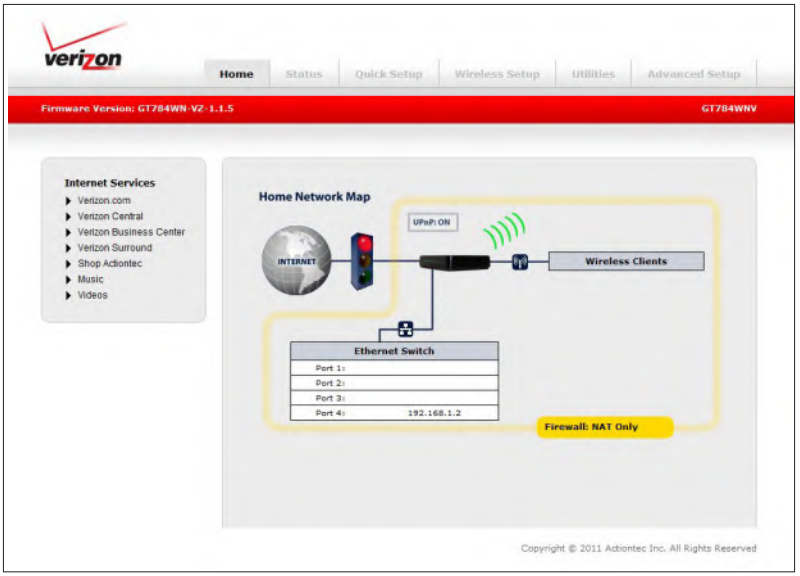
## 5.1 Accessing the Utilities Screens

To access the Utilities screens:

1. Open a Web browser. In the Address text box, type:
   **http://192.168.1.1**
   then press **Enter** on the keyboard.



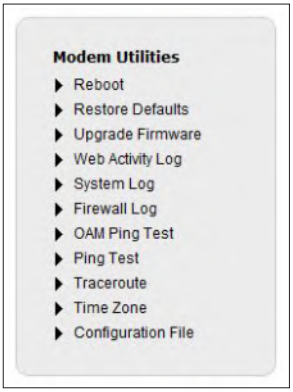

2. After entering your user name and password, the Gateway's Home screen appears. Select **Utilities** from the row of buttons above the red bar.




3. The first Utilities screen appears.

## 5.2 Utilities Screens

On the left hand side on the first Utilities screen (and every other Utilities screen) is the Utilities menu. Select any option from this menu and you will be taken to that Utilities screen.




### 5.2.1 Reboot Gateway

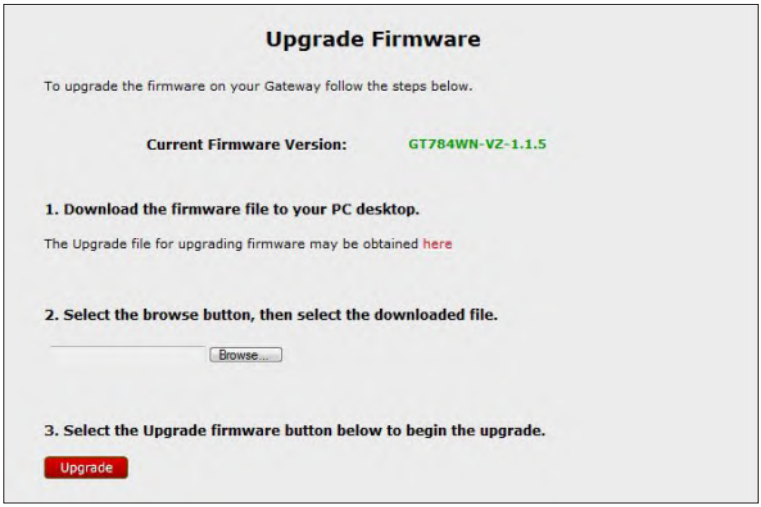
Selecting **Reboot** from the Utilities menu generates the "Reboot Gateway" screen. Click **Reboot** to reboot the Gateway.

### 5.2.2 Restore Defaults

To restore the Gateway to its factory default settings, select **Restore Default Settings** from the Utilities menu. In this screen, the Gateway's wireless settings, firewall settings, or all settings can be returned to their factory default state. Press the appropriate button to perform the chosen task. During this process, the Gateway's Power light will flash, and the Gateway is disabled until after reboot.

### 5.2.3 Upgrade Firmware

To upgrade the Gateway's firmware, select **Upgrade Firmware** from the Utilities menu. The "Upgrade Firmware" screen appears.




To upgrade the firmware:

1. Download the firmware file to your computer's desktop by following the link (click **here** in the Upgrade Firmware screen) and then following the instructions.
2. Select the location on the computer's hard drive where the firmware file was downloaded during step 1.
3. Click **Upgrade**.

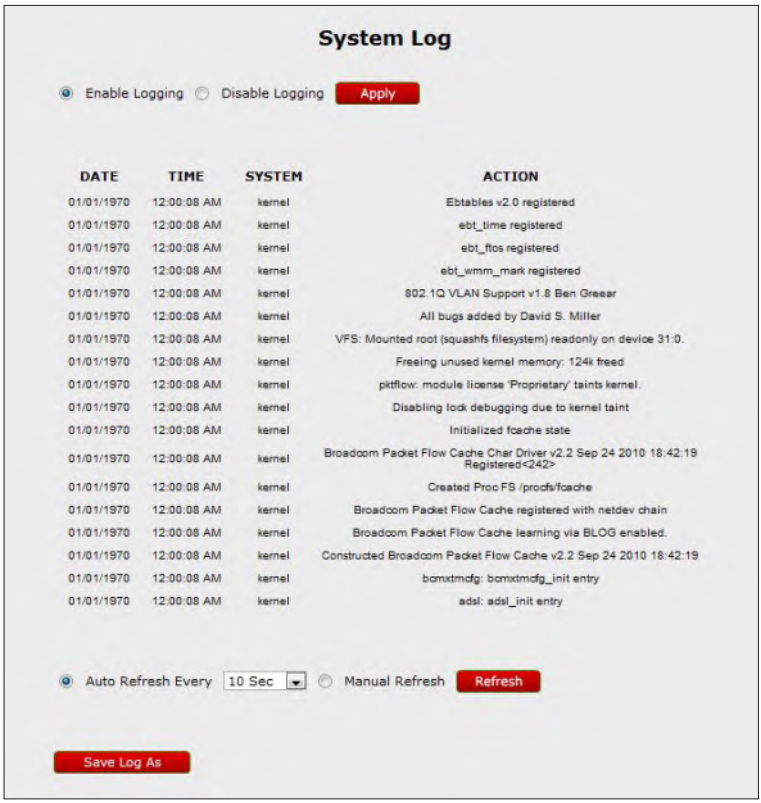
### 5.2.4 Web Activity Log

The Web Activity Log saves 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 menu.


Enable Web activity logging by clicking the "Enable Logging" radio button, then clicking **Apply**. To refresh the log automatically, click in the "Auto Refresh Every" radio button, then select a time period at which to refresh. To refresh manually, click in the "Manual Refresh" radio button, then click **Refresh**.

### 5.2.5 System Log

The System Log saves information about the Gateway's operation. To access the System Log, select **System Log** from the Utilities menu.




Enable System logging by clicking the "Enable Logging" radio button, then clicking **Apply**. To refresh the log automatically, click the "Auto Refresh Every" radio button, then select a time period at which to refresh. To refresh manually, click in the "Manual Refresh" radio button, then click **Refresh**. To save the log, click **Save Log As**, and then follow the onscreen instructions.

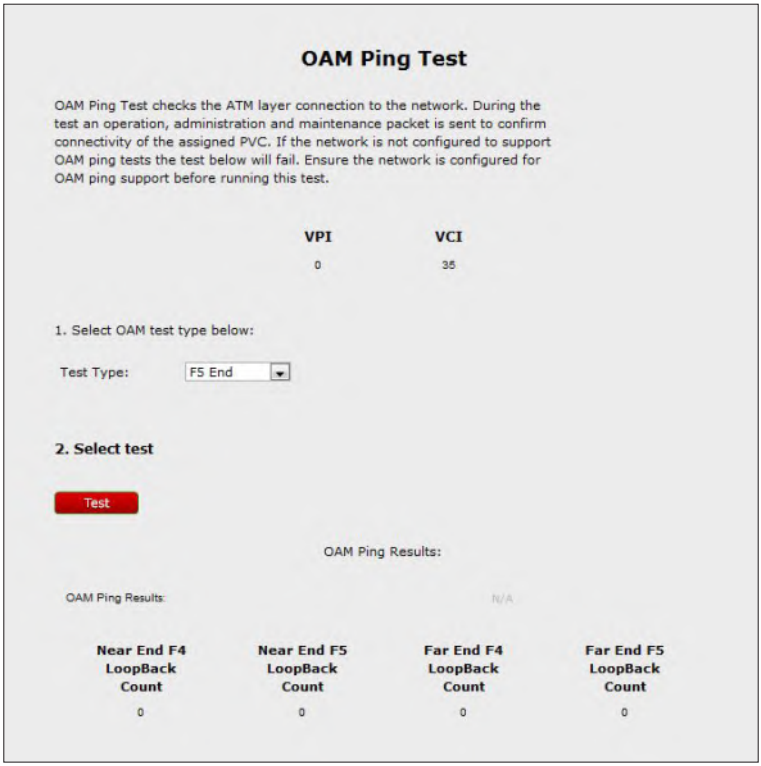
### 5.2.6 Firewall Log

The Firewall Log saves information about the Gateway's firewall. To access the Firewall Log, select **Firewall Log** from the Utilities menu.


To refresh the log automatically, click in the "Auto Refresh Every" radio button, then select a time period at which to refresh. To refresh manually, click in the "Manual Refresh" radio button, then click **Refresh**. To display firewall log information for certain period time only, select the time period from the "Show Firewall Logs up to" drop-down list. Click **Log Settings** to generate a new screen of Firewall logging parameters that will be displayed in the Firewall Log. Finally, click **Save Log As** to save the Firewall Log to your computer.

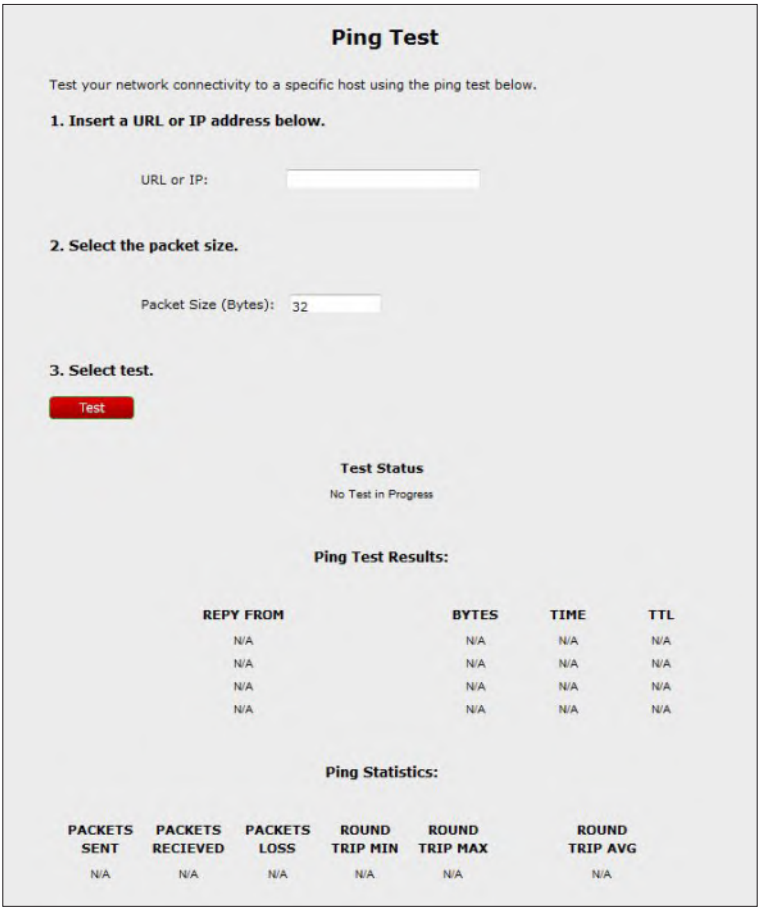
### 5.2.7 OAM Ping Test

Selecting **OAM Ping Test** from the Utilities menu 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.



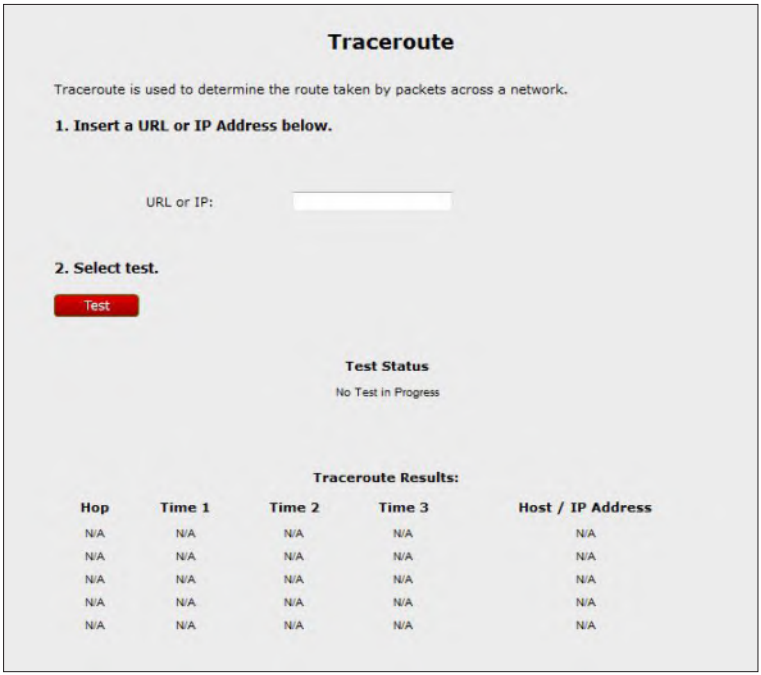
### 5.2.8 Ping Test

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



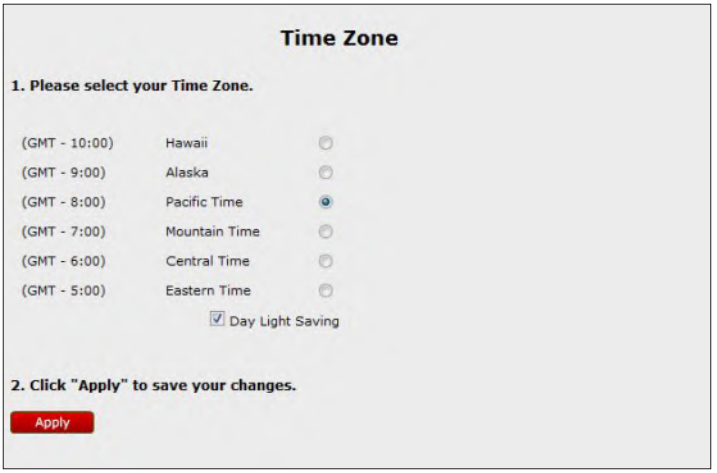
### 5.2.9 Traceroute

Selecting **Traceroute** from the Utilities menu generates the "Traceroute" screen, which is used by network technicians to check which routes packets take across the Gateway's network. Follow the on-screen instructions to perform the test.



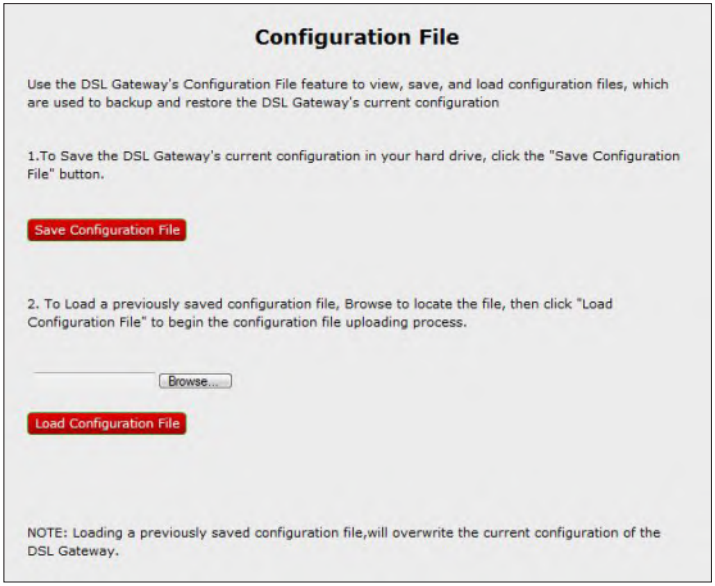
### 5.2.9 Time Zone

Selecting **Time Zone** from the Utilities menu generates the "Time Zone" screen. Set the proper time zone on the Gateway by clicking the appropriate radio button, then activating or deactivating "Day Light Saving." Click **Apply** to save changes.



### 5.2.10 Configuration File

A configuration file is like a snapshot of the Gateway's settings. Creating a configuration file saves the Gateway's settings, and allows you to reload those settings at a future time, which can be useful if the current configuration file gets corrupted, or some other mishap occurs with the Gateway.
Selecting **Configuration File** from the Utilities menu generates the "Configuration File" screen. Save the current settings of the Gateway by clicking **Save Configuration File**. Load a previously created configuration file by locating the file on your computer's hard drive (click **Browse** to search), and then clicking **Load Configuration File**.



# 6



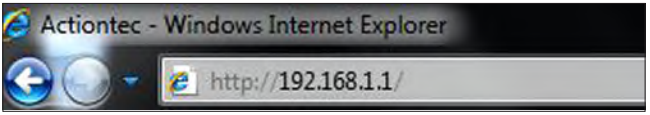
# Advanced Settings

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

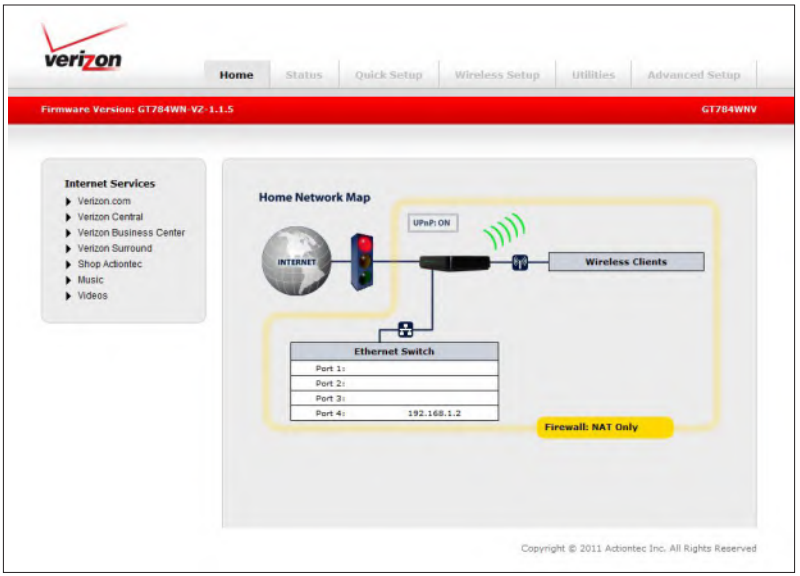
## 6.1 Accessing the Advanced Settings Screens

To access the Gateway's Advanced Settings screen:

1. Open a Web browser. In the "Address" text box, type:
   **http://192.168.1.1**
   then press **Enter** on the keyboard.



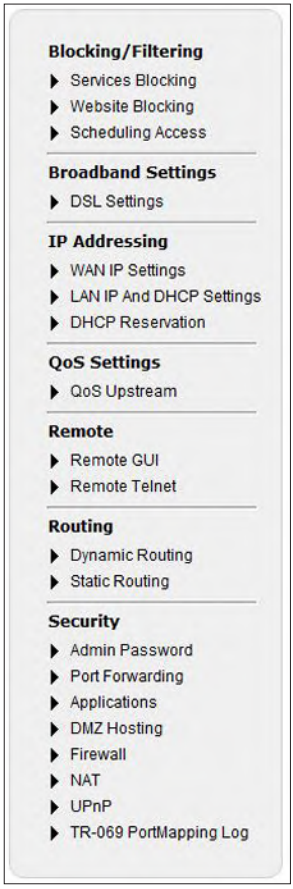

2. The "Home" screen appears. Click **Advanced Setup.**




3. The first "Advanced Setup" screen appears.

## 6.2 Advanced Screens

On the left hand side of the first Advanced screen (and every other Advanced screen) is the Advanced menu. Select any option from this menu and you will be taken to that Advanced screen.



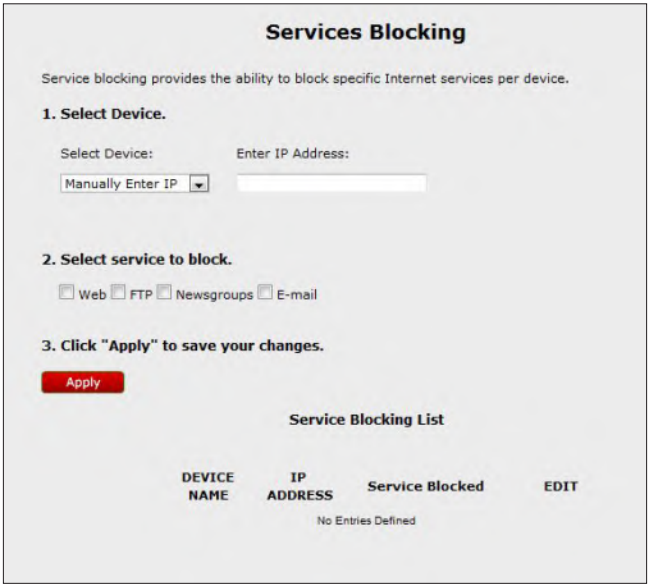
## 6.3 Blocking and Filtering

These three Advanced Settings (Services Blocking, Scheduling, Website Access, and Scheduling Access) allow and deny access to Internet services and websites, to devices on the Gateway's network.

### 6.3.1 Services Blocking

Services blocking is used to prevent a device on the Gateway's network from accessing particular services available on the Internet, such as receiving email or downloading files from FTP sites. To set up services blocking on a networked device:

1. Click **Services Blocking** from the Advanced Setup menu. The "Services Blocking" screen appears.




2. Select the device on which you wish to block services from the "Select Device" drop-down list, or enter the device's IP address in the "Enter IP Address" text box.

3. Select a service, or multiple services, to block by clicking in the appropriate check box below "Select service to block."

4. Click **Apply** to save changes.

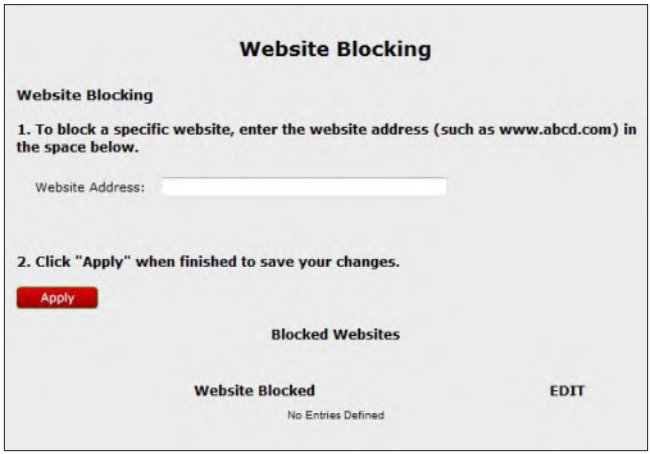
5. Repeat steps 2-4 to block services on another device on the Gateway's network.

The devices that are blocked from accessing services are listed at the bottom of the screen.

### 6.3.2 Website Blocking

Web site blocking is used to prevent all devices on the Gateway's network from accessing particular web sites on the Internet. To set up web site blocking on the Gateway's network:

1. Click **Website Blocking** from the Advanced Setup menu. The "Website Blocking" screen appears.




2. Enter the web site address of the web site to be blocked in the Website Address text box.

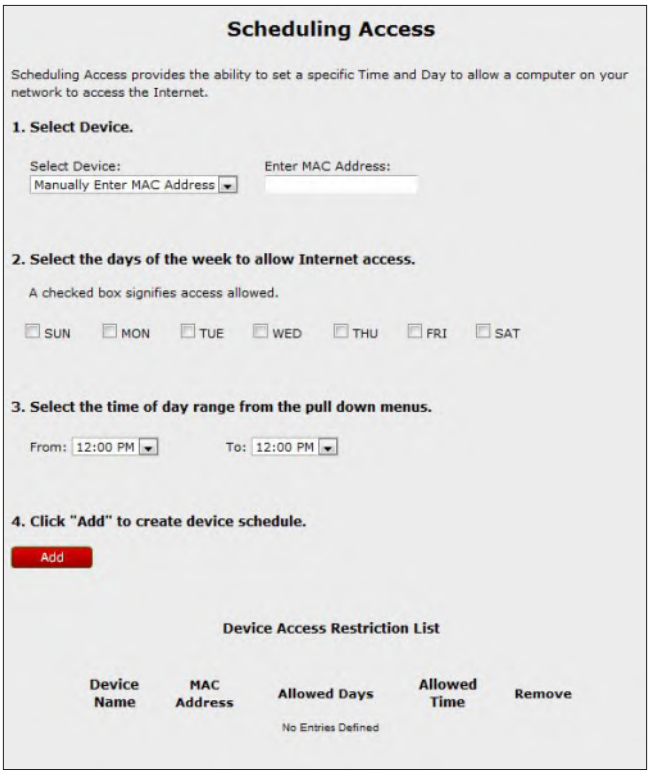
3. Click **Apply** to save changes.

4. Repeat steps 2-3 to block other web sites from being accessed on the Gateway's network.

### 6.3.3 Scheduling Access

Scheduling access is used to allow a device on the Gateway's network to access the Internet at certain times of the day, or certain days of the week, only. During times not configured in the Scheduling Access screen, the device will not be able to access the Internet. To set up scheduling access on a networked device:

1. Click **Scheduling Access** from the Advanced Setup menu. The "Scheduling Access" screen appears.



2. Select the device on which you want to schedule Internet access from the "Select Device" drop-down list, or enter the device's MAC address in the "Enter MAC Address" text box.

3. Select the days of the week during which you want to allow Internet access by clicking in the appropriate check box below "Select the days of the week…".

4. If applicable, set the time range during which you want to allow Internet access. This time range will apply only to the days activated in step 3.

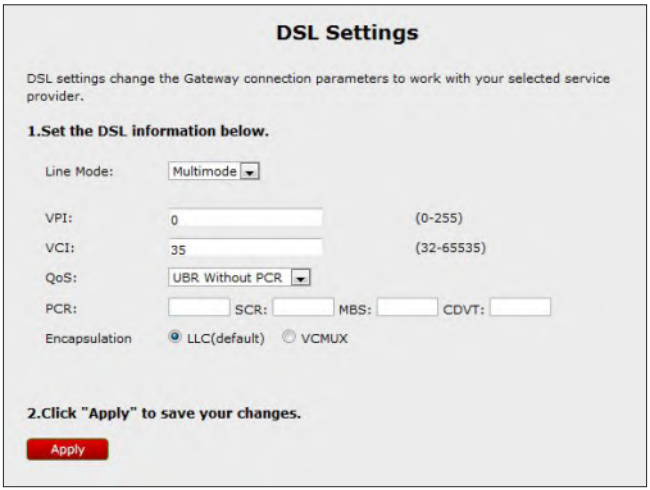
5. Click **Add** to create a schedule access.

6. Repeat steps 2-5 to create multiple access schedules for other devices on the Gateway's network.

The devices that are configured with an access schedule are listed at the bottom of the screen.

## 6.4 DSL Settings

Selecting **DSL Settings** from the Advanced menu generates the "DSL Settings" screen. This screen is used to configure settings related to the connection between the service provider and the Gateway. Do not change these settings unless you are an experienced network technician.

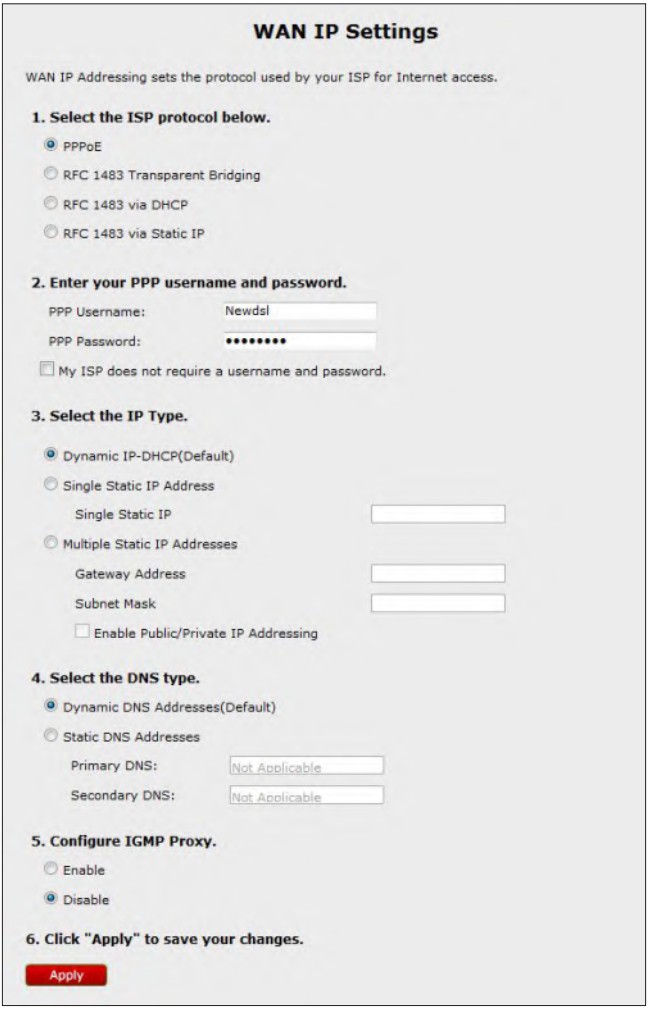


## 6.5 IP Addressing

These three Advanced Settings (WAN IP settings, LAN IP and DHCP settings, and DHCP Reservation) relate to the network connections of the Gateway.

### 6.5.1 WAN IP Settings

Selecting **WAN IP Settings** from the Advanced menu generates the "WAN IP Settings" screen.



WAN IP Address allows manual set up of the WAN IP address of the Gateway, which is the Gateway's connection to the service provider and the Internet. Do not make changes to this screen unless instructed to do so by your service provider. Making changes to the settings in this screen could cause problems with the Gateway's connection to the service provider.

**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.

To make changes to WAN IP Settings:

1. Select the ISP protocol, depending on the type of connection the ISP uses. Consult the service provider for more information.

2. If using PPPoE was selected in step 1, enter the user name and password in the appropriate text boxes. If one of the RFC connections was selected, enter the information requested under Step 2.

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.

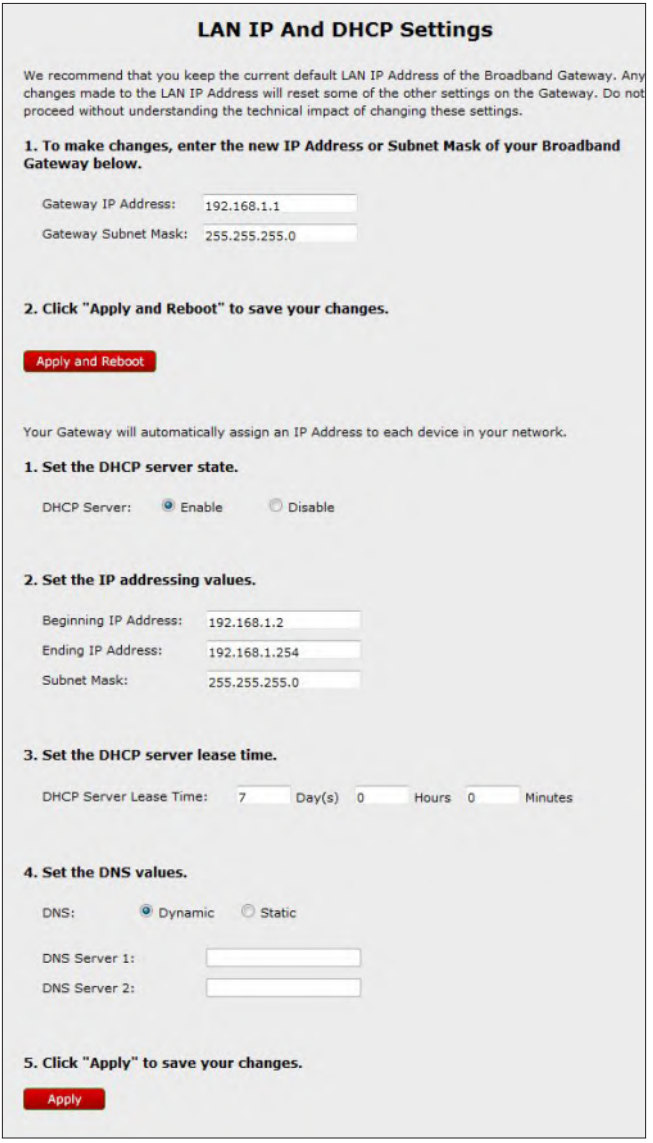
5. Select the DNS type. If static DNS address was selected, enter the primary DNS address and, optionally, the secondary DNS address in the appropriate text boxes.

6. Enable or disable the IGMP proxy by clicking the appropriate radio button below step 5.

When finished, click **Apply** to save changes.

### 6.5.2 LAN IP and DHCP Settings

Selecting **LAN IP and DHCP Settings** from the Advanced menu generates the "LAN IP and DHCP Settings" screen.



LAN IP and DHCP Settings allows manual set up of the LAN IP address of the Gateway, which handles the Gateway's local wired and wireless networks. Do not make changes to this screen unless you are an experienced network technician. Making changes to the settings in this screen could cause problems with the Gateway's network.

## LAN Settings

To configure LAN settings, enter the new IP address and subnet mask of the Gateway in the appropriate text boxes. These settings will establish the Gateway's new LAN network. Click **Apply and Reboot** to save changes.

## DHCP Server

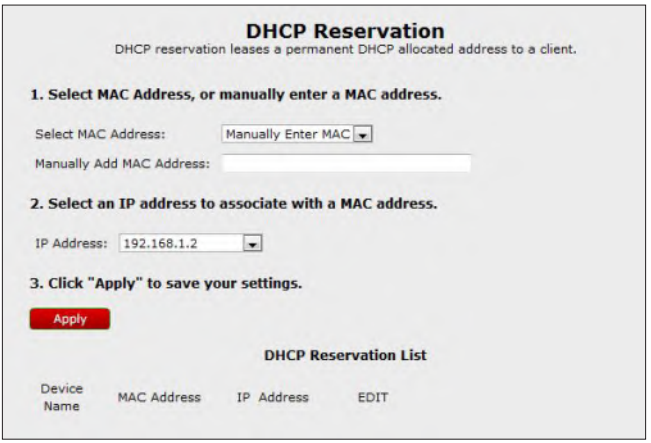
We strongly recommend leaving the DHCP Server option enabled. To set up the DHCP server:

1. Ensure the DHCP server is enabled by clicking the appropriate radio button.
2. Enter the beginning and ending IP addresses. These 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 192.168.1.2 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
3. Enter the IP address of the DHCP server's subnet mask.
4. Configure the DHCP server lease time. This time period represents the amount of time (in seconds) the DHCP server holds onto a specific IP address.
5. Set the DNS values. Select the type of DNS (dynamic or static), then enter the DNS server addresses provided by the service provider. If no DNS server information is provided, leave the text box empty.
6. Click **Apply** to save changes.

### 6.5.3 DHCP Reservation

Selecting **DHCP Reservation** from the Advanced menu generates the "DHCP Reservation" screen. Here, you can reserve a DHCP address for a particular device on your network. To do this:

1. Select a MAC address from the "Select MAC address" drop-down list. If "Manually enter MAC" is selected, enter the MAC address in the appropriate text box.




2. Select an IP address from the "IP Address" drop-down list.
3. Click **Apply** to save changes.

The "DHCP Reservation List" displays all reserved DHCP addresses.

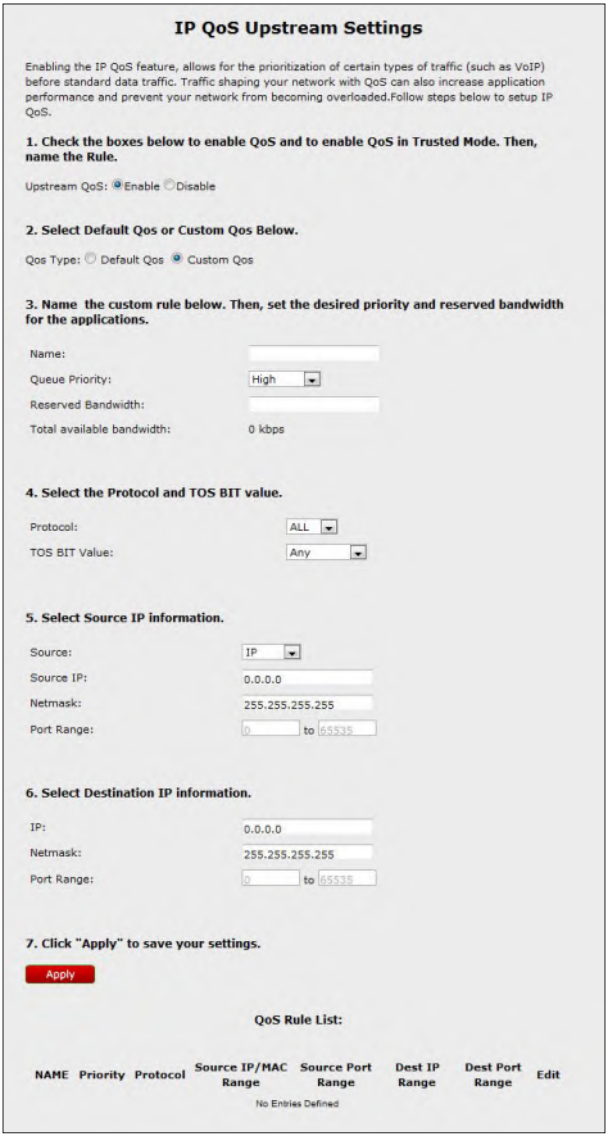
## 6.6 QoS Settings

QoS (Quality of Service) allows you to prioritize certain data traffic (such as VoIP) over others. Selecting **QoS Upstream** from the Advanced menu generates the "IP QoS Upstream Settings" screen.


To enable QoS, click the "Enable" radio button. Click the "Default QoS" radio button to have the Gateway operate with default QoS settings, then click **Apply**.

To configure custom QoS settings:

1. Click the "Custom QoS" radio button. The Custom QoS settings appear.



2. Enter the name of the rule in the "Name" text box.

3. Select a queue priority from the "Queue Priority" drop-down list box (High, Medium, Low).

4. Enter the amount of bandwidth to reserve in the "Reserve Bandwidth" text box. The amount of bandwidth available is shown below the text box.

5. Select the type of protocol from the "Protocol" drop-down list.

6. Select the TOS bit value from the "TOS Bit Value" drop-down list.

7. Enter the source IP information in the appropriate text boxes below "5. Select Source IP Information."

8. Enter the destination IP information in the appropriate text boxes below "6. Select Destination IP Information."

9. Click **Apply** to save changes.

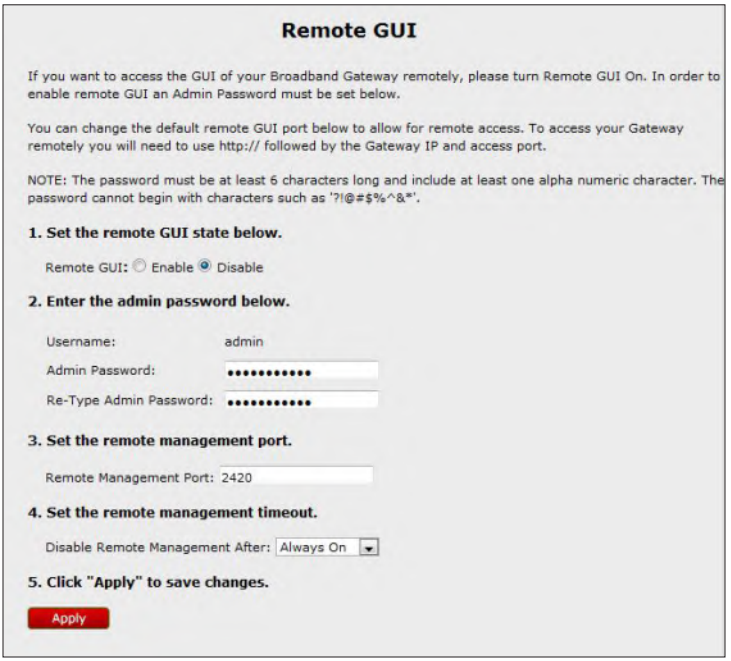
## 6.7 Remote

These two settings allow you to set up remote access to the Gateway. Remote GUI configures the Gateway to be accessed via a web browser, while Remote Telnet allows the Gateway to be accessed via telnet.

### 6.7.1 Remote GUI

Selecting **Remote GUI** from the Advanced menu generates the "Remote GUI" screen. Remote GUI allows access to the Gateway through the Internet via the web browser another computer. To set up:

1. Activate Remote GUI by clicking the "Enable" radio button.




2. Enter the admin password in the appropriate text boxes.

3. If applicable, enter the remote management port in the "Remote Management Port" text box.

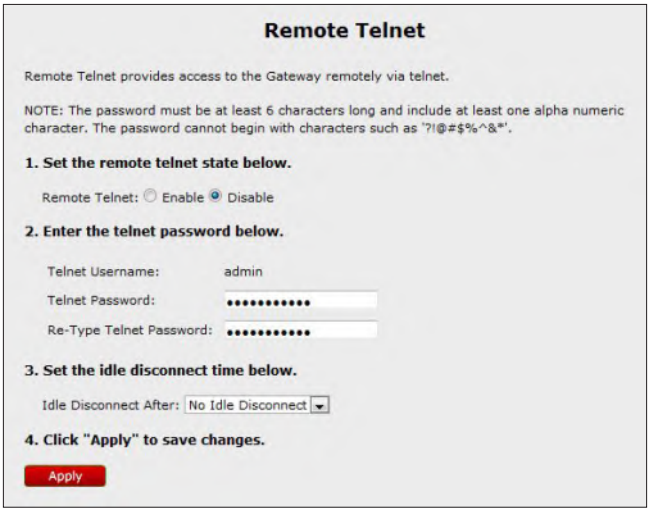
4. Set how long before remote management access times out from the "Disable Remote Management After" drop-down list.

5. Click **Apply** to save changes.

To access the Gateway from 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.

### 6.7.2 Remote Telnet

1. Activate Remote Telnet by clicking the "Enable" radio button.




2. Enter the admin password in the appropriate text boxes.

3. Set how long before remote telnet access times out from the "Idle Disconnect After" drop-down list.

4. Click **Apply** to save change.

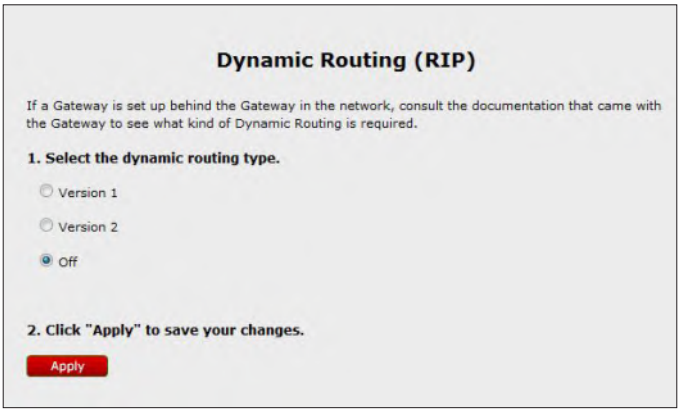
To access the Gateway from a computer using telnet (need more info).

## 6.8 Routing

These two settings involve the Gateway's routing abilities.

### 6.8.1 Dynamic Routing

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



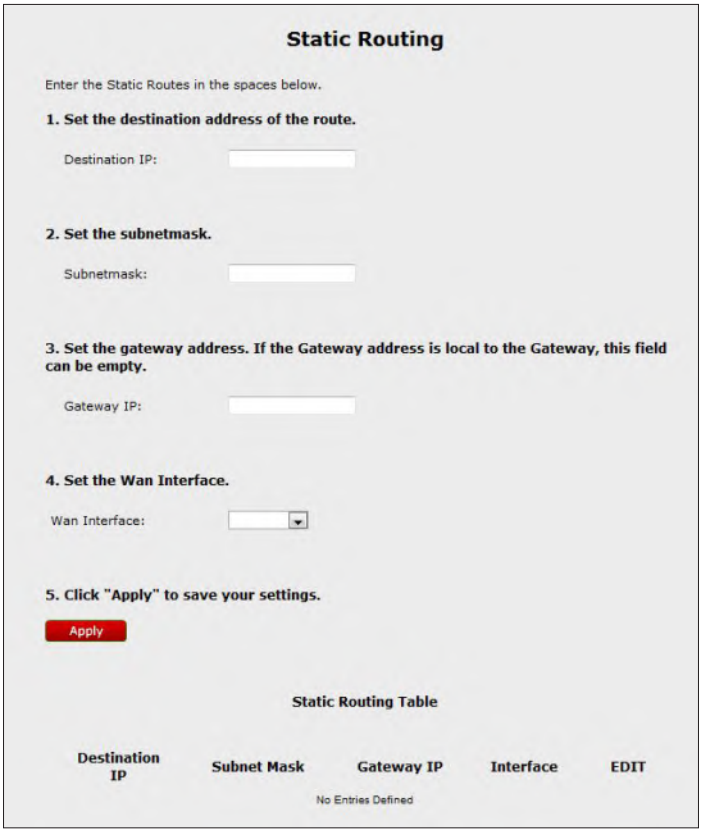

If another device is set up behind the Gateway in the network configuration, consult the documentation that came with the other device to see what kind of Dynamic Routing is required, then select the required option.

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

### 6.8.2 Static Routing

Selecting **Static Routing** in the Advanced menu generates the "Static Routing" screen. To configure:

1. Enter the Static Route destination and subnet mask addresses in their respective text boxes.




2. If applicable, enter the gateway address.
3. Select a WAN interface from the "WAN Interface" drop-down list.

**4.** Click **Apply** to save change.

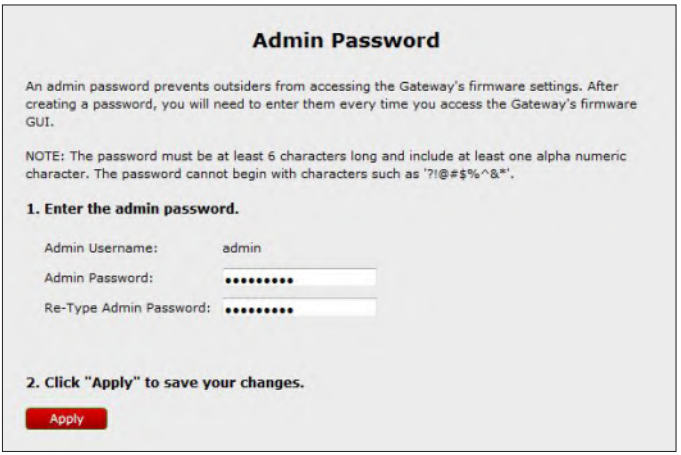
The created static route will appear in the "Static Routing Table." To remove an address, highlight it by clicking on it in the Static Routing Table, then click **Remove**.

## 6.9 Security

These options allow you to configure the security settings on the Gateway.

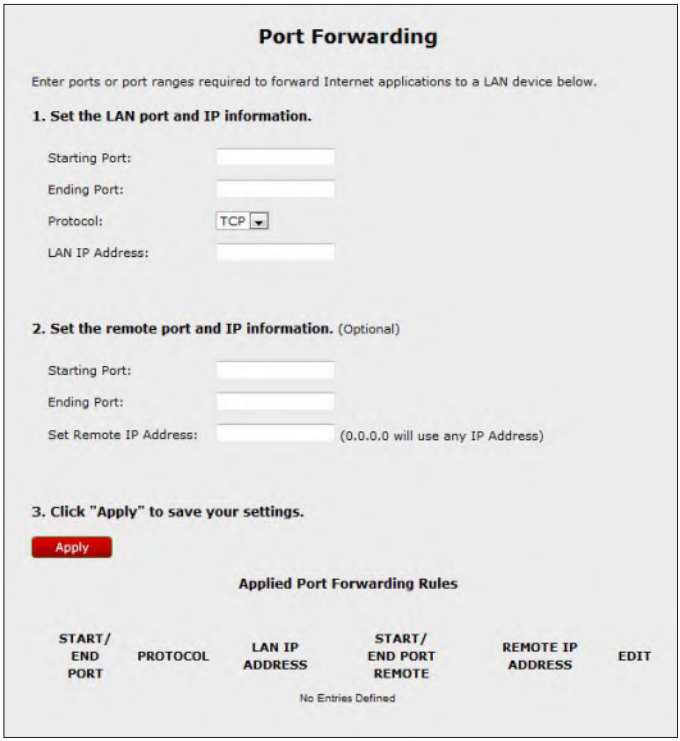
### 6.9.1 Admin Password

Selecting **Admin Password** generates the "Admin Password" screen. Change the password to access the Gateway's GUI here. Click **Apply** to save changes.



### 6.9.2 Port Forwarding

Selecting **Port Forwarding** generates the "Port Forwarding" screen. Activating Port Forwarding allows the network to be exposed to the Internet in certain limited and controlled ways, enabling some applications to work from the local network (game, voice, and chat applications, for example), as well as allowing Internet access to servers in the local network.




To set up port forwarding:

1. Enter the LAN starting port in the "Starting Port" text box.
2. Enter the LAN ending port in the "Ending Port" text box.
3. Select a protocol from the "Protocol" drop-down list box.

4. Enter the LAN IP address in the "LAN IP Address" text box.

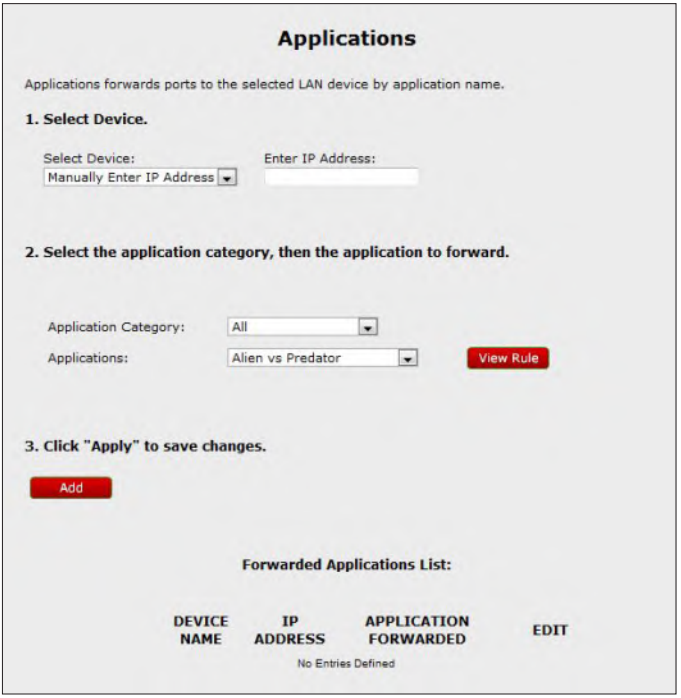
5. If applicable, enter the remote port and IP information.

6. Click **Apply** to save changes.

The list of forwarded ports will be displayed in the "Applied Port Forwarding Rules" table at the bottom of the screen.

### 6.9.3 Applications

Selecting **Applications** generates the "Applications" screen. This screen is an extension of the port forwarding screen, allowing you to quickly and easily set up commonly-used applications that require port forwarding.



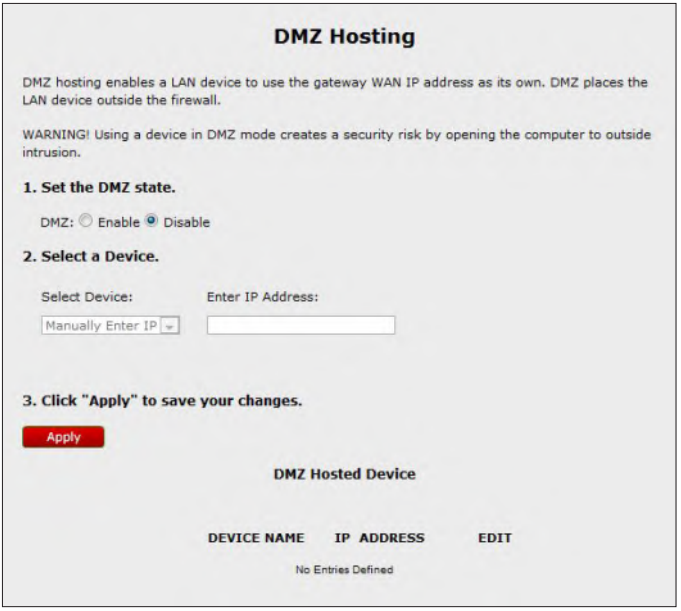
To set up a forwarded application:

1. Select a networked device by selecting it from "Select Device" drop-down list, or enter its IP address in the "Enter IP Address" text box.
2. Select the application's category from the "Application Category" drop-down list, or select **All** to see all the applications provided.
3. Select the application from the "Applications" drop-down list.
4. If desired, view the rule by clicking the **View Rule** button. A new screen appears, listing the application's port forwarding details. Click **Back** to return to the Applications screen.
5. Click **Apply** to save changes.
6. Repeat steps 1-5 to configure additional applications.

The list of forwarded applications will be displayed in the "Forwarded Applications List" at the bottom of the screen.

### 6.9.4 DMZ Hosting

Selecting **DMZ Hosting** generates the "DMZ Hosting" screen. The DMZ (De-Militarized Zone) Hosting feature allows a device on the network to operate outside the firewall to use an Internet service that otherwise would be blocked, or to expose a networked device to all services without restriction or security.




**Caution!** A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the local network at risk. When designating a DMZ host, consider the security implications and protect it if necessary.

To designate a local computer as a DMZ host:

1. Click the "Enable" radio button to activate DMZ hosting.
2. Select a networked device by selecting it from "Select Device" drop-down list, or enter its IP address in the "Enter IP Address" text box.

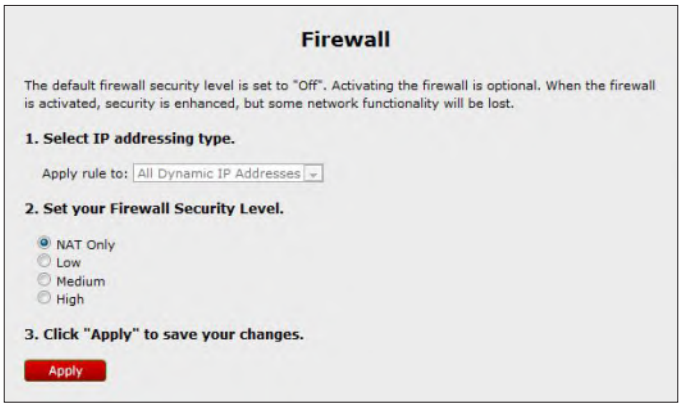
**3.** Click **Apply** to save changes.

The DMZ host will be displayed in the DMZ Hosted Device table at the bottom of the screen. Only one device at a time on the Gateway's network can be designated as a DMZ host.

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

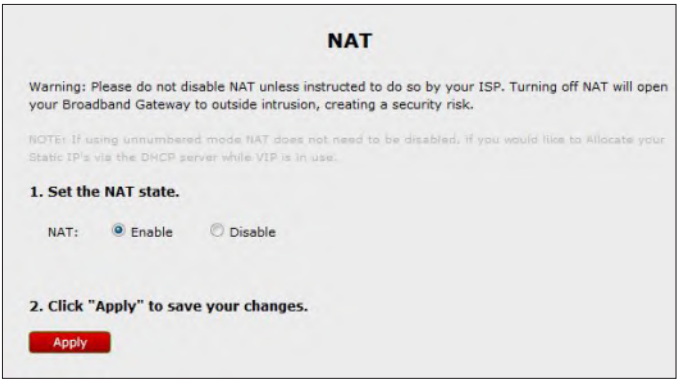
### 6.9.5 Firewall

Selecting **Firewall** generates the "Firewall" screen. Set the firewall security level from this screen. Set the level (options: NAT Only, Low, Medium, or High) from the onscreen options, then click Apply to save changes. If Low, Medium, or HIgh is selected a table of enabled/disabled services appears.



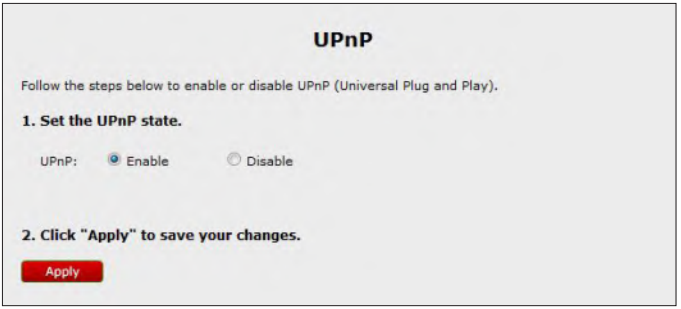
### 6.9.6 NAT

Selecting **NAT** generates the "NAT" screen. NAT (network address translation) translates the IP addresses of data as it travels across the Gateway. We recommend leaving NAT enabled (its default state).



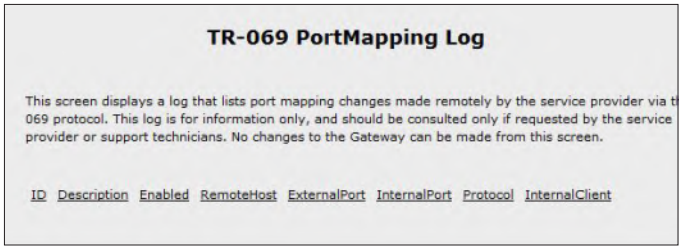

### 6.9.7 UPnP

Selecting **UPnP** generates the "UPnP" screen. UPnP (Universal Plug and Play) allows devices on the Gateway's network to locate and communicate with each other without additional configurations. We recommend leaving UPnP enabled (its default state).



### 6.9.8 TR-069 Port Mapping Log

Selecting **TR-069 Port Mapping Log** generates the "TR-069 Port Mapping Log" screen.



# A



# Specifications

This appendix lists the Gateway's specifications, including standards, cabling types, and environmental parameters. Note that the specifications listed in this appendix are subject to change without notice.

# A.1 General

## Model Number
GT784WNV (Wireless DSL Gateway)

## Standards
IEEE 802.3x, 802.3u
IEEE 802.11b, g, n (wireless)
G.dmt
G.lite
t1.413
RFC 1483, 2364, 2516

## Protocol
**LAN:** CSMA/CD
**WAN:** PPP, DHCP, Static IP

## WAN
Full-rate ADSL2+ interface

## LAN
10/100 Rj-45 switched port
USB host port

## Speed
**Wired:**
LAN Ethernet (10/100/1000 Mbps auto-sensing)
**Wireless:**
802.11b - up to 11 Mbps
802.11g - up to 54 Mbps
802.11n - up to 144 Mbps

## Cabling Type
**Ethernet 10BaseT**: UTP/STP Category 3 or 5
**Ethernet100BaseTX**: UTP/STP Category 5
**USB**

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

## A.2 Wireless Operation

### Indoors/Outdoors
Up to 144 Mbps

### Topology
Star (Ethernet)

## A.3 LED Indicators

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

## A.4 Environmental

### Power
External, 12V DC, 600mA

### Operating Temperature
0º C to 40º C (32º F to 104º F)

### Storage Temperature
-20º C to 70º C (-4º F to 158º F)

### Operating Humidity
8% to 93% (non-condensing)

### Storage Humidity
5% to 100% (non-condensing)

# B



# Computer Security

This appendix covers the basics of computer, gateway, and electronic security.

## B.1 Overview

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.

## B.2 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.

## B.3 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.

## B.4 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.

### B.4.1 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.

### B.4.2 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.

### B.4.3 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.

### B.4.4 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.

## B.5 Electronic Security

The following are two methods to secure your computer electronically.

### B.5.1 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.

### B.5.2 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



# Glossary

This appendix contains a list of terms and definitions concerning the gateway and its technologies.

# C.1 Glossary

## Access Point

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

## 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.

# Federal Communications Commission (FCC) Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

## RF exposure warning

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.