



---

# High Speed Internet DSL Modem

GT701C

## User's Manual

---

# Table of Contents

|          |                                      |           |
|----------|--------------------------------------|-----------|
| <b>1</b> | <b>Introduction</b>                  | <b>1</b>  |
|          | Minimum System Requirements          | 1         |
|          | Features                             | 2         |
|          | Getting to Know the Modem            | 3         |
| <b>2</b> | <b>Performing a Quick Setup</b>      | <b>7</b>  |
|          | Accessing Quick Setup Screens        | 7         |
|          | Changing the Password                | 10        |
| <b>3</b> | <b>Viewing the Modem's Status</b>    | <b>13</b> |
|          | Broadband Connection Status          | 13        |
|          | Network Status                       | 16        |
| <b>4</b> | <b>Configuring Advanced Settings</b> | <b>17</b> |
|          | Accessing Advanced Setup Screens     | 17        |
|          | DSL Settings                         | 20        |
|          | DHCP Settings                        | 20        |
|          | LAN IP Address                       | 22        |
|          | WAN IP Address                       | 23        |
|          | QoS Settings Upstream                | 26        |
|          | QoS Settings Downstream              | 28        |
|          | QoS Status                           | 29        |
|          | Remote Management/Telnet             | 29        |
|          | Telnet Timeout Setting               | 30        |
|          | Dynamic Routing                      | 31        |
|          | Static Routing                       | 31        |
|          | UPnP (Universal Plug and Play)       | 32        |
|          | USB Port Detection                   | 32        |
|          | Time Zone                            | 33        |
|          | Remote Syslog Capture                | 33        |
| <b>5</b> | <b>Configuring Security Settings</b> | <b>35</b> |
|          | Accessing Security Screens           | 35        |
|          | Admin User Name and Password         | 37        |
|          | Firewall                             | 37        |
|          | Applications                         | 40        |
|          | DMZ Hosting                          | 43        |
|          | NAT (Network Address Translation)    | 43        |
|          | Port Mapping                         | 44        |

|          |   |           |
|----------|---|-----------|
| <b>6</b> | <b>Configuring Parental Controls</b>          | <b>45</b> |
|          | Accessing Parental Control Screens            | 45        |
|          | Services Blocking                             | 47        |
|          | Website Blocking                              | 48        |
|          | Schedule Rules                                | 48        |
| <b>7</b> | <b>Configuring the Modem's Utilities</b>      | <b>51</b> |
|          | Accessing the Utilities Screens               | 51        |
|          | Restore Default Settings                      | 53        |
|          | Upgrade Firmware                              | 54        |
|          | Multiple PVC                                  | 54        |
|          | Web Activity Log                              | 55        |
|          | System Log                                    | 56        |
|          | OAM Ping Test                                 | 57        |
|          | Ping Test                                     | 57        |
|          | Reboot  | 58        |
| <b>8</b> | <b>Troubleshooting</b>                        | <b>59</b> |
|          | Troubleshooting                               | 59        |
|          | Frequently Asked Questions                    | 61        |
| <b>A</b> | <b>Reference</b>                              | <b>65</b> |
|          | Locating Computer Information                 | 65        |
|          | Locating Windows Operating System Files       | 66        |
| <b>B</b> | <b>Switching to Static IP on the Computer</b> | <b>69</b> |
|          | Windows 98 SE                                 | 69        |
|          | Windows Me                                    | 73        |
|          | Windows 2000                                  | 77        |
|          | Windows XP                                    | 81        |
| <b>C</b> | <b>Computer Security</b>                      | <b>85</b> |
|          | Comparing DSL Service with a Dial-Up Modem    | 85        |
|          | Modem Security                                | 86        |
|          | Computer Security                             | 86        |
|          | Electronic Security                           | 87        |
| <b>D</b> | <b>Specifications</b>                         | <b>89</b> |
|          | General                                       | 89        |
|          | LED Indicators                                | 90        |
|          | Environmental                                 | 90        |
| <b>E</b> | <b>Glossary</b>                               | <b>91</b> |
| <b>F</b> | <b>Service Acronyms</b>                       | <b>95</b> |
|          | Service Acronym Definitions                   | 95        |

# Introduction

# 1

Thank you for purchasing the High Speed Internet DSL Modem. The Modem 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 High Speed Internet DSL Modem 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) for USB connections only.
- 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 services
- USB 1.1 device specification compliance
- 12 Mbps USB data rate (full speed) support
- Precise ATM traffic shaping
- IP packet routing
- RIP-1, RIP-2, and static routing protocol support
- Built-in NAT, DHCP server
- PAP/CHAP authentication, administrative passwords through Telnet
- 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

## **Getting to Know the Modem**

This section contains a quick description of the Modem's lights, ports, etc. The Modem 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 Modem features five lights (LEDs): Power, DSL, Internet, Ethernet, and USB.



#### ***Power Light***

The Power light displays the Modem's current status. If the Power light glows steadily green, the Modem is receiving power and fully operational. When the Power light is rapidly flashing, the Modem is initializing. If the Power LED glows red when the Power cord is connected to a known working outlet power, the Modem has failed to initialize; contact Technical Support.

#### ***DSL Light***

When the Modem connects to the DSL service, the DSL light will glow solid green. If the DSL light blinks rapidly, the Modem is in training mode. If the DSL light blinks slowly, DSL service has been lost; contact the ISP.

### ***Internet Light***

The Internet light glows green when connected to the ISP. It may blink while sending or receiving data.

### ***Ethernet Light***

The Ethernet light illuminates when the Modem is connected to a computer via its yellow Ethernet port, using an Ethernet cable.

### ***USB Light***

The USB light illuminates when the Modem is connected to a computer via its USB port, using a USB cable.

## **Rear Panel**

The rear panel of the Modem contains four ports (DSL, USB, Ethernet, and Power), as well as Reset and Power switches.



### ***DSL Port***

The DSL port is used to connect the Modem to a DSL (Digital Subscriber Line) connection.

### ***USB Port***

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

### **Ethernet Port**

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



**Note:** Use a crossover Ethernet cable to connect the Modem only if connecting to a hub/switch that lacks an uplink port.

### **Reset Switch**

Depressing the Reset switch restores the Modem's factory default settings. To reset the Modem, depress and hold the Reset switch until the Power light changes from green to orange. When the Power light glows orange, release the Reset switch (this may take from 4 to 7 seconds). The reset process starts after releasing the switch.

### **Power Port**

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



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

### **Power Switch**

The Power switch is used to power the Modem 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 Modem, including how to connect the Modem 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.

---

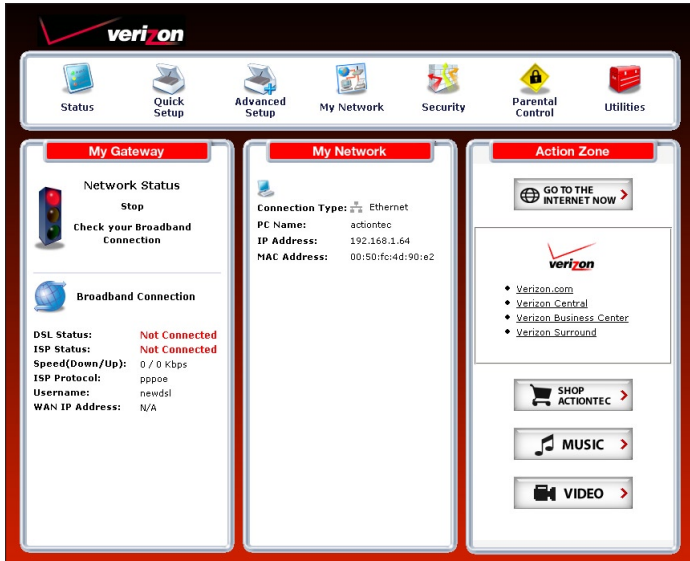
## Accessing Quick Setup Screens

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.

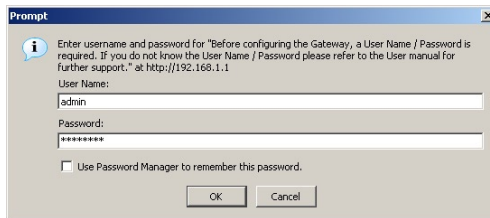


- The “Home” screen appears. Click **Quick Setup**.




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

Firefox:



Internet Explorer:

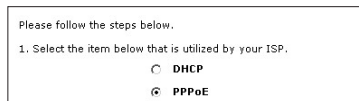


 **Note:** The default user name is “admin.” The default password is “password.”

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.

3. Select the IP Type.

☒ Dynamic IP-DHCP(Default)

☐ Single Static IP Address

- 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.

**Optional**  
Select the DNS type.

☒ Dynamic DNS Addresses(Default)

☐ Static DNS Addresses

Primary DNS

Secondary DNS

- 7.** Click **Apply** at the bottom of the screen.
- 8.** Read the instructions on the next screen. The Modem is successfully configured.

Please wait while we apply the changed settings to the gateway. When gateway changes are applied successfully, you will be taken back to the page apply was selected on.

The Power light flashes rapidly while the Modem restarts, then glows steadily green when fully operational. The Internet light will also glow steadily green. The Modem 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 Modem’s Web Configuration screens, follow these instructions:

1. From the “Home” screen, select **Quick Setup**.
2. The “Welcome to the Quick Setup” 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 box, 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 Modem’s Web Configuration screens in the future.

**Admin User Name and Password**  
Enter an admin username and password to prevent outsiders from accessing the Gateway's firmware settings. After creating a username and password, you will need to enter them everytime you access the gateway's firmware settings.  
  
**Admin User Name:**   
**Admin Password:**

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.

Please wait while we apply the changed settings to the gateway. When gateway changes are applied successfully, you will be taken back to the page apply was selected on.

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

**This page left intentionally blank.**


# Viewing the Modem's Status

# 3

After configuring the Modem, the Modem'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 Modem'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 Modem, including model number, firmware version, IP address, and gateway IP address.

Broadband Connection Status

Connect

Disconnect

Model:

GT701C

Firmware Version:

3.20.4.3.5.0.9.2.10

Gateway MAC Address:

00:18:01:DA:2E:FC

WAN IP Address:

N/A

Subnet Mask:

Gateway IP Address:

N/A

DNS Address #1:

207.244.64.140

DNS Address #2:



## PPP Status

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

| PPP Status               |                      |
|--------------------------|----------------------|
| Status:                  | <input type="text"/> |
| User Name:               | <input type="text"/> |
| LCP State:               | <input type="text"/> |
| IPCP State:              | <input type="text"/> |
| Authentication Failures: | <input type="text"/> |
| Session Time:            | <input type="text"/> |
| Packets Sent:            | <input type="text"/> |
| Packets Received:        | <input type="text"/> |

## DSL Status

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

| DSL Status                              |                      |
|---|----------------------|
| VPI:                                    | <input type="text"/> |
| VCI:                                    | <input type="text"/> |
| DSL Mode Setting:                       | <input type="text"/> |
| DSL Negotiated Mode:                    | <input type="text"/> |
| Connection Status:                      | <input type="text"/> |
| Speed (down/up):                        | <input type="text"/> |
| ATM QoS class:                          | <input type="text"/> |
| Near End CRC Errors :                   | <input type="text"/> |
| Far End CRC Errors :                    | <input type="text"/> |
| Near End CRC(Within last 30 mins) :     | <input type="text"/> |
| Far End CRC(Within last 30 mins) :      | <input type="text"/> |
| Near End RS FEC :                       | <input type="text"/> |
| Far End RS FEC :                        | <input type="text"/> |
| Near End FEC(Within last 30 mins) :     | <input type="text"/> |
| Far End FEC(Within last 30 mins) :      | <input type="text"/> |
| Discarded Packets(Within last 30 mins): | <input type="text"/> |
| SNR Margin (Downstream/Upstream):       | <input type="text"/> |
| Attenuation (Downstream/Upstream):      | <input type="text"/> |

Reset

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 Modem supports between the networked computers and the Internet.

| Protocol | Timeout | SRC IP | SRC Port | DST IP | DST Port |
|----------|---------|--------|----------|--------|----------|
|          |         |        |          |        |          |

### Routing Table

Selecting **Routing Table** generates the “Routing Table” screen. This screen displays an overview of the Modem's network routes.

| Valid | Destination | Netmask       | Gateway |
|-------|-------------|---------------|---------|
| ✓     | 192.168.1.0 | 255.255.255.0 | 0.0.0.0 |
| ✓     | 239.0.0.0   | 255.0.0.0     | 0.0.0.0 |

## Network Status

To view the Modem's network status, select **My Network** from the strip of icons at the top of any GUI 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 Advanced Settings

# 4

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

---

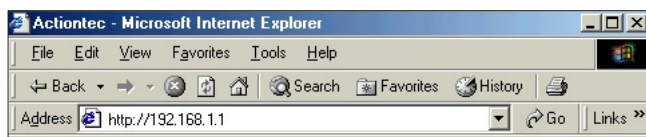
## Accessing Advanced Setup Screens

To access the Advanced Setup screens, follow these instructions:

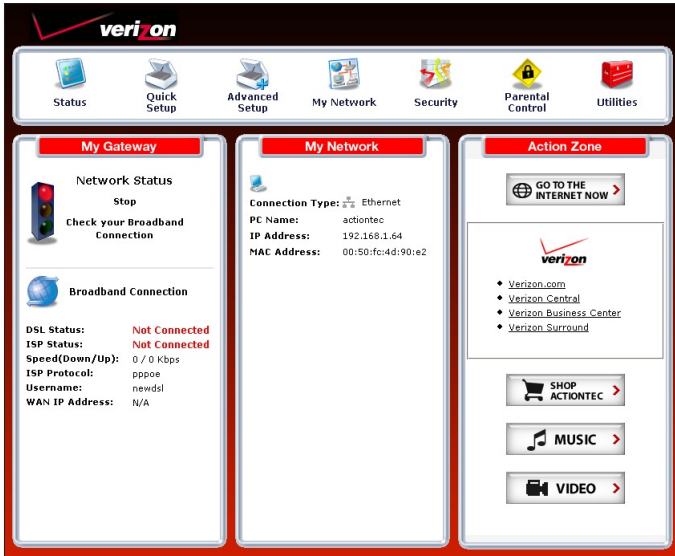
1. Open a Web browser. In the "Address" text box, type:

**http://192.168.1.1**

then press **Enter** on the keyboard.

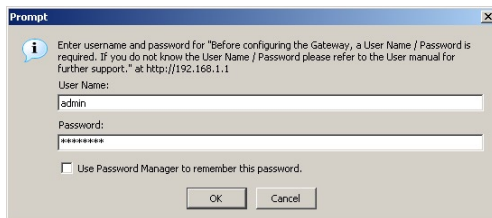


- The “Home” screen appears. Click **Advanced Setup**.




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

Firefox:

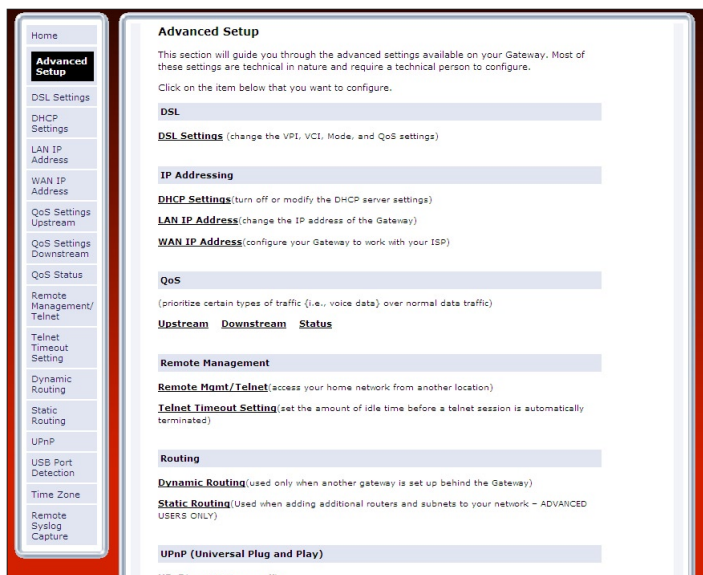


Internet Explorer:



 **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 Modem’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.

**DSL Settings**  
 This screen will allow you to modify the default DSL settings for connection to your DSL Service Provider. Make sure and click on **Apply** to save your changes.  
**WARNING!** Do not change these values until you have consulted with your DSL Service Provider.

☐ VPI/VCI Scan List [Edit List](#)  
**VPI(0 - 255):**   
**VCI(32 - 65535):**   
**Mode:**   
**QoS:**   
**PCR:**   
**SCR:**   
**MBS:**   
**CDVT:**

## DHCP Settings

Selecting **DHCP Settings** in the “Advanced Setup” screen generates the “DHCP Settings” screen. The Modem 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**.

**DHCP Settings**  
 Your DSL Gateway will automatically assign an IP Address to each device in your network. If you are using an additional Router to assign these IP Addresses, you will need to turn this function Off.  
 Please make your selection and then click **Apply** to save your changes.

**DHCP Server**  
☒ On ☐ Off  
☐ I would like to adjust the DHCP Server settings.

Once you have adjusted your settings below, please click **Apply** to save your changes.

**Beginning IP Address:**   
**Ending IP Address:**   
**Subnet Mask:**   
**Lease Time:**   
**Domain Name:**   
**DNS:** ☒ Dynamic ☐ Static  
**DNS Server 1:**   
**DNS Server 2:**

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 Modem. 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 Modem. If the default values are left intact, the Modem 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 Modem must be on the same subnet as the IP address range it generates. For instance, if the Modem’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.

**LAN IP Address**  
**WARNING!!**  
Any changes made to the LAN IP Address will reset some of the other settings on the gateway.  
Do not proceed without understanding the technical impacts of changing this feature.  
**Do you want to proceed?**

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

The “LAN IP Address” screen appears.

**LAN IP Address**  
Actiontec recommends that you keep the current default LAN IP Address of the DSL Gateway, which is 192.168.1.1.  
To make changes, enter the new IP Address or Subnet Mask of the DSL Gateway below.  
**Modem IP Address:**   
**Modem Subnet Mask:**

The values in the “Modem IP Address” and “Modem Subnet Mask” text boxes are the IP and subnet mask address of the Modem 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 Modem’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.

**WAN IP Address**  
  
**WARNING!!**  
  
Any changes made to the WAN IP Address will reset some of the other settings on the gateway.  
Do not proceed forward unless you have been instructed to do so by your ISP support personnel.  
  
**Do you want to proceed?**

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

The “WAN IP Address” screen appears.

**WAN IP Address**  
Please follow the steps below.  
1. Select the item below that is utilized by your ISP.  
☐ DHCP  
☒ PPPoE  
☒ PPP Auto Connect  
2. Enter your PPP User Name and Password. (PPPoE ONLY)  
PPP User Name   
PPP Password   
3. Select the IP Type.  
☒ Dynamic IP-DHCP(Default)  
☐ Single Static IP Address  
☐ Block of Static IP Addresses(Unnumbered Mode)  
Single Static IP   
Gateway Address(Unnumbered Mode)   
Subnet Mask(Unnumbered Mode)   
☐ Enable Public/Private IP Addressing  
4. Select the DNS type.  
☒ Dynamic DNS Addresses(Default)  
☐ Static DNS Addresses  
Primary DNS   
Secondary DNS   
5. Select Dial on-demand (optional)  
☐ Dialout on-demand      idle timeout:  minutes  
6. Adjust MTU settings (optional)  
MTU:   
7. Now click **Apply** below to save your changes.

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



**Note:** Some DSL providers use PPPoE to establish communication with an end user. Other types of broadband Internet connections 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 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 Modem 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 Modem 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 Modem 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 Upstream Settings**

Enabling the IP QoS feature, allows for the prioritization of certain types of traffic (such as VoIP) over data traffic.

☐ Enable IP QoS ☒ Trusted Mode

---

Please input the percentage for low and medium traffic flow:

low priority weight:  medium priority weight:

**Rule parameters:**

Priority:

Protocol:  ☐ Set DSCP

**Source**

IP:  Port Range:  to

Netmask:

**Destination**

IP:  Port Range:  to

Netmask:

**Rule List:**

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 prioritized 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.

### QoS Downstream Settings

Enabling the IP QoS feature, allows for the prioritization of certain types of traffic (such as VoIP) over data traffic.

☐ Enable IP QoS
 ☐ Trusted Mode

---

Please input the percentage for low and medium traffic flow:

low priority weight: 
 medium priority weight:

**Rule parameters:**

Priority: 
 Protocol: 
☐ Set DSCP

**Source**

 IP: 
 Port Range:  to

Netmask:

**Destination**

 IP: 
 Port Range:  to

Netmask:

**Rule List:**

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 “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.

QoS Status

Data will be displayed when IP QoS is enabled in Advanced Setup.  
Unit: bit rate, kbps, packet rate, packet per second, sent, dropped, packet.

Upstream Status

High Priority

Bit Rate

Packet Rate

Sent

Dropped

Medium Priority

Bit Rate

Packet Rate

Sent

Dropped

Low Priority

Bit Rate

Packet Rate

Sent

Dropped

Downstream Status

High Priority

Bit Rate

Packet Rate

Sent

Dropped

Medium Priority

Bit Rate

Packet Rate

Sent

Dropped

Low Priority

Bit Rate

Packet Rate

Sent

Dropped

Main

Remote Management/Telnet

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

Remote Management/Telnet

The default Remote Management/Telnet settings are set to Off for security reasons. If you want to access your DSL Gateway remotely, please turn Remote Management On. In order to enable remote management an Admin User Name and Password must be set below.

Actiontec does NOT recommend turning on Remote Telnet unless requested by authorized DSL personnel.

1.

Admin User Name:

admin

Admin Password:

\*\*\*\*\*

2.

Remote Management:

☐ On

☒ Off

Remote Telnet:

☐ On

☒ Off

Apply



## Remote Management

To access the Modem from the Internet, activate Remote Management by selecting the appropriate **On** radio button and writing down the WAN IP address of the Modem (see “WAN IP Address”). On a computer outside of the network, open a Web browser and enter the Modem’s WAN IP address in the address text box. The Modem’s Home screen (or a password prompt, if a password has been set) appears in the browser window.

## Telnet

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



**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.”

**Telnet Timeout Setting**  
Select the amount of idle time that you want for each Telnet session before the session is automatically disconnected.  
  

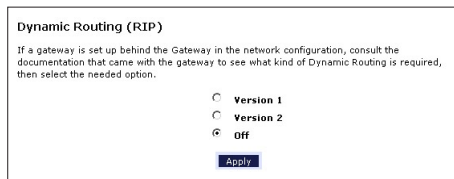
☒ 30 minutes  
☐ 12 hours  
☐ 1 day  
☐ 7 days  
☐ No idle disconnect timeout

**Apply**

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.



**Dynamic Routing (RIP)**

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

☐ Version 1

☐ Version 2

☒ Off

**Apply**

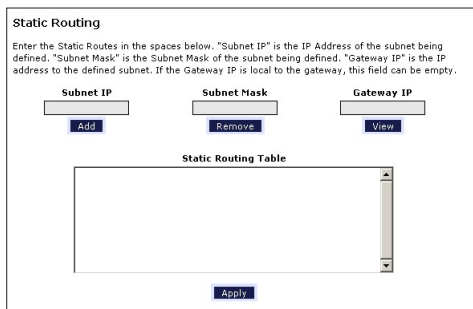
If another gateway or router is set up behind the Modem in the network configuration, consult the documentation that came with the other gateway to see what kind of Dynamic Routing is required, then select the needed option.

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**.



**Static Routing**

Enter the Static Routes in the spaces below. "Subnet IP" is the IP Address of the subnet being defined. "Subnet Mask" is the Subnet Mask of the subnet being defined. "Gateway IP" is the IP address to the defined subnet. If the Gateway IP is local to the gateway, this field can be empty.

| Subnet IP            | Subnet Mask          | Gateway IP           |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <b>Add</b>           | <b>Remove</b>        | <b>View</b>          |

**Static Routing Table**

|             |
|-------------|
| <div></div> |
|-------------|

**Apply**

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.



**UPnP**


**Warning:** UPnP is disabled by default. If you enable it, it may allow applications to configure the box and allow unexpected traffic to access local devices.

☐ On ☒ Off

Click **Apply** to continue.

**Apply**

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.

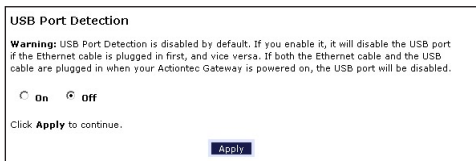
 **Note:** Activating UPnP presents a slight security risk. After finishing with the hardware or software using UPnP, we recommend deactivating UPnP.

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 Modem first, or the Ethernet port will be disabled if the a USB cable is plugged into the Modem first. If this option is turned on when both an Ethernet and a USB cable are plugged into the Modem, the USB port will be disabled.



**USB Port Detection**

**Warning:** USB Port Detection is disabled by default. If you enable it, it will disable the USB port if the Ethernet cable is plugged in first, and vice versa. If both the Ethernet cable and the USB cable are plugged in when your Actiontec Gateway is powered on, the USB port will be disabled.

☐ On ☒ Off

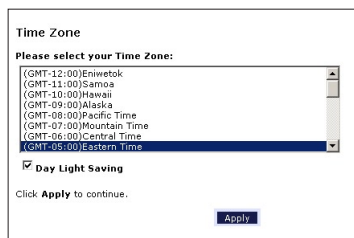
Click **Apply** to continue.

**Apply**

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 Modem is being used. Click in the “Day Light Saving” check box if Daylight Savings Time is currently in effect where the Modem is being used.

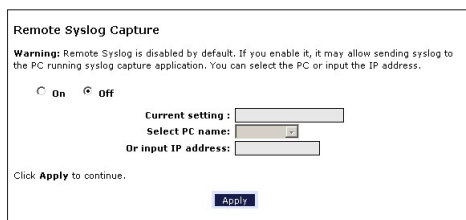


The screenshot shows the 'Time Zone' configuration window. At the top, it says 'Time Zone'. Below that, it says 'Please select your Time Zone:'. There is a list box containing the following options: (GMT-12:00)Eniwetok, (GMT-11:00)Samoa, (GMT-10:00)Hawaii, (GMT-09:00)Alaska, (GMT-08:00)Pacific Time, (GMT-07:00)Mountain Time, (GMT-06:00)Central Time, and (GMT-05:00)Eastern Time. The '(GMT-05:00)Eastern Time' option is selected and highlighted. Below the list box, there is a checkbox labeled 'Day Light Saving' which is checked. At the bottom, it says 'Click **Apply** to continue.' and there is an 'Apply' button.

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 Modem to allow a remote computer to access the Modem’s system activity logs.



The screenshot shows the 'Remote Syslog Capture' configuration window. At the top, it says 'Remote Syslog Capture'. Below that, there is a warning message: 'Warning: Remote Syslog is disabled by default. If you enable it, it may allow sending syslog to the PC running syslog capture application. You can select the PC or input the IP address.' Below the warning, there are two radio buttons: 'On' and 'Off'. The 'Off' radio button is selected. To the right of the radio buttons, there is a section with three labels: 'Current setting:', 'Select PC name:', and 'Or input IP address:'. Each label is followed by a text input field. The 'Current setting:' field is empty. The 'Select PC name:' field has a dropdown arrow. The 'Or input IP address:' field is empty. At the bottom, it says 'Click **Apply** to continue.' and there is an 'Apply' button.

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

**This page left intentionally blank.**

# Configuring Security Settings

# 5

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

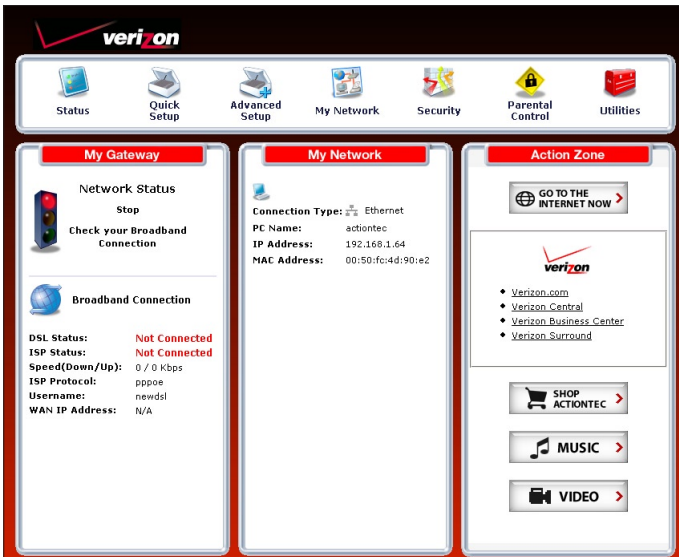
## Accessing Security Screens

To access the 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.

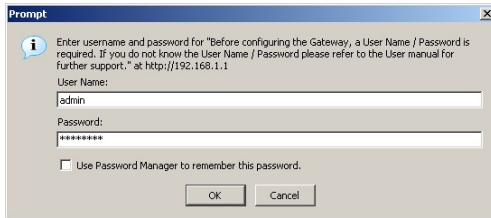


2. The "Home" screen appears. Click **Security**.




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

Firefox:

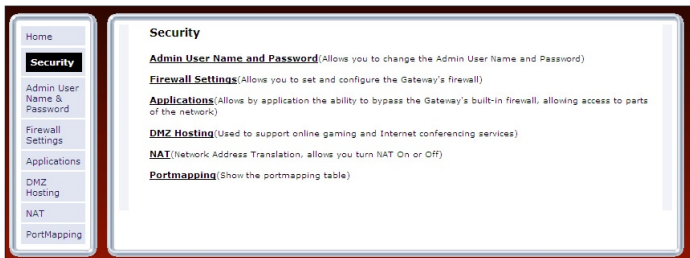


Internet Explorer:



 **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.



**Note:** If VPN connections need to be made through the Modem, the Firewall must be set to Off. No VPN connections can be made if the Firewall setting is at Custom, High, Medium, or Low. Also note that DMZ hosting, Port Forwarding, and Application Level Modem settings are active only when the Firewall is Off.

## 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.

☒ High  
☐ Medium  
☐ Low  
☐ Off

Firewall Info

**Note:** If a check appears in a box, that service is open (or allowed). An empty box signifies the service is closed (or blocked). Any Services not listed below are not allowed.

| Service   | Port  | In                                  | Out                                 |
|-----------|-------|-------------------------------------|-------------------------------------|
| HTTP      | 80    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| DNS       | 53    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| FTP       | 20,21 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IMAPV3    | 220   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| SMTP      | 25    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| POP3      | 110   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| NNTP      | 119   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IPSEC IKE | 500   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IPSEC ESP | esp   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| HTTPS     | 443   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IMAP      | 143   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Apply



## 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.

☐ High  
☒ Medium  
☐ Low  
☐ Off

Firewall Info

**Note:** If a check appears in a box, that service is open (or allowed). An empty box signifies the service is closed (or blocked). Any services not listed below are not allowed.

| Service   | Port  | In                                  | Out                                 |
|-----------|-------|-------------------------------------|-------------------------------------|
| HTTP      | 80    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| DNS       | 53    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| FTP       | 20,21 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IMAPV3    | 220   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| SMTP      | 25    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| POP3      | 110   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| NNTP      | 119   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IPSEC IKE | 500   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IPSEC ESP | esp   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| HTTPS     | 443   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| IMAP      | 143   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Apply

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.

☐ High  
☐ Medium  
☒ **Low**  
☐ Off

Firewall Info

**Note:** If a check appears in a box, that service is open (or allowed). An empty box signifies the service is closed (or blocked). Any services not listed below are allowed.

| Service      | Port | In                                  | Out                                 |
|--------------|------|-------------------------------------|-------------------------------------|
| NETBIOS-SSN  | 139  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| DNS          | 53   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| EPMAP        | 135  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| PROFILE      | 136  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| NETBIOS-NS   | 137  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| NETBIOS-DGM  | 138  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| MICROSOFT-DS | 445  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| SNMP         | 161  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| LDAP         | 389  | <input type="checkbox"/>            | <input type="checkbox"/>            |
| MICROSOFT-GC | 3268 | <input type="checkbox"/>            | <input type="checkbox"/>            |

Apply

### Off

If **Off** is selected in the “Firewall Security Level” screen, firewall filtering is based solely on the basic NAT firewall. At this setting, VPN connections can be made, and DMZ hosting, Port Forwarding, and Application Level Modem settings are active.



**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.

### Applications

When running or accessing certain Internet Applications from your home network, a required port or range of ports specific to the application will need to be opened through the Gateway's firewall.

Follow the steps below to open the appropriate ports through the firewall.

**Step 1.** If not already listed, select the PC that will utilize the application.

**Step 2.** Choose the selected application under the Category section below. A default list of available rules specific to that category will be generated.

**Step 3.** In the **Available Rules** box, select the rule that applies to your application then click **Add**. (To view the rule settings, highlight the desired rule and click the **View Rule** button).

**Step 4.** Click the **Apply** button for the settings to take affect.

**Note:** If the category and available rule is not listed for your application, you can create a rule by choosing the **User** option under the **Category** section. This will generate the **New**, **Edit** and **Delete** buttons. Click the **New** button to create the rule. Once the rule has been created, the ability to **Edit** or **Delete** the rule is available by clicking on the appropriate button.

PC Name:

**Category**

- ☐ Games
- ☐ VPN
- ☐ Audio/Video
- ☐ Apps
- ☐ Servers
- ☐ User

**Available Rules**

Add>>
Remove

**Applied Rules**

View Rule

Apply

This screen allows certain programs to bypass the Modem'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.

Rule Management

Rule Name

Protocol

Port Start  Port End

Port Map Start

| Protocol | Port Start | Port End | Port Map | Delete |
|----------|------------|----------|----------|--------|
|----------|------------|----------|----------|--------|

In this screen, the user can create a custom rule not defined in the programming. To do this (using a single port):

1. Enter the rule name in the “Rule Name” text box. The name is usually based on the application or game title.
2. Set “Protocol” to “TPC.”
3. Enter the port number in the “Port Start,” “Port End,” and “Port Map Start” text boxes. For example, if a server is running on port 8080, enter “8080” in all three text boxes.
4. Click **Apply**.
5. Change Protocol to “UDP.”
6. Enter the port number again, as in step 3.
7. Click **Apply** again. The rule’s TPC and UDP mapping appear at the bottom of the screen.
8. Click **Back**.
9. Select the computer on which to open the ports, then click **User**.
10. Select the rule, then click **Add** to move the rule to the “Applied Rule” text box.
11. Click **Apply**.

For multiple ports:

1. Enter the rule name in the “Rule Name” text box. The name is usually based on the application or game title.
2. Set “Protocol” to “TPC.”
3. Enter the starting port number of the port range in the “Port Start” and “Port Map Start” text boxes, and the last port of the range in the “Port End” text box. For example, if the port range is 5000 to 6000, enter “5000” in the “Port Start” and “Port Map Start” text boxes, and “6000” in the “Port End” text box.
4. Click **Apply**.
5. Change Protocol to “UDP.”
6. Enter the port numbers again, as in step 3.
7. Click **Apply** again. The rule’s TPC and UDP mapping appear at the bottom of the screen.
8. Click **Back**.
9. Select the computer on which to open the ports, then click **User**.
10. Select the rule, then click **Add** to move the rule to the “Applied Rule” text box.
11. Click **Apply**.

### 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**  
Your DSL Gateway can be configured to support online gaming and Internet conferencing services. To use this feature:  

1. Enter the Name of the computer in the DMZ Host PC Name field below.
2. Make sure the circle next to On is selected
3. Click **Apply** to save your changes.

**WARNING!** Using a computer in DMZ mode opens the computer to outside intrusion, thus creating a security risk.

DMZ Host PC Name:

☐ On ☒ Off

**Apply**

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 Modem’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 Modem’s basic firewall security is based on NAT. Disabling NAT allows the computers connected to the Modem 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.

**NAT**  

**Warning:** Please do not disable NAT unless instructed to do so by your ISP. Turning off NAT will open your DSL Gateway to outside intrusion, creating a security risk.

Click **Apply** to continue.

☒ On ☐ Off

**Apply**

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 Modem can be made from this screen.

**PortMapping Table**

| ID | Description | Enabled | RemoteHost | ExternalPort | InternalPort | Protocol | InternalClient |
|----|-------------|---------|------------|--------------|--------------|----------|----------------|
|----|-------------|---------|------------|--------------|--------------|----------|----------------|

# Configuring Parental Controls

# 6

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

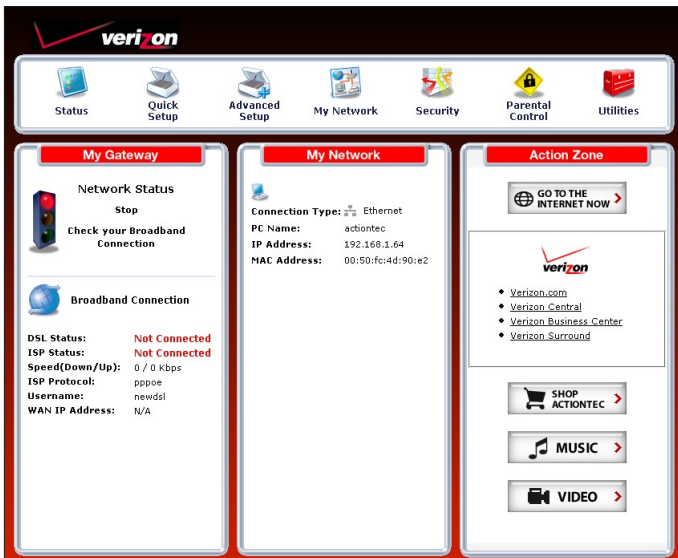
## Accessing Parental Control Screens

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.



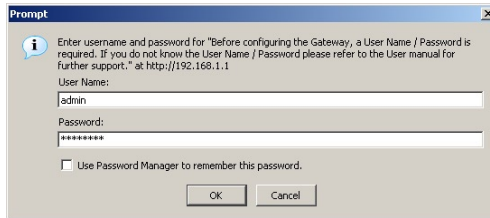
2. The “Home” screen appears. Click **Parental Control**.






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

Firefox:

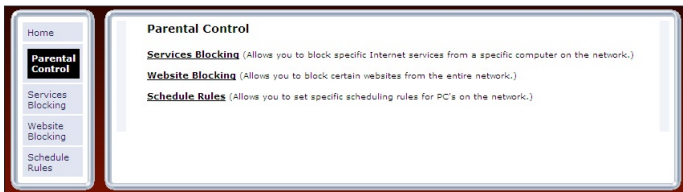


Internet Explorer:



 **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.

**Services Blocking**  
To block Internet Services from a computer on your network, follow the steps below.  
**Step 1.** If not already listed, select the **PC Name** that the Internet blocking will be applied to.  
**Step 2.** Choose the **Internet Services** to be blocked then click **Apply** for your settings to take affect.  
To remove blocked Internet Services unselect the **Blocked Service** then click **Apply** for your settings to take affect.  
**PC Name:**  
  
**Internet Services Blocked**  
☐ Web      ☐ FTP      ☐ Newsgroups      ☐ E-mail

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 Modem 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**.

### Website Blocking

Follow the steps below to block a PC from accessing certain websites.

**Step 1.** If not already listed, select the **PC Name** to be blocked.

**Step 2.** Type the name of the website you wish to be blocked in the **Website to be blocked** field then click **Add**. Example: www.actiontec.com

**Step 3.** Click the **Apply** button for your settings to take affect.

**Note:** Repeat the steps above to block additional websites.

To remove a blocked website, select the **PC Name** and highlight the Website from the **Blocked Website List** then click **Remove**. Click the **Apply** button for your settings to take affect.

PC Name: actiontec

Website to be blocked:

**Add**

**Remove**

**Blocked Website List:**


**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.

### Schedule Rules

To View the Schedule Rules for a specific PC on your Network, select the PC Name and click the “View/Edit Access Details” link.

 PC Name: actiontec [View/Edit Access Details](#)

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.

**actiontec**

Schedule Rules provides the ability to set a specific Time and Day to allow a computer on your network to access the Internet. To set a Schedule Rule

**Step 1.** Click the appropriate button, Daily or Weekly, that you wish to set.  
**Step 2.** Select the scheduled time that you wish to allow Internet access.  
**Step 3.** Click the **Add** button. The rule will be displayed in the **Rules** box to the right.  
**Step 4.** Click **Apply** for the settings to take affect.

**Note:** To remove a rule, highlight the rule you wish to remove located in the **Rules** box then click the **Remove** button. Click **Apply** for the settings to affect.

---

**Allowed Application and Times**

**Note:** Only a Daily or Weekly web browsing option can be set. Setting Daily and Weekly options together will not apply. Once you have set a rule, it will take up to 5 minutes for the rule to take effect.

**Web Browsing**

☒ **Daily**  
☐ **Weekly**

**Time**

From: 9:00 AM **Add**  
 To: 9:00 AM **Remove**

**Rules**


**Apply**

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 Modem.

## 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 Modem's Utilities

# 7

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

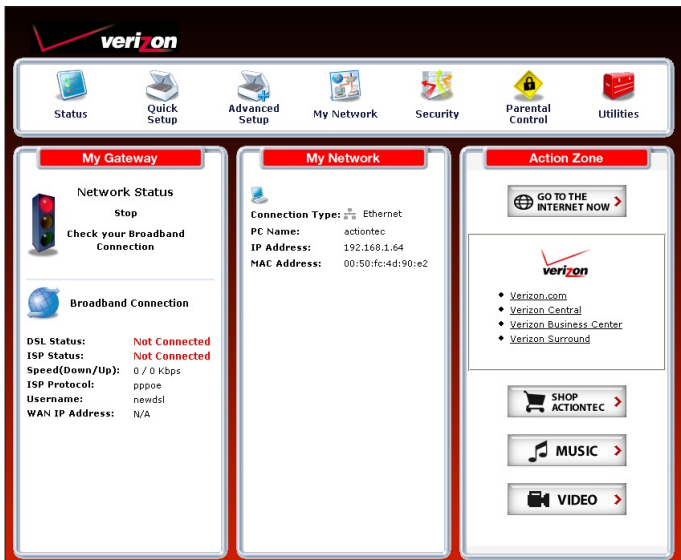
## Accessing the Utilities Screens

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.

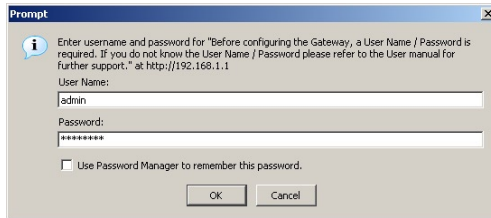


2. The "Home" screen appears. Click **Utilities**.




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

Firefox:

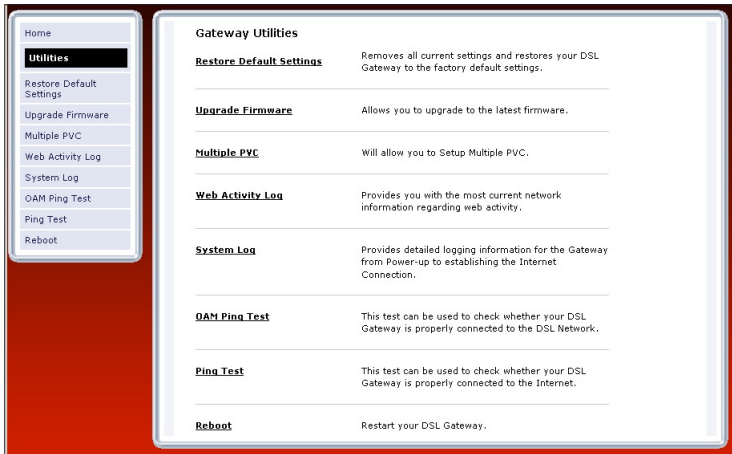


Internet Explorer:



 **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 Modem 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 Modem’s settings will be lost and the factory default settings restored. During this process, the Modem’s Power light flashes and the Modem is disabled.



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

When the Power Light stops flashing and glows steadily green, the Modem 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 Modem’s capabilities. Follow the instructions on-screen to upgrade the Modem’s firmware.

### Upgrade Firmware

The Upgrade file for upgrading firmware may be obtained [here](#).

**Step 1:** Please download the Upgrade file and save it to your local hard disk.

**Step 2:** Use the 'Browse' button to select the Upgrade file.

**Step 3:** Click 'Upgrade' button to start the Upgrade process.

New Firmware Image:

**IMPORTANT:** Please do not refresh or minimize the browser until a successful upgrade message appears.

---

The upgrade process may take 3-6 minutes.

Please read carefully through the following instructions to ensure a successful firmware upgrade:

1. Please do not **RELOAD** or **CLOSE** the browser during the upgrade process.
2. Do not **DISCONNECT** your network cable or power off the DSL Gateway during the firmware upgrade process.
3. Do not run the firmware upgrade if you are connected to the DSL Gateway via **WIRELESS**.
4. It is strongly recommended that you **STOP** any networking activities using the DSL Gateway before starting the upgrade process.
5. If the firmware upgrade process fails, **DO NOT** reboot your DSL Gateway. Please run the upgrade program again.

## Multiple PVC

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

### Multiple PVC

Multiple PVC allows up to 8 PVC channels to pass through the DSL Gateway. You may add Multiple PVC here.

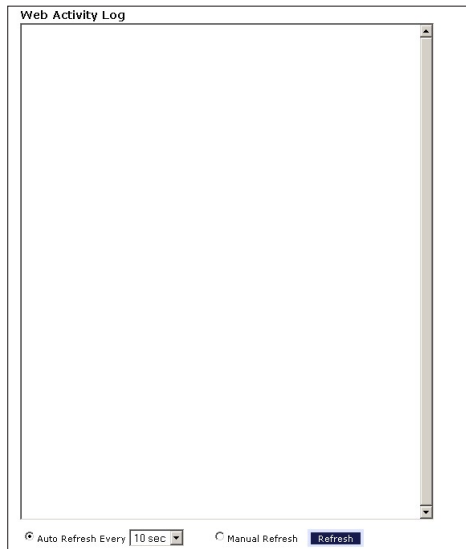
| VPI/VCI   | QoS                              | PCR                  | SCR                  | NBS                  | CDVT                 | Encapsulation                            |
|---|----------------------------------|----------------------|----------------------|----------------------|----------------------|--|
| <input type="text" value="0"/> <input type="text" value="0"/> | <input type="text" value="UBR"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text" value="Bridged LLC"/> |

List of Multi-PVC

Click **Apply** to continue.

### Web Activity Log

The Web Activity Log provides information about the Web sites each computer on the Modem'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 Modem's activity. To access the System Log, select **System Log** from the Utilities screen.

**System Log**  
View the most recent system activity log.

☒ **System Log** 10k **Apply**

**Display** System Log **Save Log As...**

```
(GMT-05:00)20:16:18 Sun Oct 29 2006 udhcpd: SENDING ACK to actiontec
(GMT-05:00)20:16:18 Sun Oct 29 2006 udhcpd: sending ACK to 192.168.1.64
(GMT-05:00)20:16:18 Sun Oct 29 2006 udhcpd: ADD 00:50:fc:4d:90:e2 192.168.1.64
86400 actiontec
(GMT-05:00)20:16:38 Sun Oct 29 2006 udhcpd: SENDING ACK to actiontec
(GMT-05:00)20:16:38 Sun Oct 29 2006 udhcpd: sending ACK to 192.168.1.64
(GMT-05:00)20:16:38 Sun Oct 29 2006 udhcpd: ADD 00:50:fc:4d:90:e2 192.168.1.64
86400 actiontec
(GMT-05:00)20:16:43 Sun Oct 29 2006 logic: fw_trans_query kp.key =
report_all_clients0
(GMT-05:00)20:16:58 Sun Oct 29 2006 udhcpd: SENDING ACK to actiontec
(GMT-05:00)20:16:58 Sun Oct 29 2006 udhcpd: sending ACK to 192.168.1.64
(GMT-05:00)20:16:58 Sun Oct 29 2006 udhcpd: ADD 00:50:fc:4d:90:e2 192.168.1.64
86400 actiontec
(GMT-05:00)20:17:00 Sun Oct 29 2006 logic: fw_trans_query kp.key =
```

### 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 Modem is properly connected to the network. Follow the on-screen instructions to perform the test.

**OAM Ping Test**  
This test can be used to check whether your DSL Gateway is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your "Test Type" from the list and press the Test button.

| Connection | VPI | VCI |
|------------|-----|-----|
| Test       | 0   | 35  |

**Test Type** FS End **Test Result:** Waiting for Test

Test

**OAM Statistics**  
Near End F4 Loop Back Count 0  
Near End F5 Loop Back Count 0  
Far End F4 Loop Back Count 0  
Far End F5 Loop Back Count 0

Clear

### Ping Test

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

**Ping Test**  
This test can be used to check whether your DSL Gateway is properly connected to the Internet. This test may take a few seconds to complete. To perform the test, insert the URL or IP Address that you would like to ping and click the Test button.

URL or IP Address: 192.168.1.1

Number of Pings: 3

Test

PING 192.168.1.1 (192.168.1.1): 64 data bytes  
72 bytes from 192.168.1.1: icmp\_seq=0 ttl=255  
time=0.0 ms  
72 bytes from 192.168.1.1: icmp\_seq=1 ttl=255  
time=0.0 ms  
72 bytes from 192.168.1.1: icmp\_seq=2 ttl=255  
time=0.0 ms  
--- 192.168.1.1 ping statistics ---  
3 packets transmitted, 3 packets received, 0%

### Reboot

Selecting **Reboot** from the Utilities screen generates the “Reboot” screen. From this screen, the Modem can be rebooted. To do this:

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



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



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



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

# Troubleshooting

# 8

This chapter contains a list of problems that may be encountered while using the Modem, 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 Modem is properly installed, the LAN connections are correct, and the power is on.
- Confirm the computer and Modem 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 (192.168.1.64 through 198.168.1.254). If the computer is not using an IP address within the range, it will not connect to the Modem.
- 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 Modem’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 64 through 254).

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 is in the 192.168.1.x network (with "x" defining a range from 64 through 254).

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 Modem 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 Modem is on and connected properly.
- Verify the Modem’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 Modem, and answers to those questions.

### **General**

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

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



### ***Which protocols does the Modem support?***

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

### ***Which connection speeds does the Modem support?***

The LAN connections on the Modem support 10/100 Mbps. The WAN connection supports 8 Mbps, because of the physical restrictions placed on broadband connections.

### ***Will my Xbox work with the Modem?***

Yes, the Modem 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 Modem 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 Modem function as a DSL modem?***

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

## **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 Modem 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 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 Modem?***

The Modem 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 Modem?***

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 Modem, change the default password. Remote management will not be available on the Modem until the default password is changed.

### ***Does the Modem function as a firewall?***

Yes. The Modem 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 Modem supports pass-through for PPTP, L2TP, and IPSec. The VPN pass-through is enabled by default and does not require any additional configuration.

# 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 Modem 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 Modem 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 Modem's factory default IP address. If the Modem's IP address has been changed, enter the new IP address when instructed to enter an IP address.

---

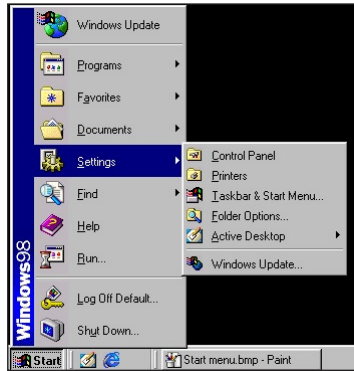
## Windows 98 SE

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

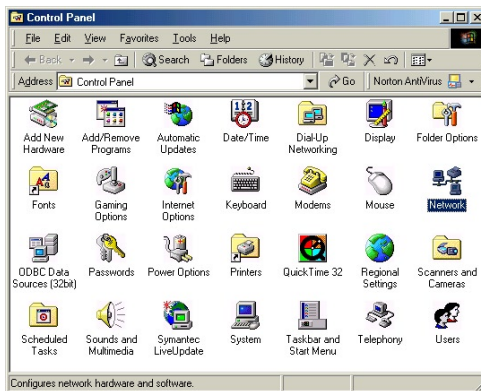




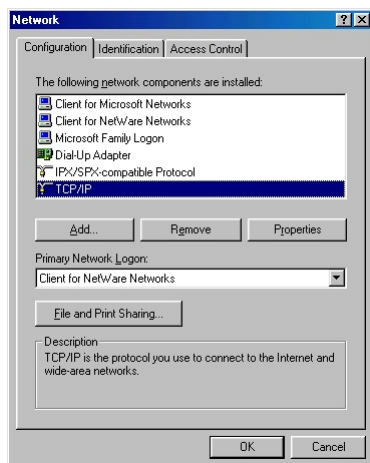
3. Another menu appears. Select **Control Panel**.



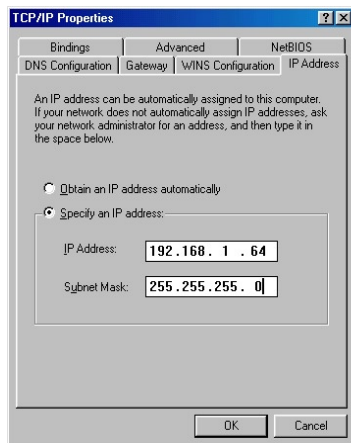
4. When the “Control Panel” window appears, double-click **Network**.



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. 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:  
**192.168.1.64**  
Do not include the periods; they are automatically entered.

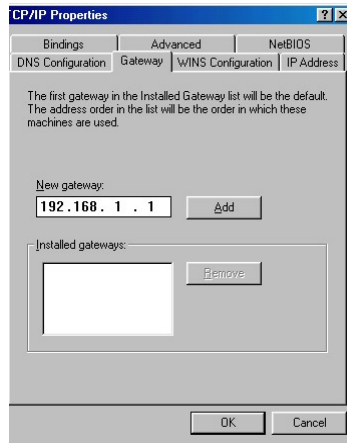
9. Enter the following numbers in the “Subnet mask” text box:

**255.255.255.0**

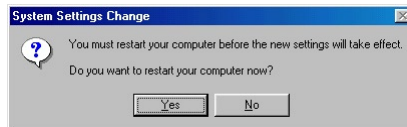
Do not include the periods; they are automatically entered.

10. Select **Gateway**, and, in the “New gateway” text box, enter

**192.168.1.1**



11. If applicable, select “DNS Configuration.” Click “Enable DNS” and enter the DNS servers needed.
12. Click **OK**. The TCP/IP Properties window disappears.
13. In the Network window, click **OK**. The Network window disappears.
14. The “System Settings Change” window appears, asking whether the computer should be restarted. Click **Yes**.



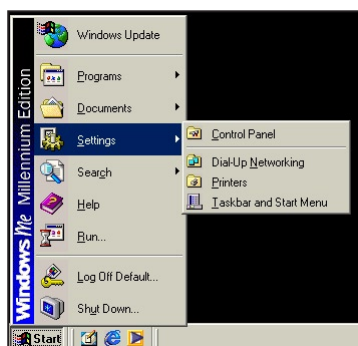
The computer restarts. It is now set up with a static IP address, allowing the user to access the Modem’s Web Configuration Utilities (Advanced Setup, Utilities, etc.).

## Windows Me

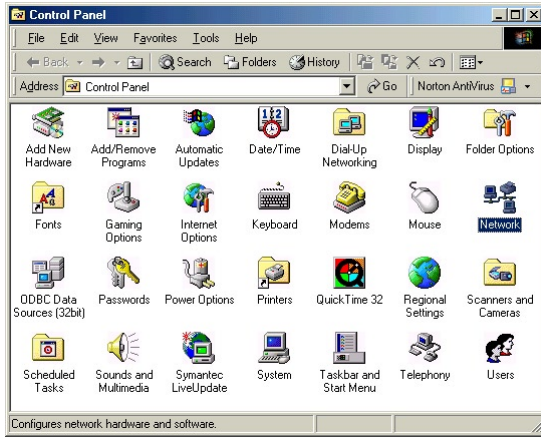
1. From the desktop, click **Start** in the lower left corner.
2. From the menu that appears, select **Settings**.



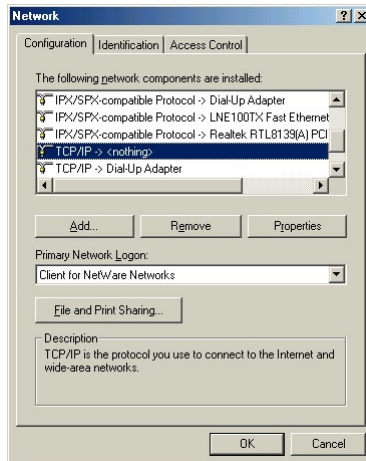
3. Another menu appears. Select **Control Panel**.



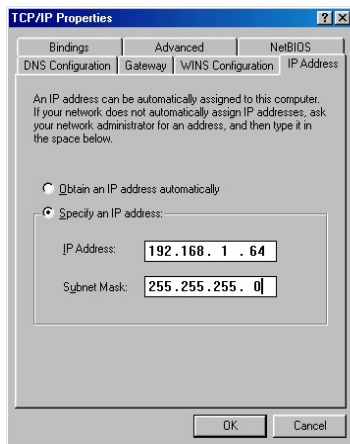
4. When the “Control Panel” window appears, double-click **Network**.



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

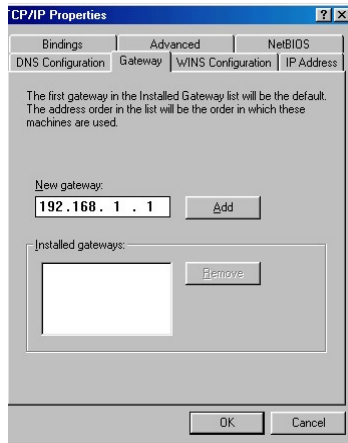


- The “TCP/IP Properties” window appears. Click **IP Address**.

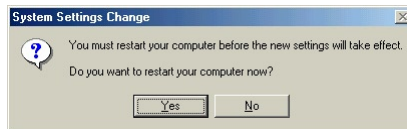


- In the “IP Address” tab, make sure the the circle next to “Specify an IP Address” is selected. When active, a black dot appears in the circle. If the circle already contains a black dot, leave it alone.
- Enter the following numbers in the “IP Address” text box:  
**192.168.1.64**  
Do not include the periods; they are automatically entered.
- Enter the following numbers in the “Subnet mask” text box:  
**255.255.255.0**  
Do not include the periods; they are automatically entered.

10. Select **Gateway**, and, in the “New gateway” text box, enter  
**192.168.1.1**



11. If applicable, select “DNS Configuration.” Click “Enable DNS” and enter the DNS servers needed.
12. Click **OK**. The TCP/IP Properties window disappears.
13. If there is a check in the box next to “Detect connection to network media,” click on it to uncheck the box.
14. In the Network window, click **OK**. The Network window disappears.
15. The “System Settings Change” window appears, asking whether the computer should be restarted. Click **Yes**.



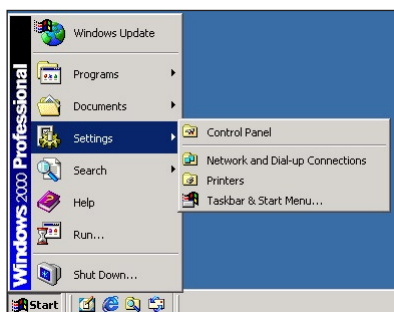
The computer restarts. It is now set up with a static IP address, allowing the user to access the Modem’s Web Configuration Utilities (Advanced Setup, Utilities, etc.).

## **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**.

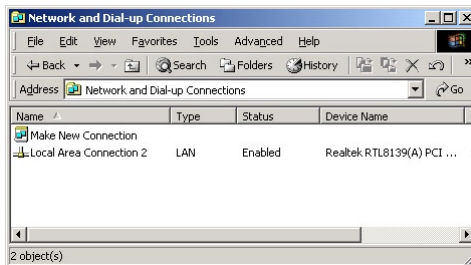




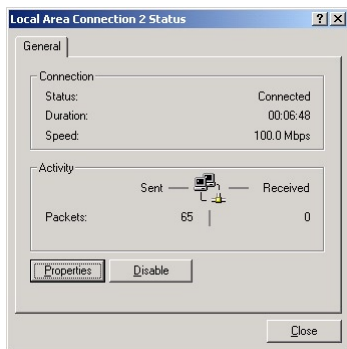
4. When the “Control Panel” window appears, double-click **Network and Dial-up Connections**.



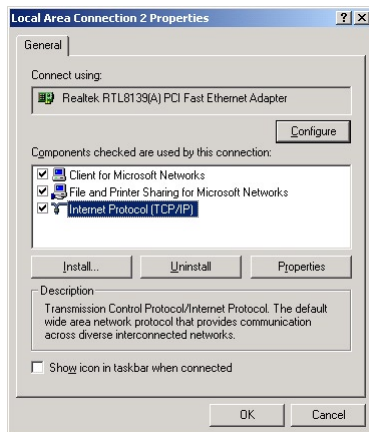
5. In the “Network and Dial-up Connections” window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If there is more than one Local Area Connection listed, locate the one that corresponds to the network card installed in the computer by finding the name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



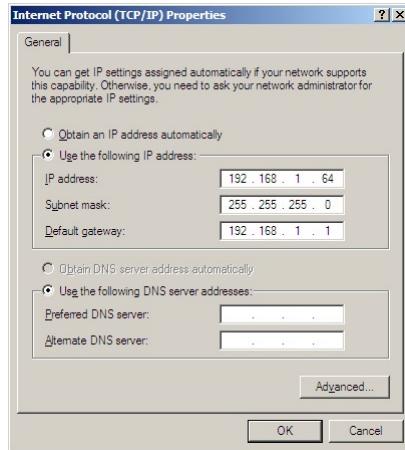
- The “Local Area Connection Status” window appears. Select **General**, then click **Properties**.



- The “Local Area Connection Properties” window appears. Click **General**.
- 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:  
**192.168.1.64**  
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. Enter the following numbers in the “Default gateway” text box:  
**192.168.1.1**  
Do not include the periods; they are automatically entered.
14. Enter the preferred DNS server IP address in the appropriate text box.
15. Click **OK**. The “Internet Protocol (TCP/IP) Properties” window disappears.
16. In the “Local Area Connection Properties” window, click **OK**. The Local Area Connection Properties window disappears.
17. Click **Close** in the Local Area Connection Status window. The window disappears.

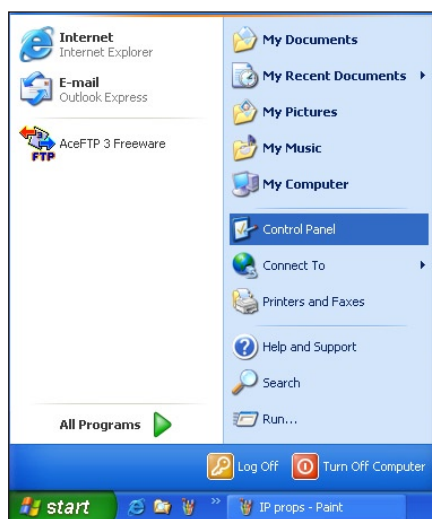
18. Close the Network and Dial-up Connections window by clicking on the “x” button at the upper right corner of the window.

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

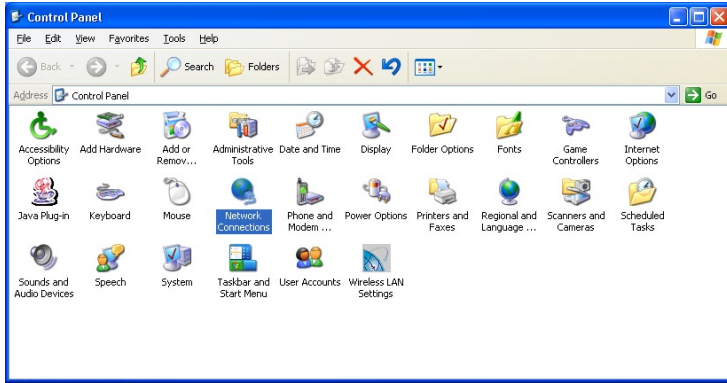
---

## Windows XP

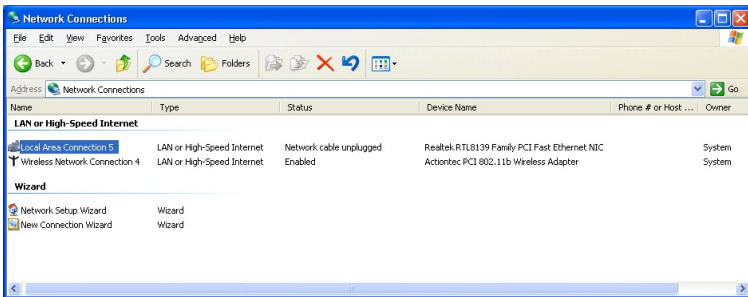
1. From the desktop, click **Start** button in the lower left corner.
2. From the menu that appears, select **Control Panel**.



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

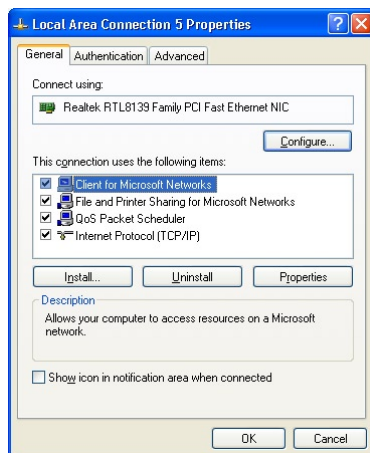


4. In the “Network Connections” window, double-click **Local Area Connection**. A number may be displayed after the Local Area Connection. If more than one Local Area Connection is listed, locate the one that corresponds to the network card installed in your computer by finding the name of the network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

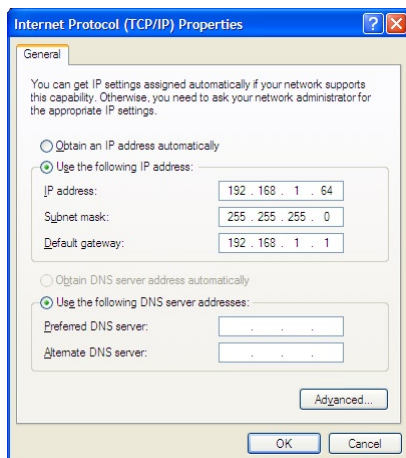


5. The “Local Area Connection Properties” window appears. Select **General**.

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:  
**192.168.1.64**  
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.** Enter the following numbers in the “Default gateway” text box:

**192.168.1.1**

Do not include the periods; they are automatically entered.

- 12.** Enter the preferred DNS server IP address in the appropriate text box.

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

- 14.** In the Local Area Connection Properties window, click **Close**. 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 Modem’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.



## Modem Security

If connecting to the ISP through Point-to-Point Protocol (PPP), be sure to provide the Modem an administrative password. If a password is not set, someone on the Internet can access the Modem 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 Modem 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



---

## General

### Model Number

GT701-C (DSL Modem)

### Standards

IEEE 802.3 (10BaseT)  
IEEE 802.3u (100BaseTX)  
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

### Cabling Type

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

## LED Indicators

Power, DSL, Internet, Ethernet, USB,

---

## Environmental

### Power

External, 12V DC, 600mA

### Certifications

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

### Operating Temperature

0° C to 40° C (32°F to 104°F)

### Storage Temperature

-20°C to 70°C (-4°F to 158°F)

### Operating Humidity

10% to 85% non-condensing

### Storage Humidity

5% to 90% non-condensing

# Glossary

## **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.

## **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.

**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.





# Service Acronyms



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 Name System.** A data query system used to translate host names into Internet addresses (i.e., [www.somewebsite.com](http://www.somewebsite.com) translates to 888.999.000.111). Uses UDP 53 and TCP 53.

### ***EPMAP***

**EndPoint Mapper.** Uses UDP 135 and TCP 135.

### ***FTP***

**File Transfer Protocol.** A protocol used to transfer files over the Internet. Uses TCP 20 and 21.

### ***HTTP***

**HyperText Transfer Protocol.** 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***

**HyperText Transfer Protocol using Secure Socket Layer.** A secure version of the protocol that delivers information over the Internet. Uses UDP 443 and TCP 443.

### ***IMAP, IMAPv3***

Internet Message Access Protocol. 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 Directory Access Protocol. 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 Basic Input Output System. 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 News Transfer Protocol. A protocol used to distribute and retrieve news articles over the Internet. Uses TCP 119.

### ***POP3***

Post Office Protocol 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 Mail Transfer Protocol.** 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 Network Management Protocol.** A set of protocols for managing networks. Uses UDP 161.

**This page left intentionally blank.**