Actiontec
GT704-WG-B
Wireless DSL Gateway
User Manual

Introduction 1

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

Minimum System Requirements

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

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

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

Features

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

Getting to Know the Gateway

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

Front Panel

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

Power Light

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

DSL Light

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

Internet Light

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

Ethernet Lights

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

USB Light

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

Wireless Light

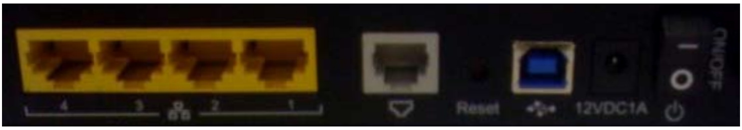
The Wireless light illuminates when the Gateway is connected wirelessly (if the Gateway's Wireless feature is turned on).

WPS Button

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

Rear Panel

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



Ethernet Ports

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

DSL Port

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

Reset Switch

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

USB Port

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

Power Port

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

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

Power Switch

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

This page left intentionally blank.

Performing a Quick Setup

2

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

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

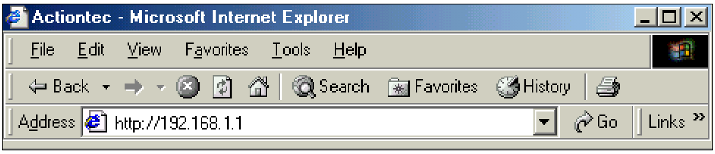
Accessing Quick Setup Screens

To access the Quick Setup screens:

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

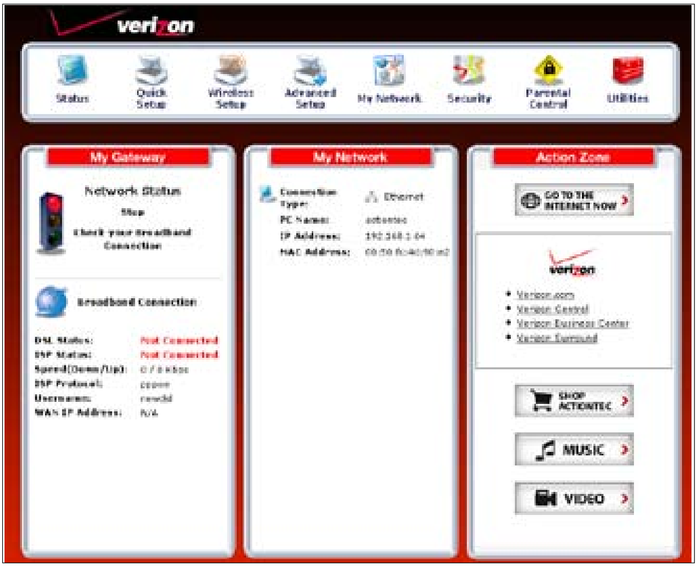
   `http://192.168.1.1`

   then press **Enter** on the keyboard.



http://192.168.1.1

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



Network Status

Stop

Check your Broadband Connection

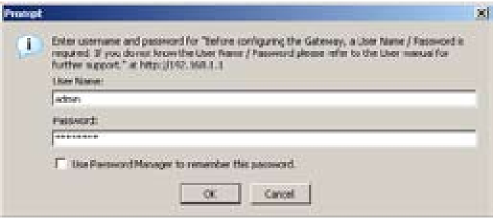
Broadband Connection

DSL Status: Not Connected
ISP Status: Not Connected
Speed(Down/Up): 0 / 0 Kbps
ISP Protocol: PPPoE
Username: [illegible]
WAN IP Address: N/A

Connection Type: Ethernet
PC Name: [illegible]
IP Address: 192.168.1.64
MAC Address: [illegible]

- Verizon.com
- Verizon Central
- Verizon Business Center
- Verizon Surround

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



Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1

User Name:

admin

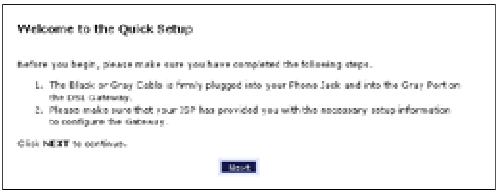
Password:

****

□ Use Password Manager to remember this password.

☞ ***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**.



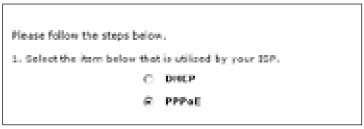
Welcome to the Quick Setup

Before you begin, please make sure you have completed the following steps.

1. The Black or Gray Cable is firmly plugged into your Phone Jack and into the Gray Port on the DSL Gateway.
2. Please make sure that your ISP has provided you with the necessary setup information to configure the Gateway.

Click **NEXT** to continue.

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



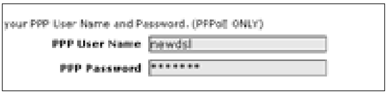
Please follow the steps below.

1. Select the item below that is utilized by your ISP.

○ **DHCP**

● **PPPoE**

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.

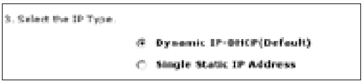


your PPP User Name and Password. (PPPoE ONLY)

PPP User Name newdsl

PPP Password *******

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.

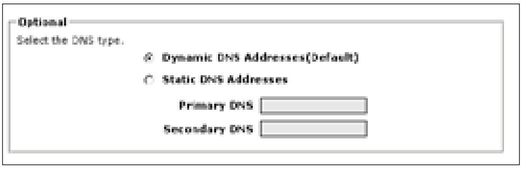


3. Select the IP Type.

● **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)**

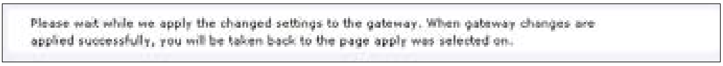
○ **Static DNS Addresses**

Primary DNS

Secondary DNS

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

8. Read the instructions on the next screen. The Gateway 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.

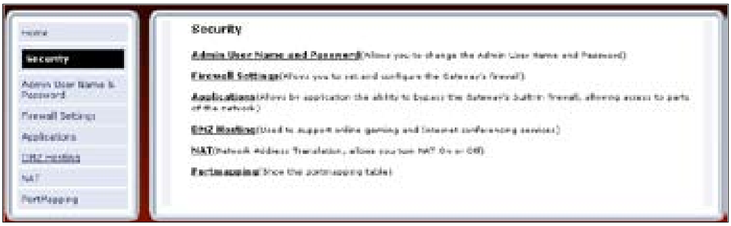
The Power light flashes rapidly while the Gateway restarts, then glows steadily green when fully operational. The Internet light will also glow steadily green. The Gateway is now configured and users can start surfing the Internet.
If an error appears, stating the Web browser was unable to connect to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

Changing the Password

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

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

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



Security

Admin User Name and Password(Allows you to change the Admin User Name and Password)

Firewall Settings(Allows you to set and configure the Gateway's firewall)

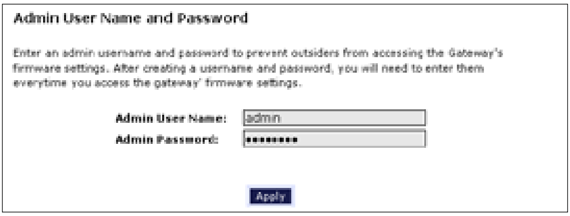
Applications(Allows an application the ability to bypass the Gateway's built-in firewall, allowing access to parts of the network)

DMZ Hosting(Used to support online gaming and Internet conferencing services)

NAT(Network Address Translation, allows you turn NAT On or Off)

Portmapping(Show the portmapping table)

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



Admin User Name and Password

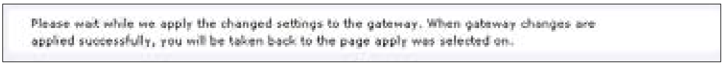
Enter an admin username and password to prevent outsiders from accessing the Gateway's firmware settings. After creating a username and password, you will need to enter them everytime you access the gateway' firmware settings.

Admin User Name: admin

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

This page left intentionally blank.

Viewing the Gateway's Status 3

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

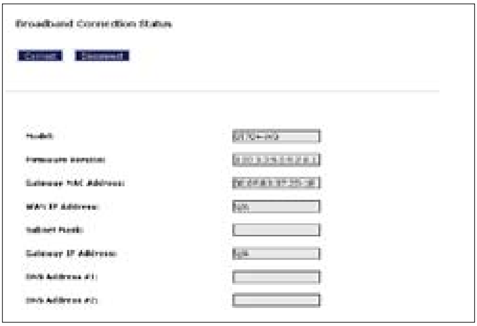
Broadband Connection Status

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

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

General Statistics

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

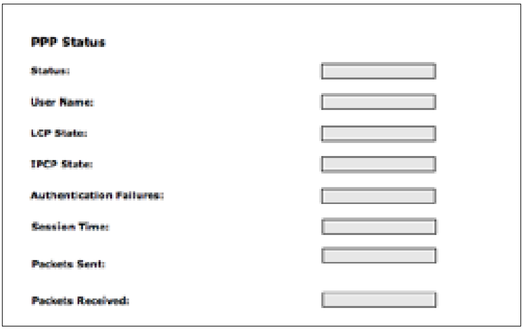


Broadband Connection Status

Model:	[illegible]
Firmware Version:	[illegible]
Gateway MAC Address:	[illegible]
WAN IP Address:	N/A
Subnet Mask:	
Gateway IP Address:	N/A
DNS Address #1:	
DNS Address #2:	

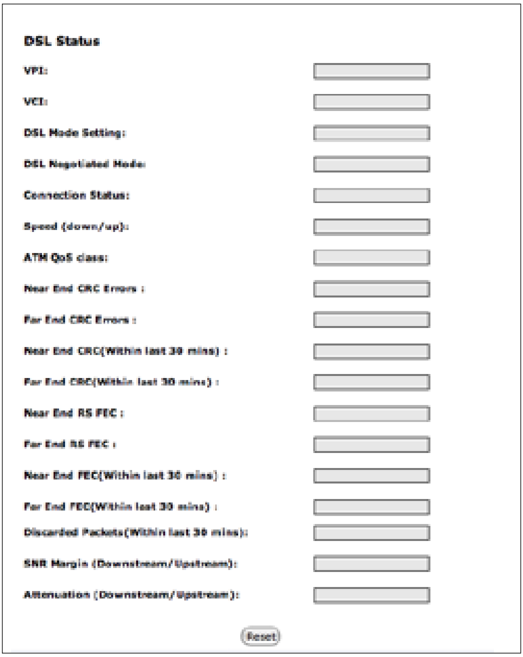
PPP Status

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



DSL Status

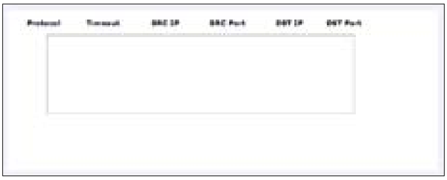
The bottom section of the Broadband Connection Status screen displays the status of the Gateway's DSL connection, including mode settings, connection status, and number of discarded packets. Click **Reset** to refresh all statistics on this screen


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

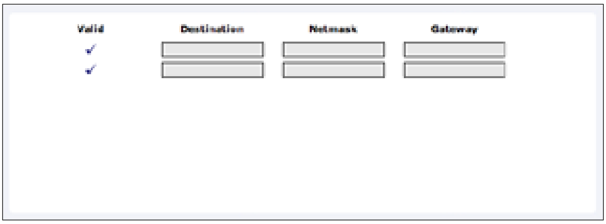
Selecting **NAT Table** generates the "NAT Table" screen. This screen displays an overview of the current list of open connections through NAT (Network Address Translation) the Gateway supports between the networked computers and the Internet.



Protocol	Timeout	SRC IP	SRC Port	DST IP	DST Port

Routing Table

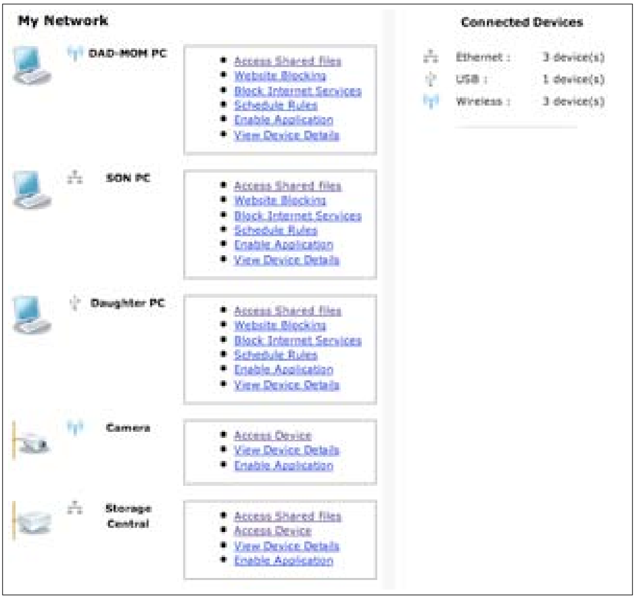
Selecting **Routing Table** generates the "Routing Table" screen. This screen displays the an overview of the Gateway's network routes.



Valid	Destination	Netmask	Gateway
✓			
✓			

Network Status

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



My Network

DAD-MOM PC
- Access Shared files
- Website Blocking
- Block Internet Services
- Schedule Rules
- Enable Application
- View Device Details

SON PC
- Access Shared files
- Website Blocking
- Block Internet Services
- Schedule Rules
- Enable Application
- View Device Details

Daughter PC
- Access Shared files
- Website Blocking
- Block Internet Services
- Schedule Rules
- Enable Application
- View Device Details

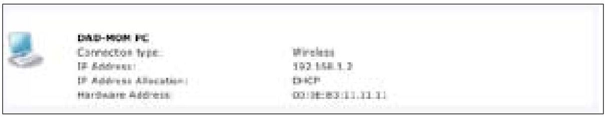
Camera
- Access Device
- View Device Details
- Enable Application

Storage Central
- Access Shared files
- Access Device
- View Device Details
- Enable Application

Connected Devices

Ethernet :	3 device(s)
USB :	1 device(s)
Wireless :	3 device(s)

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.



DAD-MOM PC

Connection type:	Wireless
IP Address:	192.168.1.2
IP Address Allocation:	DHCP
Hardware Address:	00:0E:83:11:11:11

Configuring Wireless Settings 4

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

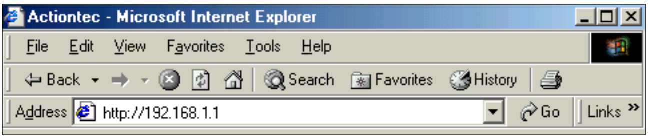
Accessing Wireless Setup

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

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

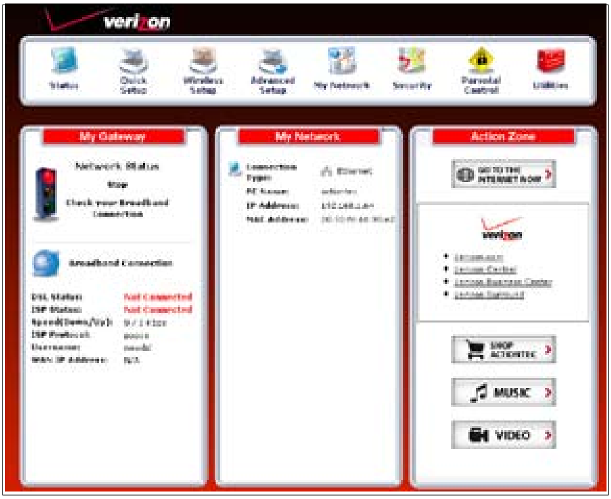
   ```
   http://192.168.1.1
   ```

   then press **Enter** on the keyboard.



Address http://192.168.1.1

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



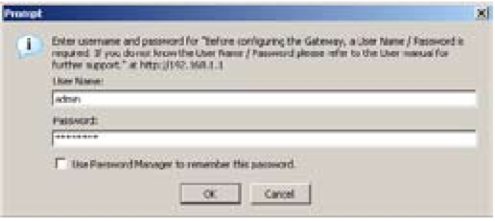
Network Status
Stop
Check your Broadband Connection

Broadband Connection

DSL Status: Not Connected
ISP Status: Not Connected
Speed(Down/Up): [illegible]
ISP Protocol: [illegible]
Username: [illegible]
WAN IP Address: N/A

Connection Type: Ethernet
PC Name: [illegible]
IP Address: [illegible]
MAC Address: [illegible]

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



Prompt

Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1

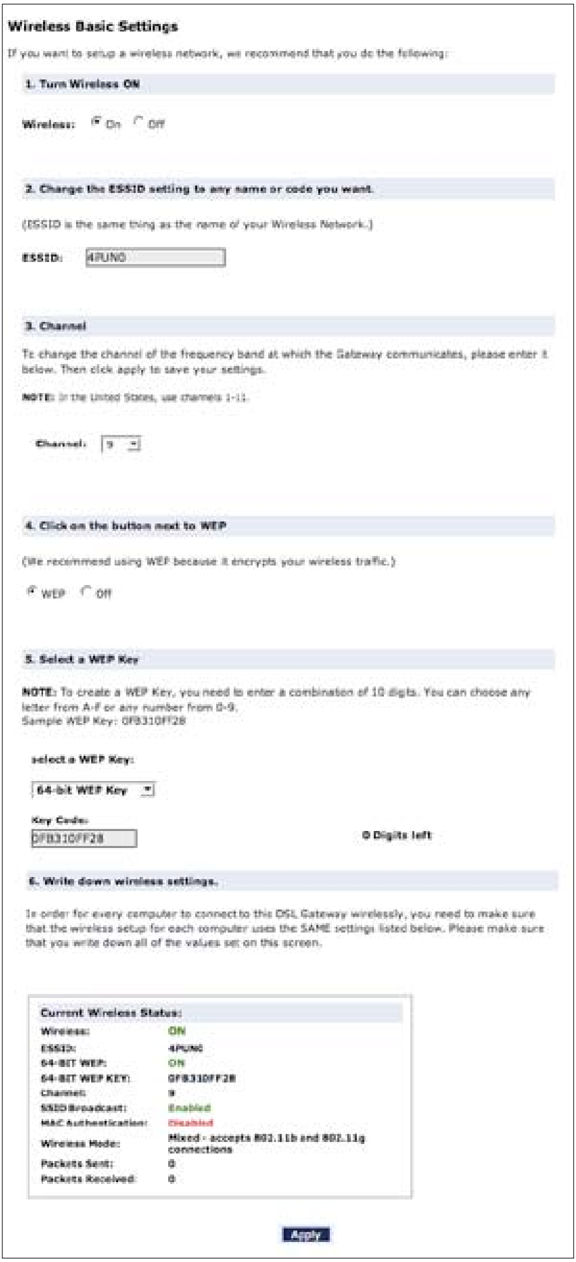
User Name: admin

Password: ********

□ Use Password Manager to remember this password.

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

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



Wireless Basic Settings

If you want to setup a wireless network, we recommend that you do the following:

1. Turn Wireless ON

Wireless: ● On ○ Off

2. Change the ESSID setting to any name or code you want.

(ESSID is the same thing as the name of your Wireless Network.)

ESSID: 4PUNO

3. Channel

To change the channel of the frequency band at which the Gateway communicates, please enter it below. Then click apply to save your settings.

NOTE: In the United States, use channels 1-11.

Channel: 9

4. Click on the button next to WEP

(We recommend using WEP because it encrypts your wireless traffic.)

● WEP ○ Off

5. Select a WEP Key

NOTE: To create a WEP Key, you need to enter a combination of 10 digits. You can choose any letter from A-F or any number from 0-9.
Sample WEP Key: 0FB310FF28

select a WEP Key:

64-bit WEP Key

Key Code:

0FB310FF28

0 Digits left

6. Write down wireless settings.

In order for every computer to connect to this DSL Gateway wirelessly, you need to make sure that the wireless setup for each computer uses the SAME settings listed below. Please make sure that you write down all of the values set on this screen.

Current Wireless Status:	
Wireless:	ON
ESSID:	4PUNO
64-BIT WEP:	ON
64-BIT WEP KEY:	0FB310FF28
Channel:	9
SSID Broadcast:	Enabled
MAC Authentication:	Disabled
Wireless Mode:	Mixed - accepts 802.11b and 802.11g connections
Packets Sent:	0
Packets Received:	0

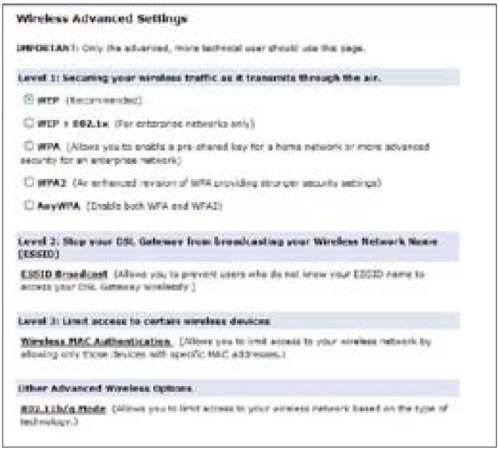
Basic Wireless Setup

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

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

Wireless Advanced Settings

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



Wireless Advanced Settings

IMPORTANT: Only the advanced, more technical user should use this page.

Level 1: Securing your wireless traffic as it transmits through the air.

● **WEP** (Recommended)

○ **WEP + 802.1x** (For enterprise networks only)

○ **WPA** (Allows you to enable a pre-shared key for a home network or more advanced security for an enterprise network)

○ **WPA2** (An enhanced revision of WPA providing stronger security settings)

○ **AnyWPA** (Enable both WPA and WPA2)

Level 2: Stop your DSL Gateway from broadcasting your Wireless Network Name (ESSID)

ESSID Broadcast (Allows you to prevent users who do not know your ESSID name to access your DSL Gateway wirelessly.)

Level 3: Limit access to certain wireless devices

Wireless MAC Authentication (Allows you to limit access to your wireless network by allowing only those devices with specific MAC addresses.)

Other Advanced Wireless Options

802.11b/g Mode (Allows you to limit access to your wireless network based on the type of technology.)

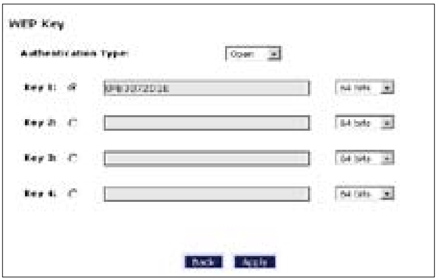
This generates the "Wireless Advanced Settings" screen. In this screen, the security of the wireless network can be activated and fortified.

Wireless Security

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

WEP

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



WEP Key

Authentication Type: Open

Key 1: ● 0F83272D16 — 64 bits

Key 2: ○ — 64 bits

Key 3: ○ — 64 bits

Key 4: ○ — 64 bits

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

64-bit WEP - 64-bit WEP requires one or more keys, each key comprising five hexadecimal pairs. One key (Key 1) is automatically generated by the Gateway at start-up, based on the Gateway's MAC address. This key is also displayed on a sticker on the bottom of the Gateway. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 64-bit WEP key is: 4E-A3-3D-68-72. To create a new set of 64-bit WEP keys, activate one or more keys by clicking in the appropriate circles, then enter five hexadecimal digit pairs in each activated **Key** text box (**Key 1-**, **Key 2-**, **Key 3-**, **Key 4-**). After activating 64-bit WEP, a computer with wireless capability can join the network only if these same keys are entered in the computer's wireless encryption scheme.

128-bit WEP - 128-bit WEP requires one or more keys, each key comprising 13 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. An example of a 128-bit WEP key is: 3D-44-FE-6C-A1-EF-2E-D3-C4-21-74-5D-B1. To create a 128-bit WEP key, activate **Key 1** by clicking in the appropriate circle, select "128 bit" from the drop-down list on the right, then enter 13 hexadecimal digit pairs in the **Key** text box. After activating 128-bit WEP, a computer with wireless capability can join the network only if this key is entered in the computer's wireless encryption scheme.

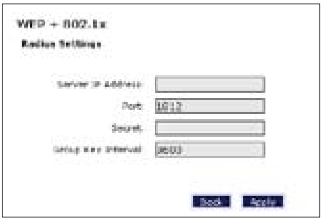
256-bit WEP - 256-bit WEP requires one or more keys, each key comprising 29 hexadecimal pairs. A hexadecimal digit consists of an alphanumeric character ranging from 0-9 or A-F. To create a 256-bit WEP key, activate **Key 1** by clicking in the appropriate circle, select "256 bit" from the drop-down list on the right, then enter 29 hexadecimal digit pairs in the **Key** text box. After activating 256-bit WEP, a computer with wireless capability can join the network only if this key is entered in the computer's wireless encryption scheme.

☞ ***Note***: Not all wireless PC Cards support 128- or 256-bit WEP. Ensure all PC Cards installed in the networked computers support 128- or 256-bit WEP before activating.

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

WEP+802.1x

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



WEP + 802.1x

Radius Settings

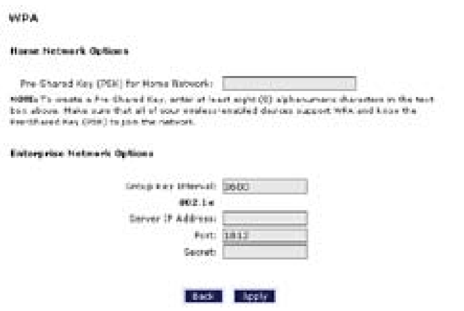
Server IP Address:
Port: 1812
Secret:
Group Key Interval: 3600

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

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

WPA, WPA2, AnyWPA

Activating any of the three **WPA** (Wi-Fi Protected Access) options in the Wireless Advanced Settings screen generates a "Wireless WPA Settings" screen. The three WPA options use identical procedures to activate, although WPA2 provides stronger security than standard WPA. AnyWPA activates both WPA and WPA2.



WPA

Home Network Options

Pre-Shared Key (PSK) for Home Network:

NOTE: To create a Pre-Shared Key, enter at least eight (8) alphanumeric characters in the text box above. Make sure that all of your wireless-enabled devices support WPA and know the PreShared Key (PSK) to join the network.

Enterprise Network Options

Group Key Interval: 3600

802.1x

Server IP Address:

Port: 1812

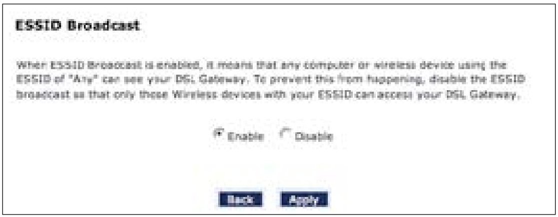
Secret:

There are two levels of WPA. "Pre-Shared Key (PSK) for Home Network" is for home network security. To set up a PSK (Pre-Shared Key), enter 8-63 alphanumeric characters in the text box. All wireless-enabled devices must support WPA and know the PSK to join the network.
The "Group Key Interval," "Server IP Address," "Port," and "Secret" text boxes are enterprise network specific, and should only be accessed by an information systems professional. See "WEP+802.1x" on the previous page for more information.

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

ESSID Broadcast

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



ESSID Broadcast

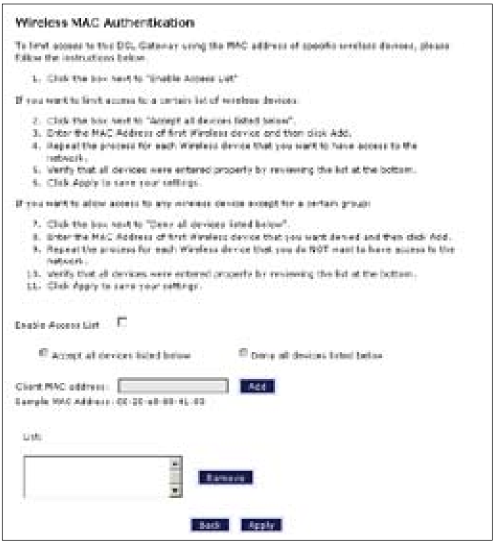
When ESSID Broadcast is enabled, it means that any computer or wireless device using the ESSID of "Any" can see your DSL Gateway. To prevent this from happening, disable the ESSID broadcast so that only those Wireless devices with your ESSID can access your DSL Gateway.

● Enable ○ Disable

To prevent a unwanted computers from joining the Gateway's wireless network by using an ESSID of "Any," select **Disable** in the ESSID Broadcast screen. To broadcast the wireless network's ESSID, select **Enable**.
When finished with this screen, click **Apply** to save all changes. To return to the Wireless Advanced Settings screen, click **Back**.

Wireless MAC Authentication

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



Wireless MAC Authentication

To limit access to this DSL Gateway using the MAC address of specific wireless devices, please follow the instructions below.

1. Click the box next to "Enable Access List"

If you want to limit access to a certain list of wireless devices

2. Click the box next to "Accept all devices listed below".
3. Enter the MAC Address of first Wireless device and then click Add.
4. Repeat the process for each Wireless device that you want to have access to the network.
5. Verify that all devices were entered properly by reviewing the list at the bottom.
6. Click Apply to save your settings.

If you want to allow access to any wireless device except for a certain group

7. Click the box next to "Deny all devices listed below".
8. Enter the MAC Address of first Wireless device that you want denied and then click Add.
9. Repeat the process for each Wireless device that you do NOT want to have access to the network.
10. Verify that all devices were entered properly by reviewing the list at the bottom.
11. Click Apply to save your settings.

Enable Access List ☐

○ Accept all devices listed below ○ Deny all devices listed below

Client MAC address:

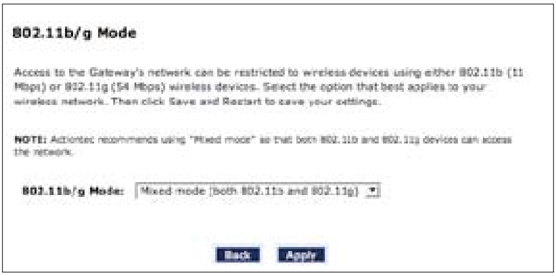
Sample MAC Address : 00-20-e0-00-41-02

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

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

802.11b/g Mode

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



802.11b/g Mode

Access to the Gateway's network can be restricted to wireless devices using either 802.11b (11 Mbps) or 802.11g (54 Mbps) wireless devices. Select the option that best applies to your wireless network. Then click Save and Restart to save your settings.

NOTE: Actiontec recommends using "Mixed mode" so that both 802.11b and 802.11g devices can access the network.

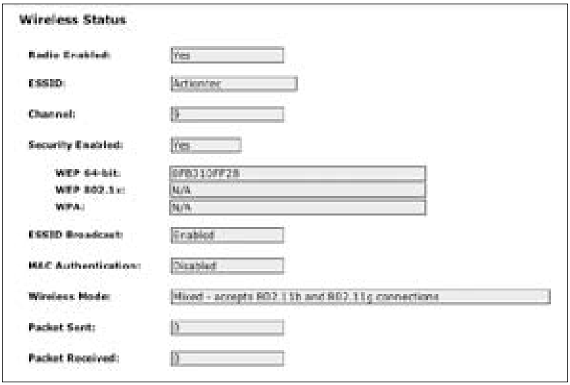
802.11b/g Mode: Mixed mode (both 802.11b and 802.11g)

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

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

Wireless Status

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



Wireless Status

Radio Enabled: Yes

ESSID: Actiontec

Channel: 1

Security Enabled: Yes

WEP 64-bit: 0FB310FF28

WEP 802.1x: N/A

WPA: N/A

ESSID Broadcast: Enabled

MAC Authentication: Disabled

Wireless Mode: Mixed - accepts 802.11b and 802.11g connections

Packet Sent: 0

Packet Received: 0

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

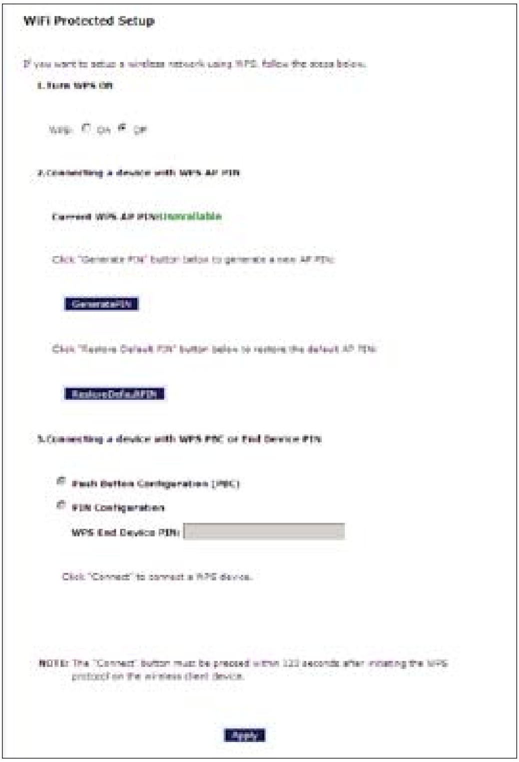
WPS (WiFI Protected Setup)

WiFi Protected Setup (WPS) provides an easier way to set up a wireless network. Instead of entering passwords or multiple keys on each wireless client (laptop, printer, external hard drive, etc.), the Router can create a wireless network that only requires pressing buttons (one on the Router, and one on the client [either built-in, or on a compatible wireless card]) to allow wireless clients to join the Router's wireless network.

Activating WPS

To activate WPS on the Router:

1. From the Router's Home screen, click **Wireless Setup**, then select **WPS** from the menu on the left side. The "WiFi Protected Setup" screen appears.



WiFi Protected Setup

If you want to setup a wireless network using WPS, follow the steps below.

1.Turn WPS ON

WPS: ○ On ● Off

2.Connecting a device with WPS AP PIN

Current WPS AP PIN:Unavailable

Click "Generate PIN" button below to generate a new AP PIN:

Click "Restore Default PIN" button below to restore the default AP PIN:

3.Connecting a device with WPS PBC or End Device PIN

○ Push Button Configuration (PBC)

○ PIN Configuration

WPS End Device PIN:

Click "Connect" to connect a WPS device.

NOTE: The "Connect" button must be pressed within 120 seconds after initiating the WPS protocol on the wireless client device.

2. Activate WPS by clicking the "On" radio button under "Turn WPS ON."

3. Click **Apply** at the bottom of the screen. The Router is now ready to accept WPS clients on its wireless network.

Joining the WPS Wireless Network

To join the WPS wireless network, press the “Wi-Fi Protected Setup” button on the front panel of the Router, then press the WPS button on the wireless client. The Router and client will search and locate each other, then auto-configure whatever wireless security (WPA, etc.) is being used. It can take up to 2 minutes for the Router and client to finish the connection procedure. When the connection proecedure has completed, the client will be on the secure wireless network.

Alternatively, a client can join the Router’s WPS wireless network by entering the Router’s WPS PIN number in the client’s wireless network setup GUI. The Router’s WPS AP PIN number is displayed in the WiFi Protected Setup screen. If no PIN appears, click **Generate PIN** to create one.

This page left intentionally blank.

Configuring Advanced Settings 5

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

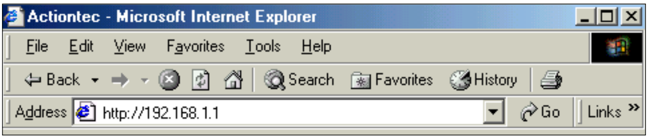
Accessing Advanced Setup Screens

To access the Advanced Setup screens, follow these instructions:

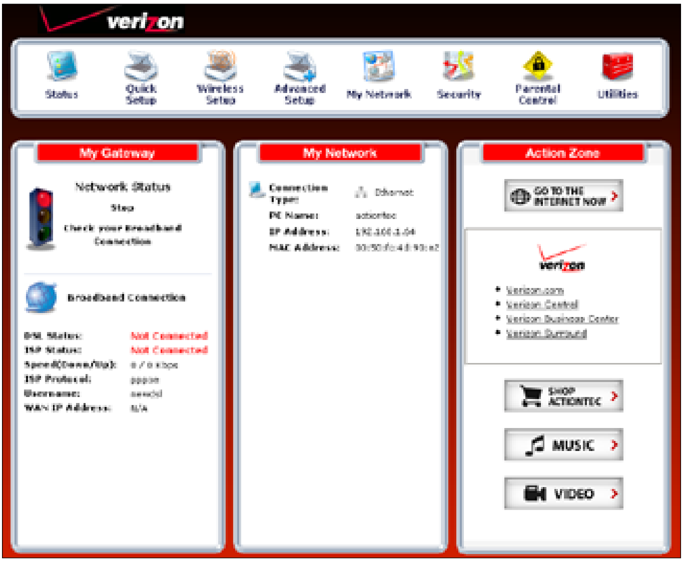
1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.1.1`

   then press **Enter** on the keyboard.



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



Network Status

Stop

Check your Broadband Connection

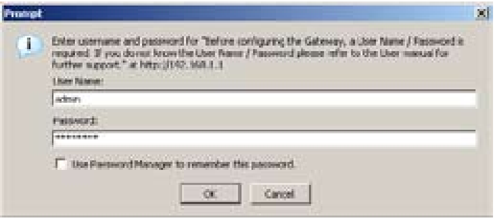
Broadband Connection

DSL Status: Not Connected
ISP Status: Not Connected
Speed(Down/Up): 0 / 0 Kbps
ISP Protocol: pppoe
Username: sewsld
WAN IP Address: N/A

Connection Type: Ethernet
PC Name: actiontec
IP Address: 192.168.1.64
MAC Address: 00:50:fc:4f:93:e2

- Verizon.com
- Verizon Central
- Verizon Business Center
- Verizon Surround

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



Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1

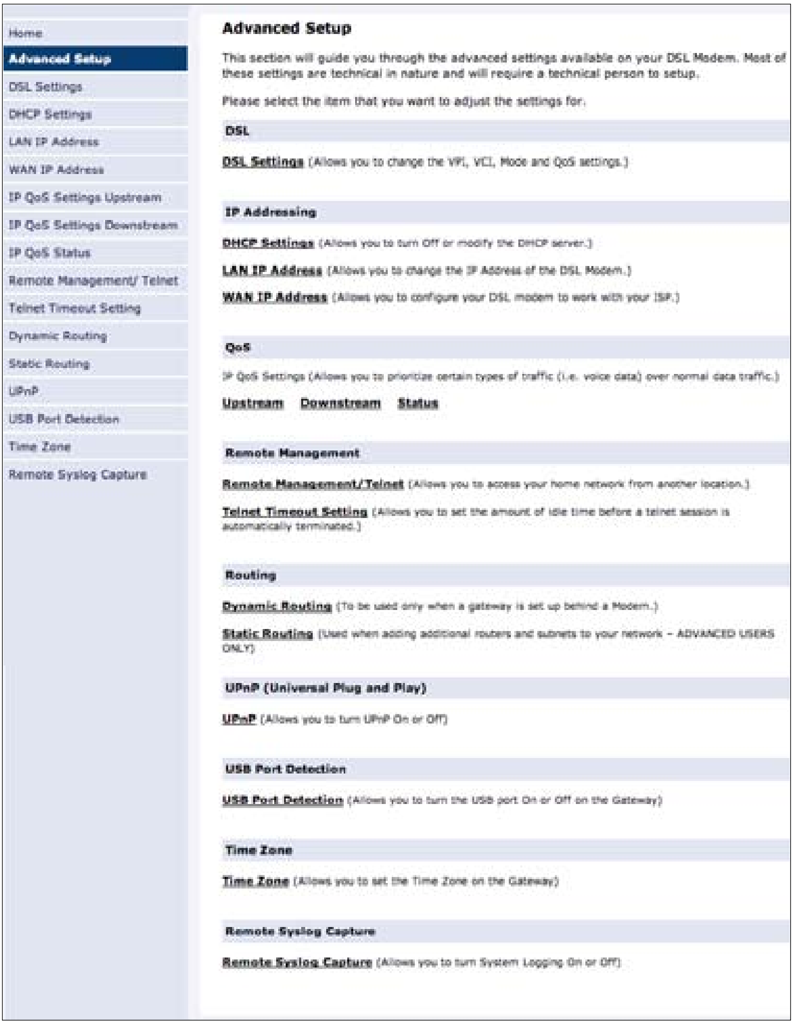
User Name: admin

Password: ********

□ Use Password Manager to remember this password.

☞ ***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.



Advanced Setup

This section will guide you through the advanced settings available on your DSL Modem. Most of these settings are technical in nature and will require a technical person to setup.

Please select the item that you want to adjust the settings for.

DSL

DSL Settings (Allows you to change the VPI, VCI, Mode and QoS settings.)

IP Addressing

DHCP Settings (Allows you to turn Off or modify the DHCP server.)

LAN IP Address (Allows you to change the IP Address of the DSL Modem.)

WAN IP Address (Allows you to configure your DSL modem to work with your ISP.)

QoS

IP QoS Settings (Allows you to prioritize certain types of traffic (i.e. voice data) over normal data traffic.)

Upstream **Downstream** **Status**

Remote Management

Remote Management/Telnet (Allows you to access your home network from another location.)

Telnet Timeout Setting (Allows you to set the amount of idle time before a telnet session is automatically terminated.)

Routing

Dynamic Routing (To be used only when a gateway is set up behind a Modem.)

Static Routing (Used when adding additional routers and subnets to your network – ADVANCED USERS ONLY)

UPnP (Universal Plug and Play)

UPnP (Allows you to turn UPnP On or Off)

USB Port Detection

USB Port Detection (Allows you to turn the USB port On or Off on the Gateway)

Time Zone

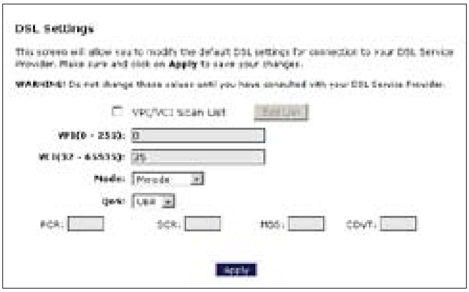
Time Zone (Allows you to set the Time Zone on the Gateway)

Remote Syslog Capture

Remote Syslog Capture (Allows you to turn System Logging On or Off)

DSL Settings

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



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): 0

VCI(32 - 65535): 35

Mode: Pmode

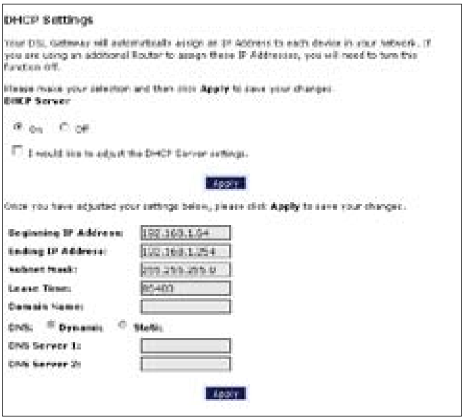
QoS: UBR

PCR: SCR: MBS: CDVT:

DHCP Settings

Selecting **DHCP Settings** in the “Advanced Setup” screen generates the “DHCP Settings” screen. The Gateway has a built-in DHCP (Dynamic Host Configuration Protocol) server that automatically assigns a different IP address to each computer on the network, eliminating IP address conflicts.

The factory default setting is **On**. To disable the DHCP Server, select **Off**, then click **Apply**.



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: 192.168.1.64

Ending IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Lease Time: 86400

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 Gateway. For more information, see "DHCP Server Configuration."

DHCP Server Configuration

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

Beginning IP Address

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

Ending IP Address

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

The beginning and ending IP addresses define the IP address range of the Gateway. If the default values are left intact, the Gateway supplies a unique IP address between 192.168.1.64 and 192.168.1.254 to each computer on the network. Note that the first three groups of numbers of the addresses are identical; this means they are on the same subnet. The IP address of the Gateway must be on the same subnet as the IP address range it generates. For instance, if the Gateway's IP address is changed to 10.33.222.1, set the beginning IP address to 10.33.222.2, and the ending IP address to 10.33.222.254.

Subnet Mask

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

Lease Time

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

Domain Name

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

DNS (Dynamic or Static)

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

DNS Server 1

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

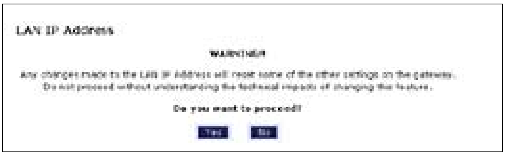
DNS Server 2

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

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

LAN IP Address

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



LAN IP Address

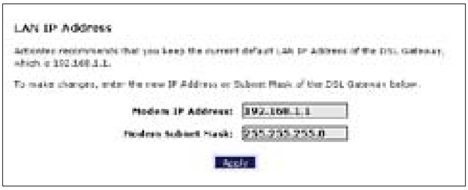
WARNING

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: 192.168.1.1

Modem Subnet Mask: 255.255.255.0

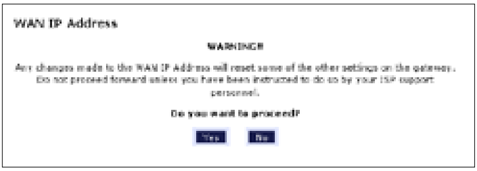
The values in the “Modem IP Address” and “Modem Subnet Mask” text boxes are the IP and subnet mask address of the Gateway as seen on the network. These values can be modified for your LAN network, but we recommend keeping the default factory settings (IP address 192.168.1.1; subnet mask address 255.255.255.0).

☞ ***Note***: If the Gateway’s LAN IP Address is modified, verify the DHCP Server range is within the same subnet. For more information, see “DHCP Server Configuration.”

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

WAN IP Address

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



WAN IP Address

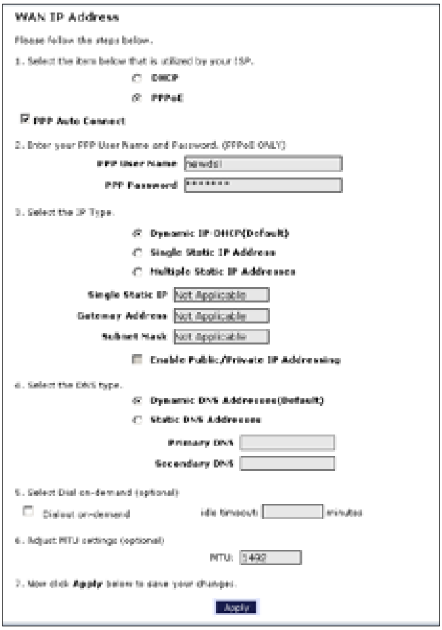
WARNING!

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: newdsl

PPP Password: *******

3. Select the IP Type.

● Dynamic IP DHCP(Default)

○ Single Static IP Address

○ Multiple Static IP Addresses

Single Static IP: Not Applicable

Gateway Address: Not Applicable

Subnet Mask: Not Applicable

□ 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: 1492

7. Now click **Apply** below to save your changes.

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

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

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

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

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

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

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

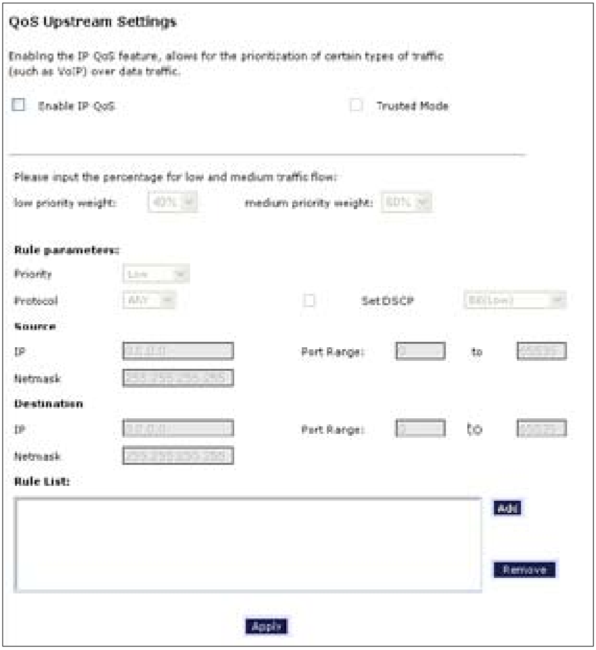
6. Select Dialout on-demand (optional). To have the Gateway automatically connect to the Internet whenever needed (when a Web browser is opened, for example), activate "Dialout on-demand" by clicking in the appropriate check box. When Dialout on-demand is activated, the user can also set the Gateway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

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

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

QoS Settings Upstream

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



QoS 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: 40% medium priority weight: 60%

Rule parameters:

Priority: Low

Protocol: ANY ☐ Set DSCP: BE(Low)

Source

IP: 0.0.0.0 Port Range: 0 to 65535

Netmask: 255.255.255.255

Destination

IP: 0.0.0.0 Port Range: 0 to 65535

Netmask: 255.255.255.255

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 prioritzed using QoS.

Enable QoS

Clicking in this check box activates/deactivates QoS.

Trusted Mode

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

Total Available Bandwidth

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

High Priority Bandwidth

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

Priority

Always set to “High” and cannot be changed.

Protocol

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

Source

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

Destination

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

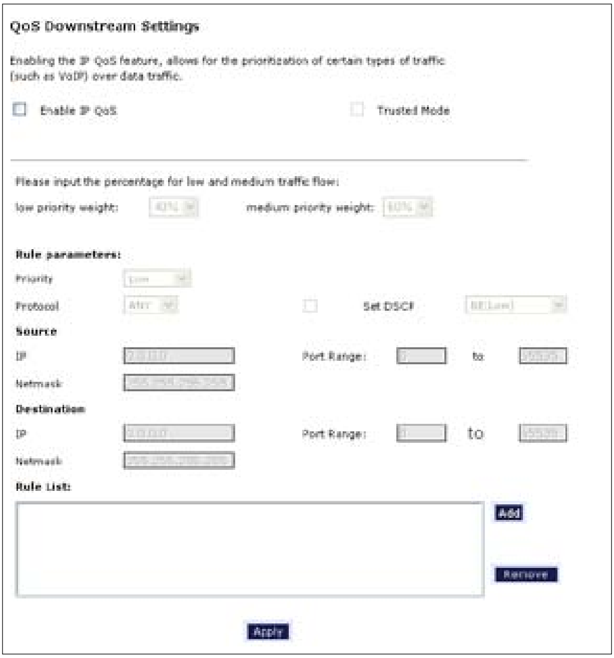
Rule List

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

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

QoS Settings Downstream

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



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: 40% medium priority weight: 60%

Rule parameters:

Priority: Low

Protocol: ATM □ Set DSCP BE(Low)

Source

IP: 0.0.0.0 Port Range: 0 to 65535

Netmask: 255.255.255.255

Destination

IP: 0.0.0.0 Port Range: 0 to 65535

Netmask: 255.255.255.255

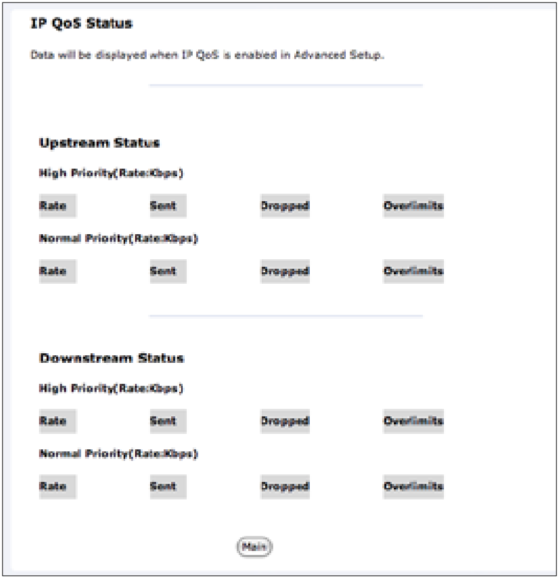
Rule List:

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



IP QoS Status

Data will be displayed when IP QoS is enabled in Advanced Setup.

Upstream Status

High Priority(Rate:Kbps)

Rate	Sent	Dropped	Overlimits

Normal Priority(Rate:Kbps)

Rate	Sent	Dropped	Overlimits

Downstream Status

High Priority(Rate:Kbps)

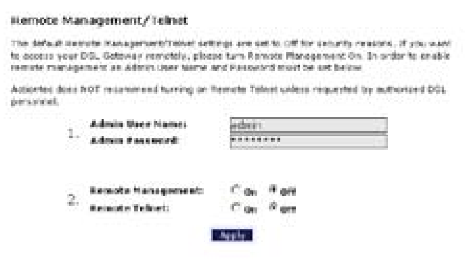
Rate	Sent	Dropped	Overlimits

Normal Priority(Rate:Kbps)

Rate	Sent	Dropped	Overlimits

Remote Management/Telnet

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



Remote Management/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

Remote Management

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

Telnet

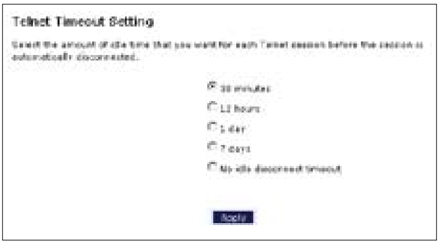
To access the Gateway via Telnet, activate Telnet by selecting the appropriate “On” radio button and writing down the WAN IP address of the Gateway (see “WAN IP Address”). On a computer outside the network running a Telnet program, enter the Gateway’s WAN IP address to access the Gateway.

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

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

Telnet Timeout Setting

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



Telnet Timeout Setting

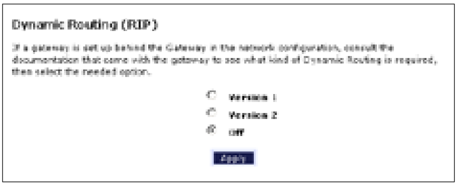
Select the amount of idle time that you want for each Telnet session before the session is automatically disconnected.

● 30 minutes
○ 12 hours
○ 1 day
○ 7 days
○ No idle disconnect timeout

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.

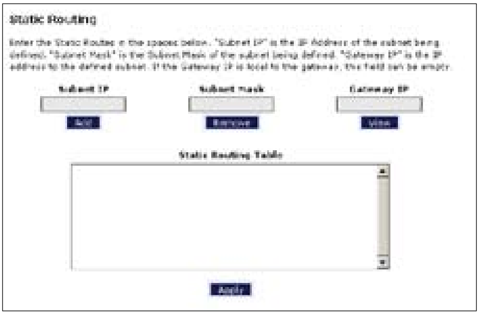
○ Version 1
○ Version 2
● Off

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

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

Static Routing

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



Static Routing

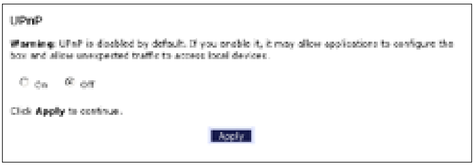
Enter the Static Routes in the spaces below. "Subnet IP" is the IP Address of the subnet being defined. "Subnet Mask" is the Subnet Mask of the subnet being defined. "Gateway IP" is the IP address to the defined subnet. If the Gateway IP is local to the gateway, this field can be empty.

Subnet IP
Subnet Mask
Gateway IP

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.

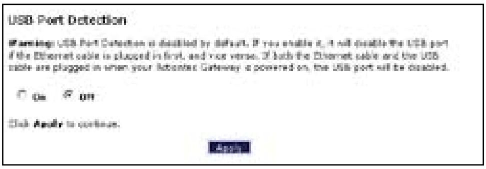
Universal Plug and Play is a zero-configuration networking protocol that allows hardware and software (such as Netmeeting) to operate more efficiently. If Netmeeting is not running properly, activate UPnP.

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

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

USB Port Detection

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



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.

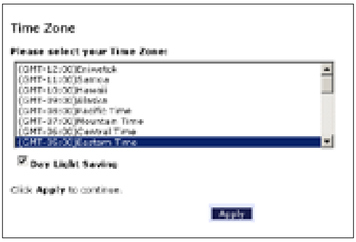
○ On ● Off

Click **Apply** to continue.

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

Time Zone

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



Time Zone

Please select your Time Zone:

(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
(GMT-05:00)Eastern Time

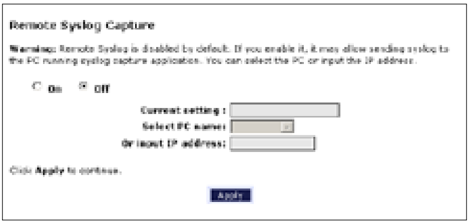
☑ **Day Light Saving**

Click **Apply** to continue.

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

Remote Syslog Capture

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



Remote Syslog Capture

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.

○ **On** ● **Off**

Current setting :
Select PC name:
Or input IP address:

Click **Apply** to continue.

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

This page left intentionally blank.

Configuring Security Settings 6

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

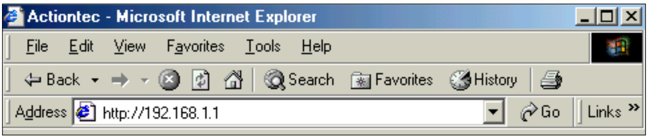
Accessing Wired Security Screens

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

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

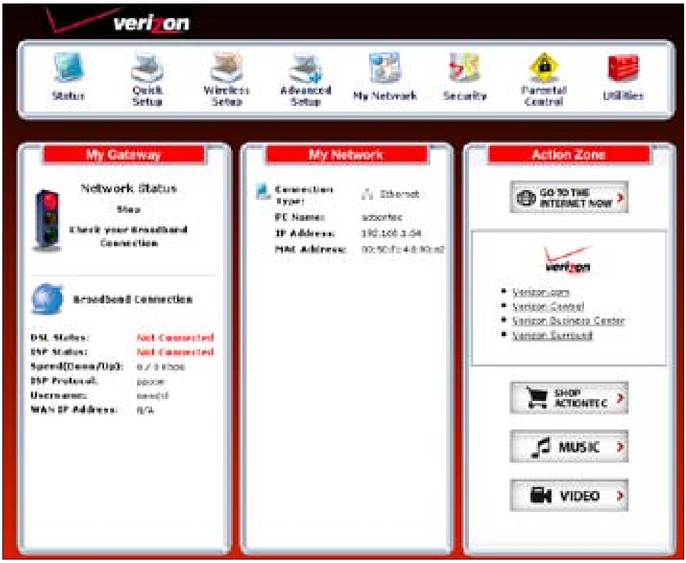
   `http://192.168.1.1`

   then press **Enter** on the keyboard.


Actiontec - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Go Links

Address http://192.168.1.1

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



Network Status

Stop

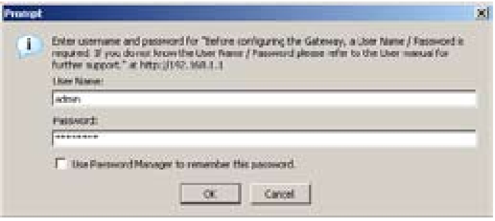
Check your Broadband Connection

Broadband Connection

DSL Status: Not Connected
ISP Status: Not Connected
Speed(Down/Up): 0 / 0 Kbps
ISP Protocol: pppoe
Username: [illegible]
WAN IP Address: N/A

Connection Type: Ethernet
PC Name: actiontec
IP Address: 192.168.1.64
MAC Address: [illegible]

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



Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1

User Name:

admin

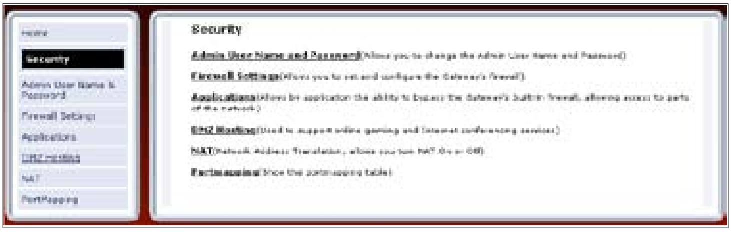
Password:

****

□ Use Password Manager to remember this password.

☞ ***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.



Security

Admin User Name and Password(Allows you to change the Admin User Name and Password)

Firewall Settings(Allows you to set and configure the Gateway's firewall)

Applications(Allows an application the ability to bypass the Gateway's built-in firewall, allowing access to parts of the network)

DMZ Hosting(Used to support online gaming and Internet conferencing services)

NAT(Network Address Translation, allows you to turn NAT On or Off)

Portmapping(Show the portmapping table)

Admin User Name and Password

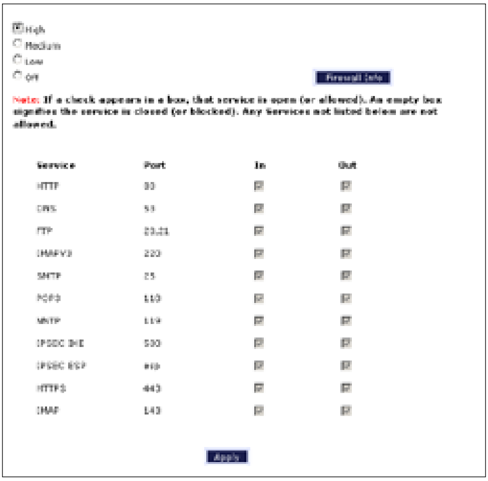
See “Changing the Password” on page 11.

Firewall

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

High

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



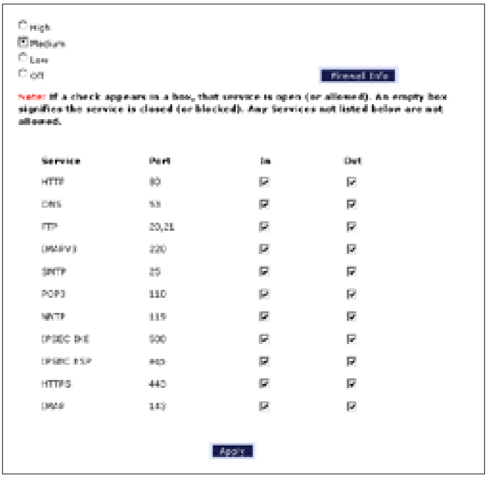
● High
○ Medium
○ Low
○ Off

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	☑	☑
DNS	53	☑	☑
FTP	20,21	☑	☑
IMAPV3	220	☑	☑
SMTP	25	☑	☑
POP3	110	☑	☑
NNTP	119	☑	☑
IPSEC IKE	500	☑	☑
IPSEC ESP	50	☑	☑
HTTPS	443	☑	☑
IMAP	143	☑	☑

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

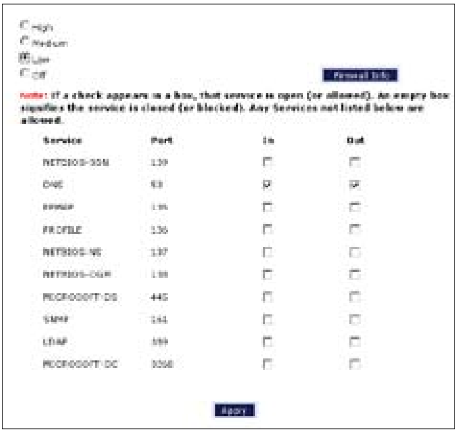
Note: If a check appears in a box, that service is open (or allowed). An empty box signifies the service is closed (or blocked). Any Services not listed below are not allowed.

Service	Port	In	Out
HTTP	80	☑	☑
DNS	53	☑	☑
FTP	20,21	☑	☑
IMAPV3	220	☑	☑
SMTP	25	☑	☑
POP3	110	☑	☑
NNTP	119	☑	☑
IPSEC IKE	500	☑	☑
IPSEC ESP	[illegible]	☑	☑
HTTPS	443	☑	☑
IMAP	143	☑	☑

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

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	□	□
DNS	53	☑	☑
EPMAP	135	□	□
PROFILE	136	□	□
NETBIOS-NS	137	□	□
NETBIOS-DGM	138	□	□
MICROSOFT-DS	445	□	□
SNMP	161	□	□
LDAP	389	□	□
MICROSOFT-GC	3268	□	□

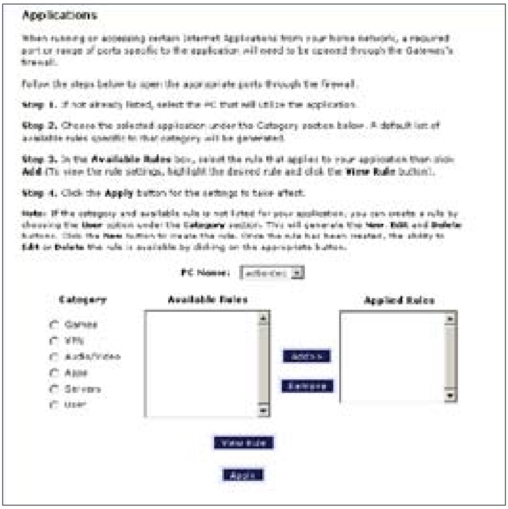
Off

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

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

Applications

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



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 effect.

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: [illegible]

This screen allows certain programs to bypass the Gateway's built-in firewall, allowing access to parts of the network (for hosting a Web or ftp server, for example). To use, select the name of a computer on the network from the "PC Name" drop-down list, then click **Add**. Next, select a "Category" by clicking the appropriate radio button. In the "Available Rules" list box, select a game, application, server, etc., then click **Add**>>. The selected item appears in the "Applied Rules" list box. Repeat for each item needed

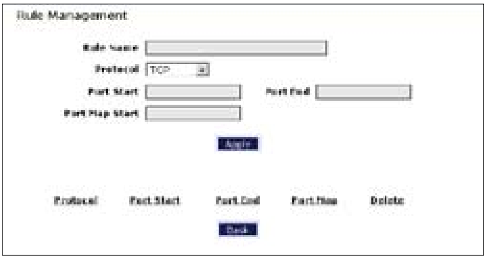
To remove an item from the Applied Rules list, highlight it, then click **Remove**.

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

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

Rule Management

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



Rule Management

Rule Name

Protocol TCP

Port Start

Port End

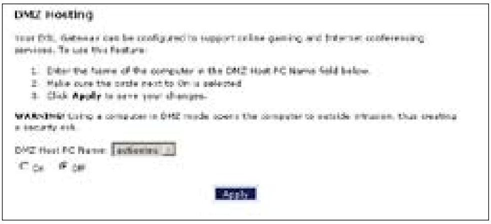
Port Map Start

Protocol	Port Start	Port End	Port Map	Delete

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

DMZ Hosting

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



DMZ Hosting

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: [illegible]

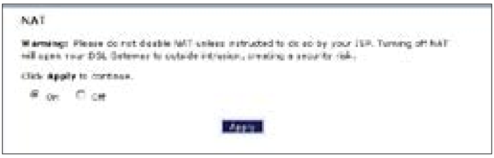
○ On ● Off

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

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

NAT (Network Address Translation)

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



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.

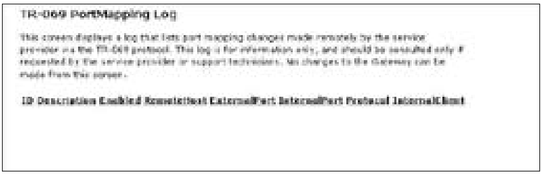
Click **Apply** to continue.

● On ○ Off

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

Port Mapping

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



TR-069 PortMapping Log

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

ID	Description	Enabled	RemoteHost	ExternalPort	InternalPort	Protocol	InternalClient

Configuring Parental Controls 7

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

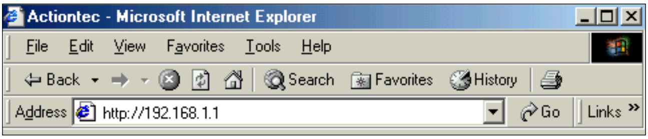
Accessing Parental Control Screens

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

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

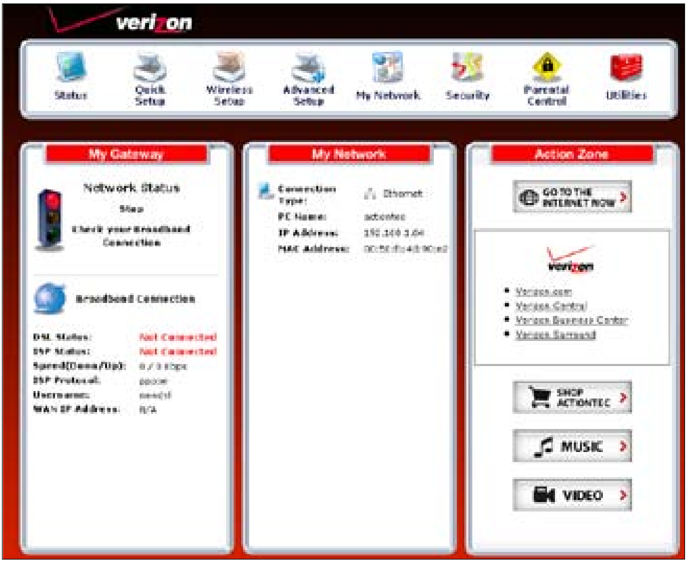
   `http://192.168.1.1`

   then press **Enter** on the keyboard.



Address http://192.168.1.1

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



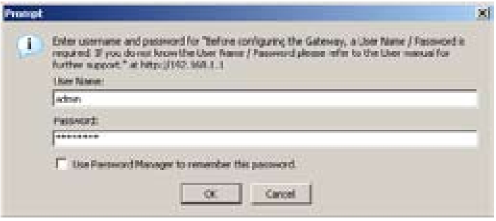
Network Status
Stop
Check your Broadband Connection

Broadband Connection

DSL Status: Not Connected
ISP Status: Not Connected
Speed(Down/Up): 0 / 0 Kbps
ISP Protocol: pppoe
Username: newuser
WAN IP Address: N/A

Connection Type: Ethernet
PC Name: actiontec
IP Address: 192.168.1.64
MAC Address: 00:50:f1:4f:90:e2

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



Prompt

Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1

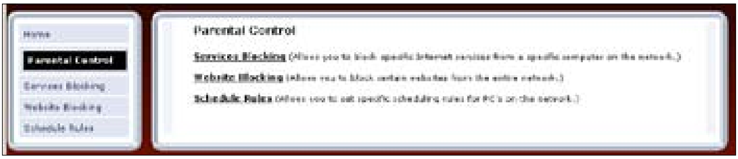
User Name: admin

Password: ********

□ Use Password Manager to remember this password

☞ *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.



Parental Control

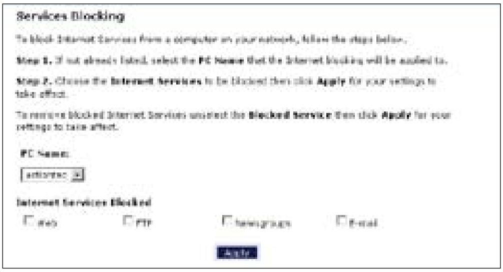
Services Blocking (Allows you to block specific Internet services from a specific computer on the network.)

Website Blocking (Allows you to block certain websites from the entire network.)

Schedule Rules (Allows you to set specific scheduling rules for PC's on the network.)

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 effect.

To remove blocked Internet Services unselect the **Blocked Service** then click **Apply** for your settings to take effect.

PC Name: actiontec

Internet Services Blocked

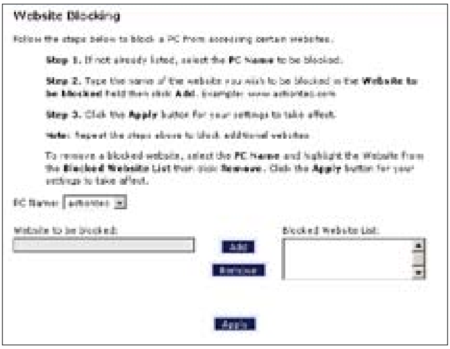
□ Web □ FTP □ Newsgroups □ E-mail

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 Gateway to block Web sites to any or all computers on the network. To block a Web site, select the computer name from the "PC Name" drop-down menu. Then, enter the address of the Web site to be blocked in the "Website" text box and click **Add**. The blocked Web site address will be displayed in the "Blocked Website List" text box, and will not be available to the selected computer on the network. To block the Web site from another computer on the network, repeat the process. To remove a blocked Web site, click on it in the "Blocked Website List," then click **Remove**. When finished, click **Apply**.



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 effect.

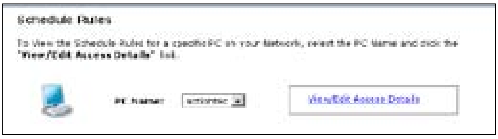
Note: Repeat the steps above to block additional websites.

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 effect.

PC Name: actiontec

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

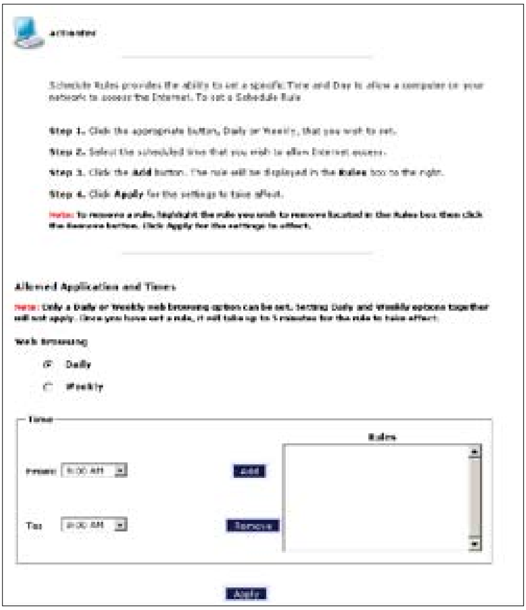
To View the Schedule Rules for a specific PC on your Network, select the PC Name and click the **"View/Edit Access Details"** link.

PC Name: actiontec

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 effect.

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 effect.**

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: 8:00 AM

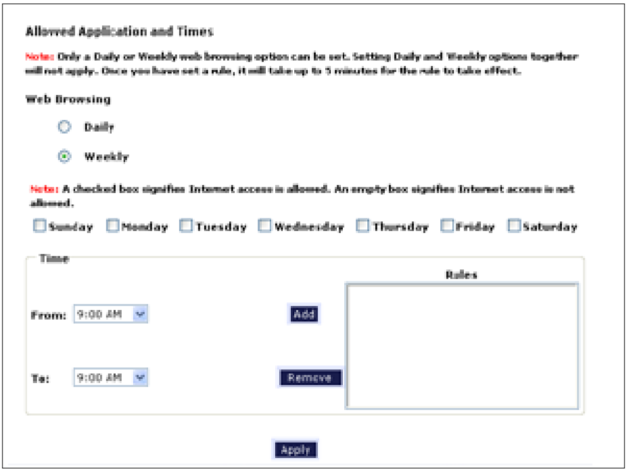
To: 8:00 AM

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.



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

Note: A checked box signifies Internet access is allowed. An empty box signifies Internet access is not allowed.

□ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Time

From: 9:00 AM

To: 9:00 AM

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

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

Removing a Schedule Rule

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

Configuring the Gateway's Utilities 8

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

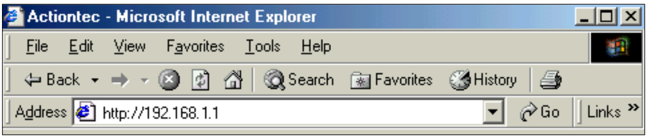
Accessing the Utilities Screens

To access the Utilities configuration screens, follow these instructions:

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

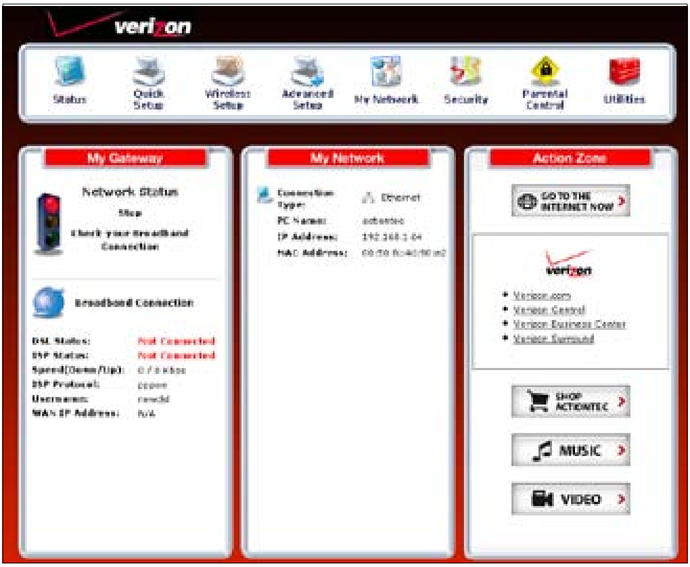
   ```
   http://192.168.1.1
   ```

   then press **Enter** on the keyboard.



Address: http://192.168.1.1

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



Network Status

Stop

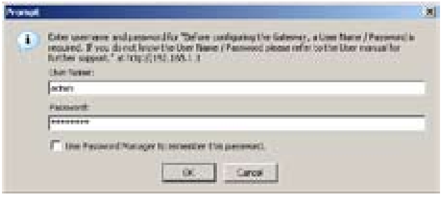
Check your Broadband Connection

Broadband Connection

DSL Status:	Not Connected
ISP Status:	Not Connected
Speed(Down/Up):	0 / 0 Kbps
ISP Protocol:	pppoe
Username:	[illegible]
WAN IP Address:	N/A

Connection Type:	Ethernet
PC Name:	actiontec
IP Address:	192.168.1.64
MAC Address:	[illegible]

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



Enter username and password for "Before configuring the Gateway, a User Name / Password is required. If you do not know the User Name / Password please refer to the User manual for further support." at http://192.168.1.1

User Name:

admin

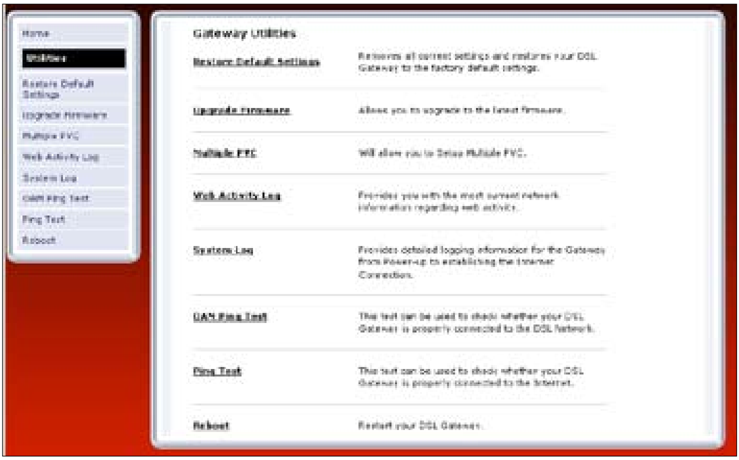
Password:

****

□ Use Password Manager to remember this password.

☞ ***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.



Gateway Utilities

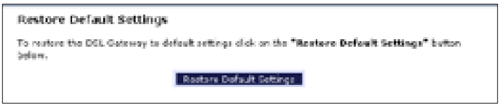
Restore Default Settings	Restores all current settings and restores your DSL Gateway to the factory default settings.
Upgrade Firmware	Allows you to upgrade to the latest firmware.
Multiple PVC	Will allow you to Setup Multiple PVC.
Web Activity Log	Provides you with the most current network information regarding web activity.
System Log	Provides detailed logging information for the Gateway from Power-up to establishing the Internet Connection.
OAM Ping Test	This test can be used to check whether your DSL Gateway is properly connected to the DSL Network.
Ping Test	This test can be used to check whether your DSL Gateway is properly connected to the Internet.
Reboot	Restart your DSL Gateway.

Restore Default Settings

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

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

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

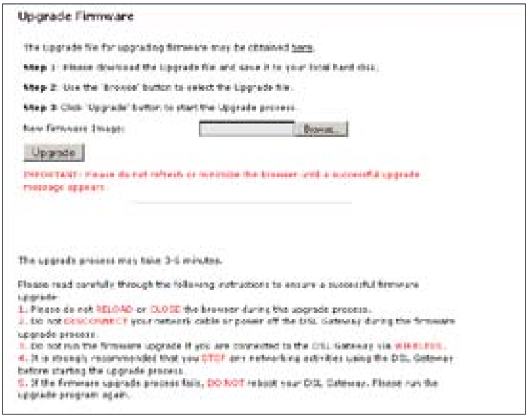


Restore Default Settings

To restore the DSL Gateway to default settings click on the **"Restore Default Settings"** button below.

Upgrade Firmware

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



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.

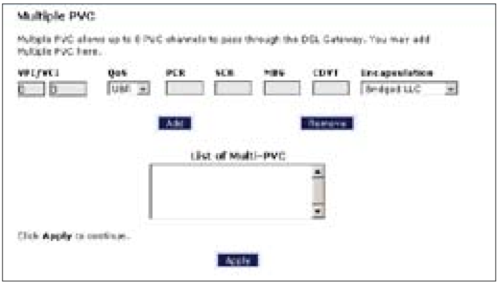
The upgrade process may take 3-5 minutes.

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

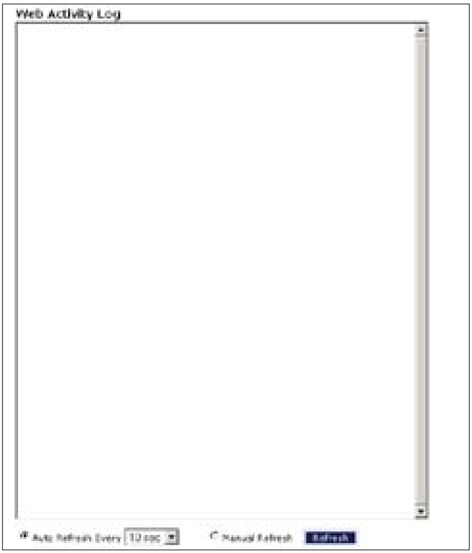
Multiple PVC allows up to 8 PVC channels to pass through the DSL Gateway. You may add Multiple PVC here.

VPI/VCI		QoS	PCR	SCR	MBS	CDVT	Encapsulation
0	0	UBR					Bridged LLC

Click **Apply** to continue.

Web Activity Log

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



Web Activity Log

● Auto Refresh Every 10 sec ○ Manual Refresh

Auto Refresh

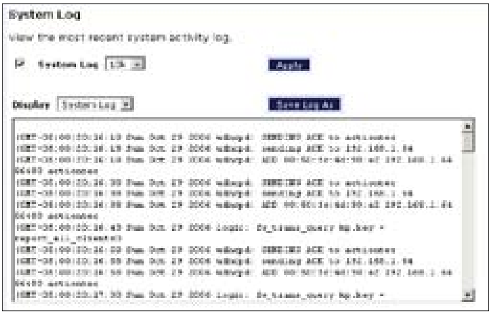
To set the Web Activity Log screen to automatically refresh at certain intervals, activate the circle next to "Auto Refresh Every" at the bottom of the Web Activity Log screen, then enter a time value (in seconds) in the text box, or click on the down arrow and select a time value from the menu that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

Manual Refresh

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

System Log

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



System Log

View the most recent system activity log.

☑ System Log 1k

Display System Log

```
[illegible] SENDING ACK to [illegible]
[illegible] sending ACK to 192.168.1.64
[illegible]
[illegible]
[illegible] SENDING ACK to [illegible]
[illegible] sending ACK to 192.168.1.64
[illegible]
[illegible]
[illegible] Logic: [illegible]
report_all_[illegible]
[illegible] SENDING ACK to [illegible]
[illegible] sending ACK to 192.168.1.64
[illegible]
[illegible]
[illegible] Logic: [illegible]
```

System Log (Size)

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

Display

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

Apply

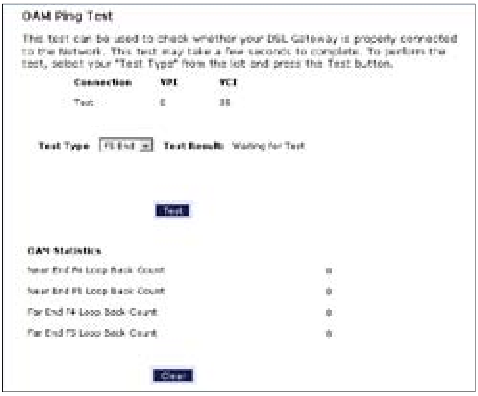
Pressing this button saves any changes to the System Log screen and causes the Save and Restart screen to appear.

Save Log As

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

OAM Ping Test

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



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

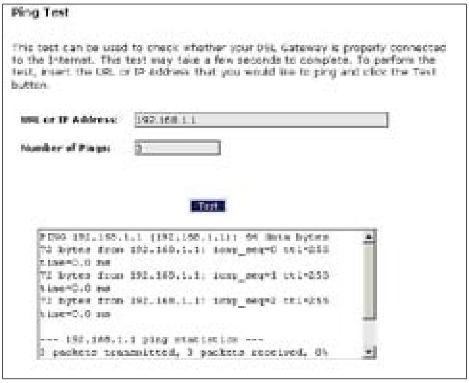
Test Type F5 End **Test Result:** Waiting for Test

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

Ping Test

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



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

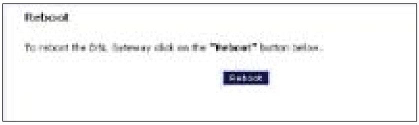
```
PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255
time=0.0 ms

--- 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 Gateway can be rebooted. To do this:

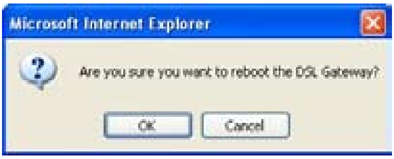
1. From the first Reboot screen, click **Reboot**.



Reboot

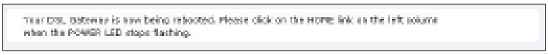
To reboot the DSL Gateway click on the "Reboot" button below.

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



Are you sure you want to reboot the DSL Gateway?

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



Your DSL Gateway is now being rebooted. Please click on the HOME link on the left column
when the POWER LED stops flashing.

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

Specifications

General

Model Number

GT704-WG (Wireless DSL Gateway)

Standards

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

Protocol

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

WAN

Full-rate ADSL Interface

LAN

10/100 RJ-45 switched port
USB port

Speed

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

Cabling Type

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

Wireless Operating Range

Indoors

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

Outdoors

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

Topology

Star (Ethernet)

LED Indicators

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

Environmental

Power

External, 12V DC, 600mA

Certifications

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

Operating Temperature

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

Regulatory Compliance Notices

Class B Equipment

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

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

Modifications

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

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

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

1. This device may not cause harmful interference;

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

Important Note

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

The tramsmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

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