Actiontec®

# Wireless VDSL Modem Router

**Model #: V1000H**

# User Manual

**Ver 1.0**

*Solutions for the Digital Life™*

# Table of Contents

# Introduction 1

Thank you for choosing the Actiontec Wireless VDSL Modem Router. With its powerful wireless N radio, gigabit Ethernet switch, and WAN port, as well as its dual-core processor and support for HPNA, the Modem Router will propel you to new speeds as you traverse the Internet. We are sure the Modem Router will provide you with years of hassle-free performance.

## Minimum System Requirements

- Active ADSL2+ service
- Computer with an 10 Mbps or 10/100/1000 Mbps Ethernet connection
- Microsoft Windows 2000, XP, Vista; Mac OS 7.1+, 8.0+, 9.0+, OS X+
- Internet Explorer (7.0 or higher), Firefox, Safari web browsers
- TCP/IP network protocol installed on each computer

## Features

- Gigabit Ethernet (WAN and LAN)
- VDSL 2 access technology (backward compatible to ASDL2+/ASDL2)
- HPNA coax support
- Optional Java Virtual Machine and Java Runtime software
- TR-069 support with remote management
- TR-064 local management

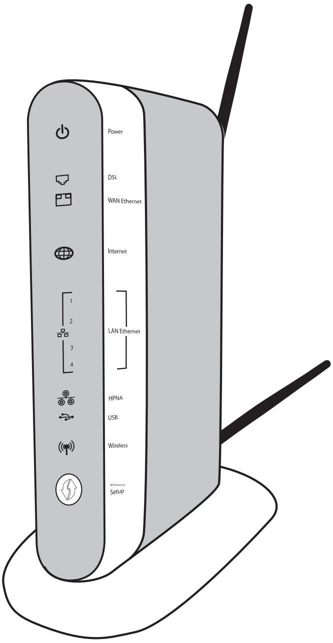
- 64-, 128-, and 256-bit WEP/WPA/WPA2 wireless LAN security
- IEEE 802.3 Ethernet standard compliance
- Four 10/100/1000 Base-T Ethernet ports (LAN)
- One 10/100/1000 Base-T Ethernet ports (WAN)
- DHCP server option
- MAC address cloning
- QoS support, including diffserv and random early detection
- PPPoE support
- External Radius support
- Web-based configuration support
- FTP firmware upgradeable
- Web download support
- 802.11b/g/n support
- WPS support
- Advanced firewall
- ALG

## Getting to Know the Modem Router

This section contains a quick description of the Modem Router's lights, ports, etc. The Modem Router 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 Modem Router features 11 LEDs: Power, DSL, Internet, WAN Ethernet, Internet, Ethernet (4), HPNA, USB, Wireless and WPS Push Button.



### *Power*

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

### *DSL*

The DSL LED illuminates when the Modem Router is connected to an xDSL line. If the DSL LED is flashing, the Modem Router is in training for DSL service.

### *WAN Ethernet*

When the WAN Ethernet LED glows steadily, the Modem Router is connected to an Ethernet WAN. When it flashes, it signifies that data traffic is traveling across the connection.

### *Internet*

When the Internet LED glows steadily, the Modem Router is connected to the DSL provider. When it flashes, data traffic is passing across the Modem Router.

### *LAN Ethernet*

The LAN Ethernet LEDs illuminate when the Modem Router is connected to another device via one of its LAN Ethernet ports. When one of the LAN Ethernet LEDs flashes, data traffic is passing across the corresponding connection.

### *HPNA*

The HPNA LED illuminates when the Modem Router is connected to another device via its HPNA port. When it flashes, data traffic is passing across the connection.

### *USB*

The USB LED illuminates when a USB device is connected via the Modem Router's USB port. This port is not currently operational, but may be enabled in a future firmware update.

### *Wireless*

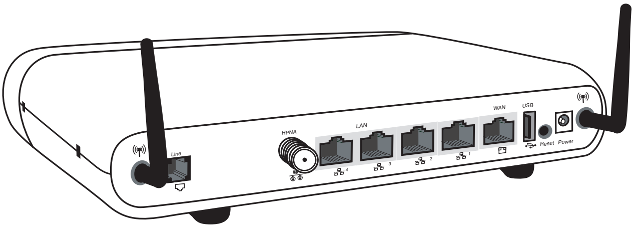
The Wireless LED illuminates when the Modem Router is connected wirelessly, assuming the Modem Router's Wireless feature is turned on.

### *WPS Button*

The WPS button activates WPS (WiFi Protected Setup) on the Modem Router. To use WPS, press the WPS button on the Modem Router, then, within two minutes, press the WPS button on a device you wish to connect to the Modem Router's wireless network. The device will automatically join the Modem Router's wireless network. Repeat for other wireless devices.

## Rear Panel

The rear panel of the Modem Router features 8 ports (Line, HPNA, LAN Ethernet, WAN Ethernet, USB, and Power), as well as a Reset switches.



### *Line Port*

The Line port is used to connect the Modem Router to a telephone line connection.

### *HPNA Port*

The HPNA port is used to connect the Modem Router to an HPNA connection via coaxial cable.

### *LAN Ethernet Ports (4)*

The LAN Ethernet ports are used to connect computers to the Modem Router via Ethernet cable. The Ethernet ports are 10/100/1000 Mbps auto-sensing ports, and either a straight-through or crossover Ethernet cable can be used when connecting to the ports.

### *WAN Ethernet Port*

The WAN Ethernet port is used to connect the Modem Router to a WAN via an Ethernet cable.

### *USB Port*

The USB port is used to connect the Modem Router to a USB device. This port is not yet active; it may be activated in a future firmware update.

### *Reset Switch*

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

### *Power Port*

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

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

# Getting Started With the Modem Router

# 2

This chapter gives an overview of how to get started with the Modem Router, including describing the Modem Router's Home screen and setting up the Modem Router through the Quick Start screens.

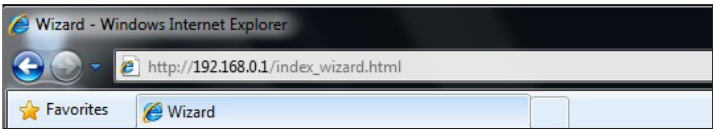
## Accessing the Home Screen

To access the Wireless screens:

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

   ```
   http://192.168.0.1
   ```

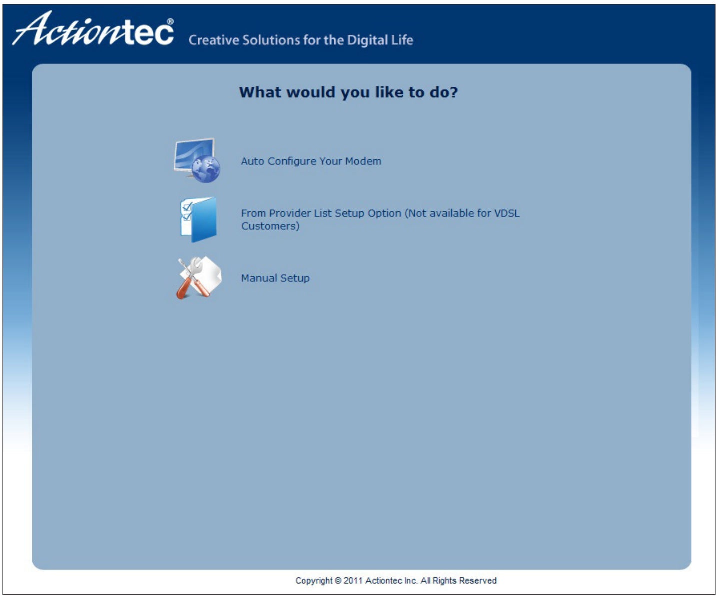
   then press **Enter** on the keyboard.



Wizard - Windows Internet Explorer

http://192.168.0.1/index_wizard.html

2. The Modem Router’s host screen appears. Click **Manual Setup**.



What would you like to do?

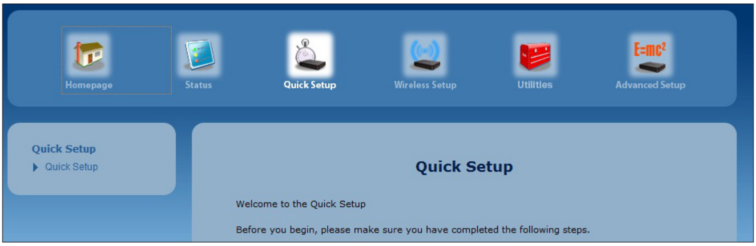
Auto Configure Your Modem

From Provider List Setup Option (Not available for VDSL Customers)

Manual Setup

Copyright © 2011 Actiontec Inc. All Rights Reserved

3. The Quick Setup screen appears, with a row of large icons across the top of the screen. Click **Homepage**.

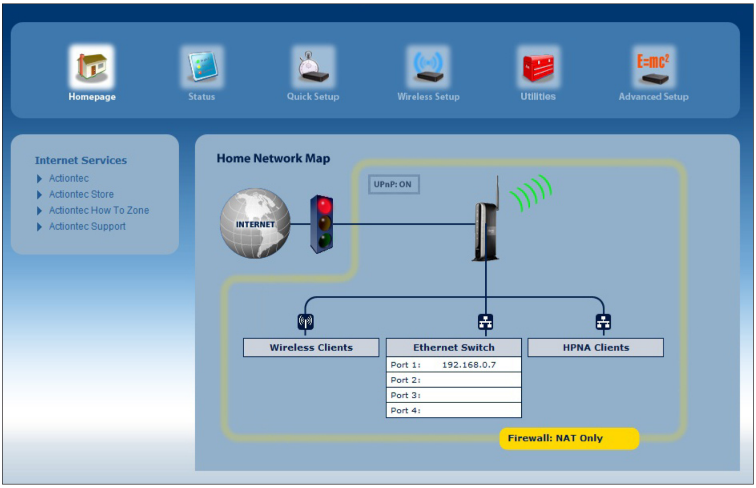


Quick Setup

Welcome to the Quick Setup

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

**4.** The Modem Router's Home screen appears.



| Ethernet Switch | |
|---|---|
| Port 1: | 192.168.0.7 |
| Port 2: | |
| Port 3: | |
| Port 4: | |

## Icon Bar

At the top of the Home screen is the Icon Bar. Here, you can quickly access the other four main sections of the Modem Router's firmware by clicking on the appropriate icon: Status; Quick Setup, Wireless Setup; Utilities; and Advanced Setup. Clicking the Home icon in any other firmware screen generates the Home screen.

## Internet Services

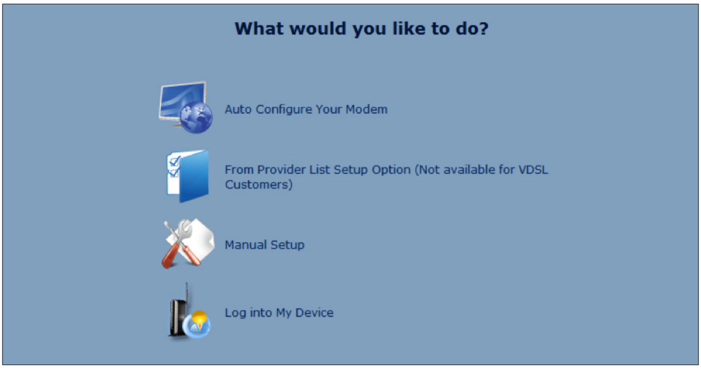
On the right side of the screen is the Internet Services menu, where there is a series of four Actiontec links (Actiontec, Actiontec Store, Actiontec How To Zone, and Actiontec Support) that can help you get the most out of the Modem Router.

## Home Network Map

The Home Network map on the Home screen is a graphical representation of the Modem Router's network, including how it is connected to the ISP, all devices connected to it through its networks, and the state of the firewall.

## Host Screen

The Modem Router's Host screen is the first one you will see when connecting to the Modem Router. It contains four options: Auto Configure Your Modem, From Provider List Setup Option, Manual Setup, and Log into My Device.



What would you like to do?

Auto Configure Your Modem

From Provider List Setup Option (Not available for VDSL Customers)

Manual Setup

Log into My Device

### Auto Configure Your Modem

Selecting this option generates a procedure wizard that guides you through automatically connecting the Modem Router with your ISP.

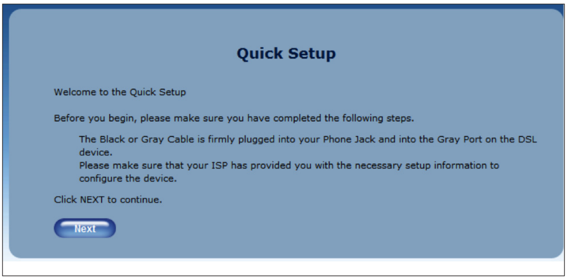
### From Provider List Setup Option

Selecting this option generates a procedure wizard that guides you through connecting the Modem Router with an ISP that appears on the list that appears. Only ADSL customers can access this option.

## Manual Setup

Selecting this option takes you to the Quick Setup screen. To perform a quick setup:

1. In the first Quick Setup screen, follow the onscreen instructions, then click **Next**.



Quick Setup

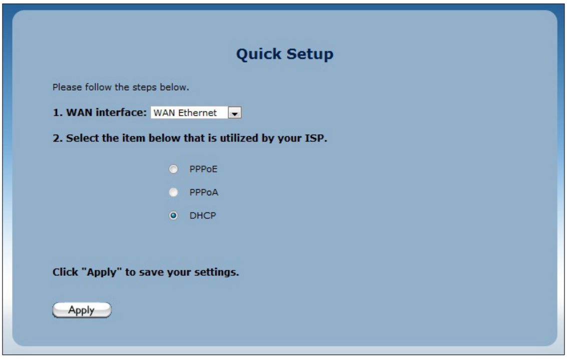
Welcome to the Quick Setup

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

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

Click NEXT to continue.

2. Another Quick Setup screen appears. Select the WAN interface you are using from the WAN Interface drop-down list.



Quick Setup

Please follow the steps below.

**1. WAN interface:** WAN Ethernet

**2. Select the item below that is utilized by your ISP.**

○ PPPoE
○ PPPoA
● DHCP

**Click "Apply" to save your settings.**

3. Select the protocol used by your ISP by clicking in the appropriate radio button. If PPPoE or PPPoA was selected, enter the PPP username and password in the text boxes that appear.

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

## Log Into My Device

Selecting this option generates a screen asking for your username and password. After entering them correctly, the Home screen appears, where you can access the Modem Router's graphical user interface.

# Configuring Wireless Settings

# 3

This chapter explains the options provided in the Wireless section of the Modem Router's firmware, including setting up wireless security and WPS.

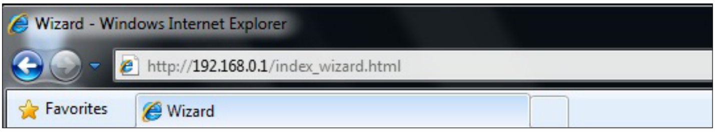
## Accessing Wireless Settings

To access the Wireless screens:

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

   ```
       http://192.168.0.1
   ```

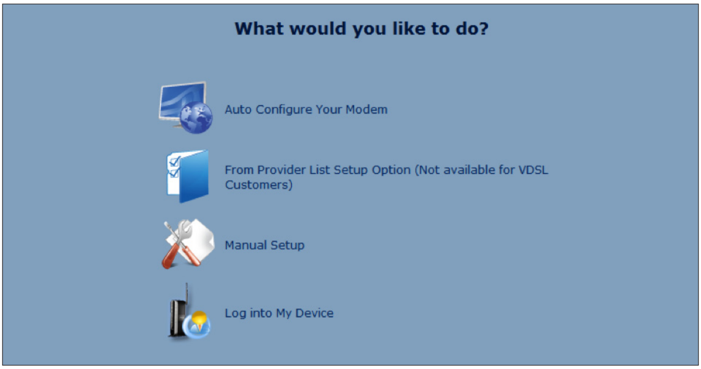
   then press **Enter** on the keyboard.



Wizard - Windows Internet Explorer

http://192.168.0.1/index_wizard.html

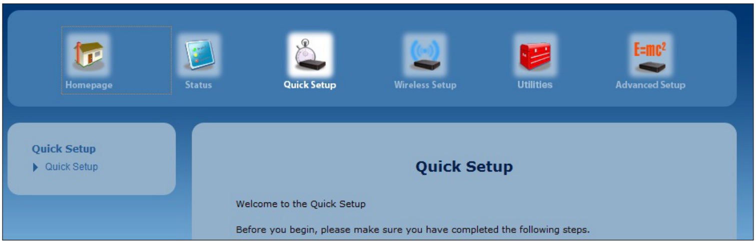
2. The Modem Router's host screen appears. Click **Manual Setup**.



What would you like to do?

Auto Configure Your Modem
From Provider List Setup Option (Not available for VDSL Customers)
Manual Setup
Log into My Device

3. The Quick Setup screen appears, with a row of large icons across the top of the screen. Click **Wireless Setup**.

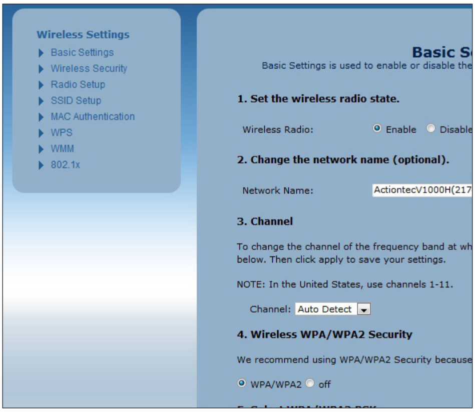


Quick Setup

Welcome to the Quick Setup

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

**4.** The Wireless Setup screen appears, with list of options on the left side of the screen.



Basic S

Basic Settings is used to enable or disable the

1. Set the wireless radio state.

Wireless Radio: ● Enable ○ Disable

2. Change the network name (optional).

Network Name: ActiontecV1000H(217

3. Channel

To change the channel of the frequency band at wh below. Then click apply to save your settings.

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

Channel: Auto Detect

4. Wireless WPA/WPA2 Security

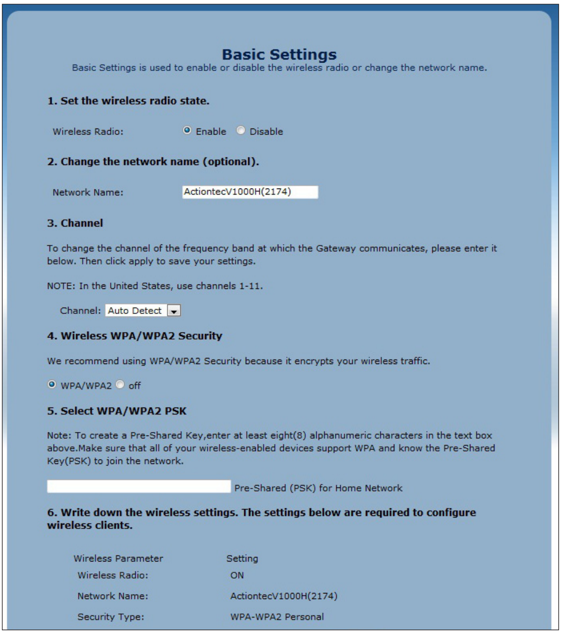
We recommend using WPA/WPA2 Security because

● WPA/WPA2 ○ off

The rest of this chapter explains the options found in the menu on the left side of every wireless settings screen.

## Basic Settings

Click **Basic Settings** from any Wireless screen to generate the Basic Settings screen. This screen displays step-by-step instructions to set up a secure wireless network with the Modem Router.



### Basic Settings

Basic Settings is used to enable or disable the wireless radio or change the network name.

**1. Set the wireless radio state.**

Wireless Radio: ● Enable ○ Disable

**2. Change the network name (optional).**

Network Name: ActiontecV1000H(2174)

**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: Auto Detect

**4. Wireless WPA/WPA2 Security**

We recommend using WPA/WPA2 Security because it encrypts your wireless traffic.

● WPA/WPA2 ○ off

**5. Select WPA/WPA2 PSK**

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 Pre-Shared Key(PSK) to join the network.

Pre-Shared (PSK) for Home Network

**6. Write down the wireless settings. The settings below are required to configure wireless clients.**

| Wireless Parameter | Setting |
|---|---|
| Wireless Radio: | ON |
| Network Name: | ActiontecV1000H(2174) |
| Security Type: | WPA-WPA2 Personal |

To configure the basic wireless settings of the Modem Router:

1. Enable the wireless radio of the Modem Router by clicking in the Enable radio button to activate it.

2. If needed, change the name of the Modem Router’s wireless network by entering a new one in the Network Name text box. Otherwise, you can use the one that is already entered the the text box. You should write this name down, so that you can refer back to it later, when connecting other wireless devices (such as smartphones or laptop computers) to the Modem Router’s wireless network.

**3.** If needed, change the channel on which the Modem Router's wireless network will operate once it is activated. In the U.S., wireless networks can operation on channels 1 through 11. If your network is not working properly because of outside interference, you can change it to another channel here. Also, if you select the Auto Detect option, the Modem Router will automatically select a channel.

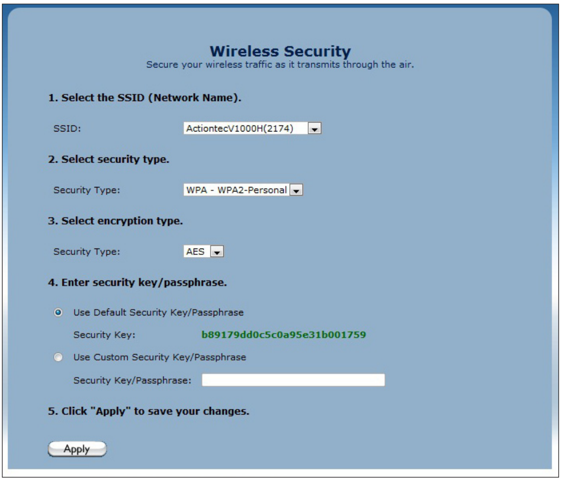
**4.** Activate wireless security by clicking in the radio button next to WPA/WPA2. This type of wireless security is the recommended choice, and will secure the Modem Router's wireless network against outside intruders who try to gain access to the wireless network without your knowledge.

**5.** Enter a pre-shared key (PSK) in the text box next to Pre-Shared Key (PSK) for Home Network. A PSK is the password that other wireless devices will need to join the Modem Router's wireless network. It must be at least 8 characters long, and is made up of numbers and letter. Once you create a PSK, write it down for future reference.

**6.** Click **Apply**. The Modem Router's wireless network is now on and other wireless devices can join it.

## Wireless Security

Click **Wireless Security** from any Wireless screen to generate the Wireless Security screen. This screen lets you make other changes to the security of the Modem Router's wireless network.



Wireless Security

Secure your wireless traffic as it transmits through the air.

1. Select the SSID (Network Name).

SSID: ActiontecV1000H(2174)

2. Select security type.

Security Type: WPA - WPA2-Personal

3. Select encryption type.

Security Type: AES

4. Enter security key/passphrase.

● Use Default Security Key/Passphrase

Security Key: b89179dd0c5c0a95e31b001759

○ Use Custom Security Key/Passphrase

Security Key/Passphrase:

5. Click "Apply" to save your changes.

To change the security settings of the Modem Router's wireless network:

1. If needed, change the name of the Modem Router's wireless network by selecting a new one from the Network Name drop-down list. Otherwise, use the one already selected. You should write this name down, so that you can refer back to it later, when connecting other wireless devices (such as smartphones or laptop computers) to the Modem Router's wireless network.

2. Select a security type from the Security Type drop-down list below step 2. For all types of except WEP, continue with this procedure. If you select WEP, see the following section, WEP Wireless Security.

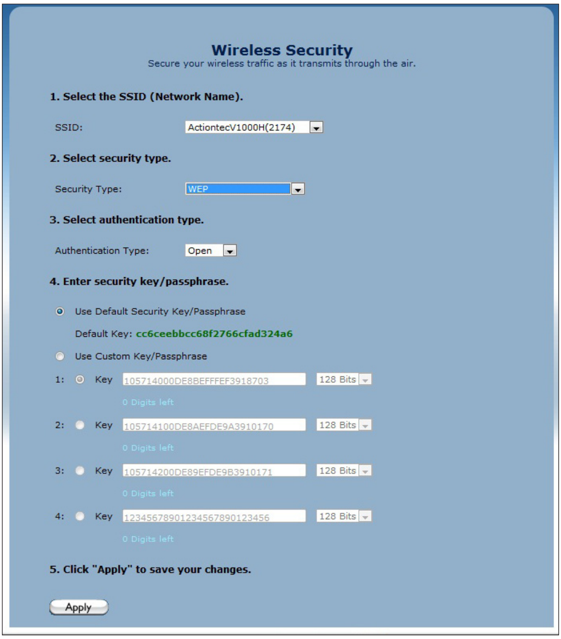
3. Select an encryption type from the Security Type drop-down list below step 3. TKIP should be used for networks with older equipment, while AES is a more secure encryption for newer network equipment. If using 802.11n wireless networking, your must select AES.

4. Under step 4 in the Wireless Modem Router screen, select the radio button next to Use Default Security Key/Passphrase. The Modem Router automatically generates a strong security key that is difficult to crack. Be sure to write down the secuirty key, which appears in green text. You will need it to connect other wireless devices to the Modem Router's wireless network.

5. Click **Apply**. The Modem Router's wireless network is now functional and using the security type you selected.

## WEP Wireless Security

If you selected WEP in step 2 of the previous procedure, the following screen appears:



Wireless Security

Secure your wireless traffic as it transmits through the air.

1. Select the SSID (Network Name).

SSID: ActiontecV1000H(2174)

2. Select security type.

Security Type: WEP

3. Select authentication type.

Authentication Type: Open

4. Enter security key/passphrase.

● Use Default Security Key/Passphrase

Default Key: cc6ceebbcc68f2766cfad324a6

○ Use Custom Key/Passphrase

1: ● Key 105714000DE8BEFFFEF3918703 128 Bits
0 Digits left

2: ○ Key 105714100DE8AEFDE9A3910170 128 Bits
0 Digits left

3: ○ Key 105714200DE89EFDE9B3910171 128 Bits
0 Digits left

4: ○ Key 12345678901234567890123456 128 Bits
0 Digits left

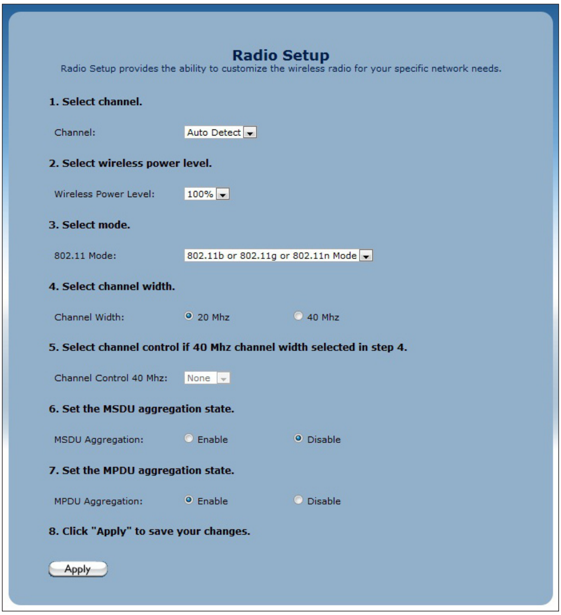
5. Click "Apply" to save your changes.

To change the security settings of the Modem Router’s wireless network to WEP:

1. Select an encryption type from the Security Type drop-down list below step 3.
2. Under step 4, select the radio button next to Use Default Security Key/ Passphrase. The Modem Router automatically generates a strong security key that is difficult to crack. Be sure to write down the secuirty key, which appears in green text. You will need it to connect other wireless devices to the Modem Router’s wireless network.
3. Click **Apply**. The Modem Router’s wireless network is now functional and using WEP security.

## Radio Setup

Click **Radio Security** from any Wireless screen to generate the Radio Secuirity screen. This screen lets you make changes to the radio signal of the Modem Router’s wireless network.



**Radio Setup**

Radio Setup provides the ability to customize the wireless radio for your specific network needs.

**1. Select channel.**

Channel: Auto Detect

**2. Select wireless power level.**

Wireless Power Level: 100%

**3. Select mode.**

802.11 Mode: 802.11b or 802.11g or 802.11n Mode

**4. Select channel width.**

Channel Width: ● 20 Mhz ○ 40 Mhz

**5. Select channel control if 40 Mhz channel width selected in step 4.**

Channel Control 40 Mhz: None

**6. Set the MSDU aggregation state.**

MSDU Aggregation: ○ Enable ● Disable

**7. Set the MPDU aggregation state.**

MPDU Aggregation: ● Enable ○ Disable

**8. Click "Apply" to save your changes.**

To change the radio settings of the Modem Router's wireless network (if needed; you do not need to make all the changes in this procedure, as they can be changed independently of each other):

1. Select the radio's channel from the Channel drop-down list.

2. Select the level of the wireless radio's power level.

3. Select the wireless network's mode. Options include whatever mix of 802.11b, g, and n modes you prefer (except b/n only).

4. Select the channel width by clicking in either the 20 Mhz or 40 Mhz radio buttons.

5. If 40 Mhz was selected in step 5, select the channel's width (**Upper** or **Lower**).

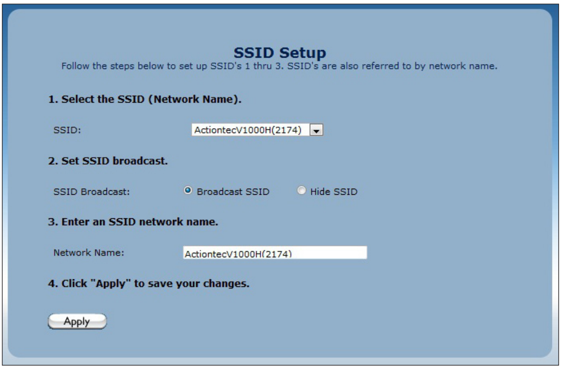
6. Set the MSDU (MAC-Layer Service Data Unit) aggregation state by clicking in the Enable or Disable radio buttons below step 6. MDSU should only be enabled/disabled by an experienced network technician.

7. Set the MPDU (MAC-Layer Protocol Data Unit) aggregation state by clicking in the Enable or Disable radio buttons below step 7. MPDU should only be enabled/disabled by an experienced network technician.

8. Click **Apply**.

## SSID Setup

Click **SSID Setup** from any Wireless screen to generate the SSID Setup screen. This screen lets you make changes to the name of the Modem Router's wireless network name, as well as letting you turn off the wireless network name broadcast option.



SSID Setup

Follow the steps below to set up SSID's 1 thru 3. SSID's are also referred to by network name.

1. Select the SSID (Network Name).

SSID: ActiontecV1000H(2174)

2. Set SSID broadcast.

SSID Broadcast: ● Broadcast SSID ○ Hide SSID

3. Enter an SSID network name.

Network Name: ActiontecV1000H(2174)

4. Click "Apply" to save your changes.

To change the network name settings of the Modem Router's wireless network (if needed; you do not need to make all the changes in this procedure; they can be changed independently of each other):

1. If needed, change the name of the Modem Router's wireless network by selecting a new one from the SSID drop-down list. Otherwise, use the one already selected. You should write this name down, so that you can refer back to it later, when connecting other wireless devices (such as smartphones or laptop computers) to the Modem Router's wireless network.

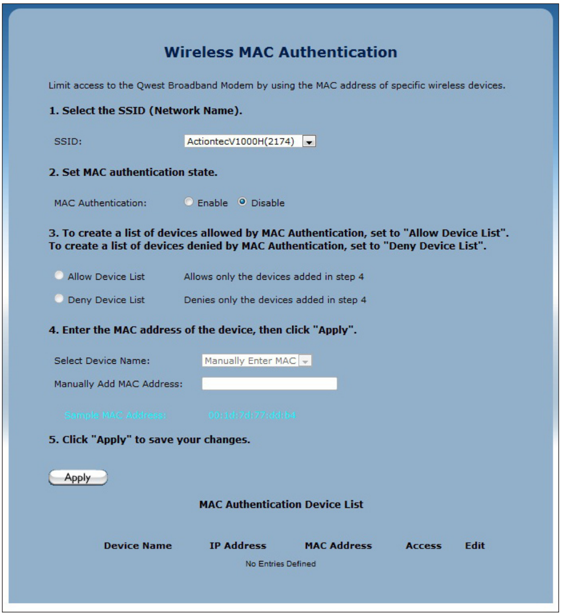
2. Click the Broadcast SSID radio button to activate SSID broadcasting, which allows any computer searching for available wireless networks to detect this network (however, if this network is protected with some form of wireless security, they will not be able to join the network unless they know the security password). Clicking "Hide SSID" turns off SSID broadcasting.

3. If you want to have a custom name for your wireless network, enter it in the Network Name text box under step 3.

4. Click **Apply**.

## Wireless MAC Authentication

Click **Wireless MAC Authentication** from any Wireless screen to generate the Wireless MAC Authentication screen. This screen lets you allow or deny access to the Modem Router's wireless network for any wireless devices (such as laptop computers) by the devices' MAC address. A MAC address is a unique code that identifies every wireless-capable device (printers, computers, hard drives, etc.).



**Wireless MAC Authentication**

Limit access to the Qwest Broadband Modem by using the MAC address of specific wireless devices.

**1. Select the SSID (Network Name).**

SSID: ActiontecV1000H(2174)

**2. Set MAC authentication state.**

MAC Authentication: ○ Enable ● Disable

**3. To create a list of devices allowed by MAC Authentication, set to "Allow Device List". To create a list of devices denied by MAC Authentication, set to "Deny Device List".**

○ Allow Device List — Allows only the devices added in step 4

○ Deny Device List — Denies only the devices added in step 4

**4. Enter the MAC address of the device, then click "Apply".**

Select Device Name: Manually Enter MAC

Manually Add MAC Address:

Sample MAC Address: 00:1d:7d:77:dd:b4

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

**MAC Authentication Device List**

| Device Name | IP Address | MAC Address | Access | Edit |
|---|---|---|---|---|
| No Entries Defined | | | | |

To set up authentication on the Modem Router's wireless network using MAC addresses:

1. Select a wireless network name from the SSID drop-down list.
2. Turn on MAC authentication by clicking in the Enable radio button.
3. Select a filtering method. Activating the radio button next to Allow Device List creates a list of wireless devices that will be allowed to join the wireless network–all other devices will not be able to join. Activating the radio button next to Deny Device List creates a list of wireless devices that cannot join the wireless network–all other devices will be able to join.

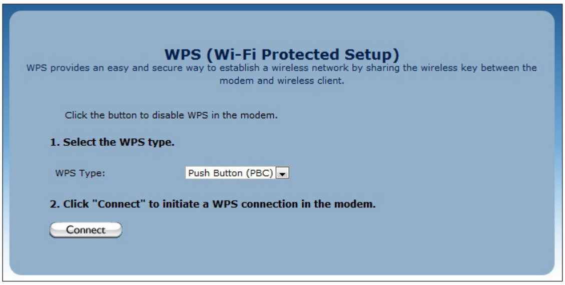
4. Begin creating your list by selecting a wireless device that appears on the Select Device Name drop-down list. You can also enter a devices MAC address in the Manually Add MAC Address text box.

5. Click **Apply**. The device will appear in the MAC Authentication Device List at the bottom of the screen.

6. Repeat steps 4 and 5 to add more wireless devices.

## WPS

Click **WPS** in any Wireless screen to generate the WPS (Wi-Fi Protected Setup) screen.WPS provides a simple method of setting up a wireless network by automatically sharing the network key between the Modem Router and other wireless devices.



WPS (Wi-Fi Protected Setup)

WPS provides an easy and secure way to establish a wireless network by sharing the wireless key between the modem and wireless client.

Click the button to disable WPS in the modem.

1. Select the WPS type.

WPS Type: Push Button (PBC)

2. Click "Connect" to initiate a WPS connection in the modem.

There are three ways to set up WPS on the Modem Router: Push Button (PBC), AP PIN, and End Device PIN.

### Push Button (PBC)

1. Select Push Button (PBC) from the drop-down list.

2. Click **Connect**.

3. Press the PBC-compatible button on another wireless device within two minutes to have that device join the wireless network.

### AP Pin

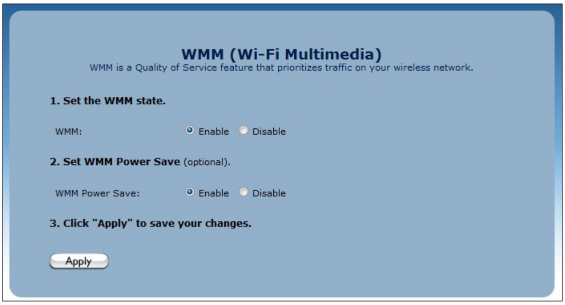
1. Select AP PIN from the drop-down list.
2. A PIN is created on the Modem Router. Write it down.
3. Enter the PIN on another wireless device's WPS AP PIN configuration to have that device join the wireless network.

### End Device PIN

1. Select End Device PIN from the drop-down list.
2. Enter the end device's PIN in the appropriate text box.
3. Click **Connect**. The Modem Router joins the existing wireless network.

## WMM

Click **WMM** in any Wireless screen to generate the WMM (Wi-Fi Multimedia) screen. Wi-fi Multimedia provides a way to control the bandwidth of certain types of data, prioritizing one type over another to ease congestion.



WMM (Wi-Fi Multimedia)

WMM is a Quality of Service feature that prioritizes traffic on your wireless network.

1. Set the WMM state.

WMM: ● Enable ○ Disable

2. Set WMM Power Save (optional).

WMM Power Save: ● Enable ○ Disable

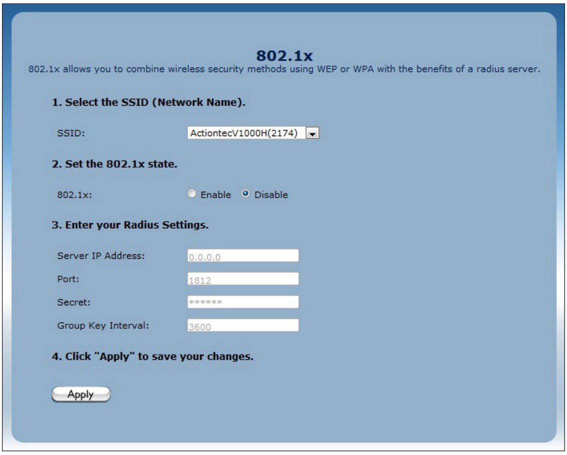
3. Click "Apply" to save your changes.

To set up WMM:

1. Click in the radio button next to Enable under step 1.
2. If applicable, click in the radio button next to Enable under step 2.
3. Click **Apply**.

## 802.1x

802.1x  is a robust security protocol that uses port control with dynamically changing encryption keys automatically updated over the network. 802.1x uses a RADIUS (Remote Authentication Dial-in Service) server for authentication purposes. This server must be physically connected to the Modem Router. Also, the user must enable the RADIUS client embedded in the Modem Router.



802.1x

802.1x allows you to combine wireless security methods using WEP or WPA with the benefits of a radius server.

1. Select the SSID (Network Name).

SSID: ActiontecV1000H(2174)

2. Set the 802.1x state.

802.1x: ○ Enable ● Disable

3. Enter your Radius Settings.

Server IP Address: 0.0.0.0

Port: 1812

Secret: ******

Group Key Interval: 3600

4. Click "Apply" to save your changes.

To set up 802.1x security:

1. Select the Modem Router's wireless network name from the SSID drop-down list.
2. Click in the radio button next to Enable under step 2.
3. Enter the RADIUS server's port number in the Radius Port text box.
4. Enter the RADIUS server's shared secret in the Radius Key text box.
5. Enter the group key interval in the Group Key Interval text box.
6. Click **Apply** to save your changes.

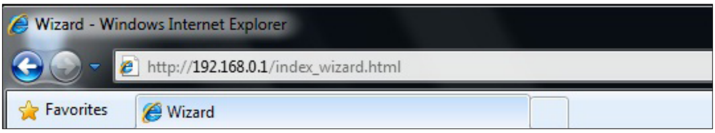
# Configuring the Modem Router's Utilities 4

This chapter will explain the options provided in the Utilities section of the Modem Router's firmware, including services blocking, restoring the Modem Router to factory default settings, and performing a ping test.

## Accessing Utilities

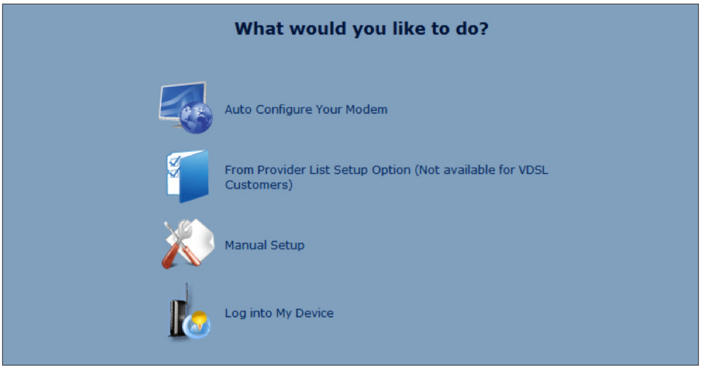
To access the Utilities screens:

1. Open a Web browser. In the Address text box, type:
   **`http://192.168.0.1`**
   then press **Enter** on the keyboard.



http://192.168.0.1/index_wizard.html

2. The Modem Router's host screen appears. Click **Manual Setup**.



What would you like to do?

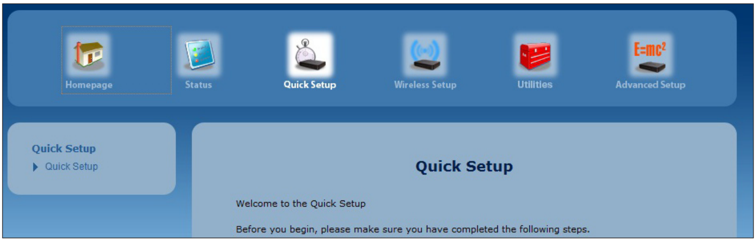
Auto Configure Your Modem

From Provider List Setup Option (Not available for VDSL Customers)

Manual Setup

Log into My Device

3. The Quick Setup screen appears, with a row of large icons across the top of the screen. Click **Utilities**.



Quick Setup

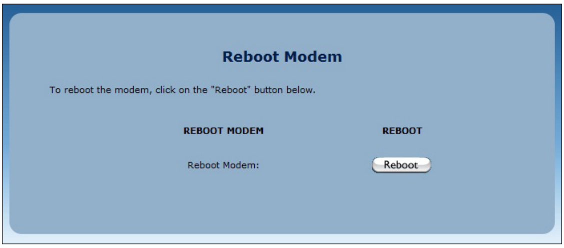
Welcome to the Quick Setup

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

## Rebooting the Modem Router

To reboot the Modem Router:

1. Click **Reboot** from the menu on the left side of any Utilities screen. The Reboot Modem screen appears.



Reboot Modem

To reboot the modem, click on the "Reboot" button below.

| REBOOT MODEM | REBOOT |
|---|---|
| Reboot Modem: | Reboot |

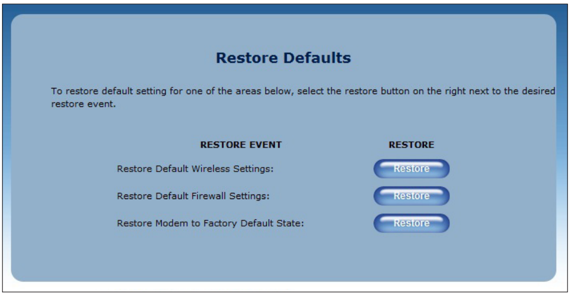
2. Click **Reboot** to reboot the Modem Router. This may take up to one minute.

To reenter the Modem Router's firmware after restarting the Modem Router, click the web browser's Refresh button.

## Restoring Factory Default Settings

If the Modem Router's factory default settings need to be restored (to build a new network from the beginning, for example), use the following procedure:

1. Click **Restore Defaults** in any Utilities screen. The "Restore Defaults" screen appears.



Restore Defaults

To restore default setting for one of the areas below, select the restore button on the right next to the desired restore event.

| RESTORE EVENT | RESTORE |
|---|---|
| Restore Default Wireless Settings: | Restore |
| Restore Default Firewall Settings: | Restore |
| Restore Modem to Factory Default State: | Restore |

2. If you want to restore only the Modem Router's default wireless settings, click the "Restore" button across from Restore Default Wireless Settings. The Modem Router's current wireless settings will be deleted, and the factory default wireless settings restored.

3. If you want to restore only the Modem Router's default firewall settings, click the Restore button across from Restore Default Firewall Settings. The Modem Router's current firewall settings will be deleted, and the factory default firewall settings restored.

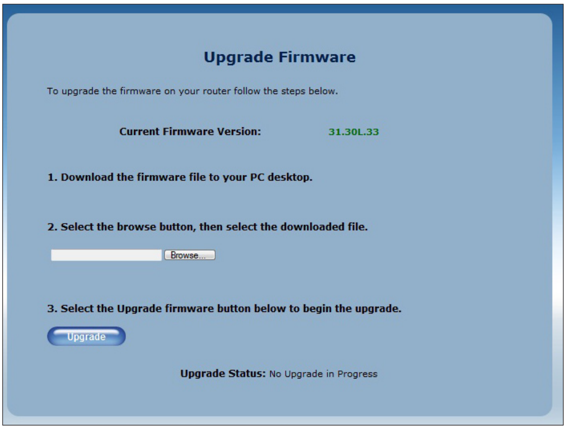
4. If you want to restore all the Modem Router's default settings, click the Restore button across from Restore Modem to Factory Default Settings. All of the Modem Router's current settings (including wireless and firwall settings) will be deleted, and the factory default settings restored.

> ***Note*:** All of the Modem Router's settings and parameters will be restored to their default values after performing the Restore Factory Default procedure. This includes the user name and password; the user-specified user name and password will no longer be valid.

## Upgrade Firmware

Selecting **Upgrade Firmware** from any Utilities screen generates the Upgrade Firmware screen, which is used to upgrade the Modem Router's firmware. Actiontec periodically updates the Modem Router's firmware to enhance performance, add new capabilities, and eradicated software bugs. To upgrade the Modem Router's firmware:

1. Go to the Actiontec support web site (http://www.actiontec.com/support/) and select the product from the Product Categories section. Check to see if there is a newer firmware version available for the Modem Router by comparing the available firmware upgrade revision to the one currently running on the Modem Router. The Modem Router's current firmware revision number appears in the Upgrade Firmware screen.



Upgrade Firmware

To upgrade the firmware on your router follow the steps below.

**Current Firmware Version:** 31.30L.33

**1. Download the firmware file to your PC desktop.**

**2. Select the browse button, then select the downloaded file.**

**3. Select the Upgrade firmware button below to begin the upgrade.**

**Upgrade Status:** No Upgrade in Progress

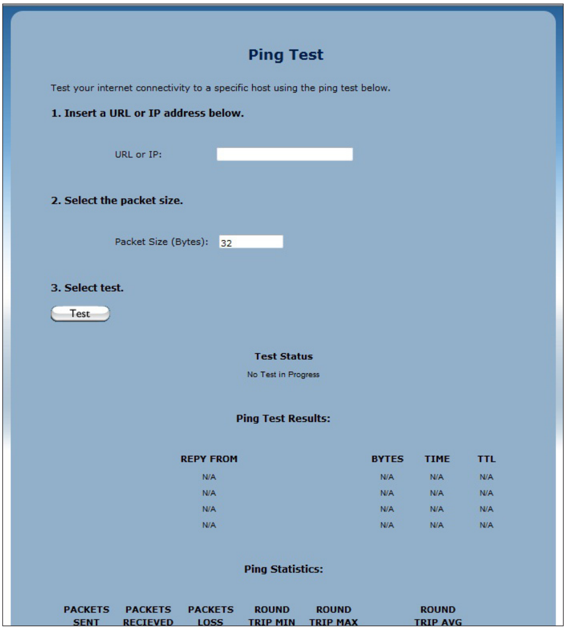
2. If there is new firmware available, download it to your computer. Note its location on the computer's hard drive.

3. Click **Browse** and in the window that appears, locate the downloaded firmware file, and select it.

4. Click **Upgrade**. The new firmware is loaded on the Modem Router. When the process is complete, the Modem Router will be running with the new firmware.

## Ping Test

Selecting **Ping Test** from any Utilities screen generates the Ping Test screen, which is used to check whether the Modem Router is properly connected to the Internet. Follow the on-screen instructions to perform the test. The results will be displayed at the bottom of the screen.



Ping Test

Test your internet connectivity to a specific host using the ping test below.

**1. Insert a URL or IP address below.**

URL or IP:

**2. Select the packet size.**

Packet Size (Bytes): 32

**3. Select test.**

**Test Status**

No Test in Progress

**Ping Test Results:**

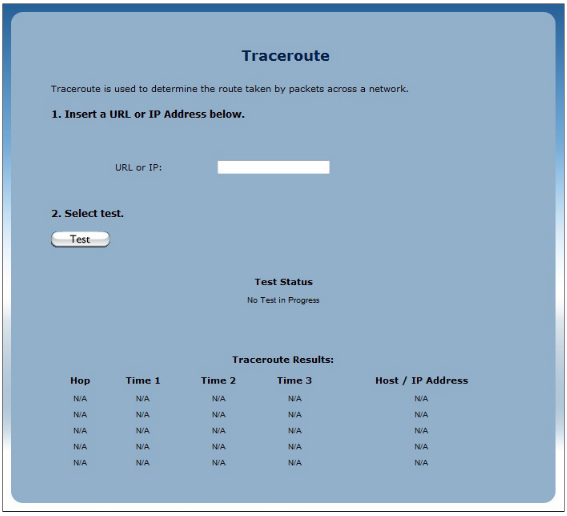
| REPY FROM | BYTES | TIME | TTL |
|---|---|---|---|
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A |

**Ping Statistics:**

| PACKETS SENT | PACKETS RECIEVED | PACKETS LOSS | ROUND TRIP MIN | ROUND TRIP MAX | ROUND TRIP AVG |
|---|---|---|---|---|---|

## Traceroute

Selecting **Traceroute** from any Utilities screen generates the Traceroute screen, which is used to determine the route taken by packets across a network. Follow the on-screen instructions to perform the test. The results will be displayed at the bottom of the screen.



### Traceroute

Traceroute is used to determine the route taken by packets across a network.

**1. Insert a URL or IP Address below.**

URL or IP:

**2. Select test.**

**Test Status**

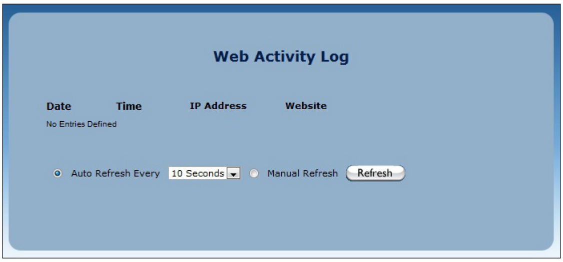
No Test in Progress

**Traceroute Results:**

| Hop | Time 1 | Time 2 | Time 3 | Host / IP Address |
|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A | N/A |
| N/A | N/A | N/A | N/A | N/A |

## Web Activity Log

To check the web activity on the Modem Router's network, click Web Activiy Log from any Utilities screen. The Web Activity Log appears:



Web Activity Log

| Date | Time | IP Address | Website |
|---|---|---|---|
| No Entries Defined | | | |

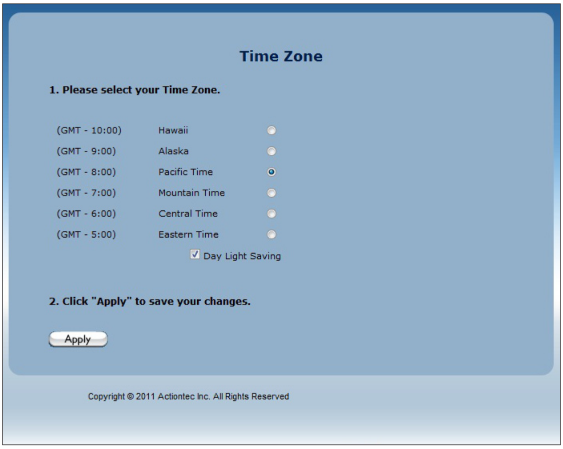
● Auto Refresh Every 10 Seconds ○ Manual Refresh

To change the automatic refresh period of the Web Activity Log, select a new time period from the Auto Refresh Every drop-down list. To refresh the Log, click **Refresh**.

## Time Zone

To set the correct time zone on the Modem Router:

1. Click **Time Zone** from the left side of any Advanced Setup screen. The Time Zone screen appears.



Time Zone

1. Please select your Time Zone.

| | | |
|---|---|---|
| (GMT - 10:00) | Hawaii | ○ |
| (GMT - 9:00) | Alaska | ○ |
| (GMT - 8:00) | Pacific Time | ● |
| (GMT - 7:00) | Mountain Time | ○ |
| (GMT - 6:00) | Central Time | ○ |
| (GMT - 5:00) | Eastern Time | ○ |

☑ Day Light Saving

2. Click "Apply" to save your changes.

Copyright © 2011 Actiontec Inc. All Rights Reserved

2. Click in the appropriate radio button for your time zone.

3. If daylight saving is currently in effect, click in the "Day Light Saving" check box to activate

4. Click **Apply** to save your settings.

# Configuring Advanced Setup

# 5

This chapter will explain the options provided in the Advanced Setup section of the Modem Router's firmware, including services blocking, firewall options, and setting up QoS (Quality of Service).

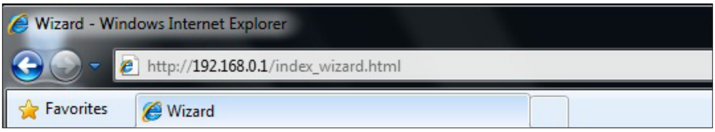
## Accessing Advanced Setup Options

To access the Advanced Setup screens:

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

   ```
   http://192.168.0.1
   ```

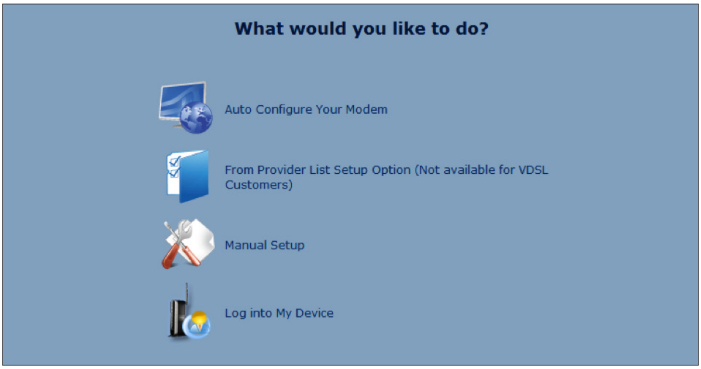
   then press **Enter** on the keyboard.



Wizard - Windows Internet Explorer

http://192.168.0.1/index_wizard.html

2. The Modem Router’s host screen appears. Click **Manual Setup**.



What would you like to do?

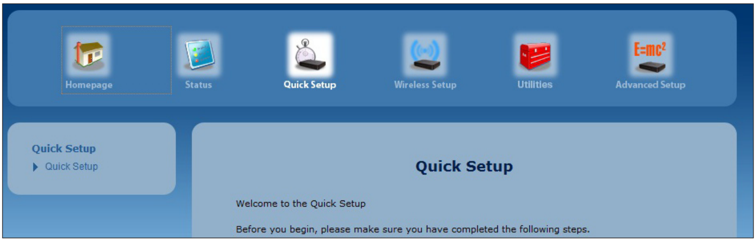
Auto Configure Your Modem

From Provider List Setup Option (Not available for VDSL Customers)

Manual Setup

Log into My Device

3. The “Quick Setup” screen appears, with a row of large icons across the top of the screen. Click **Advanced Setup**.

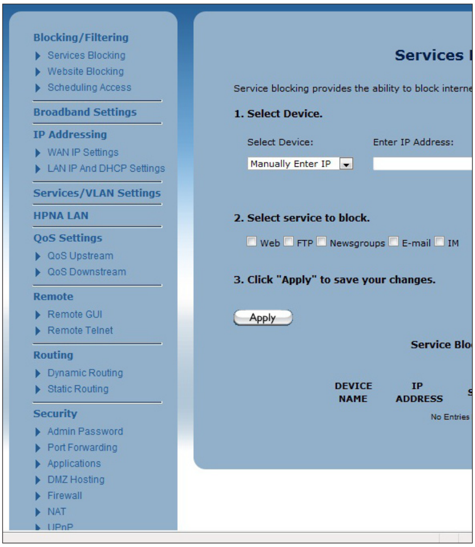


Quick Setup

Welcome to the Quick Setup

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

4. An “Advanced Setup” screen appears, with list of options on the left side of the screen.



Services I

Service blocking provides the ability to block interne

1. Select Device.

Select Device: Manually Enter IP

Enter IP Address:

2. Select service to block.

□ Web □ FTP □ Newsgroups □ E-mail □ IM

3. Click "Apply" to save your changes.

Service Blo

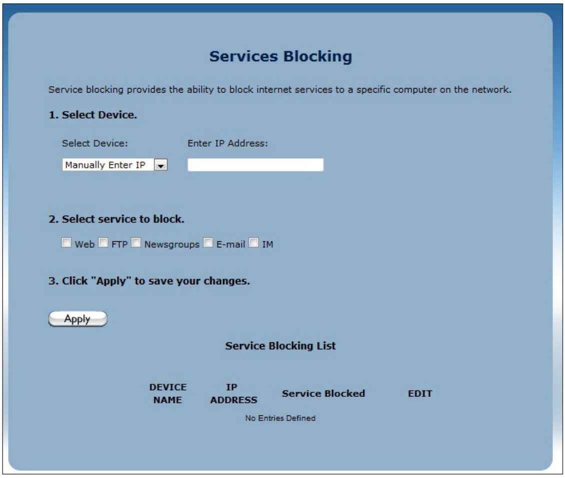
| DEVICE NAME | IP ADDRESS | S |
|---|---|---|
| | No Entries | |

The rest of this chapter explains the options found in the menu on the left side of every advanced setup settings screen.

## Services Blocking

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

1. Click **Services Blocking** from the menu on the left side of any Advanced Setup screen. The Services Blocking screen appears.



Services Blocking

Service blocking provides the ability to block internet services to a specific computer on the network.

1. Select Device.

Select Device: Manually Enter IP

Enter IP Address:

2. Select service to block.

□ Web □ FTP □ Newsgroups □ E-mail □ IM

3. Click "Apply" to save your changes.

Service Blocking List

| DEVICE NAME | IP ADDRESS | Service Blocked | EDIT |
|---|---|---|---|
| No Entries Defined | | | |

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

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

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

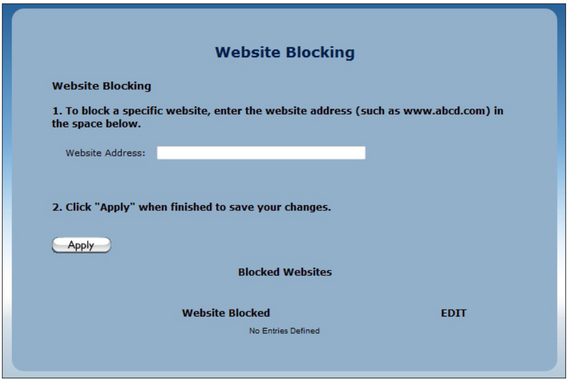
5. Repeat steps 1-4 to block services on another device on the network.

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

## Website Blocking

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

1. Click **Website Blocking** from the menu on the left side of any Advanced Setup screen. The Website Blocking screen appears.



Website Blocking

Website Blocking

1. To block a specific website, enter the website address (such as www.abcd.com) in the space below.

Website Address:

2. Click "Apply" when finished to save your changes.

Blocked Websites

| Website Blocked | EDIT |
|---|---|
| No Entries Defined | |

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

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

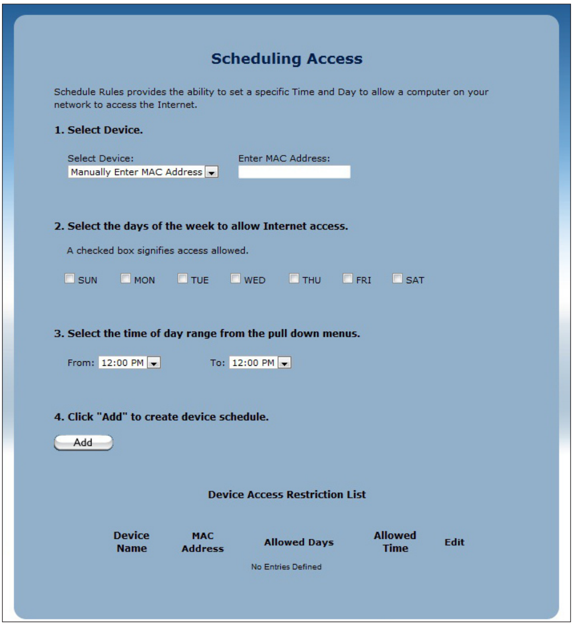
4. Repeat steps 1-3 to block other web sites from being acesssed on the Modem Router's network.

The web sites blocked from being accessed on the Modem Router's network are listed at the bottom of the screen.

## Scheduling Access

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

1. Click **Scheduling Access** from the menu on the left side of any Advanced Setup screen. The Scheduling Access screen appears.



Scheduling Access

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

1. Select Device.

Select Device: Manually Enter MAC Address

Enter MAC Address:

2. Select the days of the week to allow Internet access.

A checked box signifies access allowed.

□ SUN □ MON □ TUE □ WED □ THU □ FRI □ SAT

3. Select the time of day range from the pull down menus.

From: 12:00 PM To: 12:00 PM

4. Click "Add" to create device schedule.

Device Access Restriction List

| Device Name | MAC Address | Allowed Days | Allowed Time | Edit |
|---|---|---|---|---|
| | | No Entries Defined | | |

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

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

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

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

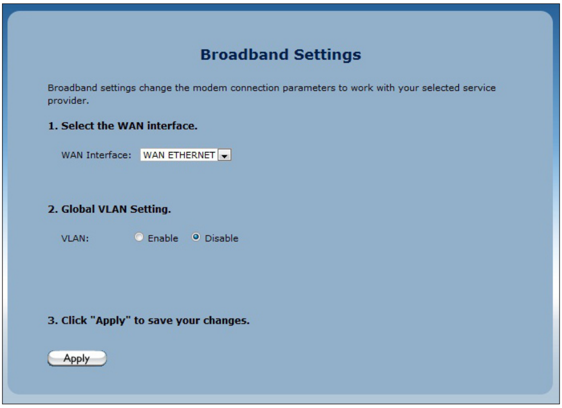
6. Repeat steps 1-5 to create multiple access schedules for other devices on the Modem Router's network.

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

## Broadband Settings

The Broadband Settings screen allows the Modem Router to connect to different service providers, which may have different connection parameters than the Modem Router's default settings. To change Broadband Settings:

1. Click **Broadband Settings** from the menu on the left side of any Advanced Setup screen. The Broadband Settings screen appears.



Broadband Settings

Broadband settings change the modem connection parameters to work with your selected service provider.

1. Select the WAN interface.

WAN Interface: WAN ETHERNET

2. Global VLAN Setting.

VLAN: ○ Enable ● Disable

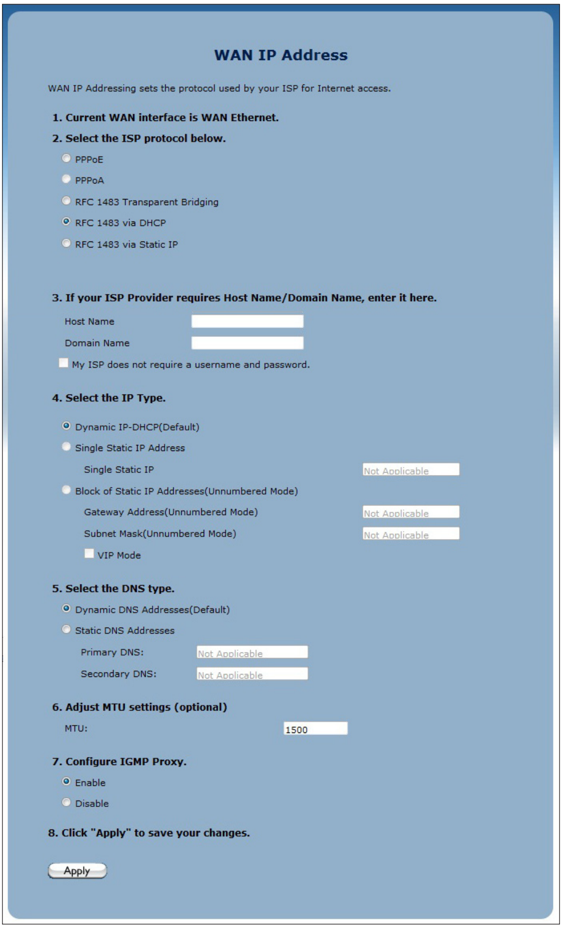
3. Click "Apply" to save your changes.

2. Select the type of WAN interface the service providers uses. Options are WAN Ethernet, WAN DSL PTM, and WAN DSL ATM.
3. Enable or disable Global VLAN on the Modem Router by clicking in the appropriate radio button. Global VLANs are used on the WAN and LAN sides to create virtual networks. Do not enable or disable Global VLAN unless instructed to do so by your ISP.
4. Click **Apply** to save your changes.

## WAN IP Address

The WAN IP Address screen allows you to manually set up the WAN IP address of the Modem Router. To do this:

1. Click **WAN IP Address** from the menu on the left side of any Advanced Setup screen. The WAN IP Address screen appears.



### WAN IP Address

WAN IP Addressing sets the protocol used by your ISP for Internet access.

**1. Current WAN interface is WAN Ethernet.**

**2. Select the ISP protocol below.**

○ PPPoE
○ PPPoA
○ RFC 1483 Transparent Bridging
● RFC 1483 via DHCP
○ RFC 1483 via Static IP

**3. If your ISP Provider requires Host Name/Domain Name, enter it here.**

Host Name
Domain Name
□ My ISP does not require a username and password.

**4. Select the IP Type.**

● Dynamic IP-DHCP(Default)
○ Single Static IP Address
Single Static IP: Not Applicable
○ Block of Static IP Addresses(Unnumbered Mode)
Gateway Address(Unnumbered Mode): Not Applicable
Subnet Mask(Unnumbered Mode): Not Applicable
□ VIP Mode

**5. Select the DNS type.**

● Dynamic DNS Addresses(Default)
○ Static DNS Addresses
Primary DNS: Not Applicable
Secondary DNS: Not Applicable

**6. Adjust MTU settings (optional)**

MTU: 1500

**7. Configure IGMP Proxy.**

● Enable
○ Disable

**8. Click "Apply" to save your changes.**

2. Select the type of connection the ISP uses.

   > ***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.

3. If using PPPoA or PPPoE was selected in step 1, enter the user name and password in the appropriate text boxes. If the ISP requires no user name or password, click in the "My ISP does not require a username and password" check box.

4. Select the IP type. If Single Static IP Address was selected, enter the IP address in the "Single Static IP" text box. If "Block of Static IP Addresses (Unnumbered Mode)" was selected, enter the designated gateway IP address and subnet mask address in the "Modem Address" and "Subnet Mask" text boxes, respectively. Also, "VIP Mode" can be activated by clicking in the appropriate check box. VIP mode works in concert with unnumbered mode and allows computers not assigned a static IP to receive a DHCP LAN side private IP address.

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. If applicable, enter a different MTU value in the MTU text box.

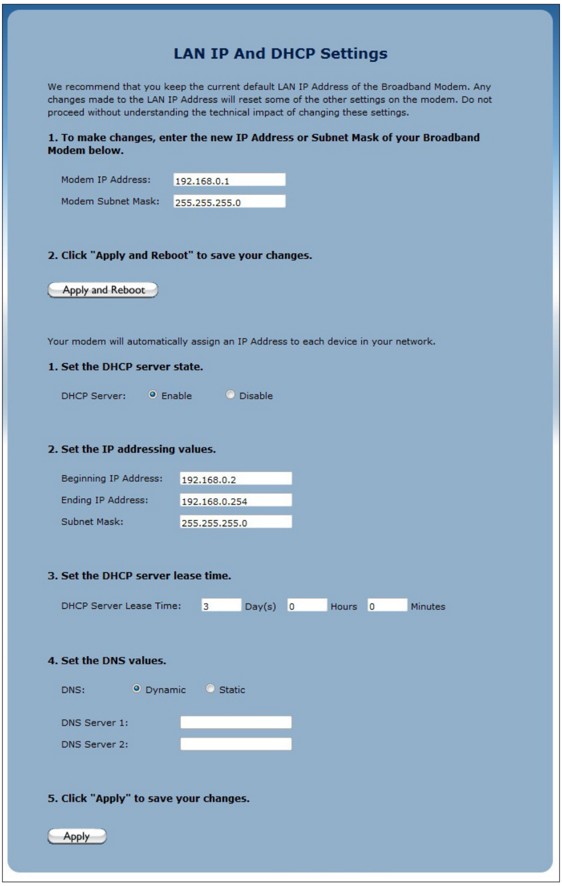
7. Enable or disable IGMP proxy by clicking in the appropriate radio button.

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

## LAN IP and DHCP Settings

The LAN IP and DHCP Settings screen allows you to change the Modem Router's default LAN IP address, and adjust the DHCP settings. To change the LAN IP:

1. Click **LAN IP and DHCP Settings** from the menu on the left side of any Advanced Setup screen. The LAN IP and DHCP Settings screen appears.



LAN IP And DHCP Settings

We recommend that you keep the current default LAN IP Address of the Broadband Modem. Any changes made to the LAN IP Address will reset some of the other settings on the modem. Do not proceed without understanding the technical impact of changing these settings.

**1. To make changes, enter the new IP Address or Subnet Mask of your Broadband Modem below.**

Modem IP Address: 192.168.0.1

Modem Subnet Mask: 255.255.255.0

**2. Click "Apply and Reboot" to save your changes.**

Your modem will automatically assign an IP Address to each device in your network.

**1. Set the DHCP server state.**

DHCP Server: ● Enable ○ Disable

**2. Set the IP addressing values.**

Beginning IP Address: 192.168.0.2

Ending IP Address: 192.168.0.254

Subnet Mask: 255.255.255.0

**3. Set the DHCP server lease time.**

DHCP Server Lease Time: 3 Day(s) 0 Hours 0 Minutes

**4. Set the DNS values.**

DNS: ● Dynamic ○ Static

DNS Server 1:

DNS Server 2:

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

2. Enter the new modem IP address and modem subnet mask in the appropriate text boxes.

3. Click **Apply and Reboot**. The Modem Router reboots with the new settings.

To change the Modem Router's DHCP settings:

4. Click **Enable** to activate the Modem Router's DHCP server.

5. Enter the DHCP server's beginning IP address, ending IP address, and subnet mask address in the appropriate text boxes.

6. Enter the DHCP server's lease time period by entering the days, hours, and minutes in the appropriate text boxes.

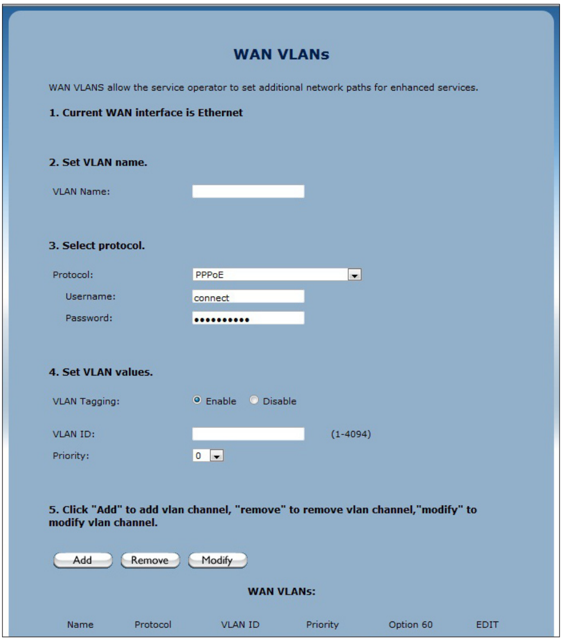
7. Set the DNS values by selecting Dynamic or Static (clicking in the appropriate radio button), then, if needed enter the IP addresses for DNS server 1 and 2.

8. Click **Apply** to save your changes.

## WAN VLAN

The WAN VLAN screen allows the service operator to create additional network paths to accomodate new services. To use:

1. Click **Services/VLAN Settings** from the menu on the left side of any Advanced Setup screen. The WAN VLANs screen appears.



WAN VLANs

WAN VLANS allow the service operator to set additional network paths for enhanced services.

1. Current WAN interface is Ethernet

2. Set VLAN name.

VLAN Name:

3. Select protocol.

Protocol: PPPoE

Username: connect

Password: ••••••••••

4. Set VLAN values.

VLAN Tagging: ● Enable ○ Disable

VLAN ID: (1-4094)

Priority: 0

5. Click "Add" to add vlan channel, "remove" to remove vlan channel,"modify" to modify vlan channel.

WAN VLANs:

| Name | Protocol | VLAN ID | Priority | Option 60 | EDIT |
|---|---|---|---|---|---|

2. Enter the name of the VLAN in the VLAN name text box.

3. Select a protocol from the drop-down list (options are PPPoE, RFC 1483 Transparent Bridging, and RFC 1483 via DHCP), then enter a user name and password in the appropriate text boxes.

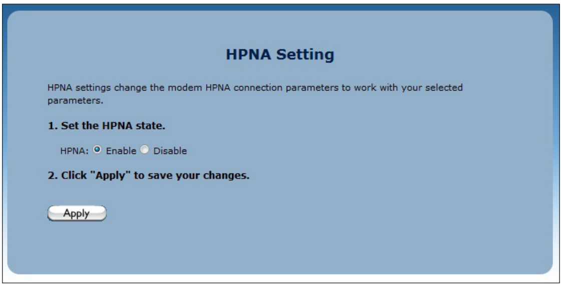
4. If applicable, enable VLAN tagging by clicking in the radio button next to Enable under step; 4, then entering a VLAN ID (1 to 4094) and selecting a Priority (0-7).

5. Click **Add** to add the VLAN to the VLAN list, which appears at the bottom of the screen.

You can also delete existing VLANs by clicking **Delete**, or modify a VLAN's settings by clicking **Modify**.

## HPNA Settings

The HPNA Settings screen allows you to enable HPNA. Click in the Enable radio button to activate.



**HPNA Setting**

HPNA settings change the modem HPNA connection parameters to work with your selected parameters.

**1. Set the HPNA state.**

HPNA: ● Enable ○ Disable

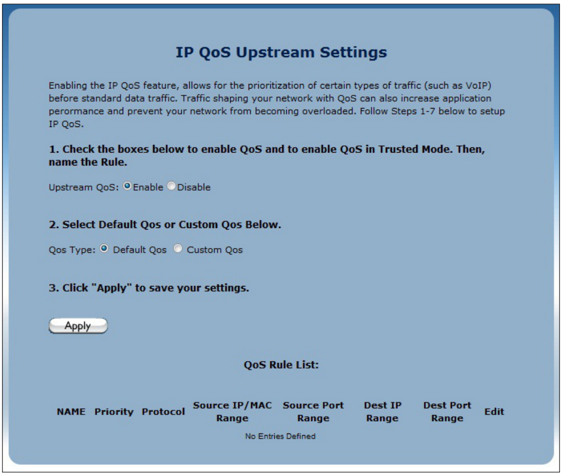
**2. Click "Apply" to save your changes.**

## QoS Settings

The QoS Settings screens allow you to prioritize certain types of data traffic (video, for example) over other data traffic on the Modem Router's network. Both incoming data traffic (QoS Upstream) and outgoing data traffic (QoS Downstream) can be configured.

### QoS Upstream

1. Click **QoS Upstream** from the menu on the left side of any Advanced Setup screen. The QoS Upstream screen appears.



IP QoS Upstream Settings

Enabling the IP QoS feature, allows for the prioritization of certain types of traffic (such as VoIP) before standard data traffic. Traffic shaping your network with QoS can also increase application perormance and prevent your network from becoming overloaded. Follow Steps 1-7 below to setup IP QoS.

**1. Check the boxes below to enable QoS and to enable QoS in Trusted Mode. Then, name the Rule.**

Upstream QoS: ● Enable ○ Disable

**2. Select Default Qos or Custom Qos Below.**

Qos Type: ● Default Qos ○ Custom Qos

**3. Click "Apply" to save your settings.**

**QoS Rule List:**

| NAME | Priority | Protocol | Source IP/MAC Range | Source Port Range | Dest IP Range | Dest Port Range | Edit |
|---|---|---|---|---|---|---|---|

No Entries Defined

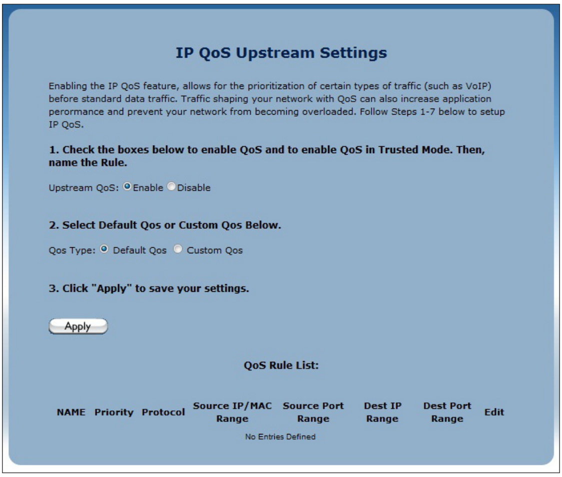
1. Click in the Enable radio button next to Upstream QoS to activate.

2. Select the type of QoS to enable. If selecting Custom QoS, you will have to enter a number of values: Name, Queue Priority, Reserved Bandwidth, Protocol, TOS Bit Value, Source IP or MAC address information, Destination IP Address, Netmask IP Address, and Port Pange. Do not select Custom QoS unless you are an experienced network technician. For most wireless networks, the Default QoS option should be sufficient.

3. Click **Apply** to save your changes. The new QoS setting will appear at the bottom of the screen, under QoS Rule List.

## QoS Downstream

1. Click **QoS Downstream** from the menu on the left side of any Advanced Setup screen. The QoS Downstream screen appears.



**IP QoS Upstream Settings**

Enabling the IP QoS feature, allows for the prioritization of certain types of traffic (such as VoIP) before standard data traffic. Traffic shaping your network with QoS can also increase application perormance and prevent your network from becoming overloaded. Follow Steps 1-7 below to setup IP QoS.

**1. Check the boxes below to enable QoS and to enable QoS in Trusted Mode. Then, name the Rule.**

Upstream QoS: ● Enable ○ Disable

**2. Select Default Qos or Custom Qos Below.**

Qos Type: ● Default Qos ○ Custom Qos

**3. Click "Apply" to save your settings.**

**QoS Rule List:**

| NAME | Priority | Protocol | Source IP/MAC Range | Source Port Range | Dest IP Range | Dest Port Range | Edit |
|---|---|---|---|---|---|---|---|

No Entries Defined

1. Click in the Enable radio button next to Downstream QoS to activate.

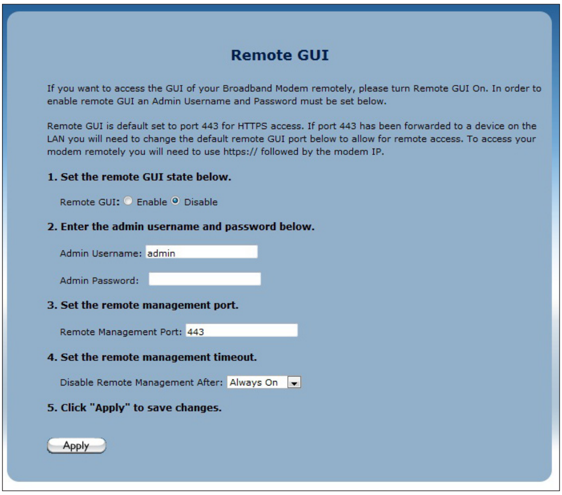
2. Select the type of QoS to enable. If selecting Custom QoS, you will have to enter a number of values: Name, Queue Priority, Reserved Bandwidth, Protocol, TOS Bit Value, Source IP or MAC address information, Destination IP Address, Netmask IP Address, and Port Pange. Do not select Custom QoS unless you are an experienced network technician. For most wireless networks, the Default QoS option should be sufficient.

3. Click **Apply** to save your changes. The new QoS setting will appear at the bottom of the screen, under QoS Rule List.

## Remote GUI

The Remote GUI screen allows you to setup the Modem Router so that it can be accessed from a remote location. To use:

1. Click **Remote GUI** from the menu on the left side of any Advanced Setup screen. The Remote GUI screen appears.



### Remote GUI

If you want to access the GUI of your Broadband Modem remotely, please turn Remote GUI On. In order to enable remote GUI an Admin Username and Password must be set below.

Remote GUI is default set to port 443 for HTTPS access. If port 443 has been forwarded to a device on the LAN you will need to change the default remote GUI port below to allow for remote access. To access your modem remotely you will need to use https:// followed by the modem IP.

**1. Set the remote GUI state below.**

Remote GUI: ○ Enable ● Disable

**2. Enter the admin username and password below.**

Admin Username: admin

Admin Password:

**3. Set the remote management port.**

Remote Management Port: 443

**4. Set the remote management timeout.**

Disable Remote Management After: Always On

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

2. Click in the Enable radio button next to Remote GUI to activate.

3. Enter a user name and password in the appropriate text boxes beneath step 2.

4. Set the remote management port. It is set to port 443 by default. If the remote management port number has been changed, you will need to use the URL "https://" followed by the Modem Router's IP address, a colon (:), then the port number to which the remote management port was changed.
   Example: https://192.170.1.1:234.

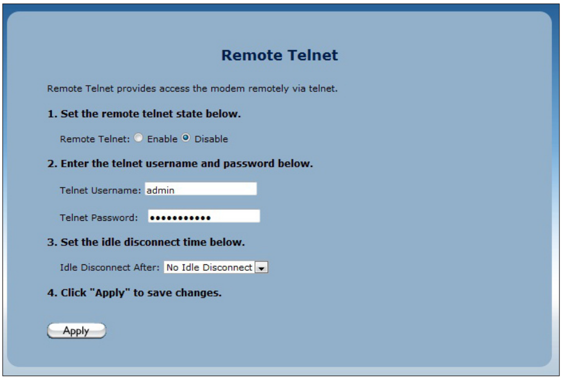
5. Select the remote management timeout. If you select one of the time periods provided in the drop-down list, remote management of the Modem Router will stop after the selected time period, if no actions are detected.

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

## Remote Telnet

The Remote Telnet screen allows you to set up the Modem Router so that it can be accessed from a remote (not local) telnet device. To use:

1. Click **Remote Telnet** from the menu on the left side of any Advanced Setup screen. The Remote Telnet screen appears.



Remote Telnet

Remote Telnet provides access the modem remotely via telnet.

1. Set the remote telnet state below.

Remote Telnet: ○ Enable ● Disable

2. Enter the telnet username and password below.

Telnet Username: admin

Telnet Password: •••••••••••

3. Set the idle disconnect time below.

Idle Disconnect After: No Idle Disconnect

4. Click "Apply" to save changes.

2. Click in the Enable radio button next to Remote Telnet to activate.

3. Enter a username and password in the appropriate text boxes beneath step 2.

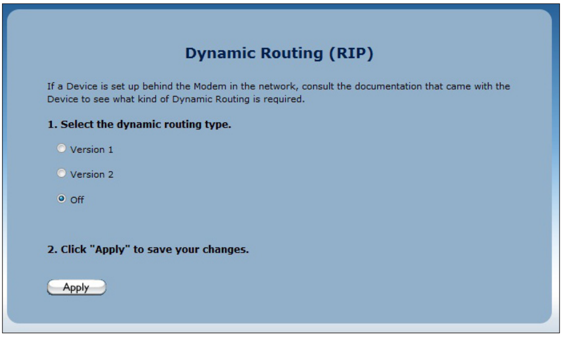
4. Select the idle disconnect time. If you select one of the time periods provided in the drop-down list, remote telnet management of the Modem Router will stop after the selected time period, if no actions are detected.

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

## Dynamic Routing

The Dynamic Routing screen allows you to set up the Modem Router for dynamic routing, which is useful if the Modem Router is set up in a network behind a modem To use:

1. Click **Dynamic Routing** from the menu on the left side of any Advanced Setup screen. The Dynamic Routing screen appears.



Dynamic Routing (RIP)

If a Device is set up behind the Modem in the network, consult the documentation that came with the Device to see what kind of Dynamic Routing is required.

1. Select the dynamic routing type.

○ Version 1

○ Version 2

● Off

2. Click "Apply" to save your changes.

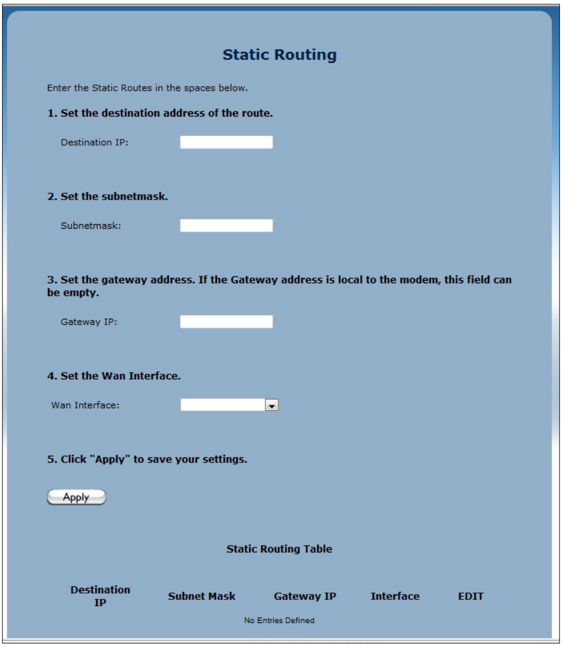
2. Select the version of dynamic routing you want to use (Version 1, Version 2) by clicking in the appropriate radio button. Consult the documentation that came with the modem set up in front of the Modem Router on the network to find out which version to use.

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

## Static Routing

The Static Routing screen allows you to set up static routes on the Modem Router. To use:

1. Click **Static Routing** from the menu on the left side of any Advanced Setup screen. The Static Routing screen appears.



Static Routing

Enter the Static Routes in the spaces below.

1. Set the destination address of the route.

Destination IP:

2. Set the subnetmask.

Subnetmask:

3. Set the gateway address. If the Gateway address is local to the modem, this field can be empty.

Gateway IP:

4. Set the Wan Interface.

Wan Interface:

5. Click "Apply" to save your settings.

Static Routing Table

| Destination IP | Subnet Mask | Gateway IP | Interface | EDIT |
|---|---|---|---|---|

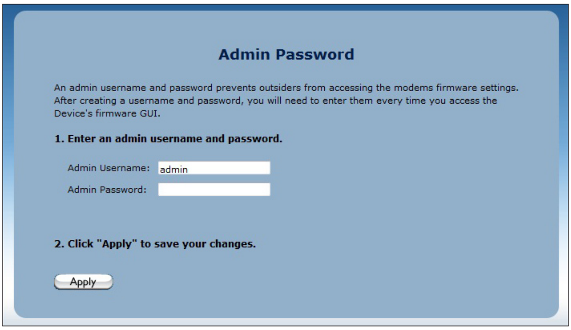
No Entries Defined

2. Enter the destination IP address of the static route in the Destination IP text box.
3. Enter the subnet mask IP address in the Subnetmask text box.
4. If applicable, enter the gateway IP address in the Gateway IP text box.
5. Select a WAN interface from the WAN Interface drop-down list.
6. Click **Apply** to save your changes.

## Admin Password

To change the password that allows access to the Modem Router's firmware screens:

1. Click **Admin Password** from the menu on the left side of any Advanced Setup screen. The Admin Password screen appears.



Admin Password

An admin username and password prevents outsiders from accessing the modems firmware settings. After creating a username and password, you will need to enter them every time you access the Device's firmware GUI.

**1. Enter an admin username and password.**

Admin Username: admin

Admin Password:

**2. Click "Apply" to save your changes.**

2. If needed, enter a new username in the text box next to Admin username.

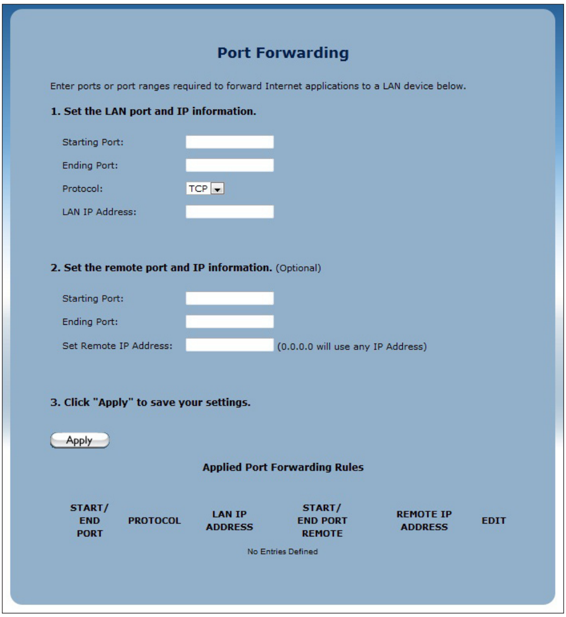
3. Enter a new password in the text box next to Admin Password.

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

## Port Forwarding

Port forwarding is used for Internet applications that need access to devices connected to the Modem Router's network:

1. Click **Port Forwarding** from the menu on the left side of any Advanced Setup screen. The Port Forwarding screen appears.



Port Forwarding

Enter ports or port ranges required to forward Internet applications to a LAN device below.

1. Set the LAN port and IP information.

Starting Port:
Ending Port:
Protocol: TCP
LAN IP Address:

2. Set the remote port and IP information. (Optional)

Starting Port:
Ending Port:
Set Remote IP Address: (0.0.0.0 will use any IP Address)

3. Click "Apply" to save your settings.

Applied Port Forwarding Rules

| START/ END PORT | PROTOCOL | LAN IP ADDRESS | START/ END PORT REMOTE | REMOTE IP ADDRESS | EDIT |
|---|---|---|---|---|---|

No Entries Defined

2. Enter a starting and ending LAN port numbers in the appropriate text boxes beneath step 1.

3. Select a protocol from the Protocol drop-down list (TCP, UDP, GRE).

4. Enter the LAN IP address of the port in the appropriate text box.

5. If applicable, enter the starting, ending, and remote IP address of the remote port in the appropriate text boxes.

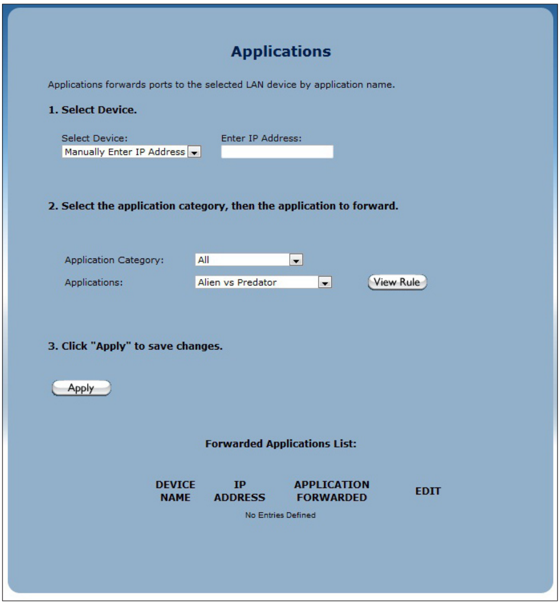
6. Click **Apply** to save your changes.

The port forwarding rules you create are listed at the bottom of the screen, under Applied Port Forwarding Rules.

## Applications

The Modem Router comes preloaded with a list of popular applications that require port forwarding. Instead of entering all the port forwarding values in the port forwarding screen, you can simply select the application in this screen to configure all of its ports.

1. Click **Applications** in any Advanced Setup screen. The Applications screen appears.



Applications

Applications forwards ports to the selected LAN device by application name.

1. Select Device.

Select Device: Manually Enter IP Address

Enter IP Address:

2. Select the application category, then the application to forward.

Application Category: All

Applications: Alien vs Predator

3. Click "Apply" to save changes.

Forwarded Applications List:

| DEVICE NAME | IP ADDRESS | APPLICATION FORWARDED | EDIT |
|---|---|---|---|
| No Entries Defined | | | |

2. Select the device on the Modem Router's network that you want the application to work with. Alternatively, you can enter the device's IP address in the appropriate text box.
3. Select the application from the Applications drop-down list. To make searching easier, you can select an application category from the Application Category drop-down list first, which will limit the applications in the Application list to that category.
4. After selecting an application, you can click **View Rule**. A new screen appears, displaying the rule's details.
5. Click **Apply** to save your changes.

The applications' port forwarding details will be listed at the bottom of the screen, underneath Forwarded Applications List.

### User Created Rules

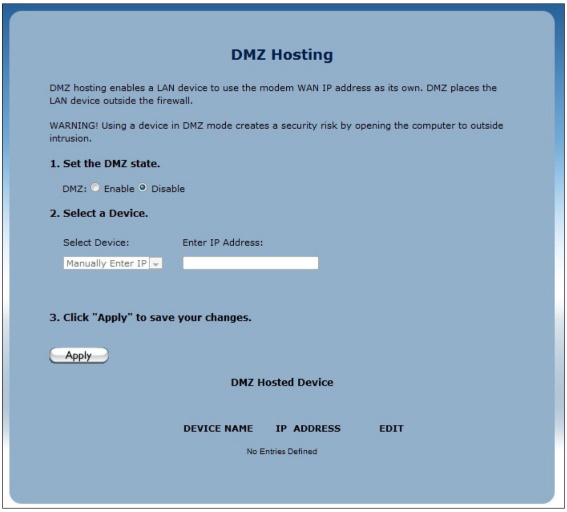
If, in step 3 of the previous procedure, User Created Rules was chosen, click Create Rule to generate a screen in which you can create a custom rule. Enter the rule name, select a protocol, and enter a port start, port end, and port map in the appropriate text boxes, then click Apply. The new rule will be listed at the bottom of the Applications screen.

## DMZ Hosting

Selecting **DMZ Hosting** from any Advanced Setup screen generates the DMZ Hosting screen. DMZ hosting allows a device on the Modem Router's network to be set up outside the Modem Router's firewall.

> ***WARNING***! The DMZ hosted device poses a security risk, since the device will be vulnerable to outside intrusion.

1. Click **DMZ Hosting** in any Advanced Setup screen. The DMZ Hosting screen appears.



**DMZ Hosting**

DMZ hosting enables a LAN device to use the modem WAN IP address as its own. DMZ places the LAN device outside the firewall.

WARNING! Using a device in DMZ mode creates a security risk by opening the computer to outside intrusion.

**1. Set the DMZ state.**

DMZ: ○ Enable ● Disable

**2. Select a Device.**

Select Device: Manually Enter IP

Enter IP Address:

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

**DMZ Hosted Device**

| DEVICE NAME | IP ADDRESS | EDIT |
|---|---|---|
| No Entries Defined | | |

2. Click in the Enable radio button to activate DMZ hosting.

3. Select the device on the Modem Router's network that you want use as the DMZ host. Alternatively, you can enter the device's IP address in the appropriate text box.

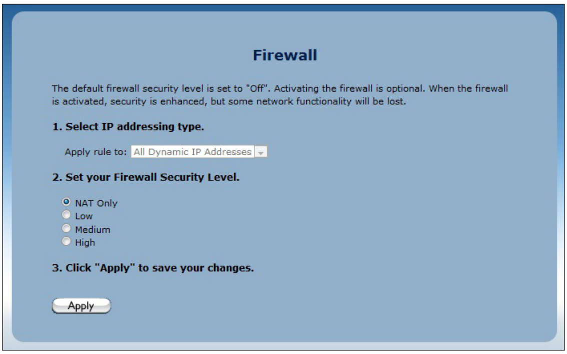
4. Click **Apply** to save your changes.

Afterwards, the DMZ hosted device details will be listed at the bottom of the screen, underneath DMZ Hosted Device.

## Firewall

Selecting **Firewall** from any Advanced Setup screen generates the Firewall screen. The Modem Router's firewall allows you to set up comprehensive security around your network, although some network functionality will be lost. To use:

1. Click **Firewall** in any Advanced Setup screen. The Firewall screen appears.



**Firewall**

The default firewall security level is set to "Off". Activating the firewall is optional. When the firewall is activated, security is enhanced, but some network functionality will be lost.

**1. Select IP addressing type.**

Apply rule to: All Dynamic IP Addresses

**2. Set your Firewall Security Level.**

● NAT Only
○ Low
○ Medium
○ High

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

2. Select one or all device(s) on the Modem Router's network from the Apply rule to drop-down list on which you want to apply the firewall.

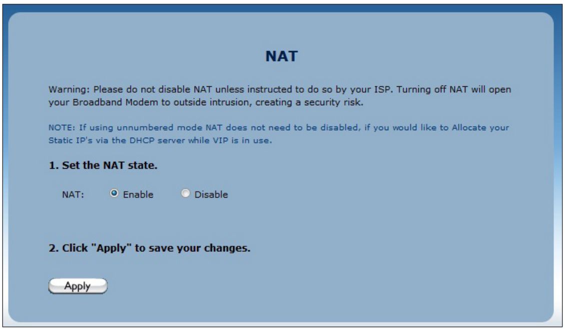
3. Select a firwall security level by clicking in the appropriate radio button below step 2.

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

If you selected Low, Medium, or High in step 3, you can do additional tweaking to the firewall by allowing or denying access to certain applications that appear in the Firewall screen.

## NAT

Selecting **NAT** from any Advanced Setup screen generates the NAT screen, which is used to enable or disable NAT, at the request of your ISP. If your ISP requires you to disable NAT, click in the Disable radio button, then click **Apply**. This action should be undertaken by an experienced network technician only.



NAT

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

NOTE: If using unnumbered mode NAT does not need to be disabled, if you would like to Allocate your Static IP's via the DHCP server while VIP is in use.

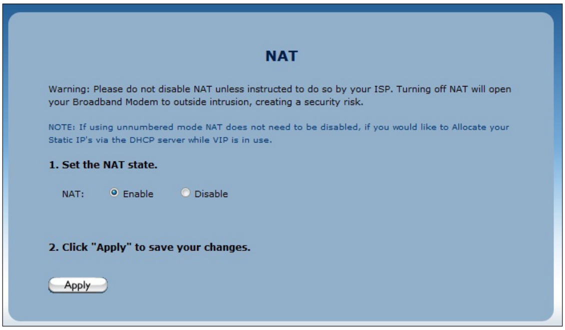
1. Set the NAT state.

NAT: ● Enable ○ Disable

2. Click "Apply" to save your changes.

## UPnP

Selecting **UPnP** (Universal Plug and Play) from any Advanced Setup screen generates the UPNP screen, which is used to set up gaming consoles on the Modem Router's network. To activate UPnP, click in the Enable radio button, then click **Apply**.



NAT

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

NOTE: If using unnumbered mode NAT does not need to be disabled, if you would like to Allocate your Static IP's via the DHCP server while VIP is in use.

1. Set the NAT state.

NAT: ● Enable ○ Disable

2. Click "Apply" to save your changes.

# Viewing the Modem Router's Status

# 6

This chapter gives an overview of the various status tables provided by the Modem Router, which allow you check on various parameters, including WAN connections, WAN Etherent connection, and wireless status.

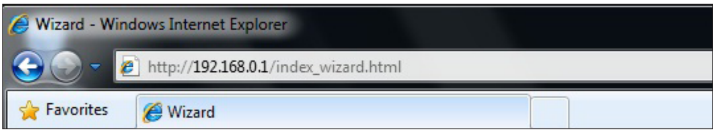
## Accessing Wireless Settings

To access the Wireless screens:

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

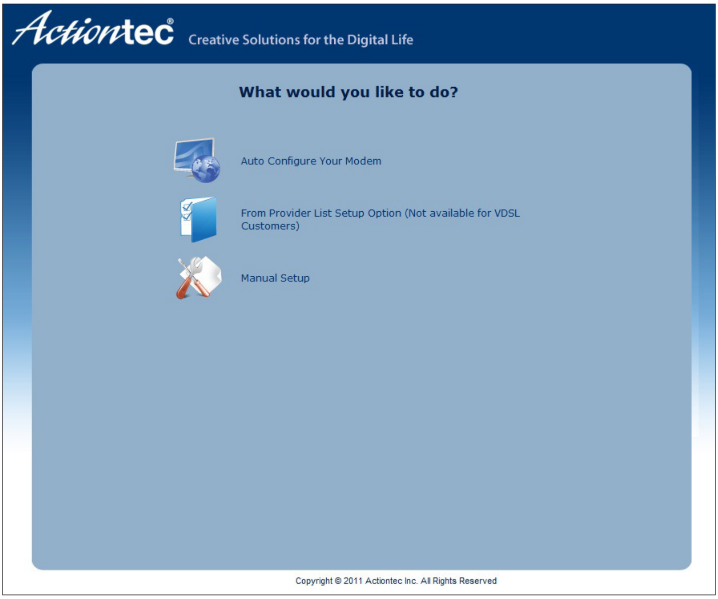
   ```
   http://192.168.0.1
   ```

   then press **Enter** on the keyboard.



Wizard - Windows Internet Explorer
http://192.168.0.1/index_wizard.html
Favorites
Wizard

2. The Modem Router's host screen appears. Click **Manual Setup**.



Actiontec Creative Solutions for the Digital Life

What would you like to do?

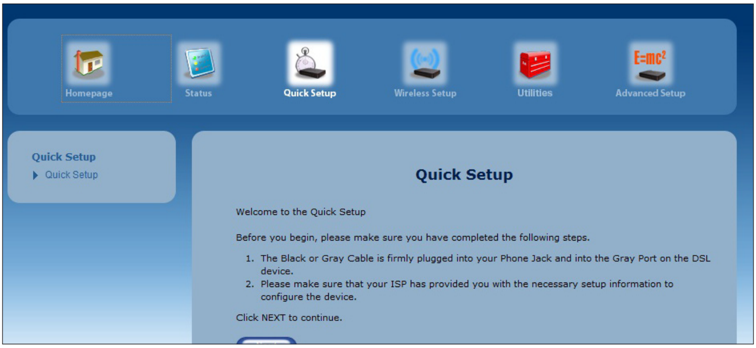
Auto Configure Your Modem

From Provider List Setup Option (Not available for VDSL Customers)

Manual Setup

Copyright © 2011 Actiontec Inc. All Rights Reserved

3. The Quick Setup screen appears, with a row of large icons across the top of the screen. Click **Status**.



Quick Setup

Welcome to the Quick Setup

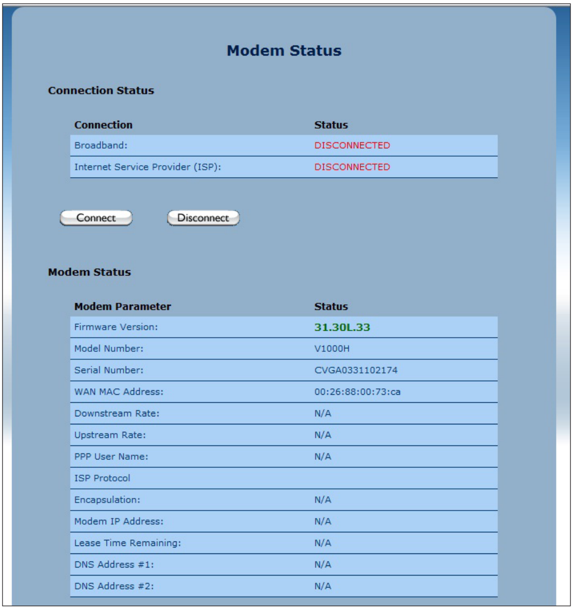
Before you begin, please make sure you have completed the following steps.

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

Click NEXT to continue.

## Connection Status

Click **Connection Status** from any Status screen to generate the Modem Status screen. This table displays various parameters regarding the Internet connection of the Modem Router, including broadband and ISP connection status, upstream rate, least time remaining, and DNS addresses. The only user-configurable option in the screen are the Connect and Disconnect buttons, which, when clicked, connects and/or disconnects Modem Router from your service provider.



Modem Status

Connection Status

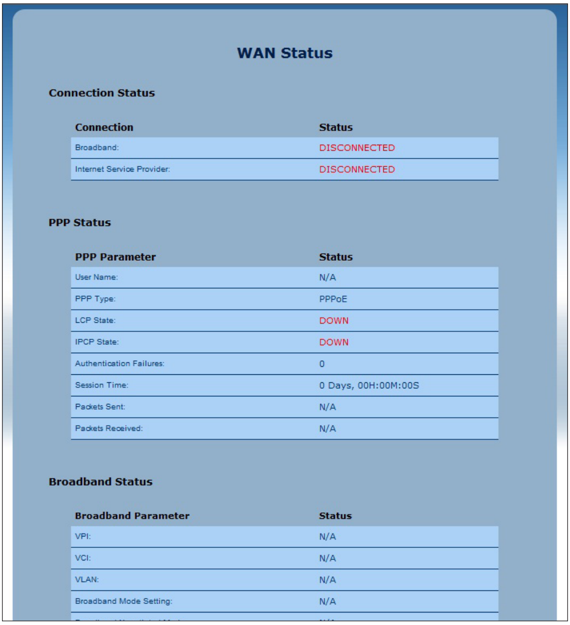
| Connection | Status |
|---|---|
| Broadband: | DISCONNECTED |
| Internet Service Provider (ISP): | DISCONNECTED |

Modem Status

| Modem Parameter | Status |
|---|---|
| Firmware Version: | 31.30L.33 |
| Model Number: | V1000H |
| Serial Number: | CVGA0331102174 |
| WAN MAC Address: | 00:26:88:00:73:ca |
| Downstream Rate: | N/A |
| Upstream Rate: | N/A |
| PPP User Name: | N/A |
| ISP Protocol | |
| Encapsulation: | N/A |
| Modem IP Address: | N/A |
| Lease Time Remaining: | N/A |
| DNS Address #1: | N/A |
| DNS Address #2: | N/A |

## WAN Status

Click **WAN Status** from any Status screen to generate the WAN Status screen. This table displays various parameters relating to the WAN connection of the Modem Router, including PPP and broadband status. There are no user-configurable options in this screen, but there is a Clear button at the bottom of the screen (not shown) that resets all of the statistics back to zero, at which time the statistics will begin accumulating again.



WAN Status

Connection Status

| Connection | Status |
|---|---|
| Broadband: | DISCONNECTED |
| Internet Service Provider: | DISCONNECTED |

PPP Status

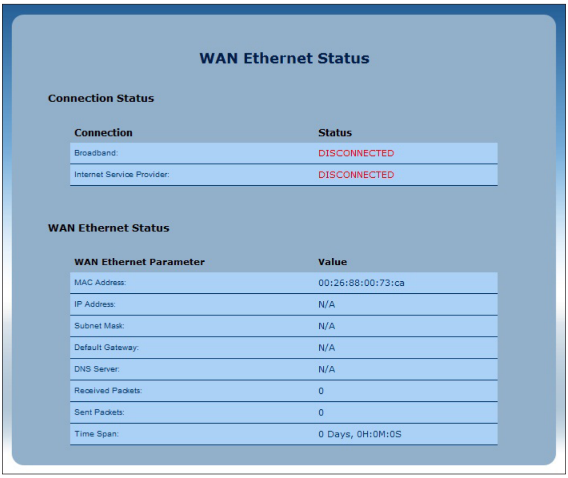
| PPP Parameter | Status |
|---|---|
| User Name: | N/A |
| PPP Type: | PPPoE |
| LCP State: | DOWN |
| IPCP State: | DOWN |
| Authentication Failures: | 0 |
| Session Time: | 0 Days, 00H:00M:00S |
| Packets Sent: | N/A |
| Packets Received: | N/A |

Broadband Status

| Broadband Parameter | Status |
|---|---|
| VPI: | N/A |
| VCI: | N/A |
| VLAN: | N/A |
| Broadband Mode Setting: | N/A |

## WAN Ethernet Status

Click **WAN Ethernet Status** from any Status screen to generate the WAN Ethernet Status screen. This table displays various parameters relating to the WAN Ethernet connection of the Modem Router, including subnet mask, default Modem Router, and sent packets. There are no user-configurable options in this screen.



WAN Ethernet Status

Connection Status

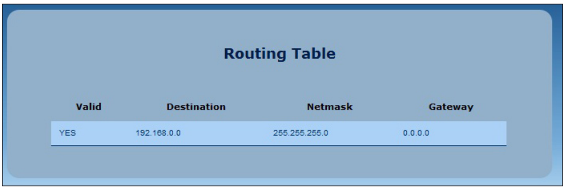
| Connection | Status |
|---|---|
| Broadband: | DISCONNECTED |
| Internet Service Provider: | DISCONNECTED |

WAN Ethernet Status

| WAN Ethernet Parameter | Value |
|---|---|
| MAC Address: | 00:26:88:00:73:ca |
| IP Address: | N/A |
| Subnet Mask: | N/A |
| Default Gateway: | N/A |
| DNS Server: | N/A |
| Received Packets: | 0 |
| Sent Packets: | 0 |
| Time Span: | 0 Days, 0H:0M:0S |

## Routing Table

Click **Routing Table** from any Status screen to generate the Routing Table screen. This screen displays the Modem Router's routing table. There are no user-configurable options in this screen.

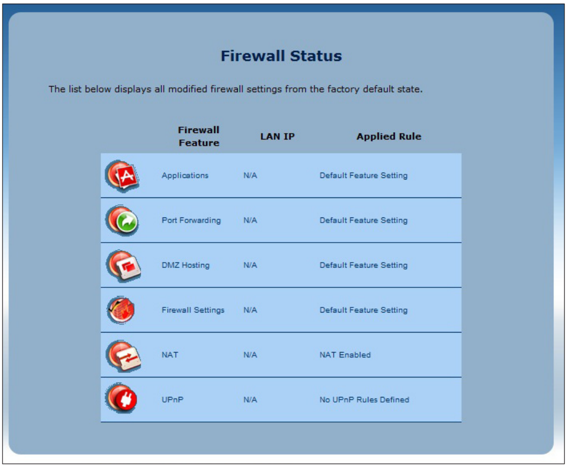


Routing Table

| Valid | Destination | Netmask | Gateway |
|---|---|---|---|
| YES | 192.168.0.0 | 255.255.255.0 | 0.0.0.0 |

## Firewall Status

Click **Firewall Status** from any Status screen to generate the Firewall Status screen. This table displays the status of the Modem Router's firewall. There are no user-configurable options in this screen. For more details, see the "Configuring the Firewall Settings" chapter of this manual.



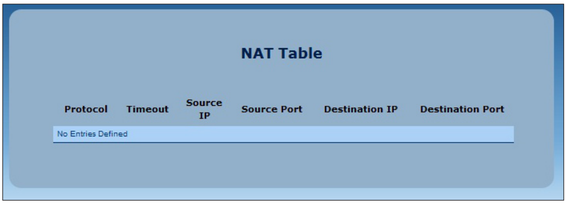
Firewall Status

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

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

## NAT Table

Click **NAT Table** from any Status screen to generate the "NAT Table" screen. This screen displays the Modem Router's NAT table. There are no user-configurable options in this screen.

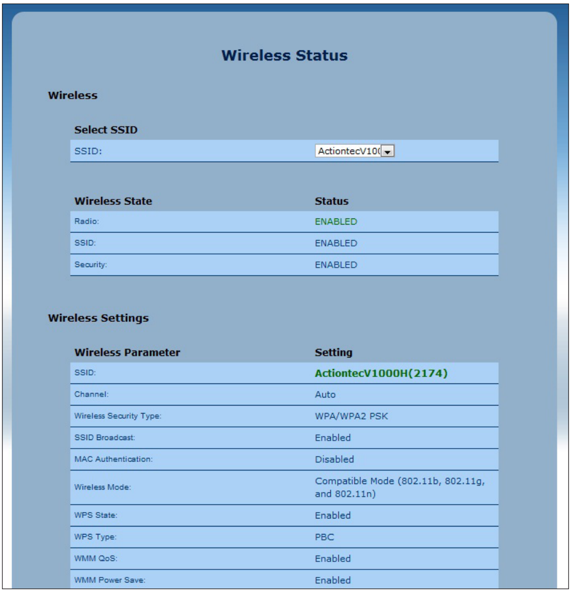


NAT Table

| Protocol | Timeout | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|---|
| No Entries Defined | | | | | |

## Wireless Status

Click **Wireless Status** from any Status screen to generate the "Wireless Status" screen. This table displays the Modem Router's wireless network statistics, including wireless security type, wireless mode, and packets received.



Wireless Status

Wireless

Select SSID

| | |
|---|---|
| SSID: | ActiontecV10( |

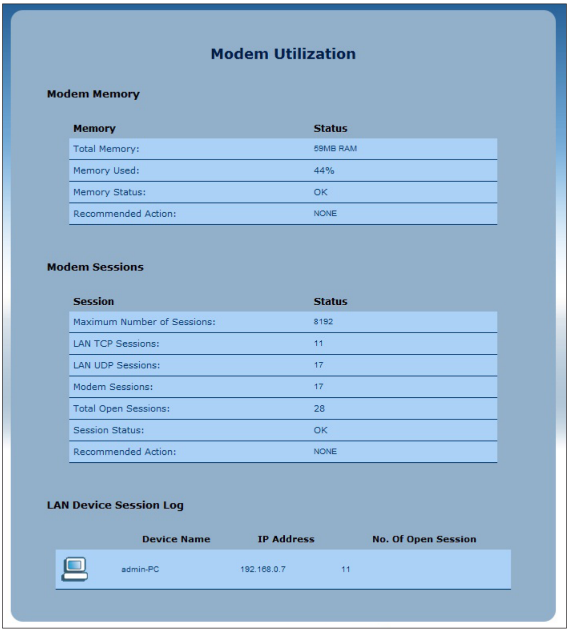
| Wireless State | Status |
|---|---|
| Radio: | ENABLED |
| SSID: | ENABLED |
| Security: | ENABLED |

Wireless Settings

| Wireless Parameter | Setting |
|---|---|
| SSID: | ActiontecV1000H(2174) |
| Channel: | Auto |
| Wireless Security Type: | WPA/WPA2 PSK |
| SSID Broadcast: | Enabled |
| MAC Authentication: | Disabled |
| Wireless Mode: | Compatible Mode (802.11b, 802.11g, and 802.11n) |
| WPS State: | Enabled |
| WPS Type: | PBC |
| WMM QoS: | Enabled |
| WMM Power Save: | Enabled |

## Modem Utilization

Click **Modem Utilizations** from any Status screen to generate the Modem Utilization screen. This table displays the Modem Router's modem statistics, including wireless memory used, LAN TCP settings, and, at the bottom of the screen, a LAN device session log. There are no user-configurable options in this screen.



Modem Utilization

Modem Memory

| Memory | Status |
|---|---|
| Total Memory: | 59MB RAM |
| Memory Used: | 44% |
| Memory Status: | OK |
| Recommended Action: | NONE |

Modem Sessions

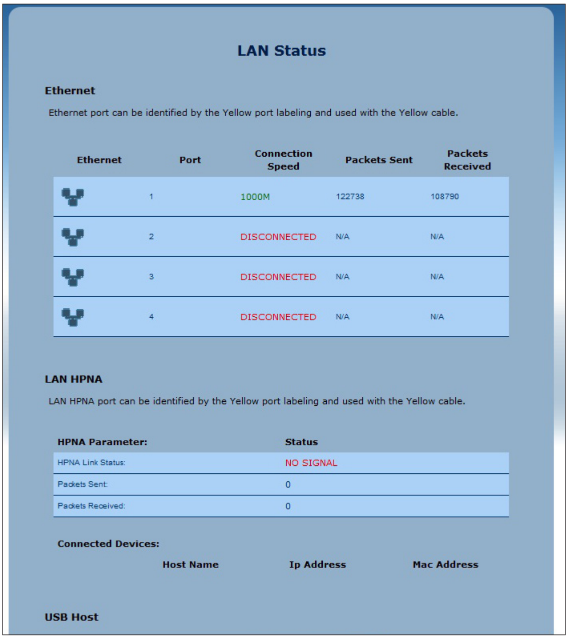
| Session | Status |
|---|---|
| Maximum Number of Sessions: | 8192 |
| LAN TCP Sessions: | 11 |
| LAN UDP Sessions: | 17 |
| Modem Sessions: | 17 |
| Total Open Sessions: | 28 |
| Session Status: | OK |
| Recommended Action: | NONE |

LAN Device Session Log

| | Device Name | IP Address | No. Of Open Session |
|---|---|---|---|
| 🖥 | admin-PC | 192.168.0.7 | 11 |

## LAN Status

Click **LAN Status** from any Status screen to generate the LAN Status screen. This table displays the Modem Router's LAN (local network) statistics, including Ethernet connections, HPNA link status, and various networked device details. There are no user-configurable options in this screen.



LAN Status

**Ethernet**

Ethernet port can be identified by the Yellow port labeling and used with the Yellow cable.

| Ethernet | Port | Connection Speed | Packets Sent | Packets Received |
|---|---|---|---|---|
|  | 1 | 1000M | 122738 | 108790 |
|  | 2 | DISCONNECTED | N/A | N/A |
|  | 3 | DISCONNECTED | N/A | N/A |
|  | 4 | DISCONNECTED | N/A | N/A |

**LAN HPNA**

LAN HPNA port can be identified by the Yellow port labeling and used with the Yellow cable.

| HPNA Parameter: | Status |
|---|---|
| HPNA Link Status: | NO SIGNAL |
| Packets Sent: | 0 |
| Packets Received: | 0 |

**Connected Devices:**

| Host Name | Ip Address | Mac Address |
|---|---|---|

**USB Host**

# Specifications

# A

## General

### Model Number

V1000H (Wireless VDSL Modem Router)

### Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX)
IEEE 802.3ab (1000BaseTX)
IEEE 802.11b/g/n (Wireless)
G.dmt, G.lite
t1.413
RFC 1483, 2364, 2516

### Protocol

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

### WAN

VDSL2 interface

### LAN

10/100/1000 RJ-45 switched ports

### Speed

**LAN Ethernet**: 10/100/1000 Mbps auto-sensing
**Wireless**: 802.11n 300 Mbps optimal (see "Wireless Operating Range" for details)

### Cabling Type

**Ethernet 10BaseT**: UTP/STP Category 3 or 5
**Ethernet 100BaseTX**: UTP/STP Category 5
**Ethernet 1000BaseTX**: UTP/STP Category 5

## Wireless Operating Range

### Indoors

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

### Outdoors

Up to 457M (1500 ft.) @ 300 Mbps

### Topology

Star (Ethernet)

## LED Indicators

Power, DSL, WAN Ethernet, Internet, LAN Ethernet (4), HPNA, USB, Wireless

## Environmental

### Power

External, 10V DC, 1.6A

### 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

# Notices

## Regulatory Compliance Notices

### Class B Equipment

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

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

## Modifications

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

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

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

**1**. This device may not cause harmful interference;

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

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

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

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

## GPL (General Public License)

This product includes software code developed by third parties, including software code subject to the enclosed GNU General Public License (GPL) or GNU Lesser General Public License (LGPL). The GPL Code and LGPL Code used in this product are distributed WITHOUT ANY WARRANTY and are subject to the copyrights of the authors, and to the terms of the applicable licenses included in the download. For details, see the GPL Code and LGPL Code for this product and the terms of the GPL and the LGPL, which are available on the enclosed product disk and can be accessed by inserting the disk into your CD-ROM drive and opening the “GPL.exe” file.

# Limited Warranty

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

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

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

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

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

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

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

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

**WARRANTIES EXCLUSIVE**: IF AN ACTIONTEC ELECTRONICS' PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT ACTIONTEC ELECTRONICS' OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, TERMS OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ACTIONTEC ELECTRONICS NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

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

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

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

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

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