Actiontec®

# Wireless Router

Model # R3000

User Guide v1

# Table of Contents

# Introduction 1

Thank you for choosing the R3000. With its powerful wireless N radio, gigabit Ethernet switch, and WAN port, as well as its dual-core processor and support for HPNA, the R3000 will propel you to new speeds as you traverse the Internet. We are sure the R3000 will provide you with years of hassle-free performance.

## Minimum System Requirements

- 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)
- 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
- 802.11n/ac support
- WPS support
- Advanced firewall
- ALG

## Getting to Know the R3000

This section contains a quick description of the R3000's lights, ports, etc.
The R3000 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 R3000 features 11 LEDs: Power, WAN Ethernet, Internet, Ethernet (4), USB, 2.4G WiFi, 5G WiFi and WPS Push Button.

### *Power*

The Power LED displays the R3000's current status. If the Power LED glows steadily green, the R3000 is receiving power and fully operational. When the Power LED is rapidly flashing, the R3000 is initializing. If the Power LED is glows red when the Power cord is plugged in, the R3000 has suffered a critical error and technical support should be contacted. If the Power LED is flashing red, the R3000 is performing a firmware update.

### *WAN Ethernet*

When the WAN Ethernet LED glows steadily, the R3000 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 R3000 is connected to the DSL provider. When it flashes, data traffic is passing across the R3000.

### *LAN Ethernet*

The LAN Ethernet LEDs illuminate when the R3000 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.

### *USB*

The USB LED illuminates when a USB device is connected via the R3000'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 R3000 is connected wirelessly, assuming the R3000's Wireless feature is turned on.

### *WPS Button*

The WPS button activates WPS (WiFi Protected Setup) on the R3000. To use WPS, press the WPS button on the R3000, then, within two minutes, press the WPS button on a device you wish to connect to the R3000's wireless network. The device will automatically join the R3000's wireless network. Repeat for other wireless devices.

## Rear Panel

The rear panel of the R3000 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 R3000 to a telephone line connection.

### *HPNA Port*

The HPNA port is used to connect the R3000 to an HPNA connection via coaxial cable.

### *LAN Ethernet Ports (4)*

The LAN Ethernet ports are used to connect computers to the R3000 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 R3000 to a WAN via an Ethernet cable.

### *USB Port*

The USB port is used to connect the R3000 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 R3000's factory default settings. To reset the R3000, 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 R3000.

**WARNING**! Do not unplug the Power cord from the R3000 during the reset process. Doing so may result in permanent damage to the R3000.

# Performing a Quick Setup

# 2

This chapter is a guide through a quick set up of the R3000, including how to connect the R3000 to the ISP.

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

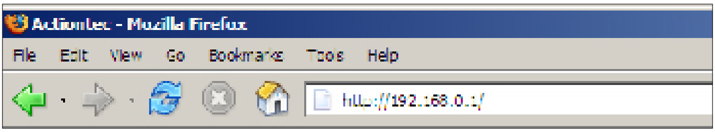
## Accessing Quick Setup Screens

To access the Quick Setup screens:

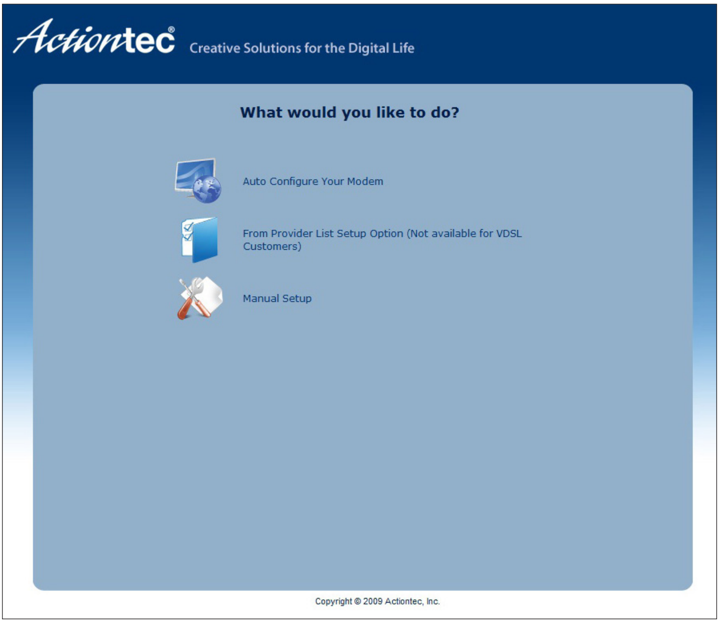
1. Open a Web browser. In the "Address" text box, type:

   `http://192.168.0.1`

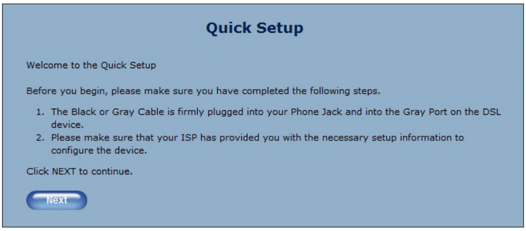
   then press **Enter** on the keyboard.



**2.** Another screen appears. Click **Manual Setup for Internet Access**.


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 © 2009 Actiontec, Inc.

**3.** Follow the instructions in the "Quick Setup" screen, then click **Next**.



Quick Setup

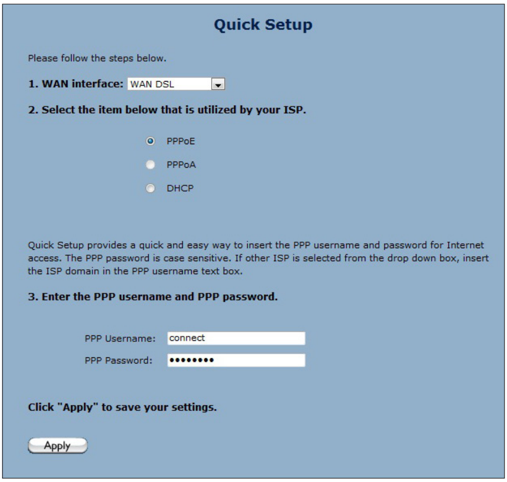
Welcome to the Quick Setup

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.

**4.** At the top of the next window, select **the type of connection used by the ISP.**



Quick Setup

Please follow the steps below.

1. WAN interface: WAN DSL

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

● PPPoE
○ PPPoA
○ DHCP

Quick Setup provides a quick and easy way to insert the PPP username and password for Internet access. The PPP password is case sensitive. If other ISP is selected from the drop down box, insert the ISP domain in the PPP username text box.

3. Enter the PPP username and PPP password.

PPP Username: connect
PPP Password: ••••••••

Click "Apply" to save your settings.

**5.** If PPPoA or PPPoE was selected in step 4, the default user name and password are entered in the appropriate text boxes.

If "DHCP" was selected, go to step 5.

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

**7.** The Power light flashes rapidly while the R3000 restarts, then glows steadily green when fully operational. The Internet light will also glow steadily green. The R3000 is now configured and users can start surfing the Internet.
If an error appears, stating the Web browser was unable to connect to the Internet, check the configuration settings. Ensure all the information required by the ISP is entered correctly.

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

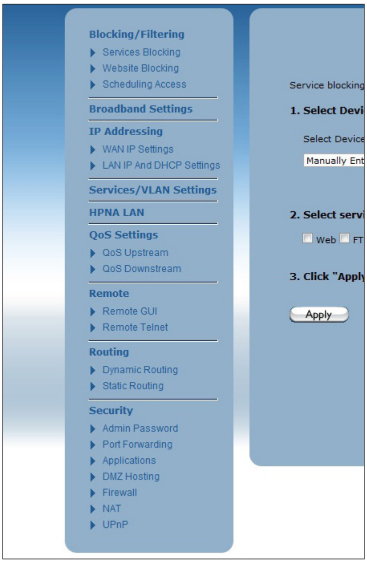
Once the R3000 has rebooted, the new user name and password are active. To access the R3000's Web Configuration screens, the new user name and password must be entered.

## Changing the Password

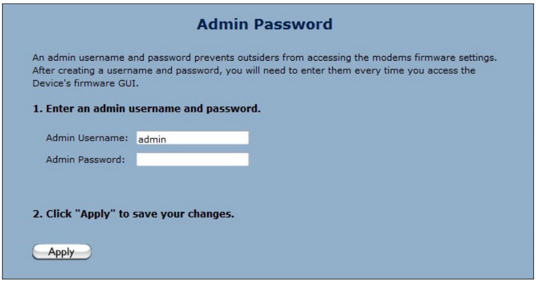
To create or change the password allowing access to the R3000's Web Configuration screens, follow these instructions:

1. From the "Home" screen, select **Advanced Setup**.

2. The "Advanced Setup" screen appears. Select "Admin Password" from the menu on the left side of the screen (underneath "Security").



3. The "Admin Password" screen appears. Enter a new user name and password in the appropriate text boxes. Make sure to write down the user name and password and keep it in a secure location. They will be needed to access the R3000's Web Configuration screens in the future.



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.

# Configuring Wireless Settings

# 3

This chapter explains the options provided in the Wireless section of the R3000's firmware, including setting up wireless security and WPS.

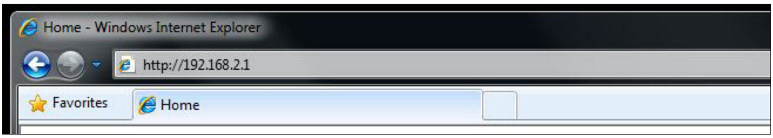
## Accessing Wireless Settings

To access the Wireless screens:

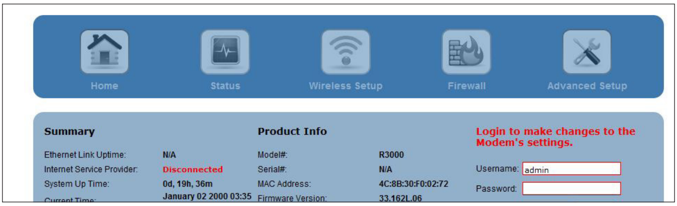
1. Open a Web browser. In the Address text box, type:

   ```
   http://192.168.2.1
   ```

   then press **Enter** on the keyboard.



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



Summary

| | |
|---|---|
| Ethernet Link Uptime: | N/A |
| Internet Service Provider: | Disconnected |
| System Up Time: | 0d, 19h, 36m |
| Current Time: | January 02 2000 03:35 |

Product Info

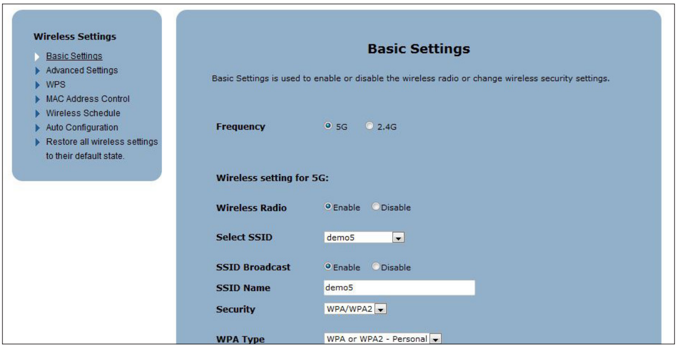
| | |
|---|---|
| Model#: | R3000 |
| Serial#: | N/A |
| MAC Address: | 4C:8B:30:F0:02:72 |
| Firmware Version: | 33.162L.06 |

Login to make changes to the Modem's settings.

Username: admin

Password:

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



Basic Settings

Basic Settings is used to enable or disable the wireless radio or change wireless security settings.

Frequency ● 5G ○ 2.4G

Wireless setting for 5G:

Wireless Radio ● Enable ○ Disable

Select SSID demo5

SSID Broadcast ● Enable ○ Disable

SSID Name demo5

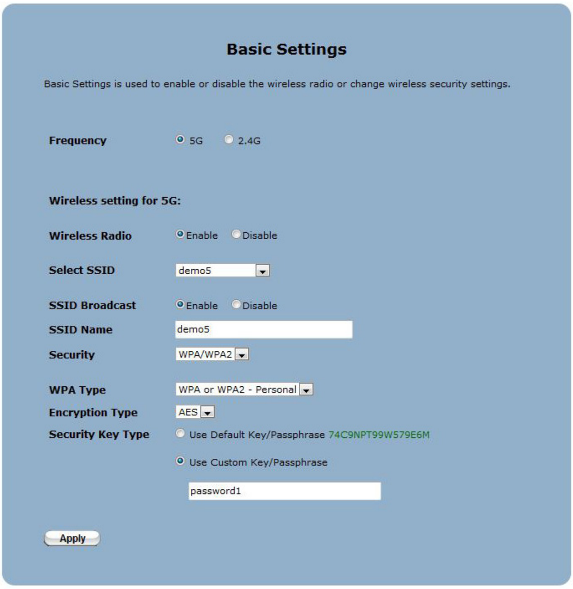
Security WPA/WPA2

WPA Type WPA or WPA2 - Personal

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 wireless security settings.

Frequency ● 5G ○ 2.4G

Wireless setting for 5G:

Wireless Radio ● Enable ○ Disable

Select SSID: demo5

SSID Broadcast ● Enable ○ Disable

SSID Name: demo5

Security: WPA/WPA2

WPA Type: WPA or WPA2 - Personal

Encryption Type: AES

Security Key Type ○ Use Default Key/Passphrase 74C9NPT99W579E6M

● Use Custom Key/Passphrase

password1

To configure the basic wireless settings of the R3000:

1. Select a frequency at which the wireless signal will be broadcast (5G or 2.4G).
2. Click in the *Enable* button next to Wireless Radio.
3. Enter an SSID name in the appropriate text box. Alternatively, select a name from the drop-down menu by clicking on the down arrow.
4. Enable/disable SSID broadcasting by clicking in the appropriate button next to *SSID Broadcasting*. Enabling this option broadcasts the name of the network to any wireless devices in range; disabling prevents the network name from being detected by wireless devices.

5. Select a WPA type (WPA2-Personal, WPA- or WPA2-Personal, or WPA-Personal).

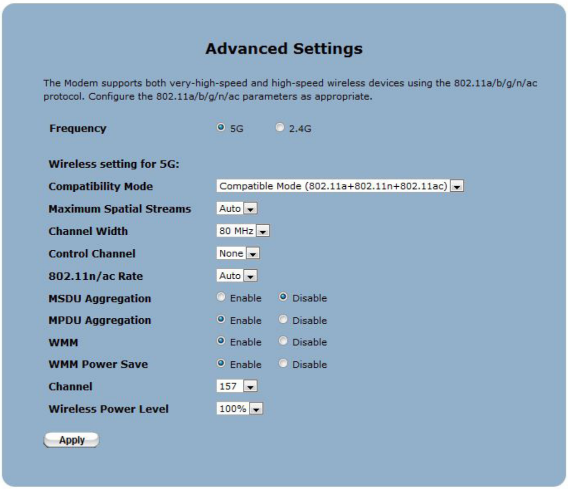
6. To use the default security key, click in the button next to *Use Default Key/ Passphrase*. Make sure to write the passkey down (displayed in green text), as it will be needed to access the wireless network.

7. To create a custom password, click in the button next to *Use Custom Key/ Passphrase*, then enter the password in the text box at the bottom of the screen.

8. Click **Apply**.

## Advanced Settings

Click **Advanced Settings** from any Wireless screen to generate the *Advanced Settings* screen. After making any changes in this screen, click **Apply**.



**Advanced Settings**

The Modem supports both very-high-speed and high-speed wireless devices using the 802.11a/b/g/n/ac protocol. Configure the 802.11a/b/g/n/ac parameters as appropriate.

| | | |
|---|---|---|
| **Frequency** | ● 5G | ○ 2.4G |
| **Wireless setting for 5G:** | | |
| **Compatibility Mode** | Compatible Mode (802.11a+802.11n+802.11ac) ▾ | |
| **Maximum Spatial Streams** | Auto ▾ | |
| **Channel Width** | 80 MHz ▾ | |
| **Control Channel** | None ▾ | |
| **802.11n/ac Rate** | Auto ▾ | |
| **MSDU Aggregation** | ○ Enable | ● Disable |
| **MPDU Aggregation** | ● Enable | ○ Disable |
| **WMM** | ● Enable | ○ Disable |
| **WMM Power Save** | ● Enable | ○ Disable |
| **Channel** | 157 ▾ | |
| **Wireless Power Level** | 100% ▾ | |

### Frequency

To change the wireless network's frequency, click in the appropriate button.

### Compatibility Mode

Select the wireless networking standard with which the network will work. Selections include 802.11a, n, and ac.

### Channel Width

Select the channel width. Options include 20, 40, and 80MHz.

### MDSU Aggregation

Enable/disable MDSU aggragation by clicking in the appropriate button.

### MPDU Aggregation

Enable/disable MPDU aggragation by clicking in the appropriate button.

### WMM

Enable/disable WMM by clicking in the appropriate button.

### WMM Power Save

Enable/disable WMM Power Save by clicking in the appropriate button.

### Channel

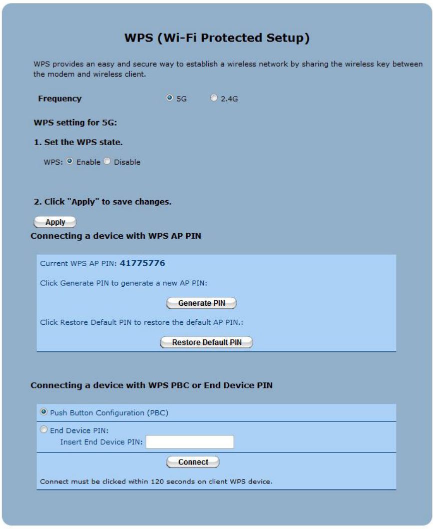
Select a channel number by clicking on the down arrow, then making a selection from the drop-down menu.

### Wireless Power Level

Select a wireless power level by clicking on the down arrow, then making a selection from the drop-down menu.

## 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 R3000 and other wireless devices. To begin, select the frequency of the network, enable WPS by clicking in the appropriate button, then click **Apply**.



**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.

**Frequency** ● 5G ○ 2.4G

**WPS setting for 5G:**

**1. Set the WPS state.**

WPS: ● Enable ○ Disable

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

**Connecting a device with WPS AP PIN**

Current WPS AP PIN: **41775776**

Click Generate PIN to generate a new AP PIN:

Click Restore Default PIN to restore the default AP PIN.:

**Connecting a device with WPS PBC or End Device PIN**

● Push Button Configuration (PBC)

○ End Device PIN:
Insert End Device PIN:

Connect must be clicked within 120 seconds on client WPS device.

There are three ways to set up WPS on the R3000: AP PIN, Push Button (PBC), and End Device PIN.

### AP Pin

1. Use the current WPS AP PIN (displayed in blue), or generate another PIN by clicking **Generate PIN**. Clicking **Restore Default PIN** uses the factory default PIN.

2. Write the PIN down.

3. Enter the PIN on another wireless device's WPS AP PIN configuration to have that device join the wireless network.

### Push Button (PBC)

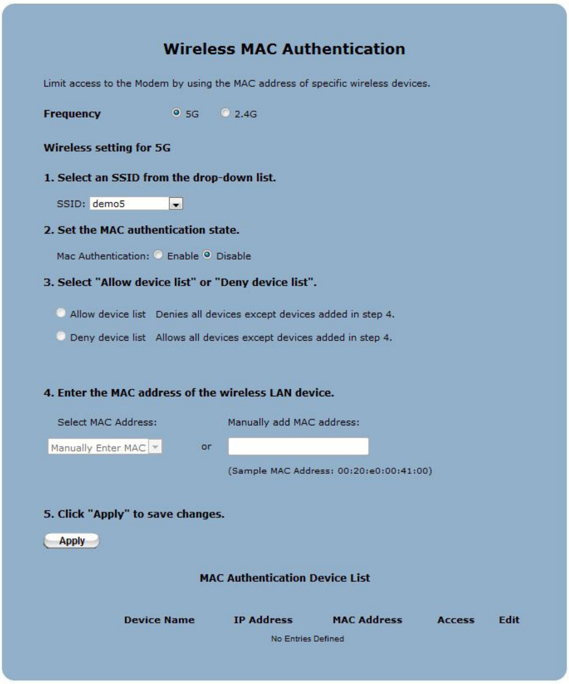
1. Click in the button next to *Push Button Condfiguration (PBC)*.
2. Click **Connect**.
3. Press the PBC-compatible button on another wireless device within two minutes to have that device join the wireless network.

### End Device PIN

1. Click in the button next to *End Device PIN*.
2. Enter the end device's PIN in the appropriate text box.
3. Click **Connect**. The R3000 joins the existing wireless network.

## Wireless MAC Authentication

Click **MAC Address Control** from any Wireless screen to generate the *Wireless MAC Authentication* screen. From here, the user can allow or deny access to the R3000's wireless network for wireless devices using the devices' MAC address. A MAC address is a unique code that identifies every wireless-capable device (printers, computers, tablets, smartphones, etc.).



**Wireless MAC Authentication**

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

**Frequency** ● 5G ○ 2.4G

**Wireless setting for 5G**

**1. Select an SSID from the drop-down list.**

SSID: demo5

**2. Set the MAC authentication state.**

Mac Authentication: ○ Enable ● Disable

**3. Select "Allow device list" or "Deny device list".**

○ Allow device list Denies all devices except devices added in step 4.

○ Deny device list Allows all devices except devices added in step 4.

**4. Enter the MAC address of the wireless LAN device.**

Select MAC Address: Manually Enter MAC or Manually add MAC address:

(Sample MAC Address: 00:20:e0:00:41:00)

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

**MAC Authentication Device List**

| Device Name | IP Address | MAC Address | Access | Edit |
|---|---|---|---|---|

No Entries Defined

To set up authentication on the R3000's wireless network using MAC addresses:

1. Select the wireless network frequency by clicking in the appropriate button.
2. Select a wireless network name from the SSID drop-down list.
3. Turn on MAC authentication by clicking in the *Enable* button.

4. Select a filtering method. Clicking it the 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. Clicking the button next to *Deny Device List* creates a list of wireless devices that cannot join the wireless network–all other devices not on the list will be able to join.

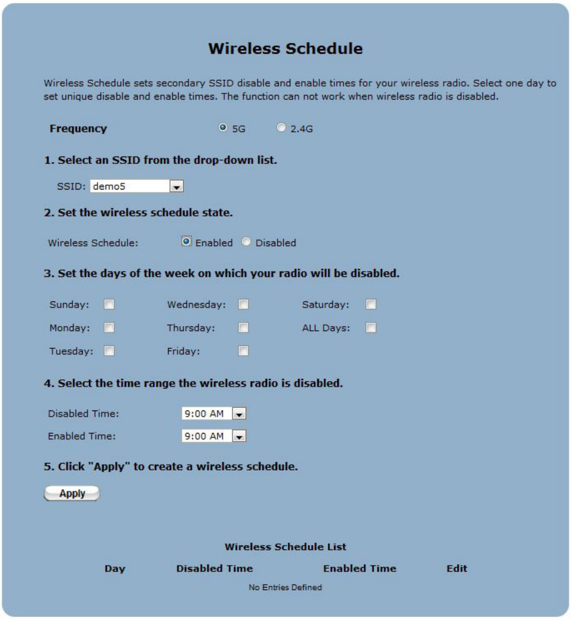
5. Begin creating a list by selecting a wireless device that appears on the *Select Device Name* drop-down menu. Alternatively, enter a device's MAC address in the *Manually Add MAC Address* text box.

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

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

## Wireless Schedule

Click **Wireless Schedule** in any Wireless screen to generate the *Wireless Schedule* screen. Wireless Schedule provides a way to control when a wireless network created on the R3000 is operational.



**Wireless Schedule**

Wireless Schedule sets secondary SSID disable and enable times for your wireless radio. Select one day to set unique disable and enable times. The function can not work when wireless radio is disabled.

**Frequency** ● 5G ○ 2.4G

**1. Select an SSID from the drop-down list.**

SSID: demo5

**2. Set the wireless schedule state.**

Wireless Schedule: ● Enabled ○ Disabled

**3. Set the days of the week on which your radio will be disabled.**

| | | | | | |
|---|---|---|---|---|---|
| Sunday: | □ | Wednesday: | □ | Saturday: | □ |
| Monday: | □ | Thursday: | □ | ALL Days: | □ |
| Tuesday: | □ | Friday: | □ | | |

**4. Select the time range the wireless radio is disabled.**

Disabled Time: 9:00 AM

Enabled Time: 9:00 AM

**5. Click "Apply" to create a wireless schedule.**

**Wireless Schedule List**

| Day | Disabled Time | Enabled Time | Edit |
|---|---|---|---|

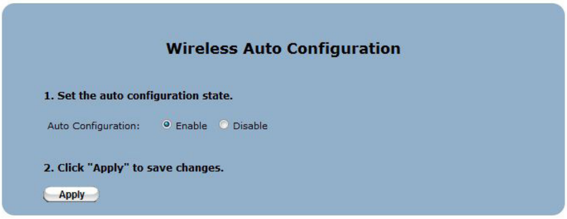
No Entries Defined

To set up a wireless network schedule:

1. Select the wireless network frequency by clicking in the appropriate button.
2. Select the SSID (wireless network) to be scheduled from the *SSID* drop-down menu.
3. Click in the *Wireless Schedule - Enable* button.
4. Select the day(s) during which the selected wireless network will be disabled by clicking in the appropriate check boxes.
5. Select the daily time range by selecting a *Disabled Time* and *Enabled Time* from the appropriate drop-down menus. The wireless network will be disabled between these times on the days selected in step 4.
6. Click **Apply**. The schedule appears in the *Wireless Schedule List* at the bottom of the screen.
7. Repeat steps 1 through 6 to create more wireless network schedules.

## Wireless Auto Configuration

Click **Wireless Auto Configuration** in any Wireless screen to generate the *Wireless Auto Configuration* screen. Click in the *Enable* button to enable wireless auto configuration, then click **Apply**.


Wireless Auto Configuration

1. Set the auto configuration state.

Auto Configuration: ● Enable ○ Disable

2. Click "Apply" to save changes.

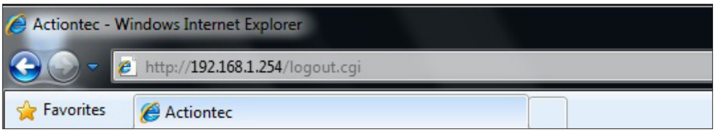
# Configuring Firewall Settings 4

This chapter will explain the options provided in the Firewall section of the R3000's firmware, including various firewall options, port forwarding, and DMZ hosting.

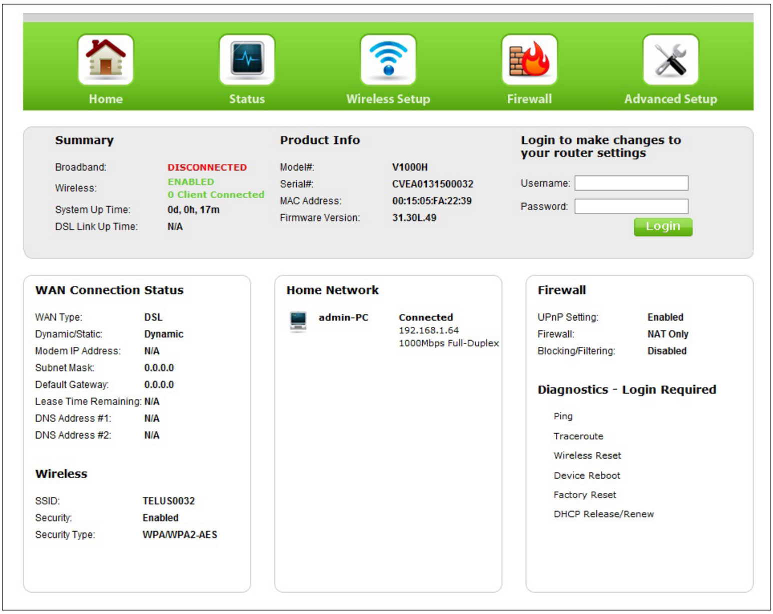
## Accessing Firewall Settings

To access the Firewall screens:

1. Open a Web browser. In the "Address" text box, type:
   `http://192.168.1.254`
   then press **Enter** on the keyboard.


Actiontec - Windows Internet Explorer
http://192.168.1.254/logout.cgi
Favorites
Actiontec

2. The Router's Home screen appears. Enter your user name and password, then click the "Firewall" icon from the row of icons at the top of the screen.



**Summary**

Broadband: DISCONNECTED
Wireless: ENABLED
0 Client Connected
System Up Time: 0d, 0h, 17m
DSL Link Up Time: N/A

**Product Info**

Model#: V1000H
Serial#: CVEA0131500032
MAC Address: 00:15:05:FA:22:39
Firmware Version: 31.30L.49

**Login to make changes to your router settings**

Username:
Password:

**WAN Connection Status**

WAN Type: DSL
Dynamic/Static: Dynamic
Modem IP Address: N/A
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
Lease Time Remaining: N/A
DNS Address #1: N/A
DNS Address #2: N/A

**Wireless**

SSID: TELUS0032
Security: Enabled
Security Type: WPA/WPA2-AES

**Home Network**

admin-PC Connected
192.168.1.64
1000Mbps Full-Duplex

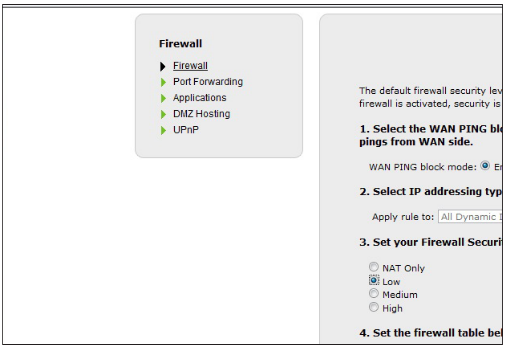
**Firewall**

UPnP Setting: Enabled
Firewall: NAT Only
Blocking/Filtering: Disabled

**Diagnostics - Login Required**

Ping
Traceroute
Wireless Reset
Device Reboot
Factory Reset
DHCP Release/Renew

3. The "Firewall" screen appears, with various firewall options listed in the menu on the left side of the screen.



The default firewall security lev
firewall is activated, security is

1. Select the WAN PING bl
pings from WAN side.

WAN PING block mode: ● E

2. Select IP addressing typ

Apply rule to: All Dynamic I

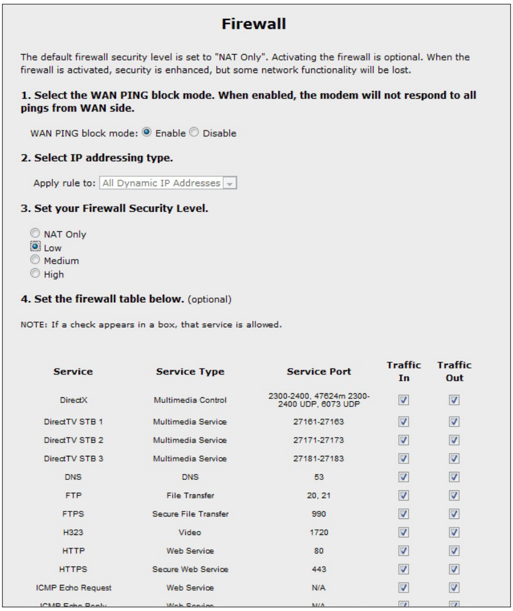
3. Set your Firewall Securi

○ NAT Only
● Low
○ Medium
○ High

4. Set the firewall table be

# Firewall

Click **Firewall** from any Firewall screen to generate the “Firewall” screen. This screen allows you to configure the firewall settings of the Router. If you make changes in this screen, click **Apply** at the bottom of the screen to save them.



## Firewall

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

**1. Select the WAN PING block mode. When enabled, the modem will not respond to all pings from WAN side.**

WAN PING block mode: ● Enable ○ Disable

**2. Select IP addressing type.**

Apply rule to: All Dynamic IP Addresses

**3. Set your Firewall Security Level.**

○ NAT Only
● Low
○ Medium
○ High

**4. Set the firewall table below.** (optional)

NOTE: If a check appears in a box, that service is allowed.

| Service | Service Type | Service Port | Traffic In | Traffic Out |
|---|---|---|---|---|
| DirectX | Multimedia Control | 2300-2400, 47624m 2300-2400 UDP, 6073 UDP | ☑ | ☑ |
| DirectTV STB 1 | Multimedia Service | 27161-27163 | ☑ | ☑ |
| DirectTV STB 2 | Multimedia Service | 27171-27173 | ☑ | ☑ |
| DirectTV STB 3 | Multimedia Service | 27181-27183 | ☑ | ☑ |
| DNS | DNS | 53 | ☑ | ☑ |
| FTP | File Transfer | 20, 21 | ☑ | ☑ |
| FTPS | Secure File Transfer | 990 | ☑ | ☑ |
| H323 | Video | 1720 | ☑ | ☑ |
| HTTP | Web Service | 80 | ☑ | ☑ |
| HTTPS | Secure Web Service | 443 | ☑ | ☑ |
| ICMP Echo Request | Web Service | N/A | ☑ | ☑ |
| ICMP Echo Reply | Web Service | N/A | ☑ | ☑ |

### WAN Ping Block Mode

Click the “Enable” radio button next to “WAN PING block mode” to activate the WAN Ping Block Mode. This will block all pings originating from the WAN (i.e., the Internet) side of the network. Clicking “Disable” turns off the block mode.

### IP Addressing Type

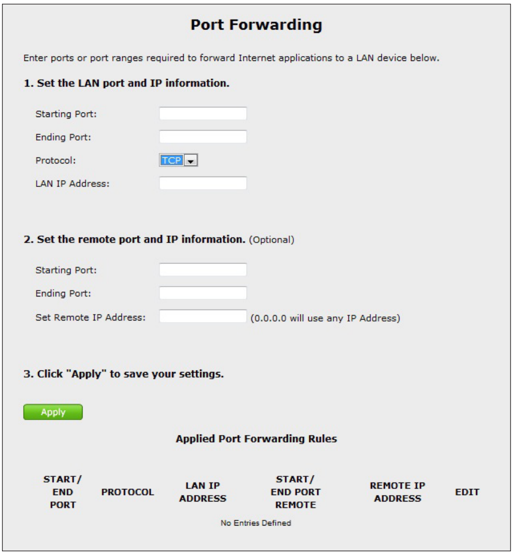
This option is non-configurable and always set to “All Dynamic IP Addresses.”

### Firewall Security Level

Select the level of firewall security level here, by clicking in the appropriate radio button. “None” provides no firewall security, while “Low,” “Medium,” and “High” provide different levels of security, as displayed in the Firewall table in the lower part of the screen. Additionally, after choosing a level of firewall security, you can manually allow (by clicking in a check box to generate a check mark) or deny (by clicking in a check box to delete a check mark) selected Internet services listed in the Firewall table.

## Port Forwarding

Activating “Port Forwarding” allows the network to be exposed to the Internet in certain limited and controlled ways, enabling some applications to work from the local network (game, voice, and chat applications, for example), as well as allowing Internet access to servers in the local network. Click **Port Forwarding** from any Firewall screen to generate the “Port Forwarding” screen. This screen allows you to configure the port forwarding settings of the Router. If you make changes in this screen, click **Apply** at the bottom of the screen to save them.



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 | | | |

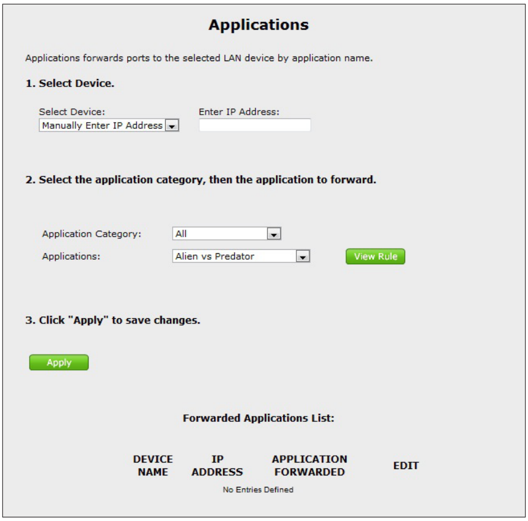
To set up port forwarding

1. Enter the LAN starting port in the "Starting Port" text box.
2. Enter the LAN ending port in the "Ending Port" text box.
3. Select a protocol from the "Protocol" drop-down list box
4. Enter the LAN IP address in the "LAN IP Address" text box.
5. If applicable, enter the remote port and IP information
6. Click **Apply** to save your changes.

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

## Applications

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



### 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

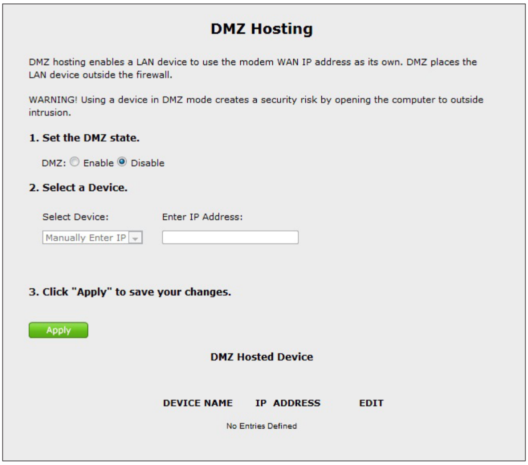
To set up a forwarded application:

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

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

## DMZ Hosting

Click **DMZ Hosting** from any Firewall screen to generate the “DMZ Hosting” screen. The DMZ (De-Militarized Zone) host feature allows one device on the network to operate outside the firewall to use an Internet service that otherwise would be blocked, or to expose a networked device to all services without restriction or security.



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 | | |

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

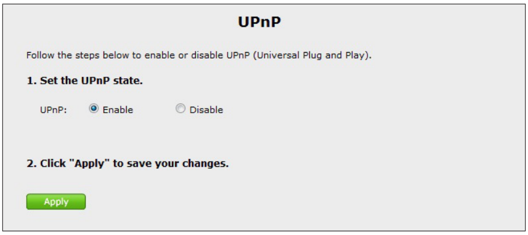
To designate a local computer as a DMZ host:

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

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

## UPnP

Click **UPnP** from any Firewall screen to generate the "UPnP" screen. UPnP (Universal Plug and Play) allows all supported devices on the Router's network to discover and interface with each other without additional configuration. To enable UPnP on the Router's network, click in the "Enable" radio button.



UPnP

Follow the steps below to enable or disable UPnP (Universal Plug and Play).

1. Set the UPnP state.

UPnP: ● Enable ○ Disable

2. Click "Apply" to save your changes.

# Configuring Advanced Setup

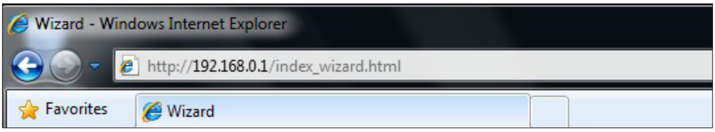
# 5

This chapter will explain the options provided in the Advanced Setup section of the R3000's firmware, including services blocking, firewall options, and setting up QoS (Quality of Service).

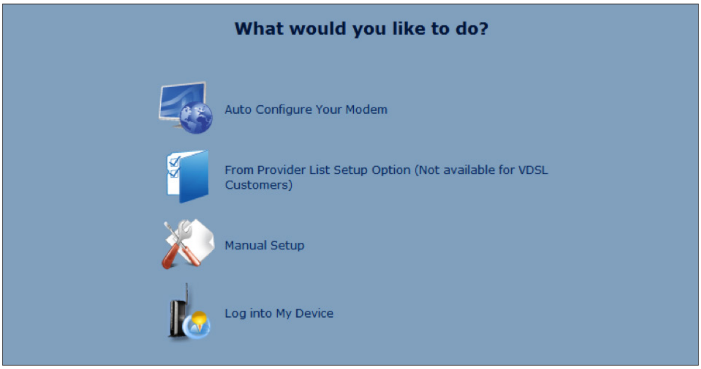
## Accessing Advanced Setup Options

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
Favorites
Wizard

2. The R3000’s host screen appears. Click **Manual Setup**.



What would you like to do?

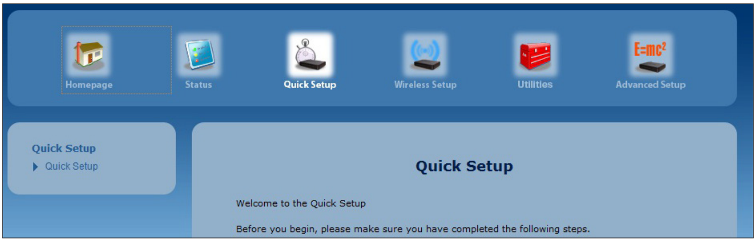
Auto Configure Your Modem

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**.

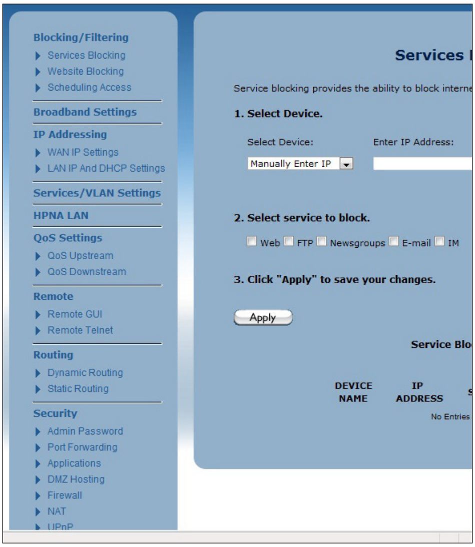


Quick Setup

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

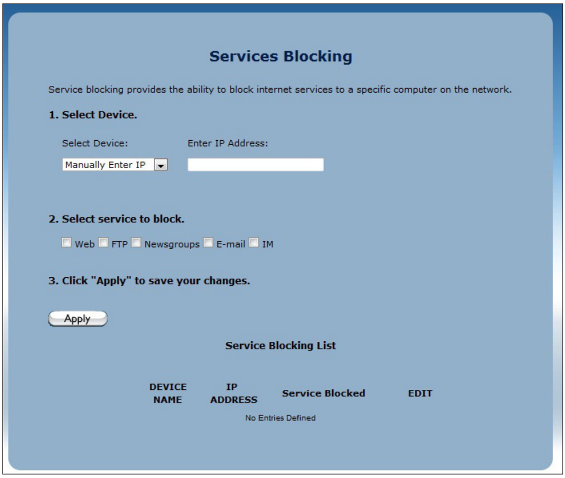
| DEVICE NAME | IP ADDRESS | S |
|---|---|---|
| | No Entries | |

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 R3000'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.

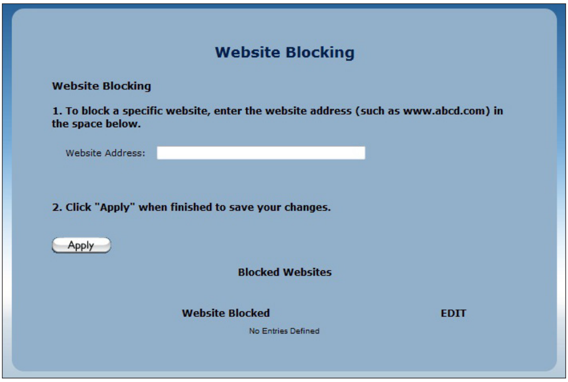
5. Repeat steps 1-4 to block services on another device on the network.

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 R3000's network from accessing particular web sites on the Internet. To set up web site blocking on the R3000'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.

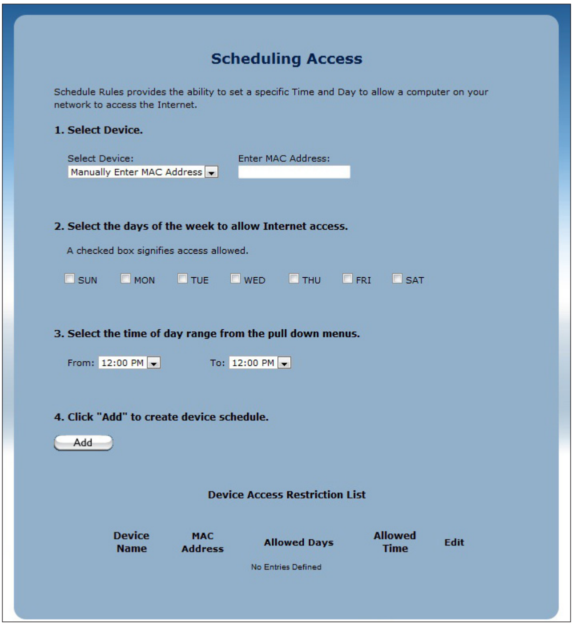
4. Repeat steps 1-3 to block other web sites from being acesssed on the R3000's network.

The web sites blocked from being accessed on the R3000's network are listed at the bottom of the screen.

## Scheduling Access

Scheduling access is used to allow a device on the R3000'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.

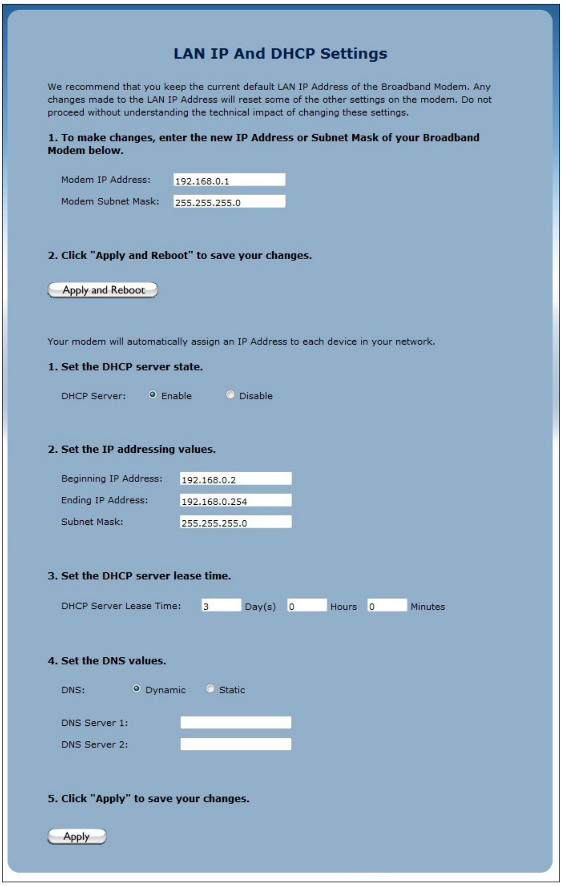
3. Select the days of the week during which you want to allow Internet access by clicking in the appropriate check box below “Select the days of the week…”
4. Set the time range during which you want to allow Internet access. This time range will apply only to the days you activated in step 3.
5. Click **Add** to create a schedule access.
6. Repeat steps 1-5 to create multiple access schedules for other devices on the R3000’s network.

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

## LAN IP and DHCP Settings

The LAN IP and DHCP Settings screen allows you to change the R3000'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 R3000 reboots with the new settings.

To change the R3000's DHCP settings:

4. Click **Enable** to activate the R3000'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.

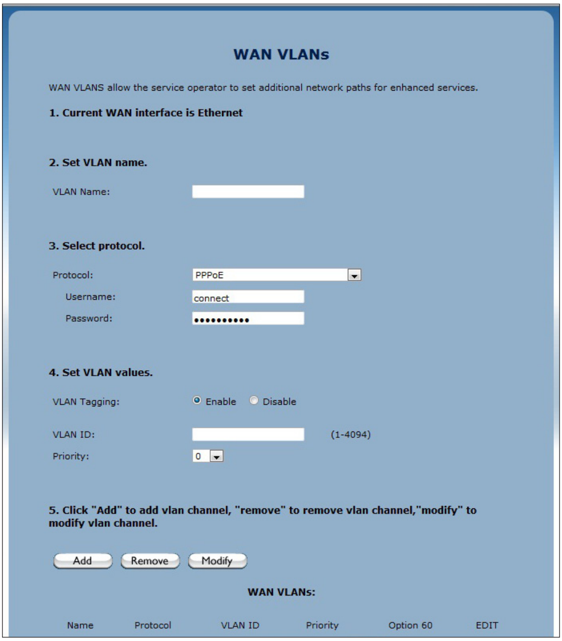
7. Set the DNS values by selecting Dynamic or Static (clicking in the appropriate radio button), then, if needed enter the IP addresses for DNS server 1 and 2.

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.

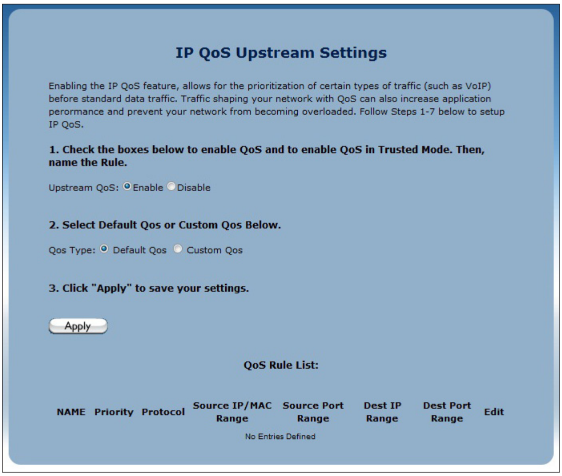
You can also delete existing VLANs by clicking **Delete**, or modify a VLAN's settings by clicking **Modify**.

## QoS Settings

The QoS Settings screens allow you to prioritize certain types of data traffic (video, for example) over other data traffic on the R3000'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.

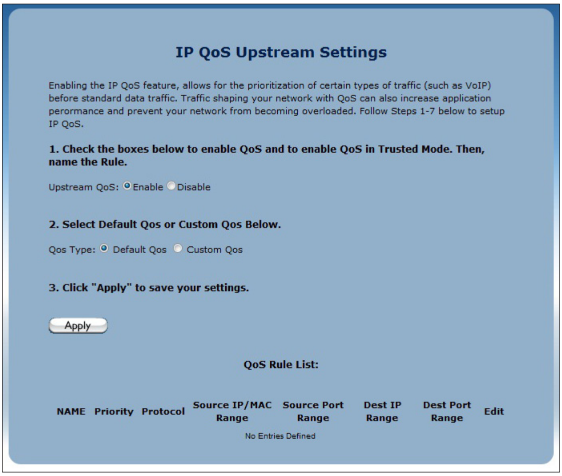
2. Select the type of QoS to enable. If selecting Custom QoS, you will have to enter a number of values: Name, Queue Priority, Reserved Bandwidth, Protocol, TOS Bit Value, Source IP or MAC address information, Destination IP Address, Netmask IP Address, and Port Pange. Do not select Custom QoS unless 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.

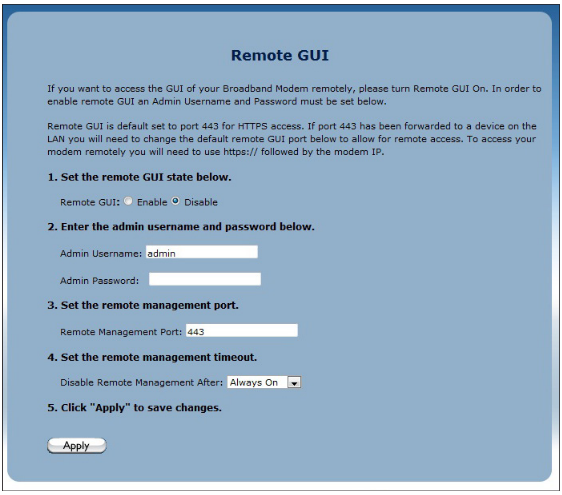
2. Select the type of QoS to enable. If selecting Custom QoS, you will have to enter a number of values: Name, Queue Priority, Reserved Bandwidth, Protocol, TOS Bit Value, Source IP or MAC address information, Destination IP Address, Netmask IP Address, and Port Pange. Do not select Custom QoS unless 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 R3000 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 R3000's IP address, a colon (:), then the port number to which the remote management port was changed.
   Example: https://192.170.1.1:234.

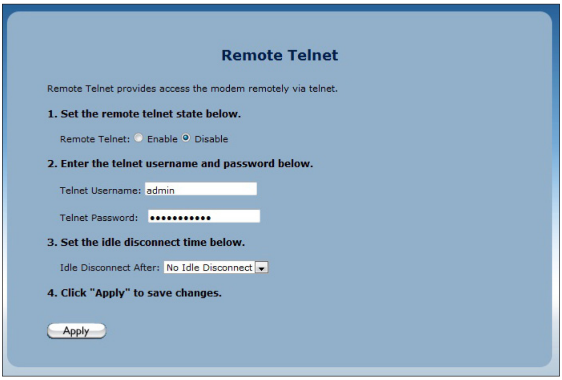
5. Select the remote management timeout. If you select one of the time periods provided in the drop-down list, remote management of the R3000 will stop after the selected time period, if no actions are detected.

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

## Remote Telnet

The Remote Telnet screen allows you to set up the R3000 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.

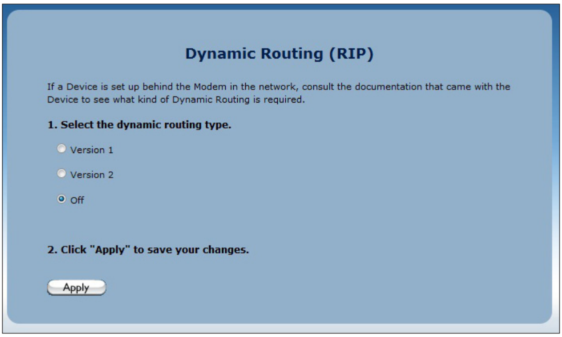
4. Select the idle disconnect time. If you select one of the time periods provided in the drop-down list, remote telnet management of the R3000 will stop after the selected time period, if no actions are detected.

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

## Dynamic Routing

The Dynamic Routing screen allows you to set up the R3000 for dynamic routing, which is useful if the R3000 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.

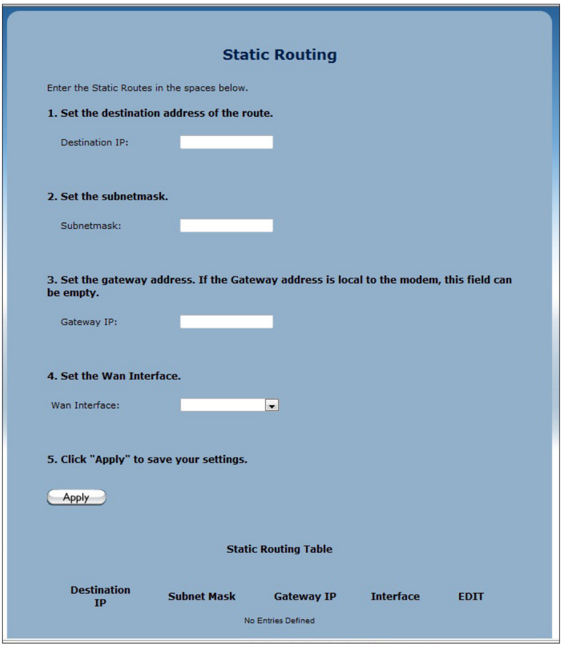
2. Select the version of dynamic routing you want to use (Version 1, Version 2) by clicking in the appropriate radio button. Consult the documentation that came with the modem set up in front of the R3000 on the network to find out which version to use.

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

## Static Routing

The Static Routing screen allows you to set up static routes on the R3000. 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 router IP address in the Router IP text box.

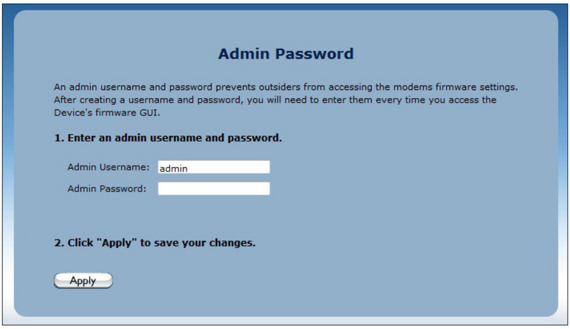
5. Select a WAN interface from the WAN Interface drop-down list.

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

## Admin Password

To change the password that allows access to the R3000'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:

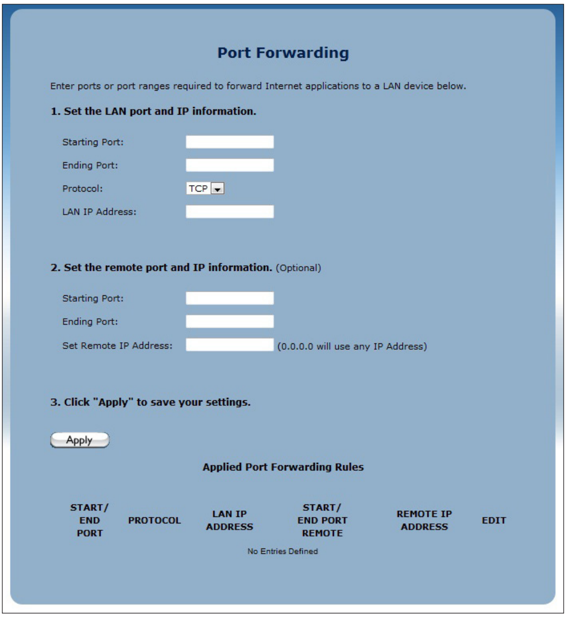
2. Click "Apply" to save your changes.

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 R3000'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.

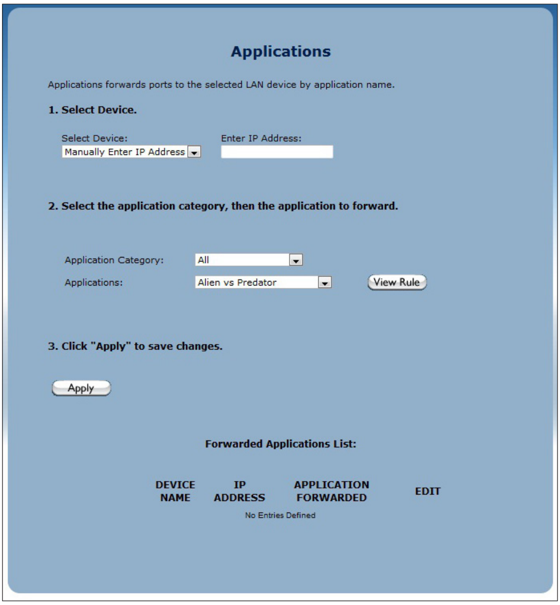
6. Click **Apply** to save your changes.

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

## Applications

The R3000 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 R3000'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

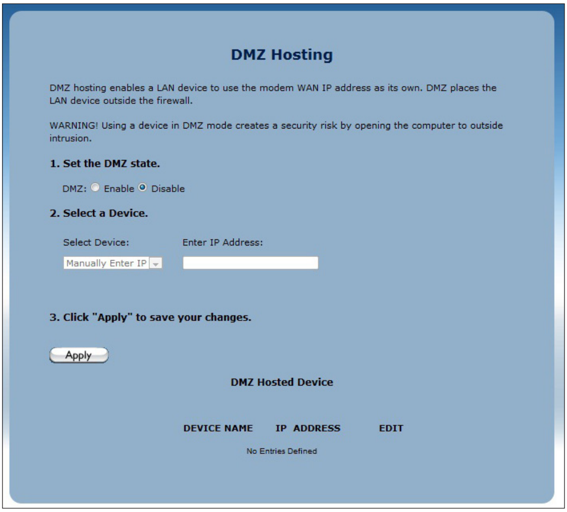
If, in step 3 of the previous procedure, User Created Rules was chosen, click Create Rule to generate a screen in which you can create a custom rule. Enter the rule name, select a protocol, and enter a port start, port end, and port map in the appropriate text boxes, then click Apply. The new rule will 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 R3000's network to be set up outside the R3000'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 R3000's network that you want use as the DMZ host. Alternatively, you can enter the device's IP address in the appropriate text box.

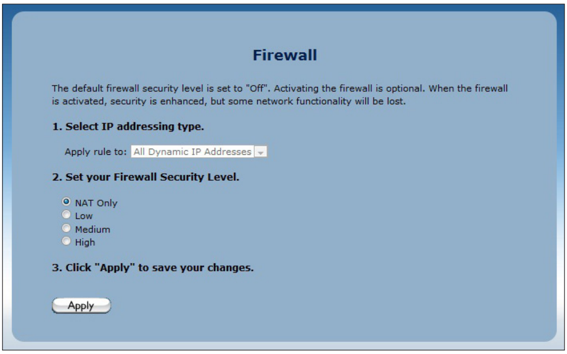
**4.** Click **Apply** to save your changes.

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 R3000'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 R3000's network from the Apply rule to drop-down list on which you want to apply the firewall.

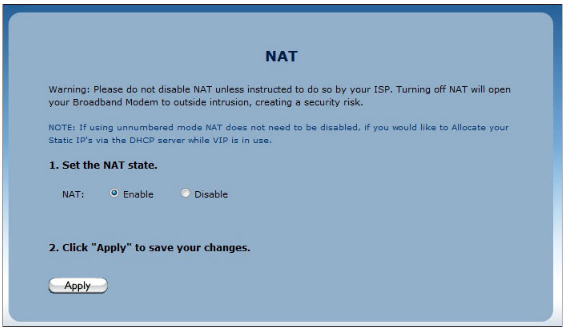
**3.** Select a firwall security level by clicking in the appropriate radio button below step 2.

**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.

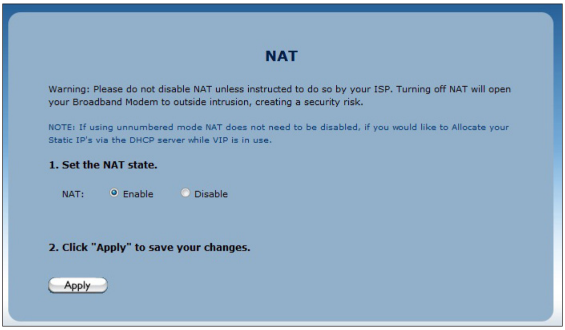
1. Set the NAT state.

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 R3000'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 R3000's Status

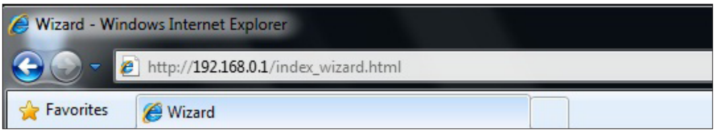
# 6

This chapter gives an overview of the various status tables provided by the R3000, which allow you check on various parameters, including WAN connections, WAN Etherent connection, and wireless status.

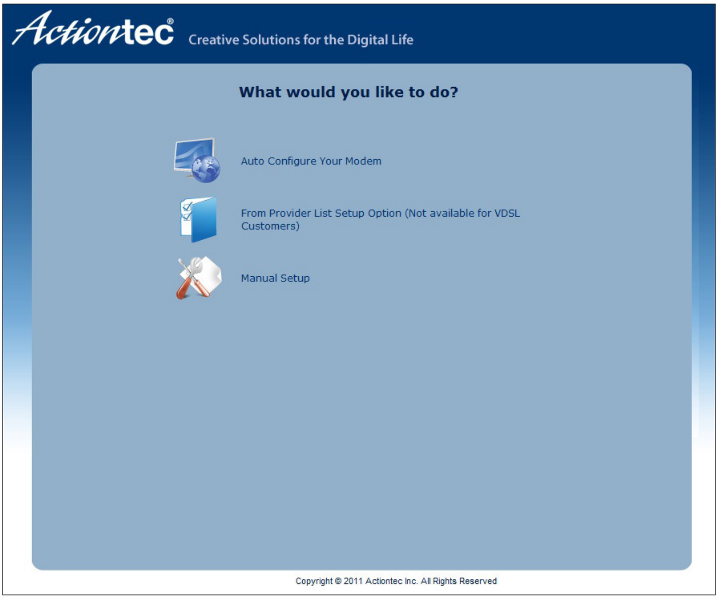
## Accessing Wireless Settings

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

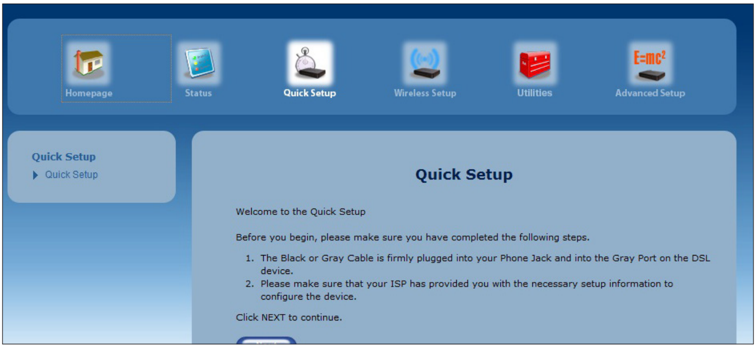
2. The R3000's host screen appears. Click **Manual Setup**.


Actiontec
Creative Solutions for the Digital Life
Auto Configure Your Modem
From Provider List Setup Option (Not available for VDSL Customers)
Manual Setup

What would you like to do?

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

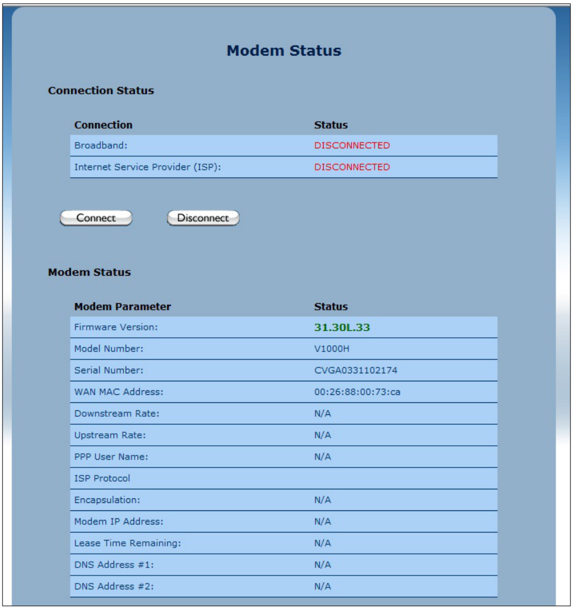
Before you begin, please make sure you have completed the following steps.

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 R3000, 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 R3000 from your service provider.



Modem Status

Connection Status

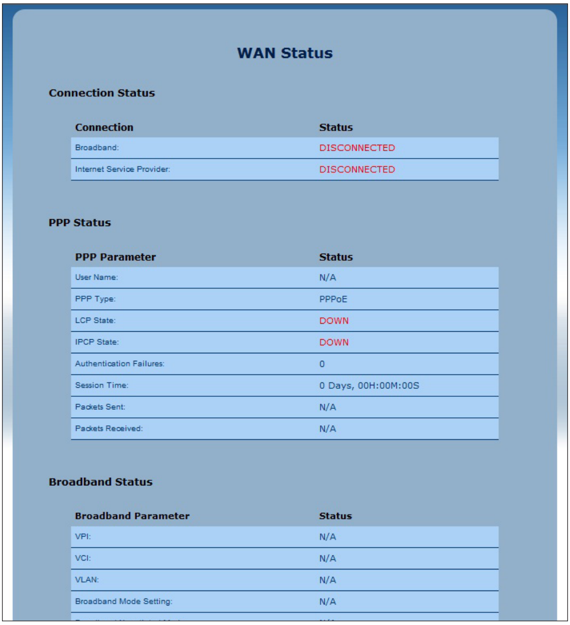
| Connection | Status |
|---|---|
| Broadband: | DISCONNECTED |
| Internet Service Provider (ISP): | DISCONNECTED |

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 R3000, 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

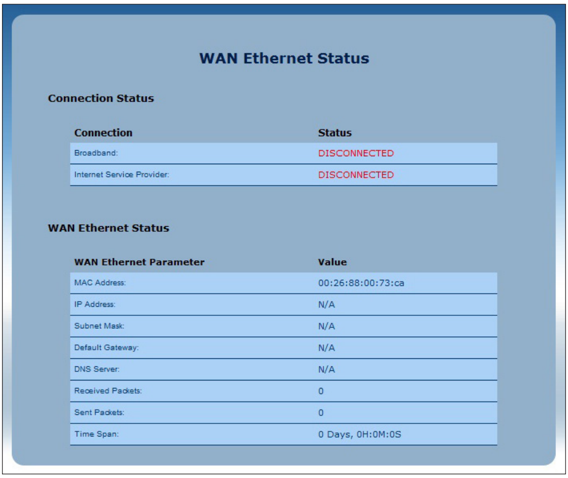
| PPP Parameter | Status |
|---|---|
| User Name: | N/A |
| PPP Type: | PPPoE |
| LCP State: | DOWN |
| IPCP State: | DOWN |
| Authentication Failures: | 0 |
| Session Time: | 0 Days, 00H:00M:00S |
| Packets Sent: | N/A |
| Packets Received: | N/A |

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 R3000, including subnet mask, default R3000, and sent packets. There are no user-configurable options in this screen.



WAN Ethernet Status

Connection Status

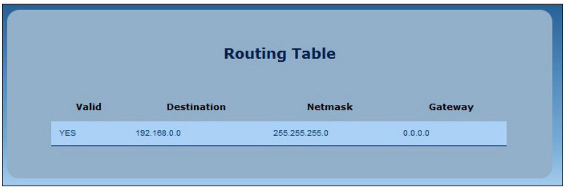
| Connection | Status |
|---|---|
| Broadband: | DISCONNECTED |
| Internet Service Provider: | DISCONNECTED |

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 R3000's routing table. There are no user-configurable options in this screen.

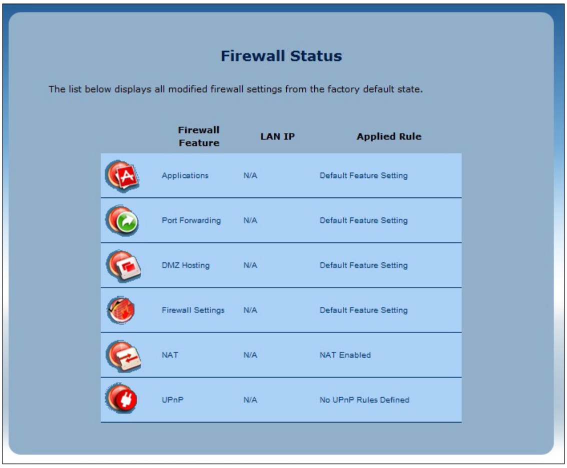


Routing Table

| 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 R3000's firewall. There are no user-configurable options in this screen. For more details, see the "Configuring the Firewall Settings" chapter of this manual.



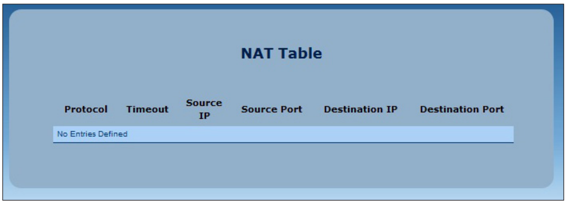
Firewall Status

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 R3000’s NAT table. There are no user-configurable options in this screen.

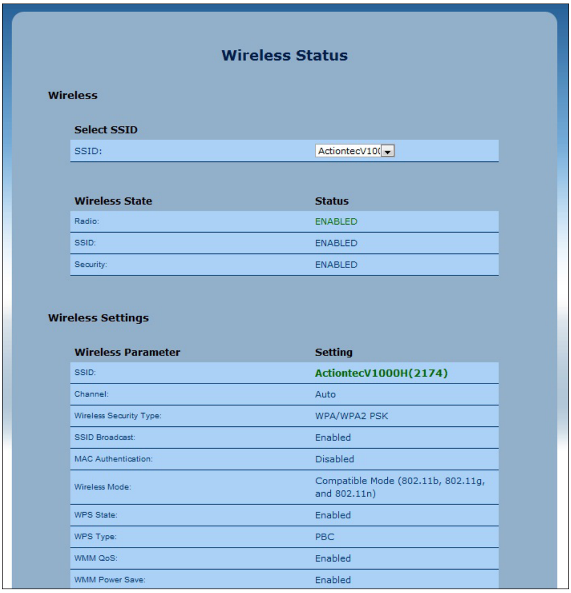


NAT Table

| 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 R3000’s wireless network statistics, including wireless security type, wireless mode, and packets received.



Wireless Status

Wireless

Select SSID

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

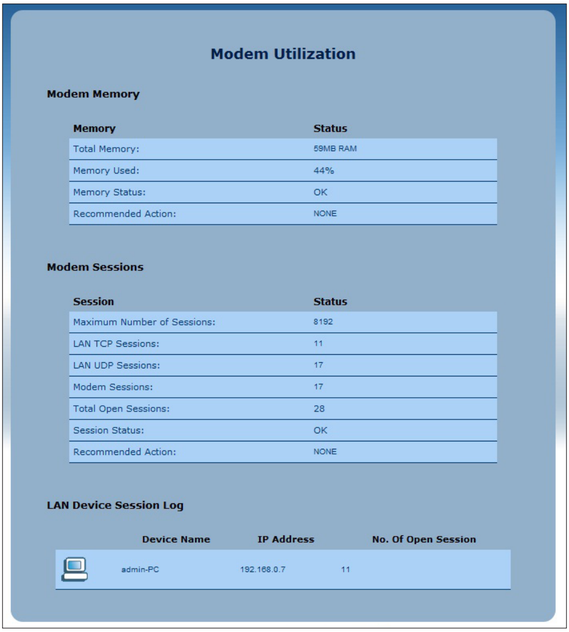
| Wireless State | Status |
|---|---|
| Radio: | ENABLED |
| SSID: | ENABLED |
| Security: | ENABLED |

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 R3000'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**

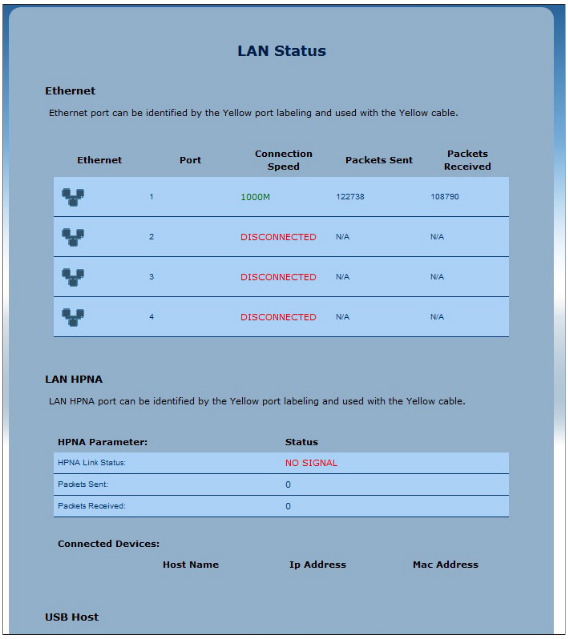
| Session | Status |
|---|---|
| Maximum Number of Sessions: | 8192 |
| LAN TCP Sessions: | 11 |
| LAN UDP Sessions: | 17 |
| Modem Sessions: | 17 |
| Total Open Sessions: | 28 |
| Session Status: | OK |
| Recommended Action: | NONE |

**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 R3000's LAN (local network) statistics, including Ethernet connections, 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

R3000

### Standards

IEEE 802.3 (10BaseT)
IEEE 802.3u (100BaseTX)
IEEE 802.3ab (1000BaseTX)
IEEE 802.11b/g/n (Wireless)
RFC 1483, 2364, 2516

### Protocol

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

### LAN

10/100/1000 RJ-45 switched ports

### Speed

**LAN Ethernet**: 10/100/1000 Mbps auto-sensing
**Wireless**: 802.11n/ac 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, WAN Ethernet, Internet, LAN Ethernet (4), HPNA, USB, Wireless

## Environmental

### Power

12V DC, 3A

### Certifications

FCC Class B, FCC Class C (part 15), 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 25 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.