

# **IMPORTANT SECURITY UPDATE**

Internet Security is a top priority at Verizon. To make sure we do all we can to protect your personal information, our wireless routers have security settings that are available to help protect your home wireless network. Using the strongest network security available will go a long way to protect your home wireless network and secure your information against unauthorized access. Verizon strongly recommends Wi-Fi Protected Access (WPA2) encryption, which is the highest level of security available.

Your router's default encryption setting may have been set to WEP encryption, which is an earlier standard that does not provide the same level of protection for your home network and personal information as WPA2 encryption. We strongly recommend changing your settings to WPA2 encryption now, if you have not done so already.

For more information and help in upgrading your router's encryption settings, please go to <u>http://verizon.com/securemyfiosnetwork</u>.

Tip:

Once you've updated your router to WPA2 protocol, you'll want to be sure your wireless networking devices are also upgraded to WPA2

# Verizon FiOS<sup>®</sup> Router Model 9100EM

# User Guide



www.verizon.com/fios



# CONTENTS

1.	PROD	UCT DESCRIPTION	5
2.	REGU	LATORY INFORMATION	6
	2.1	FCC Compliance Note	6
	2.2	Canada Certification Notice	7
3.	NETW	ORKING REQUIREMENTS	8
4.	HARD	WARE FEATURES	9
	4.1	LED Indicators	9
	4.2	Cable Connectors and Switch Locations	.10
	4.3	Front Panel LEDs	.11
	4.4	Connector Descriptions	.12
5.	INSTA	ILLING THE ROUTER	.13
	Before	you begin	.13
	5.1	Connecting Your Router to Your Broadband (Internet) Service	.14
	5.2	Connecting Ethernet Devices to Your Router	.14
	5.3	Connecting Wireless Devices to Your Router	.15
6.	ACCE	SSING YOUR ROUTER	.16
	6.1	Logging on to Your Router	.16
7.	CONF	IGURING YOUR BROADBAND CONNECTION	.19
	7.1	Confirming Your Coax Connection	. 19
	7.2	Connecting to the Internet	. 19
	7.3	Logging Out of the Router's Web Pages	.24
8.	SETTI	NG UP MACINTOSH OS X	.25
	8.1	Opening the System Preference Screen	.25
	8.2	Choosing the Network Preferences	.25
	8.3	Creating a New Location	.26
	8.4	Naming the New Location	.26
	8.5	Selecting the Ethernet Configuration	.26
	8.6	Checking the IP Connection	.27
	8.7	Accessing Your Router	.28
9.	BASIC	CONFIGURATION	.29
10.	MAIN	(HOME PAGE)	.30
	10.1	Router Status	.31



Ver	rizon Fi	OS Router (Model 9100EM)	User Guide
	10.2	Quick Links	
	10.3	Network Status	
	10.4	Start Surfing	
11.	WIRE	LESS	
	11.1	Wireless Status	
	11.2	Basic Security Settings	
	11.3	Advanced Security Settings	
12.	MY N	ETWORK	55
	12.1	Network Status	
	12.2	Network Connections	67
13.	FIREV	VALL SETTINGS	
	13.1	General Firewall Security Settings	
	13.2	Access Control	
	13.3	Port Forwarding	95
	13.4	DMZ Host	
	13.5	Port Triggering	
	13.6	Remote Admin	
	13.7	Static NAT	
	13.8	Advanced Filtering	
	13.9	Security Log	
	13.10	Connections	
14.	PARE	NTAL CONTROLS	
15.	ADVA	NCED	
	15.1	Diagnostics	
	15.2	Restore Defaults	
	15.3	Reboot	
	15.4	MAC Cloning	
	15.5	ARP Table	
	15.6	Users	
	15.7	Quality of Service	
	15.8	Remote Administration	
	15.9	DNS	
	15.10	Personal Domain (Dynamic DNS)	
	15.11	Network Objects	
		ى. 	



Ve	rizon Fi	OS Router (Model 9100EM)	User Guide			
	15.12	Protocol				
	15.13	UPnP				
	15.14	System Settings				
	15.15	Configuration File				
	15.16	Date and Time Rules				
	15.17	Editing the Time Server Table				
	15.18	Editing Clock Set				
	15.19	Scheduler Rules				
	15.20	Firmware Upgrade				
	15.21	Routing				
	15.22	IGMP Configuration				
	15.23	PPPoE Relay				
	15.24	IP Address Distribution				
16.	SYST	EM MONITORING				
	16.1	Gateway Status				
	16.2	Gateway Status				
	16.3	System Log				
17.	TECH	NICAL SUPPORT INFORMATION				
18.	PROD	UCT SPECIFICATIONS				
19.	SOFT	WARE LICENSE AGREEMENT				
20.	PUBL	). PUBLICATION INFORMATION				



User Guide

# **1. PRODUCT DESCRIPTION**

The Verizon<sup>®</sup> FiOS<sup>®</sup> Router is designed to deliver today's most exciting broadband services to and throughout your home. Built around a state of the art, dual-core network processor, this versatile product helps ensure that data and services reach your connected home devices without interruption or delay. The Router allows you to transfer data over your existing in-home coax cables and simultaneously supports both "wired" and "wireless" connection options. This flexibility allows for the connection of a wide range of network enabled devices such as desktop computers, laptop computers, digital media players, and network attached storage (NAS) units.

Hereafter, the Verizon FiOS Router will be referred to as the "Router."

Key Features:

- Multimedia over Coax interface (MoCA)
- 4-Port 10/100 BaseT Ethernet LAN switch
- Integrated 802.11g Access Point
- Embedded Firewall
- IP Quality of Service
- IGMP Proxy Functionality

This User Guide is intended to provide installation and configuration information on the Verizon<sup>®</sup> FiOS<sup>®</sup> Router and assumes the user of this Router has a medium to advanced understanding of computing, routing and internet networking.



## 2. REGULATORY INFORMATION

## **2.1 FCC Compliance Note**

#### (FCC ID: CH89100VMXX-10)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the Federal Communication Commission (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 one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to a different circuit from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.
- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**WARNING:** While this device is in operation, a separation distance of at least 20 cm (8 inches) must be maintained between the radiating antenna and users exposed to the transmitter in order to meet the FCC RF exposure guidelines. Making changes to the antenna or the device is not permitted. Doing so may result in the installed system exceeding RF exposure requirements. This device must not be co-located or operated in conjunction with any other antenna or radio transmitter. Installers and end users must follow the installation instructions provided in this guide.

#### Modifications made to this device, unless expressly approved, could void the users' rights to operate this device.

#### PART 68 – COMPLIANCE REGISTRATION

This equipment is designated to connect to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. An FCC compliant telephone cord and modular plug is provided with the equipment. See the Installation Information section of this User Guide for details.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instruction for details.

If this terminal equipment (Model 9100EM) causes harm to the telephone network, the telephone company may request you to disconnect the equipment until the problem is resolved. The telephone company will notify you in advance if temporary discontinuance of service is required. If advance notification is not practical, the telephone company will notify you as soon as possible. You will be advised of your right to file a complaint with the FCC if you believe such action is necessary. If you experience trouble with this equipment (Model 9100EM), do not try to repair the equipment yourself. The equipment cannot be repaired in the field. Contact Verizon for instructions.

User Guide



User Guide

The telephone company may make changes to their facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make the modifications necessary to maintain uninterrupted service.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Model 9100EM) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer. This equipment cannot be used on public coin phone service provided by the telephone company. Connection of this equipment to party line service is subject to state tariffs.

## 2.2 Canada Certification Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operations and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specification. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment. The Ringer Equivalence Number (REN) is 0.0. The Ringer Equivalence Number that is assigned to each piece of terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local Telecommunication Company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Connection to a party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Model 9100EM) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

If you experience trouble with this equipment (Model 9100EM), do not try to repair the equipment yourself. The equipment cannot be repaired in the field and must be returned to the manufacturer. Repairs to certified equipment should be coordinated by a representative, and designated by the supplier. Contact Verizon for instructions.

The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five. Users should ensure, for their own protection, that the electrical ground connections of the power utility, telephone lines, and internal, metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.



Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.



User Guide

# **3. NETWORKING REQUIREMENTS**

The following minimum system specifications are required for optimum performance of your Router.

#### **Requirements for 10/100 Base-T/Ethernet**

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (XP, 2000, ME, NT 4.0, 98 SE) Macintosh® OS X, or Linux installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- 10/100 Base-T Network Interface Card (NIC)
- Internet Explorer 5.5 or later or Netscape Navigator 7.x or higher or Firefox 1.0.7 or later
- Computer Operating System CD-ROM

#### **Requirements for Wireless**

- Pentium<sup>®</sup> or equivalent class machines or higher
- Microsoft® Windows® (XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer 5.5 or later or Netscape Navigator 7.x or higher or Firefox 1.0.7 or later
- IEEE 802.11b/g PC adapter
- Computer operating system CD-ROM

#### System Requirements for Coax

- Pentium® or equivalent class machines or higher
- Microsoft® Windows® (XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer 5.5 or later or Netscape Navigator 7.x or higher or Firefox 1.0.7 or later
- Computer operating system CD-ROM

8



User Guide

# 4. HARDWARE FEATURES

# 4.1 LED Indicators

This section explains the Router's LED states and descriptions. View the LEDs to confirm the unit's operation and status.

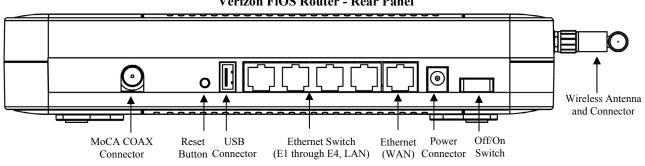
		Front Panel LEDs				
LED	State	Description				
	Solid Green	Power is ON.				
	Flashing Green	Router is performing power on self test (POST).				
POWER	Solid Red	Router failed POST or Device Malfunction. Note: The Power LED should be red no longer than two seconds after the power on self test passes.				
	OFF	Power is OFF.				
	Solid Green	WAN physical link established.				
COAX WAN	Flashing Amber	Low signal rate or noisy Coax line. Service should not be affected.				
POWER COAX WAN ETHERNET WAN INTERNET WIRELESS SETUP (LAN ETHERNET) COAX WIRELESS Left Ethernet LED	OFF	Router power is OFF or no WAN signal detected.				
	Solid Green	WAN link established.				
ETHERNET WAN	OFF	Router power is OFF or no WAN signal detected.				
	Solid Green	Internet link established; the Router has a WAN connection and IP address.				
INTERNET	Flashing Green	Internet link established; IP traffic is passing through the device in either direction.				
	Amber	Internet link not established or attempting to establish.				
	OFF	Router power is OFF or the Router does not have a WAN address.				
WIRELESS	Solid Green	LED currently disabled				
SETUP	OFF	LED currently disabled				
	Solid Green	Powered device is connected to the associated port.				
1,2,3,4	Flashing Green	10/100 Base-T LAN activity is present (traffic in either direction).				
(LAN ETHERNET)	OFF	Router power is OFF, or no cable or no powered device is connected to the associated port.				
	Solid Green	A physical connection has been established.				
COAX	Flashing Green	Activity is present on the Coax link.				
	OFF	Router power is OFF.				
WIRELESS	Solid Green	Wireless link established. Wireless LAN activity is present (traffic ir either direction). IP connection established and IP traffic is passing through device.				
	OFF	Router power is OFF or No wireless link.				
		Rear Panel LEDs				
	Solid Green	100 Mbps link established.				
Left Ethernet LED	Flashing Green	LAN activity at 100 Mbps (traffic in either direction).				
	OFF	No 100 Mbps link.				
	Solid Green	10 Mbps link established.				
Right Ethernet LED	Flashing Green	LAN activity at 10 Mbps (traffic in either direction).				
	OFF	No 10 Mbps link.				



User Guide

# 4.2 Cable Connectors and Switch Locations

- Coax connector •
- Reset push button •
- USB connector •
- Four LAN Ethernet connectors (RJ-45) ٠
- WAN Ethernet connector (RJ-45) •
- Power connector (12 VDC) barrel ٠
- OFF/ON power switch •
- Wireless 802.11b/g SMA connector and antenna ٠



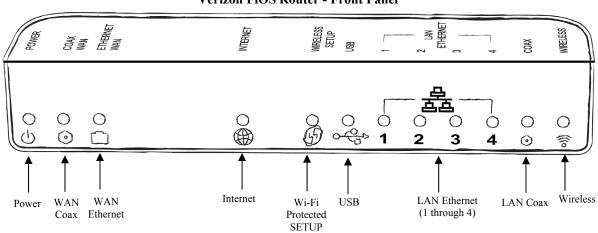
#### Verizon FiOS Router - Rear Panel



User Guide

# 4.3 Front Panel LEDs

- Power
- WAN Coax
- WAN Ethernet
- Internet
- Wi-Fi Protected SETUP (Currently Disabled)
- USB
- LAN Ethernet (1,2,3,4)
- LAN Coax
- Wireless



#### Verizon FiOS Router - Front Panel



User Guide

# 4.4 Connector Descriptions

The following chart describes the Router's rear panel connector and switches.

NAME	Түре	FUNCTION			
COAX	F-type coaxial connector	Connects the Router to the in home coaxial cabling. Compatible with the Multimedia over Coax Alliance (MoCA) standards.			
USB	USB Connector	Connects the Router to peripheral devices (e.g. storage) via USB. Note: This port may not be enabled in all UltraLine Series3 units.			
LAN	8-pin (RJ-45) modular jack	Connects the Router's 10/100 Base-T Ethernet swtich to a local computer or other Ethernet-enabled device.			
WAN	8-pin (RJ-45) modular jack	Connects the Router to a broadband modem or router, enabling access to the Internet or Wide Area Network (WAN).			
POWER Barrel connector		Connects to the Router's DC 12V power supply. <b>Only use the power supply provided with the Router.</b>			
OFF/ON	Off/On Switch	Allows you to turn the Router on or off.			
WIRELESS ANTENNA and CONNECTOR	SMA connector and antenna	Antenna for trasmitting and receiving wireless signals for Wi-Fi (802.11b/g) connected devices.			



User Guide

# 5. INSTALLING THE ROUTER

This section explains the hardware installation procedures for connecting your Router to your broadband service as well as to devices in your home, such as computers or media players.

# Before you begin

Make sure that your kit contains the following items:

- Verizon FiOS Router
- Power Supply
- RJ-45 Ethernet cable (straight-through) (yellow)
- RJ-45 Ethernet cable (straight-through) (white)
- Verizon CD-ROM containing User Guide in PDF format
- Wireless antenna
- Router Stand

#### Before you install your Router, please read the following notes:

#### NOTE:

- 1. It is recommended that you use a surge suppressor to protect equipment attached to the power supply. Use only the power supply provided with your kit.
- 2. If the Ethernet card in your PC does not auto-negotiate, set it to half duplex. Refer to the Ethernet card manufacturer's instructions for installing and configuring your Ethernet card.
- 3. Additional Ethernet cables may be required depending on the installation method you are using. Ethernet cables can be purchased at your local computer hardware retailer.



User Guide

## 5.1 Connecting Your Router to Your Broadband (Internet) Service

- 1. Connect one end of your coaxial cable to the coax connection on you wall. Connect the other end of the coaxial cable to the connector marked **Coax** on the Router.
- 2. Connect the power supply cord to the power connector marked **12 VDC** on the back of the Router. Plug the other end of the power supply into an AC wall socket, and then turn on the Router by pressing the Off/ON switch on the back of the Router.
- 3. Check to see if the Router's **POWER** LED is solid green. This indicates that the Router is powered on.
- 4. Check to see if the Router's **Coax WAN** LED is solid green. This means the COAX connection is functioning properly. (Note: Your **Coax WAN** Led may also be amber which is acceptable)

Now that you have connected your Router to your broadband service and turned on the Router, you can connect Ethernet and Wireless devices to the Router, allowing for Internet connection throughout your home without disrupting your cable or satellite television services. Refer to the following sections for instructions on connecting devices to your Router:

- Section 5.2 explains how to connect Ethernet devices to your broadband Router.
- Section 5.3 explains how to connection Wireless devices to your broadband Router.

## 5.2 Connecting Ethernet Devices to Your Router

To connect PCs to your Router using 10/100-BaseT Ethernet installation, please follow the steps below:

- 1. Connect your Router to your broadband service as explained in section 5.1.
- Connect the yellow Ethernet cable (provided with your kit) from any one of the four Ethernet jacks marked 1, 2, 3, 4 on the back of the Router to the Ethernet port on your computer. Turn on the computer.

**NOTE:** Use any of the four LAN Ethernet jacks on the Router's rear panel; each jack serves as an Ethernet switch. Repeat this step to connect up to three additional PCs to the Router.

- 3. Check to see if the Router's **POWER** LED is solid green. This indicates that the Router is powered on.
- 4. Check to see if any of the Router's **ETHERNET** LEDs (1,2,3,4) are solid green. Solid green indicates that the Ethernet connection is functioning properly. Check the **ETHERNET** LED for each Ethernet jack to which you are connected at the rear of the Router.
- 5. Check to see if the Router's **COAX WAN** LED is solid green (or flashing amber). This means the Coax connection is functioning properly.
- 6. After you have logged on to you account and established an Internet connection, as explained later in this document, check to see if the Router's **INTERNET** LED is solid green. Solid green indicates that the Internet link has been established.

Congratulations! You have completed the steps to connect Ethernet devices to your Router. Now proceed to section 6 to access your Router's Web pages.



User Guide

## 5.3 Connecting Wireless Devices to Your Router

**IMPORTANT:** If you are connecting to the Router via a wireless network adapter, the SSID must be the same for both the Router and your PC's wireless network adapter. The default SSID for the Router is the serial number of the unit (located below the bar code on the bottom of the router and also on the shipping carton). The SSID is also provided in the Router's Web pages, in the Wireless section. On your PC, locate and run the utility software provided with your PC's wireless network adapter. Then, enter the Router's SSID value (in order to communicate with the Router, the PC's wireless network adapter must be configured with the SSID). Later, for privacy, you can change the SSID by following the procedures outlined in section 11.2, "Basic Security Settings."

**NOTE**: Client PCs can use any Wireless 802.11b/g card to communicate with the Router. By default your Router is enabled for Wired Equivalent Privacy (WEP) security. Whenever, WEP is configured in the Router, the PC's wireless card must use the same WEP security code type as the one provided in Router. The WEP security code is also located on a label on the bottom of the Router. Always check that your PC's wireless adapter is configured properly for whichever network setting you use: WEP or WPA. You can configure the settings in the advanced properties of the PC's wireless network adapter.

To network your Router to PCs in your home or office using a wireless installation, follow the steps below:

- 1. Connect your Router to your broadband service as explained in section 5.1.
- 5. Ensure that each PC on your wireless network has an 802.11b/g wireless network adapter installed.
- 6. Ensure that appropriate drivers for your wireless adapter have been installed on each PC.
- 7. Make sure the wireless antenna is screwed on to the connector on the rear of the router and firmly locked into place. Then, orient the antenna to appropriate position.
- 8. Connect the power supply cord to the power connector marked **12 VDC** on the back of the Router. Plug the other end of the power supply into an AC wall socket, and then power up the Router.
- 9. Check to see if the Router's **POWER** LED is solid green. This indicates that Router is powered on.
- 10. Check to see if the Router's **COAX WAN** LED is solid Green. This means the COAX connection is functioning properly.
- 11. Check to see if the Router's **WIRELESS** LED is solid Green. This means that the wireless interface is functioning properly.
- 12. After you have logged on to your account and established an Internet connection, as explained later in this document, check to see if the Router's **INTERNET** LED is solid green. Solid green indicates that an Internet link has been established.

Congratulations! You have completed the steps to connect wireless devices to your Router. Now proceed to section 6 to access your Router's Web pages.



User Guide

# 6. ACCESSING YOUR ROUTER

## 6.1 Logging on to Your Router

This section explains the logon procedures for your Verizon Broadband Router. This procedure should be used any time you want to access or make changes to the Router's configurable settings, such as wireless security and firewall.

**IMPORTANT:** Your Router is capable of automatically sensing protocol type (DHCP or PPPoE). This process is designed to start after you have connected the Router. To access your Router, your PC must be configured for DHCP. Refer to your Windows help screen for information on configuring your computer for DHCP. At your PC, click **Start**, then click **Help** to access the Windows help screen.

To log on to the Router, start your Web browser, and then type the following IP address in the browser's address bar:

## http://192.168.1.1

After you type the IP address, press Enter on your keyboard. The following screen will display the message:

This is your first login to the Management Console. Use http://192.168.1.1 in order to access the Router's Management Console. To conveniently access the Management Console, you can click Add to Favorites. You should make sure that cookies are enabled in the browser. To enable cookies, go to Tools->Internet Options->Privacy->Advanced.

Click OK in the Welcome screen.

Welcome to Wireless Broadband Router	
Attention	
This is your first login to Wireless Broadband Router Management Console. Use <u>http://192.168.11</u> in order to access Wireless Broadband Router Management Console. To conveniently access Wireless Broadband Router Management Console you can click <u>Add to Favorites</u> . You should make sure that cookies are enabled in the browser. To do that, you should go to Tools->Internet Options- >Privacy->Advanced.	
<u> </u>	



User Guide

By default **admin** appears in the **User Name** field; however, you can change this to the user name of your choice. Type your password in the **New Password** fields. Your password must be 6 or more characters long and contain at least 1 numeral. As you type your password, asterisks will appear for security purposes.

#### NOTE: Please write down your user name and password and save them for future use.

veri <mark>zo</mark>	n	
		ogin Setup
	User Name: New Password: Retype New Password: Time Zone:	admin Enter your EST (GMT-05:00)
		<u>√ oκ</u>

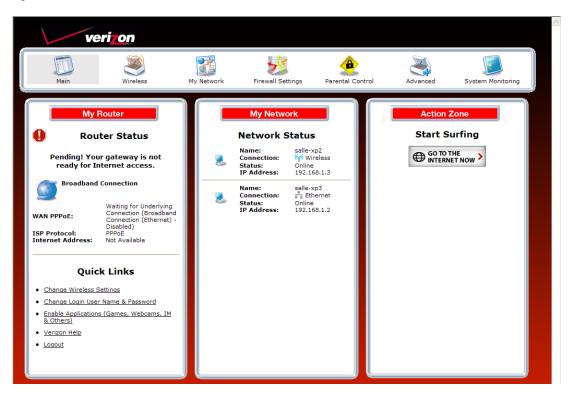
After you have entered your password, select the desired option from the **Time Zone** drop-down menu. Then click **OK** to continue.

Login Setup         Please configure Wireless Broadband Router's username and password:         User Name:         New Password:         Retype New Password:         Time Zone:         EST (GMT-05:00)         EST (GMT-05:00)         EST (GMT-05:00)         EST SEDT (GMT-05:00)         MST7MDT (GMT-07:00)         MST7MDT (GMT-07:00)         PST8PDT (GMT-08:00)         Pacific/Honolulu (GMT-10:00)		veri <mark>zon</mark>		
New Password:            Retype New Password:            Time Zone:         EST (GMT-05:00)           EST (GMT-06:00)         EST (GMT-06:00)           EST (GMT-07:00)         MST (GMT-07:00)           MST (GMT-07:00)         MSTRUPT (GMT-07:00)	Í	-	-	ssword:
Retype New Password:            Time Zone:         EST (GMT-05:00)         ▼           CST6CDT (GMT-06:00)         EST(6MT-06:00)         EST(6MT-06:00)           EST(5MT-05:00)         MST (GMT-07:00)         MST (GMT-07:00)           PST8PDT (GMT-06:00)         PST8PDT (GMT-06:00)         MST/MDT (GMT-07:00)		User Name:	admin	
Time Zone:         EST (GMT-05:00)         ▼           CST6CDT (GMT-06:00)         EST(EMT-06:00)         EST(EMT-06:00)           FST6EDT (GMT-07:00)         MST (GMT-07:00)           MSTMDT (GMT-07:00)         PST8PDT (GMT-08:00)		New Password:	•••••	
CST6CDT (GMT-06:00) EST (GMT-05:00) EST5EDT (GMT-05:00) MST (GMT-07:00) PST8PDT (GMT-07:00) PST8PDT (GMT-07:00)		Retype New Password:	•••••	
EST (GMT-05:00) ESTEDT (GMT-07:00) MST (GMT-07:00) PST8PDT (GMT-07:00) PST8PDT (GMT-08:00)		Time Zone:	EST (GMT-05:00)	
ESTSEDT (GMT-05:00) MST (GMT-07:00) MST7MDT (GMT-07:00) PST8PDT (GMT-08:00)				
			EST5EDT (GMT-05:00) MST (GMT-07:00) MST7MDT (GMT-07:00)	



#### User Guide

After you have logged on to your Router, the following screen will appear. This is the main page of your Router's Web pages, also referred to in this document as the home page. You can access this page by clicking **Main** in the navigation menu located across the top of the Router's Web pages. Details on this page will be explained in the following sections.



Throughout this User Guide, the following icons are used to indicate clicking actions that you can take with your mouse to configure your Router's settings.

Icon	Description
1	Edit Clicking this icon allows you to edit the assocaiated entry/setting.
4	Add/New Clicking this icon allows you to add a new entry/setting.
*	Delete Clicking this icon deletes the associated entry/setting from your Router.
9	View Clicking this icon allows you to view or run a diagnostics test on your Router.
*	Move Down Click this icon allows you to change the order of your list by moving an entry down in the list.
1	Move Up Click this icon allows you to change the order of your list by moving an entry up in the list.



User Guide

## 7. CONFIGURING YOUR BROADBAND CONNECTION

To browse the Internet using your Router, first confirm your coax link and establish an Internet connection with Verizon. The procedures for configuring your Router for Internet connection are explained in this section.

## 7.1 Confirming Your Coax Connection

**IMPORTANT:** You must have active broadband service before the Router can synchronize with Verizon's equipment and establish an Internet connection.

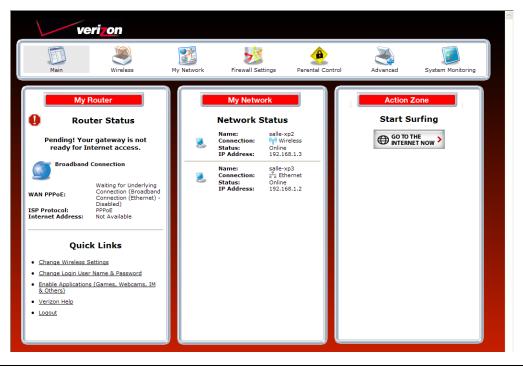
To determine if the Router has established coax link, at the Router's front panel, check to see if the Router's **COAX WAN** LED is solid green or flashing amber— this indicates that a coax link is established.

After confirming your coax link, proceed to section 7.2 to configure your Router's Internet connection settings.

### 7.2 Connecting to the Internet

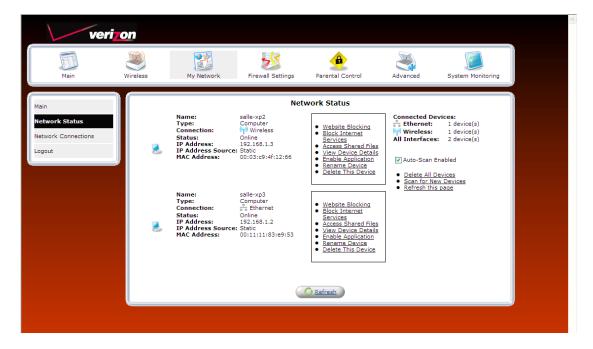
After you have logged on to the Router, the following home page will appear. Use this page to determine the Router's Internet connection status. If you do not have an Internet connection, the **Internet Address** field will display "Not Available."

To begin your connection setup, at top navigation menu, click My Network.





User Guide



The Network Status page will appear. Next, in the left submenu, click Network Connections.

In the Network Connections screen, click the Quick Setup button.

The **Quick Setup** page allows you to select the protocol type for your Internet connection, or choose to configure a static IP address. Verizon will inform you of which protocol to use to establish your Internet connection.



User Guide

# 7.2.1 DHCP Protocol Type

**IMPORTANT:** Do not change the settings in the **Quick Setup** screen unless Verizon instructs you to change the settings. Your Router is designed to automatically detect the correct connection type to the network.

If you need to change the configuration to only use DHCP protocol to connect to Internet, at the **Quick Setup** screen, do the following:

- 1. From the **Broadband Detect Default** drop-down menu, select **Automatic IP (DHCP)**. Note: DHCP is the Router's default protocol type. If you use this protocol, you do not need to enter a Login User Name or Login Password.
- 2. Click **Apply** to save the settings.
- 3. Click **OK** to continue.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Quick Setup Logout		WAN Interface Internet Conn Broadband Co Protocol Mode © Continue Broadba Current Protoc Name: Status: Login User Na Login Passwor	nnection Device e: ections nnection Protocol :: ous Auto Protocol detect nd Detect Default: col Type: me: rd: dvanced Settings	Auto  Auto  Auto  Auto  Auto DETECTION Automatic IP (DHCP)  Automatic IP (DHCP) PIPP over Ethernet Disconnected - Logi verizonfics	l over Ethernet (Pi	PPoE)
			Press the <b>Refresh</b>	button to update the sta	tus.	



User Guide

# 7.2.2 PPPoE Protocol Type

**IMPORTANT:** Do not change the settings in the **Quick Setup** screen unless Verizon instructs you to change the settings. Your Router is designed to automatically detect the correct connection type to the network.

If you need to change the configuration to only use PPPoE protocol to connect to Internet, at the **Quick Setup** screen, do the following:

- 1. From the Broadband Detect Default drop-down menu, select PPP over Ethernet.
- 2. Enter your Login User Name and Password (provided by Verizon) in the fields provided.
- 3. Click **Apply** to save the settings.
- 4. Click **OK** to continue.

veri	<b>70</b> n						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Quick Setup Logout		WAN Interface Internet Conn Broadband Co Protocol Mode © Continue Broadba Current Protoo Name: Status: IP Address: Default Gatewar DNS Server Login User Na Login Passwoo	nnection Device e: ections nnection Protocol :: ous Auto Protocol detect nd Detect Default: col Type: y: me:	PPP over Ethernet	v ccol over Ethernet (PP	PoE)	
		-		Broadband Connection	atus.		



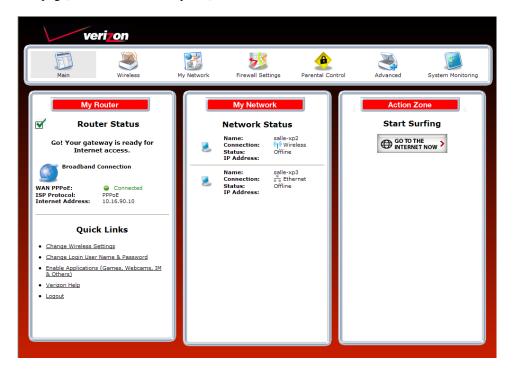
User Guide

To configure additional PPPoE settings, in **Quick Setup** screen, click the link labeled <u>Click Here for Advanced</u> <u>Settings</u>. The following screen appears.

**NOTE:** To configure additonal WAN PPPoE properties, select **Routing** and **PPP** in the left submenu. If you change any settings in these screens, click **Apply** to save the settings.



After you have selected your protocol and clicked **OK** in the preceding screen, click **Main** to return to the home page. In the **My Router** panel, the message **Go! Your gateway is ready for Internet access** should now be displayed. In addition, the **Internet Address** field will display the WAN IP address of your Router. To quickly access your default Web page, in the **Action Zone** panel, click **GO TO THE INTERNET NOW.** 





User Guide

# 7.3 Logging Out of the Router's Web Pages

When you are ready to log out of the Router's web pages, click the **Logout** link in the left submenu in any of the Web screens.

**NOTE:** If you want to close the Router's Web page, simply click the "X" in the upper-right corner of the window. Logging out or closing the window does not affect your Internet connection. However, you will need to log in to the Router again when you are ready to access the Router's pages.

verizon					
Main Wireless	My Network	Firewall Settings	Parental Control	Advanced System Monitoring	
<section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header><section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header></section-header>	2	My Network         Detwork Status         Connection:       Salle-xp         Status:       Offline         IP Address:       Salle-xp         Name:       Salle-xp         Connection:       Salle-xp         TP Address:       Offline         IP Address:       Offline	eless	<section-header><section-header></section-header></section-header>	



User Guide

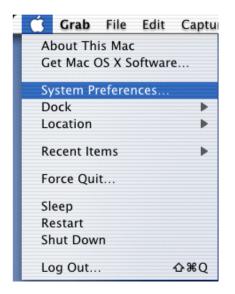
# 8. SETTING UP MACINTOSH OS X

This section provides instructions on how to use Macintosh Operating System 10 with the Router. Follow the instructions in this section to create a new network configuration for Macintosh OS X.

**NOTE:** Macintosh computers must use the Router's Ethernet installation. Refer to section 5, "Installing the Hardware," for details.

## 8.1 Opening the System Preference Screen

After you have connected the Router to the Ethernet port of your Macintosh, the screen below will appear. Click the "**Apple**" icon in the upper-left corner of the screen and select **System Preferences**.



## 8.2 Choosing the Network Preferences

After selecting System Preferences from the previous screen, the following screen will appear. Click the Network icon.





User Guide

## 8.3 Creating a New Location

After clicking the Network icon, the Network screen will appear. Select New Location from the Location field.

000		Network					
j 🛋		۵		2			
Show All	Displays	Sound	Star	tup Disk	Network		
		Location	/ Auto	matic	-		
Configure:	Internal M	lodem		Location.			
		TCP/IP	PPP	Proxies	Modem		

## 8.4 Naming the New Location

After selecting **New Location** in the **Network** screen, the following screen will appear. In the field labeled **Name your new location:**, change the text from "**Untitled**" to "**Westell**." Click **OK**.

All users of this computer will be able to	
choose this location in the Apple menu without entering a password.	

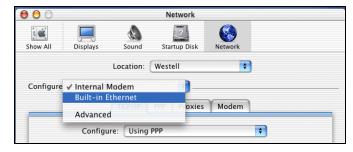
# 8.5 Selecting the Ethernet Configuration

After clicking **OK** in the preceding screen, the **Network** screen will appear. The **Network** screen shows the settings for the newly created location. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**. Click **Save** to save the settings.

**NOTE:** Default settings for the Built-in Ethernet configuration are sufficient to operate the Router.



User Guide



# 8.6 Checking the IP Connection

To verify that the computer is communicating with the Router, follow the instructions below.

- 1. Go to the "Apple" icon in the upper-left corner of the screen and select System Preferences.
- 2. In the System Preferences screen, click the Network icon. The Network screen will appear.
- 3. In the Configure field in the Network screen, select Built-in Ethernet.
- 4. View the IP address field. An IP address that begins with 192.168.1 should appear.

**NOTE:** The Router's DHCP server provides this IP address. If this IP address is not displayed, check the Router's wiring connection to the PC. If necessary, refer to section 5, "Installing the Hardware," for installation instructions.

000			Network		~			-
Show All	Displays	Sound	Startup Disk	Ne	work			
		Location: (	Westell		\$			
Configure:	Built-in Eth	ernet	ŧ					
	Т	CP/IP PP	PoE Apple	Talk	Proxies			
	Configur	e: Using I	DHCP			\$		
IP	Address: 19 (Pro	2.168.1.15 ovided by DH0	1	Domaiı	n Name S	erver:	5 (Optio	nal)
DHCP	Client ID:	tional)						
	(0)	(ional)		Search	Domain	S	(Optio	nal)
Ethernet	Address: 00	30:65:e1:8	4:ba					
				Example	apple.co	m, eart	hlink.ne	t
Click	the lock to pre	vent further	changes.				S	ave )



User Guide

# 8.7 Accessing Your Router

In your Internet Explorer Web browser's address bar, type http://192.168.1.1, and then press Enter on your keyboard.

000	)					01	WireSpee	d Dual Con	inect			
d Back P	Forward	X	Refresh	n Home		AutoFill	Print	Mail				e
Address	http://	/192.168.1.	-									) go
@ Live	Home Page	Apple	🔘 Apple Supp	ort @	) Appl	e Store	iTools	🔘 Mac OS X	🔞 Microsoft MacTopia	Office for Macintosh	MSN (	
<[]]												
Fax												

The **Login** screen will appear. Please refer to the **Login** screen in section 6.1 of this User Guide for logon instructions.

Attention           Use <a href="http://192.168.1.1">http://192.168.1.1</a> in order to access Wireless Broadband Router Management Console.           To conveniently access Wireless Broadband Router Management Console you can click <u>Add to Favorites</u> .           You should make sure that cookies are enabled in the browser. To do that, you should go to Tools->Internet Options->Privacy->Advanced.



User Guide

# 9. BASIC CONFIGURATION

**IMPORTANT:** The following sections assume that you have active broadband Internet service.

The Router allows you to make changes to the configurable features such as connection settings, routing configurations, and firewall settings. The following sections explain each feature and show you how to make changes to the Router's settings. The navigation menu displayed at the top of each page allows you to navigate to the various configuration screens of your Router. Whenever you change settings in your Router, you must click **Apply** to allow the changes to take effect in the Router.

#### NOTE:

- 1. If you need help, go to the **Quick Links** section in the home page and then click the **Verizon Help** link. Clicking this link takes you to Verizon's Online Help site where you can find additional information about your Router.
- 2. If you click **OK** or **Apply** in a screen and then experience a delay, you may need to refresh the screen; press the **Refresh** button (where applicable) or press **F5** on your keyboard.
- 3. If you want to logout of the Router's Web page, click the **logout** link in the home page. Clicking this link does not affect your Internet connection; it only closes the Router's Web page. To log in, you will need to enter your username and password in the **Login** screen.

To configure the basic settings in your Router, follow the instructions provided in sections 10 through 14.



User Guide

# **10. MAIN (HOME PAGE)**

After you have logged on to your Router and established an Internet connection with Verizon, click **Main** in the top navigation menu. The following home page will appear. The home page allows you to view connection information reported by your Router and quickly access Internet services provided by Verizon. The following sections discuss each panel in the Main page. The Main page will be referred to as the home page throughout this User Guide.

verizon					_
Main Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
My Router         Image: Construction of the second secon		My Network Name: sallex Connection: Status: Offline IP Address: Name: Status: Offline IP Address:	p2 eless	Action 20 Start Su GO TO TH INTERNET	rfing



User Guide

## **10.1 Router Status**

In the home page, the **Router Status** pane allows you to view the status of your Router's Internet connection. Whenever you have an Internet connection, a green check mark is displayed. This signals you to Go! You can now browse the Internet. In addition, the Router's connection type and WAN IP address will also be displayed.

# 10.2 Quick Links

The **Quick Links** pane allows access to your broadband connection settings, and provides a link to Help information related to your Router. The following links are displayed in the **Quick Links** panel.

Quick Links				
Change Wireless Settings	Click this link to access the Router's wireless settings pages.			
Change Login User Name &	Click this link to changea permissions needed to manage network			
Password Password	connections, or to set up privileges for new users and groups on your			
	network.			
Enable Applications (Games, Web	Click this link to open a tunnel between remote (Internet) computers and a			
Cams, Instant Messaging, & Others)	specific device port inside your local area network (LAN).			
Verizon Help	Click this link to access Verizon's Online Help site.			
Logout	Click this link to log out of the Router's Web pages.			

## **10.3 Network Status**

In the home page, the **Network Status** pane allows you to view information about devices that are connected to your network. If your network provides access to shared files, you can access the files by clicking the **Access Shared Files** link. The following details are displayed in the **Network Connections** panel.

Network Status				
Computer Name	The ASCII (text) name or MAC address of the device connected to the network.			
Connection Type	The physical or wireless connection used to interface with your Router.			
Status	The Internet status of the connected device: Offline or Online.			
IP Address	The IP address assigned to a device on your network.			

## **10.4 Start Surfing**

In the home page, the **Start Surfing** pane allows quick access to Internet services provided by Verizon. Click **GO TO THE INTERNET NOW** to go to your PCs default Web page.



User Guide

## **11. WIRELESS**

## **11.1 Wireless Status**

If you click **Wireless** in the top navigation menu and then select **Wireless Status** in the left submenu, the following screen will appear. This screen allows you to view details about your wireless connection.

**NOTE:** If you change the Router's wireless settings, wireless access to the Router may be interrupted and wireless stations may require reconfiguration.

verizon				
Main Wireless	My Network Firewall S	ettings Parental Control	Advanced	System Monitoring
Main		Wireless Status		
Wireless Status	Radio Enabled:	YES		
	SSID:	DK9QN		
Basic Security Settings	Channel:	Automatic		
Advanced Security Settings	Security Enabled:	YES		
Device List	WEP 64-bit KEY 1 (HEX):	4C44463747		
Logout	WEP 802.1x:	N/A		
	WPA:	N/A		
	SSID Broadcast:	Enabled		
	MAC Authentication:	Disabled		
	Wireless Mode:	Mixed - accepts 802.11b and 802.11	g connections	
	Packets Sent Total:	8721		
	Packets Received:	1639		



User Guide

# **11.2 Basic Security Settings**

If you select **Wireless** from the top navigation menu and then select **Basic Security Settings** in the left submenu, the following screen will appear. Your Router also functions as a wireless access point for wireless devices. To configure your wireless settings, enter the appropriate values in the fields provided. Then, click **Apply** to allow the settings to take effect. The following table explains the details of this screen.

#### **IMPORTANT:**

- 1. If you are connecting to the Router via a wireless network adapter, the computer's wireless network adapter must be configured with the Router's Service Set ID (SSID); that is, the SSID used in the wireless network adapter must be identical to the Router's SSID. The default SSID and WEP key for the Router are both located on the right-hand side of the label, which is located on the bottom of the router. Locate and run the utility software provided with the wireless network adapter, and then enter the identical SSID and WEP encryption security settings displayed in the Router into the wireless adapter. For privacy, you can change the SSID and security settings to your desired values. SSIDs are case sensitive and can contain up to 32 alphanumeric characters, including spaces.
- 2. In order for every computer on your network to connect to your Router wirelessly, confirm that each computer's wireless adapater is using the same security settings that you have configured in the Router's Basic Security Settings screen. After you have configured all the settings in this screen, please record the settings for future reference.



User Guide

#### Verizon FiOS Router (Model 9100EM)

verizo	n				
Main V	Vireless My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main W Min Wireless Status Basic Security Settings Device List Logout	If you wai 1. Turn V Wireless 2. Chang (SSID is t SSID: 3. Chann To change it below th NOTE: In Channel: 4. Click of We recom • WEP 5. Select NOTE: To any letter Sample W Select a 64/40 bh Key Codo 4C4446374 Number 0 6. Write In order f that the w make sur Current SSID: 64-BIT W Channel: SSID SID SID Bro MC Auth Wireless I	Basic S  Int to setup a wireless network  Vireless ON.   It is the SSID setting to any  the same thing as the name of  the same thing as the name of  the United States, use channel  on the button next to WEP.  The one of the button next to the one of the button next to the one of the button next to the the one of the button next to the one of the button next to the one of the one of the button next to the one of the button next to the one of the button next to the one of	Security Settings c, we recommendyou do OFF name or code you wan f your Wireless Network) DK9QN Ind at which the Router cu- ettings. els 1-11. Automatic  (FCC ancrypts wireless traffic. WPA/WPA2, 802.1x) to enter a combination o n 0-9. to this Router wirelessly ter uses the SAME setting is values set on this screen 802.11b and	the following:	
	L				



User Guide

	Wireless Settings
Wireless (ON/OFF)	By default, the wireless feature is enabled. To completely turn off the wireless networking feature and the Router's internal wireless radio, select OFF.
Change SSID	The SSID is the name of your wireless network. This string is case-sensitive and must be 30 characters or less. To connect to the Router, the SSID on a computer's wireless card must be identical the SSID on the Router. The Router comes pre-configured with the SSID; however, you can change the SSID to any name or code you want.
Channel	This is the channel of the frequency band at which the Router communicates. The Router transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the Router. A computer's wireless card does not have to be set to the same channel as the Router; the wireless card can scan all channels and look for a Router to connect to. (In the United States, use channels 1 through 11). For better performance, select a channel that is not being used or being used the least by other wireless devices such as cordless phones or other Routers in the area. If "Automatic" is selected, the Router will determine the optimal channel to use.
WEP Security	Factory Default = WEP WEP security encrypts the Router's wireless traffic and prevents unauthorized access to the Router's network. If "Advanced" is selected, it means that current wireless security setting is configured using advanced options (See 'Advanced Security Settings' for additional security options.) Selecting "NO SECURITY" will disable wireless security and is not recommended.
WEP Key Length	A WEP encryption key is used to protect your wireless transmissions. These keys are of varying lengths. The key can include the numbers $0-9$ and letters $a,b,c,d,e,$ and $f$ . The number of characters must be either 10 (for 64/40 bit encryption) or 26 (for 104 bit encryption). If this page is used to configure WEP, key 1 will be used as the active key. You should note this value as you will have to enter it into each device which is connecting wirelessly
WEP Key	This is the actual security key value. You should note this value as you will have to enter it into each device which is connecting wirelessly.
Number of Required Digits	This field indicates how many more characters are needed to complete the security key. The security key is not complete unless this counter indicates 0.
Configure Wireless Client Settings to match Router's settings	For wireless clients, such as computers and other devices with wireless cards to establish a wireless connection to this Router, the clients' settings, especially the SSID, channel, wireless mode, and security (i.e., WEP) settings must match the Router's settings as summarized in the table. If channel is set to Automatic, the Router will determine the optimal channel to use. (If settings, particularly if using advance security options, are changed in other or "Advanced" sections, the sections where the changes were made must be consulted for reference.)



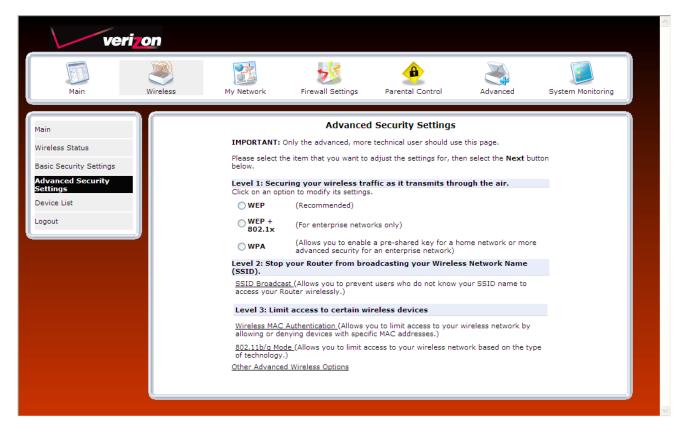
User Guide

# **11.3 Advanced Security Settings**

If you select **Wireless** from the top navigation menu and then select **Advanced Security Settings** in the left submenu, the following screen will appear. Generally, most owners of the Router will not need to modify these wireless options.

From this menu, you can change your wireless security level by selecting the desired choice: WEP, WEP + 802.1x, or Wireless Protected Access (WPA). You can also enable/disable the SSID broadcast feature for the product. If you want to limit connected wireles dievces to only the 802.11g (54Mbps) standard, chose the 802.11 b/g mode link and select the desired mode.

For full access to all wireless and secuity settings on one page, click on the **Other Advanced Wireless Options** link at the bottom of the page. Details on this page are provided in section 11.3.4.

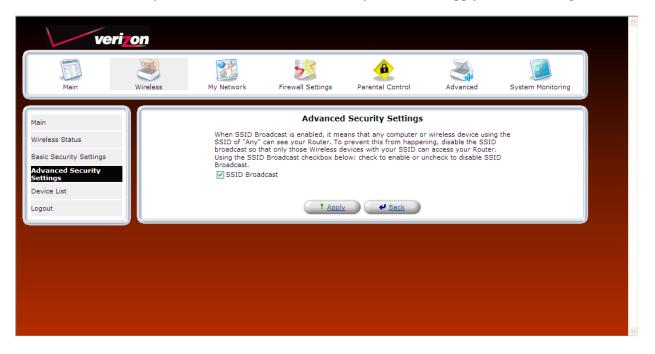




User Guide

# **11.3.1 SSID Broadcast**

If you clicked the **SSID Broadcast** link, the following screen will appear. By disabling the SSID broadcast, your Router will no longer send out messages indicating that it is in place. Disabling the SSID broadcast does not disable the wireless interface and clients configured with the correct SSID and wireless security key (when enabled) will still be able to connect. If you enable or disable SSID Broadcast, you must click **Apply** to save the change.





User Guide

# 11.3.2 Wireless MAC Authentication

If you clicked the **Wireless MAC Authenticaton** link, the following screen will appear. Set up your MAC Filtering settings, and then click **Apply** to save the settings.

verizo	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Wireless Status Basic Security Settings Advanced Security Settings Device List Logout		ALLOW: Only M access. DENY: MAC Ad If MAC Filtering Filtering will op	C Filtering, select a MAC f MAC Addresses in the MA ddresses in the MAC Filte g Settings table below is perate in disabled mode u the "New MAC Address" g Mode:	C Filtering Settings table below v empty, MAC Filtering Mod- intil an entry is added to t link. Disable V New MAC Address	vill be DENIED acces e will be ignored so M he table. To ADD an	s. MAC	

For example, if you select "Allow" from the **MAC filtering Mode** drop-down list, this option will allow only the devices whose MAC Addresses are active in the list to connect to the Router. To add a MAC address, click the **New MAC Address** link.

ver	i <mark>zon</mark>					_	
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main			Advanced	l Security Settings			
Wireless Status		To enable MAC Filtering, select a MAC Filtering Mode. ALLOW: Only MAC Addresses in the MAC Filtering Settings table below will be ALLOWED access.					
Basic Security Settings Advanced Security		DENY: MAC Addresses in the MAC Filtering Settings table below will be DENIED access. If MAC Filtering Settings table below is empty, MAC Filtering Mode will be ignored so MAC Filtering will operate in disabled mode until an entry is added to the table. To ADD an					
Settings Device List		MAC Filtering		Disable 🗸			
Logout		MAC Filtering	Settings	Disable Address Allow Deny	5		
C				v e Back			



User Guide

The following screen will appear. Enter the MAC address of the device that you want to allow access to the Router. Then, click **OK** to continue.



After you have entered a valid MAC address, the following **Advanced Security Settings** screen will display all the MAC addresses that have been added to the MAC filtering table. Be sure to select the desired option from the **MAC Filtering Mode** drop-down list. Then, click **Apply** to allow the settings to take effect in the Router.

To edit a MAC address, click the pencil icon next to the address you want to edit. To delete a MAC Address, click the "X" icon next to the address you want to delete. To add a new MAC address, click the plus icon, or click the **New MAC Address** link.

ver	i <mark>zon</mark>						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main			Advanced	Security Settings			
Wireless Status Basic Security Settings Advanced Security Settings Device List		To enable MAC Filtering, select a MAC Filtering Mode. ALLOW: Only MAC Addresses in the MAC Filtering Settings table below will be ALLOWED access. DENY: MAC Addresses in the MAC Filtering Settings table below will be DENED access. If MAC Filtering Settings table below is empty, MAC Filtering Mode will be ignored so MAC Filtering will operate in disabled mode until an entry is added to the table. To ADD an entry, click on the "New MAC Address" link. MAC Filtering Mode:					
Device List		MAC Filtering					
Logout			MAC Address		Action		
		00:33:14:ff:bb	:22		S 🗱 👘 🕹		
		00:22:ee:13:2	4:19		N 🗱 👘		
		New MAC Add	dress		4		
				e Back			



User Guide

# 11.3.3 802.11b/g Mode

If you clicked the **802.11b/g Mode** link, the following screen will appear. Access to the Router's wireless network can be controlled by designating a wireless LAN technology specification 802.11b (11 Mbps) or 802.11g (54 Mbps). Use an option that is most compatible with your wireless clients.

ver	i <mark>zon</mark>					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main		Access to the F		I Security Settings	ices using either 802.	.11b
Wireless Status Basic Security Settings Advanced Security Settings		(11 Mbps) or 8	02.11g (54 Mbps) wireles network. Click Apply butt	ss devices. Select the opt on to save your settings. 802.11b/g Mixed 💙	ion that best applies	to
Device List Logout				<u>A Back</u>		

Select the desired mode from the drop-down list, and then click Apply to save the settings.

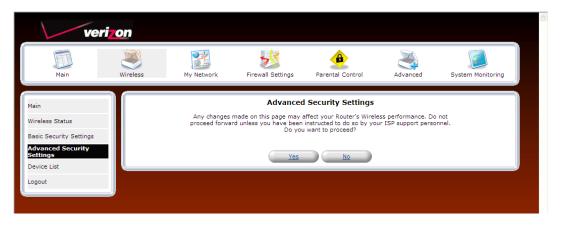
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main				Security Settings		
Wireless Status Basic Security Settings		(11 Mbps) or 80	02.11g (54 Mbps) wireles etwork. Click Apply butte	estricted to wireless devices devices. Select the option to save your settings. 802.11b/g Mixed V	es using either 802. on that best applies t	11b to
Advanced Security Settings Device List				802.11b/g Mixed 802.11g Only 802.11b Only Back		
Logout						



User Guide

# **11.3.4 Other Advanced Wireless Options**

If you clicked the Other Advanced Wireless Options link, the following screen will appear. Click Yes to proceed.



The following screen will appear. Enter the desired values, and then click **Apply** to save the settings. The following table explains the details of this screen.

verizon					
	22		٨	No.	
Main Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Wireless Main Mineless Status Basic Security Settings Advanced Security Device List Logout	Wireless Acc Enable Wireles SSID: SSID Broad 802.11 Mode: Channel: Network Auth MAC Filtering MAC Filtering 00:33:14:ff:bb 00:22:ee:13:2 New MAC Add Transmission CTS Protectio Beacon Inter DTIM Interva Fragmentatic RTS Threshol Maximum Mui Wireless Sect Stations Sect	Advanced ass Point ass: cast mode: Settings MAC Address 222 4:19 ress Rate: n Mode: n Type: cast iticast Data Rate: iticast Data Rate: iticast Data Rate: arthy ticast Data Rate: art	J Security Settings	ation V	System Monitoring



User Guide

	Advanced Security Settings
Wireless Access Point	The Router also functions as a wireless access point for wireless devices.
Enable Wireless	By default, the wireless feature is enabled. To disable this feature, clear the check box.
SSID	The SSID is the name of your wireless network. This string is case-sensitive and must be
	30 characters or less. To connect to the Router, the SSID on a computer's wireless card
	must be identical the SSID on the Router. The Router comes pre-configured with the SSID;
	however, you can change the SSID to any name or code you want.
SSID Broadcast	Select this check box to enable SSID (a check mark will appear in the box).
	When this box is cleared, the Router will not broadcast its SSID.
	When SSID Broadcast is enabled, any computer or wireless device using the SSID of
	"ANY" can see the Router. To prevent this from happening, click the <b>Disable</b> option
	button. This will disable SSID Broadcast so that only the wireless devices that are
	configured with your SSID can access your Router.
802.11 Mode	Allows you to limit access to your Router based on technology type.
	11b only: Communication with the Router is limited to 802.11b
	11g only: Communication with the Router is limited to 802.11g
	802.11 b/g Mixed: Computers using 802.11b or 802.11g rates can communicate with the
<u>Cl</u> 1	Router.
Channel	This is the channel of the frequency band at which the Router communicates.
	The Router transmits and receives data on this channel. The number of channels to choose
	from is pre-programmed into the Router. A computer's wireless card does not have to be
	set to the same channel as the Router; the wireless card can scan all channels and look for a
Network Authentication	Router to connect to. (In the United States, use channels 1 through 11).
Network Authentication	Open System Authentication: If Open System authentication is selected, this will allow any
	station to associate with the wireless network, but only stations with a valid WEP key can send or receive data from the Router.
	Shared Key Authentication: If Shared Key Authentication is selected, a station must
	authenticate with the Router (using the WEP key) before it can connect to the Router's
	wireless network.
	Both: If "Both" is selected, the Router will allow both Open System and Shared Key
	Authentication to be used.
MAC Filtering Mode	Disable: If Disable is selected, MAC Filtering Mode will be deactivated.
	Allow: If Allow is selected, the Router will allow only the devices that are configured in
	the MAC filter table.
	Deny: If Deny is selected, the Router will deny all devices that are configured in the MAC
	filter table.
MAC Filtering Settings	Click this link to add a MAC address to the MAC filtering list. Details on this feature are
6 6	discussed later in this section.
Transmission Rate	Selecting a transmission rate allows you to adjust the bit rate of the Router's wireless
	transmissions. Select a transmission rate from the drop-down list, or select Auto to allow
	the Router to automatically select the best transmission rate.
CTS Protection Mode	Clear to Send (CTS) allows the 802.11 b/g networks to operate a maximum efficiency.
	Auto: Select Auto to activate CTS.
	None: Select None to deactivate CTS.
	Always: Select Always to allow CTS to always be activated.
CTS Protection Type	CTS (Clear to Send) protection mode allows mixed 802.11b/g networks to operate at
	maximum efficiency.
	RTS (Request to Send) controls what size data packet the low level RF protocol issues to
	an RTS packet.



User Guide

	Select cts_only to activate this feature.
	Select cts_rts to activate this feature.
Beacon Interval	Enter the beacon interval value.
(in milliseconds)	The beacon interval is the time between beacon frame transmissions. Beacons are
	transmitted by the Router to help identify wireless networks. Beacons contain rate and
	capability information. Beacons received by stations can be used to identify the wireless
	access points in the area.
DTIM Interval	Enter the DTIM (Delivery Traffic Indication Message) interval value. A DTIM is a
(in milliseconds)	countdown mechanism for the Router. It informs wireless network clients of the next
· · · · · · · · · · · · · · · · · · ·	window for listening to broadcast and multicast messages.
Fragmentation Threshold	Setting the fragmentation threshold can increase the reliability of frame transmissions on
5	the wireless network. Any MAC Service Data Unit (MSDU) or MAC Protocol Data Unit
	(MPDU) larger than this value will be fragmented into an MPDU of the specified size.
RTS Threshold	Enter the RTS (Request to Send) threshold. This setting controls what size data packet the
	low level RF protocol issues to an RTS packet.
	RTS/CTS handshaking will be performed for any data or management MPDU containing a
	number of bytes greater than the threshold. If this value is larger than the MSDU size
	(typically set by the fragmentation threshold), no handshaking will be performed. A value
	of zero will enable handshaking for all MPDUs.
Maximum Multicast Data	The maximum rate (in kb/s) at which multicast packets are transmitted over your network.
Rate	The maximum rate (in Roys) at which manipulate packets are transmitted over your network.
Wireless Security	When this feature is enabled (the box contains a check mark), wireless security is activated,
whereas security	and the security type can be configured.
	When the box is clear, wireless security is deactivated. By factory default, Wireless
	Security is disabled.
Stations Security Type	Set the type of security for the Router's wireless network. Choose from the following
Stations Security Type	options: WPA, WPA2, WPA and WPA2, 802.1x WEP, Non-802.1x WEP, Authentication
	Only. Details on these options are discussed later in this section.
Authentication Method	This is the authentication method used with the security type.
Wireless QoS (WMM)	Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification, based on the IEEE 802.11e
	draft standard. It provides basic Quality of Service (QoS) features to IEEE 802.11
	networks. If your wireless card supports WMM, enable this feature by checking its
	'Enabled' check-box.
Power Save (WMM)	WMM® Power Save is a set of features for Wi-Fi networks that help conserve battery
	power in small devices such as phones, PDAs, and audio players.



User Guide

# **11.3.5** Configuring the Stations Security Type

To configure the Router's wireless security type for the wireless network, in the Advanced Security Settings screen, select an option from the Stations Security Type drop-down list. The following sections describe each security type.

Wireless Status     Wireless Access Point       Enable Wireless:     ✓ Enabled       Basic Security Settings     SSID:       Advanced Security     ✓ SSID Broadcast       Settings     802.11 Mode:       Device List     Channel:       Network Authentication:     Open System Authentication:	veriz	on I		<del>5</del> 1	<u></u>		
Wireless Status Basic Status Basic Status Basic Scurity Settings Advanced Security Settings Device List Logout	Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Settings       B02.11 Mode:       B02.11bg Moved w         Device List       Automatic (FCC)         Logout       Open System Authentication (CCC)         MAC Filtering Mode:       Disble w         MAC Filtering Settings       Action         00:33:14:ff:bb:22       0:22:ee:13:24:19         New MAC Address       0:22:ee:13:24:19         New MAC Address       0:22:ee:13:24:19         New MAC Address       0:22:ee:13:24:19         Transmission Rate:       Auto w         CTS Protection Mode:       Auto w         CTS Protection Type:       rs_cts w         Beacon Interval:       10 ms         DTIM Interval:       1 ms         Fragmentation Threshold:       2346         RTS Threshold:       2347         Maximum Multicast Data Rate:       2000         Vireless Security Type:       Non-802 LX WEP v         Active       Encryption Key       WVPA2         0:1       4C44463747       H         0:2       Asout WWPA2       40 bt w         0:3       Active Consolitation Only       40 bt w         0:4       ASCI W       40 bt w	Main Wireless Status Basic Security Settings		Enable Wireless: SSID:	Point	Enabled		
MAC Address Action   00:33:14:ff:bb:22 )   00:23:14:ff:bb:22 )   00:22:19 )   New MAC Address )   Transmission Rate: Auto ♥   CTS Protection Mode: Auto ♥   CTS Protection Type: rts_cts ♥   Beacon Interval: 10   DTIM Interval: 1   ms Fragmentation Threshold:   2345 RTS Threshold:   Stations Security ♥ Enabled   Vireless Security Type: Non-802:1X WEP   0:1 40 bt ♥   40 bt ♥ 40 bt ♥	Advanced Security Settings Device List Logout		802.11 Mode: Channel: Network Authent MAC Filtering Mod	ication: de:	Automatic V (FCC) Open System Authentic	ation 💌	
CTS Protection Mode: Auto   CTS Protection Type: rts_cts   Beacon Interval: 100 ms   DTIM Interval: 1 ms   Fragmentation Threshold: 2346   RTS Threshold: 2347   Maximum Multicast Data Rate: 2000   Wireless Security V Enabled   Stations Security Type: Non-802 1X WEP   Active Encryption Key   VIPA 40 bit v   4 ASCII v   40 bit v   40 bit v   40 bit v			MAC 00:33:14:ff:bb:22 00:22:ee:13:24:19	Address			
Fragmentation Threshold: 2346   RTS Threshold: 2347   Maximum Multicast Data Rate: 2000   Wireless Security V Enabled   Stations Security Type: Non-802.1X WEP *   Active Encryption Key   VPA2 40 bit *   0 1 4C44463747   VPA2 40 bit *   0 2 Abox -802.1X WEP   0 3 Authentication Only   4 ASCI *   Wireless QoS (WMM) V Enabled			CTS Protection M CTS Protection Ty	ode:	Auto 💙 rts_cts 🗸		
Stations Security Type:       Non-802 1X WEP         Active       Encryption Key       WPA         I       4C44463747       H WPA2       40 bit Image: Additional stress of the stress of t			Fragmentation T RTS Threshold:		2346 2347		
Wireless QoS (WMM) V Enabled			Stations Security Active 1 4C444 2 3 3	Type: Encryption Key	Non-802.1X WEP WPA He WPA2 A 802.1X WEP Non-802.1X WEP A Authentication Only	40 bit 💙 40 bit 💙	
			Wireless QoS (WI		C Enabled	40 bit 💌	



User Guide

## 11.3.5.1 WPA (Wi-Fi Protected Access v.1)

If you select **WPA** in the **Stations Security Type** drop-down list, the following screen will appear. WPA allows you to enable a pre-shared key for your home network or for advanced security for an enterprise network. This option allows stations that support WPA v.1 to connect to the Router.

veri	on			
Main	Wireless	My Network Firewall Settings	Parental Control	System Monitoring
Main		Advanced	l Security Settings	
		Wireless Access Point		
Wireless Status		Enable Wireless:	Enabled	
Basic Security Settings		SSID:	DK9QN	
Advanced Security		SSID Broadcast		
Settings		802.11 Mode:	802.11b/g Mixed 😪	
Device List		Channel:	Automatic 🖌 (FCC)	
Logout		Network Authentication:	Open System Authentication 🗸	
Logout		MAC Filtering Mode:	Disable 💙	
<i>u</i>	2 I I I I I I I I I I I I I I I I I I I	MAC Filtering Settings		
		MAC Address 00:33:14:ff:bb:22	Action	
		00:22:ee:13:24:19	X 🛱	
		New MAC Address	4	
		Transmission Rate:	Auto 🗸	
		CTS Protection Mode:	Auto 🗸	
		CTS Protection Type:	rts_cts 🗸	
		Beacon Interval:	100 ms	
		DTIM Interval:	1 ms	
		Fragmentation Threshold:	2346	
		RTS Threshold:	2347	
		Maximum Multicast Data Rate:	2000	
		Maximum Multicast Data Rate: Wireless Security	Enabled	
		Stations Security Type:	WPA V	
		Authentication Method:	Pre-Shared Key V	
		Pre-Shared Key:	ASCI	
		Encryption Algorithm:	TKIP	
		Group Key Update Interval:	900 Seconds	
		Wireless QoS (WMM)	Enabled	
		Power Save (WMM)		
		Swel Save (will)		
			A Back	

	WPA Wireless Security					
Wireless Security	Factory Default = Enabled					
	When this feature is enabled (the box contains a check mark), wireless security in activated.					
	If the box is cleared, wireless security will be deactivated.					
Stations Security Type	Factory Default = Non-8.2.1x WEP					
	Set the type of security for the Router's wireless network. Choose from the following options:					
	Details on these options are discussed later in this section.					
	WPA – Allows stations that support WPA v.1 to connect to the Router.					
	WPA2 – Allows stations that support WPA v.2 to connect to the Router.					
	WPA and WPA2 – Allows stations that support WPA and WPA2 to connect to the Router.					
	802.1x WEP – Allows stations that support 802.1x WEP to connect to the Router.					
	Non-802.1x WEP – Allows stations that support Non-802.1x WEP to connect to the Router.					
	Authentication Only – Allows stations that support Authentication Only to connect to the Router.					
Authentication Method	Factory Default = Personal (Pre-Shared Key)					



User Guide

	Pre-Shared Key – WPA stations share a pre-shared key (string format) with the Router and do
	not authenticate with the RADIUS server.
	802.1x – WPA stations authenticate with the RADIUS server using EAP-TLS over 802.1x, a
	standard for passing extensible authentication protocol (EAP) for authentication purposes. EAP
	is used to communicate authentication information between the supplicant and the authentication
	server. With 802.1x, EAP messages are packaged in Ethernet frames, rather than using and PPP.
Pre-Authentication	Factory Default = Disabled
	To Enable this feature, click the box (a check mark will appear in the box).
WPA Pre-Shared Key	The WPA key can be either 8 to 63 text (ASCII) characters or 64 hexadecimal (Hex) characters.
	The only allowable hexadecimal characters are: A-F and 0-9.
Encryption Algorithm	Factory Default = TKIP
	Select the encryption algorithm you want to use (TKIP, AES, or TKIP and AES).
	TKIP: Select this option to enable the Temporal Key Integrity Protocol for data encryption.
	AES: Select this option to enable the Advanced Encryption Standard for data encryption.
	TKIP and AES: Select this option to enable the Router to accept TKIP and AES encryption.
Group Key Update	The number of seconds between rekeying the WPA group key. A value of zero means that
Interval (in seconds)	rekeying is disabled.

After you have selected WPA as the security type, select the desired authentication method from the Authentication Method drop-down list.

Main	Wireless	My Network Firewal	Settings Pa	rental Control	Advanced	System Monitoring
ain	1		Advanced Secu	urity Settin	gs	
		Wireless Access Point				
fireless Status		Enable Wireless:	[	Enabled		
asic Security Settings		SSID:		0K9QN		
dvanced Security		SSID Broadcast				
ettings		802.11 Mode:		802.11b/g Mixed	*	
evice List		Channel:		Automatic 🔽 (	FCC)	
		Network Authentication	: · · · · ·	Open System Au	thentication 🛩	
ogout		MAC Filtering Mode:		Disable 🗸		
	~	MAC Filtering Settings				
		MAC Addre 00:33:14:ff:bb:22	255		Action	
		00:22:ee:13:24:19			38	-
		New MAC Address				_
		Transmission Rate:		Auto 🗸	<b>T</b>	
		CTS Protection Mode:		Auto 🗸		
		CTS Protection Type:		rts_cts 🗸		
		Beacon Interval:	-		ns	
		DTIM Interval:				
				2346	ns	
		Fragmentation Thresho RTS Threshold:		2347		
		Maximum Multicast Data		2000		_
		Wireless Security		Enabled		
		Stations Security Type: Authentication Method:		WPA	~	
				Pre-Shared Key Pre-Shared Key		
		Pre-Shared Key:	1	302.1x	ASCI 🛩	
		Encryption Algorithm:				
		Group Key Update Inte		900 Seco	nds	_
		Wireless QoS (WMM)		Enabled		
		Power Save (WMM)	l	Enabled		
			Apply	€ Back		



User Guide

#### 11.3.5.1.1 Authentication Method—Pre-Shared Key

If you select **Pre-Shared key** as the authentication method for WPA, the following screen will appear. Configuring Pre-Shared Key in the Router allows devices that know the pre-shared key to connect to the Router.

**NOTE:** A WPA pre-shared key is treated as either a string of text (ASCII) characters or a set of hexadecimal (Hex) characters. The key can be either 8 to 63 text (ASCII) characters or 64 hexadecimal (Hex) characters. The only allowable hexadecimal characters are: 0-9 and A-F.

To configure the WPA Pre-Shared Key, do the following:

- 1. Select the string type (ASCII or HEX) in the **Pre-Shared Key** drop-down list.
- 2. Enter the desired pre-shared key values in the field provided.
- 3. Select the desired option from the Encryptoin Algorithm drop-down list.
  - TKIP: Select this option to enable the Temporal Key Integrity Protocol for data encryption.
  - AES: Select this option to enable the Advanced Encryption Standard for data encryption.
  - TKIP and AES: Select this option to enable the Router to accept TKIP and AES encryption.
- 4. Enter the desired Group Key Update Interval, and confirm that the adjacent box contains a check mark. (By factory default, Group Key Interval is enabled for 900 seconds.)
- 5. Click **OK** to save the wireless settings in the Router.

Main	Wireless	My Network Firewall Settin	gs Parental Control	Advanced	System Monitoring
n		Adva	nced Security Settings		
		Wireless Access Point			
eless Status		Enable Wireless:	C Enabled		
ic Security Settings		SSID:	DK9QN		
anced Security		SSID Broadcast			
tings		802.11 Mode:	802.11b/g Mixed 💌		
ice List		Channel:	Automatic 💙 (FCC)		
out		Network Authentication:	Open System Authentica	ition 👻	
		MAC Filtering Mode:	Disable 💙		_
		MAC Filtering Settings MAC Address	Ac	tion	
		00:33:14:ff:bb:22	5	*	
		00:22:ee:13:24:19	5	. 🗱	
		New MAC Address		<b>*</b>	
		Transmission Rate:	Auto 🐱		
		CTS Protection Mode:	Auto 💙		
		CTS Protection Type:	rts_cts 🗸		
		Beacon Interval:	100 ms		
		DTIM Interval:	1 ms		
		Fragmentation Threshold:	2346		
		RTS Threshold:	2347		
		Maximum Multicast Data Rate:	2000		
		Wireless Security	C Enabled		
		Stations Security Type:	WPA 💙		
		Authentication Method:	Pre-Shared Key 😪		
		Pre-Shared Key:		ASCI 🗸	
		Encryption Algorithm:	ткір 🛩		
		Group Key Update Interval:	900 Seconds		
		Wireless QoS (WMM)	C Enabled		
		Power Save (WMM)	Enabled		
			Apply & Back		



User Guide

#### 11.3.5.1.2 Authentication Method—802.1x

If you select 802.1x as the authentication method for WPA, the following screen will appear. Configuring 802.1x allows devices that support 802.1x to connect to the Router.

To configure WPA authentication for 802.1x, do the following:

- 1. Select the desired option from the **Encryptoin Algorithm** drop-down list.
  - TKIP: Select this option to enable the Temporal Key Integrity Protocol for data encryption.
  - AES: Select this option to enable the Advanced Encryption Standard for data encryption.
  - TKIP and AES: Select this option to enable the Router to accept either TKIP or AES encryption.
- 2. Enter the desired Group Key Update Interval, and confirm that the box contains a check mark. (By factory default, Group Key Interval is enabled for 900 seconds.)
- 3. Configure the Radius Server:
  - a. Enter the Radius Server IP address in the fields provided.
  - b. Enter the desired Server Port value.
  - c. Enter the Shared Secret.
- 4. Click **OK** to save the wireless settings in the Router.

Main Wireless	My Network Firewall	Settings Parental Control	Advanced	System Monitoring	
Main Wireless	Wireless Access Point Enable Wireless: SSID: ♥SSID Broadcast 802.11 Mode: Channel: Network Authentication: MAC Filtering Mode: MAC Filtering Mode: MAC Address MAC Address MAC Address Transmission Rate: CTS Protection Mode: CTS Protection Type: Beacon Interval: DTIM Interval: Fragmentation Threshold: RTS Threshold: Maximum Multicast Data Wireless Security Stations Security Type: Authentication Method: Encryption Algorithm: ♥ Group Key Update Inter RADUS Server	dvanced Security Settings	c) ntication V Action Action V	System Monitoring	
	Shared Secret: Wireless QoS (WMM)	✓ Enabled			



User Guide

## 11.3.5.2 WPA2 (Wi-Fi Protected Access v. 2)

If you select **WPA2** in the **Stations Security Type** drop-down list, the following screen will appear. This option allows stations that support WPA v.2 to connect to the Router. The configuration settings for WPA2 are similar to the settings in WPA. Please refer to section 11.3.5.1 for instructions on configuring WPA2.

ver	ri <mark>zo</mark> n					
T	۷		<u>i</u>	3		
Main	Wireless	My Network Firewal	l Settings Parental Control	Advanced	System Monitoring	
	~					
Main			Advanced Security Setting	js		
		Wireless Access Point				
Wireless Status		Enable Wireless:	✓ Enabled			
Basic Security Settings		SSID:	DK9QN			
Advanced Security		SSID Broadcast				
Settings		802.11 Mode:	802.11b/g Mixed	~		
Device List		Channel:	Automatic 🗸 (F			
		Network Authentication				
Logout		MAC Filtering Mode:	Disable 🗸			
	-	MAC Filtering Settings				
		MAC Addre	255	Action		
		00:33:14:ff:bb:22		- N 🗱		
		00:22:ee:13:24:19		_\ <b>X</b>		
		New MAC Address				
		Transmission Rate:	Auto 🗸			
		CTS Protection Mode:	Auto 🛩			
		CTS Protection Type:	rts_cts 🗸			
		Beacon Interval:	100 m	IS		
		DTIM Interval:	1 m	IS		
		Fragmentation Thresho	ld: 2346			
		RTS Threshold:	2347			
		Maximum Multicast Data	a Rate: 2000			
		Wireless Security	✓ Enabled			
		Stations Security Type:		~		
		Authentication Method:		~		
		Pre Authentication	002.10			
		Encryption Algorithm:	AES 🗸			
		Group Key Update Inte				
		RADIUS Server	secon secon	lus		
		Server IP:	0.0	. 0 . 0		
		Server Port:	1812	······		
		Shared Secret:	1012			
			Enabled			
		Wireless QoS (WMM)	Enabled			
		Power Save (WMM)				
			Apply & Back			
			- Appry - Dack			



User Guide

## 11.3.5.3 WPA and WPA2

If you select **WPA2 and WPA2** in the **Stations Security Type** drop-down list, the following screen will appear. This option allows stations that support both WPA v.1 and WPA v.2 to connect to the Router. The configuration settings for this feature are similar to the settings in WPA. Please refer to section 11.3.5.1 for instructions on configuring WPA and WPA2.

		ے 🔒		
Main Wireless	My Network Firewall Settings	Parental Control Advanced	System Monitoring	
lain	Advanced	l Security Settings		
ireless Status	Wireless Access Point			
	Enable Wireless:	🗹 Enabled		
asic Security Settings	SSID:	DK9QN		
dvanced Security ettings	SSID Broadcast			
	802.11 Mode:	802.11b/g Mixed 💙		
Device List	Channel:	Automatic V (FCC)		
ogout	Network Authentication:	Open System Authentication 🗸		
	MAC Filtering Mode:	Disable 🗸		
	MAC Filtering Settings MAC Address	Action		
	00:33:14:ff:bb:22	\ <b>X</b>		
	00:22:ee:13:24:19	N 84		
	New MAC Address	4		
	Transmission Rate:	Auto 🗸		
	CTS Protection Mode:	Auto 👻		
	CTS Protection Type:	rts_cts 🗸		
	Beacon Interval:	100 ms		
	DTIM Interval:	1 ms		
	Fragmentation Threshold:	2346		
	RTS Threshold:	2340		
	Maximum Multicast Data Rate:	2000		
	Wireless Security	Enabled		
	Stations Security Type:	WPA and WPA2 V		
	Authentication Method:	802.1x		
	Pre Authentication	AES		
	Encryption Algorithm:			
	Group Key Update Interval:	900 Seconds		
	RADIUS Server	0 . 0 . 0 . 0		
	Server Port:			
		1812		
	Shared Secret:			
	Wireless QoS (WMM)	Enabled		
	Power Save (WMM)	Enabled		



User Guide

## 11.3.5.4 802.1x WEP

If you select **802.1x WEP** in the **Stations Security Type** drop-down list, the following screen will appear. The 802.1x WEP feature allows you to enable WEP keys for wireless security. In addition, 802.1x WEP security uses a Remove Authentication Dial-in Service (RADIUS) server for authentication purposes. The server must be physically connected to the Router. The Router's card supports 40-bit or 104-bit WEP encryption. If 802.1x WEP is used, any station can connect to the Router as long as its SSID and WEP key values match the Router's values.

**NOTE**: Client PCs can use any Wireless 802.11b/g card to communicate with the Router. By default your Router is configured (enabled) for 802.1X WEP (Wired Equivalent Privacy) security. Whenever, WEP is configured, the PC's wireless card must use the same WEP security code type as the one provided in Router. The WEP security code is located on a label on the bottom of the Router. Always check that your PC's wireless adapter is configured properly for whichever network setting you use: WEP or WPA. You can configure the settings in the advanced properties of the PC's wireless network adapter.

Main	Wireless	My Network Firewall Settings	Parental Control	System Monitoring
n		Advanced	l Security Settings	
		Wireless Access Point		
eless Status		Enable Wireless:	🔽 Enabled	
ic Security Settings		SSID:	DK9QN	
anced Security		SSID Broadcast	·	
vanced Security tings		802.11 Mode:	802.11b/g Mixed 💙	
rice List		Channel:	Automatic 🗸 (FCC)	
		Network Authentication:	Open System Authentication 🗸	
out		MAC Filtering Mode:	Disable 🗸	
	2 I	MAC Filtering Settings		
		MAC Address 00:33:14:ff:bb:22	Action	_
				_
		00:22:ee:13:24:19	<b>A</b>	_
		New MAC Address		
		Transmission Rate:	Auto 🗸	
		CTS Protection Mode:	Auto 🗸	
		CTS Protection Type:	rts_cts 🗸	
		Beacon Interval:	100 ms	
		DTIM Interval:	1ms	
		Fragmentation Threshold:	2346	
		RTS Threshold:	2347	
		Maximum Multicast Data Rate:	2000	
		Wireless Security	C Enabled	
		Stations Security Type:	802.1X WEP	
		🔽 Generate Keys Automatically	(Disable to allow 802.1x-MD5 stations to connect)	
		Group Key Update Interval:	900 Seconds	
		RADIUS Server		
		Server IP:	0.0.0.0	
		Server Port:	1812	
		Shared Secret:		
		Wireless QoS (WMM)	✓ Enabled	
		Power Save (WMM)	Enabled	
			Z Back	



User Guide

#### 11.3.5.4.1 Configuring Automatic WEP Encryption Keys

The 802.1x WEP security protocol uses port control with dynamically changing encryption keys automatically updated over the network. To configure 802.1x WEP to generate keys automatically, do the following:

1. Select the **Generate Keys Automatically** check box if you want the Router to automataically create the WEP security keys. A check mark will appear in the box, and the **Encryption Key** table will be removed from the screen.

**NOTE:** Disable (clear) the **Generation Keys Automatically** check box to allow 802.1x-MD5 stations to connect to the Router

- 2. Enter the desired Group Key Update Interval, and confirm that the box contains a check mark. (By factory default, Group Key Interval is enabled for 900 seconds.)
- 3. Configure the Radius Server:
  - a. Enter the Radius Server IP address in the fields provided.
  - b. Enter the desired Server Port value.
  - c. Enter the Shared Secret.
- 4. Click **OK** to save the wireless settings in the Router.

#### 11.3.5.4.2 Configuring Manual WEP Encryption Keys

To configure 802.1x WEP with manual encryption keys, do the following:

1. Clear the Generate Keys Automatically check box. The Key Encryption table will appear in the screen.

**NOTE:** Disable (clear) the Generation Keys Automatically check box to allow 802.1x-MD5 stations to connect to the Router.

- 2. At the Key Encryption table, select a key (1 through 4) that you want to activate.
- 3. Enter the desired encryption key.

**NOTE:** A WEP encryption key is treated as either a string of text (ASCII) characters or a set of hexadecimal (Hex) characters. The number of text characters must be either 5 (for 40 bit encryption) or 13 (for 104 bit encryption). The number of Hex characters must be either 10 (for 40 bit encryption) or 26 (for 104 bit encryption). The only allowable hexadecimal characters are: A-F and 0-9.

- 4. Select the Entry Method (ASCII or Hex) from the drop-down list.
- 5. Select the Key Length (40 bit or 104 bit) from the drop-down list.
- 6. Enter the desired Group Key Update Interval, and confirm that the box contains a check mark. (By factory default, Group Key Interval is enabled for 900 seconds.)
- 7. Configure the Radius Server by doing the following:
  - a. Enter the Radius Server IP address in the fields provided.
  - b. Enter the desired Server Port value.
  - c. Enter the Shared Secret.
- 8. Click **OK** to save the wireless settings in the Router.



User Guide

### 11.3.5.5 Non-802.1x WEP

If you select **Non-802.1x WEP** in the **Stations Security Type** drop-down list, the following screen will appear. The Non-802.1x WEP feature allows you to enable a WEP key for wireless security without using a RADIUS server. The Router's card supports 40-bit or 104-bit WEP encryption. Whenever Non-802.1x WEP is used, any station can connect to the Router as long as its SSID and WEP key values match the Router's values.

To configure the Router for Non-802.1x WEP, do the following:

- 1. At the Key Encryption table, select a key (1 through 4) that you want to activate.
- 2. Enter the desired encryption key.

**NOTE:** A WEP encryption key is treated as either a string of text (ASCII) characters or a set of hexadecimal (Hex) characters. The number of text characters must be either 5 (for 40-bit encryption) or 13 (for 104-bit encryption). The number of Hex characters must be either 10 (for 40-bit encryption) or 26 (for 104-bit encryption). The only allowable hexadecimal characters are: A-F and 0-9.

- 3. Select the Entry Method (ASCII or Hex) from the drop-down list.
- 4. Select the Key Length (40 bit or 104 bit) from the drop-down list.
- 5. Click **OK** to save the wireless settings in the Router.

veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main			Advanced	l Security Settings			
		Wireless Acco	ess Point				
Wireless Status		Enable Wirele		Enabled			
Basic Security Settings		SSID:		DK9QN			
Advanced Security Settings		SSID Broad	cast				
Settings		802.11 Mode:		802.11b/g Mixed 💟			
Device List		Channel:		Automatic 💙 (FCC)			
Logout		Network Auth		Open System Authenti	cation 🔽		
		MAC Filtering		Disable 💙			
		MAC Filtering	Settings MAC Address		Action		
		00:33:14:ff:bb					
		00:22:ee:13:24	4:19		X 🗱		
		New MAC Add	ress		4		
		Transmission	Rate:	Auto 🔽			
		CTS Protectio	n Mode:	Auto 🔽			
		CTS Protectio	n Type:	rts_cts 💟			
		Beacon Inter	val:	100 ms			
		DTIM Interva	l:	1 ms			
		Fragmentatio	n Threshold:	2346			
		RTS Threshol	d:	2347			
		Maximum Mul	ticast Data Rate:	2000			
		Wireless Secu	irity	C Enabled			
		Stations Secu	rity Type:	Non-802.1X WEP			
		Active	Encryption Key	Entry Method	Key Length		
		1     40	244463747	Hex 💙	40 bit 🗸		
		O 2		ASCII 🗸	40 bit 🔽		
		O 3		ASCII 🛩	40 bit 🔒		
		O 4		ASCI 💙	40 bit 🛩		
		Wireless QoS	(WMM)	Enabled			
		Power Save (	WMM)	Enabled			
				Y Back			



User Guide

### 11.3.5.6 Authentication Only

If you select **Authentication Only** in the **Stations Security Type** drop-down list, the following screen will appear. This feature allows you to enable wireless security in your Router without using encryption keys or a RADIUS server. However, a station's SSID must match the Router's SSID in order to connect to the Router.

veri	Ton				
Main	Wireless	My Network Firewall Settings	Parental Control	Advanced	System Monitoring
Main		Advance	d Security Settings		
Wireless Status Basic Security Settings Advanced Security Device List Logout		Wireless Access Point Enable Wireless: SSID: ✓ SSID Broadcast 802.11 Mode: Channel: Network Authentication: MAC Filtering Mode: MAC Filtering Settings MAC Address 00:33:14:ff:bb:22 00:22:ee:13:24:19 New MAC Address Transmission Rate: CTS Protection Mode: CTS Protection Type: Beacon Interval: DTIM Interval: Fragmentation Threshold: RTS Threshold: Maximum Multicast Data Rate: Wireless Security Stations Security Type: Authentication Method:	Clean Mac List	ion	
		Wireless QoS (WMM) Power Save (WMM)	Enabled     Enabled		



# **12. MY NETWORK**

This section provides details on your Router's network connections.

## **12.1 Network Status**

To view your Router's network settings, from the top navigation menu, select **Network Connections**. The following screen appears. This screen displays information about the devices connected to your local area network (LAN). Click **Refresh** to update this screen and display the most current information about devices on your network.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
ain etwork Status etwork Connections ogout	2	Name: Tonnection: Status: IP Address: IP Address: MAC Address: Vane: Connection: Status: IP Address Source: MAC Address:	salle:xp2 Computer (jf) Wireless Online 192.168.1.3 Static 00:03:c9:4f:12:66 salle:xp3 Computer ************************************	work Status     Website Blocking     Block Internet     Block Internet     Access Shared Files     Merc Device Details     Delate This Device      Website Blocking     Block Internet     More Device Details     More Device Details     More Device Details     Delate This Device      Website Blocking     Block Internet     Block Internet     Scalad Application     Delate This Device	Connected Dev To Ethernet: () Wireless: All Interfaces: Auto-Scan En Delste All on Scan for New Befresh this i	1 device(s) 1 device(s) 2 device(s) abled vices Devices
			C	O Refresh		

	Network Status
Name	The name of the device.
Туре	The type of device connected to the network.
Connection	The interface used to connect to the Router. Ethernet: Displays the number of devices that are connected to the Router via Ethernet 10/100 BaseT connection. Wireless: Displays the number of devices that are connected to the Router wirelessly. Note: If you have computers on your network that are not being displayed, check the firewall setting on the PCs to ensure that the firewall is disabled.
Status	The status of the Inernet connection.
IP Address	The IP address assigned to the computer.
IP Address Source	The method by which the computer receives its IP address.
MAC Address	The Media Access Controller; the hardware address assigned to the device by the manufacturer.
Connected Devices	The interface used to connect the device to the Router, and the devices connected. Ethernet: Displays the number of devices that are connected to the Router via Ethernet 10/100 BaseT connection. Wireless: Displays the number of devices that are connected to the Router wirelessly. Note: If you have computers on your network that are not being displayed, check the firewall setting on the PCs to ensure that the firewall is disabled.
Delete All Devices	Click this link to delete all devices from your network.
Scan for New Devices	Click this link to allow the Router to scan the network for new devices that may have recently connected to the network.

User Guide



User Guide

# 12.1.1 Website Blocking

You can configure your Router to restrict access to certain websites to computers on your network. On the **Network Status** page, when you click the **Website Blocking** link it will take you to the **Parental Control** section.

Note: Please refer to the Parental Control Section for more information on setting up parental controls.

veri	on								
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring			
Main Parental Control				ental Control from the LAN to websites	i.				
Logout		ocal Host Local Add	ress Restricted	Website Restricte	ed IP Address	Status Action			
		Press the <b>Refresh</b> button to update the data.							
		✓ OK I Apply X Cancel Resolve Now O Refresh							

The following screen will appear. In the **Restricted Website** field, enter the URL of the website to which you want to restrict access. From the Local Host drop-down list, select the local host device to which you want to apply this restriction.

- Select **Always** to allow the rule to be active all the time.
- Select User Defined to allow the rule to be active only at certain time, as defined by the rules you set up.

If desired, select a schedule from the **Schedule** drop-down list. If you select **User Defined**, refer to the procedure explained in section 15.19, "Scheduler Rules," to set up a schedule rule. Otherwise, select **Always**, and then click **OK** to continue.

ver	i <b>zo</b> n						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Restricted Website				icted Website			
Logout	Loc	stricted Website: cal Host hedule		Any 🗸 Always 🗸			
				X Cancel			



User Guide

After you have entered the desired values in the preceding **Restricted Website** screen and click **OK**, the following screen will appear. To edit an entry, click the pencil icon. To delete an entry, click the "X" icon.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Restricted Website				icted Website osite you wish to restrict:		
Logout		Restricted Website: Local Host		www.homework.com		
		Schedule Name				Action
		Saturday Restrictions	Sat between 08:0	Settings 10-05:00 on the next day		
				Cancel		



User Guide

## **12.1.2 Block Internet Services**

In the **Network Status** page, click the **Block Internet Services** link. The following **Access Control** screen will appear. This feature allows you to block specific computers within the local network (or even the entire network) from accessing certain services on the Internet. For example, one computer can be prohibited from surfing the Internet, another computer from transferring files using FTP, and the whole network from receiving incoming email. To configure Access Control, click the **New Entry** link.

ver	i <mark>zon</mark>						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main General				ess Control et services from within the	e LAN.		
Access Control Port Forwarding	New E	Local Host ntry	Local Address	Protocols	Status	Action	
DMZ Host Port Triggering			Apply	X Cancel Resolve 1	Now Q Refres	h	
Remote Administration							
Remote Administration Static NAT							
Static NAT							
Static NAT Advanced Filtering							

If you clicked **New Entry**, the following screen will appear. Enter the desired values in this screen, and then click **OK** to save the settings.

Image: Name       Image: Name	veriz	on					
Add Access Control Rule Add Access Control Rule Address Any Protocols Any Protocols Any CReply an HTML Page to the Blocked Client Schedule Always	Main	Wireless	My Network	Firewall Settings	<u> </u>	Advanced	System Monitoring
Address Any  Protocols Any  Reply an HTML Page to the Blocked Client Schedule Always	Main Add Access Control Rule			Add Acc	ess Control Rule		
Reply an HTML Page to the Blocked Client      Schedule      Always							
Schedule Always 💌	Logour				Any 💙		
				e Blocked Client			
✓ OK X Cancel			Schedule		Always 🗸		
					X Cancel		



User Guide

### 12.1.2.1 Selecting an Address

From the **Address** drop-down list, select the desired computer for which you want to apply access. Your detected computers should appear in the list.

veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main			Add Acc	cess Control Rule			
Add Access Control Rule	Pro	<b>dress</b> otocols Reply an HTML Page to tl	he Blocked Client	Any  Any User Defined SALLE-XP3 SALLE-XP2			
		hedule		Always ¥			
			<u> </u>	X <u>Cancel</u>			

After you have selected a computer, the following screen will appear. Proceed to section 12.1.2.2 to select a protocol.

veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Add Access Control Rule			Add Acc	cess Control Rule			
Logout		Address Name DHCP Add	SALLE-XP3	Address		Action	
		Protocols Reply an HTML Page to t Schedule	the Blocked Client	Any 👻 Always 👻			
			√ ok	X Cancel			



User Guide

## 12.1.2.2 Selecting a Protocol

From the **Protocols** drop-down list, select the desired option that you want to prohibit the computer from using. You can opt to redirect the user to a browser message (HTML page) by clicking the check box. To disable this feature, click to clear the check box.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Access Control Rule			Add Acc	ess Control Rule		
Logout		Address Name DHCP	SALLE-XP3	Address		Action
	" I I	Add	SALLE-AFS			· · · · · · · · · · · · · · · · · · ·
		Protocols		Any 🗸		
		Reply an HTML Page to t	he Blocked Client	Any User Defined		
		Schedule		Show All Services FTP		
				HTTP		
				HTTPS IMAP		
			✓ OK	L2TP Ping		
			UK DK	POP3		
				SMTP		
				Telnet		
				TFTP		
				Traceroute		

After you have selected the protocol, the following screen will appear. Proceed to section 15.19 to configure a schedule rule.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Add Acc	ess Control Rule		
Add Access Control Rule	Addre					
Logout		Name		Address		Action
-	DHCP		SALLE-XP3			*
	Add	~				
	Proto					
		Name		Ports		Action
		File Transfer	TCPAny -> 21			*
	Add	*				
	Re	ply an HTML Page to t	he Blocked Client			
	Sched			Always 🗸		
			<u> √ ok</u>	X Cancel		



User Guide

## 12.1.2.3 Configuring a Schedule Rule

You can choose to only apply the rule during a particular time, or a particular day. This is done via the Schedule Rule. You may select and already defined schedule from the drop down list, or define your own schedule. If you select **User Defined**, refer to the procedure explained in section 15.19, "Scheduler Rules," to set up a schedule rule. Otherwise, select **Always** to always enforce the rule, and then click **OK** to continue.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Access Control Rule			Add Acc	ess Control Rule		
		Address		Any 💙		
Logout		Protocols		Any	*	
	2 I I I	Reply an HTML Page to th	ne Blocked Client			
		Schedule		Always 💙		
				Always User Defined		
				X Cancel		

## 12.1.2.4 Completing the Access Control Rule Configuration

After you have entered the desired values in the Access Control Rule screen and clicked OK, following screen will appear. Click OK to save the settings.

Veri	Vireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitorir
1ain	1		Add Acc	ess Control Rule		
Add Access Control Rule	Addr					
Logout		Name		Address		Action
	DHCP		SALLE-XP3			*
	Add					
	Proto					
		Name File Transfer	7000 04	Ports		Action
			TCPAny -> 21			<b>A</b>
	Add	*				
	Re	ply an HTML Page to t	he Blocked Client			
	Sche	dule				
		Name		Settings		Action
	Sched	luler Rule	Sun between 05:0	0-05:00 on the next day		🔨 🗶



User Guide

If you clicked **OK**, the following screen will appear. The Router is attempting to resolve the configuration. Click **Resolve Now** to continue.

ver	<b>7</b> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main General				ccess Control	he LAN.	
Access Control		ocal Host	Local Address	Protocols FTP - TCP Any -> 21	Status Resolving	Action
Port Forwarding DMZ Host		Entry SALL	CARS (Unresolved)	FIF - TOP ANY -> 21	Kesolving	4
Port Triggering Remote Administration			Apply	X Cancel Resolve	Now	sh
Static NAT						
Advanced Filtering Security Log						
Connections						

The **Resolve Now button** will translate the rule from the computer name to the correct IP address (all rules are actually controlled by the IP address) If you clicked **Resolve Now**, the following screen will appear. The rule has been added to the list of security rules. To disable the security rule for an entry, click the adjacent check box, and then click **Apply**. To add additional access control rules, click the **New Entry** link.

veri	on					
Main	Wireless	My Netw	ork Firewall Sett	ings Parental Control	Advanced	System Monitoring
Main General			Block access t	Access Control o Internet services from withi	n the LAN.	
Access Control		Local Host	Local Address	Protocols	Status	Action
Port Forwarding		SALLE-XP3 w Entry	SALLE-XP3	FTP - TCP Any -> 21	Inactive	
DMZ Host						
Port Triggering						
Remote Administration				Cancel Reso	Ive Now	sh
Static NAT						
Advanced Filtering						
Security Log						
Connections						
Logout						
L						



User Guide

# **12.1.3 Access Shared Files**

In the **Network Status** page, click the **Access Shared Files** link to access files from a device on your local network. (The device from which you will access files must have file sharing enabled.) If the device has a firewall turned on, you will not be able to access shared files from the device.

D-3238-1714 (Hmcgr-xp) - Mic File Edit View Favorites Tools		
File       Edt       Vew Favorites       Tools         Petwork Tasks       Image: Comparison of the text of the text of the text of the text of t	Sheduled Tasks	
2 objects		



User Guide

# **12.1.4 View Device Details**

In the Network Status page, click the View Device Details link. The following screen will appear. Click Refresh to refresh the details on this screen. After you have finished viewing this screen, click OK to return to the Network Status page.

ver	i <b>zo</b> n						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Network Status Network Connections Logout		Name: Type: Connection: Status: IP Address: IP Address Sou MAC Address: UPnP: NetBIOS:	salle-xı Compu (r) Wir Online 192,16 rce: Static	ter eless 8.1.3 c9:4f:12:66 d	Website Block     Block Internet     Access Share     Enable Applics     Rename Devic     Delete This De	<u>: Services</u> <u>d Files</u> ation ce	
				Refresh			



User Guide

# **12.1.5 Enable Application**

In the **Network Status** page, click the **Enable Application** link to set up applications for your service profile, such as port forwarding services. This feature enables applications (Games, Webcams, IM & Others) by opening a tunnel between remote (Internet) computers and a specific device port inside your local area network (LAN). Details on this screen are discussed later in section 13.3, "Port Forwarding."

ver	<mark>7</mark> 0n						
Main	Wireless	My Network	Firewall Settings	Parenta	Control	Advanced	System Monitoring
Main General			Po Expose services on	<b>rt Forward</b> the LAN to exi	-	sers.	
Access Control Port Forwarding	✓ local			Public IP Address	Protocols TCP Any -> 456	Status 7 Active	Action
DMZ Host Port Triggering Remote Administration	<u>New E</u>	ntry					4
Remote Administration Static NAT Advanced Filtering		<u> √ ok</u>		X <u>Cancel</u>	Resolve No	w Refre	esh
Security Log							
Logout							



User Guide

## 12.1.6 Rename Device

In the **Network Status** page, click the **Rename Device** link. This screen allows you to rename a device on your network. In the following screen, type the desired name in the **Name** field. Next, click **OK** to allow the changes to take effect. Click **Cancel** to return to the **Network Status** page.

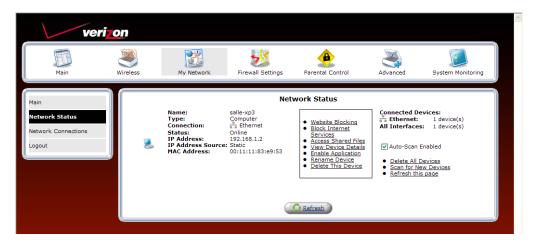
ve	ri <mark>zon</mark>						1		
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring			
Main			Rer	name Device					
Rename Device		Rename Device							
	IP Addr Name:	ess:	192.168.1.3 salle-xp2						
			<ul> <li>▲ <u>ok</u></li> </ul>	X Cancel					



User Guide

## **12.1.7 Delete Device**

In the Network Status page, click the Delete Device link to remove a device from your network.



## **12.2 Network Connections**

Your Router supports various local area network (LAN) and wide area network (WAN, on Internet) connections via Ethernet or coaxial cables. The Network Connections screen is used to configure the various parameters of the Router's network and Internet connections, and to create new connections.

To edit your connection settings, from the top navigation menu, select **My Network.** Next, select **Network Connections** in the left submenu. The following screen will be displayed.

First, determine which screen you are viewing by looking at the buttons on the bottom of the page. If the third button from the left displays **Advanced**, as shown below, this means you are viewing the basic Network Connections screen. To go to the advanced Network Connections screen, click the **Advanced** button.

veri	on					_
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main				rk Connections		
Network Status	Jel Net	twork (Home/Office)	Name		<u>Status</u> Connected	Action
Network Connections		adband Connection (Co	oax)		Connected	
		N PPPoE			Connected	× ×
Logout	New Co	nnection				4
			Quick Setup	Status Advan	<u>ced &gt;&gt;</u>	



User Guide

If the third button from the left displays **Basic**, as shown below, this means you are viewing the advanced Network Connections screen. To go to the basic screen, click the **Basic** button. The advanced Network Connections screen displays links that allow you to access various connection settings in your Router. The following sections describe different network connections available on the Router, as well as the connection types that can be created.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
in			Netwo	rk Connections		
Network Status			Name		Status	Action
	Vetv	work (Home/Office)			ected	A 🗱
etwork Connections		<u>Coax</u>		Dow	1	<u> </u>
gout	S	Ethernet Switch		1 Po	ts Connected	<u> </u>
gout	) 🌒	Wireless 802.11g Acc	ess Point	Conr	ected	🔨 🎇
	Sec. Broa	adband Connection (Et	hernet)	Disa	bled	<u> </u>
	S Broa	adband Connection (Co	pax)	Conr	ected	<u> </u>
	NAM 🖉	N PPPoE		Conr	ected	🔨 🎇
	New Cor	nnection				4



User Guide

# 12.2.1 Network (Home/Office) Properties

In the **Network Connections** screen, click the **Network (Home/Office)** link to access the Router's local network properties. The Network (Home/Office) connection is a bridge that is used to combine several network devices under one single "virtual network". For example, a home/office network can be created that includes your Ethernet Switch as well as your Wireless computers. Network (Home/Office) is the Router's default setting.

At this screen, do any of the following:

- Click the Ethernet Switch link to edit the Router's Ethernet Switch properties.
- Click the **Coax** link to edit the Router's Coax properties.
- Click the Wireless 802.11g Access Point link to edit the Router's Wireless 802.11g Access Point properties.
- Click the IP Address Distribution link to access the Router's IP Address Distribution settings.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Network (Ho	ne/Office) Propert	ties	
Connection Properties Configure Connection Routing Bridging Advanced Logout		Name: Device Name: Status: Network: Underlying Devi Gonnection Typ MAC Connection Typ MAC Connection Typ MAC droftes: Subnet Mask: <u>IP Address Diat</u> Packets Sent To Packets Receiv Time Span:	e: <u>ribution:</u> ital:	Network (Home/Office br:0 network (Home/Office Network (Home/Office Enternet: Switch Coax Wirreless 802,11a A Bridge 00042,188,11 255,255,255,00 DHCP Server 83869 17316 23338:12	ice) ccess Point	
				! Apply	ncel	



User Guide

## 12.2.1.1 Ethernet Switch Properties

For example, if you click the **Ethernet Switch** link in the **Network (Home/Office) Properties** screen, the following screen appears. View the properties in this screen. If you change the connection name, click **Apply** to save the changes. Then, click **OK** to return to the **Network Connections** screen.



## 12.2.1.2 COAX

If you click the **Coax** link in the **Network (Home/Office) Properties** screen, the following screen will appear. View the coax properties in this screen. If you change the connection name, click **Apply** to save the changes. Then, click **OK** to return to the **Network Connections** screen.





User Guide

## **Configure Connection (Coax)**

If you select **Configure Connection** from the left submenu, the following screen will appear. In this screen, you can do any of the following:

- Enter the desired properties for the coax connection, and then click Apply to save the settings.
- Click the View Coax Node Detailed Stats link to view the Coax statistics page
- Click the **Go to Coax Stat** link to view the coax statistics

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Cor	figure Coax		
Connection Properties Configure Connection Logout		General Device Name: Status: Schedule: Network: Connection Ty	/pe:	LAN-en2210 Down Always V Network (Home/Office Multimedia over Coa		
		MOCA Settings Vendor ID: Channel: Operating Fre MOCA QoS: MOCA Privacy:	quency:	WESTELL Automatic Channel Sca Scanning in Progres P Enabled		
		Password: CM Ratio: <u>View Coax Node</u> Go to Coax Stat	e Detailed Stats	66947388374966 Network Coordinator	🔘 Client 💿 Auto	
				! Apply X Can		



User Guide

#### View Coax Node Detailed Stats

If you clicked the **View Coax Node Detailed Stats** link in the **Configure Coax** screen, the following screen appears. This screen displays information on the Router's MoCA stats.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
			Coax No	ode Detailed Stats		
Detailed Stat	Detailed S	stats				
Detailed Stat	Node Id:			0		
t	Link State Network S			DOWN		
•	CM Ratio:	state:		CM		
	BestCMNo	deId:		0		
	BackupCM	NodeId:		ō		
	SOC Stats	:	-			-
	TX Maps:		0	RX Maps:		0
	TX Map Err	ors:	0	RX Map Errors:		0
	TX Rsrv:		0	RX Map Dropped: RX Rsrv:		0
	TX RSIV:		0	RX RSIV: RX RSIV Errors:		0
	TX RSTV ET	rors:	0	RX Rsrv Dropped:		0
	TX LC:		432	RX LC:		0
	TX LC Erro	re-	432	BX LC Errors:		0
	TX EC EITO	19.	0	RX LC Dropped:		0
	TX Adm:		1377	RX Adm:		432
	TX Adm Er	rors:	0	RX Adm Errors:		12
				RX Adm Dropped:		20859
	TX Probes:		0	RX Probes:		0
	TX Probe E		0	RX Probe Errors:		0
				RX Probe Dropped:		0
	TX Async:		0	RX Async:		0
	TX Async E	rrors:	0	RX Async Errors:		0
				RX Async Dropped:		0
	Ctl Descr F		0	Upd Descr Failed:		0
	Stat Descr		0	Buf Alloc Failed:		0
	RS bytes o	orr:	0			
	Events:		1502	Interrupts:		1404
	Other Info					
	RF Freque Network 1			1150.0 Fully Meshed		
	Node Bit I			0x01		
	TX Channe		0x00			0×00
	TX IQ Imb		0	RX IQ Imbalance (I):		0
	TX IQ Imb		0	RX IQ Imbalance (Q)		0
		alance (D)):	0	RX IQ Imbalance (D)		0

### Go to Coax Stats

If you clicked the **Go to Coax Stats** link in the **Configure Coax** screen, the following screen appears. This screen displays the Tx/Rx rate between the Router and other devices or nodes in a MoCA network. View the information in this screen, and then click **Close** to return to the **Configure Coax** screen.

Main	Wireless My Ne	twork Firewall Se	ttings	Parental C	Control	Adva	nced	System	Monitoring
1ain			Соа	x Stats					
Coax Connection Stats	Coax Settings Channel: MOCA Privacy: Password:		Automatic Disabled 66947388374966						
	Coax Stats								
	Connection Speed		Node 1		Node 3	Node 4			Node 7
	MAC Address	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	IP Address	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 0 (Router)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 5	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 7	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A



User Guide

### 12.2.1.3 Wireless 802.11g Access Point

To view the wireless access properties, in the Network (Home/Office) Properties screen, click the Wireless 802.11g Access Point link.

ver	i <mark>70</mark> n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Network (Ho	me/Office) Propert	ties	
Connection Properties Configure Connection		Name: Device Name: Status: Network:		Network (Home/Office br0 Connected Network (Home/Off Ethernet Switch	,	
Routing Bridging Advanced		Underlying Dev Connection Typ MAC Address: IP Address:		Coax Wireless 802.11g A Bridge 00:18:3a:a4:96:b6 192.168.1.1		
Logout	J	Subnet Mask: <u>IP Address Dist</u> Packets Sent To Packets Receiv Time Span:	otal:	255.255.255.0 DHCP Server 86330 17847 24:05:48		
					Disable	

The following screen will appear. View the wireless properties in this screen. If you change the connection name, click **Apply** to save the changes. Then, click **OK** to return to the **Network Connections** screen.

ver	<mark>7</mark> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Wireless 802.11	g Access Point Proj	perties	
Connection Properties Configure Connection Wireless Status Basic Security Settings Advanced Security Settings Device List Advanced		Name: Device Name: Status: Network: Connection Typ Download Rate: Upload Rate: MAC Address IP Address Dist Encryption: Packets Receive Time Span:	ribution: otal:	Network (Home/Office ath0 Connected Network (Home/Off Wireless 802.11g Ar 54 MB 00:1d:19:12:e0:fd Disabled WEP 4445 1121 4:19:07	ice)	
Logout				: Apply	ncel	



User Guide

### **Configure Connection—Wireless Access Point**

If you select **Configure Connection** from the left submenu, the following screen will appear. Configure your wireless access point properties, and then click **Apply** to save the settings.

Please refer to section 11, "Wireless," for details on the following wireless features listed in the left submenu of this screen.

- Wireless Status
- Basic Security Settings
- Advanced Security Settings
- Device List
- Advanced

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Configure Wirele	ess 802.11g Access	i Point	
Connection Properties Configure Connection Wireless Status		General Device Name: Status: Schedule: Network: Connection Ty Physical Addr	/pe:	ath0 Connected Always V Network (Home/Office Wireless 802.11g A 00:1d:19:12:e0:fd		
Basic Security Settings Advanced Security Settings Device List		MTU:			1500	
Advanced Logout						

### 12.2.1.4 IP Address Distribution

If you click the **IP Address Distribution** link in the **Network (Home/Office) Properties** screen, the following screen appears. This screen allows you to access your Router's DHCP settings. See section for details on DHCP settings.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main IP Address Distribution		Name Network (Home/Office)	Service S		namic IP Range 1 - 192.168.1.254	Action
Logout			Close	nnection List	Control	



User Guide

## 12.2.2 Broadband Connection (Ethernet)

The Router's Broadband Connection describes the hardware used to connect the Router to the Internet. A Broadband Ethernet connection connects the Router to the Internet using an Ethernet cable. By default Broadband Connection Ethernet is Disabled. However, you can use the Ethernet port labeled **WAN** on the back of the Router to connect your Router to the Internet. In this setup, you will install the Router so that it connects (via Ethernet) to another Internet device that provides WAN access. If you use the Router's **WAN** port, you will also need to change the Router's network connection settings.

To change the Router's network connection settings, in the **Network Connections** screen, click the **Broadband Connection (Ethernet)** link.

veriz	on					
Main	Wireless	My Network	Firewall Settings	Parental Contro	Advanced	System Monitoring
Main			Netwo	rk Connection	5	
Network Status	1.		Name		Status	Action
		ork (Home/Office)			Connected	<u>\</u> *
Network Connections		Coax			Down	
Logout		Ethernet Switch	and Daliat		1 Ports Connected Connected	
Logout		Wireless 802.11g Acce dband Connection (Eth			Disabled	
		dband Connection (Et dband Connection (Co			Connected	
		PPPoE	<u>1071</u>		Connected	
		nection			Connected	

The following screen appears. View the connection setting properties in this screen. If you change the connection name, click **Apply** to save the changes.

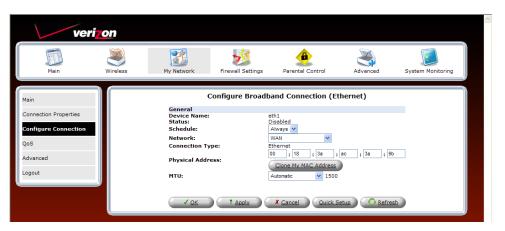
veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Connection Properties		Name:	Broadband Conne	ection (Ethernet) Pr Broadband Connection			
Configure Connection		Device Name: Status: Network: Connection Typ MAC Address: IP Address Distr		eth1 Disabled WAN Ethernet 00:18:3a:ac:3a:9b Disabled			
Advanced Logout		Packets Sent To Packets Receive Time Span:	tal:	0 0 0:00:12			
				: Apply			



User Guide

### 12.2.2.1 Configure Connection—Broadband Connection Ethernet

In the **Broadband Connection (Ethernet) Properties** screen, select **Configure Connection** in the left submenu. The following screen appears. Next, click the **Quick Setup** button.



The following screen appears. Select **Ethernet** from the **WAN Interface** drop-down list. Selecting **Ethernet** means that the WAN Ethernet port on the rear of the Router will be Enabled, ready for connection to another device through which you will connect to the Internet. Click **Apply** to save the settings.

**NOTE:** Verizon provides the protocol mode for your connection to the Internet. Depending on your connection type, a login user name and password may be required. These values are provided by Verizon.

veriz	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Quick Setup Logout		WAN Interface Internet Comm Broadband Cor Protocol Hode Continue Broadband Current Protoc Name: Bradies: Default Gateway DNS Server Login Vaser Nat Login Passwor Click Here for A	mection Device sections matching Protocol us Auto Protocol detect nd Detect Default: sol Type: me: d: dvanced Settings <u>Detect E</u>	Automatic IP (DHCP) Point-to-Point Protoct WAN PPPE Connected 10.16.90.10 10.16.16.2 10.16.16.2 username@yourisp.net 		PPoE)



User Guide

### 12.2.2.2 QoS—Broadband Connection Ethernet

NOTE: This section is only intended to be modified by a Verizon technician. Any changes to this section may result in a disruption of service.

If you select **QoS** in the left submenu of the **Broadband Connection (Ethernet) Properties** screen, the following screen appears.

ver	i <mark>zo</mark> n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties		B VLAN Settings Ingress Policy		ction (Ethernet)	Properties	
Configure Connection QoS		VLAN ID 5 Ur 7 Ur	Egress Polio ntagged (Remove VLAN ntagged (Remove VLAN	Header)		
Advanced Logout		New Entry Egress Rate Li D Enabled QoS Classifier:		<b>*</b>		
		♥ 8021p ♥ dscp port				
			<u>√ ok</u>		ancel	

You may use this section to remove VLAN tags to your incoming (Ingress) packets, or allow specific tagged packets to enter. To add a new entry, click the **New Entry** link. The following screen appears. Enter the desired port in the **VLAN ID** in the field, and then select an Egress Policy from the drop-down list. Click **OK**.

veriz	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Port to a VLAN Logout		VLAN ID: Egress Policy:	Add F	Port to a VLAN Untagged (Remove VL Tagged (Do Not Remove Untagged (Remove VL X Cancel	e VLAN Header)	



User Guide

The following screen appears. The VLAN ID displays the port that you added and the policy assigned to the port. Click **Apply** to save the settings.

ver	<mark>7</mark> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties		VLAN Settings		ction (Ethernet) Pro	operties	
Configure Connection		Ingress Policy: VLAN ID 7 Un <u>New Entry</u>	Untagged (Do Egress Polic tagged (Remove VLAN			
Advanced Logout		Egress Rate Lir Enabled QoS Classifiers				
L		♥ dscp port				
				! Apply		

For outgoing (Egress) packets you may enable a **Rate Limit** by checking the rate limit check box, and you may also enable the pass through of standard QoS classifiers. These are 802.1p, DSCP, and port tags. Note that any changes to your egress setting will likely result in a disruption of your FiOS service.

### 12.2.2.3 Advanced—Broadband Connection Ethernet

If you select **Advanced** in the left submenu of the **Broadband Connection (Ethernet) Properties** screen, the following screen appears.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties Configure Connection		Additional IP	Broadband Conner Addresses	tion (Ethernet) Pr New IP Address		-
QoS Advanced Logout						

To add a new IP address, click the New IP Address link.



User Guide

The following screen appear. Enter the desired IP Address and Subnet Mask in the fields provided. Then, click **Apply** to allow the settings to take effect.

ver	<b>70</b> n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Additional IP Address Settings Logout		IP Addre Subnet M	:55:		. 0 . 0 . 0 . 0	

The entry will be added to the list of broadband connection IP addresses.

ver	i <mark>zon</mark>					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main				ction (Ethernet) Pr	operties	
Connection Properties		Additional IP / II	Addresses P Address	Subnet Mask	Action	
Configure Connection		10.16.90.12		255.255.255.0		
QoS		10.16.90.28 New IP Addre	55	255.255.255.0		
Advanced						
Logout				! Apply		



User Guide

## **12.2.3 Broadband Connection (Coax)**

To access the Router's broadband configurations (Coax), click **My Network** in the main menu. Then click **Network Connections** in the left submenu. The following screen appears. Broadband Connection describes the hardware used to connect the Router to the Internet. This screen displays Ethernet and Coax as broadband connection options. In this setup, Coax is Connected, and Ethernet is Disabled. This means that Coax is the hardware used to connect the Router to the Internet.

veri	<mark>7</mark> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Contr	rol Advanced	System Monitoring
Main			Netwo	rk Connection	IS	
Network Status	11.0		Name		Status	Action
	<u> </u>	Vetwork (Home/Office)			Connected Down	<u> </u>
Network Connections		Coax Ethernet Switch			1 Ports Connected	
Logout		Wireless 802.11g Acc	ess Point		Connected	×*
-		roadband Connection (Et			Disabled	
		roadband Connection (Co			Connected	<u> </u>
	<u>\</u>	AN PPPoE			Connected	<b>N X</b>
	New C	Connection				-
			Quick Setup	Status	Basic <<	

To view the Router's broadband connection properties, in the preceding **Network Connections** screen, click the **Broadband Connection (Coax)** link. The following screen appears. If you change the name, click **Apply** to save the change.

ver	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties Configure Connection Logout		Name: Device Name: Status: Network: Connection Typ MAC Address: Packets Secoiv Operating Frequ	e: otal: ed:	Ecction (Coax) Prop Broadband Connection WAN-en2210 Connected WAN Multimedia over Coi 00183:sia:49:66:b7 3425 3138 1000 MHz	(Coax) ax (MOCA)	



User Guide

### 12.2.3.1 Configure Connection —Broadband Connection Coax

To configure the Router's Coax settings, click **Configure Connection** in the left submenu. The following screen appears. Enter the desired settings for your broadband connection (coax), and then click **Apply** to save the settings.

veriz	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main		C	onfigure Broad	Iband Connection (	(Coax)	
Connection Properties Configure Connection Logout		General Device Name: Status: Schedule: Network: Connection Type Physical Address MTU:	: N	VAN-en2210 Connected Always V WAN Aultimedia over Coax (MC 00 : 18 : 3a : Automatic V 1500	a4 : 96 : b7	
		MOCA Settings Vendor ID: Channel:	L	WESTELL 9 (1000 MHz) V		
		MOCA QoS: Auto Detection: MOCA Privacy: Password:		Enabled     On     Enabled     66947388374966	<b>○ off</b>	
		CM Ratio: Operating Frequ View Broadband C	ency: onnection (Coax) No connection (Coax) S	Network Coordinator 1000 MHz de Detailed Stats	Client ④ Auto	
			Apply	X Cancel Quick S	Setup	



User Guide

#### View Broadband Connection (Coax) Node Detailed Stats

If you click the View Broadband Connection (Coax) Node Detailed Stats link in the Configure Broadband Connection (Coax) screen, the following screen appears. View the information in this screen, and then click Close to return to the Configure Broadband Connection (Coax) screen.

NOTE: This screen is only intended for use by Verizon technicians. Any errors indicated do not necessarily indicate a problem with your service.

Main	Wireless My N	etwork Firewall Settings	Parental Control	Advanced	System Monitoring
n		Broadband Connect	tion (Coax) Node Detai	led Stats	
	Detailed Stats				
OCA Detailed Stat	Node Id: Link State: Network State: CM Ratio: BestCMNodeId: BackupCMNodeId: SOC Stats:		0 UP 8 SLAVE 1 0		
	TX Maps:	1633	RX Maps:		1507019
	TX Map Errors:	0	RX Map Errors:		0
			RX Map Dropped:		0
	TX Rsrv:	1507019	RX Rsrv:		1430
	TX Rsrv Errors:	0	RX Rsrv Errors:		0
			RX Rsrv Dropped:		202
	TX LC:	2519	RX LC:		4203
	TX LC Errors:	0	RX LC Errors:		0
			RX LC Dropped:		0
	TX Adm:	279	RX Adm:		111688
	TX Adm Errors:	0	RX Adm Errors:		21
			RX Adm Dropped:		1186
	TX Probes:	1258	RX Probes:		1228
	TX Probe Errors:	0	RX Probe Errors:		0
			RX Probe Dropped:		0
	TX Async:	361	RX Async:		369
	TX Async Errors:	0	RX Async Errors:		0
			RX Async Dropped:		0
	Ctl Descr Failed:	0	Upd Descr Failed:		0
	Stat Descr Failed:	0	Buf Alloc Failed:		0
	RS bytes corr:	525			
	Events: Other Info:	1620447	Interrupts:		1620440
	RF Frequency: Network Type: Node Bit Mask:		1000.0 Fully Meshed 0x03		
	TX Channel Bit Mask:	0x1			0x02
	TX IQ Imbalance (I):	22			0
	TX IQ Imbalance (Q):	-11			144
	TX IQ Imbalance (D)):	: 10	RX IQ Imbalance (D)		5



User Guide

#### Go to Broadband Connection (Coax) Stats

If you click the **Go to Broadband Connection (Coax) Stats** link in the **Configure Broadband Connection (Coax)** screen, the following screen appears. View the information in this screen, and then click **Close** to return to the **Configure Broadband Connection (Coax)** screen.

Main	Wireless	Wireless My Network			Firewall Settings Parental Control		Advanced		System Monitoring	
n				Соа	x Stats					
ax Connection Stats	Coax Settings Channel: MOCA Privacy: Password:				Automati Disabled 6694738	-				
	Coax Stats									
	Connection		outer (Node 0)	Node 1			Node 4	Node 5		Node 7
	MAC Address	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A
	IP Address	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 0 (Router)	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 1	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 2	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 3 Node 4	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A
	Node 4 Node 5	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
	Node 5 Node 6	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
	Node 5 Node 7	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
	Node /	N/A		N/A	N/A	N/A	N/A	N/A	N/A	N/A

12.2.3.2 QoS—Broadband Connection Coax

NOTE: This section is only intended to be modified by a Verizon technician. Any changes to this section may result in a disruption of service.

If you select **QoS** in the left submenu of the **Broadband Connection (Coax) Properties** screen, the following screen appears.

ver	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties		VLAN Settings		ection (Coax) Pro	perties	
Configure Connection		Ingress Policy VLAN ID	Egress Poli			
QoS		New Entry	ntagged (Remove VLAN	Header) 🗱		
Advanced Logout		Egress Rate L Enabled QoS Classifier				
	1	✓ dscp □ port				
				! Apply	ncel	



User Guide

You may use this section to remove VLAN tags to your incoming (Ingress) packets, or allow specific tagged packets to enter. To add a new entry, click the **New Entry** link. The following screen appears. Enter the desired port in the **VLAN ID** in the field, and then select an Egress Policy from the drop-down list. Click **OK**.

veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Add Port to a VLAN Logout		VLAN ID: Egress Policy:	Add I	Port to a VLAN Untagged (Remove VI Tagged (Do Not Remov Untagged (Remove VI X Cancel	ve VLAN Header)		

The following screen appears. The VLAN ID displays the port that you added. Click Apply to save the settings.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties		VLAN Setting Ingress Poli		Not Add VLAN Header)	-	
Configure Connection		VLAN ID	Egress Poli			
Configure Connection			Untagged (Remove VLAN	Header) 💢		
QoS		7	Untagged (Remove VLAN			
Advanced		New Entry				
		Egress Rate	Limit			
Logout		■ Enabled QoS Classifie ♥ 8021p	ers			
		✓ dscp				
		port				
				! Apply	Cancel	

For outgoing (Egress) packets you may enable a **Rate Limit** by checking the rate limit check box, and you may also enable the pass through of standard QoS classifiers. These are 802.1p, DSCP, and port tags. **Note that any changes to your egress setting will likely result in a disruption of your FiOS service.** 



User Guide

Verizon FiOS Router (Model 9100EM)

#### 12.2.3.3 Advanced—Broadband Connection Coax

If you select Advanced in the left submenu of the Broadband Connection (Coax) Properties screen, the following screen appears.

To add a new IP address, click the New IP Address link.

ver	i <mark>7</mark> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties		Additional IP		ection (Coax) Prop	perties	_
Configure Connection QoS				! Apply	ncel	
Advanced Logout						

The following screen appear. Enter the desired IP Address and Subnet Mask in the fields provided. Then, click **Apply** to allow the settings to take effect.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Additional IP Address Settings Logout		IP Addr Subnet	ess:		5 0 . 0 0 . 0	
<u> </u>				! Apply	ncel	

The entry will be added to the list of broadband connection IP addresses.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
ain		Additional IP		nection (Coax) Prope	erties	
Connection Properties			P Address	Subnet Mask	Action	
Configure Connection		10.16.90.40		255.255.255.0	A 🗱	
-		10.16.90.25		255.255.255.0	A 🗱	
QoS		New IP Addre	<u>:55</u>			



User Guide

## **12.2.4 WAN PPPoE**

WAN Point-to-Point Protocol over Ethernet (PPPoE) is a protocol used to connect the Router to the Internet. PPPoE enables Ethernet-networked computers to exchange information with computers on the Internet.

**NOTE:** The protocol used for your Internet connection is determined by Verizon. The Router is capable of automatically detecting the protocol used for your Internet connection.

If you are configuring your Router's protocol setting for WAN PPPoE, in the **Network Connections** screen, select the **WAN PPPoE** link.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Netwo	rk Connections		
Natural Otatua			Name		Status	Action
Network Status	4 N	etwork (Home/Office)		-	onnected	<u>\</u> #
Network Connections		Coax			own	<u> </u>
		Ethernet Switch		1	Ports Connected	<u> </u>
Logout		Wireless 802.11g Acc	ess Point	C	onnected	N 🗱 🕹
	💧 💧 в	roadband Connection (Eth	hernet)	Di	sabled	<u>\</u>
	💧 💧 В	roadband Connection (Co	bax)	C	onnected	1
	N 🖉	AN PPPOE		0	onnected	N 🗱 🕹
	New C	Connection				-

The following screen will appear. View the details in this screen. If you change the name, click **Apply** to save the changes. Select the menu option in the left submenu to access the desired configuration page:

- Select Configure Connection to access the WAN PPPoE Properties screen.
- Select **Routing** to configure the Routing properties for your WAN PPPoE. Refer to section 15.21 for details on Routing.
- Select **PPP** to configure the Router's PPP settings.

verizo	n				
Main Wi	ireless My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Connection Properties Configure Connection Routing PPP Logout	Name: Device Name: Status: Network: Unormeticion Pafault Gafer DHS Server: Service Name: Packets Recor Packets Recor Time Span:	vice: pe: ay: : total:	PPOE Properties           WAN PPPE           pop0           ponnected           WAN           BEPDE           10.6.90.10           10.16.90.11           10.16.60.1           10.16.60.1           10.16.60.2           username@yourisp.00           0           0           0:01:48	unet Disable	



User Guide

### **Configure Connection—WAN PPPoE**

To configure the WAN PPPoE properties, click **Configure Connection** in the left submenu of the **WAN PPPoE Properties** screen. The following screen appears. Enter the desired settings and click **Apply** to save the settings.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Configu	ure WAN PPPoE		
Connection Properties Configure Connection		General Device Name: Status: Schedule:		ppp0 Connected Always		
Routing		Network: Connection Typ MTU:	e:	WAN PPPoE Automatic V 1492	~	
PPP		Internet Protoc		Obtain an IP Address		
Logout		_	net Mask:		0.0	_
Logout		Override Subr DNS Server		0.0.	0 . 0 dress Automatically V	<u>ah</u>

### PPP-WAN PPPoE

NOTE: The settings in the screen are provided by Verizon. Do not change the settings unless instructed by Verizon.

To configure the Router's PPP properties, click **PPP** in the left submenu screen. The following screen appears. If you change the settings in this screen, click **Apply** to save the settings.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			WAN P	PPoE Properties		
Connection Properties		PPP PPP Authentic			. ]	
Configure Connection		Login User Na Login Passwo		username@yourisp.ne	rt -	
Routing		-	encrypted Password (PA			
РРР			allenge Handshake Auth			
			rosoft CHAP (MS-CHAP) rosoft CHAP Version 2 (			
Logout		PPP Compress		(10 CITAP V2)		
	~	BSD:		Allow 💙		
		Deflate:		Allow 💙		
			✓ OK	! Apply	ncel	



User Guide

### 12.2.5 Status

To view the status of the Router's connections, in the **Network Connections** screen, click the **Status** button. The following screen will appear. This screen displays connection information for devices connected to your Router. At this screen, do any the following:

- Turn off Automatic Refresh by clicking the Automatic Refresh Off button. When Automatic Refresh is enabled, the screen will be updated automatically to display the most current statistics.
- Manually refresh this screen by clicking the **Refresh** button.
- Click the links in this screen to access the Router's connection settings.
- Click Close to return to the Network Connections screen.

lame	<u>Network</u> (Home/Office)	Ethernet Switch	Broadband Connection (Ethernet)	<u>Coax</u>	Broadband Connection (Coax)	Wireless 802.11g Access Point	WAN PPPoE
Device Name	br0	eth0	eth1	LAN-en2210	WAN-en2210	ath0	рррО
Status	Connected	1 Ports Connected	Disabled	Down	Connected	Connected	Connected
	Network	Network	WAN	Network		Network	WAN
Underlying Device	(Home/Office) Ethernet Switch Coax Wireless 802.11q Access Point	(Home/Office)		(Home/Office)		(Home/Office)	Broadband Connection (Coax)
	Bridge	Hardware Ethernet Switch	Ethernet	Multimedia over Coax (MOCA)	Multimedia over Coax (MOCA)	Wireless 802.11g Access Point	PPPoE
Download Rate						54 MB	
Jpload Rate						54 MB	
14.0	00:18:3a:ac:3a:9a	00:18:3a:ac:3a:9a	00:18:3a:ac:3a:9b		00:18:3a:ac:3a:9b	00:1d:19:59:d7:2f	
	192.168.1.1						10.16.90.10
Subnet	255.255.255.0						
nask Default							10.16.90.1
Sateway							
DNS Server							10.16.16.8 10.16.16.2
	DHCP Server	Disabled	Disabled			Disabled	
Service Name							
Jser Name							erizonfios
Incryption						WEP	
Sent Lotal	4869	3018	0	0	385	1871	0
Bytes Sent Fotal	1531545	1238411	0	0	56699	710948	0
Packets Sent Broadcast Packets	515	550	U	U	41	547	214/449160
Sent Total Errors	0	0	0	0	0	0	0
Dropped	0	0	0	0	0	0	0
Received	1464	1278	0	0	719	435	0
HW Accelerated	0	350	0	0	347	0	0
Total	519738	164135	0	0	44817	47873	0
Unicast	1332	1189	0	0	668	435	4033608972
Multicast	16	8	0	0	0	0	262027148
Broadcast	116	81	0	0	51	0	4294298472
Total Errors	0	0	0	0	0	0	0
Packets Received Total Dropped	0	0	0	0	0	0	0
Time Span	0:18:45	0:18:45	0:13:17			0:18:39	0:13:12
Operating Frequency					1000 MHz		



User Guide

# **13. FIREWALL SETTINGS**

The **Firewall Settings** section provide access to all your router security functions. Click **Firewall Settings** in the top navigation menu to enter the settings menu.

CAUTION: Only Advanced Users should access the firewall settings.



### 13.1 General Firewall Security Settings

This section explains how to configure your Router's firewall security features. The Router's firewall security settings allow you to reduce the risk of unauthorized access to your network by prohibiting certain types of inbound and outbound network traffic and by allowing you to configure specific firewall rules.

**IMPORTANT:** If you need help, click **Main** in the top navigation menu to go to the home page. In the **Quick Links** section of the home page, click **Verizon Help**. Clicking this link takes you to Verizon's Online Help site, where you can access additional information about your Router.

To change your firewall security level, click the option button next to the desired security setting. Next, click **Apply** to allow the changes to take effect.





User Guide

	General Firewall Settings
Maximum Security	High security level only allows basic Internet functionality. Only Mail, News, Web,
(High)	FTP, VoIP/SIP and IPSEC traffic is allowed. All other traffic is prohibited.
Typical Security	Like High security, Medium security only allows basic Internet functionality by
(Medium)	default. However, Medium security allows customization of Network Address
	Translation (NAT) so you can enable certain types of traffic. This is the factory
	default security level.
Minimum Security	Low security setting will allow all traffic except for known malicious attacks. With
(Low)	Low security, your Router is visible to other computers on the Internet.
Block IP Fragments	This option can prevent hackers from using fragmented data packets to possibly sabotage your network. Note: Some VPN and UDP services use IP fragments, and this feature may need to be disabled. If you have questions about this feature, check
	with Verizon technical support. It is disabled by default.

### 13.2 Access Control

If you select **Firewall Settings** in the top navigation menu and then select **Access Control** in the left submenu, the following screen will appear.

Access Control is used to block specific computers within the local network (or even the whole network) from accessing certain services on the Internet. For example, one computer can be prohibited from surfing the Internet, another computer from transferring files using FTP, and the whole network from receiving incoming E-mail. Access control defines restrictions on the types of requests that can pass from the local network out to the Internet, and thus may block traffic flowing in both directions.

To add an Access Control rule, click the New Entry link or, alternatively, click the plus icon.

veri	on					
Main	Wireless M	y Network Fi	irewall Settings	Parental Control	Advanced	System Monitoring
Main General		Blo		ess Control et services from within	the LAN.	
Access Control Port Forwarding DMZ Host	Local Hos MAC <u>New Entry</u>	iMAC		Protocols CP Any -> 21	Status Inactive	Action
Port Triggering Remote Administration			! Apply	X Cancel Resolv	ve Now	h
Static NAT Advanced Filtering						
Security Log Connections						
Logout						

Adding a new entry will allow you to choose a device from the known network devices (Ex. Your computers) or enter a MAC address of a new device. Then you must choose the Protocol (or service) to be blocked.



User Guide

### **13.2.1 Selecting an Address**

From the Address drop-down list, select the desired computer to which you want this rule applied.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Access Control Rule			Add Acc	ess Control Rule		
		Address		Any 💙		
Logout		Protocols		Any User Defined		
·	<b>*</b>	Reply an HTML Page to t	ne Blocked Client	iMAC		
		Schedule		Always 💙		
				X Cancel		

If your computer or device is not listed in the drop-down, you may create a new Network Object manually by choosing the **User Defined** option. Please see the Network Object section for more details on setting up a network object (Section 15.11).

After you have selected a computer, the following screen will appear. Next, proceed to section 13.2.2 to select a protocol.

verizo	n						
Main W	Vireless	My Network	Firewall Settings	Parental Control	Advanced	System Monito	oring
Main			Add Acce	ess Control Rule			
Add Access Control Rule		Address					
Logout		Name DHCP	SALLE-XP3	Address		Action	
		Add 💌					
		Protocols		Any	~		
		Reply an HTML Page to t	he Blocked Client				
		Schedule		Always 💌			
			<u> √ ok</u>	X Cancel			



User Guide

## **13.2.2 Selecting an Protocol**

From the **Protocols** drop-down list, select the desired option that you want to prohibit the computer from using. To notify the user of this blockage via an HTML (Web) page, click the check box (a check mark will appear in the box). Note: This feature only works for HTTP services.

To see more than the basic listed services choose **Show All Services** from the **Protocols** drop-down. This will show you many pre-defined services such as games and IM clients.

Add Acce	ess Control Rule
Address	Any 🗸
Protocols	Any 🗸
Reply an HTML Page to the Blocked Client	Any User Defined
Schedule	Show All Services
<u>√ ok</u>	HTTP HTTPS IMAP L2TP Ping
	POP3 SMTP SNMP
	Teinet
	Traceroute

After you have selected the protocol, the following screen will appear. Proceed to section 15.19 to configure a schedule rule.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Access Control Rule			Add Acc	ess Control Rule		
		Address		Address		Action
Logout		Name DHCP	IMAC	Address		Action
		Add	in AC			
		Protocols				
		Name		Ports		Action
		FTP - File Transfer	TCPAny -> 21			*
		Add	~			
		Reply an HTML Page to t	he Blocked Client	Always		
				X Cancel		



User Guide

# 13.2.3 Configuring a Schedule Rule

After you have selected the protocol, the following screen will appear. If desired, select a schedule from the **Schedule** drop-down menu. If you select **User Defined**, refer to the procedure explained in section 15.19, "Scheduler Rules," to set up a schedule rule. Otherwise, select **Always**, and then click **OK** to continue.

- Select **Always** to allow the rule to be active all the time.
- Select User Defined to allow the rule to be active only at certain time, as defined by the rules you set up.

veriz	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Access Control Rule			Add Acc	ess Control Rule		
Logout		Address Name DHCP	SALLE-XP3	Address		Action
		Add V				
		Name FTP - File Transfer Add	TCP4 -> 21	Ports		Action 💥
		✓ Reply an HTML Page to t				
		Schedule		Always  Always User Defined		
			✓ OK	X Cancel		

If you clicked **OK** in the preceding screen, the following screen will appear. Click **OK** to save the settings.

veriz	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Add Access Control Rule			Add Acc	ess Control Rule			
	Ado	Iress					
Logout	DHO	Name	SALLE-XP3	Address		Action	
	Add		SALLE-XPS				
		tocols					- 1
	Pro	Name		Ports		Action	
	FTP	- File Transfer	TCP4 -> 21			*	
	Add	i	~				
	Sch	Reply an HTML Page to t edule Name eduler Rule		Settings 10-05:00 on the next day		Action	
			<u> √ ok</u>	Cancel			



User Guide

## **13.2.4** Completing the Access Control Rule Configuration

If you clicked **OK**, the following screen will appear. The rule has been added to the list of security rules. To disable the security rule for an entry, click the adjacent check box, and then click **Apply**. To add additional access control rules, click the **New Entry** link.

veriz	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main General				ccess Control	ne LAN.	
Access Control	Lo	cal Host	Local Address	Protocols	Status	Action
Port Forwarding	SALLE		ALLE-XP3	FTP - TCP 4 -> 21	Inactive	A 🗱
MZ Host	New Ent	ry .				4
ort Triggering emote Administration		<u>√ 0</u> K	Apply	X Cancel Resolve	Now O Refres	h
Static NAT						
dvanced Filtering						
Security Log						
Connections						
Logout						



User Guide

### **13.3 Port Forwarding**

If you select **Firewall Settings** in the top navigation menu and then select **Port Forwarding** in the left submenu, the following screen will appear.

By default the Router blocks all external users from connecting to your network. However, you can configure specific applications on your network to be accessible from the Internet. Port Forwarding allows the Router to enable applications (Games, Webcams, IM & Others) by opening a tunnel between remote (Internet) computers and a specific device port inside your local area network (LAN). Services on the LAN will be exposed to external Internet users.

Main	Wireless	My Network	Firewall Set	tings Parenta	B I Control	Advanced	System Monitoring
Main General			Expose servi	Port Forward	-	ers.	
Access Control	Local Ho	stLocal Address	Network Address	Public IP Address	Protocols	Status	Action
Port Forwarding	✓ localho New Ent		Any	Any	TCP Any -> 4567	Active	4
DMZ Host	New Line	<u>I Y</u>					T
Port Triggering							
Remote Administration		<ul> <li>✓ <u>ок</u></li> </ul>	Apply	Cancel	Resolve Now	Refres	<u>h</u>
Static NAT							
Advanced Filtering							
Security Log							
Connections							
Logout							
	ļ						



User Guide

## 13.3.1 Setting Up a Predefined Port Forwarding Rule

To set up a predefined port forwarding rule, at the Security screen, click the New Entry link.

Main	Wireless	My Network	Firewall Set	ttings Parent	al Control	Advanced	System Monitoring
Main General			Expose servi	Port Forwar	r <b>ding</b> xternal Internet use	rs.	
Access Control		ost Local Address	Network Address	Public IP Address	Protocols	Status	Action
Port Forwarding	New Ent		iny	Any	TCP Any -> 4567	Active	4
Port Triggering							
Remote Administration		<u> √ ок</u>	Apply	Cancel	Resolve Now	Refres	<u>h</u>
Static NAT							
Advanced Filtering							
Security Log							
Connections							
Logout							

If you clicked **New Entry**, the following screen will appear. In the **Local Host** field, enter a local host name or IP address of the computer providing the service. If you will use a public IP address, click the check box next to **Specify Public IP Address**.

**NOTE:** Only one computer can be assigned to provide a specific service or application. If you use public IP addresses in your Router's configuration, you must first obtain them from Verizon.

Specify Public IP Address	
Local Host:	
Specify Network IP Address	
Protocols	Any 🗸
Forward to Port:	Same as Incoming Port 💌
Schedule	Always 🗸



User Guide

Next, select a predefined service from the **Protocol** drop-down list.

**NOTE:** For your convenience, the Router provides predefined protocols for applications, games, and VPN-specific programs.

The screen below displays the protocols of basic services provided in the Router. If you select **Show All Services** from the **Protocol** drop-down list, all available services will be displayed in the drop-down list.

Main Wireless Wy Network Firewall Settings Parental Control Advanced System Monitoring
Main         Add Port Forwarding Rule         Logout         Descript Public IP Address         Local Host:         Specify Network IP Address         Protocols         Any         Schedule         Siteward to Port:         User Defined         Schedule         Siteward to Port:         User Defined         Schedule         Siteward to Port:         User Defined         Siteward to

Select a predefined service from the protocol drop-down list.



User Guide

After you have selected a predefined service, the following screen will appear. Next select an option from the **Forward to Port** drop-down list to indicate the port to which traffic will be forwarded.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitorin	ng
Main			Add Port I	Forwarding Rule			
Add Port Forwarding Rule		Specify Public IP Address Local Host: Specify Network IP Addres	s				
		Protocols Name		Ports		Action	
		Alien vs. Predator	TCPAny -> 2300-4 Any -> 7000-1 UDPAny -> 2300-4 Any -> 7000-1 Any -> 80	000 0000 000		X	
		Add	~				
		Forward to Port:		Same as Incoming Por	t 🛩		
		Schedule		Same as Incoming Port Specify			
			<u>√ ok</u>	X Cancel			

If you selected **Same as Incoming Port** from the **Forward to Port** drop-down list, the following screen will appear. Click **OK** to continue.

	Add Port Forv	warding Rule	
Specify Public IP Address			
Local Host:			
Specify Network IP Address			
Protocols			
Name		Ports	Action
Alien vs. Predator	TCPAny -> 2300-4000 Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80		*
Add	/		
Forward to Port:		Same as Incoming Port ⊻	
Schedule		Always 🗸	
		X Cancel	



User Guide

Next, set up a schedule rule using the instructions explained in section 15.19 "Configuring a Schedule." After you have set up a schedule, enter the address of the local Host, and then click **OK** to save the settings.

Specify Public IP Address		
Local Host:		
Specify Network IP Addres	s	
Protocols		
Name	Ports TCPAny -> 2300-4000	Action
Alien vs. Predator	Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80	*
Add	★	
Forward to Port:	Same as Incoming Port 💌	
Schedule		
Name	Settings	Action
Scheduler Rule	Fri between 08:05-02:10 on the next day	🔨 🎉

If you clicked **OK** the following screen will appear. The predefined port forwarding rule has been assigned.

			Port F	orwarding		
Expose services on the LAN to external Internet users.						
Local Host	Local Address	Network Address	Public IP Address	Protocols	Status	Action
✓ localhost	127.0.0.1	Any	Any	TCP Any -> 4567	Active	
✓ 192.168.1.2	192.168.1.2	Any	Any	Alien vs. Predator - TCP Any -> 2300-4000 TCP Any -> 7000- 10000 UDP Any -> 2300- 4000 UDP Any -> 7000- 10000 UDP Any -> 80	Inactive	<b>\ #</b>
New Entry						-
	<u>√ ok</u>			Cancel Resolve Nor		



User Guide

## **13.3.2 Setting Up a User Defined Port Forwarding Rule**

To set up a user-defined port forwarding rule, in the Security screen, click the New Entry link.

			Port Forwar	ding		
		Expose servic	es on the LAN to e	ternal Internet use	ers.	
Local Host	Local Address	, Network Address	Public IP Address	Protocols	Status	Action
✓ localhost	127.0.0.1	Address	Address	TCP Any -> 4567	Active	
New Entry	,					4

- Specify the local computer that the port forwarding rule will apply to. This is done in the Local Host field. The field will accept either your computer name (the NetBios name; for example DADS-PC) or the computer IP address. These values can be found on your **My Network page**.
- If you are setting up a NAT/NAPT rule you must also specify the public IP address that data will be coming in on. Check the **Specify Public IP Address** check-box and enter a specific external IP address such as the WAN IP address of the router or a Static NAT IP address.
- Optionally you can specify a remote network (to forward packets to (this is a network that it outside the control of your Router). This is common in a small business or advanced configuration that uses multiple routers. Select the **Specify Network IP Address** check-box if you would like to apply this rule to send packets to a host IP address outside the local network (such as a remote gaming server). The screen will refresh and present you with a field in which to insert this IP address.

**NOTE:** Only one computer can be assigned to provide a specific service or application. If you use public IP addresses in your Router's configuration, you must first obtain them from Verizon.

Specify Public IP Address
Specify Network IP Address
Protocols Any
Forward to Port: Same as Incoming Port 💌
Schedule Always 🔽



User Guide

Next you must choose the protocol that you want to forward. A large list is provided of many common applications. If you need to define your own select **User Defined.** 

Main Wireless My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Add Port Forwarding Rule Logout  Protocols Forward to Port: Schedule		Any Any User Defined Show Basic Services Alien vs. Predator CuSeeMe Dark Reign Dark Reign Dark Reign Deta Forces Deta Forces Deta Forces Deta Force Deta Force Deta StarCraft(Battle Direck Sames DNS ALG Diablo, StarCraft(Battle Direck Sames DNS ALG FIP HITP Vice Access HITPS HITP Secondary HITP Vice Access HITPS HITP Secondary HITP Vice Access HITPS HIT			

If you selected **User Defined**, the following screen will appear. Give your service a name using the text box and then define the ports that define your newly created service.

NOTE: At least one server	port entry must be defined before you	u can enter a service name.

Edit Service	
Application	
Server Ports	Action
	Application



User Guide

Clicking the New Server Ports link, will bring up the following screen that allows you to define your ports.

	Edit Service Server Ports
Protocols	Other 💌
Protocol Number:	0
	✓ <u>OK</u> Cancel

Next, select the desired protocol from the **Protocol** drop-down list. This information should be provided by your application developer or documentation.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Edit Service Server Ports Logout		Protocols Protocol Numt		Other V UDP ICAP GRE ESP AH Other ncel		



User Guide

For example, if you selected **TCP**, from the drop-down list, the following screen will appear. Select the desired source and destination port settings from the drop-down lists.

	Edit Service Server Ports	
Protocols	TCP 💌	
Source Ports	Any 💌	
Destination	orts: Any 💌	

To set up a range of ports, select "Range" from the Source Ports and Destination Ports drop-down lists.

Next, enter the desired port range values in the fields provided, and then click **OK** to continue.

	Edit Service Server Ports
Protocols	TCP 💌
Source Ports:	Range 💙 2 - 4
Destination Ports:	Range 💙 6 - 8
	✓ <u>OK</u> X <u>Cancel</u>



User Guide

If clicked **OK** in the preceding screen, the following screen will appear. Click **OK** to save the settings.

Service Name:	Application	
Server Ports		
Protocols	Server Ports	Action
TCP	2-4 -> 6-8	🔨 🗶
New Server Ports		-

Now you must specify a local host for which you to assign this user-defined port forwarding rule. To assign the rule to a public IP address, click the **Specify Public IP Address** check box.

<b>NOTE:</b> Only one computer can be assigned to provide a specific service or application.	If you use public IP
addresses in your Router's configuration, you must first obtain them from Verizon.	

At the Add Port Forwarding Rule screen you can enter the name of a local host or click the Specify Public IP Address check box to indicate the host or IP Address to which the port forwarding rule will be assigned.

	Add Port For	warding Rule	
Specify Public IP Address			
Local Host:			
Specify Network IP Address			
Protocols			
Name		Ports	Action
Application	TCP2-4 -> 6-8		🔨 🎇
Add	<b>~</b>		
Forward to Port:		Same as Incoming Port 💌	
Schedule		Always 🗸	
		Cancel	



User Guide

To assign the port forward rule to a NAT policy (or external IP address) click the **Specify Public IP Address** check box and enter the appropriate IP address.

Specify Public IP Address Public IP Address: Local Host: Specify Network IP Address		0.0.0.0	
Protocols			
Name Application	TCP2-4 -> 6-8	Ports	Action
	~		
Forward to Port:		Same as Incoming Port 💌	
Schedule		Always 💙	
	<b>√</b> <u>ok</u>	X Cancel	

From the **Forward to Port** drop-down list, select the desired option to indicate the port to which traffic will be forwarded. This is almost always the same as the incoming port. You may define a custom port map by specifying a new port to send this traffic to. (For example you could forward all the incoming traffic to an external IP address coming in on Port 80 to your internal computer but Port 81)

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Add Port Forwarding Rule		Specify Public IP Address		Forwarding Rule		
Logout		Local Host: Specify Network IP Addre Protocols				
		Name Application Add Forward to Port:	TCP2-4 -> 6-8	Ports Same as Incoming Pol	t 🗸	Action
		Schedule		Same as Incoming Por Specify		
			<u> </u>	X <u>Cancel</u>		



User Guide

After you have entered a local host, specified a port, and clicked **OK** in the preceding screen, the following screen will appear. The user-defined rule has been added to the port forwarding table, and the status is **Active**. You may need to click **Resolve Now** while the Router is attempting to save the rule to the local host.

		Expose serv	Port For	to external Internet use	ers.	
Local Host	Local Address	Network Address	Public IP Address	Protocols	Status	Action
✓ localhost	127.0.0.1	Any	Any	TCP Any -> 4567	Active	
✓ 192.168.1.2	2192.168.1.2	Any	Any	Application - TCP 2-4 -> 6-8	Active	🔨 🗶
New Entry						

If you want to disable a port forwarding rule, clear the check box next to the host name or IP address. Then click **Apply** to save the setting.

		Expose serv	Port Forv	<b>varding</b> to external Internet use	ers.	
Local Host	Local Address	Network Address	Public IP Address	Protocols	Status	Action
✓ localhost	127.0.0.1	Any	Any	TCP Any -> 4567	Active	
192.168.1.2	2192.168.1.2	Any	Any	Application - TCP 2-4 -> 6-8	Disabled	1
New Entry						4



User Guide

# 13.3.3 Configuring a Schedule Rule

If desired, select a schedule from the **Schedule** drop-down menu. If you select **User Defined**, refer to the procedure explained in section 15.19, "Scheduler Rules," to set up a schedule rule. Otherwise, select **Always**, and then click **OK** to continue.

- Select **Always** to allow the rule to be active all the time.
- Select User Defined to allow the rule to be active only at certain time, as defined by the rules you set up.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Add Port	Forwarding Rule		
Add Port Forwarding Rule		Specify Public IP Address				
Logout		Local Host:				
		Specify Network IP Addre	ISS			
		Protocols Forward to Port:		Any Same as Incoming Port	Y	
		Schedule		Always V		
				Always User Defined		
			<ul> <li>✓ <u>ok</u></li> </ul>	X Cancel		



User Guide

After you have added port forwarding rules and clicked OK, in the **Port Forwarding** screen, the following screen will appear. Enter the domain name in the **Local Host** field or click the check box to specify a public IP address or to specify a network IP address. Then, click **OK** to continue.

Specify Public IP Address		
Local Host:	192.168.1.2	]
Specify Network IP Addre	SS	-
Protocols	Dente	
Name Application	Ports TCP2-4 -> 6-8	Action
Add	▼	
Forward to Port:	Same as Incoming Port 💙	
Schedule		
Name Scheduler Rule	Settings Fri between 08:05-02:10 on the next day	Action

If you clicked **OK**, the following screen will appear. Click **Apply** to save the settings.

Port Forwarding								
Expose services on the LAN to external Internet users.								
Local Host	Local Address	Network Address	Public IP Address	Protocols	Status	Action		
✓ localhost	127.0.0.1	Any	Any	TCP Any -> 4567	Active			
✓ 192.168.1.2	.2 192.168.1.2 Any Any Application - TCP 2-4 Disabled							
New Entry								



User Guide

### 13.4 DMZ Host

If you select Firewall Settings in the top navigation menu and then select DMZ Host in the left submenu, the following screen will appear. The DMZ (Demilitarized) Host feature allows the user to forward unsolicited inbound WAN traffic to any single IP on the LAN. One computer on your LAN will be fully exposed to the Internet. The designated computer will be connected to your network without regard to firewall security or restrictions. Use this feature in cases where you want to use Internet services that are not available in the Port Forwarding list, such as Web games or video-conferencing.

WARNING: The computer that is configured as a DMZ Host will not have security or firewall protection.

To configure a computer for DMZ Host, click the **DMZ Host IP Address** check box, and then enter the IP Address of the computer that you want to be accessible from the Internet. The computer will answer to the default WAN IP address of the Router. Click **Apply** to save the settings.

To disable DMZ Host (if previously enabled), click to clear the check box. Then click Apply to save the settings.

veri	on							
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring		
Main General		AI	[ llow a single LAN comput	MZ Host er to be fully exposed to	the Internet.			
Access Control Port Forwarding		DMZ Host IP Address: 192 . 168 . 1 . 0						
DMZ Host Port Triggering				! <u>Apply</u> <u>X</u> Car	ncel			
Remote Administration Static NAT								
Advanced Filtering								
Security Log Connections								
Logout								



User Guide

# 13.5 Port Triggering

If you select **Firewall Settings** in the top navigation menu and then select **Port Triggering** in the left submenu, the following screen will appear. You can define port triggering rules to dynamically open the firewall for specific protocols or ports. The specified ports will be opened for incoming traffic. Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering because the outbound traffic triggers the ports to which inbound traffic is directed.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Co	ontrol Advanced	System Monitoring
Main General				ort Triggering		
Access Control		Protocols		Frigger Ports	Incoming Ports to Open	Action
Port Forwarding DMZ Host		L2TP - Layer Two Tunneling TFTP - Trivial File Transfer			Any -> Same as Initiating Po Any -> Same as Initiating Po	
Port Triggering Remote Administration						
Static NAT				Apply	X Cancel	
Advanced Filtering Security Log						
Connections						
Logout	J					



User Guide

# 13.5.1 Setting Up a User Defined Port Triggering Rule

To set up a user-defined port triggering rule, in the Add drop-down list, select User Defined.

veri	<b>7</b> 0n						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main General				t <b>Triggering</b> of ports for incoming dat	a.		
Access Control Port Forwarding			Outgoing Trig	01 UDP Any -> S	<b>g Ports to Open</b> ame as Initiating Ports	••	
DMZ Host Port Triggering Remote Administration	Add Add User Def	~	Protocol UDP 1024-6553	15 -> 69 UDP Any -> S	ame as Initiating Ports	*	
Static NAT Advanced Filtering	CuSeeMe Delta For ICQ Rainbow Tiberian	ce Six		T Apply			
Security Log	Titerian	San					
Connections Logout							

### 13.5.1.1 Configuring Outgoing Trigger Ports

If you selected **User Defined** in the preceding screen, the following screen will appear. Enter the desired name in the **Service Name** field. Next, click the **New Trigger Ports** link to configure outgoing trigger ports.

Image: Name	veri	on					
Edit Port Triggering Rule     Service Name:     Application       Logout     Outgoing Trigger Ports     Action       New Trigger Ports     Image: Control of the server Ports     Action       New Trigger Ports     Image: Control of the server Ports     Image: Control of the server Ports       New Opened Ports     Opened Ports     Action	Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Cutgoing Trigger Ports       Action         New Trigger Ports       Image: Comparison of the point	Main			Edit Port	t Triggering Rule		
Protocols Server Ports Action New Triager Ports Incoming Ports to Open Protocols Opened Ports Action New Opened Ports	Edit Port Triggering Rule	Service	e Name:	Application			
New Trigger Ports     Image: Ports of the po	Logout	Outgoir					
Protocols Opened Ports Action New Opened Ports		New Tr			Server Ports		
Protocols Opened Ports Action New Opened Ports		Incomi	ng Ports to Open				
			Protocols		Opened Ports		
				<ul> <li>✓ <u>ok</u></li> </ul>	X Cancel		



User Guide

If you clicked **New Trigger Ports**, the following screen will appear. Select the desired protocol from the **Protocol** drop-down list.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Edit Serv	vice Server Ports		
Edit Service Server Ports		Protocols		Other 💌		
Logout		Protocol Num	ber:	0		
				X Cancel		

For example, if you selected **TCP** from the **Protocol** drop-down list, the following screen will appear. Select the desired source and destination settings from the drop-down lists.

veri	on					_	~
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Edit Service Server Ports			Edit Ser	vice Server Ports			
Logout		Protocols Source Ports: Destination Po		TCP V Any V Any V			
			<u> √ ok</u>				
							~



User Guide

For example, if you selected **Single**, the following screen will appear. Enter the desired source port and destination port values, and then click **OK** to save the settings.

veri	on						1
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main			Edit Serv	vice Server Ports			
Edit Service Server Ports Logout		Protocols Source Ports:		TCP V Single V	]		
	1	Destination Por	ts:	Single 💙 0			
			<u> </u>	Cancel			

If you entered source and destination port values clicked **OK** in the preceding screen, the following screen will appear. If you desire to configure incoming trigger port, proceed to section 13.5.1.2. Otherwise, click **OK** to continue.

veri	<b>7</b> 0n									
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring				
Main		Edit Port Triggering Rule								
Edit Port Triggering Rule	Service	Service Name: Application								
Logout	Outgoi	ng Trigger Ports				Action				
	ТСР	Protocols	20 -> 23	20 -> 23						
	New Tr	igger Ports								
	Incomi	ng Ports to Open								
	New O	Protocols Dened Ports		Opened Ports		Action				
				X Cancel						



User Guide

If you clicked **OK**, the following screen will appear. Click **Apply** to save the settings. If you want to edit a rule, click the pencil icon next to the rule that you want to edit. To delete a rule, click the "X" icon next to the rule that you want to delete.

ver	<b>7</b> 0N						
Main	Wireless	My Network	Firewall Settings	Parental	Control Adva	anced System Mo	onitoring
Main General			Port Ti Trigger opening of p		-		
Access Control		Protocols	Outgoing Trigger		Incoming Ports to		
Port Forwarding DMZ Host		- Trivial File Transfer F	Protocol UDP 1024-65535 -: TCP 20 -> 23		IDP Any -> Same as In IDP Any -> Same as In	-	
Port Triggering Remote Administration	Add	*					
Static NAT			√ок !	Apply	X Cancel		
Advanced Filtering Security Log							
Connections							
Logout							

### 13.5.1.2 Configuring Incoming Trigger Ports

To configure incoming trigger ports, in the Edit Port Triggering Rule screen, click the New Opened Ports link.

veriz	on				
Main	Wireless My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main		Edit Port	t Triggering Rule		
Edit Port Triggering Rule	Service Name:	Application			
Logout	Outgoing Trigger Ports Protocols		Server Ports		Action
L	TCP	20 -> 23	barrentores		\ <b>X</b>
	New Trigger Ports				4
	Incoming Ports to Open				
	Protocols		Opened Ports		Action
	New Opened Ports				
		<u> </u>	Cancel		



User Guide

If you clicked **New Opened Ports**, the following screen will appear. Select a protocol from the **Protocol** drop-down list.

veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Edit Service Opened Ports			Edit Serv	vice Opened Ports			
Logout		Protocols Protocol Numb	er:	Other  TCP UDP ICMP			
				GRE ESP AH Other ncel			

For example, if you select **UDP**, the following screen will appear. Select the desired source port and destination port settings from the drop-down lists.

veri	on						-
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main			Edit Serv	vice Opened Ports			
Edit Service Opened Ports Logout		Protocols Source Ports:		UDP 💙 Any 🗸			
(		Destination Po	orts:	Any	*		
			<ul> <li>✓ <u>ok</u></li> </ul>	X Cancel			
							5



User Guide

Next, enter the desired source and destination port values in the fields provided, and click **OK** to continue.

veri	on						
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main Edit Service Opened Ports		Protocols	Edit Serv			_	
Logout		Source Ports Destination P		Single 27 Single	▶ 28		
				X Cancel			

If you clicked **OK**, the following screen will appear. Click **OK** to continue.

	on	<b>*</b>	<b>4</b> 3	<u>^</u>		
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
			Edit Dor	Triggering Rule		
Main			Eult Poli	The second se		
Edit Port Triggering Rule	Servic	e Name:	Application			
Logout	Outgoi	ng Trigger Ports Protocols		Server Ports		Action
	ТСР		20 -> 23			1.2
	New T	rigger Ports				4
	Incom	ing Ports to Open				
		Protocols		Opened Ports		Action
	UDP		27 -> 28			S 🗱 🖉
	New O	pened Ports				<b>+</b>
				X Cancel		



#### User Guide

If you clicked **OK**, the following screen will appear. This screen shows that the triggering rule has been added to the list of triggering services. Click **Apply** to save the settings. If you want to edit a rule, click the pencil icon next to the rule that you want to edit. To delete a rule, click the "X" icon next to the rule that you want to delete.

veri	<b>7</b> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main General				Triggering	data.	
Access Control		Protocols	Outgoing Trig		ming Ports to Open	Action
Port Forwarding		P - Layer Two Tunneling			> Same as Initiating Ports	
DMZ Host		P - Trivial File Transfer Pi			Same as Initiating Ports	
Port Triggering	Add	lication	TCP 20 -> 23	UDP 27 ->	× 28	2 🗱
	Add	•				
Remote Administration						
Static NAT			<b>Г</b> ок		Cancel	
Advanced Filtering						
Security Log						
Connections						



User Guide

# **13.5.2 Setting Up a Predefined Port Triggering Rule**

To set up a predefined port triggering rule, in the Add drop-down list, select a predefined service.

ver	on							
Main	Wireless	My Network	Firewall Settings	Parental	Control	Advanced	System Monitoring	
Main General			<b>Po</b> Trigger openin	<b>rt Triggeri</b> g of ports for i	-			
Access Control		Protocols	Outgoing Tr	igger Ports	Incoming	Ports to Open	Action	
Port Forwarding	V L	2TP - Layer Two Tunneling	Protocol UDP Any -> 1	.701 U	IDP Any -> Sa	me as Initiating Ports		
DMZ Host	_	FTP - Trivial File Transfer P				me as Initiating Ports		
		Application	TCP 20 -> 23	U	DP 27 -> 28		<b>N</b>	
Port Triggering	Add							
Remote Administration	User	Defined						
Static NAT	CuSe							
Advanced Filtering	Delta	Force		Papply	Cance	el		
-	Rain	bow Six ian Sun						=
Security Log	Tiber							
Connections								
Logout								

After you have selected a service, the following screen will appear. The service that you selected will be displayed. Click **Apply** to save the settings.

veri	on							
Main	Wireless	My Network	Firev	wall Settings	Parental	Control	Advanced	System Monitoring
Main General				<b>Port Ti</b> Trigger opening of p		-	а.	
Access Control		Protocols		Outgoing Trigger	Ports	Incomin	g Ports to Open	Action
Port Forwarding	L2TF	P - Layer Two Tunneling	Protocol	UDP Any -> 1701	U	DP Any -> Si	ame as Initiating Ports	
DMZ Host	TFTP	- Trivial File Transfer	Protocol	UDP 1024-65535 -:	⊳69 U	DP Any -> S	ame as Initiating Ports	
	Appl	ication		TCP 20 -> 23	U	DP 27 -> 28		A 🗱
Port Triggering		bow Six		TCP Any -> 2346	Т	CP Any -> 23	346	*
Remote Administration	Add	*						
Static NAT								
Advanced Filtering			_					
					Apply	) 💙 X <u>Can</u>	cel	
Security Log								
Connections								
Logout								



User Guide

### 13.6 Remote Admin

If you select **Firewall Settings** in the top navigation menu and then select **Remote Administration** in the left submenu, the following screen will appear.

It is possible to access and control your Router not only from within the home network, but also from the Internet. This allows you to view or change settings while traveling. It also enables you to allow your service provider to change settings or help you troubleshoot functionality or communication issues from a remote location. Remote access to your Router is blocked by default to ensure the security of your network. However, your Router supports the following services, and you can use the Remote Administration screen to selectively enable these services if they are needed.

**WARNING:** With Remote Administration enabled, your network will be at risk from outside attacks. Note that remote command line access (Telnet) is not enabled on this Router.

To configure Remote Administration, enter the appropriate settings, and then click Apply to save the settings.

veriz	on					_
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main General			Remote	Administration		
Access Control	Allowing	remote administration	to Wireless Broadband R	Attention outer is a security risk.		
Port Forwarding DMZ Host			ing WAN Access to th	e Telnet Server		
Port Triggering		X Using Secor X Using Secur	ary Telnet Port (23) ndary Telnet Port (8023) re Telnet over SSL Port ( <b>sing WAN Access to W</b>	(992)		
Remote Administration Static NAT		Using Prim	nary HTTP Port (80) ondary HTTP Port (8080)			
Advanced Filtering		Using Seco	nary HTTPS Port (443) ondary HTTPS Port (844)	3)		
Security Log		Diagnostic T Allow Inco queries)	ools ming WAN ICMP Echo Re	equests (e.g. pings and IC	CMP traceroute	
Connections			ming WAN UDP Tracerou			
Logout				! Apply		



User Guide

### 13.7 Static NAT

If you select **Firewall Settings** in the top navigation menu and then select **Static NAT** in the left submenu, the following screen will appear.

**NOTE:** A block of static IP addresses must be purchased from Verizon to configure this feature. This Router supports 253 static IP addresses.

Static NAT allows LAN devices to use public IP addresses (different from the Router's public IP address). The LAN devices are still configured with private IP addresses (either statically or dynamically through DHCP). Traffic between the LAN devices and the Internet is still "NAT'ed", but the Static NAT mappings allow packets from specific devices to use a distinct public IP address; and packets sent to different public IP addresses to be forwarded to specific devices.

With Static NAT, devices that are behind the firewall and that are configured with private IP addresses appear to have public IP addresses on the Internet. This allows an internal host, such as a Web server, to have an unregistered (private) IP address and still be reachable over the Internet. This section also allows you to perform port translations (NAPT)

There are three steps to setting up a Static NAT entry:

- 1. Create an address pool These are addresses on your WAN network side
- 2. Create a NAT rule This defines the local computer to be NATd, the external IP address from the pool and the services that are allowed
- 3. Create a Port Forwarding Rule This matches the NAT rule you created above and forwards the packets received on the WAN side to reach your internal computer.

To configure Static NAT, you must first define what external addresses are available. You add them to the address pool by clicking the **New IP Address** link or the plus icon. These addresses should be provided by your ISP.

Main	Wireless	My Network	Firewall Settings	Parental Contro	ol Advan	ced S	System Monitoring
Main General		lresses Pool	IP Address	Static NAT		Act	
Access Control	New IP Add					4	
Port Forwarding	Rule ID So	urce Address Des Ad	Idress	otocols	Operation	Status	Action
DMZ Host	Broadband	Connection (Ether	net) Rules				<u>New Entry</u>
Port Triggering Remote Administration Static NAT		<ul> <li>✓ <u>ok</u></li> </ul>	Apply	X Cancel	esolve Now	C <u>Refresh</u>	
Advanced Filtering							
Security Log							
Connections							
Logout	ļ						



User Guide

Select the **Network Object Type** from drop-down list, select the desired object type. A single IP address, an entire subnet, a range of addresses or a specific DHCP Vendor option. (These are generic "Network" objects that are defined in the **Network Objects** section.)

Network Object Type:     IP Address       IP Address:     IP Address       IP Subnet     IP Range       DHCP Option	Add Item	
IP Subnet IP Range	Type: IP Address 🗸	Network Object Type:
✓ <u>OK</u> X <u>Cancel</u>	IP Subnet IP Range DHCP Option	IP Address:

For example, if you select **IP Address** as the network object type you must specify a single WAN IP address to add to the pool. Enter a valid WAN IP address then click **OK** to continue.

	Add Item
Network Object Type: IP Address:	IP Address  213 . 132 . 89 . 105
	OK Cancel

If you have entered an IP Address and clicked **OK** in the **Add Item** screen, you are directed back to the main screen and your network address is shown in the pool. You now must create the **NAT/NAPT Rule Set** for this new external IP Address. To create rule, under **NAT/NAPT Rule Sets**, click the **New Entry** link.

		Static NAT			
NAT IP Addresses Pool					
	IP Addre	:55		Actio	
<u>213.132.89.105</u>				1	*
New IP Address				4	
NAT/NAPT Rule Sets Rule ID Source Address	Destination Address	Protocols	Operation	Status	Action
Broadband Connection (E	thernet) Rules				New Entry
broadband Connection tr	thernet) kules				New Enti



User Guide

If you clicked New Entry, the following screen will appear.

Matching	
Source Address	Any 🗖
Destination Address	Any 🗖
Protocols	Any
Operation	
	ze IP translation rule.
NAT Addresses	Add
Logging	
🔲 Log Packets Matched by This Rule	20 (C. S.)
Schedule	Always 🗖

This screen is divided into two main sections, 'Matching' and 'Operation'. The 'Matching' section defines the LAN addresses to be translated to the external addresses, which are defined in the 'Operation' section. You define the type of traffic that should be "matched" – that is a specific source of the traffic, a specific destination and the type of traffic.

Matching: Use this section to define the rule's conditions, which are the LAN computer's parameters to be matched.

**Source Address:** The source address of packets sent or received from the LAN computer. The combo box displays all the host names or IP addresses of currently connected LAN computers, as well as the options 'Any' and 'User Defined'. Select an address from the list, or 'Any' to apply the rule on all computers. If you would like add a new address, select the 'User Defined' option in the combo-box. This will commence a sequence that will add a new *network object*, representing the LAN computer.

**Destination Address:** The specific destination address of packets coming from the above Source address. You will want to keep this set at **Any** in most cases to allow any remote destination to receive packets from the **Source Address**.

**Protocol** You may also specify a specific protocol. Selecting the 'Show All Services' option in the combobox will expand the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This will commence a sequence that will add a new *service*, representing the protocol.

In most cases your **Destination Address** and **Protocols** will be set to **Any**. This example shows setting up a NAT'd web server on your local LAN on a computer at 192.168.1.50.

**Operation:** Use this section to define the operation that will be applied on the IP addresses matching the criteria defined above. The operations available are NAT or NAPT. Selecting each from the combo-box will refresh the screen accordingly.

**NAT Addresses** The NAT address into which the original IP address will be translated. The combo box displays all of your added NAT addresses/ranges, from which you can select an entry. If you would like to add a new address, select the 'User Defined' option in the combo-box. Similarly, this will commence a sequence that will add a new network object.



User Guide

**NAPT Address:** The NAPT address into which the original IP address will be translated. The combo box displays all of your added NAPT addresses/ranges, from which you can select an entry. If you would like to add a new address, select the 'User Defined' option in the combo-box. Similarly, this will commence a sequence that will add a new network object. Note, however, that in this case the network object may only be an IP address, as NAPT is port-specific.

**NAPT Ports:** Specify the port(s) of the IP address into which the original IP address will be translated. Enter a single port or select **Range** in drop-down list. The screen will refresh, enabling you to enter a range of ports.

**Log Packets Matched by This Rule:** Check this check box to log the first packet from a connection that was matched by this rule.

**Schedule:** By default, the rule will always be active. However, you can configure scheduler rules by selecting **User Defined**, in order to define time segments during which the rule may be active. Refer to section 15.19 for details on setting up schedule rules.

After you select the desired NAT/NAPT rules, click **OK** to continue.

Matching			
Source Address Name		Address	Action
PC on LAN	192,168,1,50	Address	
	192.100.1.50		
Add 💙			
Destination Address		Any 🗸	
Protocols			
Name		Ports	Action
HTTP - Web Server	TCPAny -> 80		*
Add	*		
Operation			
NAT 💌	Source IP tra	nslation rule.	
NAT Addresses			
Name		Address	Action
NAT IP Address	213.132.89.105		*
Add 💙			
Logging			
✓ Log Packets Matched by T	his Rule		
Schedule		Always 🗸	



User Guide

If you clicked **OK**, the following screen will appear. This screen displays the active rules for the designated address.

**NOTE:** After you create the rule LAN devices, you can verify it works by checking your external IP address. You can do this from another internet connection or by using one of many public websites that display your external IP address. Note this only works if you have specified **Any** or one of the **HTTP** protocols.

	Static NAT											
NAT IP	IAT IP Addresses Pool											
IP Address Action 213.132.89.105												
New IP	Address											
NAT/NAPT Rule Sets												
Rule ID	Source Address	Destination Address	Protocols	Operation	Status	Action						
Broadb	and Connection (	(Ethernet) Rules	5									
<b>⊻</b> <u>0</u>	192.168.1.50	Any	HTTP - TCP Any -> 80	NAT -> 213.132.89.105	Active	🔨 🗱						
<u>New</u> Entry						4						
		OK I	Apply	Resolve Now	O Refresh							

After setting up your NAT/NAPT rule set you must also setup a **Port Forwarding** entry so that all incoming traffic is directed to the LAN computer you setup in the above steps.

Click on **Port Forwarding** in the left-hand navigation bar to start making your inbound rule. Create a <u>New Entry</u> by clicking the link or + sign.

Main	Wireless	My Network	Firewall Set	tings Parent	al Control	Advanced	System Monitoring
Main General			Expose servi	Port Forwar	r <b>ding</b> xternal Internet use	ers.	
Access Control	Local H	ostLocal Address	Network Address	Public IP Address	Protocols	Status	Action
Port Forwarding	✓ localh New En		Any	Any	TCP Any -> 4567	Active	
DMZ Host	New Li	<u>u v</u>					T
Port Triggering							
Remote Administration			Apply	Cancel	Resolve Now	Refres	h
Static NAT							
Advanced Filtering							



User Guide

As in the example below, you will need to specify your external IP address that you used for your NAT/NAPT rule and also specify the local host (IP or name). Also make sure that you use the same protocol as your NAT/NAPT rule. For our web server example this information is shown filled in below.

**NOTE:** When setting up your Port Forwarding setting please ensure that you enter in the same external IP address information as well as match what protocols were defined in the NAT/NAPT rule you just created.

Specify Public IP Address Public IP Address: Local Host: Specify Network IP Address		213     .     132     .     89     .     105       192.168.1.50	
Protocols Name		Ports	Action
HTTP - Web Server	TCPAny -> 80	FUILS	
Add	*		
Forward to Port:		Same as Incoming Port 💙	
Schedule		Always 🗸	

Clicking <u>**OK**</u> will take you back to the main port forwarding page and it will show your newly created rule.

Port Forwarding									
Expose services on the LAN to external Internet users.									
Local Host	Local Address	Network Address	Public IP Address	Protocols	Status	Action			
Iocalhost	127.0.0.1	Any	Any	TCP Any -> 4567	Active				
✓ 192.168.1.50	192.168.1.50	Any	213.132.89.105	HTTP - TCP Any - > 80	Active	🔨 🗶			
New Entry						-			

Refer to the Port Forwarding Section for more information on other options for port forwards.

Your NAT/NAPT rule has now been created and your machine should be accessible via the IP address you specified in your rule.



User Guide

### **13.8** Advanced Filtering

If you select **Firewall Settings** in the top navigation menu and then select **Advanced Filtering** in the left submenu, the following screen will appear.

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

This screen is divided into two sections, one for Input Rule Sets and the other for Output Rule Sets, which are for configuring inbound and outbound traffic, respectively. Each section comprises subsets, which can be grouped into three main subjects:

- Initial rules—rules defined here will be applied first, on all gateway devices.
- Network device rules—rules can be defined per each gateway device.
- Final rules—rules defined here will be applied last, on all gateway devices.

To add rules to Input or Output rules sets, click the adjacent New Entry link.

Main	Wireless My Networ	k Firewa	JII Settings Parenta	l Control Advar	nced Syst	tem Monitoring
Main			Advanced Filto	ering		
General	Input Rule Sets Rule ID Source Address	Destination Address	Protocols	Operation	Status	Action
Access Control	Initial Rules Network (Home/Office) I Ethernet Switch Rules	1001055				<u>New Entry</u> <u>New Entry</u> New Entry
Port Forwarding DMZ Host	Broadband Connection (I Wireless 802.11g Access Final Rules					<u>New Entry</u> New Entry
Port Triggering	Output Rule Sets	Destination				<u>New Entry</u>
Remote Administration	Rule ID Source Address	Address	Protocols	Operation	Status	Action
Static NAT	Network (Home/Office) I Ethernet Switch Rules	Rules				<u>New Entry</u> <u>New Entry</u> <u>New Entry</u>
Advanced Filtering	Broadband Connection (I Wireless 802.11g Access Final Rules					<u>New Entry</u> <u>New Entry</u> New Entry
Security Log	rinai kules					New Entry
Connections						
Logout			Apply Cancel	Resolve Now	C Refresh	



User Guide

For example, if you clicked the **New Entry** link for input Network (Home/Office) Rules, the following screen will appear.

Matching						
Source Address		Any	*			
Destination Address		Any	*			
Protocols		Any		1	*	
Operation						
Drop 💙	Drop packets.					
Logging						
Log Packets Matched by This Rule						
Schedule		Always	*			
	√ <u>ok</u>	X Car				

Select one of the following operation settings:

- Select **Drop** to drop packets.
- Select Reject to drop packets, and to send TCP Reset or ICMP Host Unreachable packets to the sender.
- Select Accept Connection to accept all packets related to this session.
- Select Accept Packet to accept packets matching this rule only. Do not use Stateful Packet Inspection (SPI) to automatically accept packets related to this session.

After you have entered the desired values, click **OK** to continue.

Matching		
Source Address		
Name	Address	Action
computer	192.168.1.3	*
Add 💙		
Destination Address		
Name	Address	Action
computer	192.168.1.3	× .
Add 💙		
Protocols		
Name	Ports	Action
Delta Force	TCPAny -> 3100-3999 UDPAny -> 3568	*
Add 🗸		
Operation		
Accept Packet	Accept packets matching this rule only. Do not u Inspection (SPI) to automatically accept packets session.	
Logging		
Log Packets Matched by This Rul	e	
	Always 🗸	



User Guide

If you clicked **OK**, the following screen will appear. The rule is now active.

	Advanced Filtering										
Input R	nput Rule Sets										
Rule ID Source Address Destination Address Protocols Operation Status Actio											
Initial	Initial Rules										
<b>₽</b> 0	192.168.1.3	192.168.1.3	Delta Force - UDP Any -> 356 TCP Any -> 3100-3999	B Accept Packet No Connection	Active	🔨 🗱 👘					
<u>New</u> Entry						-					
Ethern Broadb	letwork (Home/Office) Rules New Entry thernet Switch Rules New Entry roadband Connection (Ethernet) Rules New Entry Vireless 802.11g Access Point Rules New Entry										
	Final Rules Output Rule Sets Output Rule Sets										
	) Source Address	Destination Address	Protocols	Operation	Status	Action					
Initial						New Entry					
	k (Home/Office)	Rules				New Entry					
	et Switch Rules					New Entry					
	and Connection ( ss 802.11g Acces		•			<u>New Entry</u> New Entry					
		s i onic Kuics									
	Final Rules New Entry										

The order of the rules appearance represents both the order in which they were defined and the sequence by which they will be applied. By clicking the Move Up and Move Down action icons, you can change this order after your rules are already defined (without having to delete and then re-add them). After you click the desired icon, the screen will refresh and display the change.

<b>0</b>	10.10.1.5	192.168.1.50	Dark Reign 2 - TCP Any -> 26214 UDP Any -> 26214	Drop	Active	<b>↓</b> \ <b>X</b>
<u>1</u>	234.10.65.25	192.168.1.51	FTP - TCP Any -> 21	Accept Connection	Active	1 1 2



User Guide

## 13.9 Security Log

If you select **Firewall Settings** in the top navigation menu and then select **Security Log** in the left submenu, the following screen will appear.

This screen alerts you of noteworthy information sent to Router from the Internet. The screen can contain 1000 entries, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for the new entries as they occur. In this screen, do any of the following:

- Click **Close** to close the security log screen.
- Click Clear Log to remove all entries from the log.
- Click **Save** to save the settings to a syslog server.
- Click Settings to configure the security settings. Clicking this button opens a new window that contains configuration options for selecting the information that you want logged.
- Click **Refresh** to refresh the security log screen.

To configure the security log settings, click the **Settings** button.

Main	Wireless	My Net	twork	Firewall Settings	Parental Control	Advanced	System Monit	oring			
Main				S	ecurity Log						
General			Close	Clear Log	Save Log Setting	s Refres	<u>sh</u>				
Access Control		Press the <b>Refresh</b> button to update the data.									
Port Forwarding											
DM7 //		Time	Event	Event-Type		Details					
DMZ Host		Dec 31 23:31:01 2002	Setup	Firewall internal	Firewall configuration succ	eeded					
Port Triggering		Dec 31 23:31:01 2002	Firewall Setup	Firewall internal	Starting firewall configurat	ion					
Remote Administration		Dec 31 23:22:53 2002	WBM Login	User authentication success	Username: admin						
Static NAT		Dec 31 21:40:03 2002	Firewall Setup	Firewall internal	Firewall configuration succ	eeded					
Advanced Filtering		Dec 31 21:40:02 2002	Firewall Setup	Firewall internal	Starting firewall configurat	ion					
		Dec 31 21:34:48 2002	Firewall Setup	Firewall internal	Firewall configuration succ	eeded					
Security Log		Dec 31 21:34:48 2002	Firewall Setup	Firewall internal	Starting firewall configurat	ion					
Connections		Dec 31 21:31:12 2002	Firewall Setup	Firewall internal	Firewall configuration succ	eeded					
Logout		Dec 31 21:31:12 2002	Firewall Setup	Firewall internal	Starting firewall configurat	ion					
	″	Dec 31 21:10:07 2002	Firewall Setup	Firewall internal	Firewall configuration succ	eeded					
		Dec 31 21:10:07 2002	Firewall Setup	Firewall internal	Starting firewall configurat	ion					
		Dec 31 21:09:05 2002	Firewall Setup	Firewall internal	Firewall configuration succ	eeded					
		Dec 31 21:09:05 2002	Firewall Setup	Firewall internal	Starting firewall configurat	ion					
		Dec 31 21:07:32 2002		Firewall internal	Firewall configuration succ	eeded					



User Guide

If you clicked **Settings**, the following screen will appear. Select the desired settings by clicking the check boxes (a checkmark will appear in the box when a setting is enabled). Then, click **Apply** to save the settings.

	Security Log Settings	
Accepted Events  Accepted Incoming Connections  Accepted Outgoing Connections		
Blocked Events		
Winnuke	Multicast/Broadcast	ICMP Replay
Defragmentation Error	Spoofed Connection	ICMP Redirect
Blocked Fragments	Packet Illegal Options	ICMP Multicast
Syn Flood	UDP Flood	ICMP Flood
Echo Chargen		
Other Events  Remote Administration Attempts Connection States  Log Buffer Prevent Log Overrun		
	Apply X Cancel	1

Select the types of activities for which you would like to have a log message generated:

Accepted Events

Accepted Incoming Connections Write a log message for each successful attempt to establish an inbound connection to the home network.

Accepted Outgoing Connections Write a log message for each successful attempt to establish an outgoing connection to the public network.

Blocked Events

**All Blocked Connection Attempts** Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.

**Specific Events** Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message will be generated if either the corresponding check-box is checked, or the "All Blocked Connection Attempts" check-box is checked.

• Other Events

**Remote Administration Attempts** Write a log message for each remote-administration connection attempt, whether successful or not.

**Connection States** Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).

• Log Buffer

**Prevent Log Overrun** Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.



User Guide

### 13.10 Connections

If you select **Firewall Settings** in the top navigation menu and then select **Connections** in the left submenu, the following screen will appear.

The connections list displays all the connections that are currently open on the firewall, as well as various details and statistics. You can use this list to close undesired connections by clicking the "X" icons. The basic display includes the protocol type, the different ports it uses, and the direction of the secured traffic.

- Active Connections—this value represents the number of active concurrent connections.
- Approximate Max. Connections—this value represents the amount of additional concurrent connections possible.
- Connections Per Page—use this drop-down list to select the number of connections to display at once.

Click the **Advanced** button to display a more detailed connection list.

		Active Co Approxim Connectio		35 161987			
Connectio	Protocols	LAN IP:Port	Winslass B.	roadband Router IP:Port	Connection WAN IP:Port	s Per Page Direction	10 🗖
1	TCP	192.168.1.3:2643	10.16.67.127:2		10.16.16.8:139	Outgoing	ACCION
2	UDP	192.168.1.3:137	10.16.67.127:1	37	10.16.16.8:137	Outgoing	
3	UDP	192.168.1.3:123	10.16.67.127:1	23	10.16.16.8:123	Outgoing	- X
4	тср	192.168.1.3:2574	10.16.67.127:2	574	10.16.16.8:139	Outgoing	
5	TCP	192.168.1.3:2364	10.16.67.127:2	364	10.16.16.8:139	Outgoing	*
6	TCP	192.168.1.3:2308	10.16.67.127:2	308	10.16.16.8:139	Outgoing	*
7	TCP	192.168.1.3:2272	10.16.67.127:2	272	10.16.16.8:139	Outgoing	*
8	тср	192.168.1.3:2242	10.16.67.127:2	242	10.16.16.8:139	Outgoing	*
9	TCP	192.168.1.3:2086	10.16.67.127:2	086	10.16.16.8:139	Outgoing	*
10	TCP	192.168.1.3:1656	10.16.67.127:1	656	10.16.16.8:139	Outgoing	*
		√ ок	Apply	1 <u>2 3 4</u>	Refresh		

If you clicked **Advanced**, the following screen will appear. Additional details in this page include connection status (LAN/WAN), time-to-live, number of kilo-bytes and packets received and transmitted, ALG device, routing mode, and flags. To close undesired connections, click their adjacent "X" icons.

			Active Cor Approxima	nections: ate Max. Conn	ections: 162075								
Connect	ion List										nections Pe	er Page	10 🛰
Number	Protocols	LAN IP:Port	Wireless Broadband Router IP:Port	WAN IP:Port	Status LAN/WAN	Time To Live (seconds)	Kbytes Kx/1x	Packets Al	.G Device	Routing	Direction	Flags	Actio
1	тср	192.168.1.2:4638	10.16.90.10:4638	10.16.16.50:80	ESTABLISHED/ESTABLISHED		7 0.6/0.1		WAN PPPoE	NAPT	Outgoing	DEL PENDING FP-CAP FP-REQ FP-ENA	×
2	тср	192.168.1.2:4274	10.16.90.10:4274	10.16.16.50:80	ESTABLISHED/ESTABLISHED	402497	0.1/6.2	3/8	WAN PPPoE	NAPT	Outgoing	DEL PENDING FP-CAP FP-REQ FP-ENA	*
3	тср	102.168.1.2:4263	10.16.90.10:4263	10.16.16.50:80	ESTABLISHED/ESTABLISHED	402257	7 0.6/0.4	3/5	WAN PPPoE	NAPT	Outgoing	DEL PENDING FP CAP FP-REQ FP-ENA	*
4	тср	192.168.1.2:3598	10.16.90.10:3598	10.16.16.50:80	ESTABLISHED/ESTABLISHED	363077	7 0.1/6.2	3/8	WAN PPPoE	NAPT	Outgoing	DEL- PENDING FP CAP FP REQ FP ENA	*
					1 <u>2</u>								



User Guide

# **14. PARENTAL CONTROLS**

If you select **Parental Controls** in the top navigation menu and then select **Website Restrictions** in the left submenu, the following screen will appear. This feature allows you to block LAN access to certain hosts on the Internet or to certain Web sites. To configure a website restriction, click the **New Entry** link.

Main	Wireless	My Net	work Fire	ewall Settings	Parental Control	Advanced	Syst	em Monitoring
Main Parental Control Logout		Local Host	Local Address		ntal Control from the LAN to web	sites. ricted IP Address	Status	Action
		New Entry		Press the <b>Refres</b>	h button to update th			Action

If you clicked **New Entry**, the following screen will appear. In the **Restricted Website** field, enter the desired website to which you want to restrict access. You can enter a valid IP address or domain name. Next, select a host from the **Local Host** drop-down list.

	Restricte	d Website	te				
	Enter the website you wish to restrict:						
Restricted Website:							
Local Host		Any	★				
Schedule		Always	×				
		Cano	ncel				



User Guide

After you have selected a local host, the following screen will appear. Click **OK** to continue. To add a user-defined host to your list of restricted access, click **User Defined** in the **Add** drop-down list.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Restricted Website				icted Website		
Logout		Restricted Website: .ocal Host DHCP Add V Add User Defined	RSCHULAB-T200	Address		Action
			<u> √ ok</u>	X Cancel		

If you selected User Defined, the following screen will appear. Click the New Entry link.

	Add Network Object						
Network Object Description:	Network O	bject					
Items							
	Item	Action					
New Entry							
		ncel					



User Guide

If you clicked **New Entry**, the following screen will appear. Select the desired object type from the **Network Object Type** drop-down list.

**NOTE:** You can select any option from the **Network Object Type** drop-down list, and then configure the screen accordingly.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Edit Item Logout		Network Object Type IP Address:		IP Subnet IP Range MAC Address	0.0	

For example, if you selected **IP** Address, the following screen will appear. Enter the desired IP address in the field provided, and then click **OK** to continue.

	Add Item
Network Object Type: IP Address:	IP Address
	OK Cancel



User Guide

If you clicked **OK**, the following screen will appear. Enter the desired description in the **Network Object Description** field, and then click **OK** to continue.

Add Netw	Add Network Object					
Network Object Description:	First PC					
Items						
Item	Action					
<u>192.168.1.3</u>	🔪 🗶					
New Entry						
	X Cancel					

Next, select the desired schedule from the Schedule drop-down list, and then click OK to continue.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Mon	itoring
Main Restricted Website				icted Website ssite you wish to restrict:			
Logout		Restricted Website: Local Host					
		Name DHCP	RSCHULAB-T2000	Address		Action	
		First PC	192.168.1.3			× *	
		Add 💙					
		Schedule		Always 🗸			
				Always User Defined X <u>Cancel</u>			



User Guide

For example, if you selected **Always**, and then clicked **OK** in the preceding screen, the following screen will appear. This screen shows the IP address with an active website restriction. In this example, the PC that has IP address "192.168.1.3" will be prohibited from accessing the specified Web site.

**NOTE:** If the **Status** field displays **Resolving**, this means that the Router is attempting to locate the restricted Web site. Click **Resolve Now**; the restricted Web site will be resolved into the IP address that you have specified, and the **Status** field will display **Active**.

Parental Control Restrict access from the LAN to websites.											
Local Host	Local Address	Restricted Website	Restricted IP Address	Status	Action						
RSCHULAB-T2000 192.168.1.3	RSCHULAB-T2000 192.168.1.3	www.dogpile.com	www.dogpile.com	Active	1 🗱						
New Entry					-						
	Press the	Refresh button to updat	e the data.								
	Apply	Cancel	Resolve Now	sh							

To disable the website restriction, click to clear the check box adjacent to the IP address. Then, click **Apply** to allow the settings to take effect. When the restriction status displays **Disabled**, the computer will have permission to access the Web site.

	Pare	ntal Control		
	Restrict access	from the LAN to websi	tes.	
Local Host	Local Address	Restricted Website	Restricted IP Address	Status Action
□ <u>RSCHULAB-T2000</u> <u>192.168.1.3</u>	RSCHULAB-T2000 (Unresolved) 192.168.1.3	www.dogpile.com	www.dogpile.com	Disabled 🔪 🗱
New Entry				-
	Press the <b>Refres</b>	<b>h</b> button to update the	data.	
		X Cancel Reso	lve Now	h

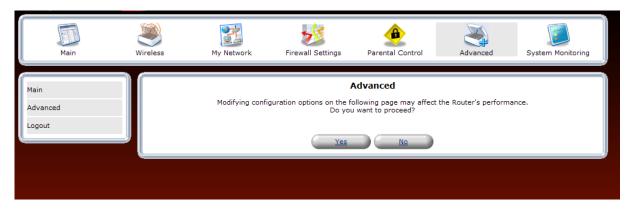


User Guide

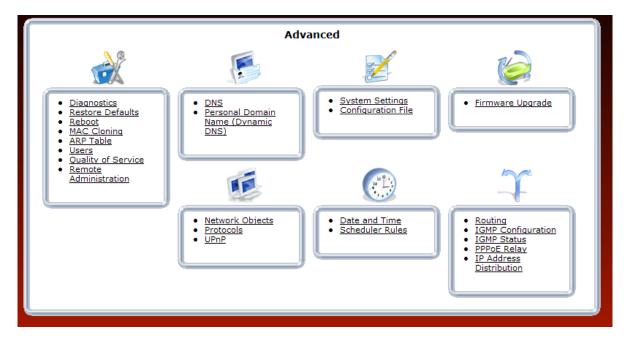
# **15. ADVANCED**

If you select **Advanced** in the top navigation menu, the following screen will appear. The Advanced section of this User Guide is intended to provide assistance with configuring the Advanced features of your Verizon FiOS Router and assumes the user has an in-depth understanding of computers, routing, and internet networking.

Click Yes to proceed to the Router's Advanced screen.



Clicking the links in the Advanced screen allows you to access various configurable settings in your Router.





User Guide

### **15.1 Diagnostics**

If you click the **Diagnostics** link in the **Advanced** screen, the following screen will appear. Using this screen, you can run the following diagnostics tests:

- To run a PING test, type the appropriate IP address or host name in the field provided, and then click Go.
- To run a Traceroute test, type the appropriate IP address or host name in the field provided, and then click Go.

	Diagnostics	
Ping (ICMP Echo) Destination: Number of pings: Status:	4	Go
Traceroute Destination: Status:		Go
	Press the <b>Refresh</b> button to update the status.	



User Guide

For example, if you enter a host name in the **Destination** field and then click **Go**, the following screen will appear. This screen shows that the Ping test succeeded. Click **Close** to return to the **Advanced** screen.

	Diagnostics	
Ping (ICMP Echo)		
Destination:	www.yahoo.com	Go
Number of pings:	4	
Status: Packets:	Test Succeeded 4/4 transmitted, 4/4 received, 0% loss Minimum = 37 ms	
Round Trip Time:	Maximum = 64 ms	
	Average = 45 ms	
Traceroute		
Destination:		Go
Status:		
	Press the <b>Refresh</b> button to update the status.	



User Guide

### **15.2 Restore Defaults**

If you click the **Restore Defaults** link in the **Advanced** screen, the following screen will appear. Click **OK** to allow the Router to be reset to factory default settings. After the Router has rebooted, you will need to log in to the Router.

**IMPORTANT:** If you click **OK**, any settings that you have configured in the Router will be erased, and any data that the Router has reported will be lost.

Restore Defaults
Attention The following items will be set to default:  User Defined Settings Network Connections (All connected DHCP clients will need to request new IP addresses) Also, Wireless Broadband Router will have to reboot.
Are you sure you want to restore Wireless Broadband Router manufacturer defaults?



User Guide

### 15.3 Reboot

If you click the **Reboot** link in the **Advanced** screen, the following screen will appear. Rebooting the Router allows the Router to be restarted. Click **OK** to allow the Router to reboot. Please wait a brief moment while the Router is rebooting. Afterwards, you will need to log in to the Router.

**IMPORTANT:** The **Reboot** feature does not reset the Router to factory default settings. If you want to reset the Router to factory default settings, follow the instructions in section 15.2, "Restore Defaults."



# 15.4 MAC Cloning

If you click the **MAC Cloning** link in the **Advanced** screen, the following screen will appear. A Media Access Control (MAC) address is a hexadecimal code that identifies a device on a network, such as a router. All networking devices have a MAC address, and in some cases, your service provider may need you to provide the MAC address of your network device. If you use MAC Cloning, you can simply enter the MAC address of the "old" Router into your Verizon Broadband Router, bypassing the need to contact the service provider with "new" MAC Address values (from the Verizon Broadband Router).

To configure MAC Cloning, enter the MAC Address of the Router you are replacing. Then, click **Apply** to save the settings.

**NOTE:** By default, this screen displays the MAC address of the Verizon Broadband Router. Replace these values with the MAC address of your "old" Router and click **Apply**.

	MAC Cloning
Set MAC of Device: To Physical Address:	Broadband Connection (Ethernet) 00 : 18 : 3a : ac : 3a : 9b
	Apply X Cancel



User Guide

# 15.5 ARP Table

If you click the **ARP Table** link in the **Advanced** screen, the following screen will appear. This screen allows you to set up static DHCP connections using Host Names, IP Addresses, or MAC addresses. To configure a static DHCP connection, click the **New Static Connection** link.

			Connec				
Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
SALLE-XP3	192.168.1.2	00:11:11:83:e9:53	Static	Network (Home/Office)	Active	1440 Minutes	2 🔪 🗶
<u>New Static</u> Connection							-
		Press the <b>Refresh</b>	button to	update the data.			
		Close		Refresh			

If you clicked **New Static Connection**, the following screen will appear. Enter the appropriate values in the fields provided, and then click **OK** to continue.

**NOTE:** You can have a total of 253 static LAN devices connected to your Verizon Router.

- Enter a host name for this connection.
- Enter the fixed IP address to assign to the computer.
- Enter the MAC address of the computer's network card.

**NOTE:** A device's fixed IP address is actually assigned to the specific network card's MAC address installed on the network computer. If this network card is replaced, the device's entry in the DHCP Connections list must be updated with the new network card's MAC address.

Host Name: IP Address:	DHCP Connection Settings
MAC Address:	00 : 00 : 00 : 00 : 00 : 00



#### User Guide

For example, if you enter an IP Address and a MAC address and then click **OK**, the following screen will appear. The screen shows that the entry has been added to the list of static DHCP connections. To run a diagnostics test on a DHCP connection, aligh the diagnostics icon *P* adjacent to the connection you want to test. To remove a host from

DHCP connection, click the diagnostics icon  $\stackrel{\text{$\sim$}}{\sim}$  adjacent to the connection you want to test. To remove a host from the table, click the appropriate "X" icon in the Action column.

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
SALLE-XP3	192.168.1.2	00:11:11:83:e9:53	Static	<u>Network</u> (Home/Office)	Active	1440 Minutes	2 🔪 🗱
new-host	192.168.1.4	00:03:04:05:06:07	Static	<u>Network</u> (Home/Office)	Expired		2 🔪 🗱
new-host1	192.168.1.16	00:16:04:05:06:07	Static	<u>Network</u> (Home/Office)	Expired		2 🔪 🗱
<u>New Static</u> Connection							4
		Press the <b>Refresh</b>	button to i	update the data.			

If you clicked the diagnostics icon, the following screen will appear. Review the status of the diagnostics test, and then click **Close** to return to the **DHCP Connections** screen.

	Diagnostics	
Ping (ICMP Echo)		
Destination:	192.168.1.16	Cancel
Status: Packets:	Testing 0/4 transmitted, 0/4 received	
Traceroute		
Destination:		Go
Status:		
	Press the <b>Refresh</b> button to update the stat	us.
	Close Refresh	



User Guide

## **15.6** Users

If you click the **Users** link in the **Advanced** screen, the following screen will appear. This feature allows you to configure user settings in the Router.

		Users				
Users						
Full Name	User Name		ermissions	Action		
Administrator	admin	Web-based Manage	ment Access	<u> </u>		
New User				-		
Groups						
Name Description Members Action						
Users						
New Group 🔶						
Close						



User Guide

### **15.6.1** Users—Adding a New Administrator

If you click the **Administrator** link in the **Users** screen, the following screen will appear. This screen allows you to set up the desired Administrator values. Enter the appropriate values, and then click **OK** to save the changes.

**NOTE**: If the Router is password protected and you are not an authorized user, you will not be allowed to change and save the values in this screen. (The Router cannot be configured unless the user is logged in.) Contact your network administrator for further instructions.

- Full Name—Enter the user's full name.
- User Name—Enter the name a remote user will use to access the home or office network. This field is casesensitive.
- New Password/Retype New Password—Enter the password for the user (and enter it again to confirm).
- Permissions—Click the check box to enable web-based management access.

	User Settings
General Full Name: User Name: New Password: Retype New Password: Permissions:	Administrator
User Name: New Password:	admin
Retype New Password: Permissions:	<ul> <li>Web-based Management Access</li> </ul>



User Guide

# 15.6.2 Users—Adding a New User

If you click the **New User** link, the following screen will appear. This screen allows specific users to have administrative permissions in the Router.

User Settings				
General Full Name: User Name:				
New Password: Retype New Password: Permissions:	Web-based Management Access			

To configure User Settings, enter the appropriate values, and then click OK to save the changes.

**NOTE:** The User Name and Password values must be at least 6 characters, and should consist of standard characters only (ASCII 32-126), excluding the special character space and any of these characters : @''|V=+>[]\*?,;. Also, user names containing capital letters are not recommended. It might cause connectivity problems on Windows 98 hosts.

General         Full Name:       DavidDoe         User Name:       davedoe         New Password:	Full Name: DavidDoe   User Name: davedoe   New Password: •••••••   Retype New Password: •••••••   Primary Group: Users 👻   Permissions: If Web-based Management Access	User Settings				
User Name: davedoe New Password: •••••• Retype New Password: •••••• Primary Group: Users V Permissions: Veb-based Management Access	User Name: davedoe New Password: •••••• Retype New Password: •••••• Primary Group: Users V Permissions: Veb-based Management Access	General				
New Password:       •••••••         Retype New Password:       •••••••         Primary Group:       Users          Permissions:       ✓ Web-based Management Access	New Password:       ••••••         Retype New Password:       ••••••         Primary Group:       Users 🗸         Permissions:       ✓ Web-based Management Access	Full Name:	DavidDoe			
Retype New Password:       •••••••         Primary Group:       Users v         Permissions:       v Web-based Management Access	Retype New Password:       •••••••         Primary Group:       Users          Permissions:       Image: Web-based Management Access	User Name:	davedoe			
Primary Group:     Users V       Permissions:     V Web-based Management Access	Primary Group:     Users        Permissions:     V Web-based Management Access	New Password:	•••••			
Permissions: Web-based Management Access	Permissions: Web-based Management Access	Retype New Password:	••••••			
		Primary Group:	Users 💟			
✓ <u>OK</u> X <u>Cancel</u>	<u>✓ OK</u> <u>Cancel</u>	Permissions:	Web-based Management Access			
✓ <u>OK</u> X <u>Cancel</u>						



User Guide

After you have entered the appropriate values and click **OK**, the following screen will appear. The user information has been added to the Router. If desired, repeat the preceding instructions to add additional users to the administrator permissions list.

Users						
Full Name User Name Permissions Action						
Administrator	admin	Web-based Manage	ement Access	<u> </u>		
DavidDoe davedoe Web-based Management Access						
New User						
Groups Name Description Members Action						
Users DavidDoe						
New Group						
Close						



User Guide

# 15.6.3 Users—Removing a User

To remove a user from the list, click the "X" icon. The following screen will appear. Click **OK** to continue.

Users	
Attention	
You are about to remove a This will cause the removal of the user's home directory and all its contents.	
Press OK to confirm.	
✓ <u>OK</u> X Cancel	



User Guide

# 15.6.4 Groups—Adding a New Group

To add a new group, click the **New Group** link.

Users						
Users						
Full Name	User Name	F	Permissions	Action		
Administrator	admin	Web-based Manage	ement Access	<u> </u>		
New User						
Name         Description         Members         Action           Users         \sqrt{2}         \sqrt{2}         \sqrt{2}						
New Group						
← <u>Close</u>						

If you click the **New Group**, the following screen will appear. Using this screen, you can configure additional groups in the Router. At this screen, do the following:

- 1. Enter a Group Name of your choice.
- 2. Enter a description of your choice.
- 3. If you want to assign administrative permissions to the group, click the **Group Members Administrator** check box; otherwise, leave this box empty.
- 4. Click **OK** to save the settings.

	Group Settings	
Name: Description:	Group	
Group Members		
	✓ <u>OK</u> Cancel	



User Guide

After you have entered the desired values and clicked **OK**, the following screen will display the group attributes. Click **Close** to return to the **Advanced** screen.

Users					
Users Full Name User Name Permissions Action					
		Web-based Manage	ement Access	<u> </u>	
New User					-
Groups					
Name         Description         Members         Action           Users         Image: Comparison of the second s					
Group Home Group			ıp		<b>\X</b>
New Group					4
Close					



User Guide

## 15.6.5 Groups—Add a User to a Group

To set up new users for a group, click the **User** link in the **Groups** section of the screen. The following screen will appear. Using this screen, you can assign users to a designated group.

At this screen, do the following:

- 1. Enter a User name of your choice.
- 2. Enter a description of your choice.
- 3. If you want to assign administrative permissions to the user, click the **Group Members Administrator** check box; otherwise, leave this box empty.
- 4. Click **OK** to save the settings.

	Group Settings					
Name:	Users					
Description:	User 1					
Group Members						

After you have entered the desired values and clicked **OK**, the following screen will display the group attributes. Click **Close** to return to the **Advanced** screen.

Users		-				
Full Name	User Name	-	Permissions	Action		
Administrator	admin	Web-based Manage	ement Access	<u>\</u>		
New User						
Groups Name Description Members Action						
Users User 1						
Group	Home Gro	up		A 🗱		
New Group 🔶						
Close						



User Guide

## 15.7 Quality of Service

The QoS feature allows you to configure Quality of Service parameters in your Router. Network-based applications and traffic are growing at a high rate, producing an ever-increasing demand for bandwidth and network capacity. Bandwidth and capacity cannot be expanded infinitely, requiring that bandwidth-demanding services be delivered over existing infrastructure, without incurring additional expensive investments. The next logical means of ensuring optimal use of existing resources are Quality of Service (QoS) mechanisms for congestion management and avoidance. Quality of Service refers to the capability of a network device to provide better service to selected network traffic. This is achieved by shaping the traffic and processing higher priority traffic before lower priority traffic.

### 15.7.1 General

If you click the **Quality of Service** link in the **Advanced** screen, the following screen appears. This screen allows you to configure general QoS settings. Enter the appropriate settings, and then click **Apply**.

NOTE: Choosing a new QoS profile will cause all previous QoS settings to be lost.

Before selecting the QoS profile that mostly suits your needs, select your bandwidth from this combo-box. If you do not see an appropriate entry, select 'User Defined', and enter your Tx and Rx bandwidths manually.

- Enter your Tx bandwidth in Kbits per second.
- Enter your Rx bandwidth in Kbits per second.

Select the profile that mostly suits your bandwidth usage. Each profile entry displays a quote describing what the profile is best used for, and the QoS priority levels granted to each bandwidth consumer in this profile.

- Default No QoS preferences
- P2P User Peer-to-peer and file sharing applications will receive priority
- Triple Play User VoIP and video streaming will receive priority
- Home Worker VPN and browsing will receive priority
- Gamer Game-related traffic will receive priority
- Priority By Host This entry provides the option to configure which computer in your LAN will receive the highest priority and which the lowest. If you have additional computers, they will receive medium priority.

**High Priority Host:** Enter the host name or IP address of the computer to which you would like to grant the highest bandwidth priority.

**Low Priority Host:** Enter the host name or IP address of the computer to which you would like to grant the lowest bandwidth priority.



Verizon FiOS Router (Model 9100EM)

Ugan	Cuida
User	Guide

Ger	neral
WAN Devices Bandwidth (Rx/Tx):	User Defined
Rx Bandwidth:	0 Kbits/s
Tx Bandwidth:	0 Kbits/s
QoS Profiles ⊛ Default	
No Quality of Service preferences	
O P2P User	
"I use peer-to-peer and file-sharing applicat browser without interference."	ions. I still want to be able to use my
HTTP/HTTPS: <b>Medium</b> Other: <b>Low</b>	
🔿 Triple Play User	
"I use VoIP applications and video streaming possible."	g. I want these applications to be as fast as
VoIP (SIP, H323): <b>High</b> Video: <b>High-Medium</b> HTTP/HTTPS: <b>Medium</b> Other: <b>Low</b>	
○ Home Worker	
"I work from home, and want my VPN and b	prowser to have priority over other traffic."
VPN (IPsec, L2TP, PPTP): <b>Medium</b> HTTP/HTTPS: <b>Medium</b> Other: <b>Low</b>	
🔘 Gamer	
"I play games over the Internet and want th possible."	e games-related traffic to be as fast as
Games Related Traffic: <b>Medium</b> Other: <b>Low</b>	
O Priority By Host	
"I want to give different hosts in my network public network,"	c different priorities when accessing the
High Priority Host:	
Low Priority Host:	
Other: Low	
Note: Choosing a new QoS profile will cause a	Il previous configuration settings to be lost



User Guide

## **15.7.2 Traffic Priority**

If you click the **Quality of Service** link in the **Advanced** screen and then click **Traffic Priority** in the left submenu, the following screen will appear. This screen allows you to configure QoS to prioritize input and output traffic.

Traffic Priority manages and avoids traffic congestion by defining inbound and outbound priority rules for each device on the Router. These rules determine the priority that packets, traveling through the device, will receive. QoS parameters (DSCP marking and packet priority) are set per packet, on an application basis.

QoS can be configured using flexible rules, according to the following parameters:

- Source/destination IP address, MAC address, or host name
- Device
- Source/destination ports
- Limit the rule for specific days and hours

The Router supports two priority marking methods for packet prioritization:

- DSCP
- 802.1p Priority

The matching of packets by rules, also known as Stateful Packet Inspection is connection-based and uses the Router's firewall mechanism. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound.

A packet can match more than one rule. Therefore:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

To set up a traffic priority rule, click the adjacent New Entry link for the input/output device you want to configure.

		Traffic Priority			
QoS Input Rules					
	estination Address	Protocols	Operation	Status	Action
All Devices					New Entry
Network (Home/Office) Rule	s				New Entry
Ethernet Switch Rules					New Entry
<b>Broadband Connection (Ethe</b>	ernet) Rules				New Entry
Wireless 802.11g Access Poi	int Rules				New Entry
WAN PPPoE Rules					New Entry
QoS Output Rules	estination				
Rule ID Source Address	Address	Protocols	Operation	Status	Action
All Devices					New Entry
Network (Home/Office) Rule	s				New Entry
Ethernet Switch Rules					New Entry
<b>Broadband Connection (Ethe</b>	ernet) Rules				New Entry
Wireless 802.11g Access Poi	int Rules				New Entry
WAN PPPoE Rules					New Entry
<ul> <li>✓ <u>ок</u></li> </ul>	) ( <u> </u>	pply X Cancel R	tesolve Now	<u>Refresh</u>	



User Guide

If you clicked New Entry, the following screen will appear. At this screen, do the following:

- 1. Select the desired Source Address, Destination Address, and Protocol options from the drop-down lists.
- 2. Click the **Device** check box if you will apply the settings to a device. By default this box is cleared.
- 3. Select the desired option from the Set Priority drop-down list. (Zero is the lowest priority level.)
- 4. Click **OK** to save the settings.

Source Address—The source address of packets sent or received from the LAN computer. The drop-down list displays all the host names or IP addresses of currently connected LAN computers, as well as the options 'Any' and 'User Defined'. Select an address from the list, or select **Any** to apply the rule on all computers. If you would like add a new address, select the **User Defined** option in the drop-down list. This will commence a sequence that will add a new network object, representing the LAN computer. The network object may be an IP address, subnet or range, a MAC address or a host name.

Destination Address—The destination address of packets sent or received from the network object. This address can be configured in the same manner as the source address. This entry enables further filtration of the packets.

Protocols—You may also specify a traffic protocol. Selecting the **Show All Services** option in the drop-down list will expand the list of available protocols. Select a protocol or add a new one using the **User Defined** option. This will commence a sequence that will add a new service, representing the protocol.

Operation—Set rule priority with Quality of Service:

Set Priority—Check this check-box to add a priority to the rule then select between one of eight priority levels, zero being the lowest and seven the highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.

The order of the rules' appearance represents both the order in which they were defined and the sequence by which they will be applied. You may change this order after your rules are already defined (without having to delete and then re-add them), by using the Move Up and Move Down action icons as shown in the following image.

<u>0</u>	Any	192.168.1.50	FTP - TCP Any -> 21	Priority 7 - High No Connection	Active	*>*
<b>1</b>	Any	192.168.1.50	FTP - TCP Any -> 21	Priority 0 - Low No Connection	Active	<u> </u>



User Guide

## 15.7.3 Traffic Shaping

If you click the **Quality of Service** link in the **Advanced** screen and then click **Traffic Shaping** in the left submenu, the following screen will appear.

Traffic Shaping is the solution for managing and avoiding congestion where the network meets limited broadband bandwidth. Typical networks use a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. This is where most bottlenecks occur. A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic. While traffic priority allows basic prioritization of packets, traffic shaping provides more sophisticated definitions, such as:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

Additionally, QoS traffic shaping rules can be defined for a default device. These rules will be used on a device that has no definitions of its own. This enables the definition of QoS rules on the default WAN, for example, and their maintenance even if the PPP or bridge device over the WAN is removed.

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the Router's firewall mechanism. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound. Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, QoS rules can be defined on SIP, and the rules will apply to both control and data ports (even if the data ports are unknown). Applications that support such inheritance have an application-level gateway (ALG) in the firewall.

To add a traffic shaping rule, click the New Entry link.



User Guide

If you clicked **New Entry**, the following screen will appear. Select a device from the **Device** drop-down list. Then, click **OK** to continue.

	Add Device Traffic Shaping
Device:	Default WAN device
	✓ <u>OK</u> Cancel

After you have selected a device and clicked **OK** in the preceding screen, the following screen will appear. Enter the bandwidth values for transmit (Tx) and receive (Rx), and then select the desired option from the TCP Serialization drop-down list. Next, click the desired **New Entry** link to add a class.

Main	Wireless	My Network	Fire	wall Settings	Parental	<u>~</u>	Advanced	System Monitoring
Main				Edit Dev	vice Traffic	Shaping		
Edit Device Traffic Shaping Logout		Device: Tx Traffic Shapi Tx Bandwidth: TCP Serializatio			Defaul 97656 Disable	t WAN device Kbits/s d 🖬		
		Class ID	Name	Priority	Bandwi Reserved	dth (Kbits/s) Maximum	Status	Action
		<u>New Entry</u> Rx Traffic Polici Rx Bandwidth:			97656 Bandwidth (K	Kbits/s		*
		Class ID <u>New Entry</u>	Name		erved	Maximum	Status	Action
			C		ι <u>Αρρίγ</u>	X Cancel	)	

#### **Tx Traffic Shaping**

The bandwidth of a device can be divided in order to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a Shaping Class. When not used by its predefined traffic type, or owner (for example VoIP), the class will be available to all other traffic. However when needed, the entire class is reserved solely for its owner. Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available. Configure the following fields:

#### Tx Bandwidth

This parameter limits the gateway's bandwidth transmission rate. The purpose is to limit the bandwidth of the WAN device to that of the weakest outbound link, for instance, the DSL speed provided by the ISP. This forces the router to be the network bottleneck, where sophisticated QoS prioritization can be performed. If the device's bandwidth is not limited correctly, the bottleneck will be in an unknown router or modem on the network path, rendering this router's QoS useless.



User Guide

#### **TCP Serialization**

You can enable TCP Serialization in its combo box, either for active voice calls only or for all traffic. The screen will refresh, adding a 'Maximum Delay' field. This function allows you to define the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer time to be transmitted, will be fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP. If you insert a delay value in milliseconds, the delay in number of bytes will be automatically updated on refresh.

Tx Traffic Shap Tx Bandwidth:	ing		97656	Kbits/s		
TCP Serialization: Maximum Delay:			Enabled [ 60	ms (7500026 l	oytes)	
			Bandwidt	n (Kbits/s)	Status	Action
Class ID	Name	Priority	Reserved	Maximum	Status	Action
New Entry						-

For example, if you click the New Entry link in the **Tx Traffic Shaping** section of the **Edit Device Traffic Shaping** screen the **Add Shaping Class** screen will appear.

Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Add §	Shaping Class		
Add Class		Name:	Class	]		
Logout				Cancel		

Name the new class and click **OK** to save the settings, e.g., Class A. Now click the class name to edit the shaping class or alternatively, click its pencil (edit) icon in the Action column.

Class ID	Name	Deigeitu	Bandwid	th (Kbits/s)	Status	Action
	Name	Priority	Reserved	Maximum	Status	ACCION
<u>o</u>	Class A	0	0	Unlimited	Active	1 2
New Entry						4



User Guide

If you clicked the edit icon in the preceding screen, the Edit Shaping Class screen will appear.

Name: Class Priority: Bandwidth:	Class A 0 (Highest) Reserved 0 Maximum Unlimited Kbits/s
Policy: Schedule	Priority Always

Configure the following fields by entering or selecting the desired values:

Name—The name of the class.

Class Priority—The class can be granted one of eight priority levels, zero being the highest and seven the lowest (note the obversion when compared to the rules priority levels). This level sets the priority of a class in comparison to other classes on the device.

Bandwidth—The reserved transmission bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting **Specify** in the drop-down list. The screen will refresh, adding yet another Kbits/s.

Policy—The class policy determines the policy of routing packets inside the class. Select one of the four options:

Priority—Priority queuing utilizes multiple queues, so that traffic is distributed among queues based on priority. This priority is defined according to packet's priority, which can be defined explicitly, by a DSCP value, or by a 802.1p value.

FIFO—The "First In, First Out" priority queue. This queue ignores any previously-marked priority that packets may have.

Fairness—The fairness algorithm ensures no starvation by granting all packets a certain level of priority.

RED— The Random Early Detection algorithm utilizes statistical methods to drop packets in a "probabilistic" way before queues overflow. Dropping packets in this way slows a source down enough to keep the queue steady and reduces the number of packets that would be lost when a queue overflows and a host is transmitting at a high rate.

Schedule—By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. Refer to section 15.19, "Scheduler Rule," for details on setting up schedule rules.

**Rx Traffic Policing:** Allows you to configure the following fields:

Rx Bandwidth This parameter specifies the maximum traffic the policing can receive from the ISP.

Rx Traffic Policing Rx Bandwidth:		97	656 Kbits/s		
Class TD	blanca	Bandwidt	h (Kbits/s)	Status	
Class ID	Name	Reserved	Maximum	Status	Action
New Entry					4



User Guide

For example, if you click the **New Entry** link in the **Rx Traffic Policing** section of the **Edit Device Traffic Shaping** screen, the **Add Policing Class** screen will appear.

	Add Policing Class	
Name:	Class B	
	✓ OK X Cancel	

Name the new class and click **OK** to save the settings, e.g. Class B. Next, click the class name to edit the shaping class or alternatively, click its pencil (edit) action icon in the Action column.

Class ID	blasse	Bandwid	Chatura	Action	
Class ID	Name	Reserved	Maximum	Status	Action
<u>0</u>	Class B	0	Unlimited	Active	1 🕺 🎗
New Entry					4

The Edit Policing Class screen will appear.

		Edit P	Policing Class				
В	Name: Bandwidth: Schedule	Class B Reserved 0 Always	Maximum Unlimited 💽 Kbits/s				
	✓ <u>OK</u> <u>X Cancel</u> <u>Resolve Now</u> <u>Refresh</u>						

Configure the following fields:

Name—The name of the class.

Bandwidth—The reserved reception bandwidth in kilo-bits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option in the combo box. The screen will refresh, adding yet another Kbits/s field.

Schedule—By default, the class will always be active. However, you can configure scheduler rules in order to define time segments during which the class may be active. Refer to section 15.19, "Scheduler Rule," for details on setting up schedule rules.



User Guide

### 15.7.4 Differentiated Service Code Point (DSCP) Settings

If you click the **Quality of Service** link in the **Advanced** screen and then click **DSCP Settings** in the left submenu, the following screen will appear.

Familiarity with the Differentiated Services model is essential to understanding DSCP. Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements, and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback, or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

Diffserv defines a field in IP packet headers referred to as the Differentiated Services Codepoint (DSCP). Hosts or routers passing traffic to a Diffserv-enabled network will typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply a particular queue handling or scheduling behavior to packets.

The Router provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method. Any of the existing DSCP setting can be edited or deleted, and new entries can be added. To add a new DSCP value, press the **New Entry** link at the bottom of this screen.

DSCP Value (hex)	802.1p Priority	Action
0x20	4 - Medium	- 🔨 🗱
0x21	4 - Medium	- 🔪 🗱
0x22	4 - Medium	- 🔨 🗱
0x23	4 - Medium	- 🔪 🎇
0x24	4 - Medium	- A 🗱
0x25	4 - Medium	N 🗱
0x26	4 - Medium	<b>\</b>
0x27	4 - Medium	A 🗱
0x28	5 - Medium	<b>N</b>
0x29	5 - Medium	<u>\</u>
0x2A	5 - Medium	<u>\</u>
0x2B	5 - Medium	<u>\</u>
0x2C	5 - Medium	× *
0x2D	5 - Medium	<u> </u>
0x2E	5 - Medium	
0x2F	5 - Medium	1
0x30	6 - High	
0x31	6 - High	1
0x32	6 - High	
0x33	6 - High	
0x34	6 - High	
0x35	6 - High	
0x36	6 - High	
0x37	6 - High	
0x37	7 - High	
0x39	7 - High	1
0x39	7 - High	
0x3A 0x3B	7 - High	
0x3C	7 - High	
0x3C	7 - High	
		1
0x3E 0x3F	7 - High	
	7 - High	
New Entry		



User Guide

If you clicked **New Entry**, the following screen will appear. Enter your hexadecimal value, and then set the priority for this value. Click **Apply** to continue.

Add DSCP Setting				
DSCP Value (hex): 802.1p Priority:	0 - Low 💙			

If you clicked **Apply**, the following screen will appear. Click **OK** to confirm. Value will be added to the **DSCP Settings** screen.

	Add DSCP Setting	
Browser Reload:	Attention Wireless Broadband Router Management Console might require reloading.	
	Press <b>OK</b> to confirm.	
	✓ <u>OK</u> Cancel	



User Guide

### 15.7.5 802.1P Settings

If you click the **Quality of Service** link in the **Advanced** screen and then click **802.1P Settings** in the left submenu, the following screen will appear.

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sublayer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established.

The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority. By default, the highest priority is seven, which might be assigned to network-critical traffic. Values five and six may be applied to delay-sensitive applications such as interactive video and voice. Data classes four through one range from controlled-load applications down to "loss eligible" traffic. Zero is the value for unassigned traffic and is used as a best effort default, invoked automatically when no other value has been set.

A packet can match more than one rule. This means the following:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) will take precedence.

Select the desired values from the drop-down lists, and then click **Apply** to save the settings.

802.1p 9	Settings
802.1p Value	Priority
0	Low 🗸
1	Low 💙
2	Low 🗸
3	Low 🗸
4	Medium 🔽
5	Medium 🔽
6	High 🗸
7	High 🗸
	pply X Cancel



User Guide

### **15.7.6 Class Statistics**

If you click the **Quality of Service** link in the **Advanced** screen and then click **Class Statistics** in the left submenu, the following screen will appear.

The Router provides accurate, real-time information on the traffic moving through the defined device classes. For example, the amount of packets sent, dropped, or delayed are just a few of the parameters monitored per each shaping class.

**NOTE:** Class statistics will be available only after defining at least one class (otherwise the screen will not display any values).

If you do not want the screen to refresh automatically, click Automatic Refresh Off.

Class Statistics						
Class	Packets Sent	Bytes Sent	Packets Dropped	Packets Delayed	Rate (bytes/s)	Packet Rate
Ethernet Switch						
Wireless 802.11g Access Point						
Class Statistics         Class       Packets Sent       Packets Dropped       Packets Delayed       Rate (bytes/s)       Packet Rate         Ethernet Switch Wireless 802.11g Access Point       Automatic Refresh On       Close       Automatic Refresh On       Close						



User Guide

### **15.8 Remote Administration**

If you click **Advanced** in the top navigation menu and then select the **Remote Administration** link, the following screen will appear.

It is possible to access and control your Router not only from within the home network, but also from the Internet. This allows you to view or change settings while traveling. It also enables you to allow Verizon to change settings or help you troubleshoot functionality or communication issues from a remote location. Remote access to your Router is blocked by default to ensure the security of your network. However, your Router supports the following services, and you may use the Remote Administration Security screen to selectively enable these services if they are needed.

#### WARNING: With Remote Administration enabled, your network will be at risk from outside attacks.

To configure Remote Administration, enter the appropriate settings, and then click **Apply** to save the settings.

**NOTE:** This Router ships with Telnet disabled.

Remote Administration	
Allowing remote administration to Wireless Broadband Router is a security risk.	
Allow Incoming WAN Access to the Telnet Server X Using Primary Telnet Port (23) X Using Secondary Telnet Port (8023) X Using Secure Telnet over SSL Port (992) Allow Incoming WAN Access to Web-Management Using Primary HTTP Port (80) Using Secondary HTTP Port (8080) Using Primary HTTPS Port (443) Using Secondary HTTPS Port (8443)	
<ul> <li>✓ OK</li> <li>✓ Cancel</li> </ul>	



User Guide

### 15.9 DNS

If you click Advanced in the top navigation menu and then select the DNS link, the following screen will appear.

The Router contains a built-in DNS server. When an IP address is assigned, the Router will interrogate the new device for a machine name using several well-known networking protocols. Any names learned will dynamically be added to the DNS server's table of local hosts.

Do any of the following:

- To rename the domain name, click a host name link.
- To add a host name, click the **New DNS Entry** link.

To add a new entry, click the **New DNS Entry** link. The following screen will appear. Enter the desired host name, and then enter the appropriate IP address. Next, click **OK** to continue.

**NOTE:** Names may not contain spaces. Only letters, digits and the special characters dash (-), underscore (\_) and dot (.) may be used. These special characters may not appear at the beginning or at the end of a name. The maximum length of a name can be is 63 characters.

	DNS Entry
Host Name: IP Address:	new-host-2 0 . 0 . 0 . 0
	✓ <u>OK</u> X Cancel



User Guide

If you have entered values in the preceding screen and clicked **OK**, the following screen will appear. The changes have been saved to the Router.

## 15.10 Personal Domain (Dynamic DNS)

If you click **Advanced** in the top navigation menu and then select the **Personal Domain Name** link, the following screen will appear.

Dynamic DNS (Domain Name Server) a dynamic IP address to be aliased to a static hostname, allowing a computer on the network to be more easily accessible from the Internet. Typically, when connecting to the Internet, the service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, while maintaining a constant domain name. This allows to user to access a device from a remote location, since the device will always have the same IP address.

When using Dynamic DNS, each time the IP address provided by the service provider changes, the DNS database changes accordingly to reflect the change. If the IP address of the computer changes often, its domain name remains constant and accessible.

NOTE: To use Dynamic DNS, you must subscribe to this service via your service provider.

To configure a new dynamic DNS entry, click the New Dynamic DNS Entry link.

Personal Dor	nain Nam	e (Dynamic	DNS)	
Host Name	Status	Provider	User Name	Action
New Dynamic DNS Entry				-
Press the <b>Refr</b>	esh button t	o update the sta	itus.	
( + <u>c</u>	lose	C Refresh		



User Guide

The following screen will appear. Enter the appropriate values in the fields provided, and then click **OK** to continue.

NOTE: Your service provider will provide you with the appropriate values to use in this screen.

Personal Domain	Name (Dynamic DNS)
Enable	
Host Name:	
Connection:	WAN PPPoE 💌
Provider:	dyndns.org 💙
Click Here to Initiate and Manage your Subscrip	btion
User Name:	
Password:	
Wildcard	
Mail Exchanger:	
Backup MX	
offline 🗌	
SSL Mode:	None 💌
₹ <u>ok</u>	TApply X Cancel

If you click the **Click Here to Initiate and Manage your Subscription** link, the following screen will appear. Enter the user name and password (provided by your service provider) in the fields provided to access your account.

NOTE: The screen displayed in this document may differ from the actual screen.

🔿 Dyn	DNS Users Pass: Login
	About Services Account Support News
My Account	Login
Create Account	A securit Logia
Login	Account Login Username: Password: Login
Lost Password?	
Search Search	Don't have an account? <u>Create one now</u> - it's free!
	© 1996-2008 Dynamic Network Sarvices, Inc Legal Notices - Contacts



User Guide

### 15.11 Network Objects

Network Objects is a method used to abstractly define a set of LAN hosts, according to one or more MAC address, IP address, and host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring the Router's security filtering settings such as IP address filtering, host name filtering or MAC address filtering. You can use network objects in order to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. Moreover, it is possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings.

If you click **Advanced** in the top navigation menu and then select the **Network Objects** link, the following screen will appear. To configure a new network object, click the **New Entry** link.

	Network Ob	ojects		
A Network Object	is a set of host names, IP addresses or MAC addre using Network C		can be applied to a	distinct LAN subset
	Network Object	Items	Action	
	New Entry			
	Close			

If you clicked **New Entry** in the preceding screen, the following screen will appear. Enter a name for the network object in the **Network Object Description** field, and then click the **New Entry** link or the plus icon to create it.



User Guide

If you clicked **New Entry**, the following screen will appear. The source address can be entered using one of the following methods listed in the **IP Address** drop-down menu:

- IP Address
- IP Subnet
- IP Range
- MAC Address
- Host Name
- DHCP Option

After you select the desired method, the screen will refresh. Enter the appropriate values in the fields provided, and then click **OK** to save the settings.

Ac	ld Item
Network Object Type:	IP Address
IP Address: ✓ <u>OK</u>	IP Address     0     0       IP Subnet     IP Range     0       MAC Address     Host Name       DHCP Option

If you have entered the desired values in the preceding screen and clicked **OK**, the following screen will appear. The network object has been configured. Click **OK** to save the configuration.

	Add Network Object	
Network Object Description:	Global Object	
Items Ite		ion
<u>192.16.1.4</u> New Entry	4	<b>26</b>
(	✓ <u>OK</u> X <u>Cancel</u>	



User Guide

If you clicked **OK**, the following screen will appear. The network object has been saved to the Router. Click **Close** to return to the **Advanced** screen.

veriz	on					
Main	Wireless I	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Network Objects Logout	A Network Object	t is a set of host r	names, IP addresses or N	York Objects NAC addresses. Security N Network Objects.	rules can be applied to	a distinct LAN subset
		Ne Global Object	twork Object	Items 192.168.1.4	Action	
		New Entry			-	
			0	₽ <u>Close</u>		



User Guide

### 15.12 Protocol

If you click **Advanced** in the top navigation menu and then select the **Protocol** link, the following screen will appear. For your convenience, the Router supports protocols for Applications, Games, and VPN-specific programs. The following chart provides port/protocol information for the supported services. The Protocol screen allows you to select the desired view: Basic Service and Advanced Service. The following sections explain the features of each service.

Protocols	Ports	Action
FTP	TCPAny -> 21	
HTTP	TCPAny -> 80	
HTTPS	TCPAny -> 443	🔨 🎇
IMAP	TCPAny -> 143	🔨 🗶
L2TP	UDPAny -> 1701	🔨 🗶 👗
Ping	ICMPEcho Request	A 🗶
POP3	TCPAny -> 110	A 🗶
SMTP	TCPAny -> 25	A 🗶
SNMP	UDPAny -> 161	A 🗶
Telnet	TCPAny -> 23	🔨 🎇
TFTP	UDP1024-65535 -> 69	A 🗶
Traceroute	UDP32769-65535 -> 33434-33523	🔨 🗶
New Entry		
	Advanced >>	



User Guide

## 15.12.1 Basic Service

To access the basic service Protocols screen (if you are in the Advanced screen), click the Basic button.

Protocols	Ports	Action
	Any -> 7000-10000	5.00
Alien vs. Predator	Any -> 2300-4000 Any -> 7000-10000	2 🗱
	Perts           TCAH 2003-4000           DDPAH 2003-4000           DATA - 2003-4000           AAH - 7003-1000           AAH - 7003-1000           AAH - 7003-1000           AAH - 7003-1000           AAH - 7044-7649           AAH - 7448-7649           UDPAH - 22032           AH - 75003           AH - 75034           AH - 75035	
	Any -> 7640	
	Any -> 7642 Any -> 7648-7649	
CuSeeMe	UDPAny -> 24032	N 🗱
	Any -> 1424	
	Any -> 1812-1813 Any -> 7648	
Dark Reign	Any -> 56800	× #
Dark Reign 2	TCPAny -> 26214	1 2
Dark Reigh 2	UDPAny -> 26214	
Decent 3	UDPAny -> 2092	🔨 🗱 🕹
	Any -> 3445 TCPAny -> 3999	
	UDPAny -> 4000	<b>X #</b>
Decent Freespace	Any -> 7000 Any -> 3493	~ ~
	Any -> 3440 TCPAny -> 3100-3999	1.00
Delta Force	UDPAny -> 3568	N 28
DHCP ALG	UDP67-68 -> 67	N 🗱
Diablo, StarCraft(Battle.net)	UDP67-88 -> 67 TCPAny -> 6112 Any -> 116-118 UDPAny -> 6122 TCPAny -> 47624-3765 Any -> 47624-3765 Any -> 47624-3765 Any -> 47624-47625 Any -> 47624-47625 Any -> 300-2400 UDPAny -> 53 TCPAny -> 31	🔨 🗱 👘
	UDPAny -> 6112 TCPAny -> 47624-47625	
DirectX Games	Any -> 2300-2400	× #
pirectA-Games	UDPAny -> 28800-28912 UDPAny -> 47624-47625	~ *
DNS ALG	Any -> 2300-2400	<b>N W</b>
DNS ALG FTP	TCPAny -> 21	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
H.323 Call Signaling	TCPAny -> 21 TCPAny -> 1720 Any -> 1503 TCPAny -> 8000-8999 UDPAny -> 1388 Any -> 5500-5600 Any -> 8000-9000	<b>N</b>
more can biglianing	Any -> 1503	~ ~
Heat.net	UDPAny -> 1398	× 🗱
	Any -> 5500-5600 Any -> 8000-9000	
HTTP	TCPAny -> 80	\_\$\$ \_\$\$
HTTP Secondary	TCRAny -> 8080	A 🗱
	TCPAny -> 3127-3128 Any -> 80-81 Any -> 8080 Any -> 8080 Any -> 8888	
HTTP Web Access	Any -> 8080 Any -> 8000	🔨 🗱
	Any -> 8888	
HTTPS	TCPAny -> 443	N 28
HTTPS Secondary	TCPAny -> 8443	
ICQ IMAP	UDPAny -> 4000 TCPAny -> 143	
	UDP500 -> 500	
IPSec	UDP500 -> 500 ESP AH	🔨 🗱
L2TP	UDPAny -> 1701	\
MGCP ALG	UDPAny -> 2727	1
Microsoft Direct Play	UDPAny -> 1000-4999	🔨 🗱
	TCPAny -> 139	
Microsoft Windows Network / Samba	Any -> 445	🔨 🗱
	UDPAny -> 2727 UDPAny -> 1000-4999 Any -> 40000-60000 TCPAny -> 139 Any -> 445 UDPAny -> 137 Any -> 138 TCPAny -> 137 Any -> 138	5.00
MSN Messenger	TCPANY -> 1003	N 28
Myth Need for Speed 5 (Porsche)	TCPAny -> 3453 UDPAny -> 9395-9405	
Ping	ICMPEcho Request	1
	TCPAny -> 10070-10080 UDPAny -> 10070	
Play-Station2	UDPAny -> 10070	
POP3	TCPAny -> 110 TCPAny -> 1723	N 28
PPTP	GRE	- 🔨 🗱
OuakeII	GRE TCPAny -> 27910 UDPAny -> 27910 TCPAny -> 2760-27670 UDPAny -> 27660-27670 TCPAny -> 2346	🔨 🗱
QuakeIII	TCPAny -> 27660-27670	N 28
Rainbow Six	UDPAny -> 27660-27670 TCPAny -> 2346	1 2
Red Alert		1 34 1 34
	TCPAny -> 554	~
	Any -> 7070 Any -> 5005	
RTSP	UDPAny -> 554	2.8
	Any -> 7070 Any -> 5005	
SIP	UDPAny -> 5009 TCPAny -> 554 Any -> 7070 Any -> 5005 UDPAny -> 554 Any -> 7070 Any -> 7070 Any -> 5005 UDPAny -> 5060	- N 🗱
SMTP	TCPAny -> 25	
SNMP	UDPAny -> 161	N 28
SSH	TCPAny -> 22	28
Teinet	TCPAny -> 23 UDP1024-65535 -> 69	2.2
TFTP	TCPAny -> 4000	~ ~
Tiberian Sun	Any -> 1140-1234	🔨 🗱
	CPAny -> 4000 Any -> 140-1234 UDPAny -> 1140-1234 TCPAny -> 100-4999 UDPAny -> 47624 Any -> 100-4999	
Total Annihilation	UDPAny -> 47624 Any -> 1000-4999	A 🗱
Traceroute	UDP32/09-05535 -> 33434-35523	
Unreal - Master Server List		- 🔨 🗱
Unreal, Unreal Tournament	UDPAny -> 7777-7779 Any -> 27900	🔨 🗱
Vonage VoIP Phone Service	TCPAny -> 5060-5070	N 28
	UDPAny -> 27900 UDPAny -> 2777-7779 Any -> 27900 TCPAny -> 5606-5070 Any -> 10000-25000 TCPAny -> 1031-2210 Any -> 2220-3212 UDPAny -> 3074 UDPAny -> 3074	
Worms 2	Any -> 2220-3212	🔨 🗱
	TCPAny -> 3074	
<u>XBoX</u>	UDPAny -> 88 Any -> 3074	N 🗱
0000		
New Entry	, any court	-



User Guide

If you clicked the **Basic** button in the preceding screen, the following screen will appear.

At this screen, you can:

- Configure ports for predefined protocols by clicking the desired link.
- Configure a new user-defined port for a protocol by clicking the New Entry link.

Protocols	Ports	Action
FTP	TCPAny -> 21	A 🗶
HTTP	TCPAny -> 80	🔨 🎉
HTTPS	TCPAny -> 443	🔨 🎉
IMAP	TCPAny -> 143	🔨 🎉
L2TP	UDPAny -> 1701	🔨 🎉
Ping	ICMPEcho Request	🔨 🎉
POP3	TCPAny -> 110	🔨 🎉
SMTP	TCPAny -> 25	🔨 🎉
SNMP	UDPAny -> 161	🔨 🎉
Telnet	TCPAny -> 23	🔨 🎉
TFTP	UDP1024-65535 -> 69	🔨 🎉
Traceroute	UDP32769-65535 -> 33434-33523	🔨 🎉
New Entry		

#### 15.12.1.1 Configuring a Predefined Protocol Service

To configure the Router for a predefined protocol service, click the desired link.

Protocols	Ports	Action
FTP	TCPAny -> 21	S 🖇 🧷
HTTP	TCPAny -> 80	🔨 🎉
HTTPS	TCPAny -> 443	🔨 🎉
IMAP	TCPAny -> 143	🔨 🗶
L2TP	UDPAny -> 1701	🔨 🎇
Ping	ICMPEcho Request	🔨 🎇
POP3	TCPAny -> 110	🔨 🎇
SMTP	TCPAny -> 25	🔨 🎇
SNMP	UDPAny -> 161	🔨 🎇
Telnet	TCPAny -> 23	A 🗶
TFTP	UDP1024-65535 -> 69	🔍 🗶
Traceroute	UDP32769-65535 -> 33434-33523	🔨 🎇
New Entry		



User Guide

For example, if you clicked **FTP** in the preceding screen, the following screen will appear. Next, click the **TCP** link to configure the service protocol values.

Service Name:	FTP	
Service Description:	File Transfer	
Server Ports		
Protocols	Server Ports	Action
TCP	Any -> 21	🔨 🗶
New Server Ports		+
	✓ <u>OK</u> ✓ <u>Cancel</u>	

If you clicked **TCP** in the **Edit Service** screen, the following screen will appear. Enter the desired values, and then click **OK** to continue.

Edi	t Service Server Ports
Protocols	ТСР 💌
Source Ports:	Any 💙
Destination Ports:	Single 💙 21
	✓ <u>OK</u> X <u>Cancel</u>



User Guide

If you have entered values and clicked **OK** in the preceding screen, the following screen will appear. A protocol service has been configured. Click **OK** to save the settings.

Service Name:	FTP	
Service Description:	File Transfer	
Server Ports		
Protocols	Server Ports	Action
TCP	4 -> 21	🔨 🎇
New Server Ports		

If you clicked **OK** in the preceding screen, the following screen will appear. The protocol service has been saved to the Router.

	Protocols	
Protocols	Ports	Action
FTP	TCP4 -> 21	
HTTP	TCPAny -> 80	S 🗶 🗶
HTTPS	TCPAny -> 443	- A 🗱
IMAP	TCPAny -> 143	S 🕺 🗶
L2TP	UDPAny -> 1701	A 🗶
Ping	ICMPEcho Request	A 🗶
POP3	TCPAny -> 110	A 🗶
SMTP	TCPAny -> 25	N 🗱
SNMP	UDPAny -> 161	N 🗱
Telnet	TCPAny -> 23	A 🗶
TFTP	UDP1024-65535 -> 69	🔨 🎉
Traceroute	UDP32769-65535 -> 33434-33523	🔨 🎇
New Entry		



User Guide

#### 15.12.1.2 Configuring a User-defined Protocol Service

To configure the Router for a user-defined protocol service, click the New Entry link.

Protocols	Ports	Action
FTP	TCP4 -> 21	<b>N</b>
HTTP	TCPAny -> 80	S 🗱
HTTPS	TCPAny -> 443	🔨 🎉
IMAP	TCPAny -> 143	🔨 🎉
L2TP	UDPAny -> 1701	🔨 🎉
Ping	ICMPEcho Request	🔨 🎉
POP3	TCPAny -> 110	🔨 🎉
SMTP	TCPAny -> 25	🔨 🎉
SNMP	UDPAny -> 161	🔨 🎉
Telnet	TCPAny -> 23	🔨 🎉
TFTP	UDP1024-65535 -> 69	🔨 🎉
Traceroute	UDP32769-65535 -> 33434-33523	🔨 🎉
New Entry		

If you clicked **New Entry**, the following screen will appear. Enter a service name and service description in the fields provided. Next, click the **New Server Ports** link.

	Edit Service	
Service Name:	Global Application	
Service Description:		
Server Ports		
Protocols	Server Ports	Action
New Server Ports		
	✓ <u>OK</u> X <u>Cancel</u>	



User Guide

If you clicked **New Server Ports**, the following screen will appear. Select a protocol from the drop-down list, and then enter a protocol number. Click **OK** to continue.

If you clicked **OK**, the following screen will appear. Click **OK** to save the settings.

	Edit Service	
Service Name:	Global Application2	
Service Description:		
Server Ports		
Protocols	Server Ports	Action
UDP	87-65535 -> 88-65535	S 🗱 🕹
New Server Ports		



User Guide

If you clicked **OK**, the following screen will appear. The protocol settings have been saved to the Router.

Protocols	Ports	Action
FTP	TCP4 -> 21	A 🗱
Global Application	UDP87-65535 -> 88-65535	A 🗶
Global Application2	UDP87-65535 -> 88-65535	
HTTP	TCPAny -> 80	
HTTPS	TCPAny -> 443	🔨 🗶
IMAP	TCPAny -> 143	🔨 🗶
L2TP	UDPAny -> 1701	🔨 🗶
Ping	ICMPEcho Request	🔨 🗶
POP3	TCPAny -> 110	🔨 🗶
SMTP	TCPAny -> 25	🔨 🗶
SNMP	UDPAny -> 161	🔨 🗶
Telnet	TCPAny -> 23	🔨 🗶
TFTP	UDP1024-65535 -> 69	🔨 🗶
Traceroute	UDP32769-65535 -> 33434-33523	A 🗶
New Entry		-



User Guide

## 15.12.2 Advanced Protocol Service

To access the advanced service **Protocols** screen (if you are in the Basic screen), click the **Advanced** button. The following advanced **Protocols** screen will appear.

At the Advanced screen, you can:

- Configure predefined application by clicking the desired link.
- Configure a new user-defined application by clicking the New Entry link.

### 15.12.2.1 Configuring a Predefined Application

To configure the Router for a predefined application, click the desired link.

Any - 5 1424           Any - 5 1424           Any - 5 1424           Any - 5 5600           Dark Reina         UDPAny - 2 1154-21157           Dark Reina 2         TCPAny - 2 1214           Dark Reina 3         UDPAny - 2 1214           Dark Reina 4         TCPAny - 2 1214           Dark Reina 5         TCPAny - 2 120           Dark Reina 5         UDPANy - 2 122           Dark Reina 6         UDPANy - 2 123           Dark 9         3593           Dark 7         2 100           Dark 9         3593           Dark 9         3593           Dark 9         3586	2 34 2 34 2 34 2 34 2 34 2 34
Any > 1434         1433           Any > 7540         1434           Any > 7540         1434           Any > 7540         1134-21137           Dark Reino         UDPAny > 21134-21137           Dark Reino         1174-21137           Dark Reino         1170-21137           Dark Reino         11070-21137           Dark Reino         2010           Dark Reino <td>2 % 2 % 2 %</td>	2 % 2 % 2 %
Dark Rein 2         UDPany -> 28214           CEAR A Bin 2         UDPany -> 2170           Desent 3         UDPany -> 2170           UDPany -> 3445         UDPany -> 3445           Desent Fresence         Any -> 3450           Data From         Any -> 3450           Data Frome         UDPany -> 3100-3999           UDPany -> 3568         UDPany -> 3568	2 % 2 %
Dark Rein 2         UDPany -> 28214           CEAR A Bin 2         UDPany -> 2170           Desent 3         UDPany -> 2170           UDPany -> 3445         UDPany -> 3445           Desent Fresence         Any -> 3450           Data From         Any -> 3450           Data Frome         UDPany -> 3100-3999           UDPany -> 3568         UDPany -> 3568	2 % 2 %
Labr.sean.2 Uppary - 5 26214 Uppary - 5 26214 Uppary - 7 262 Decent 1	× #
- Any -> 3445 	
Any -> 3440           Delta Force         TCPAny -> 3100-3999           DHCP ALG         UDPAny -> 3568	<b>× </b> #
UDPAny -> 3568 DHCP ALG UDP67-68 -> 67	× #
DHCP ALG UDP67-68 -> 67	3.
Diablo, StarCraft(Battle.net) TCPAny -> 6112 Any -> 116-118	<u>\</u> *
Distle., Star-Craft(Battis.net)         UPP Any - 5 013           UPP Any - 5 013         UPP Any - 5 013           UPP Any - 5 014         UPP Any - 5 014           UPP Any - 5 015         UPP Any - 5 015           Directic Games         UPP Any - 5 0000-00012           Directic Games         UPP Any - 5 2000-200012           Directic Games         UPP Any - 5 3	× 38
DNS ALG UDPAny -> 53	1 2
TCP4 -> 21	32
H.323 Call Signaling TCPAny -> 1720 Any -> 1503	1 28
TCPAny -> 8000-8999	× *
HTTP TCPAny -> 80	S 28
TCPANy ->         3127-3128           Any ->         302-31           HTTP Web Access         Any ->           Any ->         8080           Any ->         8080           Any ->         8080	<b>S</b> 34
	1 🗱
CQ UDPAny -> 4000	38
ICPANy -> 143	2 🗱
	× #
2TP UDPAny -> 1701	<u>&gt;</u> #
MGCP ALG UDPAny -> 2727	14
TCPAny -> 139	× #
Microsoft Windows Network / Samba UDPAny -> 445 UDPAny -> 137 Any -> 138	× #
MSN Messenger         TCPAny -> 1863           Myth         TCPAny -> 3453	
Need for Speed 5 (Porsche) UDPAny -> 3453	28
Ping ICMPEcho Request	2.2
Play-Station2 TCPAny -> 10070-10080	1.
UDPAny -> 10070	3.2
POP3 TCPAny -> 110	<u>~ #</u>
PPTP TCPAny -> 1723 GRE	× #
Trans         ICMPErion Request           Haw:Tation2         UDPAny: > 10000           DDD2         TCPAny: > 10070           DD2         TCPAny: > 10070           DD2         TCPAny: > 10070           DD2         TCPAny: > 10070           DD2         TCPAny: > 1723           Dunkoll         TCPAny: > 27800           Dankoll         UCPAny: > 27800           Balabox.Siz         TCPAny: > 23660	× ¥
Ouskelli TCPAny -> 27660-27670	S 38
UDPAny -> 27660-27670 Rainbow Six TCPAny -> 2346	N 00
Red Alert UDPAny -> 5009	
TCPAny -> 554 Any -> 7070	× #
Any -> 5005	5 . ca
	×××××××
SMTP         TCPAny -> 25           SNMP         UDPAny -> 161	34
	32
Telnet TCPAny -> 23	28
TFTP UDP1024-65535 -> 69	1 2
TODAW A 1999	× #
Total Annihilation UDPAny -> 1000-4999 UDPAny -> 1000-4999	× #
Traceroute UDP32769-65535 -> 33434-33523	1 28
Unreal - Master Server List UDPAny -> 27900	1
Unreal, Unreal Tournament UDPAny -> 7777-7779	1 24
Vonage VoIP Phone Service         Any -> 27900           Vonage VoIP Phone Service         TCPAny -> 5060-5070	1 28
7004-00 0 0000	<u>&gt;</u> ₩ \ ₩
UDPAny -> 1000-1029 TCPAny -> 3074 VDPAny -> 88	1 28
Any -> 3074	-



User Guide

For example, if you clicked the link of a predefined service in the preceding screen, the following screen will appear. If desired, enter a description in the **Service Description** field. Next, click the desired TCP or UDP link.

Service Description:		
Server Ports		
Protocols	Server Ports	Action
<u>ICP</u>	Any -> 2300-4000	<u> </u>
<u>ICP</u>	Any -> 7000-10000	🔪 🎇
JDP	Any -> 2300-4000	🔨 🗶
JDP	Any -> 7000-10000	🔪 🎇
JDP	Any -> 80 🔪 🔌	
New Server Ports		

If you selected TCP (Any -> 2300-4000) the following screen will appear. Select the desired source port and destination port values from the drop-down lists, and then click **OK**.

**NOTE:** For the Source and Destination ports, you can select a single port or a range of ports. In this example, the range for the Source port can be any value from 0 through 65535. And the range for the Destination port can be any value from 2300-4000.

	Edit Service Server Ports
Protocols	тср 💌
Source Ports:	Any 💌
Destination Ports:	Range 💙 2300 - 4000
	✓ <u>OK</u> Cancel



User Guide

After you have entered the desired values and click **OK** in the preceding screen, the following screen will appear. The TCP protocol values have been configured. Next, click **OK** to save the settings.

Service Name:	Alien vs. Predator			
Service Description:				
Server Ports				
Protocols	Server Ports	Action		
TCP	Any -> 2300-4000	N 🗱 🕹		
TCP	Any -> 7000-10000	S 🗱 🕹		
UDP	Any -> 2300-4000	🔪 🎉		
UDP	Any -> 7000-10000	🔪 🎇		
UDP	Any -> 80	🔪 🎉		
New Server Ports				

If you clicked **OK**, the protocol values will be saved to the Router, and the following screen will display the entry.

	Protocols	
Protocols	Ports	Action
Alien vs. Predator	TCPAny -> 2300-4000 Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80	× #
<u>CuSeeMe</u>	TCPAny -> 1503 Any -> 7640 Any -> 7642 Any -> 7642- UDPAny -> 24032 Any -> 1414 Any -> 1424 Any -> 1812-1813 Any -> 7648 Any -> 56800	× *
Dark Reign	UDPAny -> 21154-21157	🔨 🎇
Dark Reign 2	TCPAny -> 26214 UDPAny -> 26214	1
Decent 3	TCPAny -> 7170 UDPAny -> 2092 Any -> 3445	N 🗱
Decent Freespace	TCPAny -> 3999 UDPAny -> 4000 Any -> 7000 Any -> 3493 Any -> 3440	× #
Delta Force	TCPAny -> 3100-3999 UDPAny -> 3568	🔨 🗱
DHCP ALG	UDP67-68 -> 67	1
Diablo, StarCraft(Battle.net)	TCPAny -> 6112 Any -> 116-118 UDPAny -> 6112	× 🗱
DirectX Games	TCPAny -> 47624-47625 Any -> 2300-2400 Any -> 28800-28912 UDPAny -> 47624-47625	<b>\$</b>



User Guide

### 15.12.2.2 Configuring a New User-Defined Application

To configure new user-defined application, click the New Server Ports link in the Edit Service screen.

Service Name: Service Description:	Alien vs. Predator	
Server Ports Protocols	Server Ports	Action
TCP	Any -> 2300-4000	🔪 🌽
TCP	Any -> 7000-10000	N 🗱
UDP	Any -> 2300-4000	S 🗱
UDP	Any -> 7000-10000	
UDP	Any -> 80 🔰 🕺	
New Server Ports		

If you clicked **New Server Ports**, the following screen will appear. Select the desired protocol from the **Protocol** drop-down list, and then enter the protocol number.

	Edit Service Server Ports
Protocols	Other 💌
Protocol Number:	0
	✓ <u>OK</u> X <u>Cancel</u>



User Guide

For example, this screen shows appropriate values, click **OK** to continue.

Protocols UDP 💌	
Source Ports: Any 🗸	
Destination Ports: Range 🔽 1700 - 18	00
✓ <u>OK</u> Cancel	

If you clicked **OK**, the following screen will appear. The UDP port values have been configured. Next, click **OK** to save the settings.

verizo	on				
Main	Wireless My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main		Ec	lit Service		
Edit Service	Service Name:	Alien vs. Predator			
Logout	Service Description:				
	Server Ports Protocols		Server Ports		
	TCP	Any -> 2500-2700	Server Ports		Action
	TCP	Any -> 7000-10000			× ×
	UDP	Any -> 2300-4000			N 🗱
	UDP	Any -> 7000-10000			N 🗱
	UDP	Any -> 80			🔪 🎇
	UDP	Any -> 1700-1800			🔪 🗱
	New Server Ports				-
			X Cancel		



User Guide

If you clicked **OK**, the following screen will appear. The user-defined UDP port settings have been saved to the Router.

Protocols			
Protocols	Ports	Action	
<u>Alien vs. Predator</u>	TCPAny -> 2300-4000 Any -> 7000-10000 UDPAny -> 2300-4000 Any -> 7000-10000 Any -> 80 Any -> 1700-1800	× <b>*</b>	
<u>CuSeeMe</u>	TCPAny -> 1503 Any -> 7640 Any -> 7642 Any -> 7648-7649 UDPAny -> 24032 Any -> 1414 Any -> 1424 Any -> 1424 Any -> 1812-1813 Any -> 7648 Any -> 56800	7 🗱	
Dark Reign	UDPAny -> 21154-21157	🔨 🗶	
Dark Reign 2	TCPAny -> 26214 UDPAny -> 26214	🔨 🎗	
Decent 3	TCPAny -> 7170 UDPAny -> 2092 Any -> 3445	<b>\$</b>	
Decent Freespace	TCPAny -> 3999 UDPAny -> 4000 Any -> 7000 Any -> 3493 Any -> 3440	\ <b>X</b>	
Delta Force	TCPAny -> 3100-3999 UDPAny -> 3568	🔨 🎇	
DHCP ALG	UDP67-68 -> 67	🔨 🗶	
Diablo, StarCraft(Battle.net)	TCPAny -> 6112 Any -> 116-118 UDPAny -> 6112	S 🗱	
DirectX Games	TCPAny -> 47624-47625 Any -> 2300-2400 Any -> 28800-28912	<u>\</u>	



User Guide

# 15.13 UPnP

If you click **Advanced** in the top navigation menu and then select the **UPnP** link, the following screen will appear. This feature advertises the presence of your Router on the LAN. Universal Plug-and-Play is a networking architecture that provides compatibility among networking equipment, software and peripherals. Products that have UPnP can seamlessly connect and communicate with other Universal Plug-and-Play enabled devices, without the need for user configuration, centralized servers, or product-specific device drivers.

To configure UPnP enter the desired values and then click Apply to save the settings.

Universal Plug and Play					
Illow Other Network Users to Control Wireless Broadband Router's Network Features					
Enable Automatic Cleanup of Old Unused UPnP Services					
WAN Connection Publication:	Publish Only the Main WAN Connection 🔽				
<u>√ ок</u>	Apply X Cancel				



User Guide

### 15.14 System Settings

If you click **Advanced** in the top navigation menu and then select the **System Settings** link, the following screen will appear. Use this page to configure various system settings. Enter the desired system settings and then click **Apply** to save the settings.

**NOTE:** This Router ships with Telnet disabled. If Telnet is enabled, you can configure Secure Telnet over SSL Port/Client Authentication.

Hostname—Specify the Router's host name. The host name is the Router's URL address. Local Domain—Specify your network's local domain.

#### Wireless Broadband Router Management Console

Automatic Refresh of System Monitoring Web Pages—select this check box to enable the automatic refresh of system monitoring web pages.

Warn User Before Network Configuration Changes—select this check box to activate user warnings before network configuration changes take effect.

Session Lifetime—this value represents duration of idle time (in seconds) in which the Router will remain active. When this duration times out, the user will have to re-login.

#### **Management Application Ports**

You can configure the following management application ports:

- Primary/Secondary HTTP Management Port
- Primary/Secondary HTTPS Management Port
- Primary/Secondary Telnet Port HTTPs
- Secure Telnet over SSL Port



User Guide

#### Management Application SSL Authentication Options

You can configure the Primary and Secondary HTTPS Management Client Authentication. Select the desired option from the drop-down lists:

- Select None if you do not want to use client authentication.
- Select **Optional** if you want client authentication to be optional.
- Select **Required** if you want client authentication to be required.



System Logging—configure system logging parameters.

System Log Buffer Size—set the size of the system log buffer in Kilobytes.

Remote System Notify Level-select one of the following remote system notification level from the drop-down list:

- None
- Error
- Warning
- Information

System Logging System Log Buffer Size:	16 KB
Remote System Notify Level:	None 🗸
Security Logging Security Log Buffer Size: Remote Security Notify Level:	None Error Warning Information

Security Logging—configure security logging parameters.

Security Log Buffer Size—set the size of the security log buffer in Kilobytes.

Remote Security Notify Level—select one of the following remote security notification levels from the drop-down list:

- None
- Error
- Warning
- Information

Hardware Acceleration—To enable this feature, click the **Enable Hardware Acceleration of Network Traffic** check box (if it is not already checked).

After you have configured the desired settings, click Apply to allow the settings to take effect in the Router.

Security Logging	
Security Log Buffer Size:	16 KB
Remote Security Notify Level:	None 🗸
Hardware Acceleration	None Error Ne Warning Information
<u>чок</u> і	Apply

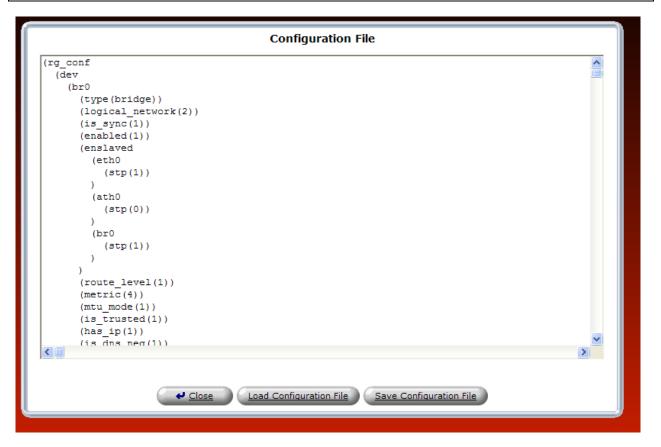


User Guide

### **15.15** Configuration File

If you click **Advanced** in the top navigation menu and then select the **Configuration File** link, the following screen will appear.

IMPORTANT: Do not change the settings in this page unless instructed by Verizon.





User Guide

### **15.16 Date and Time Rules**

If you click **Advanced** in the top navigation menu and then select the **Date and Time** link, the following screen will appear. Enter the desired values in this screen, and then click **Apply** to save the settings.

The Router can automatically detect daylight saving setting for selected time zones. If the daylight saving settings for a time zone are not automatically detected, the following fields will be displayed:

- Enabled—Click this check box to enable daylight saving time (a check mark will appear in the box).
- Start—Enter the date and time when daylight saving starts.
- End—Enter the date and time when daylight saving ends.
- Offset—Enter the time amount daylight saving time changes.
- Automatic Time Update—Click the check box to activate automatic time update (a check mark will appear in the box).
- Protocols—Click the radio button for the protocol used to perform the time update.
- Update Every—Enter the desired value (in Hours) to specify how often to perform the update.
- Time Server—This table lists the address of the time server.
- Status—Displays a time update status.
- Sync Now-Click this button to synchronize the Router's time with your computer operating system's time.

Localization Local Time:	May 28, 2008 16:59:10	
Time Zone:	EST (GMT-05:00)	
Daylight Saving Time ✓ Enabled		
Start Time:	Mar 💙 28 💙 00 : 00	
End Time:	Oct 💙 28 💙 01 : 00	
Offset:	60 Minutes	
Automatic Time Update		
Protocols:	◯ Time Of Day (TOD)	
	<ul> <li>Network Time Protocol (NTP)</li> </ul>	
Update Every:	24 Hours	Sync Now
Time Server	Action	
pool.ntp.org	<b>X</b>	
New Entry	4	
Status:	Got time update from server, Last Update: Wed May 28 14:3	3:57 2008
	Press the <b>Refresh</b> button to update the status.	
6 104		
✓ <u>ok</u>	Apply X Cancel Clock Set	<u> Refresh</u>



User Guide

## **15.17 Editing the Time Server Table**

If you click the **New Entry** link under **Time Server**, the following screen appears. Enter a server IP address or domain name in the field provided, and then click **OK** to continue.

	Time Server Settings	
	Enter server IP address or domain name:	
Time Server:		

The entry will be added to the time server table. To remove server address from the Time Server table, click the "X" icon next to the server to want to remove. Then, click **Apply** to save the changes.

	Date and Time
Localization Local Time: Time Zone:	Jun 11, 2008 11:55:42 EST (GMT-05:00)
Daylight Saving Time Time	
Start Time:	Mar 💙 28 💙 00 : 00
End Time:	Oct 💙 28 💙 01 : 00
Offset:	60 Minutes
Automatic Time Update	
Protocols:	<ul> <li>○ Time Of Day (TOD)</li> <li>⊙ Network Time Protocol (NTP)</li> </ul>
Update Every:	24 Hours Sync Now
Time Server	Action
pool.ntp.org	<u>∖</u> ¥
www.server.com	🔪 🗱
New Entry	🔶
Status:	Got time update from server, Last Update: Tue Jun 10 11:28:29 2008
	Press the Refresh button to update the status.
	Appix Cancel Clock Set



User Guide

# 15.18 Editing Clock Set

If you click the **Clock Set** button in the **Date and Time** screen, the following screen appears. Enter your local time by selecting the appropriate values from the month, day, and year drop-down lists. Next, enter your local time (starting with hours, minutes, and seconds) in the fields provided. Click **Apply** to save the settings. Then click **OK** to return to the **Date and Time** screen.

ve	eri <mark>zo</mark> n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main Clock Set Logout		Local D Local T	ate: Jun 💌 11	Clock Set 2008 V 39 ? Apply X Ca	incel	

### 15.19 Scheduler Rules

If you click **Advanced** in the top navigation menu and then select the **Scheduler Rules** link, the following screen will appear. To configure a schedule rule, click the **New Entry** link.

ve	ri <mark>zo</mark> n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Sch	eduler Rules		
Scheduler Rules Logout		Name <u>New Entry</u>	Set	tings St	atus Ac	tion
L				Refresh		



User Guide

The following screen appears. Click the New Time Segment Entry link or, alternatively, click the plus icon.

ver	i <mark>zon</mark>					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Edit S	cheduler Rule		
Edit Scheduler Rule Logout	J					
		New Time Se	Time Segm gment Entry	ents	Action	
				X Cancel		

If you clicked New Time Segment Entry, the following appears. Click the New Hours Range Entry link.

veri	on					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Edit 1	Fime Segment		
Edit Time Segment		Days of Mon				
Logout		Tue				
			dnesday			
		Thu				
		Sati				
		Sun	day			
		Hours R				
		New Ho	Start Time urs Range Entry	End Time	Action	
				X Cancel	•	



User Guide

The following screen appears. Enter the desired start time and end time values in the fields provided, and then click **OK** to continue.



If you clicked **OK** the following screen will appear. Click the check box of each day that you want in the time segment (a check mark will appear in the box.) Click **OK** to continue.

veri	<b>7</b> 0n					
Main	Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring
Main			Edit 1	Fime Segment		
Edit Time Segment Logout		☐ Thu ☐ Frid ☐ Sati ✔ Sun	iday sday Inesday Isday ay urday iday			
		Hours R 08:00 <u>New Ho</u>	Start Time	End Time 05:00	Action	
			<u> </u>	X Cancel		

After you have set up the desired time segment and clicked **OK**, the following screen will appear. If desired, you can enter a name for the schedule rule in the **Name** field.

Under Rule Activity Settings, be sure to click the setting that you want assigned to the rule:

- Click the first radio button to allow the rule to be active at the scheduled time.
- Click the second radio button to allow the rule to be inactive at the scheduled time.



User Guide

For example, this screen shows that a schedule has been added to the **Time Segments** table, and that the rule will be active at the scheduled time. To add additional schedule rules to your Router, repeat the preceding scheduler rules instructions. Then, click **OK** in the **Edit Scheduler Rule** screen to allow the settings to take effect in the Router.

Main Wireless	My Network	Firewall Settings	Parental Control	Advanced	System Monitoring	
Main		Edit S	Scheduler Rule			
Edit Scheduler Rule Logout						
	Sun between 0: New Time Sec	Time Seg 3:00-05:00 on the next o Iment Entry		Action		
			X Cancel			

## **15.20** Firmware Upgrade

If you click **Advanced** in the top navigation menu and then select the **Firmware Upgrade** link, the following screen will appear. This screen is used to update the firmware that controls the operation of your Router. The updated firmware may be loaded from a CD-ROM, from a file stored on a local hard drive within your network, or from an update file stored on an Internet server.

**IMPORTANT:** The configurable settings of your Router may be erased during the upgrade process.

Do any of the following:

• Select the desired option from the **Upgrade from the Internet** drop-down list. You can choose to perform an automatic check at the specified number of hours and URL. Or you can disable automatic check.

**NOTE:** The URL must be in the format: protocol://user:password@host:port/path where protocol is one of http, https, ftp or tftp. Either user or password, or both, may be left out. The port number is also optional.

• Click **Check Now** to retrieve the firmware update file and display any available update information. You must be connected to the Internet to use this option.

**NOTE:** If you click **Check Now** and the page returns "No new version available," this indicates that the firmware update file is not available.

• Click **Force Upgrade** to download the firmware update file and to automatically update the Router firmware if an update is available and applicable. You must be connected to the Internet to use this option.

**NOTE:** The URL must be in the format: protocol://user:password@host:port/path where protocol is one of http, https, ftp or tftp. Either user or password, or both, may be left out. The port number is also optional.

• Click **Upgrade Now** to retrieve the firmware update file from a local hard drive or CD-ROM on your Network. Internet connection is not required for this option.



User Guide

Wireless Broadband Router Firmware Upgrade
Current Version: 1.02.00.03 Upgrade From the Internet
Automatically Check for New Versions and Upgrade Wireless Broadband Router 💌
Check every 24 hours at URL Next check scheduled in 21:44 hours
Check Now
Status: OK
Internet Version: No new version available
Force Upgrade
Upgrade From a Computer in the Network
Select an updated Wireless Broadband Router firmware file from a computer's hard drive or CD on the network
Upgrade Now

### 15.21 Routing

If you click **Advanced** in the top navigation menu and then select the **Routing** link, the following screen will appear. You can choose to setup your Router to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to neighboring destinations.

### **15.21.1 Basic Routing Settings**

To create a new route, click the **New Route** link. If you change any settings in this screen, click **Apply** to save the settings.

		Routi	ng			
Routing Table	Destination	C-1	N-t	Madada	Chathar	
Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						<b>T</b>
Routing Protocols						
Routing Informatio	n Protocol (RIP)					
Poison Reverse	в					
🗌 Do not Adverti	se Direct Connected Ro	outes				
Internet Group Mai	nagement Protocol (IGI	MP)				
🔽 IGMP Fast Lear	vē					
IGMP Multicast	to Unicast					
Domain Routing (a	dd route entry according t	o interface from whic	DNS record is receiv	ved)		
	,					
	<b>√</b> <u>ok</u>	! Apply	X Cancel	Advanced >>		
				Auvanced >>	1000	



User Guide

If you clicked **New Route**, the following screen will appear. Configure the settings in this screen, and then click **OK** to continue.

- Rule Name—Select the type of network from the drop-down list.
- Destination—Enter the destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.
- Netmask—Enter the network mask is used in conjunction with the destination to determine when a route is used.
- Gateway—Enter the Router's IP address.
- Metric—Enter the desired measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.

Route	Settings
Name:	Network (Home/Office)
Destination:	0.0.0.0
Netmask:	255 . 255 . 255 . 255
Gateway:	0.0.0.0
Metric:	0
<u> ок</u>	X Cancel



User Guide

# 15.21.2 Advanced Routing Settings

To configure advanced routing settings, click the Advanced button in the Routing screen.

		Routi	ng			
Routing Table						
Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						-
Routing Protocols						
Routing Informatio	n Protocol (RIP)					
Poison Reverse	e					
🗌 Do not Adverti	se Direct Connected Ro	utes				
Internet Group Ma	nagement Protocol (IGM	IP)				
IGMP Fast Leaver	ve					
IGMP Multicast	to Unicast					
Domain Routing (a	add route entry according to	interface from which	DNS record is receiv	ved)		
	<b>√</b> <u>ok</u>	! Apply	X Cancel	Advanced >>		

If you clicked the **Advanced** button, the following screen will appear. If you change any settings in this screen, click **Apply** to save the settings.

New Route       Metric       Status       Action         Default Routes       1       Connected       Image: Co	Routing Table Name	Destination	Catoward	Netmask	Motric	Chature	Action
Default Routes       Metric       Status       Action         Device       Metric       Status       Action         WAN PPPOE       1       Connected       Image: Status       Action         Load Balancing       Enabled       Image: Status       Image: S		Destination	Gateway	Netmask	Metric	Status	
WAN PPPoE       1       Connected       Image: Connected         Load Balancing       Enabled       Image: Connected       Image: Connected <th>New Route</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>T</th>	New Route						T
WAN PPPoE       1       Connected       Image: Connected         Load Balancing       Enabled       Image: Connected       Image: Connected <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
Load Balancing         □ Enabled         DSCP-Based Policy Routing         Route all traffic with matching DSCP values to the chosen devices.         Warning: If the chosen device is marked as a default route, other traffic may also be routed to it.         DSCP       Device         Action         New Route <ul> <li>Poison Reverse</li> <li>□ Do not Advertise Direct Connected Routes</li> <li>□ Internet Group Management Protocol (IGMP)</li> <li>♥ IGMP Fast Leave</li> <li>□ IGMP Multicast to Unicast</li> </ul>		-	Metric		15		
DSCP-Based Policy Routing Route all traffic with matching DSCP values to the chosen devices. Warning: If the chosen device is marked as a default route, other traffic may also be routed to it. DSCP Device Action New Route Failover Enabled Routing Protocols Routing Information Protocol (RIP) Poison Reverse Do not Advertise Direct Connected Routes Internet Group Management Protocol (IGMP) VIGMP Fast Leave IGMP Multicast to Unicast	WAN PPPOE	1		Connected		-	<b>X</b>
New Route       Image: Control of the second s	Route all traffic with n	natching DSCP values n device is marked a		her traffic may also	be routed to it.		
Failover         Enabled         Routing Protocols         Routing Information Protocol (RIP)         Poison Reverse         Do not Advertise Direct Connected Routes         Internet Group Management Protocol (IGMP)         ✓ IGMP Fast Leave         IGMP Multicast to Unicast	Naw Dawka	DSCP		Device			
	Enabled						



User Guide

### **15.22 IGMP Configuration**

If you click **Advanced** in the top navigation menu and then select the **IGMP Configuration** link, the following screen will appear. This screen allows you to configure IGMP LAN Proxy configuration settings in your Router.

The Router supports IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a predefined group of recipients. Each member of the multicast group will receive all messages addressed to the group.

IGMP proxy enables multicast packets to be routed according to the IGMP requests of local network devices requesting to join multicast groups. To enable IGMP Proxy, click the adjacent check box, a check mark will appear in the box. Next, enter the appropriate values in the fields provided and click **Apply** to save the settings.

Internet Group Management P	rotocol (IGMP) Configuration Page
IGMP LAN Proxy Configuration IGMP Proxy Enable:	Enabled
IGMP Query Version:	
IGMP Fast Leave:	GMP Fast Leave
Robustness Variable:	2
Query Interval:	5
Query Response Interval:	4
Last Member Query Count:	2
Last Member Query Interval:	1
Client Unsolicited Report Interval:	10
Startup Query Count:	2
Startup Query Interval:	2
Snooping Fast Leave:	Image: State S
Snooping Robustness:	2
Snooping Query Timeout:	10
Filter Membership Messages	
Interface Ethernet New Membership Filter	Port Host IP Action
Multicast Group Filtering	
Multicast Group Filtering Multicast Group R	ange Action
239.0.0.0 - 239.255.255.255	× ×
New Multicast Range	



User Guide

# 15.22.1 New Membership Filter

If you clicked the New Membership Filter link in the preceding screen, the following screen will appear.

Any     Image: Control of the second se	IGMP Memb	ership Filtering	
Alost IP: 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0	Interface:	LAN Ethernet 💌	
Aulticast Address Filter List       Multicast Address       Action	Ethernet Port:	Any 🔽	
Multicast Address Action	Host IP:	0.0.0	. 0
lew Multicast Address	Multicast Address Filter List		
			Action
		Apply Close	

Select the desired settings for the membership filter you want to create. Then click Apply to save the settings.

IGMP Men	nbership Filtering	
Interface: Ethernet Port: Host IP:	LAN Ethernet Vireless	. 0
Multicast Address Filter List Multicast Address New Multicast Address		Action
New Mulicast Address		
( <u>√ok</u>	! Apply	



User Guide

## 15.22.2 New Multicast Address

If you clicked the **New Multicast Address** link in the preceding screen, the following screen will appear. Enter multicast address and then click **Apply**.

	Multicast Filter Address
Multicast Address:	0 . 0 . 0 . 0 ✓ <u>OK</u> <u>Apply</u> <u>Close</u>

If you clicked Apply, the address will be displayed in the list of Multicast Addresses.

IGMP Mem	nbership Filtering	
Interface:	LAN Ethernet 🔽	
Ethernet Port:	Any 🔽	
Host IP:	0.0.0	. 0
Multicast Address Filter List		
Multicast Address	S	Action
192.168.1.6		🔪 🎉
192.168.1.11		N 🗱
New Multicast Address		
<u> √ ok</u>	* Apply	



User Guide

### **15.22.3 IGMP Status**

If you click **Advanced** in the top navigation menu and then select the **IGMP Status** link, the following screen will appear.

NOTE: If IGMP proxy is not enabled, the IGMP Proxy Status panel will be empty.

	IGMP Proxy Status	
IGMP Proxy Status:	Not Available	

### 15.23 PPPoE Relay

If you click **Advanced** in the top navigation menu and then select the **PPPoE Relay** link, the following screen will appear. PPPoE Relay enables the Router to relay packets on PPPoE connections, while keeping its designated functionality for any additional connections.

To activate PPPoE Relay, click the check box (check mark will appear in the box). Click Apply to save the settings.

Enabled	
PPPoE Relay	



User Guide

### 15.24 IP Address Distribution

If you click **Advanced** in the top navigation menu and then select the **IP Address Distribution** link, the following screen will appear.

Your Router's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. The Router's default DHCP server is the LAN bridge.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as "taken." At this point the host is configured with an IP address for the duration of the lease.

IP Address Distribution					
Name	Service	Subnet Mask	Dynamic IP Range	Action	
Network (Home/Office)	DHCP Server	255.255.255.0	192.168.1.1 - 192.168.1.254	1	
	P Close	Connection List	Access Control		

To configure the DHCP Sever settings, click the Network (Home/Office) link, the following screen will appear. Enter the desired DHCP settings in the fields provided, and then click **Apply** to save the settings.

	DHCP Settings for N	letwor	k (	Hom	e/	Offic	e)		
Service IP Address Distrib	ution:	DHCP	Sen	/er 🗸					
DHCP Server									
Start IP Address:		192	٦.	168	٦.	1	٦.	1	
End IP Address:		192	٦.	168	٦.	1	٦.	254	
Subnet Mask:		255	٦.	255	٦.	255	٦.	0	
WINS Server:		0	٦.	0	٦.	0	٦.	0	
Lease Time in Min	utes:	1440	_						
🔽 Provide Host Nan	ne If Not Specified by Client								
IP Address Distrib	ution using DHCP Option (	50 (Vend	lor	Class	T d	entifie	er)		
Vendor ID		Range					,	QoS	
	192.168.1.100 - 192.168.1.150							5 - Medium	



User Guide

# **16. SYSTEM MONITORING**

## 16.1 Gateway Status

If you click **System Monitoring** in the top navigation menu, and then click Gateway Status in the left submenu, the following screen will appear. After you have finished viewing information about your Router, click **Close**.

Software Version: Release Date: Platform: Model Number: INI File Name: INI File Version: Hardware Version: Hardware Serial Number:	1.02.00.03 May 19 2008 Westell UltraLine Series3 A90-9100EM15-10 096-900205-02 1 22 08B405197406	<u>Upgrade</u>
	✓ Close	

Gateway Status					
Software Version	Router's software version.				
Release Date	Router's software release date.				
Platform	Router manufacturer's model name.				
Model Number	Router manufacturer's model number.				
INI File Name	Router's INI file name.				
INI File Version	Router's INI file version.				
Hardware Version	Router's hardware version.				
Hardware Serial Number	Router's serial number.				
Upgrade	Click this link to upgrade the Router's firmware. Refer to section 15.20 for				
	details on this feature.				



User Guide

### 16.2 Gateway Status

If you click **System Monitoring** in the top navigation menu, and then click **Full Status/System wide Monitoring of Connections** in the left submenu, the following screen will appear. This screen displays connection information for devices connected to your Router. At this screen, you can do any of the following:

- Turn off Automatic Refresh by clicking the **Automatic Refresh Off** button. When Automatic Refresh is enabled, the screen will be updated automatically to display the most current statistics.
- Manually refresh this screen by clicking the **Refresh** button.
- Click the links in this screen to access the Router's connection settings.
- Click Close to return to the Network Connections screen.

		Full Statu	ıs/System wid	e Monitorir	ng of Connecti	ons	
			Broadband		_		
	<u>Network</u> (Home/Office)	Ethernet Switch	Connection (Ethernet)	<u>Coax</u>	Broadband Connection (Coax)	Wireless 802.11q Access Point	WAN PPPoE
Device Name	br0	eth0	eth1	LAN-en2210	WAN-en2210	ath0	рррО
Status	Connected	1 Ports Connected	Disabled	Down	Connected	Connected	Connected
	Network (Home/Office)	Network (Home/Office)	WAN	Network (Home/Office)	WAN	Network (Home/Office)	WAN
Underlying Device	<u>Ethernet Switch</u> <u>Coax</u> Wireless 802.11q Access Point						Broadband Connection (Coax)
Connection Type	Bridge	Hardware Ethernet Switch	Ethernet	Multimedia over Coax (MOCA)	Multimedia over Coax (MOCA)	Wireless 802.11g Access Point	PPPoE
Download Rate						54 MB	
Upload Rate						54 MB	
MAC Address	00:18:3a:ac:3a:9a	00:18:3a:ac:3a:9a	00:18:3a:ac:3a:9b		00:18:3a:ac:3a:9b	00:1d:19:59:d7:2	F
IP Address	192.168.1.1						10.16.90.10
Subnet Mask	255.255.255.0						
Default Gateway							10.16.90.1
DNS Server							10.16.16.8 10.16.16.2
IP Address Distribution	DHCP Server	Disabled	Disabled			Disabled	
Service Name							
User Name							verizonfios
Encryption						WEP	
Packets Sent Total	770601	463630	0	0	92867	306918	0
Bytes Sent Total	121225994	127985042	0	0	11644231	110180567	0
Packets Sent Unicast	467533	25975	0	0	80121	4294967250	2411959316
Packets Sent Multicast	301468	436055	0	0	0	301467	4030526120
Packets Sent Broadcast	1600	1600	0	0	12746	5497	2147449160
Packets Sent Total Errors	0	0	0	0	0	0	0
Packets Sent Total	0	0	0	0	0	7	0



User Guide

# 16.3 System Log

If you click **System Monitoring** in the top navigation menu and then click **System Log** in the left submenu, the following screen will appear. This screen displays the details of your system's logged events. To save the system log, click **Save Log**, and then follow the instructions to save the log to the desired location.

System Log						
Press the <b>Refresh</b> button to update the data.						
Time	Event	Event- Type	Details			
May 28 17:30:21 2008	System Log	Message	daemon.warn sys_if_ioctl_mii_execute:507: Both tried MII ioclts 8947/89F0 failed: Operation not supported. [repeated 2 times, last time on May 28 17:30:21 2008]			
May 28 17:27:48 2008	System Log	Message	daemon.warn rmt_upd_open failed			
May 28 17:27:48 2008	System Log	Message	daemon.err Not a HTTP, HTTPS, FTP or TFTP url: [repeated 2 times, last time on May 28 17:27:48 2008]			
May 28 17:27:47 2008	System Log	Message	daemon.warn CONNECTION LOG: WAN status changed from No Internet Connection to Connected, IP address=10.16.90.10			
May 28 17:27:47 2008	System Log	Message	daemon.info secondary DNS address 10.16.16.2			
May 28 17:27:47 2008	System Log	Message	daemon.info primary DNS address 10.16.16.8			
May 28 17:27:47 2008	-	Message	daemon.info remote IP address 10.16.90.1			
May 28 17:27:47 2008	-	Message	daemon.info local IP address 10.16.90.10			
May 28 17:27:46 2008	-	Message	daemon.info Connecting: ppp0			
May 28 17:27:45 2008	-	Message	daemon.info Init IGMP proxy module			
May 28 17:27:45 2008	-	Message	daemon.info Uninit IGMP proxy module			
May 28 17:27:44 2008	-	Message	daemon.info ppp0 started			
May 28 17:27:44 2008	-	Message	daemon.info mt_igmp_changed:1852: IGMP changed: interface: ppp0			
May 28 17:27:44 2008	-	Message	daemon.info Protocol Auto Detect: created pppoe WAN connection			
May 28 17:27:44 2008		Message	daemon.info Protocol Auto Detect: found PPPoE server			
May 28 17:27:43 2008	-	Message	daemon.info PPPoE SRV Detect: Server detected on dev eth1			
May 28 17:27:43 2008		Message	kern.warn eth1: change MAC from 00:18:3A:AC:3A:9B to 00:18:3A:FFFFFAC:3A:FFFFF9B			
May 28 17:27:42 2008	System Log	Message	daemon.info eth1: link up, device will be up			



User Guide

# **17. TECHNICAL SUPPORT INFORMATION**

Contact your Internet service provider for technical support.

### **18. PRODUCT SPECIFICATIONS**

#### System Requirements for 10/100 Base-T/Ethernet

- Pentium<sup>®</sup> or equivalent class machines or higher
- Microsoft® Windows® (XP, 2000, ME, NT 4.0, 98 SE) Macintosh® OS X, or Linux installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- 10/100 Base-T Network Interface Card (NIC)
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer Operating System CD-ROM

#### System Requirements for Wireless

- Pentium<sup>®</sup> or equivalent class machines or higher
- Microsoft® Windows® (XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer 5.5 or higher or Netscape Navigator 7.x or higher
- Computer operating system CD-ROM
- IEEE 802.11b/g PC adapter

#### System Requirements for Coax

- Pentium<sup>®</sup> or equivalent class machines or higher
- Microsoft® Windows® (XP, 2000, ME, 98 SE) installed
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- Internet Explorer 5.5 or later or
- Netscape Navigator 7.x or higher or
- Firefox 1.0.7 or later
- Computer operating system CD-ROM

#### LEDs

- Power
- Coax WAN
- Ethernet WAN
- Internet
- Wireless Setup
- USB
- LAN Ethernet 1 through 4
- Coax
- Wireless

#### Connectors

- COAX
- USB
- Ethernet: Four 8-pin RJ-45 modular jacks
- WAN: 8-pin RJ-45 modular jack
- Power: Barrel connector

#### Power

• Power Supply: 120 VAC to 12 VDC wallmount power supply

#### Dimensions

- Height: 1.9 in. (4.8 cm)
- Width: 10.8 in. (27.4 cm)
- Depth: 5.75 in. (14.6 cm)

#### Weight

• Approx. 1.32 lb (0.60 kg)

#### Environmental

- Relative Humidity: 5 to 95%, non-condensing
- Storage Temperature: -20 °C to 85 °C (-4 °F to 185 °F)
- Ambient Temperature: 23 °C (73 °F)

#### EMC/Safety/Regulatory Certifications

- FCC Part 15, Class B
- FCC Part 68
- ANSI/UL Standard 60950-1
- CAN/CSA C22.2 No. 6090-1



User Guide

### **19. SOFTWARE LICENSE AGREEMENT**

READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY. THIS SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). BY INSTALLING AND OPERATING THIS PRODUCT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE SOFTWARE AND HARDWARE TO WESTELL TECHNOLOGIES, INC. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND WESTELL TECHNOLOGIES, INC. (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

1. License Grant. Licensor hereby grants to you, and you accept, a nonexclusive license to use the Compact Disk (CD) and the computer programs contained therein in machine-readable, object code form only (collectively referred to as the "SOFTWARE"), and the accompanying User Documentation, only as authorized in this License Agreement. The SOFTWARE may be used only in connection with the number of systems for which you have paid license fees as dictated in your support agreement. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this License Agreement. You agree that you may not nor allow others to reverse assemble, reverse compile, or otherwise translate the SOFTWARE.

You may retain the SOFTWARE CD for backup purposes only. In addition, you may make one copy of the SOFTWARE in any storage medium for backup purposes only. You may make one copy of the User's Manual for backup purposes only. Any such copies of the SOFTWARE or the User's Manual shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the SOFTWARE or any portions thereof may be made by you or any person under your authority or control.

2. Licensor's Rights. You acknowledge and agree that the SOFTWARE and the User's Manual are proprietary products of Licensor protected under U.S. copyright law. You further acknowledge and agree that all right, title, and interest in and to the SOFTWARE, including associated intellectual property rights, are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the SOFTWARE, but only a limited right of use revocable in accordance with the terms of this License Agreement.

3. License Fees. The fees paid by you under the support agreement are paid in consideration of the licenses granted under this License Agreement.

4. Term. This License Agreement is effective upon your opening of this package and shall continue until terminated. You may terminate this License Agreement at any time by returning the SOFTWARE and all copies thereof and extracts there from to Licensor. Licensor may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Licensor, you agree to return to Licensor the SOFTWARE and all copies and portions thereof.

5. Limitation of Liability. Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Licensor for the use of the SOFTWARE. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.



User Guide

6. Governing Law. This License Agreement shall be construed and governed in accordance with the laws of the State of Illinois. You submit to the jurisdiction of the state and federal courts of the state of Illinois and agree that venue is proper in those courts with regard to any litigation arising under this Agreement.

7. Costs of Litigation. If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

8. Severability. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

9. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.



User Guide

## **20. PUBLICATION INFORMATION**

Verizon® FiOS® Router Model 9100EM Document Part Number 030-300554 Rev. A

© 2008 Verizon. All rights reserved.

All trademarks and registered trademarks are the property of their respective owners.