LTE Internet (Installed)

User Manual

verizon | technicolor

1
Getting Started 1

1.1 Basic Concepts 3
1.2 Contents of the HBR Box 4
1.3 Getting to Know the HBR 5
1.3.1 Front Panel 6
1.3.2 Back Panel 10

2
Setup 12

2.1 Connecting the HBR to the MoCA Network 14
2.2 Powering on the HBR 15
2.3 Connecting Your Network Devices 16
2.3.1 Connecting Your Wireless Devices via WPS 17
2.3.2 Connecting Your Wireless Device Manually 19
2.3.3 Wired Connection to the HBR 23
2.4 Wall Mounting the HBR (Optional) 24

3
Graphical User Interface (GUI) 26

3.1 Main 29
3.1.1 My Router 30
3.1.2 My Network 32
3.1.3 Action Zone 33

4
GUI: Wireless Settings 34

4.1 Wireless Status 35
4.2 Basic Security Settings 37
4.3 Advanced Security Settings 40
4.3.1 Securing Your Wireless Connection 41
4.3.2 SSID Broadcast 42
4.3.3 Wireless MAC Authentication 43
4.3.4 802.11b/g/n Mode 44
4.3.5 Other Advanced Wireless Options 45

5
GUI: My Network 46

5.1 Network Status 47
5.2 Network Connections 48
5.2.1 Ethernet Properties 49
5.2.2 Wireless Access Point Properties 50
5.2.3 Coax Properties 51
5.2.4 Broadband Connection (LTE) 53

6
GUI: Firewall Settings 54

6.1 General 56
6.2 Access Control 58
6.3 Port Forwarding 60
6.4 DMZ Host 61
6.5 Port Triggering 62
6.6 Remote Aministration 64
6.7 Static NAT 66
6.8 Advanced Filtering 67
6.9 Security Log 70

7
GUI: Parental Control 71

7.1 Parental Control 72
7.2 Rule Summary 74

8
GUI: Advanced Settings 75

8.1 HBA Advanced Pages 77
8.1.1 Diagnostics 79
8.1.2 Restore Defaults 81
8.1.3 Reboot the Router 83
8.1.4 ARP Table 84
8.1.5 Quality of Service (QoS) 85
8.1.6 Local Administration 86

8.1.7 Remote Administration 87
8.1.8 Dynamic DNS 89
8.1.9 DNS Server 91
8.1.10 Configuration File 93
8.1.11 System Settings 95
8.1.12 Firmware Upgrade 98
8.1.13 Network Objects 99
8.1.14 Universal Plug and Play 101
8.1.15 SIP ALG 102
8.1.16 MGCP ALG 103
8.1.17 IGMP Proxy 104
8.1.18 Port Forwarding Rules 105
8.1.19 Date and Time 107
8.1.20 Scheduler Rules 108
8.1.21 Routing 110
8.1.22 IP Address Distribution 112
8.2 HBR Advanced Pages 114
8.2.1 Diagnostics 116
8.2.2 Restore HBR Defaults 117
8.2.3 Reboot HBR 118
8.2.4 ARP Table 119
8.2.5 Users 120
8.2.6 DNS Server 121
8.2.7 System Settings 122
8.2.8 Port Configuration 123
8.2.9 Date and Time 124
8.2.10 IP Address Distribution 125

9

GUI: System Monitoring 126

9.1 HBR Status 128
9.2 Advanced HBR Status 129
9.2.1 System Log 130
9.2.2 Full Status/System wide Monitoring of Connections 131
9.2.3 Traffic Monitoring 132
9.3 Advanced HBA Status 133
9.3.1 Bandwidth Monitoring 134
9.3.2 IGMP Proxy 135

10

Support 136

10.1 General Troubleshooting 138
10.2 Troubleshooting Your Wireless Connection 139

10.3 Resetting your HBR 141
10.4 Configuring Dynamic IP Addressing on Windows 143

1

Getting Started

1 Getting Started

Introduction

HomeFusion Broadband service has been re-branded with the following new name: LTE Internet (Installed). Although the name has changed, it does not impact the service in any way. This user manual will continue to utilize the HomeFusion Broadband name to describe the service.

This User Manual helps you get to know your HomeFusion Broadband service and guides you through the configuration of features of the HomeFusion Broadband Router.

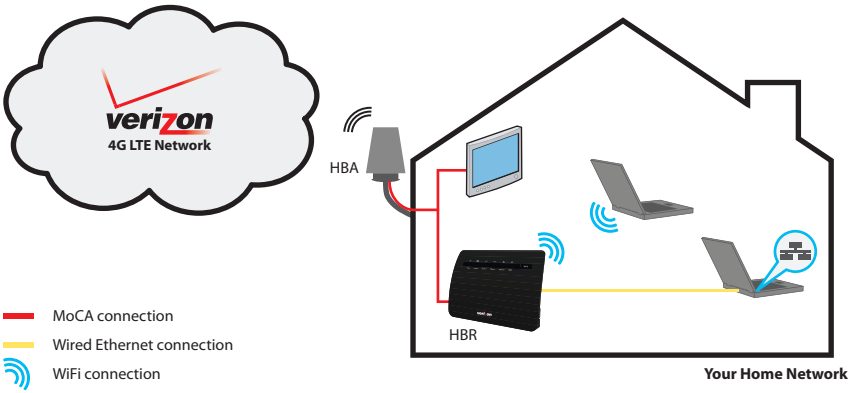
1.1 Basic Concepts

The Verizon 4G LTE Network

4G Long Term Evolution (LTE) is the latest standard for mobile Internet access and offers superior connection speeds compared to 3G, the predecessor.

The HomeFusion Broadband Router only supports 4G LTE to access the Internet. It is not possible to fall back to 3G in the event of a temporary service interruption of the 4G LTE network.

Your Home Network



Your Home Network

Your home network consists of the following components:

- One HomeFusion Broadband *Antenna* (HBA)
- One HomeFusion Broadband *Router* (HBR)
- One or more *network devices* (computers, network printers and so on)

MoCA is a standard for home networking over a coax connection.

The HBA

The HBA is mounted on the side of the house and is the interface between the Verizon 4G LTE Network and your MoCA devices.

The HBR

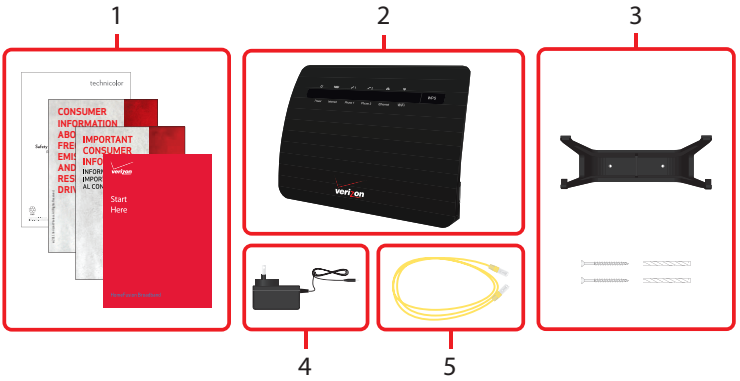
The HomeFusion Broadband Router is located in your home and is responsible for interconnecting:

- WiFi devices (for example: portable computers, wireless printers, smartphones with WiFi support and so on)
- Wired Ethernet devices (for example: computers).
- MoCA devices (for example: the HBA)

This means that all devices that are connected to the HBR will also have access to the HBA, which in turn provides access to the Verizon 4G LTE Network.

1.2 Contents of the HBR Box

Your box should contain the following items:



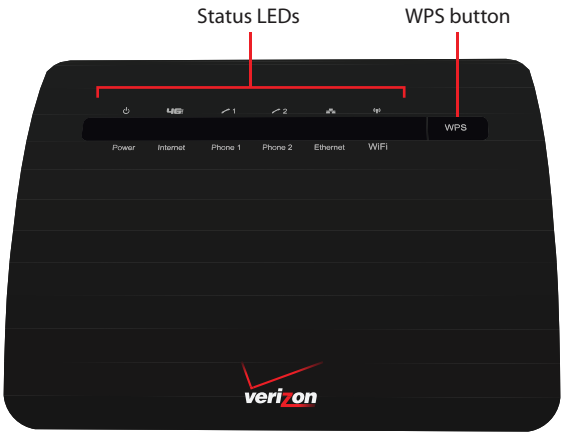
Item	Description
1	Four documents: ■ The Quick Start Guide (Start Here) ■ The Safety and Regulatory Notices ■ The Consumer Information about Radio Frequency Emissions and Responsible Driving ■ Important Consumer Information Read these documents before you start using your HBR.
2	The *H*omeFusion *B*roadband *R*outer. In this User Manual we will refer to it as *HBR*.
3	The Wall Mounting kit containing: ■ The wall mount docking station ■ Screws and plugs
4	One power supply for the HBR
5	One yellow Ethernet cable (RJ-45)

1.3 Getting to Know the HBR

This section introduces you to the different components of the HBR.

Topic	Page
"1.3.1 Front Panel"	*6*
"1.3.2 Back Panel"	*10*

1.3.1 Front Panel



Components

On the front panel of the HBR, you can find:

- The Status LEDs:
  These Status LEDs allow you to check the state of the services offered by the HBR.
- **WPS** button and LED:
  The **WPS** button allows you to add new wireless clients to your local network in a swift and easy way, without the need to enter any of your wireless settings (network name, wireless key, encryption type).

Power LED

Color	State	Description
Green	Solid	Powered on and functioning normally.
	Blinking	Starting up.
Amber	Blinking	Upgrade ongoing. Do *not* remove any cables or switch off the HBR when the HBR is upgrading.
Red	Solid	Error during startup. Call Customer Care at *800-922-0204*.
Off		The HBR is powered off.

4G LTE Internet LED

Color	State	Description
Green	Solid	Connected to the MoCA network.
	Blinking	Connected to the MoCA network, activity.
Amber	Solid	Connected to the MoCA network but internal registration failure.
	Blinking	Connected to the MoCA network, activity but internal registration failure.
Red	Solid	No link to the MoCA network.
	Blinking	Connected to the MoCA network, HBA could not be found.
Off		The HBR is either powered off or starting up.

Phone LED — Phone service is not supported at this time

Color	State	Description
Green	Solid	Connected to the Verizon telephone network.
	Blinking	Call ongoing or connecting to the Verizon telephone network.
Amber	Blinking	Voice mail message available.
Red	Solid	Failed to connect to the Verizon telephone network.
Off		The HBR is either powered off or telephony is not enabled.

Ethernet LED

Color	State	Description
Green	Solid	One or more the device(s) connected to the Ethernet port, no client data activity
	Blinking	One or more the device(s) connected to the Ethernet port, client data activity

Color	State	Description
Red	Solid	No devices connected to the Ethernet port.
Off		■ The HBR is powered off or starting up. ■ All devices connected to the Ethernet ports are powered off.

WiFi LED

Color	State	Description
Green	Solid	Wireless is enabled, no client data activity
	Blinking	Wireless is enabled, client data activity
Off		■ The HBR is powered off or starting up. ■ Wireless is disabled. For more information, see *"4.2 Basic Security Settings" on page 37*.

WPS LED

Color	State	Description
Green	Solid	WPS successful.
Amber	Solid	WPS button pressed.
	Blinking	WPS session ongoing. The session will stop in either of the following cases: ■ After a successful connection. ■ After two minutes.
Red	Blinking at a constant rate	Connection failed or other error, try again. If the problem persists, configure your wireless client manually. For more information, see *"2.3.2 Connecting Your Wireless Device Manually" on page 19*.
	Blinking with a pause pattern	Another WPS session is already ongoing. Wait for two minutes and then try again. If the problem persists, configure your wireless client manually. For more information, see *"2.3.2 Connecting Your Wireless Device Manually" on page 19*.

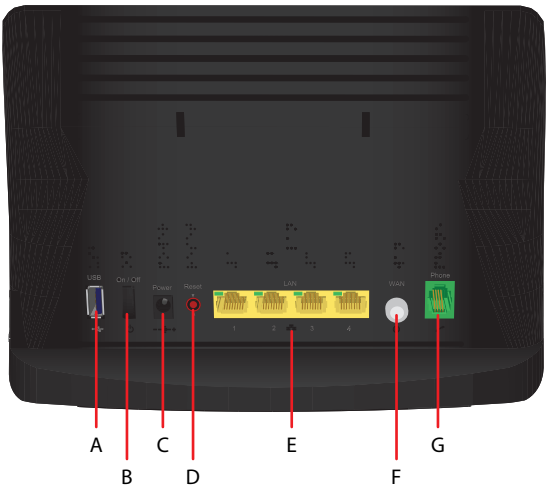
Color	State	Description
Off		■ WPS not initiated. ■ The HBR is powered off or starting up.

For more information on how to connect your wireless clients using WPS, see *"2.3.1 Connecting Your Wireless Devices via WPS" on page 17*.

1.3.2 Back Panel

Overview

The following picture gives you an overview of all the back panel components:



USB port (A)

Allows you to power or charge your USB devices. The USB port can deliver up to 500mA of current. Consult the documentation of your device to check how much current it needs to be able to power or charge.

Any other possible use of the USB port is currently not supported.

Power switch (B)

Allows you to switch the HBR on/off.

Power inlet (C)

This is where you will plug in the power adapter.

Reset button (D)

If you press this button for:

- 2 seconds, the HBR will reboot.
- 10 seconds, the HBR will return to its factory default settings. All changes that you made to the default configuration will be lost. For example: wireless settings, date and time settings, static IP address allocation and so on.

LAN Ethernet Ports (E)

Allow you to connect your local devices (for example: a laptop, network printer or gaming console) using Fast Ethernet.

Each LAN port also has a LED to indicate the state of the Ethernet connection on this port:

LED State	Description
On	Device connected to this port, *no* client data activity.
Blinking	Device connected to this port, client data activity
Off	■ The HBR is powered off or starting up. ■ No device connected to this port.

WAN coaxial cable port (F)

Allows you to connect the HBR to the HBA.

Phone port (G)

Allows you to connect your telephone to the Verizon Wireless telephone network.

The Phone service is not supported at this time.

2

Setup

Setup procedure

Complete the following steps to setup the HBR:

1. If a different router was being used previously, disconnect it. Remove all components, including power supplies and cables; they will not work with the HBR.
2. Connect the HBR to the HBA.
   For more information, see *"2.1 Connecting the HBR to the MoCA Network" on page 14*.
3. Power on the HBR.
   For more information, see *"2.2 Powering on the HBR" on page 15*.
4. Connect your network devices.
   For more information, see *"2.3 Connecting Your Network Devices" on page 16*.

Normally, the Verizon Wireless technician already took care of the installation of your HBR and HBA. So the only thing that you might need to do is add new network devices to your network.

In case of problems

If you have trouble configuring the HBR, try the following:

1. Refer to *"Support" on page 136*.
2. If you did not find a solution in the Troubleshooting section, call the Customer Care at *800-922-0204*.

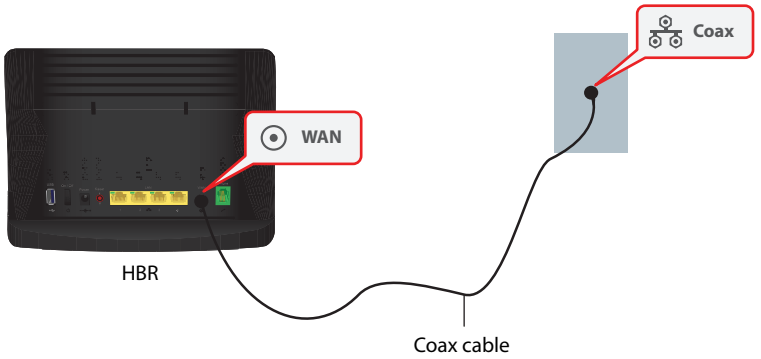
Optional configuration

After completing the setup procedure, the HBR is ready for use. Optionally, you can now:

- Further configure the HBR to your needs (for example, change the wireless security) using the Graphical User Interface (GUI) of the HBR.
  For more information, see *"Graphical User Interface (GUI)" on page 26*.
- Wall mount the HBR. For more information, see *"2.4 Wall Mounting the HBR (Optional)" on page 24*.

2.1 Connecting the HBR to the MoCA Network

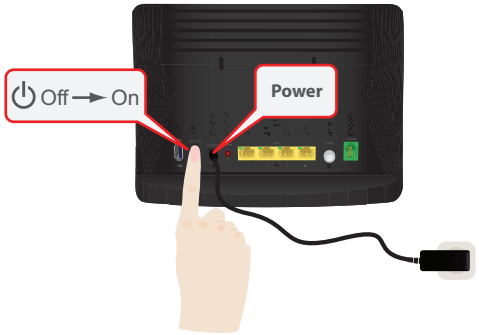
Procedure



1. Take one end of the coaxial cable and connect into the coaxial wall jack.
2. Connect the other end to the **WAN** port of the HBR.

2.2 Powering on the HBR

Procedure



1. Take the power supply that is included with your HBR.
2. Connect the power cord to the **Power** port of the HBR.
3. Plug the other end into an electrical outlet.
4. Push the **On/Off** switch to turn on the HBR.
5. Wait a few minutes to allow the HBR to complete the start up phase.
6. The **Power** LED on the front panel of the HBR must be solid green.
7. After a few minutes, the **Internet (4G LTE)** LED must be solid green.
   If this is not the case, make sure that the coaxial cable is connected properly at both ends. For more information, see *"2.1 Connecting the HBR to the MoCA Network" on page 14*.

2.3 Connecting Your Network Devices

Introduction

This section helps you to connect your network devices (for example, a computer, a network printer and so on) to the HBR network.

Connection options

If you want to connect your computer to the HBR using:

- A wireless connection, you can connect your computer:
  - Via WPS push button configuration, proceed with *"2.3.1 Connecting Your Wireless Devices via WPS" on page 17*.
  - By manually entering the settings, proceed with *"2.3.2 Connecting Your Wireless Device Manually" on page 19*.
- A wired (Ethernet) connection, proceed with *"2.3.3 Wired Connection to the HBR" on page 23*.

2.3.1 Connecting Your Wireless Devices via WPS

WPS

Wi-Fi Protected Setup (WPS) allows you to add new wireless devices to your local network in a swift and easy way, without the need to enter any of your wireless settings (network name, wireless key, encryption type).

Requirements

- Your wireless device must support WPS. Check the documentation of your wireless device for this.

  Both Windows 7 and Windows Vista Service Pack 1 have native WPS support.

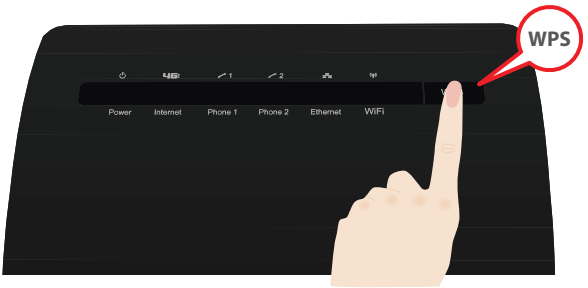
- The HBR must use WPA2 (default setting), WPA+WPA2 or WPA-TKIP.

  It is not possible to use WPS when the HBR uses WEP or no encryption.

Procedure

Proceed as follows:

1 Briefly press the WPS button on the **HBR**:



2 The **WPS** button LED starts blinking amber. This indicates that the HBR is now searching for wireless devices that are in registration mode. You now have two minutes to start WPS on your wireless device.

3 Start WPS on your wireless device.

4 The HBR is now exchanging the security settings.

5 At the end of the procedure the status of the WPS LED will change to either of the following:

- Solid green
  This indicates that you have successfully registered your wireless device. You are now connected to the HBR network.
- Blinking red at a constant rate
  This indicates that the HBR could not find your wireless device. Use the same procedure to try again (you do not need to wait until the LED turns off).

- Blinking red with a pause pattern
  This indicates that another WPS session is already ongoing. Wait for two minutes and then try again.

Troubleshooting

If you are having trouble connecting your wireless device via WPS, configure your wireless client manually. For more information, see *"2.3.2 Connecting Your Wireless Device Manually" on page 19*.

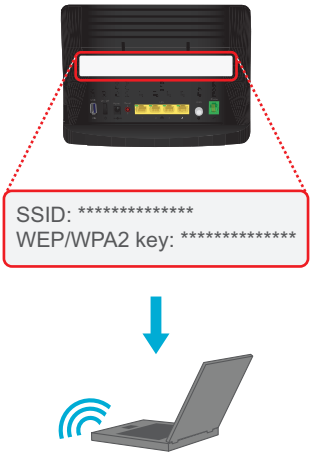
2.3.2 Connecting Your Wireless Device Manually

Requirements

- Your network device must be equipped with a WiFi-certified wireless client.
- Your network device must be configured to obtain an IP address automatically. This is the default setting.

Procedure

If you want to connect a computer using the wireless network, configure the wireless client on your computer with the wireless settings printed on the label of the HBR.



The default encryption type is *WPA2*.

To configure these settings on:

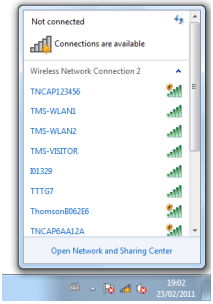
- Windows 7, proceed with *"Connect your computer on Windows 7" on page 20*.
- Windows Vista, proceed with *"Connect your computer on Windows Vista" on page 20*.
- Windows XP, proceed with *"Connect your computer on Windows XP" on page 21*.
- Mac OS X, proceed with *"Connect your computer on Mac OS X" on page 22*.
- On another operating system, consult the help of your wireless client or operating system.

Connect your computer on Windows 7

Proceed as follows:

1 Click the wireless network icon ( )in the notification area.

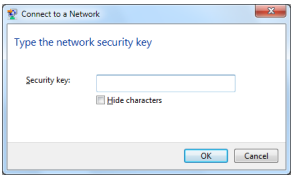
2 A list of available wireless networks appears.



Double-click the HBR access point.

The HBR is listed with the network name (**SSID**) that is printed on the back of the HBR (for example: TNCAP123456).

3 Windows prompts you to enter the network security key.



Type the **WPA2 key** that is printed on the back of the HBR in the **Network key** and **Confirm network key** box and click **Connect**.

Connect your computer on Windows Vista

Proceed as follows:

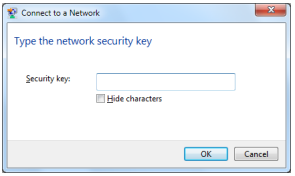
1 Click **Start** and click **Connect To**.

2 A list of available wireless networks appears.

3 Double-click the HBR access point.

The HBR is listed with the network name (**SSID**) that is printed on the back of the HBR (for example: TNCAP123456).

4 Windows prompts you to enter the network security key.



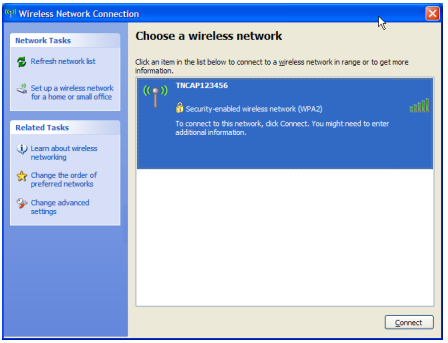
Type the **WPA2 key** that is printed on the back of the HBR in the **Network key** and **Confirm network key** box and click **Connect**.

Connect your computer on Windows XP

Proceed as follows:

1 Right-click the wireless network connection icon (or)in the notification area and then click **View Available Wireless Networks**.

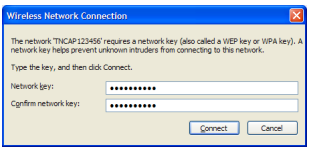
2 A list of available wireless networks appears.



Double-click the HBR access point. The HBR is listed with the network name (**SSID**) that is printed on the back of the HBR (for example: TNCAP123456).

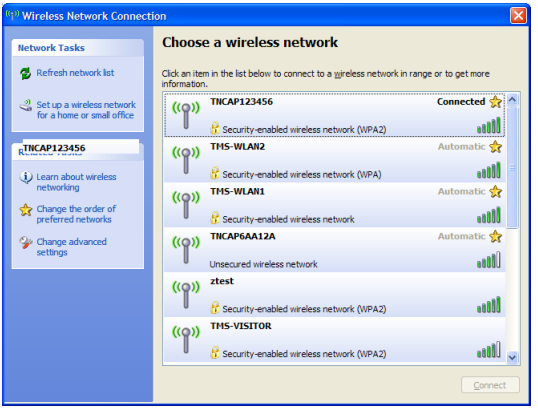
If the HBR is not in the list, see *"Windows can not find the HBR access point" on page 139*.

3 Windows prompts you to enter the network security key.



Type the **WPA2 key** that is printed on the back of the HBR in the **Network key** and **Confirm network key** box and click **Connect**.

4 You are now connected to the HBR:

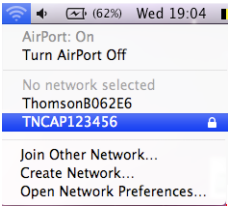


Connect your computer on Mac OS X

Proceed as follows:

1 Click the **Airport** icon on the menu bar.

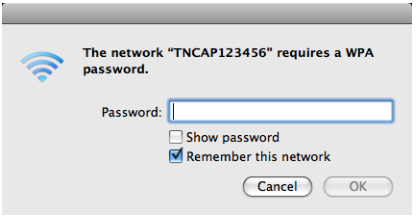
2 A list of available wireless networks appears.



Select the HBR from the list.

The HBR is listed with the network name (**SSID**) that is printed on the back of the HBR (for example: TNCAP123456).

3 The **AirPort** window prompts you to enter your WPA password.



In the **Password** box, type the **WPA2 key** that is printed on the back of the HBR and select the **Remember this network** box and click **OK**.

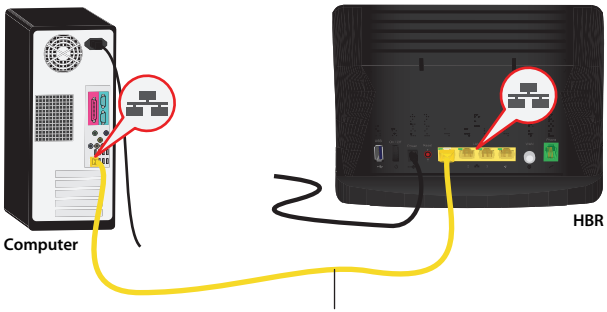
4 You are now connected to the HBR network.

2.3.3 Wired Connection to the HBR

Requirements

- Both your network device (for example, a computer, an Ethernet switch and so on) and HBR must have a free Ethernet port.
- Your network device must be configured to obtain an IP address automatically. This is the default setting. For more information, see *"10.4 Configuring Dynamic IP Addressing on Windows" on page 143*.

Procedure



Proceed as follows:

1. Take the yellow Ethernet cable that was included in your box.
2. Plug the Ethernet cable into one of the four yellow Ethernet ports on the back of the HBR.
3. Plug the other end of the yellow Ethernet cable into an Ethernet port on the computer.
4. If you have not yet started up your computer, start up your computer.
5. The LED on the connected Ethernet port should be solid green or blinking green.
6. Use the same procedure to connect your other Ethernet devices (computers, network printers and so on).

2.4 Wall Mounting the HBR (Optional)

Introduction

This section will help you to wall mount the HBR.

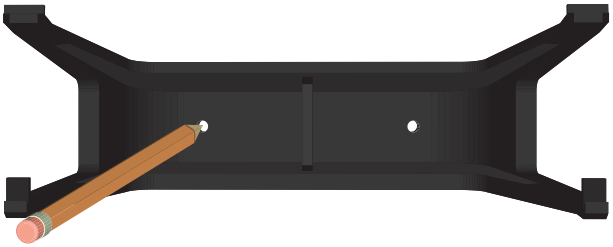
What you need

- A power drill
- A pencil to mark the mounting holes
- A small level is recommended to level the two holes
- The following box items:
  - The HBR
  - The wall mount bracket
  - The screws and wall plugs

Procedure

Proceed as follows:

1. Place the wall mount bracket against the wall at the position where you want to mount the HBR.
2. Mark the mounting holes with a pencil.

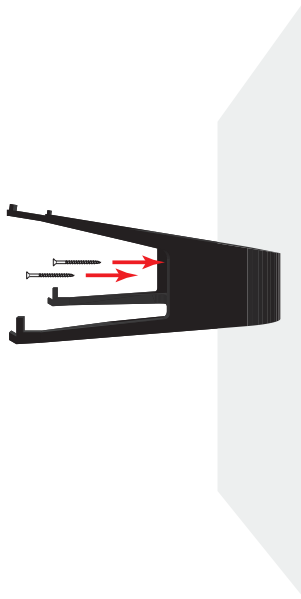


If possible, use a level placed on top of the bracket to level the bracket.

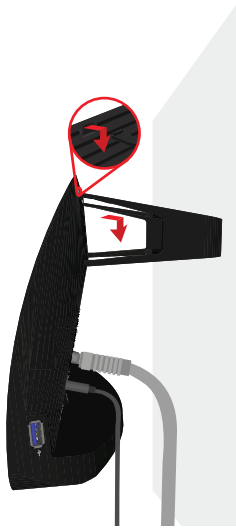
3. Put the wall mount bracket down.
4. If you want to:
   - Use wall plugs, drill the mounting holes with a 15/64 inches diameter drill bit and insert the wall plugs in the drilled holes.
   - Insert the screws directly into the wall, drill the mounting holes with a 5/64 inches diameter drill bit.

The wall plugs are used in softer material such as drywall to provide a more secure mount.

5 Place the wall mount bracket back into position and insert the screws.



6 Carefully hang the HBR on the wall mount bracket.



3

Graphical User Interface (GUI)

3 Graphical User Interface (GUI)

Introduction

The Graphical User Interface (GUI) is a web browser interface that allows you to configure both the HBR and the HBA settings.

Requirements

JavaScript must be enabled on your browser (this is the default setting). For more information, consult the help menu of your web browser.

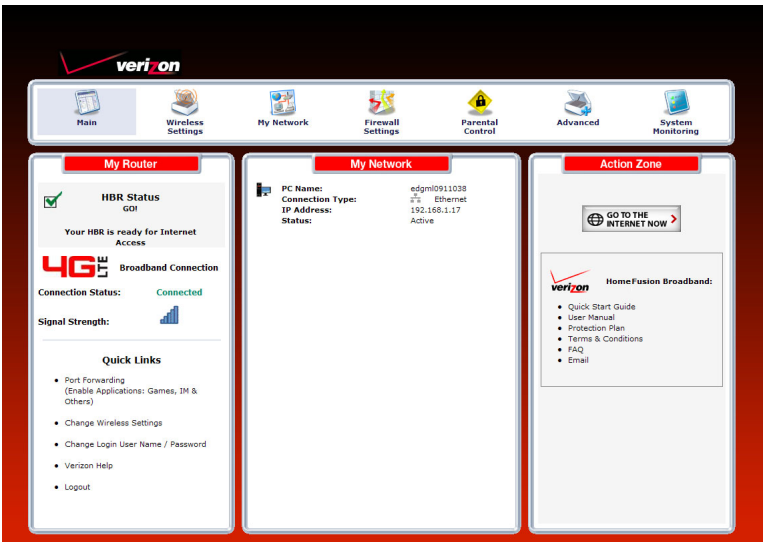
Accessing the GUI

Proceed as follows:

1. Open your web browser.
2. In the **Address** box, type http://192.168.1.254 and press ENTER.
3. The HBR prompts you to enter your user name and password. Enter your user name and password and click **OK**.

   If you did not yet change the password, type **admin** in the **User Name** box and type the **Login password** printed on the back label of your HBR in the **Password** box.

4. The HBR GUI appears.



Menu

The menu bar on the top contains the following items:

Icon	Name	For more information, see...
	Main	*"3.1 Main" on page 29*.
	Wireless Settings	*"4 GUI: Wireless Settings" on page 34*.
	My Network	*"5 GUI: My Network" on page 46*.
	Firewall Settings	*"6 GUI: Firewall Settings" on page 54*.
	Parental Control	*"7 GUI: Parental Control" on page 71*.
	Advanced	*"8 GUI: Advanced Settings" on page 75*.
	System Monitoring	*"9 GUI: System Monitoring" on page 126*.

3.1 Main

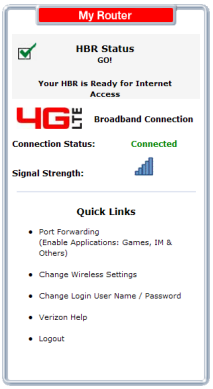
Main page

The **Main** page provides a summary view of the main services of the HBR. The content of the page is divided into three groups:

- **My Router**
  For more information, see *"3.1.1 My Router " on page 30*.
- **My Network**
  For more information, see *"3.1.2 My Network" on page 32*.
- **Action Zone**
  For more information, see *"3.1.3 Action Zone" on page 33*.

3.1.1 My Router

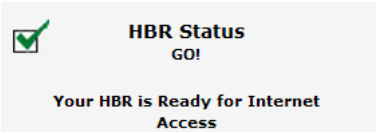
Introduction

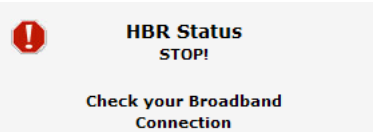


The **My Router** pane displays the status of the HBR's network and Internet connection and contains the following items:

- *HBR Status*
- *Broadband Connection*
- *Quick Links*

HBR Status

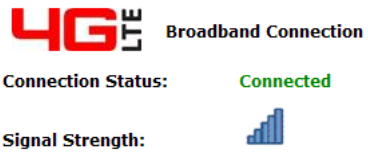


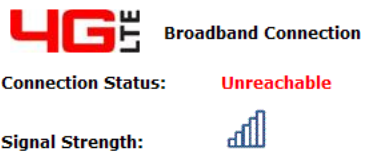


The **HBR Status** informs you about the status of your Internet connection:

Icon	Description
	Indicates that the HBR is connected to the Internet.
	Indicates that the HBR is *not* connected to the Internet.

Broadband Connection





Under **4G LTE Broadband Connection**, you can view:

- The status of the 4G LTE connection.
- The signal strength of the 4G LTE connection.

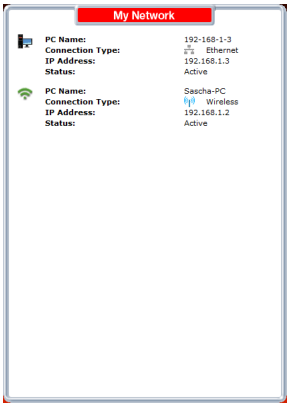
Quick Links

The **Quick Links** section provides links to frequently used pages. The following quick links are available:

- **Port Forwarding**
  Click this link to assign a service (for example a HTTP server) to a network device. Request for this service that are initiated from the Internet will automatically be forwarded to this device.
- **Change Wireless Settings**
  Click this link to configure the wireless access point of the HBR.
  For more information, see *"GUI: Wireless Settings" on page 34*.
- **Change Login User Name/Password**
  Click this link to change your login information.
  For more information, see *"8.2.5 Users" on page 120*.
- **Verizon Help**
  Click this link to view the online help of the HBR.
- **Logout**:
  Click this link to quit your session. You will need to re-enter your user name and password to return to the GUI.

3.1.2 My Network

Introduction



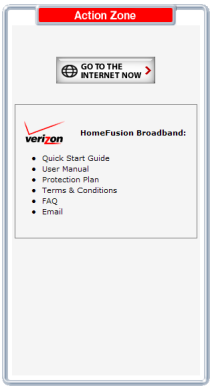
The **My Network** pane, provides you an overview of the devices that are currently connected to the HBR.

The following information is provided for each device:

- **PC Name**:
  Displays the name that will be used to reference to the device.
- **Connection Type**:
  Displays how the device is connected to the HBR (Ethernet, Wireless or Coax).
- **IP Address**:
  Displays the IP address of the device.
- **Status**:
  Displays whether the device is currently connected or not.

3.1.3 Action Zone

Introduction



The **Action Zone** pane allows you to access specific Verizon services and support information. Click:

- **GO TO THE INTERNET NOW** to browse to your home page.
- **Quick Start Guide** to view the latest version of the Quick Start Guide.
- **User Manual** to view the latest version of this User Manual.
- **Protection Plan** to view more information on the Verizon Wireless HomeFusion Broadband Protection Plan.
- **FAQ** to view the Frequently Asked Questions.
- **Email** to sign into your Verizon HomeFusion Email Account.

4

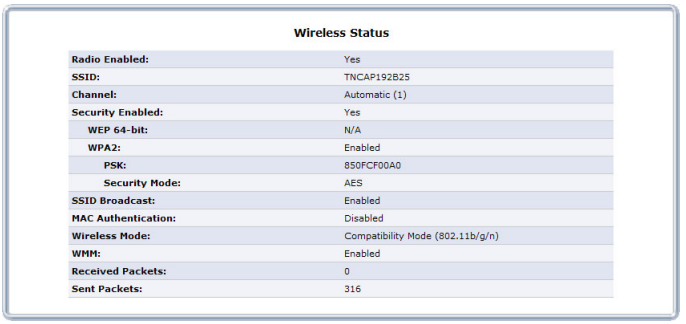
GUI: Wireless Settings

4.1 Wireless Status

Introduction

The **Wireless Status** page provides you an overview of the wireless settings that are currently used by the HBR.

Overview



The following settings are available:

- **Radio Enabled**:
  Displays whether the HBR's wireless radio is active.
- **SSID**:
  To distinguish one wireless network from another, each wireless network has its own network name, often referred to as Service Set IDentifier (SSID). All your wireless devices on your network must use this network name.
- **Channel**:
  Displays the channel to which the wireless connection is currently set. When you select **Automatic** (default setting), the HBR automatically selects the best channel for your wireless communication. The actual channel will then be displayed between parentheses (for example, **Automatic (6)** indicates that channel 6 is selected).
- **Security Enabled**:
  Displays whether wireless security is enabled. If security is enabled, the HBR is using one of the following encryption types to secure your wireless connection:
  - **WEP 64-bit or 128-bit**:
    The oldest and also least secure encryption type. We recommend to use WPA 2 instead. Only use it if your wireless client does not support WPA.
  - **WPA - TKIP**
    The first version of WPA. Only choose this option if none of your wireless clients support WPA2.

- **WPA+WPA2**:
  This is a mixed mode. In this mode, WPA2 is the preferred encryption type but wireless clients that do not support WPA2 can still use WPA as encryption type. Choose this option if not all of your wireless clients support WPA2 or if you are not sure. Wireless clients that support WPA2 will use WPA2, the others will use WPA.
- **WPA2** (default):
  The most recent and most secure version of WPA. Choose this version if you are sure that all your wireless clients support WPA2.

When you connect to the HBR, you have to enter the key that is listed next to the encryption type.

- **SSID Broadcast**:
  Displays whether the HBR is broadcasting its SSID. If activated, the SSID will appear in the list when a wireless client scans for available networks. For more information, see *"4.3.2 SSID Broadcast" on page 42*.
- **MAC Authentication**:
  If MAC authentication is enabled, only wireless clients that are included in the Access list are allowed to connect. For more information, see *"4.3.3 Wireless MAC Authentication" on page 43*.
- **Wireless Mode**:
  Displays the types of wireless device that can join the network. Options include:
  - **Compatibility Mode (802.11b/g/n)**
    In this mode 802.11b, 802.11g and 802.11n can be used to connect to the HBR.
  - **Legacy Mode (802.11b/g)**
    In this mode only 802.11b- and 802.11g connections can be used to connect to the HBR. 802.11n connections are not allowed.
- **WMM:**
  Wi-Fi Multimedia is a QoS (Quality of Service) system for your wireless connection. It prioritizes packets based on their type (voice, video, best effort and background).
- **Received Packets:**
  The number of packets received and sent since the HBR's wireless capability was activated.
- **Sent Packets:**
  Displays the number of packets received and sent since the HBR's wireless capability was activated.

4.2 Basic Security Settings

Introduction

The **Basic Security Settings** page allows you to configure the basic wireless settings of the HBR in a step-by-step approach.

Your changes will only be applied as soon as you click the Apply button.

Overview of the steps

This section describes:

Step 1: Turn Wireless ON/OFF

Step 2: Change the SSID setting to any name or code you want

Step 3: Channel

Step 4: Click on the button next to WEP

Step 5: Select a WEP Key

Step 6: Turn WPS ON

Step 7: Write down wireless settings

Step 1: Turn Wireless ON/OFF

If you want to:

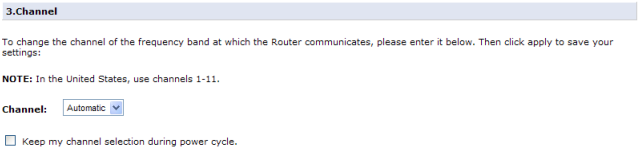
- Turn on the wireless interface, select **On**.
- Turn off the wireless interface, select **Off**.
  Be aware that wireless access will no longer be available. Make sure that nobody is using the wireless connection before turning it off.

We recommend that you leave the wireless interface turned on.

Step 2: Change the SSID setting to any name or code you want

If you want to change the default network name of your wireless network, type the new network name in the **SSID** box.

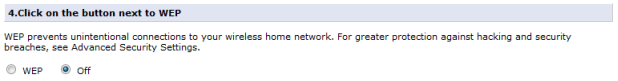
Step 3: Channel



If you want to change the channel for your wireless communication, select a new channel in the **Channel** list.

We recommend that you use **Automatic** (this is also the default). When **Automatic** is selected the HBR will choose the channel that has the least interference. Only change it if you experience wireless connectivity problems.

Step 4: Click on the button next to WEP

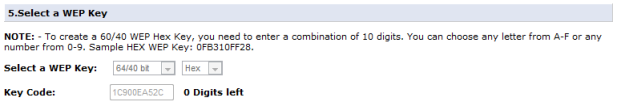


In this step you are able to use WEP encryption to secure your wireless connection. WEP has been proven to have some security issues.

The only reason why you might consider to use WEP is if you have older wireless devices in your network that only support WEP.

We recommended that you keep the **Off** option selected and *use WPA2 or WPA+WPA2 instead*. For more information, see *"4.3.1 Securing Your Wireless Connection" on page 41*.

Step 5: Select a WEP Key



If you did choose to enable WEP in the previous step, this step will allow you to choose the WEP key.

1 In the **Select a WEP key** list, select:

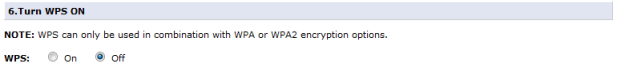
- **64/40 bit** and **Hex** to enter a combination of 10 digits. You can choose any letter from A-F or any number from 0-9. For example: **0FB310FF28**.
- **64/40 bit** and **ASCII** to enter a combination of 5 ASCII characters. For example: **hello**.
- **128/104 bit** and **Hex** to enter a combination of 26 digits. You can choose any letter from A-F or any number from 0-9. Sample HEX WEP Key: **0FB310FF280FB310FF28123456**.
- **128/104 bit** and **ASCII** to enter a combination of 13 ASCII characters. For example: **sayhelloworld**.

2 Enter the key of your choice in the **Key Code** box.

3 If needed, complete the other steps

4 Click **Apply** on the bottom of the page.

Step 6: Turn WPS ON



Wi-Fi Protected Setup (WPS) allows you to add new wireless clients to your local network in a swift and easy way, without the need to enter any of your wireless settings (network name, wireless key, encryption type).

WPS can only be turned on if you are using WPA or WPA+WPA2 to encrypt your wireless connection. If WEP or no encryption is used, the selection will be unavailable.

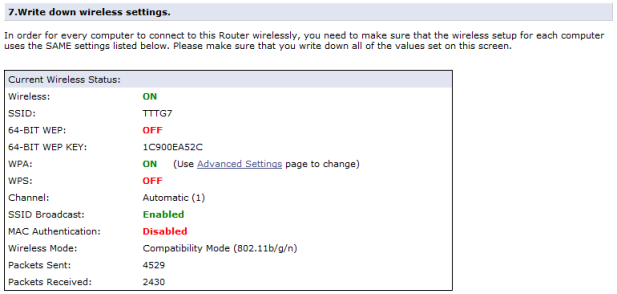
To turn WPS on/off:

1 Under WPS, select **On**/**Off**.

2 If needed complete the other steps.

3 Click **Apply**.

Step 7: Write down wireless settings



This step gives you an overview of the settings that will be active as soon as you click the **Apply** button on the bottom of the page.

You can print or write down this overview, this might be useful when configuring a wireless client.

APPLY YOUR CHANGES

Do not forget to click **Apply** on the bottom of your page to activate your changes.

4.3 Advanced Security Settings

Introduction

The **Advanced Security Settings** page allows you to take your wireless security to the next level.

To improve the security of your wireless network you can add the following security levels:

- **Level 1: Securing your wireless traffic as it transmits through the air**
  This level is allows you to encrypt your wireless traffic with a wireless key to make sure that only the sender and the receiver can read the data that is sent over your wireless connection.
  For more information, see *"4.3.1 Securing Your Wireless Connection" on page 41*.
- **Level 2: Stop your gateway from broadcasting your Wireless Network Name (SSID)**
  This level allows you to disable the broadcasting of your wireless network name to hide your wireless network from other users.
  For more information, see *"4.3.2 SSID Broadcast" on page 42*.
- **Level 3: Limit access to certain wireless devices**
  This level allows you to:
  - Limit access based on the MAC address of the wireless device.
    For more information, see *"4.3.3 Wireless MAC Authentication" on page 43*.
  - Limit access based on the wireless mode supported by the wireless device.
    For more information, see *"4.3.4 802.11b/g/n Mode" on page 44*.

4.3.1 Securing Your Wireless Connection

Encryption types

The HBR supports the following encryption types:

- **WEP**:
  The least safe encryption type used for wireless connections. WEP has been proven to have security issues. Only use this encryption if your wireless device does not support **WPA2** or **WPA**.
- **WPA - TKIP**
  The first version of WPA. Only choose this option if none of your wireless clients support WPA2.
- **WPA+WPA2**:
  This is a mixed mode. In this mode, WPA2 is the preferred encryption type but wireless clients that do not support WPA2 can still use WPA as encryption type. Choose this option if not all of your wireless clients support WPA2 or if you are not sure. Wireless clients that support WPA2 will use WPA2. The others will use WPA.
- **WPA2** (default and *recommended* encryption)**:**
  The most recent and most secure version of WPA. Choose this version if you are sure that all your wireless clients support WPA2.
- **None**

If you want to configure WPA2 on the built-in wireless utility of Windows XP Service Pack 2 (SP2), you first have to:

- Upgrade your Windows XP to Service Pack 3.

- or -

- Install the following update: http://support.microsoft.com/kb/917021.

Although the HBR allows you to use WEP or no security, we strongly advise against this! We recommend that you use **WPA2**.

Changing the encryption type

1. On the **Wireless Settings** menu, click **Advanced Security Settings**.
2. Under **Level 1**, select the encryption type of your choice.
3. Enter the pre-shared key of your choice or use the default one.
4. Click **Apply**.

Changing the wireless key

1. On the **Wireless Settings** menu, click **Advanced Security Settings**.
2. Under **Level 1**, re-select the encryption type that you are currently using.
3. Enter the pre-shared key of your choice or use the default one.
4. Click **Apply**.

4.3.2 SSID Broadcast

SSID

To be able to distinguish one wireless network from another, each wireless network has its own network name, often referred to as Service Set IDentifier (SSID). All your wireless devices on your network must use this network name (and the correct encryption).

Broadcast

By default, the HBR broadcasts its wireless SSID. Wireless clients can then detect the presence of your network and inform the users that this network is available.

Enabling SSID broadcast does not mean that everyone can connect to your network. They still need the correct wireless key to connect to the HBR network. It only informs them that your network is present.

Disabling SSID Broadcast

Proceed as follows:

1. On the **Wireless Settings** menu, click **Advanced Security Settings**.
2. Under **Level 2**, click **SSID Broadcast**.
3. The SSID Broadcast page appears:

Click:

- **Enable** to allow wireless clients to see your wireless network.
- **Disable** to prevent wireless clients from seeing your wireless network.

4. Click **Apply**.

4.3.3 Wireless MAC Authentication

MAC Address

A MAC (Media Access Control) address is a unique hexadecimal code that identifies a device on a network. Each network device has such a MAC address.

MAC Authentication

When using MAC authentication, you allow or deny devices to access to your network based on their MAC address.

Warning: MAC authentication alone is not enough!

Wireless MAC Authentication only offers a limited level of security. Hackers can easily detect a trusted MAC address and clone this trusted MAC address to their own computer, which will enable them to pass the MAC authentication filter. That's why it is important that you first secure your wireless connection (preferably with a **WPA2** encryption key). This way hackers won't be able to interpret your wireless traffic.

Enabling MAC Authentication

Proceed as follows:

1. On the **Wireless Settings** menu, click **Advanced Security Settings**.
2. Under **Level 3**, click **Wireless MAC Authentication**.
3. Select **Enable Access List**.
4. Select:
   - **Accept all devices listed below** if you want to *block all devices by default*.
   - **Deny all devices listed below** if you want to *allow all devices by default*.
5. Now you can add exceptions to the default rule: enter the MAC addresses of the device in the **Client MAC Address** box and click **Add**. Repeat this step for each device.

   If you choose **Accept all devices listed below** and you are currently connected using a wireless connection, make sure to add the MAC address of your wireless client. If you do not do so, you will be disconnected from the wireless network.
6. Click **Apply**.

4.3.4 802.11b/g/n Mode

Introduction

The **802.11b/g/n Mode** page allows you to specify which wireless standards you want to support.

Wireless standards

The HBR is able to support the following wireless standards:

- *802.11n* offers the highest speed (up to 130Mbps) and best range.
- *802.11g* offers speeds up to 54Mbps.
- *802.11b* offers speeds up to 11Mbps.

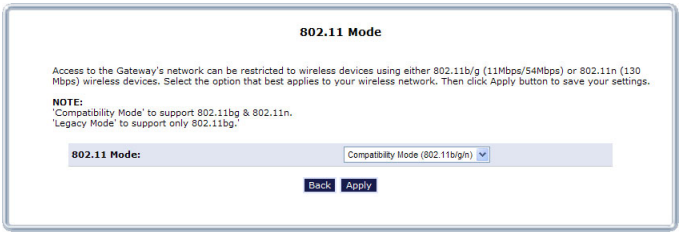
Procedure

Proceed as follows:

1 On the **Wireless Settings** menu, click **Advanced Security Settings**.

2 Under **Level 3**, click **802.11b/g/n Mode**.

3 The **802.11 Mode** page appears:



In the **802.11 Mode** list, select either of the following modes:

- **Compatibility Mode (802.11b/g/n)**
  In this mode 802.11b, 802.11g and 802.11n can be used to connect to the HBR.
- **Legacy Mode (802.11b/g)**
  In this mode only 802.11b- and 802.11g connections can be used to connect to the HBR. 802.11n connections are not allowed.

4 Click **Apply**.

4.3.5 Other Advanced Wireless Options

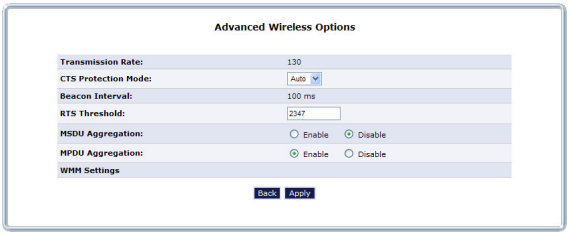
Warning

Changing the **Advanced Wireless Options** may affect your router's wireless performance. Do not make any changes to these options unless you have been instructed to do so by Verizon Wireless support personnel.

Accessing the Advanced Wireless Options page

Proceed as follows:

1. On the **Wireless Settings** menu, click **Advanced Security Settings**.
2. Under **Level 3**, click **Other Advanced Wireless Options**.
3. The HBR prompts you to confirm your choice. Click **Yes**.
4. The **Advanced Wireless Options** page appears.



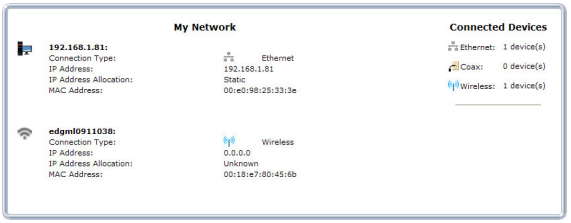
5

GUI: My Network

5.1 Network Status

Introduction

The **Network Status** page provides you an overview of the devices that are currently connected to the HBR.



Device Information

The following information is provided for each device:

- **PC Name**:
  Displays the name that will be used to reference this device.
- **Connection Type**:
  Displays how the device is connected to the HBR (Ethernet, Wireless or Coax).
- **IP Address**:
  Displays the IP address of the device.
- **IP Address Allocation**:
  Displays whether the device is using:
  - A **Dynamic** IP address
    In this case the HBR assigns the first available address in the address pool. This also means that you may get a different IP address the next time you connect.
  - A **Static** IP address
    In this case the device uses a dedicated IP address, you will always use the same IP address for your connection. You can assign a static IP address either on the HBR or your device.
- **MAC Address**:
  Displays the unique hardware address of the HBR.

Connected Devices

The **Connected Devices** pane on the right displays how many devices are connected to a specific interface on the HBR.

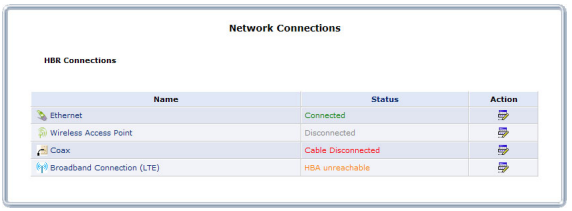
5.2 Network Connections

Warning

The settings covered in this section should be configured by experienced network technicians only!

Introduction

The **Network Connections** page allows you to configure the network connections of the HBR.

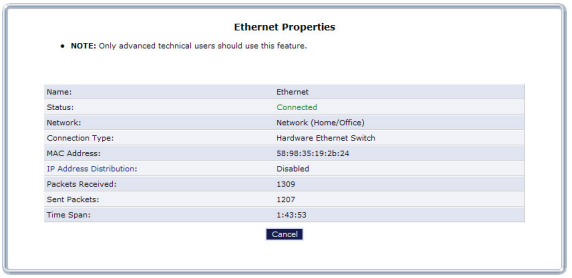


Click or the name of the connection to edit or view the settings of the connection.

5.2.1 Ethernet Properties

Introduction

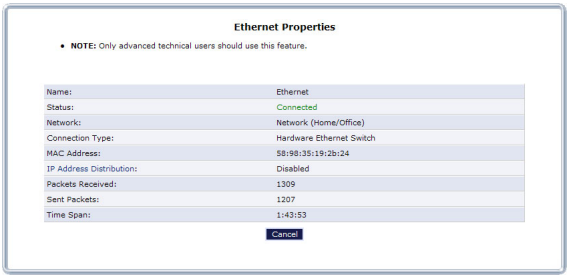
The **Ethernet Properties** page allows you to view the properties of the Ethernet switch of the HBR.



Accessing the Ethernet Properties page

Proceed as follows:

1. On the **My Network** menu, click **Network Connections**.
2. The **Network Connections** table appears. Click **Ethernet**.
3. The **Ethernet Properties** page appears:



4. If you want to change the DHCP settings of the HBR, click **IP Address Distribution**. For more information, see *"8.1.22 IP Address Distribution" on page 112*.

5.2.2 Wireless Access Point Properties

Introduction

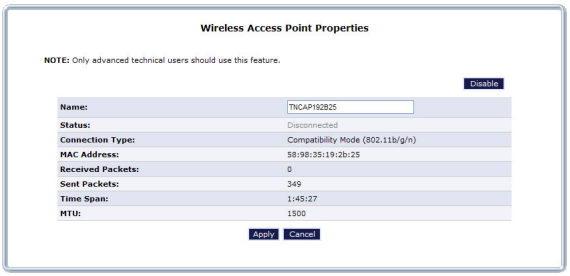
The **Wireless Access Point Properties** page allows you to:

- Disable/enable the wireless access point.
- View/ change the network name (SSID) of the wireless access point.
- View the properties of the wireless access point of the HBR.

Access

Proceed as follows:

1. On the **My Network** menu, click **Network Connections**.
2. The **Network Connections** table appears. Click **Wireless Access Point**.
3. The **Wireless Access Point Properties** page appears:



4. If you want to:
   - Turn off the wireless access point, click **Disable** in the upper-right corner.
   - Change the network name (SSID), type the new name in the **Name** box and click **Apply**.

5.2.3 Coax Properties

Introduction

A coax connection connects devices (such as set-top boxes) to the HBR using a coaxial cable.

The **Coax Properties** page allows you to:

- Disable/enable the coax connection.
- View/change the settings of the coax connection.
- View Statistics about the coax connection.

Accessing the Coax Properties page

Proceed as follows:

1. On the **My Network** menu, click **Network Connections**.
2. The **Network Connections** table appears. Click **Coax**.
3. The **Coax Properties** page appears:

Properties

The following properties are available:

- **Status**:
  Displays the status of the coax connection.
- **Network**:
  Displays the type of network.
- **Connection Type**:
  Displays the type of connection.
- **MAC Address**:
  Displays the unique hardware address of this interface.
- **IP Address Distribution**:
  To change the value, click **IP Address Distribution**. For more information, see *"8.1.22 IP Address Distribution" on page 112*.
- **Packets Received**:
  Displays the number of packets that were received on the coax interface.

- **Sent Packets**:
  Displays the number of packets that were sent over the coax interface.
- **Time Span**:
  Displays the time amount of time for which the coax interface has been connected.
- **Channel**:
  The channel used by the coax connection.

Controls

Click**:**

- **Settings** to change the following advanced settings:
  - Channel
  - Allowable frequency
  - Network Coordinator Mode
  - Transmit Power Control
  - Maximum Transmit Power
  - Privacy
- **Statistics** to view the statistics of your coax connection
- **Node statistics** to view the statistics of the devices that are using the coax connection.

5.2.4 Broadband Connection (LTE)

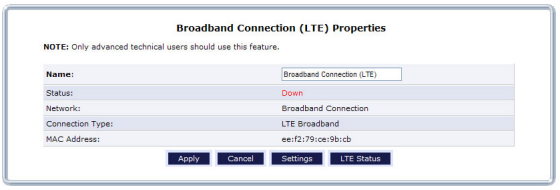
Introduction

The Broadband Connection (LTE) page allows you to access the broadband settings of the HBA.

Accessing the broadband LTE settings

Proceed as follows:

1. On the **My Network** menu, click **Network Connections**.
2. The **Network Connections** table appears. Click **Broadband Connection (LTE)**.
3. The **Broadband Connection (LTE) Properties** page appears.



6

GUI: Firewall Settings

6 GUI: Firewall Settings

Overview

This chapter describes the **Firewall Settings** pages.

Topic	Page
"6.1 General"	*56*
"6.2 Access Control"	*58*
"6.3 Port Forwarding"	*60*
"6.4 DMZ Host"	*61*
"6.5 Port Triggering"	*62*
"6.6 Remote Aministration"	*64*
"6.7 Static NAT"	*66*
"6.8 Advanced Filtering"	*67*
"6.9 Security Log"	*70*

6.1 General

Introduction

The firewall controls the flow of data between the local network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed) or rejected (barred) from passing through the HBR according to a set of rules. The rules are calculated to stop unwanted intrusions from the outside, while allowing local network users access to required Internet services.

Security levels

The HBR features three pre-defined firewall security levels:

Security Level	Internet Requests (Incoming Traffic)	Local network requests (Outgoing Traffic)
Maximum Security (High)	Blocked: No access to local network from Internet, except as configured in the Port Forwarding, DMZ host, and Remote Access screens.	Limited: Only commonly used services, such as web browsing and e-mail, are permitted. These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.
Typical Security (Medium)	Blocked: No access to local network from Internet, except as configured in the Port Forwarding, DMZ host, and Remote Access screens.	Unrestricted: All services are permitted, except as configured in the Access Control screen.
Minimum Security (Low)	Unrestricted: Permits full access from Internet to local network; all connection attempts permitted.	Unrestricted: All services are permitted, except as configured in the Access Control screen.

Configuring the firewall settings

Proceed as follows:

1 On the top menu, click **Firewall Setting**.

2 The HBR prompts you to confirm your choice. Click **Yes**.

3 The **General** page appears:

4 Select the firewall level of your choice.

5 Check the **Block IP Fragments** box to protect the local network from attacks that use fragmented data packets to sabotage the network.

VPN over IPSec and some UDP-based services make legitimate use of IP fragments. Do not select this check box if you are using one of these services.

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

6.2 Access Control

Introduction

The HBR has an integrated access control list that allows you to block access to specific services on the Internet.

You are able to configure:

- Which service has to be blocked (for example: no surfing on the Internet)
- Which computers should have this restriction (for example: your children's computers)
- When does this restriction need to be active (for example: after 10pm).

Accessing the Access Control page

Proceed as follows:

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **Access Control**.
4. The **Access Control** table appears:

To:

- Deactivate a rule, clear the check box next to the network device.
- Reactivate a rule, select the check box next to the network device.
- Edit a rule, click .
- Delete a rule, click .
- Add a new rule, click **Add** on the bottom of the table. For more information, see *"Adding new access control rules" on page 58*.

Adding new access control rules

Proceed as follows:

1. On the bottom of the **Access Control** table, click **Add**.
2. The **Add Access Control Rule** appears:

3 In the **Networked Computer / Device** list, select:

- The device that you would like to block from using the service
- **User Defined** if the device is not listed, or you want to create a group of devices. Click Add to define the new device or device group and follow the instructions.

Repeat this step for each device that you want to add.

4 In the **Protocol** list, select the protocol that you want to block.

The list contains the most frequently used protocols. To view the full list, select **Show All Services** in the **Protocol** list.

5 In the **When should this rule occur** list, select either of the following:

- **Always** to make this a permanent rule.
- **User Defined** to specify the time frames in which this rule will be applied. The configuration procedure is similar to the one described in *"8.1.20 Scheduler Rules" on page 108*.

6 Click **Apply** to activate the rule.

6.3 Port Forwarding

Introduction

In its default state, the HBR blocks all external users from connecting to, or communicating with the network, making it safe from hackers who may try to intrude on the network and damage it.

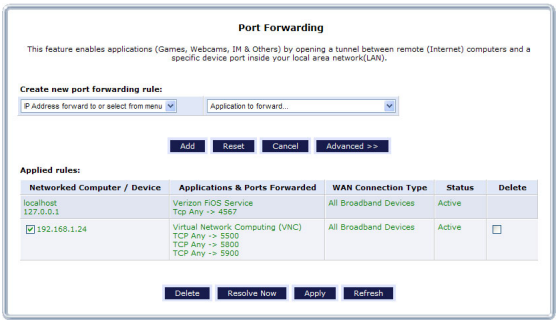
However, the network can be exposed to the Internet in certain limited and controlled ways to enable some applications to work from the local network (game, voice, and chat applications, for example) and to enable Internet access to servers in the network. Port forwarding (sometimes referred to as local servers) supports both of these functions.

To grant Internet users access to servers inside the local network, each service provided, as well as the computer providing it, must be identified.

Accessing the Port Forwarding page

Proceed as follows:

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **Port Forwarding**.
4. The **Port Forwarding** page appears:



Creating a new port forwarding rule

Under **Create new port forwarding rule**:

1. Select either of the following:
   - The device for which you want to create the rule.
   - **Specify IP** to manually enter the IP address for the device that you want to create the rule for.
2. Click **Add** to activate the rule.

6.4 DMZ Host

Introduction

The DMZ (De-Militarized Zone) host feature allows one device on the network to operate outside the firewall. To designate a DMZ host:

- To use an Internet service, such as an online game or video-conferencing program, not present in the Port Forwarding list and for which no port range information is available.
- To expose one computer to all services without restriction or security.

Only one network computer can be a DMZ host at any time.

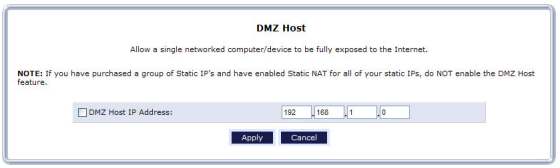
WARNING!

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

Assigning a DMZ Host

Proceed as follows:

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **DMZ Host**.
4. The **DMZ Host** page appears:



Select the check box on the left and enter the IP address of the host that you want to use as a DMZ host.

5. Click **Apply**.

Disabling the DMZ host

If, at any point, you want to disable the DMZ host:

1. Browse to the **DMZ Host** page.
2. Clear the check box on the left.
3. Click **Apply**.

6.5 Port Triggering

Introduction

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, inbound traffic is allowed to arrive at a specific network host using ports different than those used for the outbound traffic. The outbound traffic triggers which ports inbound traffic is directed to.

Example

Scenario

1. A local user accesses a remote gaming server using UDP protocol on port 2222.
2. The gaming server responds by connecting the user using UDP on port 3333 when starting gaming sessions.

Problem

- The firewall blocks inbound traffic by default. So the incoming message from the game server (UDP:3333) will be blocked.
- If it would pass the firewall, the message will be addressed to the public IP address of the HBR. Since the HBR did not have any previous UDP messages on port 3333, it will not know to which device it should forward the message.

Solution

To solve this problem, we use port triggering. This means that if the HBR detects traffic on the trigger port (in our case UDP:2222) it will automatically open a specific port (in our example: UDP:3333).

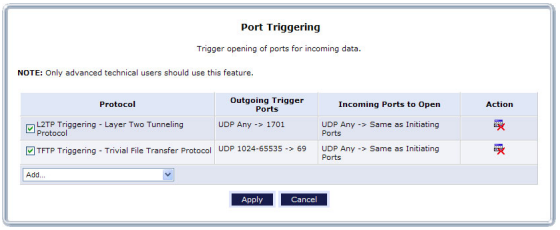
The HBR will also know that if it receives a UDP message on port 3333 it should be forwarded to the same device that sent a request via UDP port 2222.

Accessing the Port Triggering page

Proceed as follows:

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **Port Triggering**.

4 The **Port Triggering** page appears:



Click:

- **Add** to create a new port triggering rule.
- to delete a port triggering rule.

Adding a port triggering rule

On the **Port Triggering** page:

1 On the bottom of the table, click the **Add** list at the bottom of the page.

2 In the **Add** list, select either of the following:

- One of the pre-defined service.
- **User Defined** to create a new services definition if your service is not listed and specify the following information:
  - **Service Name**
    The name that you want to use to refer to this service.
  - **Outgoing Trigger Ports**
    Enter the port number(s) that the local host will be using to contact the remote host. When the HBR detects outbound traffic on this port, the HBR will open the ports specified in your rule.
  - **Incoming Ports to open**
    These ports will be opened when the rule is triggered. Incoming traffic arriving at this port will we forwarded to the host that triggered the rule.

3 The port triggering rule is now created.

6.6 Remote Aministration

WARNING

Enabling Remote Administration puts your local network at risk from outside attacks.

Introduction

On the **Remote Administration** page, you can enable/disable:

- Incoming WAN Access to the Telnet Server.
- Incoming WAN Access to Web-Management.
- Diagnostic Tools.

Telnet

Telnet is used to create a command-line session and gain access to all system settings and parameters using a text-based terminal.

Web Management

Web Management is used to obtain access to the HBR GUI and gain access to all settings and parameters, using a web browser. Both secure (HTTPS) and non-secure (HTTP) access is available.

Telnet and Web Management remote administration access may be used to modify or disable firewall settings. Local IP addresses and other settings can also be changed, making it difficult or impossible to access the HBR from the local network. Therefore, remote administration access to Telnet or Web Management services should be activated only when absolutely necessary.

Diagnostic Tools

Diagnostic Tools are used for troubleshooting and remote system management by a user or the ISP.

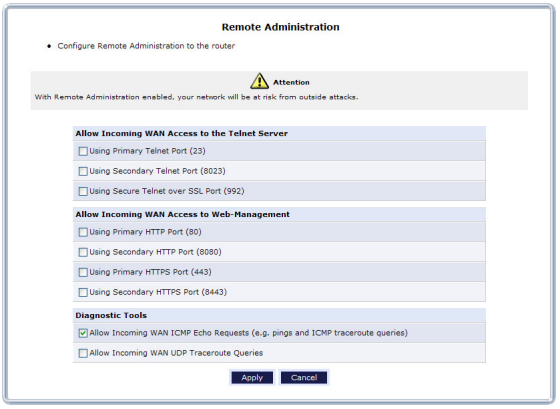
Encrypted remote administration is performed using a secure SSL connection, and requires an SSL certificate. When accessing the HBR for the first time using encrypted remote administration, a warning appears regarding certificate authentication because the HBR's SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue. Even though this message appears, the self-generated certificate is safe and provides a secure SSL connection.

Accessing the remote administration page

Proceed as follows:

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **Remote Administration**.

4 The **Remote Administration** page appears.



5 Select the services that you want to allow.

6 Click **Apply**.

6.7 Static NAT

Introduction

Static NAT allows you to direct traffic coming from the Internet to a specific local device.

For example: if you are running a web server, you want all incoming web requests to be directed to your web server.

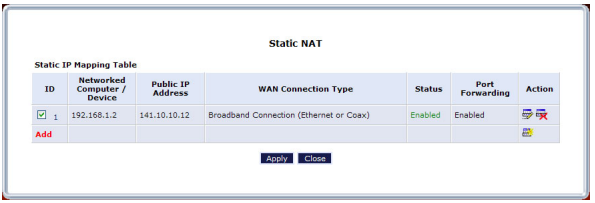
Accessing the Static NAT page

Proceed as follows:

1 On the top menu, click **Firewall Settings**.

2 The HBR prompts you to confirm your choice. Click **Yes**.

3 The **Static NAT** page appears.



Creating a new Static NAT entry

1 Click **Add** or .

2 The **Edit NAT/NAPT Rule** page appears.

3 Under **Local Host** do either of the following:

- Select **Specify Address**, and type the address of the local host.
- Select the local host from the list.

4 In the **Public IP address** box, type the public IP address on which the requests will be received.

5 If you want to make sure that the request is forwarded to the same port that it was received on, select **Enable Port Forwarding For Static NAT** and select the port forwarding rule you need.

To create new port forwarding rules, click **Port Forwarding Rules** in the **Advanced** menu. For more information see *"8.1.18 Port Forwarding Rules" on page 105*.

6 Click **Apply**.

6.8 Advanced Filtering

WARNING

Only advanced technical users should use this feature.

Introduction

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. Specific input and output rules can be defined, the order of logically similar sets of rules controlled, and distinctions made between rules that apply to the Internet and rules that apply to local network devices.

Rule sets

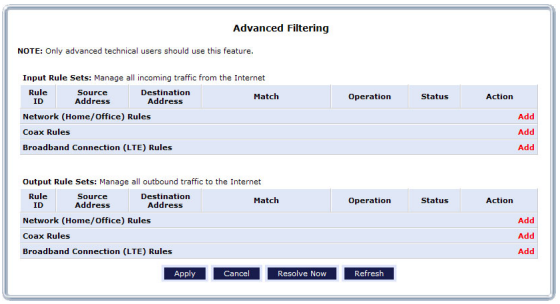
There are numerous rules automatically inserted by the firewall to provide improved security and block harmful attacks. The pre-populated rules displayed here are required for operation on the Verizon Network.

Two sets of rules can be configured:

- **Input Rule Sets** allow you to create rules for inbound traffic.
- **Output Rule Sets** allow you to create rules for outbound traffic.

Accessing the Advanced Filtering page

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **Advanced Filtering**.
4. The **Advance Filtering** page appears.



Click:

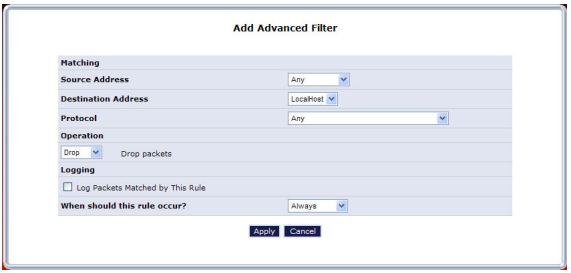
- **Add** to add a new firewall rule.
- **Refresh** to update the rule set tables.

Adding a rule

On the Advanced filtering page:

1 Click **Add** next to the interface for which your want to create a rule.

2 The **Add Advanced Filter** page appears.



The following sections are available for configuration:

- **Matching**:
  To apply a firewall rule, a match must be made between IP addresses or ranges and ports. Use the **Source Address** and **Destination Address** drop-down lists to define the coupling of source and destination traffic. Port matching will be defined when selecting protocols. For example, if the FTP protocol is selected, port 21 will be checked for matching traffic flow between the defined source and destination IPs.
- **Operation**:
  This is where the action the rule will take is defined. Select one of the following radio buttons:
  - **Drop**
    Deny access to packets that match the source and destination IP addresses and vCP reset to the origination peer.
  - **Accept**
    Allow access to packets that match the source and destination IP addresses and protocol ports defined in upper section of the screen. The data transfer session will be handled using Stateful Packet Inspection (SPI).
  - **Accept Packet**
    Allow access to packets that match the source and destination IP addresses and protocol ports defined in upper section of the screen. The data transfer session will not be handled using Stateful Packet Inspection (SPI), so other packets that match this rule will not be automatically allowed access. This setting is useful when creating rules that allow broadcasting.
- **Logging**:
  Select **Log Packets Matched by This Rule** to add entries relating to this rule to the security log. For more information, see *"6.9 Security Log" on page 70*.
- **When should this rule occur?**
  Allows you to specify when the rule must be active. Select:
  - **Always** if advanced filtering needs to be active all the time.

- **User Defined** if the rule will only be active at certain selected times. Then click **Add** to add a schedule rule. The procedure is similar to the one described in *"8.1.20 Scheduler Rules" on page 108*.

3 Click **Apply**.

6.9 Security Log

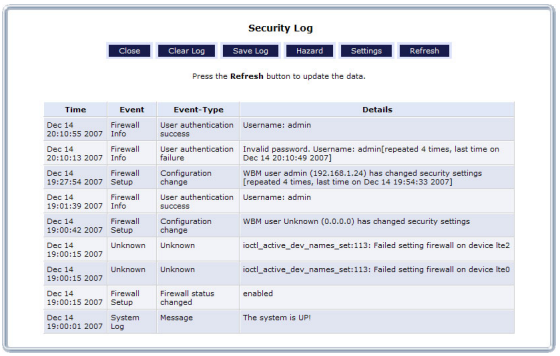
Introduction

The security log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (GUI or Telnet terminal), firewall configuration, and system start-up.

Accessing the Security Log page

Proceed as follows:

1. On the top menu, click **Firewall Settings**.
2. The HBR prompts you to confirm your choice. Click **Yes**.
3. On the left menu, click **Security Log**.
4. The **Security Log** page appears.



Security log table

The security log table provides you the following information:

- **Time**:
  The time (based on the HBR's date and time settings) the event occurred.
- **Event**:
  There are three kinds of events listed in the system log: **Firewall Info**, **Firewall Setup**, and **System Log**.
- **Event-Type**:
  The "Details" column displays more information about the packet or the event, such as protocol, IP addresses, ports, etc.
- **Details**:
  Displays a textual description of the event

7

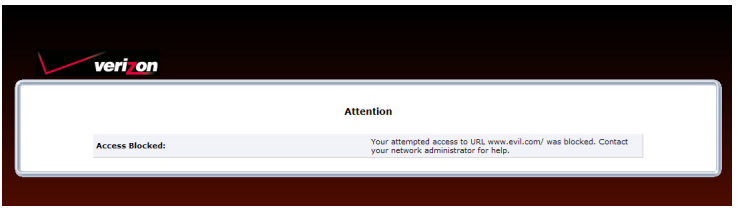
GUI: Parental Control

7.1 Parental Control

Introduction

The **Parental control** page allows you to:

- Block all Internet access.
  Users will not be able to access the internet unless you define exceptions to this rule (for example: allows www.verizon.com).
- Block websites:
  When the user tries to access the blocked page, he will get the standard page announcing that this page has been blocked.



- Redirect a website to another website.
  When the user tries to access the blocked page he/she will be redirected to the page of your choice (for example: an intranet page explaining the intranet policy).

Creating a new rule

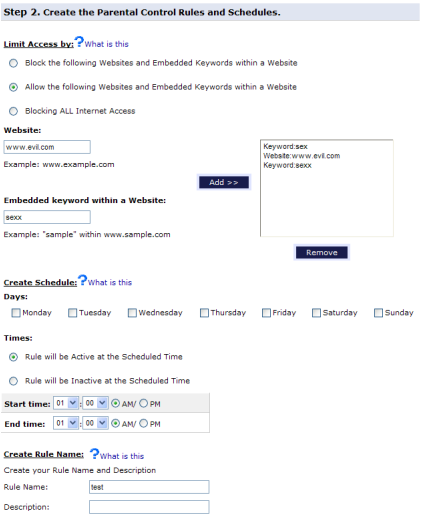
Proceed as follows:

1. On the top menu, click **Parental Control**.
2. The **Parental Control** page appears.
3. Under **Step 1**, complete the following steps:

   a. In the **Networked Computer/Device** list select the devices that you want to create the new rule for. To select multiple entries, hold down the CTRL key while selecting the entries.

   b. Click **Add**. The devices are now in the **Selected Devices** list.

4 Under **Step 2**, complete the following steps:



a Select either of the following:

- **Block the following Websites and Embedded Keywords within a Website** to create a new blocking rule**.**
- **Allow the following Websites and Embedded Keywords within a Website** to specify an exception on a blocking rule.
- **Blocking ALL Internet Access**.

b Enter the URL for the Website that you want to block in the **Website** box (for example: www.evil.com) and/or enter a keyword in the **Embedded keyword within a Website** list (for example: cracks, hacks and so on). Click **Add**.

c If needed add other website and/or keywords

d Under **Create Schedule**, you can specify when the rule will be active or inactive.

e Under **Create Rule Name**, enter a **Rule Name** and **Description**.

5 Click **Apply**.

7.2 Rule Summary

Introduction

The **Rule Summary** page allows you to view or change the existing parental control rules.

Changing a parental control rule

Proceed as follows:

1 On the **Parental Control** menu, click **Rule Summary**.

2 The **Rule Summary** page appears.

3 Click:

- to view the rule settings.
- to edit the rule settings.
  For more information, see *"7.1 Parental Control" on page 72*.
- to delete the rule.

8

GUI: Advanced Settings

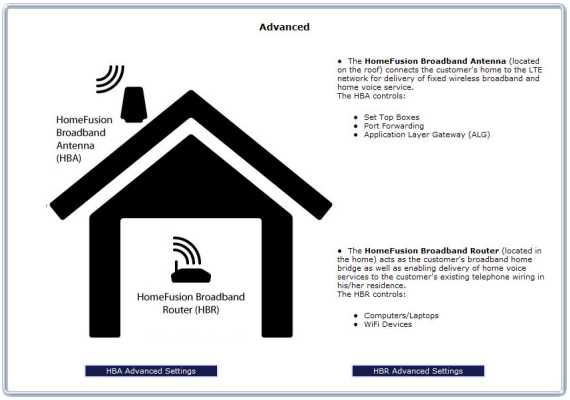
Introduction

The **Advanced** page allows you to configure the more advanced services of both the HBA and the HBR.

To access the **Advanced** page, proceed as follow:

1 On the top menu, click **Advanced**.

2 The **Advanced** page appears.



3 On the bottom of this page, click:

- **HBA Advanced Settings** to configure the settings of the HBA.
  For more information, see *"8.1 HBA Advanced Pages" on page 77*.
- **HBR Advanced Settings** to configure the settings of the HBA.
  For more information, see *"8.2 HBR Advanced Pages" on page 114*.

8.1 HBA Advanced Pages

Introduction

The **Advanced HBA** page contains links to the different configuration pages. These pages are grouped by topic:

- *Utilities*
- *DNS Servers*
- *Configuration*
- *Upgrade*
- *Network services*
- *Date and time*
- *Router*

Utilities

Click:

- **Diagnostics** to perform diagnostic tests on the HBA.
  For more information, see *"8.1.1 Diagnostics" on page 79*.
- **Restore Defaults** to reset the HBA to its default settings.
  For more information, see *"8.1.2 Restore Defaults" on page 81*.
- **Reboot Router** to restart the HBA.
  For more information, see *"8.1.3 Reboot the Router" on page 83*.
- **ARP Table** to display active devices and their IP and MAC addresses.
  For more information, see *"8.1.4 ARP Table" on page 84*.
- **Quality of Service (QoS)** to view the QoS settings.
  For more information, see *"8.1.5 Quality of Service (QoS)" on page 85*.
- **Local Administration** allow users to access the GUI from your local network.
  For more information, see *"8.1.6 Local Administration" on page 86*.
- **Remote Administration** allow users to access the GUI from the Internet.
  For more information, see *"8.1.7 Remote Administration" on page 87*.

DNS Servers

Click:

- **Dynamic DNS** to configure Dynamic DNS settings.
  For more information, see *"8.1.8 Dynamic DNS" on page 89*.
- **DNS Server** to manage the local (LAN) network for host name and IP address.
  For more information, see *"8.1.9 DNS Server" on page 91*.

Configuration

Click:

- **Configuration File** to save or restore a configuration.
  For more information, see *"8.1.10 Configuration File" on page 93*
- **System Settings** to change the system settings of the HBA.
  For more information, see *"8.1.11 System Settings" on page 95*.

Upgrade

Click **Firmware Upgrade** to upgrade your HBA with the latest software.

For more information, see *"8.1.12 Firmware Upgrade" on page 98*.

Network services

Click:

- **Network Objects** to create and manage network objects (discrete LAN subsets).
  For more information, see *"8.1.13 Network Objects" on page 99*.
- **Universal Plug & Play** to configure the interaction with other UPnP devices.
  For more information, see *"8.1.14 Universal Plug and Play" on page 101*.
- **SIP ALG** to enable/disable the SIP ALG.
  For more information, see *"8.1.15 SIP ALG" on page 102*.
- **MGCP ALG** to enable/disable the MGCP ALG.
  For more information, see *"8.1.16 MGCP ALG" on page 103*.
- **IGMP Proxy** to configure the IGMP proxy settings.
  For more information, see *"8.1.17 IGMP Proxy" on page 104*.
- **Port Forwarding Rules** to configure the port forwarding rules.
  For more information, see *"8.1.18 Port Forwarding Rules" on page 105*.

Date and time

Click:

- **Date and Time** to configure the HBA clock and calendar of the HBA.
  For more information, see *"8.1.19 Date and Time" on page 107*.
- **Scheduler Rules** to schedule the activation of firewall rules.
  For more information, see *"8.1.20 Scheduler Rules" on page 108*.

Router

Click:

- **Routing** to manage routing policies.
  For more information, see *"8.1.21 Routing" on page 110*.
- **IP Address Distribution** to manage the IP addresses of devices on the network.
  For more information, see *"8.1.22 IP Address Distribution" on page 112*.

8.1.1 Diagnostics

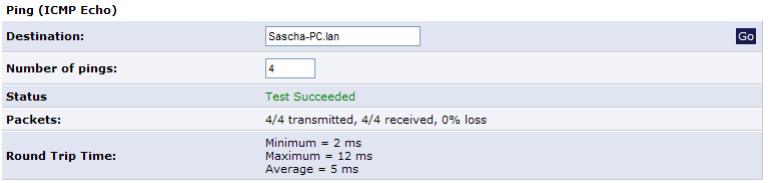
Introduction

The **Diagnostics** page allows you to let the HBA ping a device or website. Ping is used to test if a host (for example, a website or a computer) is reachable.

Procedure

To diagnose network connectivity:

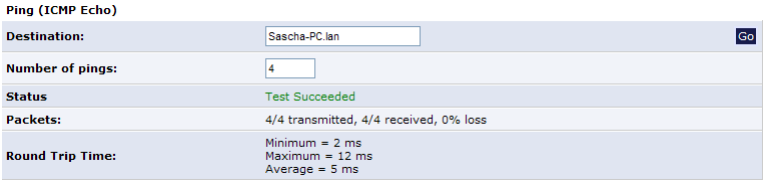
1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Diagnostics**.
4. The **Diagnostics** page appears.



In the **Destination** box, type one of the following:

- The DNS name (for example: www.google.com) or IP address (for example: 141.11.249.33) of a website.
- The DNS name (for example: Sascha-PC.lan) or IP address (for example: 192.168.1.3) of network device.

5. If needed change the number of pings in the **Number of pings box**.
6. Click **Go**.
7. The HBA is now pinging the destination. You can follow the progress in the Packets box.
8. At the end of the test the results appear.



Under:

- **Status**, you can see if the test was successful or not.
- **Packets**, you can see the number packets that were received and the percentage of packets that were lost.

- **Round trip time**, you can see the amount of time it took for the packet to get back to the HBA.

8.1.2 Restore Defaults

Introduction

The **Restore Defaults** page allows you to restore the HBA to the factory defaults.

As described in *"1.1 Basic Concepts" on page 3*, both the HBR and the HBA are responsible for bringing the Verizon services into your home.

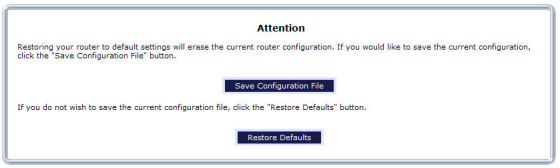
It is therefore important to know that a reset to defaults may influence specific services. If you reset:

- The HBR, local network settings such as changes to WiFi SSID or keys, the LAN address range, or time zone/DST will be lost.
- The HBA, settings of Internet-related services such as Firewall, port forwarding, and Parental controls would be reset.

Resetting the HBA

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Restore Defaults**.
4. The **Attention** page appears.



5. Optionally, click **Save Configuration File** to save the current configuration of the HBA. This allows you to restore this configuration at any time. For more information, see *"8.1.10 Configuration File" on page 93*.
6. Click **Restore Defaults**.
7. The HBA prompts you to confirm your choice.

Click **Restore OK**.

8 The HBA restores the factory defaults and restarts.

8.1.3 Reboot the Router

Introduction

The **Reboot the Router** page allows you to restart your HBA.

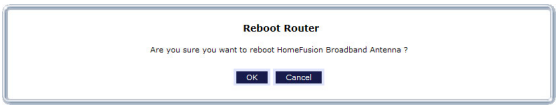
WARNING

During the reboot, all services provided by the HBA will be unavailable.

Procedure

To reboot the HBA:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Reboot Router**.
4. The HBA prompts you to confirm the reboot.



Click **OK**.

5. The HBA restarts. It may take a few minutes before all services become available.

8.1.4 ARP Table

ARP

The **Address Resolution Protocol** is a protocol that translates the IP address of a network device into its MAC address.

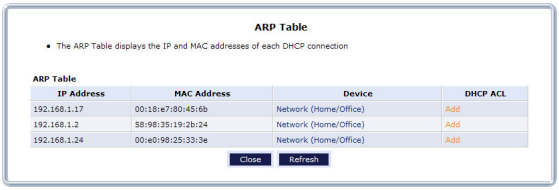
The ARP table page

The **ARP Table** page provides you a mapping between the IP address and the MAC address of the device that is using this IP address.

Viewing the ARP table

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **ARP Table**.
4. The **ARP Table** page appears.



The following fields are available:

- **IP Address**
- **MAC Address**
- **Device**
  Displays the network interface that the device is using. For more information, see *"5.2 Network Connections" on page 48*.
- **DHCP ACL**
  Click **Add** to add this device to the access control list. For more information, see *"6.2 Access Control" on page 58*.

8.1.5 Quality of Service (QoS)

QoS

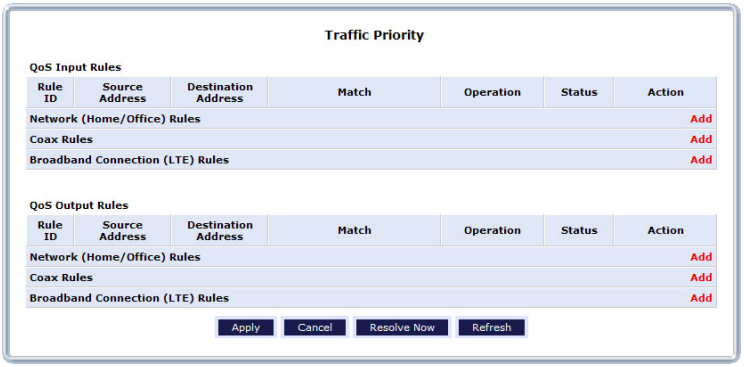
Quality of Service (QoS) is a system that allows you to assign a higher or lower priority to specific types of data.

For example: Data destined for your Setup Box must have higher priority than normal traffic.

Accessing the QoS pages

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Quality of Service (QoS)**.
4. The **Quality of Service (QoS)** pages appears.



8.1.6 Local Administration

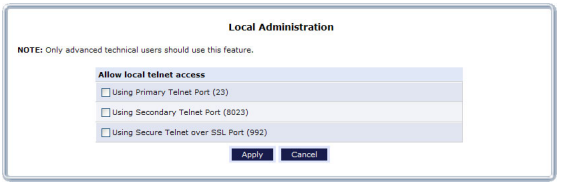
Introduction

The Local Administration page allows you to configure telnet access to your HBA.

Accessing the QoS pages

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Local Administration**.
4. The **Local Administration** page appears.



8.1.7 Remote Administration

WARNING

Enabling Remote Administration puts your local network at risk from outside attacks.

Introduction

On the **Remote Administration** page, you can enable/disable:

- Incoming WAN Access to the Telnet Server.
- Incoming WAN Access to Web-Management.
- Diagnostic Tools.

Telnet

Telnet is used to create a command-line session and gain access to all system settings and parameters using a text-based terminal.

Web Management

Web Management is used to obtain access to the HBR GUI and gain access to all settings and parameters, using a web browser. Both secure (HTTPS) and non-secure (HTTP) access is available.

Telnet and Web Management remote administration access may be used to modify or disable firewall settings. Local IP addresses and other settings can also be changed, making it difficult or impossible to access the HBR from the local network. Therefore, remote administration access to Telnet or Web Management services should be activated only when absolutely necessary.

Diagnostic Tools

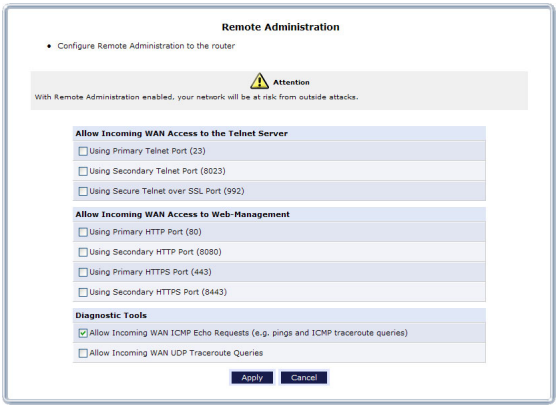
Diagnostic Tools are used for troubleshooting and remote system management by a user or the ISP.

Encrypted remote administration is performed using a secure SSL connection, and requires an SSL certificate. When accessing the HBR for the first time using encrypted remote administration, a warning appears regarding certificate authentication because the HBR's SSL certificate is self-generated. When encountering this message under these circumstances, ignore it and continue. Even though this message appears, the self-generated certificate is safe and provides a secure SSL connection.

Accessing the remote administration page

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Remote Administration**.
4. The **Remote Administration** page appears.



5. Select the services that you want to allow.
6. Click **Apply**.

8.1.8 Dynamic DNS

Introduction

The Dynamic DNS service allows you to assign a dynamic DNS host name (for example mywebpage.dyndns.org) to a broadband connection even if it is using a dynamic IP address. As soon as the device gets a new IP address, the dynamic DNS server updates its entry to the new IP address.

What you need

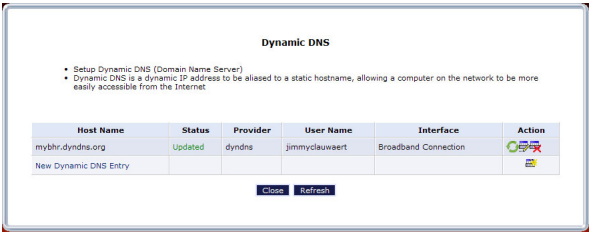
Before you can configure Dynamic DNS, you first have to create an account at a Dynamic DNS service provider. For example:

- www.dyndns.org
- www.no-ip.com
- www.dtdns.com

Accessing the Dynamic DNS page

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Dynamic DNS**.
4. The **Dynamic DNS** page appears.

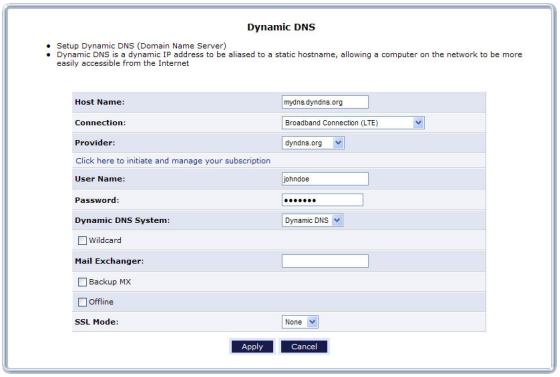


Creating a new Dynamic DNS entry

On the **Dynamic DNS** page, proceed as follows:

1. Click **New Dynamic DNS** entry.

2 The **Dynamic DNS Host Entry** page appears.



3 In the **Host Name** box, type the host name that you purchased at the Dynamic DNS provider (for example: myhbr.dyndns.org).

4 In the **User Name** box type the user name of your Dynamic DNS account.

5 In the **Password** box, type the password of your Dynamic DNS account.

6 Optionally, you can:

- Select **Wildcard** to support all URLs that contain your host name (for example, newname.myhbr.dyndns.org).
- Enter your mail exchange server in the **Mail Exchanger** box to redirect all mail arriving at the hostname address to the specified mail exchange server.
- Select **Backup MX** to specify a backup mail exchange server.
- Select **Offline** to disable your Dynamic DNS hostname at the Dynamic DNS provider.

7 Click **Apply**.

8.1.9 DNS Server

Introduction

The Domain Name System (DNS) translates domain names into IP addresses and vice versa. The HBA's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network, the DNS server learns its name and automatically adds it to the DNS table. Other network users can immediately communicate with this computer using either its name or its IP address.

Services offered

The following services are provided by the DNS server of the HBA:

- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the local network simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using the HBA's GUI.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

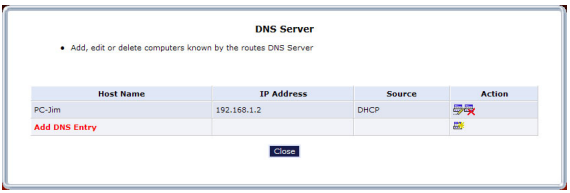
Configuration

The DNS Server does not require configuration. However, the list of computers known by the DNS can be viewed or a new computer can be added to the list.

Viewing DNS Table

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **DNS Server**.
4. The **DNS Server** page appears.



Click:

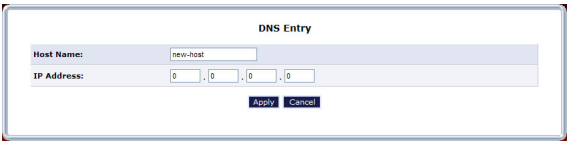
- **Add** or to add a new entry to the list. For more information, see *"Adding a DNS entry" on page 92*.

- to edit an existing DNS entry.
- to delete an existing DNS entry.

Adding a DNS entry

On the **DNS Server** page:

1. Click **Add DNS Entry** at the bottom of the page.
2. The **DNS Entry** page appears.



3. Enter a DNS name for the host in the **Host Name** box.
4. Enter the IP address of the host in the **IP Address** box.
5. Click **Apply**.

Accessing a device via its DNS name

Once a device is listed in the DNS table you can access it via **<DNS. name>.<DNS suffix>**.

Example

Your host is using **PC-Jim** as DNS name and **lan** as DNS suffix (this is the default DNS suffix).

If this host is running a web server, you can access it via http://PC-Jim.lan.

If this host is a Windows computer with shared files on it, you can access these shared files via \\PC-Jim.lan.

8.1.10 Configuration File

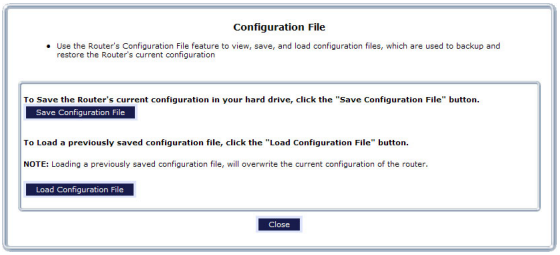
Backing up your current configuration

Once have successfully configured your HBA, it is recommended that you backup your configuration. This allows you to return to this configuration whenever you need it (for example after misconfiguration, or a reset to the factory defaults).

Backing up your current configuration

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Configuration File**.
4. The **Configuration File** page appears.



5. Click the **Save Configuration File**.
6. A window appears to prompt you to save your file. Save your file to the location of your choice.

WARNING!

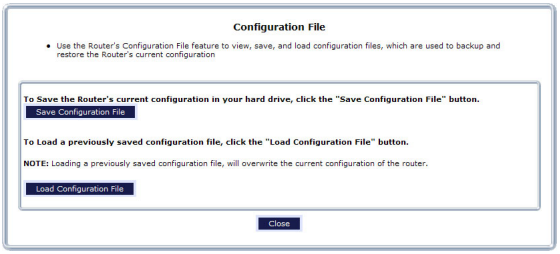
Manually editing a configuration file can cause the HBA to malfunction or become completely inoperable.

Restoring a previously saved configuration

Proceed as follows:

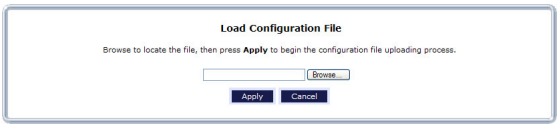
1. On the top menu, click **Advanced** and then click **Yes** to confirm that you want to access the advanced settings.
2. Under , click **Configuration File**.

3 The **Configuration File** page appears.



4 Click the **Load Configuration File**.

5 The **Load Configuration File** page appears.



6 A window appears to prompt you to save your file. Save your file to the location of your choice.

8.1.11 System Settings

Introduction

The **System Settings** page allows you to configure various system and management parameters.

The page is divided into the following groups:

- *Router Status*
- *HomeFusion Broadband Antenna*
- *Management Application Ports*
- *System Logging*
- *Security Logging*
- *Outgoing Mail Server*

Router Status

Under **Router Status**, the following properties are available:

- **HomeFusion Broadband Antenna's Hostname**
  Specify the HBA's host name by entering it into the text box. The host name is used in combination with the **Local Domain** to access the HBA.
- **Local Domain**
  Specify the network's local domain by entering it into this text box. The **Local Domain** is used in combination with the **Wireless Broadband Router's Hostname** to access the HBA.

So if you change the host name to **router** and the local domain to **home**, you will have to access the GUI using http://router.home.

HomeFusion Broadband Antenna

Under **HomeFusion Broadband Antenna**, the following properties are available:

- **Automatic Refresh of System Monitoring Web Pages**
- **Prompt for Password When Accessing via LAN**
- **Warn User Before Configuration Changes**
  Select this option if you want to receive a warning before network changes are applied.
- **Session Lifetime**
  Specifies how long the session will stay open when there is no activity on the GUI.
- **Configure a number of concurrent users that can be logged into the router**
  Allows to limit the number of users that can access the HBA at the same time. Select the number of users from the drop-down list.

Management Application Ports

Under **Management Application Ports**, you can configure the port numbers of the management services:

- Primary/secondary HTTP ports
- Primary/secondary HTTPS ports
- Primary/secondary Telnet ports
- Secure Telnet over SSL ports

System Logging

Under **System Logging**, you can configure the following items:

- **Enable Logging**
  Click in this check box to activate system logging.
- **Low Capacity Notification Enabled**
  Select this check box to activate low capacity notification (works in tandem with **Allowed Capacity Before Email Notification** and **System Log Buffer Size** options).
- **Allowed Capacity Before Email Notification**
  Enter the percentage of system log buffer capacity reached to trigger an e-mail notification.
- **System Log Buffer Size**
  Enter the size of the system log buffer in this text box.
- **Remote System Notify Level**
  This feature is used to specify the type of information received for remote system logging. Options include **None**, **Error**, **Warning**, and **Information**.

Security Logging

Under **Security Logging**, you can configure the following items:

- **Low Capacity Notification Enabled**
  Select this check box to activate low capacity notification (works in tandem with **Allowed Capacity Before Email Notification** and **System Log Buffer Size** options).
- **Allowed Capacity Before Email Notification**
  Enter the percentage of system log buffer capacity reached to trigger an e-mail notification.
- **System Log Buffer Size**
  Enter the size of the system log buffer in this text box.
- **Remote System Notify Level**
  This feature is used to specify the type of information received for remote system logging. Options include **None**, **Error**, **Warning**, and **Information**.

Outgoing Mail Server

Under **Outgoing Mail Server**, you can configure the outgoing mail server options. This server is used to format and send system and security log e-mail notifications. The following settings are available for configuration:

- **Server**
  Enter the host name of the outgoing (SMTP) server in this text box.
- **From Email Address**
  Email notifications require a "from" address. Enter a "from" email address in this text box.
- **Port**
  Enter the port number of the email server in this text box.
- **Server Requires Authentication**
  If the email server requires authentication, click in this check box, then enter a user name and password in the **User Name** and **Password** text boxes that appear.

8.1.12 Firmware Upgrade

Introduction

The **Firmware Upgrade** page allows you to update your HBA with the latest software.

Verizon Wireless automatically updates the software of your HBA. So you normally do not need to use this page.

Update mechanisms

You are able to upgrade your HBA:

- From the Internet
  The HBA checks if for new software and allows you to initiate the upgrade.
- Using an official upgrade file provided by Verizon Wireless.

Service interruption

Upgrading the software *requires a restart* of the HBA. This means that all services provided by the HBA will be unavailable during that time.

Access the Firmware Upgrade Page

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Firmware Upgrade**.
4. The **Firmware Upgrade** page appears.

8.1.13 Network Objects

Introduction

A network object is used to define a part of the HBA's network (a group of computers, for example) by MAC addresses, IP addresses, and/or host names. The defined part becomes a "network object," and settings, such as configuring system rules, can be applied to all the devices defined as part of the network object at once. For example, instead of setting the same website filtering configuration to five computers one at a time, the computers can be defined as a network object, and website filtering configuration can then be applied to all the computers simultaneously.

Network objects can be used 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 the rule application more persistent against network configuration settings.

Defining a new network object

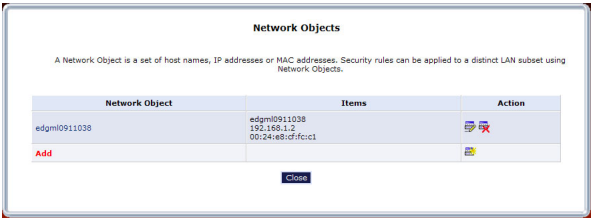
Proceed as follows:

1 On the top menu, click **Advanced**.

2 The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.

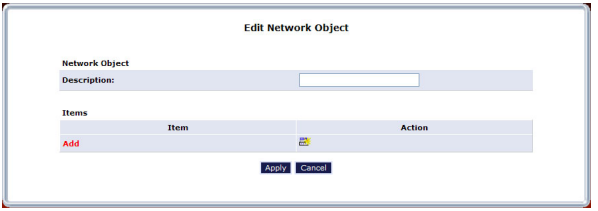
3 Under , click **Network Objects**.

4 The **Network Objects** page appears.



Click **Add**.

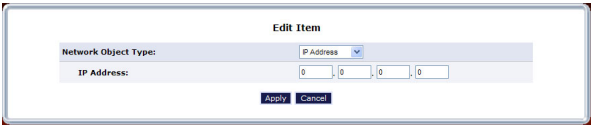
5 The **Edit Network Object** page appears.



6 Specify a name for the network object in the **Description** text box.

7 Click **Add**.

8 The **Edit Item** screen appears.



Select the type of network object type from the **Network Object Type** list box. Options include:

- IP address
- MAC Address
- Host Name

Click **Apply**.

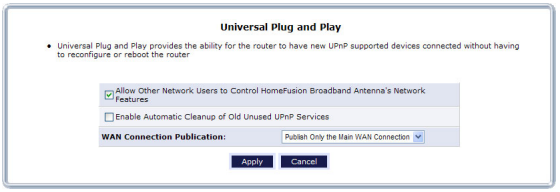
8.1.14 Universal Plug and Play

Introduction

UPnP is designed to automate the installation and configuration of a (small) network as much as possible. This means that UPnP-capable devices can join and leave a network without any effort of a network administrator.

Configuring UPnP

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Universal Plug and Play**.
4. The **Universal Plug and Play** page appears.



The following options are available:

- Select **Allow Other Network Users to Control Wireless Broadband Router's Network Features** to enable UPnP and allow UPnP services to be defined on any of the network hosts.
- Select **Enable Automatic Cleanup of Old Unused UPnP Services** to enable automatic cleanup of invalid rules. When enabled, the HBA regularly checks if all the UPnP services and rules are still valid. Old and unused UPnP defined services will be removed, unless a user-defined rule depends on it.
- In the **WAN Connection Publication** list, you can specify whether only the main or all broadband connections will have UPnP enabled.

5. Make your changes and click **Apply**.

8.1.15 SIP ALG

Introduction

The SIP ALG page allows you to enable the SIP ALG on your HBA.

Accessing the SIP ALG page

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **SIP ALG**.
4. The **SIP ALG** page appears.

8.1.16 MGCP ALG

Introduction

The MGCP ALG page allows you to enable the MGCP ALG on your HBA.

Accessing the MGCP ALG page

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **MGCP ALG**.
4. The **MGCP ALG** page appears.

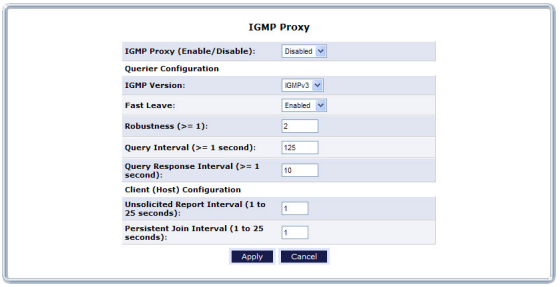
8.1.17 IGMP Proxy

Introduction

The **IGMP Proxy** page allows you to change the IGMP Proxy settings.

Accessing the IGMP Proxy Settings page

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **IGMP Proxy**.
4. The **IGMP Proxy** page appears.



8.1.18 Port Forwarding Rules

Introduction

The **Port Forwarding Rules** page allows you to define translation rules for specific protocols. This avoids having to re-enter all the port numbers each time you need to configure something for this service.

These definitions can then be used for services like:

- **Access Control**:
  For more information, see *"6.2 Access Control" on page 58*.
- **Port Forwarding**:
  For more information, see *"6.3 Port Forwarding" on page 60*.
- **Static NAT**:
  For more information, see *"6.2 Access Control" on page 58*.

Accessing the Port Forwarding Rules page

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Port Forwarding Rules**.
4. The **Port Forwarding Rules** page appears.

5. If you want to:
   - Edit an existing rule, click or the name of the protocol.

- Delete an existing rule, click .
- View a full list of rules, click the **Advanced** button under the table.

8.1.19 Date and Time

Introduction

The Date and Time page allows you to configure the date and time that the HBA will be using for:

- Scheduler Rules
  For more information, see *"8.1.20 Scheduler Rules" on page 108*.
- System logging
  For more information, see *"9.2.1 System Log" on page 130*.

Accessing the Date and Time page

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Date and Time**.
4. In the **Time Zone** list, select your time zone or select Other to create one if your time zone is not listed.
5. Under **Daylight Saving Time** you can change the daylight saving settings.
6. Under **Automatic Time Update**:
   - Select **Enabled** if you want the HBA to synchronize its time settings with a Network Time Protocol (NTP) server. This guarantees that you will always be using the correct time.
   - Clear **Enabled** if you want to set the time manually. Use the **Clock Set** button on the bottom of the page to enter the correct date and time.
7. Click **Apply**.

8.1.20 Scheduler Rules

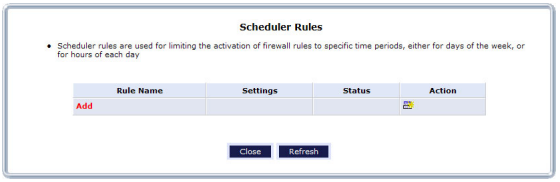
Introduction

The **Scheduler Rules** page allows you to limit the activation of firewall rules to specific time periods, either for days of the week, or for hours of each day.

Creating a scheduler rule

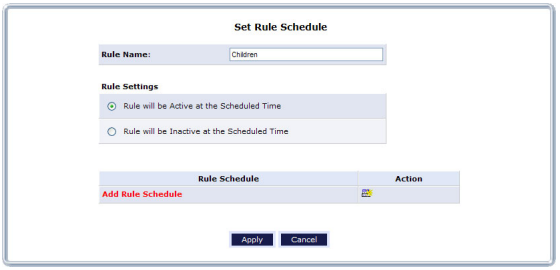
To define a rule:

1. Make sure the HBA's date and time are set correctly.
   For more information, see *"8.1.19 Date and Time" on page 107*.
2. On the top menu, click **Advanced**.
3. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
4. Under , click **Scheduler Tasks**.
5. The **Scheduler Tasks** page appears.



   Click Add.

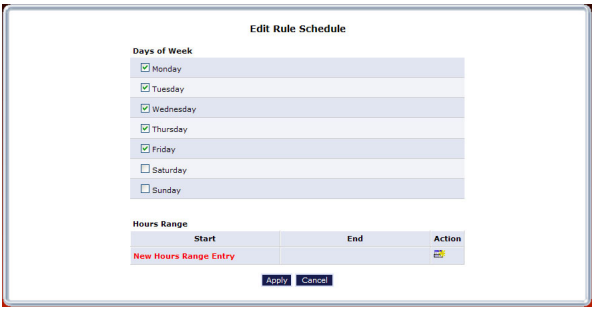
6. The **Set Rule Schedule** page appears.



7. Type a name for the rule in the **Rule Name** text box.
8. Under **Rule Settings**, select:
   - **Rule will be Active at the Scheduled Time** if you want to specify during which time slot the rule should be enabled. For example, no Internet between 10pm and 6am.
   - **Rule will be Inactive at the Scheduled Time** if you want to specify during which time slot the rule should be disabled. For example, Internet is allowed between 6am and 10pm.

9 Click **Add Rule Schedule**.

10 The **Edit Rule Schedule** screen appears.



11 Select active or inactive days of the week by clicking in the corresponding check boxes.

12 Click **New Hours Range Entry** to define start and end time for this rule.

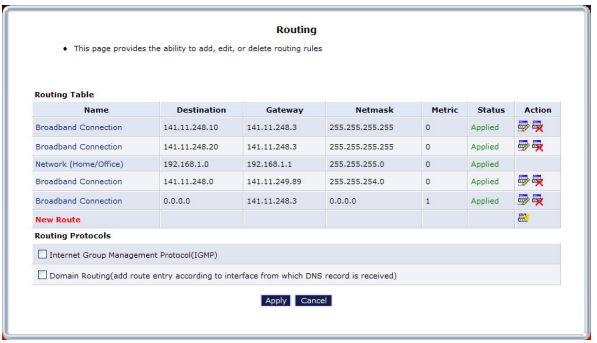
13 Click **Apply**.

8.1.21 Routing

Accessing the Routing page

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Routing**.
4. The **Routing** page appears.



Routing table

The following settings are available in the **Routing** table:

- **Route Name**
  Select the type of network from the drop-down list.
- **Destination**
  The destination is the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
- **Netmask**
  The network mask is used in conjunction with the destination to determine when a route is used.
- **Gateway**
  Enter the HBA's IP address.
- **Metric**
  A 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.

IGMP (Internet Group Management Protocol) Multicasting

The HBA provides support for 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 pre-defined group of recipients. When joining a multicast group, all messages addressed to the group will be received by the user, much like when an email message is sent to a mailing list.

Domain Routing

Domain routing is used in multi- local network configurations. Normally, to access a device connected to one from another on the network, its IP address must be used. Activating domain routing (by clicking in the appropriate check box) allows the user to access the computer by name (as well as IP address).

8.1.22 IP Address Distribution

Introduction

The HBA's DHCP server makes it possible to easily add computers configured as DHCP clients to the network. It provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to them.

For example, a client (host) sends out a broadcast message on the network 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.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease, it will also receive current information about network services,

as it did with the original lease, allowing it to update its network configurations to reflect any changes that occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration, it can send a release message to the DHCP server, which will then make the IP address available for use by others.

HBA DHCP server functions

The DHCP server of the HBA:

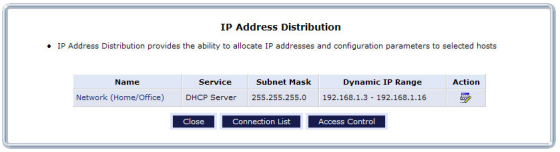
- Displays a list of all DHCP hosts devices connected to the HBA.
- Defines the range of IP addresses that can be allocated in the network.
- Defines the length of time for which dynamic IP addresses are allocated.
- Provides the above configurations for each network device and can be configured and enabled/disabled separately for each network device.
- Can assign a static lease to a network computer so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers.
- Provides the DNS server with the host name and IP address of each computer connected to the network.

Accessing the IP Address Distribution page

To view a summary of the services currently being provided by the DHCP server:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBA Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **IP Address Distribution**.

4 The **Routing** page appears.



Click:

- or the name of the entry to change the settings.
- **Connection List** to see the current DHCP connections.
- Access Control to allow/deny access for specific client based on their MAC address of the client.

8.2 HBR Advanced Pages

Introduction

The **Advanced** HBR page contains links to the different configuration pages. These pages are grouped by topic:

- *Utilities*
- *DNS Server*
- *Configuration*
- *Date and time*
- *IP Address Distribution*

Utilities

Click:

- **Diagnostics** to perform diagnostic tests on the HBR.
  For more information, see *"8.2.1 Diagnostics" on page 116*.
- **Restore HBR Defaults** to reset the HBR to its default settings.
  For more information, see *"8.2.2 Restore HBR Defaults" on page 117*.
- **Reboot HBR** to restart the HBR.
  For more information, see *"8.2.3 Reboot HBR" on page 118*.
- **Restore HBA Defaults** to reset the HBA to its default settings.
  This page is similar to the one listed under the **HBA Advanced** pages. For more information, see *"8.1.2 Restore Defaults" on page 81*.
- **Reboot HBA** to restart the HBA.
  This page is similar to the one listed under the **HBA Advanced** pages.For more information, see *"8.1.3 Reboot the Router" on page 83*.
- **ARP Table** to display active devices and their IP and MAC addresses.
  For more information, see *"8.2.4 ARP Table" on page 119*.
- **Users** to create and manage users.
  For more information, see *"8.2.5 Users" on page 120*.

DNS Server

Click **DNS Server** to manage the local (LAN) network for host name and IP address.
For more information, see *"8.2.6 DNS Server" on page 121*.

Configuration

Click:

- **System Settings** to change the system settings of the HBR.
  For more information, see *"8.2.7 System Settings" on page 122*.
- **Port Configuration** to configure the Ethernet LAN ports.
  For more information, see *"8.2.8 Port Configuration" on page 123*.

Date and time

Click **Date and Time** to configure the HBR clock and calendar of the HBR.
For more information, see *"8.2.9 Date and Time" on page 124*.

IP Address Distribution

Click **IP Address Distribution** to manage the IP addresses of devices on the network.
For more information, see *"8.2.10 IP Address Distribution" on page 125*.

8.2.1 Diagnostics

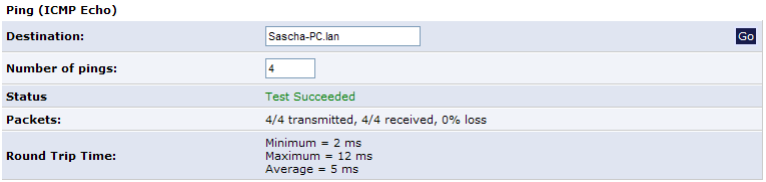
Introduction

The **Diagnostics** page allows you to let the HBR ping a device or website. Ping is used to test if a host (for example, a website or a computer) is reachable.

Procedure

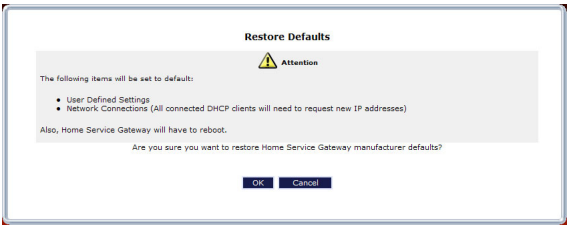
To diagnose network connectivity:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBR Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Diagnostics**.
4. The **Diagnostics** page appears.



From this point on, the procedure is identical to the one described for the HBA diagnostics page. For more information, see *"8.1.1 Diagnostics" on page 79*.

8.2.2 Restore HBR Defaults



Introduction

The **Restore Defaults** page allows you to return to the factory defaults of your HBR. For more information, see *"8.1.2 Restore Defaults" on page 81*.

8.2.3 Reboot HBR

Introduction

The **Reboot HBR** page allows you to restart your HBR.

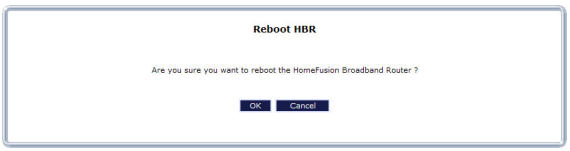
WARNING

During the reboot, all services provided by the HBR will be unavailable.

Procedure

To reboot the HBR:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBR Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **Reboot HBR**.
4. The HBR prompts you to confirm the reboot.



   Click **OK**.
5. The HBR restarts. This may take up to two minutes.

8.2.4 ARP Table

ARP

The **Address Resolution Protocol** is a protocol that translates the IP address of a network device into its MAC address.

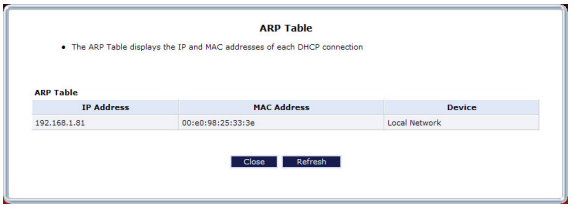
The ARP table page

The **ARP Table** page provides you a mapping between the IP address and the MAC address of the device that is using this IP address.

Viewing the ARP table

Proceed as follows:

1. On the top menu, click **Advanced**.
2. The **Advanced** page appears. Click **HBR Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
3. Under , click **ARP Table**.
4. The **ARP Table** page appears.



The following fields are available:

- **IP Address**
- **MAC Address**
- **Device**
  Displays the network interface that the device is using. For more information, see *"5.2 Network Connections" on page 48*.

8.2.5 Users

Introduction

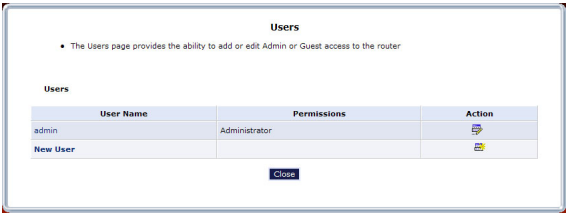
The **Users** page allows you to manage the user accounts for access to the HBR GUI.

1 On the top menu, click **Advanced**.

2 The **Advanced** page appears. Click **HBR Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.

3 Under , click **Users**.

4 The **Users** page appears.

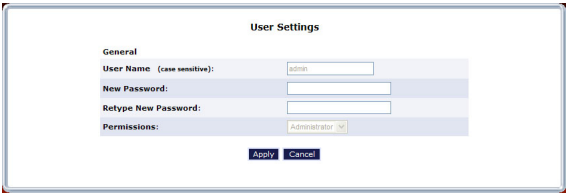


5 If you want to:

- Create a new user, click **New User**.
- Change the settings of an existing user, click the name of the user or .
- Delete a user, click .

User Settings page

When editing or creating a user account the **User Settings** page appears:



The following fields are available:

- **User Name**
  The name a remote user will use to access the home or office network. This entry is case-sensitive.
- **New Password/Retype New Password**
  The password for the user (and enter again to confirm).
- **Permissions**
  The level of access the user is allowed.

You can not change the **User Name** and **Permissions** of the **admin** user.

8.2.6 DNS Server

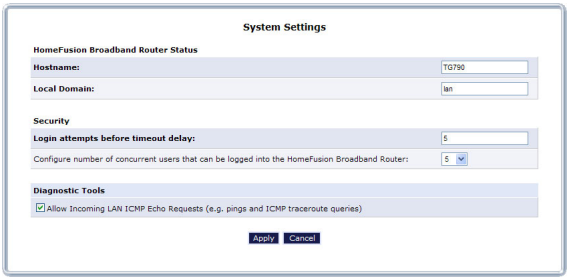
Introduction

The configuration of the HBR **DNS Server** page is similar to the configuration of the HBA **DNS Server** page. For more information, see *"8.1.9 DNS Server" on page 91*.

8.2.7 System Settings

Introduction

The **System Settings** page allows you to configure various system and management parameters.



The page is divided into the following groups:

- *HomeFusion Broadband Router Status*
- *Security*
- *Diagnostic Tools*

HomeFusion Broadband Router Status

Under **HomeFusion Broadband Router Status**, the following properties are available:

- **Hostname**
  Specify the HBR's host name by entering it into the text box. The host name is used in combination with the **Local Domain** to access the HBR.
- **Local Domain**
  Specify the network's local domain by entering it into this text box. The **Local Domain** is used in combination with the **HomeFusion Broadband Router's Hostname** to access the HBR.

So if you change the host name to **gateway** and the local domain to **home**, you will have to access the GUI using http://gateway.home.

Security

Under **Security**, you can:

- Enter how many tries a user gets to login to the GUI without blocking GUI access.
- How many users can be connected to the HBR GUI at the same time.

Diagnostic Tools

Under **Diagnostic Tools**, you can specify if you want to allow incoming ICMP requests.

8.2.8 Port Configuration

Introduction

The **Port Configuration** page allows you to set up the HBR's Ethernet ports.

Supported speeds

The HBR supports the following speeds:

- 100 Megabits per second (Mbps)
- 10 Megabits per second

The HBR also has an **Auto** setting where it automatically selects the highest speed supported by the connected device.

Supported Duplex

The HBR supports the following communication systems:

- Full-duplex:
  Supports communication in both directions and at the same time.
- Half-duplex:
  Supports communication in both directions, but only one at a time.

8.2.9 Date and Time

Introduction

The Date and Time page allows you to configure the date and time that the HBR will be using for System logging.
For more information, see *"9.2.1 System Log" on page 130*.

Accessing the Date and Time page

Proceed as follows:

1. On the top menu, click **Advanced** and then click **Yes** to confirm that you want to access the advanced settings.
2. Under , click **Date and Time**.
3. In the **Time Zone** list, select your time zone or select **Other** to create one if your time zone is not listed.
4. Under **Daylight Saving Time** you can change the daylight saving settings
5. Under **Automatic Time Update**:
   - Select **Enabled** if you want the HBR to synchronize its time settings with a Network Time Protocol (NTP) server. This guarantees you that you will always be using the correct time.
   - Clear **Enabled** if you want to set the time manually. Use the **Clock Set** button on the bottom of the page to enter the correct date and time.
6. Click **Apply**.

8.2.10 IP Address Distribution

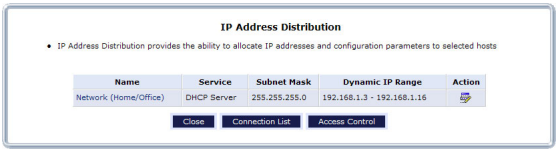
Introduction

The **IP Address Distribution** page offers the same functions as the **IP Address Distribution** page of the HBA. For mor information, see *"8.1.22 IP Address Distribution" on page 112*.

Accessing the IP Address Distribution page

To view a summary of the services currently being provided by the DHCP server:

1. On the top menu, click **Advanced** and then click **Yes** to confirm that you want to access the advanced settings.
2. Under , click **IP Address Distribution**.
3. The **IP Address Distribution** page appears.



Click:

- or the name of the entry to change the settings.
- **Connection List** to see the current DHCP connections.
- Access Control to allow/deny access for specific client based on their MAC address of the client.

9

GUI: System Monitoring

9 GUI: System Monitoring

Introduction

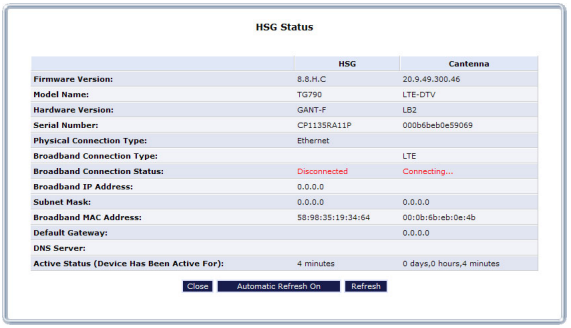
The **System Monitoring** menu consists of the following items:

- **HBR Status**
  For more information, see *"9.1 HBR Status" on page 128*.
- **Advanced HBR Status**
  For more information, see *"9.2 Advanced HBR Status" on page 129*.
- **Advanced HBA Status**
  For more information, see *"9.2 Advanced HBR Status" on page 129*.

9.1 HBR Status

Introduction

The **HBR Status** page provides basic information about your HBR.



Accessing the HBR Status page

On the top menu, click **System Monitoring**.

9.2 Advanced HBR Status

Introduction

The **Advanced Status** page contains more advanced status information that is bundled in the following groups:

- **System Logging**:
  For more information, see *"9.2.1 System Log" on page 130*.
- **Full Status/System wide Monitoring of Connections**:
  For more information, see *"9.2.2 Full Status/System wide Monitoring of Connections" on page 131*.
- **Traffic Monitoring**:
  For more information, see *"9.2.3 Traffic Monitoring" on page 132*.

WARNING

The advanced status pages are intended for advanced technical users only!

Accessing the Advanced Status page

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBR Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced HBR Status** page appears:

4. Click on the item that you want to view.

9.2.1 System Log

Introduction

The **System Logging** page summarizes the last events recorded on your HBR.

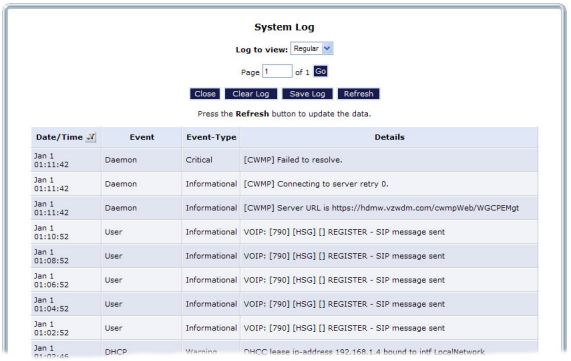
Accessing the System Logging page

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBR Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced HBR Status** page appears:

Click **System Logging**.

4. The **System Log** page appears.



9.2.2 Full Status/System wide Monitoring of Connections

Introduction

The **Full Status/System wide Monitoring of Connections** page provides an overview of all network connections.

Accessing the Full Status/System wide Monitoring of Connections page

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBR Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced HBR Status** page appears:

Click **Full Status/System wide Monitoring of Connections**.

4. The **Full Status/System wide Monitoring of Connections** page appears.

Name	Ethernet	Coax	Wireless Access Point	Broadband Connection LTE Broadband
Status	Connected	Connected	Disconnected	Disconnected
Network	Network (Home/Office)	Network (Home/Office)	Network (Home/Office)	Broadband Connection
Underlying Device				
Connection Type	Hardware Ethernet Switch	Coax	Wireless 802.11n Access Point	LTE Broadband
MAC Address	58:98:35:19:34:64	58:98:35:19:34:64	58:98:35:19:34:65	
IP Address				
Subnet Mask				
Default Gateway				
DNS Server				
IP Address Distribution	Disabled	Disabled	Disabled	
Service Name				
User Name				
Packets Received	2358	189	0	
Sent Packets	3700	2168	1986	
Received Bytes	423727	21005	0	
Sent Bytes	2004642	353497	300137	
Time Span	0:14:49	0:13:07	0:14:49	
Channel		575000000 Mhz		

5. Click:
   - **Close** to return to the **Advanced HBR Status** page.
   - **Automatic Refresh On** to let the HBR automatically update the information.
   - **Refresh** to update the information.

9.2.3 Traffic Monitoring

Introduction

The HBR constantly monitors traffic within the local network, and between the local network and the Internet. The **Traffic Monitoring** page allows you to view up-to-the-second statistical information about data received from and transmitted to the Internet, and about data received from and transmitted to computers in the local network.

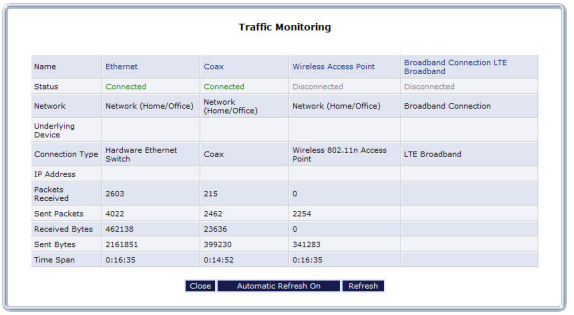
Accessing the Traffic Monitoring page

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBR Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced HBR Status** page appears:

Click **Traffic Monitoring**.

4. The **Traffic Monitoring** page appears.



Buttons

Under the overview table, the following buttons are available:

- **Close** to return to the **Advanced HBR Status** page.
- **Automatic Refresh On** to let the HBR automatically update the information every minute or **Automatic Refresh Off** to switch back to manual updating.
- **Refresh** to update the information.

9.3 Advanced HBA Status

Introduction

The **Advanced HBA Status** page contains more advanced status information that is bundled in the following groups:

- **System Logging**:
  This page is similar to the HBR's **System Logging** page. For more information, see *"9.2.1 System Log" on page 130*.
- **Full Status/System wide Monitoring of Connections**:
  This page is similar to the HBR's **Full Status/System wide Monitoring of Connections** page. For more information, see *"9.2.2 Full Status/System wide Monitoring of Connections" on page 131*.
- **Traffic Monitoring**:
  This page is similar to the HBR's **Traffic Monitoring** page. For more information, see *"9.2.2 Full Status/System wide Monitoring of Connections" on page 131*.
- **Bandwidth Monitoring**:
  For more information, see *"9.3.1 Bandwidth Monitoring" on page 134*.
- **IGMP Proxy**:
  For more information, see *"9.3.2 IGMP Proxy" on page 135*.

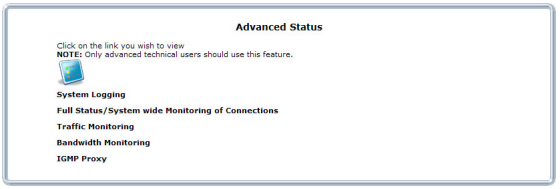
WARNING

The advanced status pages are intended for advanced technical users only!

Accessing the Advanced Status page

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBA Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced HBA Status** page appears:



4. Click on the item that you want to view.

9.3.1 Bandwidth Monitoring

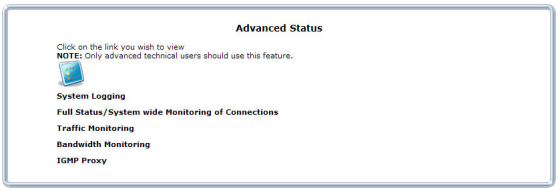
Introduction

The **Bandwidth Monitoring** page allows you to view the traffic sent or received by the HBR during a specific time slot.

Accessing the Bandwidth Monitoring page

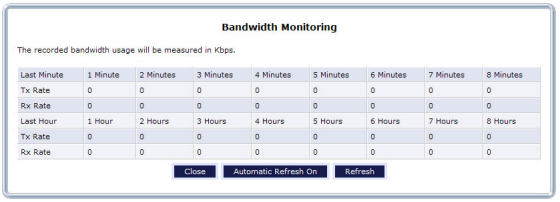
Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBA Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced Status** page appears:



Click **Bandwidth Monitoring**.

4. The **Bandwidth Monitoring** page appears.



Buttons

Under the overview table, the following buttons are available

- **Close** to return to the **Advanced HBA Status** page.
- **Automatic Refresh On** to let the HBR automatically update the information every minute or **Automatic Refresh Off** to switch back to manual updating.
- **Refresh** to update the information.

9.3.2 IGMP Proxy

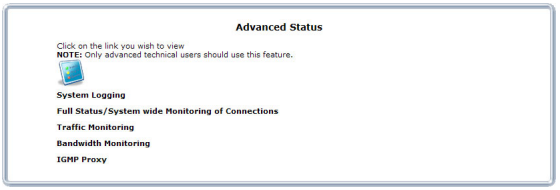
Introduction

The **IGMP Proxy** task allows you to view IGMP Proxy multicast group memberships and statistics.

Viewing the IGMP Proxy Multicast Group Membership page

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBA Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced Status** page appears:



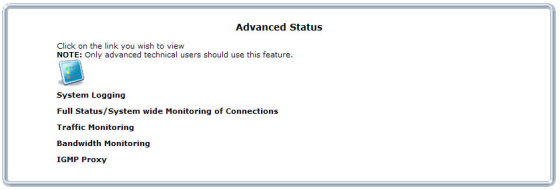
   Click **IGMP Proxy**.

4. The **Multicast Group Membership** page appears.

Viewing the IGMP Proxy Multicast Group Statistics

Proceed as follows:

1. On the top menu, click **System Monitoring**.
2. The **HBR Status** page appears. On the left menu, click **Advanced HBA Status** and then click **Yes** to confirm that you want to access the advanced settings.
3. The **Advanced Status** page appears:



   Click **Bandwidth Monitoring**.

4. The **Multicast Group Membership** page appears. On the left menu, click **IGMP Proxy Multicast Group Statistics**.
5. The **IGMP Proxy Multicast Group Statistics** page appears.

10

Support

Call Customer Care

If this Troubleshooting section does not provide a solution to your problem, please call Customer Care at *800-922-0204*.

10.1 General Troubleshooting

Check the LEDs

If the HBR does not work as expected, the status LEDs on the front panel may provide you enough information to locate the problem.

For more information, see *"1.3.1 Front Panel" on page 6*.

10.2 Troubleshooting Your Wireless Connection

WPA2 encryption not available on Windows XP

If you want to configure WPA2 on the built-in wireless utility of Windows XP Service Pack 2 (SP2), you first have to:

- Upgrade your Windows XP to Service Pack 3.

- or -

- Install the following update: http://support.microsoft.com/kb/917021.

Windows can not find the HBR access point

If the built-in Windows wireless client manager can not find your HBR access point:

- If you are using a laptop, check if your laptop has a button to enable/disable the wireless client. Switch it on and try again.
- Make sure your computer is within range.
- Make sure that wireless is enabled on your HBR:
  - **a** Take a computer that is connected to the HBR or connect your computer with an Ethernet cable (for more information, see *"2.3.3 Wired Connection to the HBR" on page 23*).
  - **b** Browse to the GUI. For more information, see *"Accessing the GUI" on page 27*.
  - **c** On the **Wireless Settings** menu, click **Basic Security Settings**.
  - **d** Under **1. Turn Wireless ON**, select **On**.

  - **e** Click **Apply**.
- Change the wireless channel:
  - **a** Take a computer that is connected to the HBR or connect your computer with an Ethernet cable (for more information, see *"2.3.3 Wired Connection to the HBR" on page 23*).
  - **b** Browse to the GUI. For more information, see *"Accessing the GUI" on page 27*.
  - **c** On the **Wireless Settings** menu, click **Basic Security Settings**.
  - **d** Under **3. Channel**, select another channel.
  - **e** Click **Apply**.

Poor wireless connectivity

Try the following:

- Change the wireless channel:
  - **a** Take a computer that is connected to the HBR or connect your computer with an Ethernet cable (for more information, see *"2.3.3 Wired Connection to the HBR" on page 23*).

b Browse to the GUI. For more information, see *"Accessing the GUI" on page 27*.

c On the **Wireless Settings** menu, click **Basic Security Settings**.

d Under **3. Channel**, select another channel.

e Click **Apply**.

- Check the signal strength, indicated by the wireless client manager. If the signal is low, try to move the HBR for optimal performance.
- Use WPA2 as encryption. For more information, see *"4.3.1 Securing Your Wireless Connection" on page 41*

10.3 Resetting your HBR

Resetting your HBR

If at some point you can no longer connect to the HBR or you want to make a fresh install, it may be useful to perform a reset to factory defaults.

Warning

A reset to factory default settings deletes all configuration changes you made. For example:

- The **SSID** and **WPA key on** the back of the HBR will be used to secure your wireless connection. So you may need to re-associate your wireless clients, as described in *"2.3.2 Connecting Your Wireless Device Manually" on page 19*.
- The **Login password** required to access the GUI pages will be reset to the one that is printed on the back of the HBR.

Methods

You can choose between:

- *Resetting the HBR via the HBR GUI*
- *Reset the HBR via the Reset button*

Resetting the HBR via the HBR GUI

Proceed as follows:

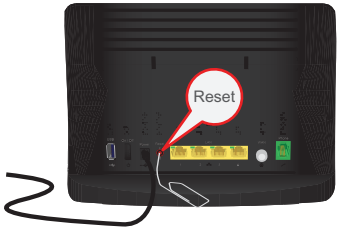
1. Browse to the GUI.
   For more information, see *"Accessing the GUI" on page 27*.
2. On the top menu, click **Advanced**.
3. The **Advanced** page appears. Click **HBR Advanced Settings** on the bottom of the page and then click **Yes** to confirm that you want to access the advanced settings.
4. Under , click **Restore Defaults**.
5. The **Restore HBR Defaults** page appears. Click **Restore Defaults**.
6. The HBR prompts you to confirm your choice, click **OK**.
7. The HBR restores the factory defaults and restarts.
8. The HBR returns to the HBR login page.

Reset the HBR via the Reset button

Proceed as follows:

1 Make sure the HBR is turned on.

2 Use a pen or an unfolded paperclip to push the recessed **Reset** button for at least 10 seconds and then release it.



3 The HBR restarts with the factory default settings

10.4 Configuring Dynamic IP Addressing on Windows

Windows 7/Vista

1. Select **Network and Sharing** in the **Control Panel**.
2. Click **View Status**, then click **Properties**.
3. Click **Continue** in the **User Account Control** window.
4. In the **General** tab of the **Local Area Connection Properties** window select **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.
5. The **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears.
6. Click the **Obtain an IP address automatically** radio button.
7. Click the **Obtain DNS server address automatically** radio button.
8. Click **OK** in the **Internet Protocol Version 4(TCP/IPv4) Properties** window, then click **OK** in the **Local Area Connection Properties** screen to save the settings.

Windows XP

1. Select **Network Connections** in the **Control Panel**.
2. Right-click **Ethernet Local Area Connection**, then click **Properties**.
3. In the **General** tab, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. The **Internet Protocol (TCP/IP) Properties** window appears.
5. Click the **Obtain an IP address automatically** radio button.
6. Click the **Obtain DNS server address automatically** radio button.
7. Click OK in the **Internet Protocol (TCP/IP) Properties** screen, then click **OK** in the **Local Area Connection Properties** screen to save the settings.

Macintosh OS X

1. Click on the Apple icon in the top left corner of the desktop.
2. From the menu that appears, select **System Preferences**.
3. The **System Preferences** window appears. Click **Network**.
4. From the **Network** window, make sure **Ethernet** in the list on the left is highlighted and displays **Connected**"
5. Click **Assist me**.
6. From the tab that appears, click **Diagnostics**.
7. Follow the instructions in the **Network Diagnostics** assistant.