



# HomePortal 3801HGV Gateway User Guide

Release 1.0

Notice to Users

©2005–2010 2Wire, Inc. All rights reserved. This manual in whole or in part, may not be reproduced, translated, or reduced to any machine-readable form without prior written approval.

2WIRE PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO THIS MANUAL, THE SOFTWARE, OR SUCH OTHER INFORMATION, IN NO EVENT SHALL 2WIRE, INC. BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES, WHETHER BASED ON TORT, CONTRACT, OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL, THE SOFTWARE, OR OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.

2Wire, Inc. reserves the right to make any modification to this manual or the information contained herein at any time without notice. The software described herein is governed by the terms of a separate user license agreement.

Updates and additions to software may require an additional charge. Subscriptions to online service providers may require a fee and credit card information. Financial services may require prior arrangements with participating financial institutions.

2Wire, the 2Wire logo, HomePortal, and MediaPortal are registered trademarks of 2Wire, Inc. All other trademarks are trademarks of their respective owners.

1202010

5100-000862-000

# Contents

	<b>About This Guide . . . . .</b>	<b>vi</b>
	Audience . . . . .	vi
	Using this Document . . . . .	vi
	Style Conventions . . . . .	vii
	Typographical Conventions . . . . .	vii
	Related Documents . . . . .	vii
	Support . . . . .	viii
<b>CHAPTER 1</b>	<b>Introducing the HomePortal 3801HGV Gateway . . . . .</b>	<b>1</b>
	Overview . . . . .	1
	What the HomePortal 3801HGV Gateway Does for You . . . . .	1
	Components . . . . .	2
<b>CHAPTER 2</b>	<b>Installing the HomePortal 3801HGV Gateway . . . . .</b>	<b>4</b>
	Determining HomePortal 3801HGV Gateway Location . . . . .	4
	Connecting the Power Adapter . . . . .	5
	Connecting Your Computer to the Gateway . . . . .	5
	Connecting through Local Ethernet . . . . .	5
	Connecting through Wireless . . . . .	6
	Connecting the Broadband Interface . . . . .	7
	Connecting VoIP Interface . . . . .	8
	Connecting HPNA Interface to IPTV set top Box . . . . .	9
<b>CHAPTER 3</b>	<b>Accessing the User Interface . . . . .</b>	<b>11</b>
	System Link Tabs . . . . .	12
	Summary . . . . .	12
	Quick Service Links . . . . .	12
	Home Network Devices . . . . .	13
	Top Networking Features . . . . .	13
<b>CHAPTER 4</b>	<b>Configuring Internet Connection . . . . .</b>	<b>14</b>
<b>CHAPTER 5</b>	<b>Viewing Subscribed Services Status . . . . .</b>	<b>17</b>
<b>CHAPTER 6</b>	<b>Configuring Voice-Based Services . . . . .</b>	<b>19</b>
	Viewing Status . . . . .	19
	Configuring SIP Server . . . . .	20
	Configuring Phone Lines . . . . .	22
	Configuring Phones . . . . .	23
	Viewing External Line Statistics . . . . .	24
<b>CHAPTER 7</b>	<b>Setting Up System Information . . . . .</b>	<b>27</b>
	Viewing System Information . . . . .	27
	Setting Up System Password . . . . .	29

	Setting Default System Password . . . . .	29
	Creating Your System Password . . . . .	30
	Configuring Date and Time . . . . .	30
	Automatically Setting up Date and Time . . . . .	31
	Manually Configuring Date and Time . . . . .	32
	Enabling Event Notifications . . . . .	32
	Enabling Notifications . . . . .	33
	Disabling Notifications . . . . .	33
<b>CHAPTER 8</b>	<b>Configuring Broadband Settings . . . . .</b>	<b>34</b>
	Viewing Broadband Status . . . . .	34
	Resetting Statistics on Status Page . . . . .	40
	Configuring Bridge Mode . . . . .	40
	Adding Static Routes . . . . .	42
	Configuring IP Multicast Sessions . . . . .	43
	Viewing Multicast Statistics . . . . .	44
	Resolving Domain Name . . . . .	47
<b>CHAPTER 9</b>	<b>Configuring LAN Devices . . . . .</b>	<b>50</b>
	Viewing LAN Status . . . . .	51
	Setting Up Wireless Network . . . . .	53
	Securing the Wireless Network Using Encryption Key . . . . .	55
	Securing the Wireless Network Using MAC Filtering . . . . .	57
	Allowing MAC Addresses . . . . .	58
	Blocking MAC Addresses . . . . .	59
	Refreshing the List of Devices . . . . .	60
	Deleting the Devices . . . . .	60
	Configuring Advance Wireless Settings . . . . .	61
	Configuring Wi-Fi Protected Setup . . . . .	62
	Setting Up WPS through the PIN Method . . . . .	62
	Setting Up WPS through the Push Button Method . . . . .	63
	Configuring Local Ethernet Ports . . . . .	64
	Configuring HomePNA 3.1 . . . . .	65
	Viewing HomePNA Status . . . . .	66
	Configuring DHCP . . . . .	66
	Allocating IP Addresses . . . . .	69
<b>CHAPTER 10</b>	<b>Configuring Firewall Settings . . . . .</b>	<b>72</b>
	Viewing Firewall Status . . . . .	72
	Configuring Firewall Settings . . . . .	73
	Creating an Application Profile . . . . .	75
	Deleting User-defined Applications . . . . .	79
	Allowing all Applications . . . . .	79
	Disabling Attack Detection . . . . .	80
	Controlling Inbound and Outbound Traffic . . . . .	82
	Configuring Firewall Security Enhancements . . . . .	83
	Configuring Application Layer Gateway . . . . .	83
<b>CHAPTER 11</b>	<b>Viewing Logs . . . . .</b>	<b>85</b>
	Viewing Event Log . . . . .	85

	Viewing All Event Logs . . . . .	85
	Filtering Logs . . . . .	87
	Clearing Event Logs . . . . .	87
	Viewing System Log . . . . .	87
	Filtering and Viewing System Logs . . . . .	88
	Inserting Mark . . . . .	89
	Clearing Logs . . . . .	89
	Viewing Upgrade Log . . . . .	89
	Viewing Firewall Log . . . . .	90
	Viewing Log . . . . .	91
	Clearing Log . . . . .	92
<b>CHAPTER 12</b>	<b>Using Diagnostics Features . . . . .</b>	<b>93</b>
	Testing Broadband Link . . . . .	93
	Viewing Link Tree . . . . .	95
	Viewing DSL Diagnostic Information . . . . .	96
	Testing IP Utilities . . . . .	97
	Testing Ping . . . . .	98
	Testing Traceroute . . . . .	100
	Testing Dnsquery . . . . .	102
	Viewing NAT Information . . . . .	103
	Enabling Syslog . . . . .	105
	Resetting the Gateway . . . . .	106
	Resetting System and Links . . . . .	107
	Resetting Configuration . . . . .	108
	Resetting Device to Factory Default . . . . .	108
<b>CHAPTER 13</b>	<b>Troubleshooting 3801HGV Gateway . . . . .</b>	<b>109</b>
	Connection Issues . . . . .	109
	VoIP Issues . . . . .	110
	Home PNA Issues . . . . .	110
	System Information Issues . . . . .	111
	Broadband Issues . . . . .	111
	LAN Issues . . . . .	112
	Firewall Issues . . . . .	113
	Diagnostic Issues . . . . .	113
<b>APPENDIX A</b>	<b>Glossary . . . . .</b>	<b>114</b>
<b>APPENDIX B</b>	<b>Regulatory Information . . . . .</b>	<b>117</b>
	Electrical . . . . .	117
	AC Adapter . . . . .	117
	Telecommunication Cord . . . . .	117
	Internal Telephone ports (VoIP) . . . . .	117
	Location – Electrical Considerations . . . . .	117
	Equipment . . . . .	118
	Declaration of Conformity . . . . .	118
	FCC / Industry Canada Compliance . . . . .	118
	Part 15 of FCC Rules . . . . .	118
	TIA 968 (Part 68 of FCC Rules) / IC CS-03 . . . . .	119
	MPE/SAR/RF Exposure Information . . . . .	119

# About This Guide

The *HomePortal 3801HGV Gateway Installation and Configuration Guide* is designed to serve as a reference to install and set up the HomePortal 3801HGV gateway. This guide contains the following major sections:

[Introducing the HomePortal 3801HGV Gateway](#) on page 1

[Installing the HomePortal 3801HGV Gateway](#) on page 4

[Accessing the User Interface](#) on page 11

[Configuring Internet Connection](#) on page 14

[Viewing Subscribed Services Status](#) on page 17

[Configuring Voice-Based Services](#) on page 19

[Setting Up System Information](#) on page 27

[Configuring Broadband Settings](#) on page 34

[Configuring LAN Devices](#) on page 50

[Configuring Firewall Settings](#) on page 72

[Using Diagnostics Features](#) on page 93

[Troubleshooting 3801HGV Gateway](#) on page 109

[Glossary](#) on page 114

[Regulatory Information](#) on page 117

## Audience

This guide is intended for use by:

- End Users
- Sales Engineers
- Support Staff
- Service Provider Technicians

## Using this Document

Each topic/subtopic in this document has the following sections:

- Objective
- Steps
- See Also

These sections help you find your topics of interest with ease, and guide you through the topics in a simple and logical manner.

The **See Also** section has cross-referenced links to other topics within this document, which may assist you in further understanding your device.

## Style Conventions

The following style conventions are used in this document:

---

**Note** Notes contain incidental information about the subject. In this guide, they are used to provide additional information about the product, and to call attention to exceptions.

---



**Caution notes identify information that helps prevent damage to hardware or loss of data.**

---



**Warning notes identify information that helps prevent injury or death.**

---

## Typographical Conventions

The following typographical conventions are used in this document:

Convention	Used For
Blue Text	Cross references
<b>Bold</b>	Interface elements that are clicked or selected
<i>Italic</i>	Emphasis, book titles, variables, list terms
Monospace	Command syntax and code
<i>Monospace Italic</i>	Variables within command syntax and code

## Related Documents

In addition to this guide, the HomePortal 3801HGV gateway documentation library includes:

- *HomePortal 3801HGV Hardware Functional Specifications*: Communicates the high level hardware related information
- *HomePortal 3801HGV Software Functional Specifications*: Communicates the high level features of the gateway
- *HomePortal 3801HGV Hardware Release Notes*: Communicates the hardware changes incorporated in the latest release
- *HomePortal 3801HGV Software Release Notes*: Communicates the known issues, resolved issues, and feature updates in the latest release

## Support

Technical support is available from the 2Wire Website: <http://support.2wire.com/index.php>.



## CHAPTER 1

# Introducing the HomePortal 3801HGV Gateway

Welcome to the 2Wire family. The HomePortal 3801HGV gateway belongs to the next generation gateway series that delivers profound user experience with its easy-to-use features. This gateway helps you connect to your ISP, and also to achieve a host of functions, which makes your home network safe, convenient, and greatly enjoyable!

This chapter offers an overview of the HomePortal 3801HGV gateway, and describes its key features.

## Overview

The 2Wire HomePortal 3801HGV gateway is an advanced gateway that either the service provider or the subscriber can install.

It is a home networking device that provides an 802.11b/g Wi-Fi access point and switching functions for connecting personal computers and other home-networked devices to the service provider network. The gateway has 4 10/100 Ethernet ports to connect to computers or devices in the home. It comes loaded with hardware capabilities that enable you to use VoIP and Video Streaming technologies.

## What the HomePortal 3801HGV Gateway Does for You

The HomePortal 3801HGV gateway gives you a seamless, high speed Internet access, amongst a host of other features:

- *Seamless Wireless Connectivity:* The gateway includes an integrated wireless access point that allows you to roam wirelessly throughout the home or office. 2Wire high-powered wireless technology helps to reduce wireless “cold spots” in the home. The high-power 400mW transmitter of the gateway increases wireless bandwidth throughout the coverage area
- *Home Networking:* Share files, printers, and a broadband connection with every computer and other network-ready device in the home or small office through the advanced LAN technology. There are 4 Ethernet ports you can use to connect to multiple devices in your network

- *Parental Controls (Internet Access Controls and Content Screening)*: Parental controls offer easy-to-use tools to limit access to specific Websites, monitor browsing history and usage, and enforce time restrictions on common applications. Parental control settings are straightforward and easily managed by users. Because this service resides at the gateway, every Internet device on the network can be protected—even visiting devices
- *Advanced Firewall Monitoring*: This feature watches for suspicious activity, helping to eliminate security issues before they have a chance to proliferate. It automatically keeps itself current with software updates. You can decide when and how to receive notification of attacks and view detailed logs through the gateway's user interface
- *Web Remote Access*: You can gain fast, easy access to your local network remotely using an Internet browser. Download files securely from anywhere using an Internet connection and network password. You can also view and manage all gateway settings, including those for other applications like Parental Controls and Firewall Monitoring
- *Voice Over IP (VoIP)*: Two FXS lines through an RJ-14 jack provide prioritized VoIP services, lowering your communication costs. This gateway also supports wireless-wireline convergence
- *HomePNA (HPNA)*: HPNA features for distributing entertainment and triple play data over existing coax cables
- *Network Address Translation (NAT)*: NAT and Network Address and Port Translation (NAPT) technology for enabling multiple hosts on private network using a common IP address
- *Internet Protocol Security (IPsec)*: IPsec for protecting data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host
- *Internet Group Management Protocol (IGMP)*: IGMP and IGMP Proxying for NAT and firewall traversal
- *Domain Name Server (DNS)*: Acts as a DNS name server to LAN devices, letting you set a simple domain name for devices instead of keeping track of their respective IP addresses
- *QoS (Quality of Service)*: QoS features such as policies, priority queuing, shaping, and management allows you effectively manage the available Internet bandwidth
- *Logs*: The gateway maintains an internal log of broadband status and WAN-side connection flows, letting you or the ISP's technician effectively diagnose issues
- *PING Client*: To ping LAN and WAN side IP addresses within your network. This lets you know whether a device is responding or not
- The HomePortal 3801HGV gateway comes loaded with a user-friendly Web interface that allows you to configure your gateway settings as per your requirements

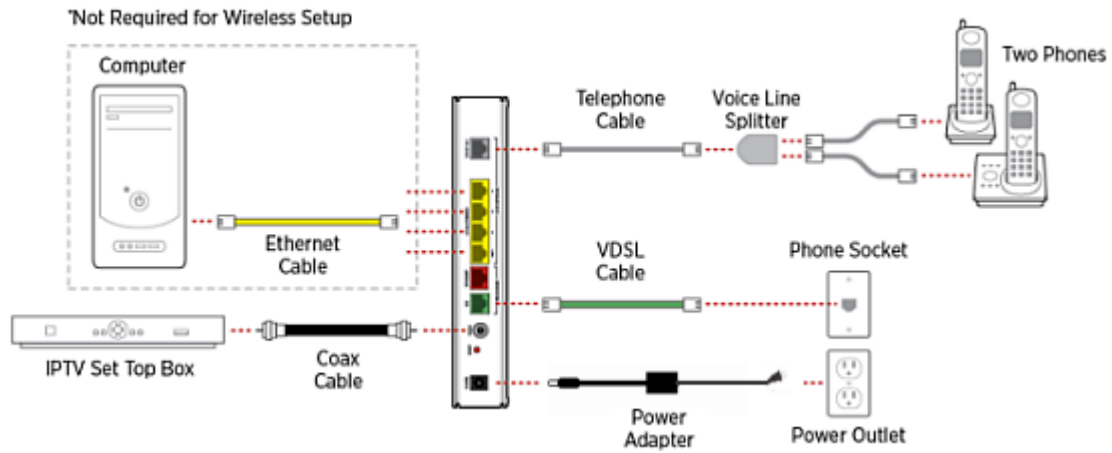
## Components

Before installing your gateway, review the package content and ensure that you have items available as shown below.

---

**Note** The gateway and the stand are packaged separately in the container. Vertical orientation is the preferred method for mounting the HomePortal 3801HGV gateway.

---



### Figure 1: Installation Components

Your HomePortal 3801HGV gateway has the following components in the box:

- 1 HomePortal 3801HGV Gateway
- 1 Power Cord & Adapter

### See Also

[Installing the HomePortal 3801HGV Gateway](#) on page 4

[Accessing the User Interface](#) on page 11

[Configuring Internet Connection](#) on page 14

[Regulatory Information](#) on page 117

## CHAPTER 2

# Installing the HomePortal 3801HGV Gateway

Installing your HomePortal 3801HGV gateway consists of the following tasks:

- [Determining HomePortal 3801HGV Gateway Location](#) on page 4
- [Connecting the Power Adapter](#) on page 5
- [Connecting Your Computer to the Gateway](#) on page 5
- [Connecting the Broadband Interface](#) on page 7
- [Connecting VoIP Interface](#) on page 8
- [Connecting HPNA Interface to IPTV set top Box](#) on page 9

## Determining HomePortal 3801HGV Gateway Location

If you have subscribed for IPTV and High Speed Internet, then the preferred location for installing the HomePortal 3801HGV gateway is near the first video set top box. If you have subscribed only for High Speed Internet access, then the HomePortal 3801HGV gateway should be installed near the first computer.

Also, you must determine a Wireless Access Point (WAP) location to deploy the HomePortal 3801HGV gateway. Wireless signals are affected by many items in homes and offices. Reliability and performance are the major considerations when planning your wireless network location. Consider the following points before determining the WAP to deploy the gateway:

- Place your gateway at least 5 feet (1.52 meters) from cordless phones, microwave ovens, or other electronic devices to avoid potential interference, and more than 6 inches (15.24 centimeters) away from your television to avoid audio hissing or static
- Place the gateway in an open area where the wireless range will not be directly affected by the surroundings. Wireless signal strength will be much stronger in an open area as opposed to an area with obstructions. In a single-story building, place the gateway as high and as close to each wireless computer as possible
- Keep the gateway away from any large metal objects. Wireless signal quality may be adversely affected as metal objects can reflect or obstruct signals

---

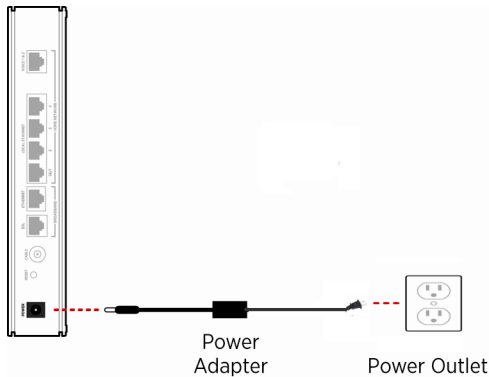
**Note** Whenever possible, use the stand provided with the gateway, and install it in the vertical position. Make sure that it is installed in a manner that nothing can be stacked on the top of it. Vertical orientation is the preferred method for mounting the HomePortal 3801HGV gateway.

---

## Connecting the Power Adapter

Follow these steps to power on the gateway:

1. Connect one end of the power adapter to the POWER port of your gateway.
2. Connect the other end of the power adapter to an electrical outlet. Once the gateway is powered on, the power LED flashes green for a brief period of time and then turns solid green.



**Figure 2: Power Connection**

---

**Note** Use the 2Wire power adapter packaged with the gateway, as it is compliant with local regulatory requirements.

---

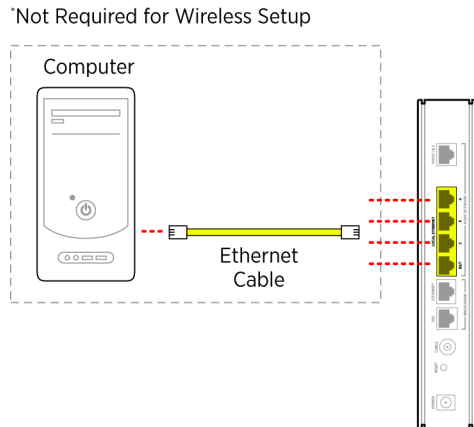
## Connecting Your Computer to the Gateway

The first computer you connect to the gateway is used to configure the HomePortal 3801HGV gateway for proper operation. You can connect your gateway to additional computers and/or other devices with Ethernet cable and wireless AP.

### Connecting through Local Ethernet

The HomePortal 3801HGV gateway has four Ethernet ports for directly connecting computers or devices. Use the Ethernet interface(s) on the gateway to create a broadband network. Follow these steps to connect the computer to the gateway using the Ethernet cable:

1. Connect one end of the Ethernet cable (yellow) to any available LOCAL ETHERNET port on the gateway.
2. Connect the other end of the Ethernet cable to the Ethernet port of the Network Interface Card (NIC) on the computer.



**Figure 3: LAN Connection**

## Connecting through Wireless

The HomePortal 3801HGV gateway has an integrated wireless access point (AP) that enables you to connect your wireless-enabled computers to your gateway. By default, the HomePortal 3801HGV gateway is shipped with WPA-PSK/WPA2-PSK enabled and a preconfigured network name.

Most laptops are equipped with an internal 802.11b/g card. If your computer is not equipped with an internal card, you can install an external wireless adapter for wireless networking.

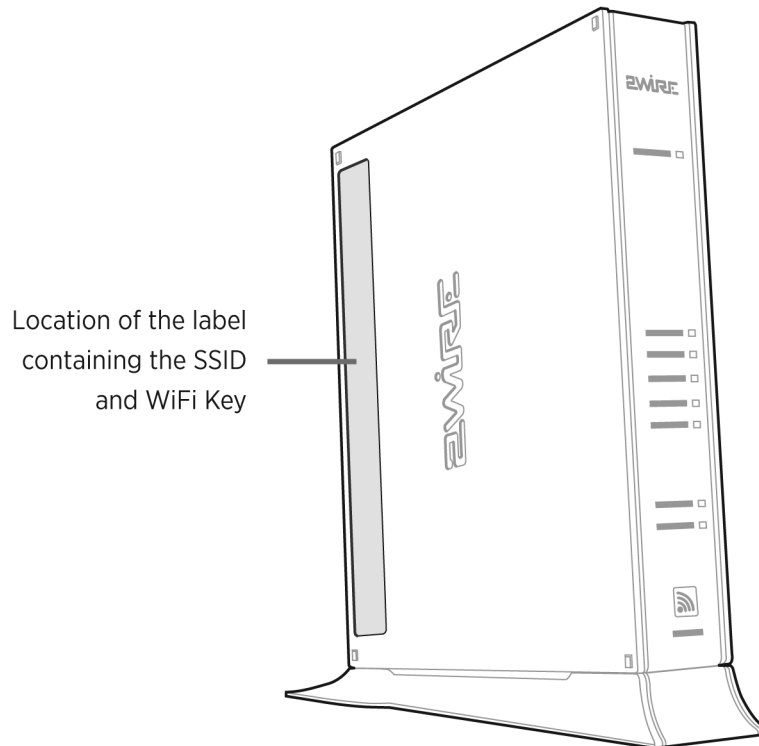
---

**Note** The default network name (SSID) is the encryption key, a 64-bit hex value located beneath the bar code on the side of the 2Wire gateway (for example, 1234567891). For Mac OS X users, you may need to enter the “\$” character at the beginning of the encryption key (for example, \$1234567891).

---

Follow these steps to connect the computer to the gateway using Wireless:

1. Push the wireless button at the bottom of the gateway front panel. Verify that the WIRELESS light on the front of the HomePortal 3801HGV gateway is solid green.
2. Install and configure your wireless adapter, if required.
3. View the available wireless network connections. Use the network adapter client or Windows Wireless Network Connection wizard to do so.
4. Select the network name of the gateway from the menu, and click Connect. A prompt to enter the network key appears.
5. Enter the encryption key and click Connect. Refer the note above for the location of the key.

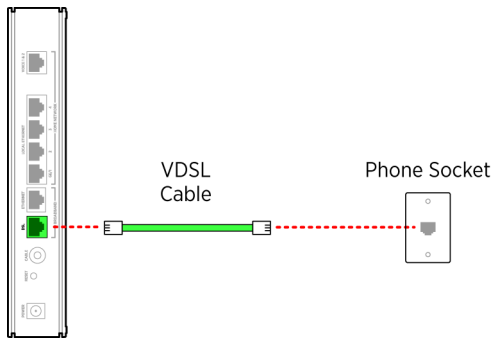


**Figure 4: Wireless Network Key Location**

## Connecting the Broadband Interface

Follow these steps to connect the gateway to Very High Bit-rate DSL (VDSL) wall jack:

1. Connect one end of the phone cord/twisted pair cable to the DSL port (green) on your gateway.
2. Connect the other end of the phone cord/twisted pair cable to the VDSL enabled wall jack outlet. Once the gateway recognizes the VDSL connection, Broadband LED flashes green for a brief period of time, and then turns solid green.



**Figure 5: VDSL Broadband Connection**

**Note** The HomePortal 3801HGV gateway must be connected to the VDSL wall jack. Do not connect the DSL port of the HomePortal 3801HGV gateway to a telephone wall jack.

## Connecting VoIP Interface

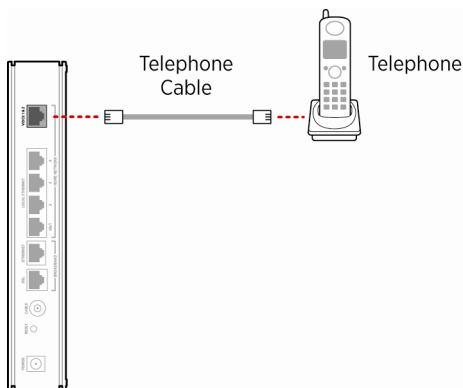
The HomePortal 3801HGV gateway includes one RJ-14 port (Voice 1 & 2) with the capacity to support 2 phone lines using a splitter or multi-jack adapter.



**Warning:** Do not connect the VoIP lines to your current home telephone wiring without contacting your service provider. This requires special installation, especially if your home has an alarm system, which requires special wiring.

Follow these steps to connect the VoIP phone to the Voice 1 & 2 port of the gateway:

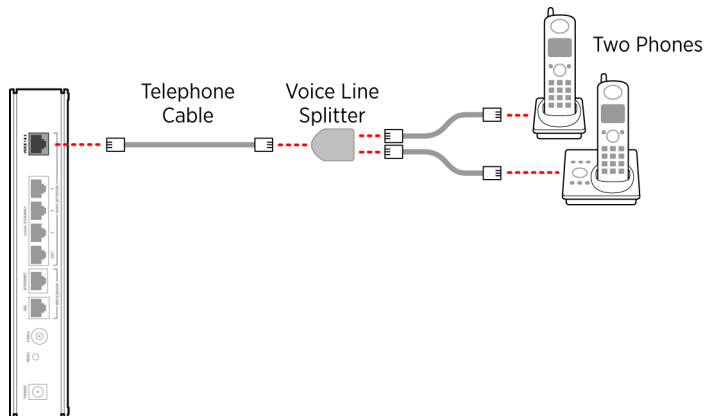
1. To connect 1 phone:
  - a. Connect one end of the phone cable to the HomePortal 3801HGV gateway **Voice 1&2** port.
  - b. Connect the other end of the phone cable to the phone jack.



**Figure 6: VoIP Connection without Splitter**



2. To connect 2 phones:
  - a. Connect one end of the line splitter to the HomePortal 3801HGV gateway **Voice 1&2** port.
  - b. Connect the phone cables to the first and second jack of the splitter.



**Figure 7: VoIP Connection Using Splitter**

## Connecting HPNA Interface to IPTV set top Box

The HomePortal 3801HGV gateway can be configured to use IPTV services through the cable port.

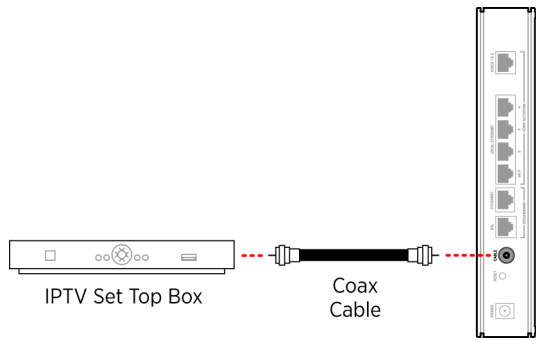
Follow these steps to connect the gateway to the set top box:

1. Connect one end of the coaxial cable to the CABLE port and the other end to the CABLE IN port of Ethernet over Coax adapter.
2. Connect one end of the Ethernet cable to the Ethernet port of Ethernet over Coax adapter and the other end to the Ethernet port on the set top box.

---

**Note** The Ethernet over Coax adapter is independently powered, and should be installed close to a power outlet. Refer to the manufacturer's instructions that came with the Ethernet over Coax adapter.

---



**Figure 8: IPTV Connection VDSL over Coax**

**See Also**

[Introducing the HomePortal 3801HGV Gateway](#) on page 1

[Accessing the User Interface](#) on page 11

## CHAPTER 3

# Accessing the User Interface

To launch the HomePortal 3801HGV gateway user interface, access the Home page of the gateway by entering one of the following URLs into a compatible browser on the computer connected to the gateway:


- <http://gateway.2Wire.net>
- <http://home>
- <http://192.168.1.254>

The **Home** page appears.



Home Services Settings Site Map

### Summary

 <b>Broadband</b> ↓ Kbps ↑ Kbps	 <b>Wireless</b> Network Name 2WIRE054	 <b>Firewall</b> Status Enabled	 <b>3801HGV</b> Serial Number: 38091 3000054
--	---	--	---

### Home Network Devices

 <b>John</b> <a href="#">Access Files</a> <a href="#">Device Details</a>	 <a href="#">Voice</a>
---	---

### Top Networking Features

- [Wireless](#) - modify security or settings
- [Refresh your Broadband Connection](#) - reconnect your broadband connection
- [Restart your System](#) - reboot
- [Home Networking](#) - find a computer, share a file
- [System Password](#) - secure your system with a password
- [Gaming and Communications](#) - modify your firewall settings

The **Home** page has the following five panes:

- System Link Tabs
  - Home
  - Services
  - Settings
  - Site Map
- Summary
- New TELCO Services Features
- Quick Service Links
- Home Network Devices
- Top Networking Features

## System Link Tabs

### Home

The **Home** tab provides the most relevant information about your broadband service at a glance. It also provides links to access more detailed information.

### Services

The **Services** tab provides links to view the status of file sharing, Web servers, VoIP, and IPTV services. You can also configure your VoIP interfaces and view the VoIP interface status and statistics.

### Settings

The **Settings** tab provides links to view and configure system information. Also, other sub-tabs let you configure Broadband services, LAN settings, Firewall settings, and perform Diagnostics on your gateway.

### Site Map

The **Site Map** tab provides a tree-diagram view of the user interface. Click any link on this page to access the relevant page. This helps you to access the desired page directly without having to navigate through the nesting on the system link tabs.

## Summary

The **Summary** pane displays the bandwidth status beside the **Broadband** icon, network name (SSID) of the gateway beside the **Wireless** icon, security status beside the **Firewall** icon, and serial number beside the gateway icon. Click an icon to access the relevant page directly.

## Quick Service Links

The **Quick Service** Links pane displays the Voice link. Click the link to access the Voice page directly.

## Home Network Devices

The **Home Network Devices** pane displays all devices that are connected to the gateway. You can click the links to view the device details or view the shared files of the connected devices.

## Top Networking Features

The **Top Networking Features** pane provides shortcuts to directly access the most commonly used gateway pages. Click a link to access the relevant page directly.

### See Also

[Introducing the HomePortal 3801HGV Gateway](#) on page 1

[Installing the HomePortal 3801HGV Gateway](#) on page 4

[Configuring Internet Connection](#) on page 14

## CHAPTER 4

# Configuring Internet Connection

### Objective

To configure the Internet connection on the gateway.

You must have PPP Authentication credentials to complete this configuration. Also, ensure the Broadband LED on the front panel of the gateway is solid green and the first computer is communicating with the gateway.

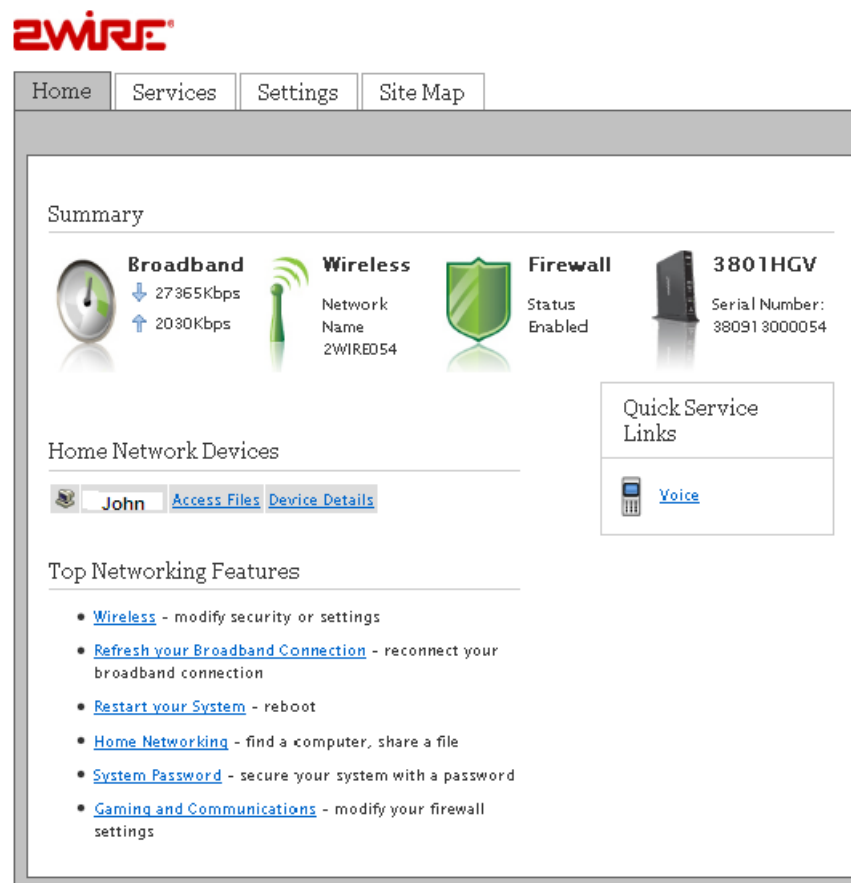
---

**Note** PPP credentials are provided by your ISP

---

### Steps

1. Access the **Home** page of the gateway.



2. Navigate to **Settings > Broadband > Link Configuration**. The **Link Configuration** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status
Link Configuration
Routing
Multicast
DNS Resolution

**Warning** Modifying the settings on this page can impact the ability of devices on your private network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on your private network.

**Broadband Interface**

Choose Interface type: Automatic Ethernet/DSL

**DSL and ATM**

DSL Line Selection: Automatic

**Connection Type**

Connection Type: PPPoE

**PPP Authentication and Settings**

Username and password are required if you select PPPoE or PPPoA connection type

Username:

Password:

Confirm Password:

PPP on Demand:  Minutes (0="always-on" connection)

**Broadband IP Network (Primary Connection)**

**IP Addressing:**

Obtain IP address automatically (dynamic IP or DHCP)

Manually specify IP address settings:

IP Address:

Subnet Mask:

Default Gateway:

**DNS:**

Obtain DNS information automatically

Manually specify DNS information:

Primary Server:

Secondary Server:

Domain Name:

**Use Broadband IPs on LAN:**  Enable (allow devices on the LAN to be configured with a broadband IP and bridge traffic)

Current IP/subnet mask: 172.16.8.12 / 255.255.255.248

Specify usable subnet mask:

Auto Firewall Open:

**System MAC Address:**

Use the built-in system MAC address: 00:26:50:7d:86:90

Override the built-in MAC address

Specify MAC address:

**Upstream MTU:**

3. Select **Automatic Ethernet/DSL** from the **Choose Interface Type** drop-down list. This enables the gateway to automatically detect the type of connection used to connect to the Broadband service.
4. Select **Automatic** from the **DSL Line Selection** drop-down list. This lets you select RJ-11 or coax interface for connecting the DSL connection to your gateway.
5. Select PPPoE from the **Connection Type** drop-down list. PPPoE user credentials authenticate the subscriber on the server of the ISP.
6. Enter the PPPoE **Username** and **Password** in the **PPP Authentication and Settings** section. This information is provided by the ISP.
7. Leave the **PPP on Demand** field as is, unless otherwise indicated by your ISP. If you increase the value, the Internet connection becomes idle after that duration.
8. Leave the selected radio buttons **Obtain IP address automatically (dynamic IP or DHCP)** and **Obtain DNS information automatically** in the **Broadband IP Network (Primary Connection)** section as they are, if you do not want to configure the associated information statically. Contact your ISP to get associated information for configuring IP address and DNS statically.
9. Leave the **Use Broadband IPs on LAN** and **System MAC Address** settings as they are, if you do not want to enable bridging on your gateway.
10. Leave the **Upstream MTU** value as is. This is the maximum size allowed on data packets, that are communicated on the network of your ISP.
11. Click **Save**. The Internet LED on the gateway becomes solid green and you can access the Internet.
12. Open a Web browser and access [www.google.com](http://www.google.com).

### See Also

[Introducing the HomePortal 3801HGV Gateway](#) on page 1

[Installing the HomePortal 3801HGV Gateway](#) on page 4

[Accessing the User Interface](#) on page 11



## CHAPTER 5

# Viewing Subscribed Services Status

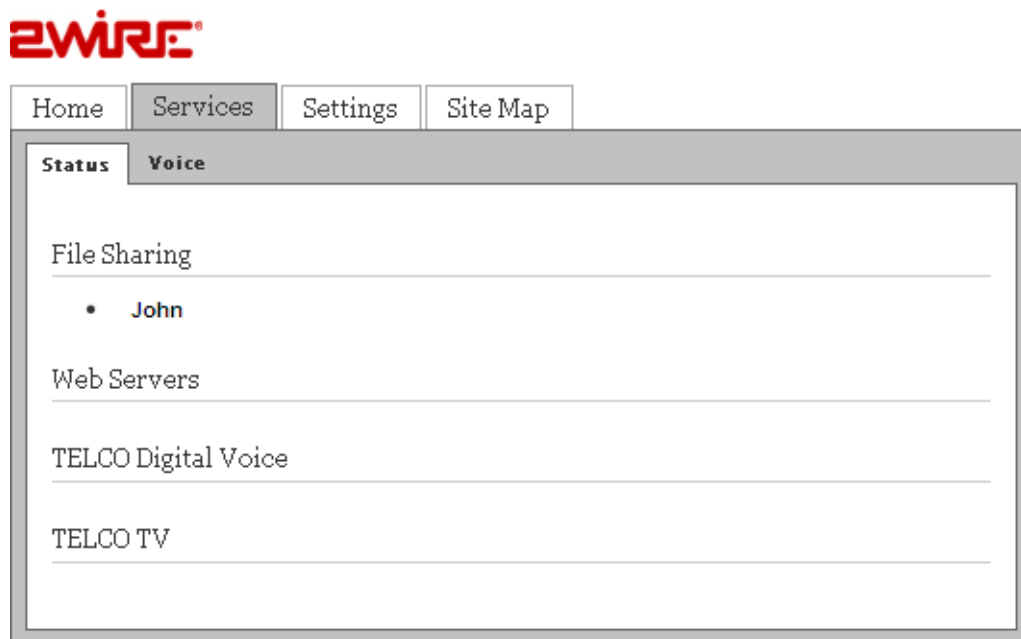
---

**NOTE TO REVIEWER:** We need images of the **Status** tab with all services enabled. We also need information about the following sections: **Web Servers**, **TELCO Digital Voice**, **TELCO TV**. What do these sections display? Will the user be able to see all these sections if he has not subscribed for a particular service?

---

This chapter provides information about the **Status** tab. You can view the status of your subscribed services in this tab.

To view the **Status** tab, navigate to **Services > Status**. The **File Sharing** page appears.



Click **Remote Access configuration** link to enable Web remote access on your system.

Refer to the following table for description of the parameters listed on the **Status** page:

<b>Parameter</b>	<b>Description</b>
<b>File Sharing</b>	Displays all devices connected to the HomePortal 3801HGV gateway. You can share files among these devices.
<b>Web Servers</b>	Displays the Web servers configured to the gateway.
<b>TELCO Digital Voice</b>	Displays the status of the VoIP lines and associated servers.
<b>TELCO TV</b>	Displays the IPTV parameters.

## CHAPTER 6

# Configuring Voice-Based Services

This chapter provides information about the tasks that you can perform in the **Voice** tab. Following are the links under the **Voice** tab, and associated tasks:

- **Status**
  - [Viewing Status](#) on page 19
- **Server**
  - [Configuring SIP Server](#) on page 20
- **Line**
  - [Configuring Phone Lines](#) on page 22
- **Phone**
  - [Configuring Phones](#) on page 23
- **Stats**
  - [Viewing External Line Statistics](#) on page 24

---

**Note** You can access this tab only if you have subscribed for the VoIP service from your provider.

---

## Viewing Status

This topic provides information about the **Status** page under the **Voice** Tab. You can view the status of your phone lines and servers on this page.

To view the server and line status, navigate to **Services > Voice > Status**. The **Status** page appears.



Home Services Settings Site Map

Status Voice

Status Server Line Phone Stats

Status

Servers:

Name	Associated Line(s)
2wire1	2wire1
2wire2	2wire2

Line Status:

Line	Number	Status
Line 1	2wire1	Disabled Voice Service Disabled: No Active VOIP service has been subscribed.
Line 2	2wire2	Disabled Voice Service Disabled: No Active VOIP service has been subscribed.

You can view the following information on this page:

Parameter	Description
<b>Servers</b>	
<b>Name</b>	Displays the name of the configured SIP server.
<b>Associated Line</b>	Displays the phone lines associated with the SIP server.
<b>Line Status</b>	
<b>Line</b>	Displays the name of the configured line.
<b>Number</b>	Displays the phone number of the configured line.
<b>Status</b>	Displays the status of the configured line on the gateway. The status can be <b>Registering</b> , <b>Enabled</b> , or <b>Disabled</b> .

## Configuring SIP Server

### Objective

To configure the SIP server.

The SIP server provides a location service which registers one or more IP addresses to identify certain names or resources on the Internet.

Your service provider gives you all the information required to configure the SIP server.

## Steps

1. Navigate to **Services > Voice > Server**. The **Server** page appears.

The screenshot shows the Z-WIRE web interface. At the top, there is a navigation bar with 'Home', 'Services', 'Settings', and 'Site Map'. Below this, there are tabs for 'Status' and 'Voice'. The 'Voice' tab is active, and the 'Server' sub-tab is selected. The main content area shows a form for configuring a server. The form includes a 'Server' section with the following fields: 'Enable' (checked), 'Server Name' (profile 1), 'SIP Registrar Server' (166.167.168.169), 'Registrar Server Port' (5060), 'User Agent Domain' (Voice Service), 'Register Expire Time' (3600), and 'Re-register Interval' (300). There are 'Save' and 'Add New Server' buttons at the bottom of the form.

2. Select the **Enable** check box.
3. Type in a name for the server in the **Server Name** text box.
4. Enter the server name in the **SIP Registrar Server Name** text box. This can be an IP address or a name provided by the service provider.
5. Enter the server port in the **Registrar Server Port** text box. The port number will be provided by the service provider. The default port is 5060.
6. Enter the domain name in the **User Agent Domain** text box. This will be provided by the service provider.
7. Enter the expire time in the **Register Expire Time** text box. This will be provided by the service provider.
8. Enter the re-register interval time in the corresponding text box. This will be provided by the service provider.
9. Click **Save**.

---

**Note** If your service provider has multiple SIP servers, you may need to configure additional servers on this page. You can do this by clicking the **Add New Server** button.

---

## Configuring Phone Lines

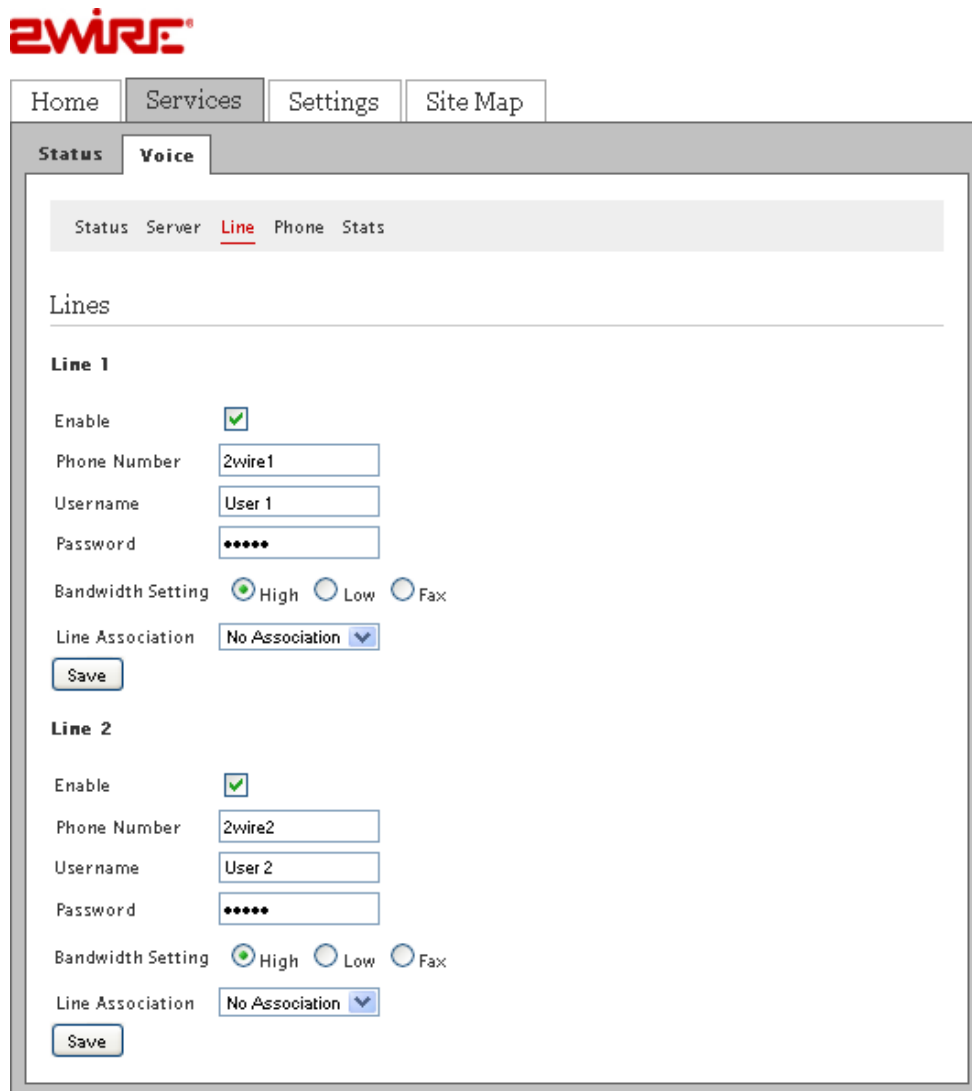
### Objective

To configure the phone lines.

You can configure your telephone number on this page. You can configure 2 telephone lines at a time in the HomePortal 3801HGV gateway. You can also configure a user name and password for your account to prevent unauthorized access.

### Steps

1. Navigate to **Services > Voice > Line**. The **Line** page appears.



The screenshot shows the 2Wire configuration interface. At the top, there is a navigation bar with tabs for Home, Services, Settings, and Site Map. Below this, there is a sub-navigation bar with tabs for Status and Voice. The main content area is titled 'Lines' and contains two sections for configuring phone lines, labeled 'Line 1' and 'Line 2'. Each section has the following fields: 'Enable' (checkbox), 'Phone Number' (text input), 'Username' (text input), 'Password' (password input), 'Bandwidth Setting' (radio buttons for High, Low, Fax), and 'Line Association' (dropdown menu). A 'Save' button is located below each section. The 'Enable' checkbox for Line 1 is checked.

**2Wire**

Home Services Settings Site Map

Status Voice

Status Server Line Phone Stats

Lines

**Line 1**

Enable

Phone Number 2wire1

Username User 1

Password •••••

Bandwidth Setting  High  Low  Fax

Line Association No Association

Save

**Line 2**

Enable

Phone Number 2wire2

Username User 2

Password •••••

Bandwidth Setting  High  Low  Fax

Line Association No Association

Save

2. Select the **Enable** check box in the **Line 1** section. This activates the line for use.

3. Enter the phone number, user name, and the password in corresponding text boxes. This will be given by the service provider.
4. Select the appropriate bandwidth setting as directed by the service provider.
5. Select the appropriate server to associate with the line in the **Line Association** drop-down list box.
6. Click **Save**.
7. Configure the second phone line (if present) in the **Line 2** section, and click **Save**.

## Configuring Phones

### Objective

To configure phones.

---

---

**NOTE TO REVIEWER:** Why do we need to configure phones separately from lines? Do we need different types of phones for VoIP? Do we set up the physical phones in this section?

---

---

## Steps

1. Navigate to **Services >Voice > Phone**. The **Phone** page appears.

2. Enter the location of the phone in the corresponding text box in the **Phone: Phone 1** section.
3. Select a line that you have configured in the **Association** drop-down list box.
4. Select the **Service Outage** check box if <insert info here>.

---

**NOTE TO REVIEWER:** Need info about the **Service Outage** check box.

---

5. Click **Save**.
6. Configure the second phone (if present) in the **Phone: Phone 2** section, and click **Save**.

---

**Note** You will get all information regarding the location, association, and service outage for your phone from the service provider.

---

## Viewing External Line Statistics

To view call statistics, navigate to **Services > Voice > Stats**. The **Stats** page appears.



To reset information about each configured line on this page, scroll down and click the **Reset** button at the end of the information for that particular line.

You can view the following information on this page:

Parameter	Description
<b>Line 1</b>	Displays status information about the phone line in use, as well as its current state.
<b>Registration Status</b>	Displays registration information about the phone line in use.
<b>Call Summary</b>	
<b>Current Call</b>	Displays call summaries for the current call.
<b>Last Completed Call</b>	Displays call summaries for the for your last completed call.
<b>Cumulative Since Last Reset</b>	Displays collective call information since you last reset the page.
<b>Call Statistics</b>	
<b>Current incoming calls</b>	Displays complete call statistics of the current incoming call(s).
<b>Current outgoing calls</b>	Displays complete call statistics of the current outgoing call(s).
<b>Last incoming call</b>	Displays complete call statistics of the last incoming call.
<b>Last outgoing call</b>	Displays complete call statistics of the last outgoing call.

	<b>All incoming calls</b>	Displays complete call statistics of all incoming calls.
	<b>All outgoing calls</b>	Displays complete call statistics of all incoming calls.

### See Also

[Viewing Subscribed Services Status](#) on page 17

[Troubleshooting 3801HGV Gateway](#) on page 109

## CHAPTER 7

# Setting Up System Information

This chapter provides information about the tasks you can perform in the **System Info** tab. Following are the links under the **System Info** tab, and associated tasks:

- **Status**
  - [Viewing System Information](#) on page 27
- **Password**
  - [Setting Up System Password](#) on page 29
- **Date & Time**
  - [Configuring Date and Time](#) on page 30
- **Event Notification**
  - [Enabling Event Notifications](#) on page 32

## Viewing System Information

View your system information at a glance. Find details pertaining to your system including the manufacturer name, model and serial number, and hardware and software versions. To view the system information, navigate to **Settings > System Info > Status**. The **Status** page appears.

**2Wire**

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Status Password Date & Time Event Notifications

System Information

<b>Manufacturer:</b>	2Wire, Inc.
<b>Model:</b>	3801HGV
<b>Serial Number:</b>	380913000054
<b>Hardware Version:</b>	000778-002
<b>Software Version:</b>	6.3.5.10-enh.tm
<b>Key Code:</b>	52AN-2374-WHE2-22AZ-B275
<b>First Use Date:</b>	January 18, 2010
<b>Current Date &amp; Time:</b>	Monday, January 18, 2010
	10:57:09 PM
	Pacific Standard Time
<b>Time Since Last Boot:</b>	0 day 16:25:22
<b>DSL Modem</b>	8.1.0
<b>System Password:</b>	None

You can view the following information on the **Status** page:

Parameter	Description
<b>Manufacturer</b>	Name of the gateway manufacturer.
<b>Model</b>	Model number of the gateway.
<b>Serial Number</b>	Serial number of the gateway. The serial number is also printed on the gateway.
<b>Hardware Version</b>	Hardware version number of the gateway.
<b>Software Version</b>	Version number of the software used for the gateway.
<b>Key Code</b>	Key code of the gateway.
<b>First Use Date</b>	Date when the gateway was powered on for the first time out of factory.
<b>Current Date and Time</b>	Your current date and time.
<b>Time Since Last Boot</b>	Time elapsed since you last booted the system.
<b>DSL Modem</b>	Hardware version of the DSL modem.
<b>System Password</b>	Displays <b>Default</b> if you use the default system for your system. Displays <b>Custom</b> if you have created your own password for your system. Displays <b>None</b> if you have not enabled password protection for your system.

## Setting Up System Password

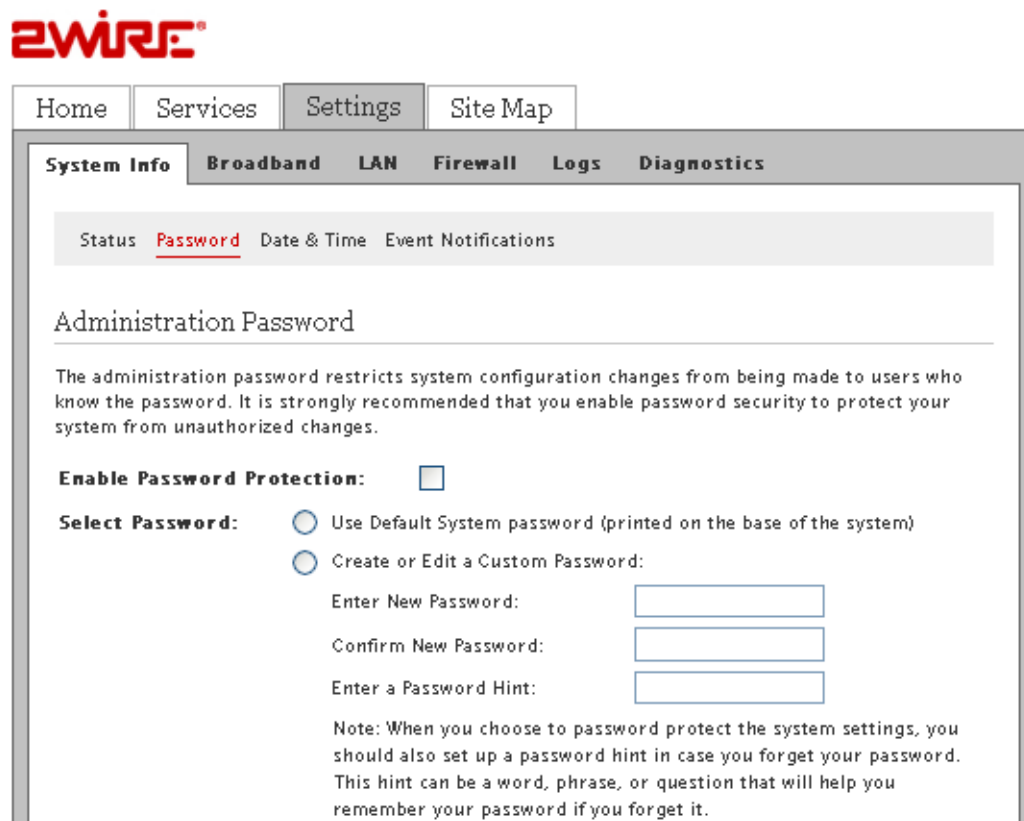
### Objective

To set up the system password.

This task allows you to set up a password for your system in order to protect it against unauthorized access. You can either set up the default system password, or create your own password.

### Steps

1. Navigate to **Settings > System Info > Password**. The **Password** page appears.



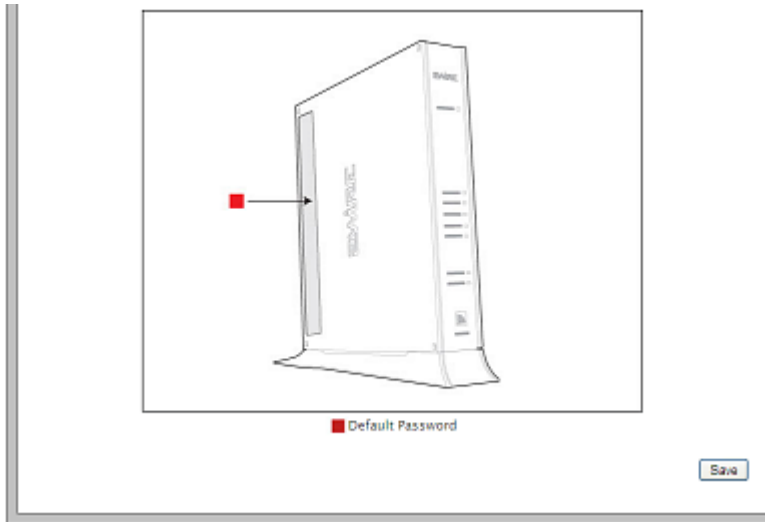
The screenshot shows the ZWIRE web interface. At the top, there is a navigation bar with tabs for Home, Services, Settings, and Site Map. Below this, there is a sub-navigation bar with tabs for System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The 'System Info' tab is selected, and within it, the 'Password' sub-tab is active. The page title is 'Administration Password'. Below the title, there is a paragraph explaining that the administration password restricts system configuration changes. There are three main sections: 'Enable Password Protection' with an unchecked checkbox, 'Select Password' with two radio button options, and three input fields for 'Enter New Password', 'Confirm New Password', and 'Enter a Password Hint'. A note at the bottom explains the purpose of the password hint.

2. You can perform one of the following tasks:
  - Set the default system password. The default system password is displayed on the side of the gateway device
  - Create your own system password

### Setting Default System Password

To set the default system password:

1. Select the **Enable Password Protection** box.
2. Click **Use Default System password (printed on the side of the gateway)**.  
The following figure shows the default password printed on the side of the gateway device.



## Creating Your System Password

To create your own system password:

1. Select the **Enable Password Protection** box.
2. Click **Create or Edit a Custom Password**.
3. Enter a password in the **Enter New Password** text box. The password is case-sensitive, and can contain up to 31 alpha-numeric characters with no spaces.
4. Enter the same password in the **Confirm New Password** text box.
5. Enter a hint in the **Enter a Password Hint** text box. A password hint can be a word, a phrase, or a question that can help you in case you forget your password.

---

**Note** Although not required, it is strongly recommended that you enter a hint to act as a reminder.

---

6. Click **Save**.

## Configuring Date and Time

### Objective

To configure the date and time of the system.

This task allows you to configure the correct date and time for your system. You can either automatically set up the date and time, or configure it manually.

## Automatically Setting up Date and Time

To automatically set up date and time:

1. Navigate to **Settings > System Info > Date & Time**. The **Date & Time** page appears.

**2WIRE**

Home Services **Settings** Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Status Password **Date & Time** Event Notifications

**Current Time Settings**

**Time Zone:** (GMT-08:00) Pacific Time (US & Canada): Tijuana

Date: Monday, January 18, 2010

Time: 10:59:41 PM

**Time Configuration**

**Manual Configuration:**  Override automatic time configuration

Set Time:  :  :  (hh:mm:ss)

Set Date:  /  /  (yyyy/mm/dd)

**Daylight Savings Time:**  Automatically adjust for daylight savings

**Internet Time Servers (NTP)**

**Time Servers:**

ntp1.2wire.com

ntp2.2wire.com

ntp3.2wire.com

ntp4.2wire.com

ntp.ucsd.edu

Save

2. Select your time zone in the **Current Time Settings** area.
3. Click **Save**.

---

**Note** Do not forget to select the **Daylight Savings Time** check box in the **Time Configuration** area if Daylight Savings Time is observed in your state.

---

## Manually Configuring Date and Time

To manually configure the date and time:

1. Navigate to **Settings > System Info > Date & Time**. The Time Configuration section appears.

Time Configuration

**Manual Configuration:**  Override automatic time configuration

Set Time:  :  :  (hh:mm:ss)

Set Date:  /  /  (yyyy/mm/dd)

**Daylight Savings Time:**  Automatically adjust for daylight savings

2. Select the **Override automatic time configuration** box in the **Time Configuration** section.
3. Set the time in the corresponding space in the hh:mm:ss format.
4. Set the date in the corresponding space in the yyyy/mm/dd format.
5. Select the **Daylight Savings Tim** check box.
6. Click **Save**.

---

**Note** When you configure the date and time manually, do not forget to select the **Override automatic time configuration** check box.

---

## Enabling Event Notifications

### Objective:

To view notifications of service impacting events.

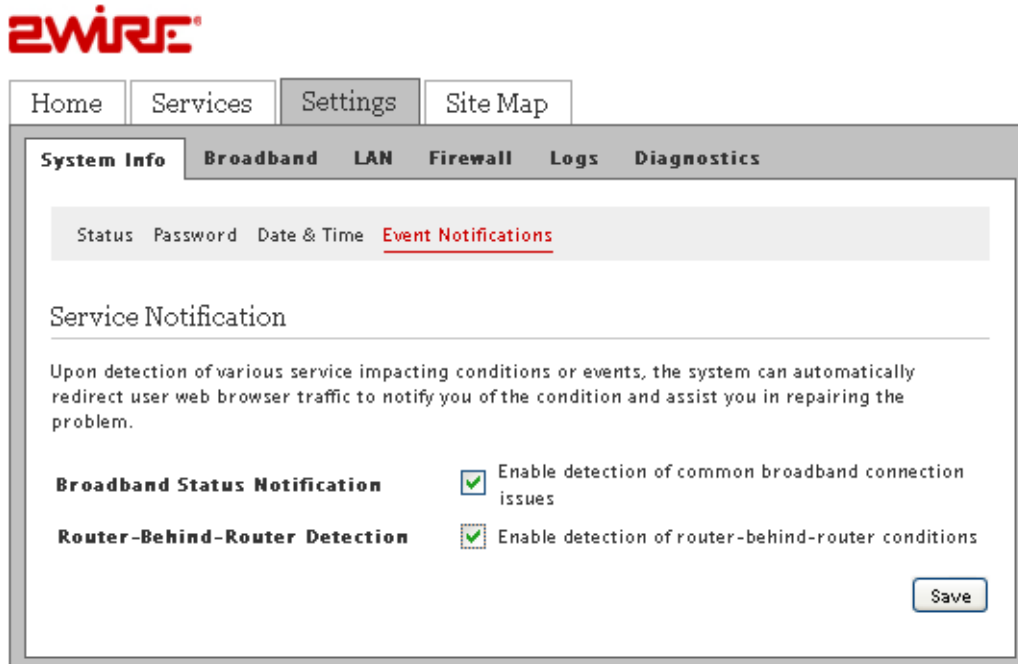
This task allows you to enable/disable event notifications. Enabling event notifications assists you in detecting any service-impacting conditions that may need repair. After enabling event notifications, the system automatically notifies you of the service-impacting conditions.



## Enabling Notifications

To enable notifications:

1. Navigate to **Settings > System Info > Event Notifications**. The **Event Notifications** page appears.



2. Select the **Broadband Status Notification** and/or **Router-Behind-Router Detection** check boxes.
3. Click **Save**.

---

**Note** To enable router-behind-router detection, make sure that DHCP and NAT are enabled, and the gateways are not in bridge mode.

---

## Disabling Notifications

To disable notifications:

1. On the **Event Notifications** page, clear the **Broadband Status Notification** and/or **Router-Behind-Router Detection** check boxes.
2. Click **Save**.

## See Also

[Using Diagnostics Features](#) on page 93

[Troubleshooting 3801HGV Gateway](#) on page 109

## CHAPTER 8

# Configuring Broadband Settings

This chapter provides information about the tasks you can perform in the **Broadband** tab. Following are the links under the Broadband tab, and associated tasks:

- **Status**
  - [Viewing Broadband Status](#) on page 34
- **Link Configuration**
  - [Configuring Bridge Mode](#) on page 40
- **Routing**
  - [Adding Static Routes](#) on page 42
- **Multicast**
  - [Configuring IP Multicast Sessions](#) on page 43
  - [Viewing Multicast Statistics](#) on page 44
- **DNS Resolution**
  - [Resolving Domain Name](#) on page 47

## Viewing Broadband Status

This task lets you view the connectivity status, Internet connection details, modem type, and traffic statistics. You can also reset the page to view up-to-date information.

---

**Note** Broadband and Service LEDs must be solid green on the front panel of the device. Also, ensure that the user interface is accessible.

---

To view broadband status, navigate to **Settings > Broadband > Status**. The **Status** page appears.

The following figure displays the **Summary Status** section of the **Status** page.



Refer to the following table for description of the **Summary Status** parameters listed on the **Status** page:

Parameter	Description
<b>Internet</b>	Status of the Internet Connection. This displays <b>Connected</b> when the ISP activates your Internet connection.
<b>DSL Link</b>	Status of the DSL connection. This displays <b>Connected</b> when the DSL port of the gateway is connected to the telephone jack. Ensure that your service provider activates the VDSL connection.

The following figure displays the **Internet Details** section of the **Status** page.

## Internet Details

<b>Broadband Link Type:</b>	Built in modem - VDSL
<b>Connection Type:</b>	PPPoE
<b>User Name:</b>	test
<b>Current Internet Connection:</b>	
IP Address:	172.16.8.16
Subnet Mask:	255.255.255.255
Default Gateway:	172.16.8.1
Primary DNS:	202.54.29.5
Secondary DNS:	202.54.10.2
Host Name:	
Domain:	
MAC Address:	00:26:50:7d:86:90
MTU:	1492
PPPoE Access Concentrator:	labdefault
PPPoE Service:	

Refer to the following table for description of the **Internet Details** parameters listed on the status page:

Parameter	Description
<b>Broadband Link Type</b>	Type of broadband connection.
<b>Connection Type</b>	Identifies the method by which the gateway connects to the Internet Service Provider (ISP). The methods can be: <ul style="list-style-type: none"> <li>• PPPoE</li> <li>• PPPoA</li> <li>• Direct IP</li> </ul>
<b>User Name</b>	User credentials to connect with your ISP. Your user name was either assigned to you or configured by you during the installation process. The correct user name is required to successfully connect to the Internet.
<b>Current Internet Connection</b>	
<b>IP Address</b>	IP address assigned by the ISP to the gateway for connecting to the Internet.
<b>Subnet Mask</b>	Used in conjunction with your Internet address.
<b>Default Gateway</b>	Default gateway is a server that assigns an IP address to your gateway for accessing the Internet.
<b>Primary DNS</b>	IP address of the primary DNS server that the gateway uses for DNS name resolution. DNS allows Internet users to specify a name (domain name) to reach a Web page (for example, www.domainname.com) instead of its Internet address (for example, 111.222.111.222). When you enter the name of a Web location (URL), the DNS looks up the name and resolves it to the Internet address of the Web page.
<b>Secondary DNS</b>	Used as a backup if the Primary DNS fails to respond.
<b>Host Name</b>	Host name is a label that is configured on the gateway.
<b>Domain</b>	Domain associates your gateway with your ISP on the broadband link.
<b>MAC Address</b>	MAC address of the gateway.
<b>MTU</b>	Maximum Transmission Unit is the maximum size of packets that are communicated on your ISP network.
<b>PPPoE Access Concentrator</b>	PPPoE server name.
<b>PPPoE Service</b>	Type of PPPoE service being used.

The following figure displays the **DSL Details** section of the **Status** page.

DSL Details		
<b>Modem Type:</b>	Built in modem - VDSL	
<b>Connection Type:</b>		
<b>DSL Line (Wire Pair):</b>	RJ-11	
<b>Current DSL Connection:</b>		
	<b>Down</b>	<b>Up</b>
Rate:	27365 kbs	2030 kbs
Max Rate:	67640 kbs	Not Available
Noise Margin:	25.8 dB	Not Available
Attenuation:	4.4 dB	Not Available
Output Power:	7.1 dBm	-31.0 dBm
Protocol:	G.993.2	
Channel:	Interleaved	
DSLAM Vendor Information	Country: {65461} Vendor: {CXY} Specific: {16898 }	
Rate Cap:	27368 kbs	
Attenuation @ 300kHz:	2.6 dB	
Required Impulse Noise Protection:	0	
Uncanceled Echo:	0.0 dB	Ok
VCO Frequency Offset:	0.0 ppm	Ok
Final Receive Gain:	-5.0 dB	Ok
Excessive Impulse Noise:	0	Ok

Refer to the following table for description of the **DSL Details** parameters listed on the status page:

Parameter	Description
<b>Modem Type</b>	Displays modem type: either built-in VDSL modem or external broadband modem through Ethernet.
<b>Connection Type</b>	Method by which the gateway connects to the ISP. The method can be: <ul style="list-style-type: none"> <li>• Direct IP</li> <li>• PPPoE</li> </ul>
<b>DSL Line (Wire Pair)</b>	Line 1 (inner pair), Line 2 (outer pair), or searching for DSL signal. During installation, the gateway auto-detects whether the DSL signal is on line 1 or line 2.
<b>Current DSL Connection</b>	

Parameter	Description
<b>Rate</b>	Upload and download speeds in kilobytes per second.
<b>Max Rate</b>	Maximum speed attained while uploading and downloading the data in kilobytes per second.
<b>Noise Margin</b>	Current downstream and upstream noise margin in dB.
<b>Attenuation</b>	Current downstream and upstream DSL attenuation in dB.
<b>Output Power</b>	Current downstream and upstream DSL transmit and receive power in dB.
<b>Protocol</b>	Protocol used to communicate between your gateway and your ISP
<b>Channel</b>	Setting in this field is determined by your ISP's DSLAM equipment. Values are Fast or Interleaved.
<b>DSLAM Vendor Information</b>	Lists information about the DSLAM, including country, DSLAM vendor, and specifics.
<b>Rate Cap</b>	Configured DSL service downstream speed.
<b>Attenuation @ 300kHz</b>	Measurement of the decrease in downstream signal strength in kilobytes per second.
<b>Required Impulse Noise Protection</b>	Measurement of how much impulse noise can be mitigated. Dependent on the current line configuration.
<b>Uncanceled Echo</b>	Measurement of the uncanceled echo relative to the background noise on the line. This is an indication of how much the uncanceled echo is affecting DSL performance, rather than an absolute measurement of the uncanceled echo.
<b>VCXO Frequency Offset</b>	Indicates the difference of crystal frequency in parts per million (ppm) on the ports of the gateway and the DSLAM.
<b>Final Receive Gain</b>	Indicates the current receive gain setting (in dB), which will depend on the length of the DSL line.
<b>Excessive Impulse Noise</b>	Indicates to what degree impulse noise is present on the line.

The following figure displays the **Traffic Statistics** section of the **Status** page.

Traffic Statistics				
IP Traffic	Bytes	Packets	Errors	%
Transmit:	310224	4432	0	0
Receive:	372578	4646	0	0

Refer to the following table for description of the **Traffic Statistics** parameters listed on the status page:

Parameter	Description
<b>Transmit</b>	Cumulative number of bytes, IP packets, errors, and percentage of errors transmitted.
<b>Recieve</b>	Cumulative number of bytes, IP packets, errors, and percentage of errors received.

The following figure displays the **DSL Link Errors** section of the **Status** page.

**DSL Link Errors**

Collected for 13:00:35

	Since	Current	Current	Time Since
	Reset 24-hr int. 15-min int. Last Event			
<b>DSL</b>				
Link Retrans:	0	0	0	0:00:00
DSL Training Errors:	0	0	0	0:00:00
Training Timeouts:	0	0	0	0:00:00
Loss of Framing Failures:	0	0	0	0:00:00
Loss of Signal Failures:	0	0	0	0:00:00
Loss of Power Failures:	0	0	0	0:00:00
Loss of Margin Failures:	0	0	0	0:00:00
Cum. Sec. w/Impulsive Events:	10	10	0	0:05:57
Cum. Seconds w/Errors:	0	0	0	0:00:00
Cum. Sec. w/Severe Errors:	0	0	0	0:00:00
Corrected Blocks:	18274	18274	0	1:05:47
Uncorrectable Blocks:	0	0	0	0:00:00
DSL Unavailable Seconds:	29	29	0	13:00:05

[Reset Statistics](#)

Refer to the following table for description of the **DSL Link Errors** parameters listed on the status page:

Parameter	Description
<b>Link Retrans</b>	Number of DSL retrains since the gateway was last restarted, and the time elapsed since the last retrain.
<b>DSL Training Errors</b>	Number of failed DSL retrains since the gateway was last restarted, and the elapsed time since the last failed retrain.
<b>Training Timeouts</b>	Number of timeouts waiting for response from ATU-C since the 2Wire gateway was last restarted, and the elapsed time since the last initialization timeout.
<b>Loss of Framing Failures</b>	Number of DSL loss of framing failures since the gateway was last restarted, and the elapsed time since the last line search initialization.
<b>Loss of Signal Failures</b>	Number of DSL loss of signal failures since the 2Wire gateway was last restarted, and the elapsed time since the last loss of signal failure.
<b>Loss of Power Failures</b>	Number of DSL loss of power indications from the ATU-C since the gateway was last restarted, and the elapsed time since the last loss of power indication.
<b>Loss of Margin Failures</b>	Number of DSL loss-of-margin failures at current data rate since the 2Wire gateway was last restarted, and the elapsed time since the last loss of margin failure.
<b>Cum. Sec. w/Impulsive Events</b>	Number of impulsively errored seconds since the gateway was last restarted, and the elapsed time since the last impulsively errored second.
<b>Cum. Seconds w/Errors</b>	Number of cumulative errored seconds since the gateway was last restarted, and the elapsed time since the last error.
<b>Cum. Sec. w/Severe Errors</b>	Number of severely errored seconds since the gateway was last restarted, and the elapsed time since the last severely errored second.
<b>Corrected Blocks</b>	Number of corrected DSL superframes that have data errors detected during reception.

Parameter	Description
<b>Uncorrectable Blocks</b>	Number of uncorrected DSL superframes that have data errors detected.
<b>DSL Unavailable Seconds</b>	Number of times the ISP connection was established since the statistics were last reset, and the elapsed time since the last establishment.

## Resetting Statistics on Status Page

After rectifying the issues that are seen in different sections of the **Status** page, you must reset this page to determine if the issue is resolved. To do this, click the **Reset Statistics** button at the bottom of the **Status** page.

## Configuring Bridge Mode

### Objective

To configure bridge mode.

Bridge mode is used to configure devices on the LAN with a broadband IP. When the gateway is into bridge mode you can use a supplementary network or a third party router to handle the traffic. The gateway will only function as a direct connection to the phone line.

---

**Note** By default, the gateway is configured in the routing mode. When routing is disabled, the NAT and the DHCP server are also disabled. Confirm with the ISP that the WAN protocol is compatible with bridging mode.

---



## Steps

1. Navigate to **Settings > Broadband > Link Configuration**. Configure the following section of the **Link Configuration** page to enable the bridge mode and add supplementary networks:

The screenshot shows the 'Link Configuration' page with the following settings:

- Use Broadband IPs on LAN:**  Enable (allow devices on the LAN to be configured with a broadband IP and bridge traffic)
- Current IP/subnet mask: 172.16.8.16 / 255.255.255.224
- Specify usable subnet mask:
- Auto Firewall Open:
- System MAC Address:**
  - Use the built-in system MAC address: 00:26:50:7d:86:90
  - Override the built-in MAC address
  - Specify MAC address:
- Upstream MTU:**

**Supplementary Network**

- Add Additional Network:**  Enable
- Router Address:
- Subnet Mask:
- Auto Firewall Open:

**Routing**

- Routing:**  Enable (Default is enabled. Routing disabled = Bridge mode)

2. Select the **Use Broadband IPs on LAN** check box. This enables bridge mode on the gateway.
3. Enter the subnet mask address in the **Specify usable subnet mask** text box. You must specify this address on the LAN devices or supplementary network devices while configuring the subnet mask. The recommended subnet mask address is 255.255.255.0.
4. Select the **Auto Firewall Open** check box. This disables the firewall of the gateway. Make sure that you select this option because the firewall must be disabled for the bridge mode to function.
5. Select the **Use the built-in system MAC address** radio button from the **System MAC Address** section to use the configured MAC address.  
OR  
Select the **Override the built-in MAC address** radio button from the **System MAC Address** section, and mention a MAC address of your choice in the **Specify MAC address** text box.
6. Leave the **Upstream MTU** value as is. This is the maximum size allowed on packets that are communicated between your network and your ISP.
7. Select the **Add Additional Network** check box to tail a router from the **Local Ethernet** port located at the back panel of the gateway. This adds a secondary network to the broadband WAN interface.
8. Enter the gateway address of the supplementary network device in the **Router Address** text box. This is the gateway address of the secondary subnet.

9. Enter the **Subnet Mask** address in the text box. This is the router mask of the secondary subnet.
10. Select the **Auto Firewall Open** check box to disable the firewall for all devices using addresses from this subnet.
11. Clear the **Routing** check box to ensure that the gateway does not assign IP addresses to LAN devices through DHCP.
12. Click **Save**.

The bridge mode is enabled on the gateway, and LAN devices are configured to take the Broadband IP address. The service LED on the front panel of the device remains off when the gateway is in bridge mode. The supplementary network represented by the router is tailed to the gateway.

## Adding Static Routes

### Objective

To add static routes.

This task lets you manually configure static routes for specifying the transmission path that the data must follow between devices outside the gateway network.

## Steps

1. Navigate to **Settings > Broadband > Routing**. The **Static Routes** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status
Link Configuration
Routing
Multicast
DNS Resolution

### Static Routes

**Add New Route**

Subnet IP:

Subnet Mask:

Gateway IP:

**Static Route List:**

Subnet IP	Subnet Mask	Gateway IP	Interface
127.0.0.1	255.255.255.255	127.0.0.1	lo0
172.16.8.16	255.255.255.255	172.16.8.16	ppp0
192.168.1.254	255.255.255.255	192.168.1.254	bridge0
172.16.8.1	255.255.255.255	172.16.8.16	ppp0
172.16.8.16	255.255.255.255	172.16.8.1	bridge0
192.168.1.0	255.255.255.0	192.168.1.254	bridge0
127.0.0.0	255.0.0.0	127.0.0.1	lo0
0.0.0.0	0.0.0.0	172.16.8.1	ppp0

2. Enter the IP address of the destination network in the **Subnet IP** text box.
3. Enter the subnet mask of the destination network in the **Subnet Mask** text box.
4. Enter the gateway address of the destination network in the **Gateway IP** text box.
5. Click **Add To List**.

The **Static Route List** section displays the new Subnet IP, Subnet Mast, Gateway IP, and Interface name.

## Configuring IP Multicast Sessions

### Objective

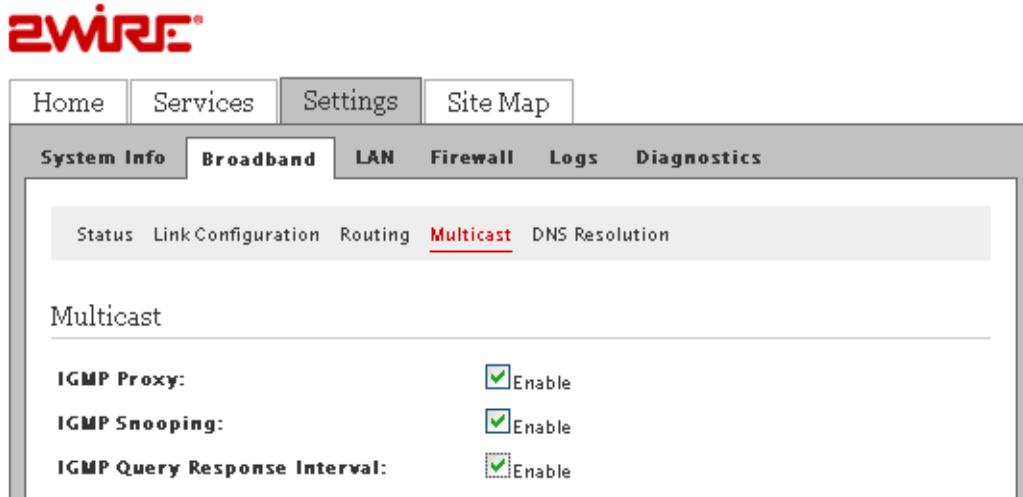
To configure IP multicast sessions.

When information is broadcast on a network, information packets are delivered to all segments on the LAN. This degrades network performance. IP multicasting is a method of forwarding information to a group of interested receivers.

Internet Group Management Protocol (IGMP) is used to manage IP Multicast sessions. IGMP provides a means to automatically control and limit the flow of multicast traffic throughout your network with the use of special multicast queriers and hosts.

## Steps

1. Navigate to **Settings > Broadband > Multicast**. The **Multicast** page appears.



2. Select the **IGMP Proxy** check box to enable the feature. When IGMP Proxy is enabled, the gateway issues IGMP host messages on behalf of the hosts discovered through standard IGMP interfaces. In other words, the gateway acts as a proxy for its hosts.
3. Select the **IGMP Snooping** check box to enable the feature. When IGMP Snooping is enabled, the gateway analyzes all IGMP packets and selectively forwards multicast traffic only to those ports where particular IP Multicast streams are accepted.
4. Select the **IGMP Query Response Interval** check box to enable the feature. When IGMP Query Response Interval is enabled, you control the number of IGMP messages allowed on the subnet during the specified duration.
5. Click **Save**.

## Viewing Multicast Statistics

To view multicast statistics, navigate to **Settings > Broadband > Multicast**. The **Multicast** page appears.

<b>IGMP Interface Name:</b>	ppp0
<b>IGMP Enable Query:</b>	FALSE
<b>IGMP Fast Update:</b>	TRUE
<b>IGMP Version:</b>	3
<b>IGMP Robustness:</b>	2
<b>IGMP Query Interval:</b>	125
<b>IGMP Query Response Interval:</b>	10.0
<b>IGMP Group Membership Interval:</b>	default
<b>IGMP Startup Query Interval:</b>	default
<b>IGMP Startup Query Count:</b>	default
<b>IGMP Last Member Query Interval:</b>	1.0
<b>IGMP Last Member Query Count:</b>	default
<b>IGMP Maximum Host Groups:</b>	256
<b>IGMP Maximum Sources:</b>	64
<b>IGMP Query Count:</b>	0
<b>IGMP Framing Errors:</b>	0
<b>IGMP Invalid Type:</b>	0
<b>IGMP Allocation Failure:</b>	0
<b>IGMP Host Group Exceeded:</b>	0
<b>IGMP Sources Exceeded:</b>	0
<b>IGMP Other Querier:</b>	0
<b>IGMP Membership Entries:</b>	0
<b>IGMP Total Received Messages:</b>	0
<b>IGMP Received Short Messages:</b>	0
<b>IGMP Bad Checksum Messages:</b>	0
<b>IGMP Inquiry Messages:</b>	0
<b>IGMP Bad Inquiry Messages:</b>	0
<b>IGMP Report Messages:</b>	0
<b>IGMP Bad Report Messages:</b>	0
<b>IGMP Own Group Report Messages:</b>	0
<b>IGMP Transmitted Reports:</b>	0
<b>IGMP Group Entries:</b>	3
<b>IGMP Cache Entries:</b>	0

IGMP Group Interface Name	IGMP Group Interface Address	IGMP Group Interface Reference Count
ppp0	224.0.0.1	1
lo0	224.0.0.1	1
bridge0	224.0.0.1	1

Refer to the following table to understand the IGMP parameters listed on the multicast page:

IGMP Parameter	Description
<b>IGMP Interface Name</b>	Name of the interface for which statistics are being reported.
<b>IGMP Enable Query</b>	Displays whether the interface has IGMP querying enabled or disabled.
<b>IGMP Fast Update</b>	Displays whether the interface has IGMP fast update enabled or disabled.
<b>IGMP Version</b>	Displays the IGMP version.

<b>IGMP Parameter</b>	<b>Description</b>
<b>IGMP Robustness</b>	Time interval that the gateway waits for a report in response to a group-specific query.
<b>IGMP Query Interval</b>	Time interval at which the gateway sends membership queries when it is the querier.
<b>IGMP Query Response Interval</b>	Time interval that the gateway waits for a report in response to a general query.
<b>IGMP Group Membership Interval</b>	Timeout period for group membership. If no report is received for these groups before the timeout expires, the group membership is removed.
<b>IGMP Startup Query Interval</b>	Amount of time in seconds between successive General Query messages sent by a querier during startup.
<b>IGMP Startup Query Count</b>	Number of general query messages sent at startup.
<b>IGMP Last Member Query Interval</b>	Time interval that the gateway waits for a report in response to a group-specific query.
<b>IGMP Last Member Query Count</b>	Number of Group-Specific Query messages sent before the gateway assumes that there are no members of the host group being queried on this interface.
<b>IGMP Maximum Host Groups</b>	Maximum number of host group members.
<b>IGMP Maximum Sources</b>	Maximum number of source-specific join and leave messages.
<b>IGMP Query Count</b>	Number of membership queries sent and received.
<b>IGMP Framing Errors</b>	Number of frame errors related to ARP, IP, and RARP.
<b>IGMP Invalid Type</b>	Number of times gateway received Invalid IGMP Type message.
<b>IGMP Allocation Failure</b>	Number of times gateway received Allocation Failure messages, such as memory allocation failure, IP address allocation failure, and so on.
<b>IGMP Host Group Exceeded</b>	Number of times host groups have exceeded in the message.
<b>IGMP Sources Exceeded</b>	Number of times source addresses have exceeded in the message.
<b>IGMP Other Querier</b>	Timeout period for group membership. If no report is received for these groups before the timeout expires, the group membership is removed.
<b>IGMP Membership Entries</b>	Number of group membership entries on an interface.
<b>IGMP Total Received Messages</b>	Number of total messages received.
<b>IGMP Received Short Messages</b>	Number of short messages received.
<b>IGMP Bad Checksum Messages</b>	Number of messages received with a bad IP checksum.
<b>IGMP Inquiry Messages</b>	Number of membership inquiry messages issued by the gateway.
<b>IGMP Bad Inquiry Messages</b>	Number of membership inquiry messages issued by the gateway that were not realized by this protocol.
<b>IGMP Report Messages</b>	Number of report messages sent by the host to the members of the querying group.
<b>IGMP Bad Report Messages</b>	Number of report messages that were sent by the host but were not realized by the members of that group.
<b>IGMP Own Group Report Messages</b>	Number of report messages sent by the host to the members of the same group.
<b>IGMP Transmitted Reports</b>	Total number of IGMP reports transmitted by the gateway.
<b>IGMP Group Entries</b>	Total number of group entries on an interface.
<b>IGMP Cache Entries</b>	Total number of cache entries on an interface.
<b>IGMP Group Interface Name</b>	Interface name of the IGMP group.
<b>IGMP Group Interface Address</b>	IP address of the IGMP group interface.
<b>IGMP Group Interface Reference Count</b>	Number of processes belonging to the IGMP group interface.

## Resolving Domain Name

### Objective

To manually add a domain name for resolving the IP address of the networked devices.

This task allows you to name network devices (such as printers or Web servers), so that they can be easily accessed by other users on the network.

---

**Note** Confirm that the domain name is not in use.

---

## Steps

1. Navigate to **Settings > Broadband > DNS Resolution**. The **Domain Name Server Resolution** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status
Link Configuration
Routing
Multicast
DNS Resolution

### Domain Name Server Resolution

Manually define a Domain Name and IP Address to resolve:

**Add a New DNS Name**

DNS Name:

IP Address:

**Name resolution table:**

DNS name	IP Address	Entry Type
John	127.0.0.1	System
homeportal	192.168.1.254	System
officeportal	192.168.1.254	System
gateway.2wire.net	192.168.1.254	System
igateway	192.168.1.254	System
gateway	192.168.1.254	System
api.home	192.168.1.254	System
dsldevice	192.168.1.254	System
home	192.168.1.254	System
unknown00C026A30BF1	192.168.1.64	System
Mkirloskar	192.168.1.65	System
localhost	127.0.0.1	System

2. Enter a name for the network device in the **DNS Name** text box.
3. Enter the IP address of the network device in the **IP Address** text box.
4. Click **Add To Name Resolution Table**. The **Name Resolution Table** section displays the newly added and existing DNS name, IP address, and Entry type.

## See Also

[Configuring LAN Devices](#) on page 50

[Configuring Firewall Settings](#) on page 72



[Using Diagnostics Features](#) on page 93

[Troubleshooting 3801HGV Gateway](#) on page 109

## CHAPTER 9

# Configuring LAN Devices

---

**NOTE TO REVIEWER: [JIRA 1515: ...Unable to determine the steps to set up multiple SSIDs and associated information on the UI of 3801HGV.]**

Please provide the necessary info to document this. How do we configure multiple SSIDs through the UI?

---

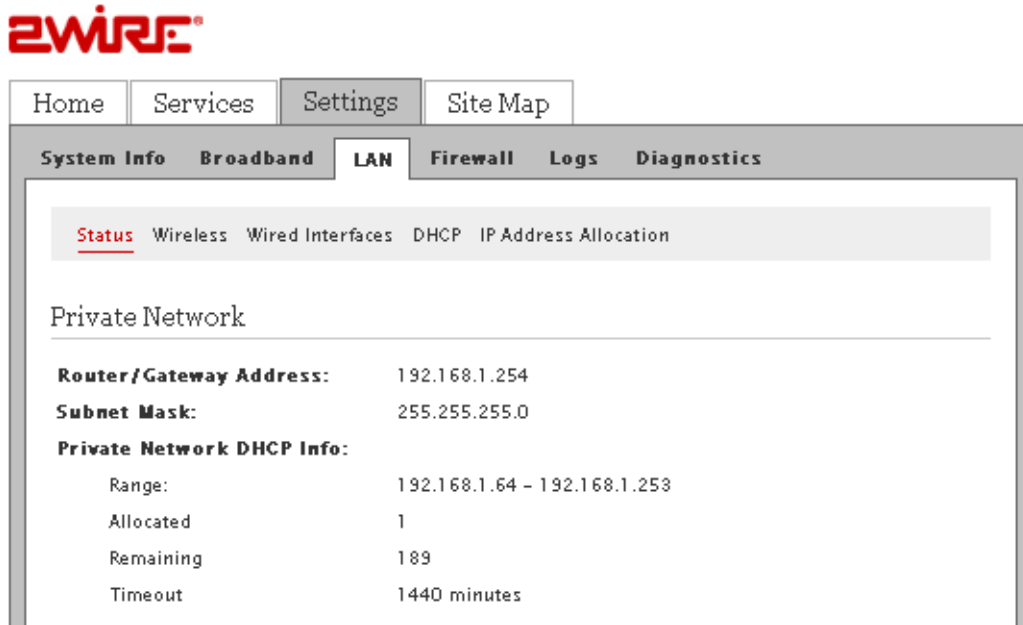
This chapter provides information about the tasks you can perform in the **LAN** tab. Following are the links under the **LAN** tab, and associated tasks:

- **Status**
  - [Viewing LAN Status](#) on page 51
- **Wireless**
  - [Setting Up Wireless Network](#) on page 53
  - [Securing the Wireless Network Using Encryption Key](#) on page 55
  - [Securing the Wireless Network Using MAC Filtering](#) on page 57
  - [Configuring Advance Wireless Settings](#) on page 61
  - [Configuring Wi-Fi Protected Setup](#) on page 62
- **Wired Interfaces**
  - [Configuring Local Ethernet Ports](#) on page 64
  - [Configuring HomePNA 3.1](#) on page 65
  - [Viewing HomePNA Status](#) on page 66
- **DHCP**
  - [Configuring DHCP](#) on page 66
- **IP Address Allocation**
  - [Allocating IP Addresses](#) on page 69

## Viewing LAN Status

To view the LAN status page, navigate to **Settings > LAN > Status**. The **Status** page appears.

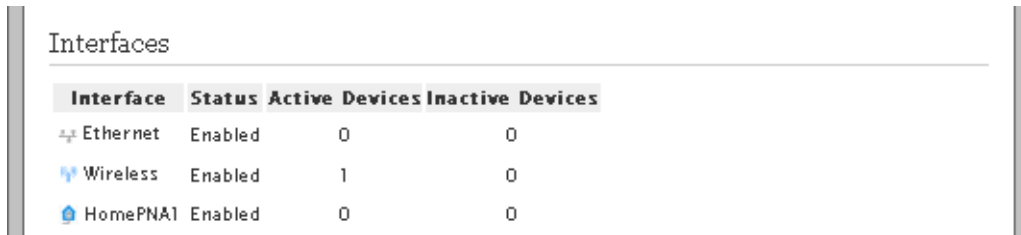
The following figure displays the **Private Network** section of the **Status** page.



Refer to the following table to understand the **Private Network** parameters listed on the **Status** page:

Parameter	Description
<b>Router/Gateway Address</b>	IP address allocated to the gateway.
<b>Subnet Mask</b>	Subnet mask allocated to the gateway.
<b>Private Network DHCP Info</b>	
<b>Range</b>	Range of IP addresses available on the network.
<b>Allocated</b>	Number of IP addresses allocated on the network.
<b>Remaining</b>	Number of IP addresses remaining on the network.
<b>Timeout</b>	Time in minutes before the DHCP lease must be renewed.

The following figure displays the **Interfaces** section of the **Status** page.

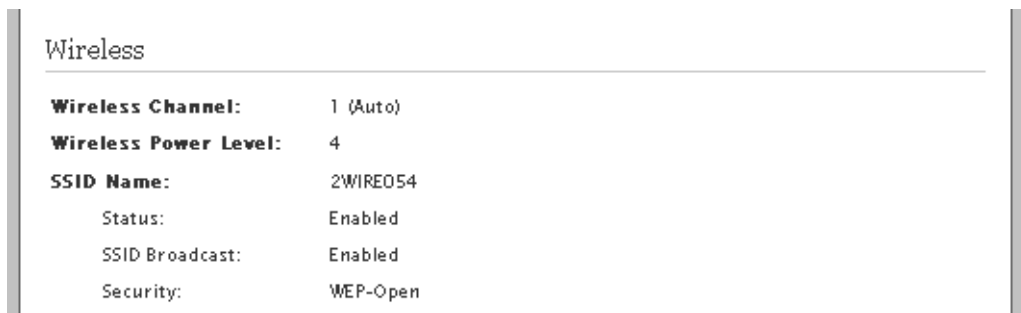


Interface	Status	Active Devices	Inactive Devices
Ethernet	Enabled	0	0
Wireless	Enabled	1	0
HomePNA1	Enabled	0	0

Refer to the following table to understand the **Interface** parameters listed on the **Status** page:

Parameter	Description
<b>Ethernet</b>	Displays whether the Ethernet interface is enabled or disabled. Also displays the number of active and inactive Ethernet devices on the network.
<b>Wireless</b>	Displays whether the wireless interface is enabled or disabled. Also displays the number of active and inactive wireless devices on the network.
<b>HomePNA1</b>	Displays whether the HPNA interface is enabled or disabled. Also displays whether the HPNA interface is active or inactive on the network.

The following figure displays the **Wireless** section of the **Status** page.

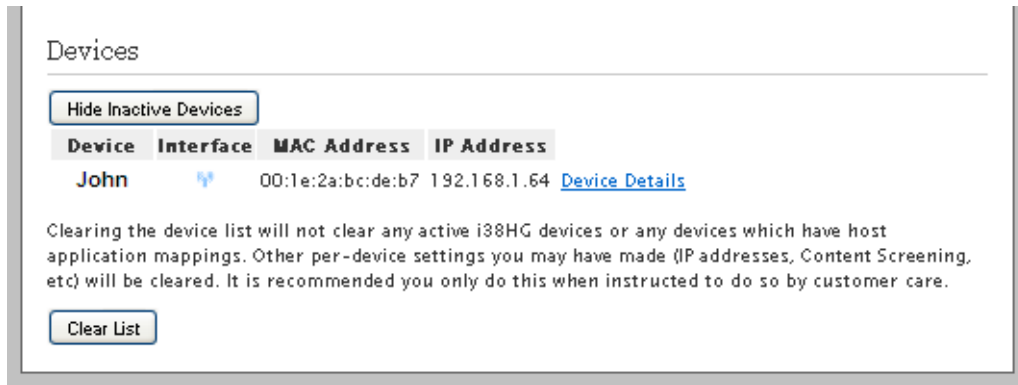


<b>Wireless Channel:</b>	1 (Auto)
<b>Wireless Power Level:</b>	4
<b>SSID Name:</b>	2WIRE054
Status:	Enabled
SSID Broadcast:	Enabled
Security:	WEP-Open

Refer to the following table to understand the **Wireless** parameters listed on the **Status** page:

Parameter	Description
<b>Wireless Channel</b>	Radio frequency band that the access point uses for your wireless network.
<b>Wireless Power Level</b>	Power level for your wireless connection.
<b>SSID Name</b>	Name assigned to your wireless network. The default is 2WIREXXX, where XXX represents the last three digits of the serial number of your gateway (for example, 2WIRE008).
<b>Status</b>	Displays whether the wireless connection is enabled or disabled.
<b>SSID Broadcast</b>	Displays whether broadcasting of SSID is enabled or disabled.
<b>Security</b>	Security method used to ensure that authorized users are accessing the wireless network.

The following figure displays the **Devices** section of the **Status** page.



Refer to the following table to hide inactive devices and clear the list of devices appearing on the **Status** page:

Step	Result
Click <b>Hide Inactive Devices</b> .	Devices that are no longer on the local network will be hidden from the <b>Devices</b> list on this page and under <b>Home Network Devices</b> on the <b>Home</b> page.
Click <b>Clear List</b> .	Devices that are no longer active on the local network are cleared from the <b>Devices</b> list on this page and under <b>Home Network Devices</b> on the <b>Home</b> page.

## Setting Up Wireless Network

### Objective

To setup your wireless network.

This configuration determines the wireless settings used to access the wireless interface of the gateway.

### Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.



Home Services **Settings** Site Map

System Info Broadband **LAN** Firewall Logs Diagnostics

Status **Wireless** Wired Interfaces DHCP IP Address Allocation

**Warning** Modifying the settings on this page can impact the ability of devices to access your wireless network.

Wireless Interface

**Enable Wireless Interface:**  Default: Enabled

Network

**Network Name (SSID):**

**SSID Broadcast:**  Default: Enabled

**Wireless Channel:**  Current: 1

Security

**Wireless Security:**  Default: Enabled

**Authentication Type:**

**Wireless Key**  Use default encryption key printed on the System Label:

Set custom encryption key:

MAC Filtering

**MAC Filtering** [Edit Blocked/Allowed Device List](#)

Advanced Settings

**Power Setting:**  Default: 4

**Wireless Mode:**  Default: 802.11 b/g

**DTIM Period:**  Default: 1

**Maximum Connection Rate:**  Default: 54 Mbps

Wi-Fi Protected Setup:

**Wi-Fi Protected Setup:**  Default: Enabled

Status: idle

2. Enable the wireless connection by selecting the **Enable Wireless Interface** check box.
3. Enter a name assigned to your wireless network in the **Network Name (SSID)** text box. The default is 2WIREXXX, where XXX represents the last three digits of your 2Wire gateway serial number (for example, 2WIRE008). This name appears next to the **Wireless** icon on the **Home** page.

---

**Note** The HomePortal 3801HGV gateway can support up to 4 SSIDs. It can support up to 4 wireless devices at a time.

---

4. Enable the broadcast of the SSID over the wireless network by selecting the **SSID Broadcast** check box. This implies that the broadcasted SSID is visible to the users who are scanning to connect to a wireless network.

---

**Note** You can disable the broadcast of the SSID by clearing the SSID Broadcast check box. When you disable **SSID Broadcast**, the LAN client cannot scan and connect to your wireless network. You have to manually add a wireless profile in the LAN client to connect to the wireless network instead of selecting the SSID name from a typical scan list.

---

5. Select a wireless channel (radio frequency band) from the corresponding drop-down list box. This is the access point used for your wireless network. Wireless clients or wireless adapter cards auto-detect the channels to use. If you are having problems with your wireless network, it could be due to radio interference. You can change the wireless channel to see if interference is reduced on a different channel. It is best to select **Auto**, because a channel is automatically selected to minimize interference.
6. Click **Save**. This ensures that the configured wireless setting is saved.

## Securing the Wireless Network Using Encryption Key

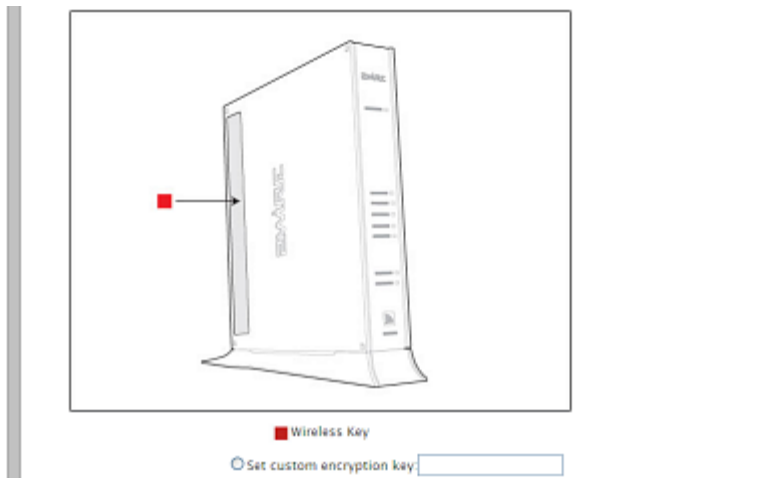
### Objective

To secure your wireless network using the encryption key.

Encrypted security setting makes it difficult for unauthorized users to access your network. It is good practice to customize an encryption key for wireless communication. When the key is defined, each wireless client must have it to connect to your wireless network.

## Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page to configure the **Security** settings appears.



2. Enable or disable the wireless security by selecting or clearing the **Wireless Security** check box. Wireless security is enabled as a default setting.
3. Select an authentication setting from the **Authentication Type** drop-down list box. Check the capabilities of the wireless clients that will be accessing this network and find a secure protocol by referring to the following table:

Authentication Type	Description
<b>WEP-Open</b>	The Wireless Encryption Protocol (WEP) is an older security protocol that allows any wireless clients within the radio range to access your network without an encryption key. This setting provides the least level of security. For security reasons, do not select this setting unless there is a compatibility issue with an older wireless client. For added protection, set an encryption key on your AP and enter the same key into your other wireless clients.
<b>WEP-Shared</b>	Similar to the <b>WEP-Open</b> setting, do not select this setting unless there is a compatibility issue with an older wireless client. Unlike the <b>WEP-Open</b> setting, the <b>WEP-Shared</b> setting prevents open access by any wireless client; therefore, it is more secure than the <b>WEP-Open</b> setting. For added protection, set an encryption key on your AP and enter the same key into your other wireless clients.
<b>WPA-PSK (TKIP)</b>	This setting provides good security and works with most newer wireless clients. This setting requires an encryption key on the AP and the wireless client configured to use Wi-Fi Protected Access – Pre-Shared Key (WPA-PSK) with the same encryption key.
<b>WPA-PSK (TKIP) and WPA2-PSK (AES)</b>	This setting allows a wireless client to use either WPA-PSK or WPA2-PSK to access your network. An encryption key must be configured on the AP and the same key must be entered on the wireless client.
<b>WPA2-PSK (AES)</b>	This setting requires that wireless clients use only WPA2-PSK to access your networks. An encryption key must be configured on the AP and entered into the wireless client. WPA2-PSK is currently the most secure Wi-Fi encryption protocol but may not be available on many wireless clients.

4. Select the **Use default encryption key printed on the System Label** radio button to use the encryption key that came with your gateway.  
OR  
Select the **Set custom encryption key** radio button to create a custom encryption key. You can define a 64-bit or 128-bit encryption key. For 64-bit encryption, enter a 10-digit hexadecimal number. For 128-bit encryption, enter a 26-digit hexadecimal number. A



hexadecimal number uses the characters 0-9, a-f, or A-F.

This security key will be used by all clients to access your wireless network.

5. Click **Save**. This ensures that the configured security setting is saved.

## Securing the Wireless Network Using MAC Filtering

### Objective

To secure your wireless network using the MAC filtering feature.

This feature enables you to block or allow wireless connection to all devices, or an individual device based on the MAC address of the device. You allow only “known and trusted” devices to associate with the wireless access point. MAC address filtering is disabled as a default setting. When enabled, the wireless connection is granted only to the MAC addresses that are pre-configured in the allowed device list.

### Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.
2. In the **MAC Filtering** section, click **Edit Blocked/Allowed Device List** link. The **Wireless MAC Filtering** page appears.

The screenshot shows the Z-Wireless configuration interface. At the top, there are navigation tabs: Home, Services, Settings (selected), and Site Map. Below this is a sub-menu with System Info, Broadband, LAN (selected), Firewall, Logs, and Diagnostics. The main content area is titled "Wireless MAC Filtering" and includes a status bar with "Wireless" highlighted. The "Enable MAC Filtering" section has an unchecked "Enable" checkbox and a "Save" button. The "Select Devices to be Allowed or Blocked" section contains instructions, a note, and two lists: "Allowed Devices" and "Blocked Devices". Between these lists are buttons for "<<", ">>", "Rescan For Devices", and "Delete". At the bottom, the "Add New MAC Address to List Manually" section has an input field for "Enter MAC address" and an "Add To List" button.

3. Enable or disable the MAC filtering by selecting or clearing the **Enable MAC Filtering** check box. MAC filtering is disabled as a default setting. Disabling MAC address filtering allows all the wireless clients to access the device.
4. Click **Save**. This ensures that the configured MAC filtering setting is saved.
5. Allow block devices to access wireless interface based on MAC filtering feature by configuring the **Select Devices to be Allowed or Blocked** pane.

## Allowing MAC Addresses

### Objective

This feature enables you allow wireless connection to all devices, or an individual device based on the MAC address of the device.

## Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page to configure the **MAC filtering** settings appears.
2. Add the MAC address of the device in the **Enter MAC address** text box.

Add New MAC Address to List Manually

Enter MAC address

3. Click **Add To List**. This populates the MAC address in the **Allowed Devices** pane.

Allowed Devices:

00:1c:bf:a9:03:ac

Blocked Devices:

<< >>

Rescan For Devices

Delete

Add New MAC Address to List Manually

Enter MAC address

## Blocking MAC Addresses

### Objective

This feature block wireless connection to all devices, or an individual device based on the MAC address of the device.

### Steps

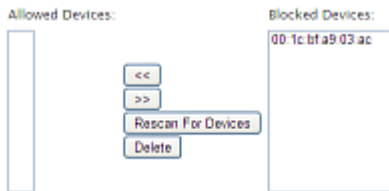
1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.
2. In the **MAC Filtering** section, click **Edit Blocked/Allowed Device List** link. The **Wireless MAC Filtering** page appears.
3. Select the device you want to block from the **Allowed Devices** pane.

---

**Note** To select multiple addresses, hold down the [Shift] or [Ctrl] keys while making your selections. Using the [Shift] key lets you make your selections in a contiguous order, while the [Ctrl] key selects the groups in a random order.

---

4. Click **>>**. This populates the MAC address in the **Blocked Devices** pane.



## Refreshing the List of Devices

### Objective

This feature enables you to refresh the list of devices while allowing or blocking wireless connection based on the MAC Addresses of the devices.

### Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.
2. In the **MAC Filtering** section, click **Edit Blocked/Allowed Device List** link. The **Wireless MAC Filtering** page appears.
3. Click **Rescan For Devices** to refresh the list of devices viewed in **Allowed Devices** and **Blocked Devices** panes.

## Deleting the Devices

### Objective

To delete a configured device. This feature enables you to delete devices from the list of allowed or blocked devices.

### Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.
2. In the **MAC Filtering** section, click **Edit Blocked/Allowed Device List** link. The **Wireless MAC Filtering** page appears.
3. Select the device from **Allowed Devices** or **Blocked Devices** pane.
4. Click **Delete**.
5. Click **Save** to retain the configuration changes.

After any configuration change you have made on this user interface, a page opens confirming that the configuration is changed.

## Configuring Advance Wireless Settings

### Objective

To configure advance wireless settings.

This allows you to further optimize wireless settings for better performance.

**Note** It is recommended that you leave the default settings as is; however, if you are experiencing connection or performance difficulties, altering these settings may improve performance.

### Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page to configure the **Advanced Settings** appears.

2. Select the power level for your wireless connection from the **Power Setting** drop-down list. The configured power level is the actual transmitted radio power at the access point. The default list is from **1** to **4**. Following table provides the output power levels for 802.11b and 802.11g types of wireless modes:

Power Settings	Radio Output Power	
	802.11b (mW)	802.11g (mW)
1 (maximum)	50	30
2	25	15
3	12	8
4	6	4

3. Select the **Wireless Mode** from the drop-down list. This allows you to force the gateway to use **802.11b/g**, **802.11b**-only, or **802.11g**-only modes of operation. Check the wireless mode supported by the wireless adapter before configuring this option.
4. Enter the **DTIM Period** (seconds) in the text box. This **Delivery Traffic Indication Message** (DTIM) value determines the interval at which the access point sends its broadcast traffic.
5. Select the **Maximum Connection Rate** from the drop-down list. This is the maximum rate at which your wireless connection works. Select **1**, **2**, **5.5**, **11**, or **22** Mbps for 802.11b-based models and **1**, **2**, **5.5**, **11**, **6**, **9**, **12**, **24**, **36**, **48**, or **54** Mbps for 802.11b/g-based models.

6. Click **Save**. This ensures that the advance wireless settings are saved.

## Configuring Wi-Fi Protected Setup

### Objective

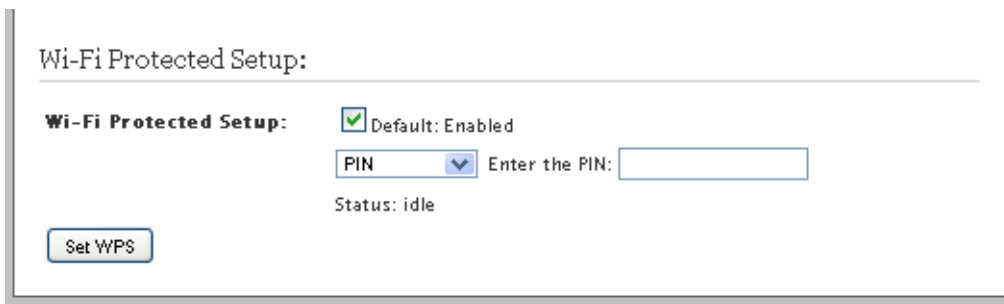
To configure Wi-Fi protected setup (WPS).

This configuration simplifies the process of connecting any home device to the wireless network. As an access point (AP), the gateway issues and revokes credentials to a network.

WPS supports both push button and PIN-based configuration methods. When WPS is enabled, the gateway automatically detects the presence of a WPS-enabled client device. Both methods require WPA or WPA2 security enabled and the predefined passphrase is provided to the WPS device.

### Steps

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.



2. In the **Wi-Fi Protected Setup** section, enable the WPS by selecting the **Wi-Fi Protected Setup** check box.

### Setting Up WPS through the PIN Method

To set up WPS through the PIN method:

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.
2. In the **Wi-Fi Protected Setup** section, enable the WPS by selecting the **Wi-Fi Protected Setup** check box.
3. Select **PIN** from the drop-down list.

4. Enter a 4 or 8 digit PIN in **Enter the PIN** text box. The PIN method requires a 4- or 8-digit PIN.
5. Click **Set WPS**. This saves the PIN configuration changes done for WPS.

### Setting Up WPS through the Push Button Method

To set up WPS through the PIN method:

1. Navigate to **Settings > LAN > Wireless**. The **Wireless** page appears.
2. In the **Wi-Fi Protected Setup** section, enable the WPS by selecting the **Wi-Fi Protected Setup** check box.
3. Select **Push Button** from the drop-down list.

4. Locate and push the WPS button found at the front panel of the device. The gateway provides a push button on the front panel to enable the synchronization between the AP and the client. You do not have to connect any devices to the gateway to enable it - simply push the button on the gateway followed by pushing the button on the client device.



5. Click **Set WPS**. This saves the **Push Button** configuration changes done for WPS.

## Configuring Local Ethernet Ports

### Objective

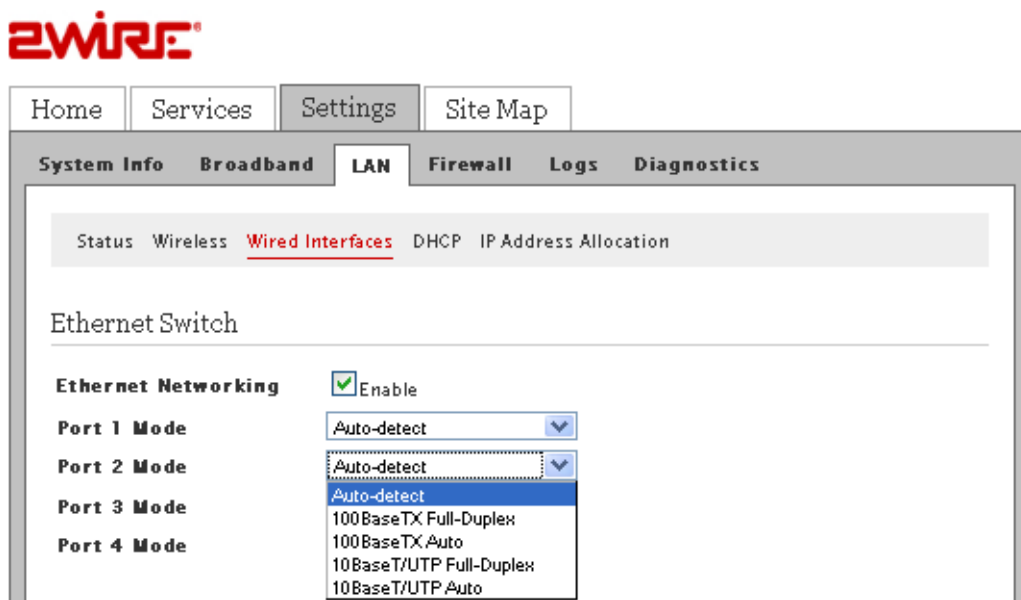
To configure local Ethernet ports.

This task lets you configure the local Ethernet ports to connect to network devices that support speeds up to 10 Mbits (10BaseT/UTP) and 100 Mbits (100BaseTX), and require a unique setting.

By default, the Ethernet ports are pre-configured to auto-detect mode.

### Steps

1. Navigate to **Settings > LAN > Wired Interfaces**. The **Ethernet Switch** page appears.



2. Enable or disable the local Ethernet networking by selecting or clearing the **Ethernet Networking** check box.
3. Match the mode of the Local Ethernet port located at the back panel of the gateway with the Ethernet port of the LAN client. Select one of the following options from the **Port 1 Mode** drop-down list:
  - **Auto-detect**
  - **100BaseTX Full-Duplex**
  - **100BaseTX Auto**
  - **10BaseT/UDP Full-Duplex**
  - **10BaseT/UDP Auto**
4. Select the relevant modes for the remaining ports as mentioned in Step 3.
5. Click **Save**. This saves the configuration changes done to the Local Ethernet ports.



## Configuring HomePNA 3.1

### Objective

To configure Home Phoneline Networking Alliance (HPNA) on the Cable port.

This task lets you configure HPNA interface on the Cable port of the gateway.

### Steps

1. Navigate to **Settings > LAN > Wired Interfaces**. The **HPNA 3.1 (Coax)** configuration page appears.

2. Enable or disable HPNA by selecting or clearing the **HomePNA Networking** check box.
3. Select **Coax** or **DSL** from the **Select Output Jack** drop-down list. This is the type of gateway port that you use to connect to the set top box. If you select Coax it implies that you are using CABLE port. If you select DSL it implies that you are using DSL port.

---

**NOTE TO REVIEWER:** Unsure whether the user can actually use the DSL port to configure the HPNA interface. The device has only one DSL port which is used to connect Internet. My understanding is that the device must have an addition RJ-11 port to configure HPNA interface. Need inputs for the same.

---

4. Select **493** or **340** from the **Noise Margin** drop-down list. This is the signal to noise ratio. Signal quality is inversely proportional to noise margin.
5. Select **1063**, **859**, or **646** from the **Per** drop-down list.

---

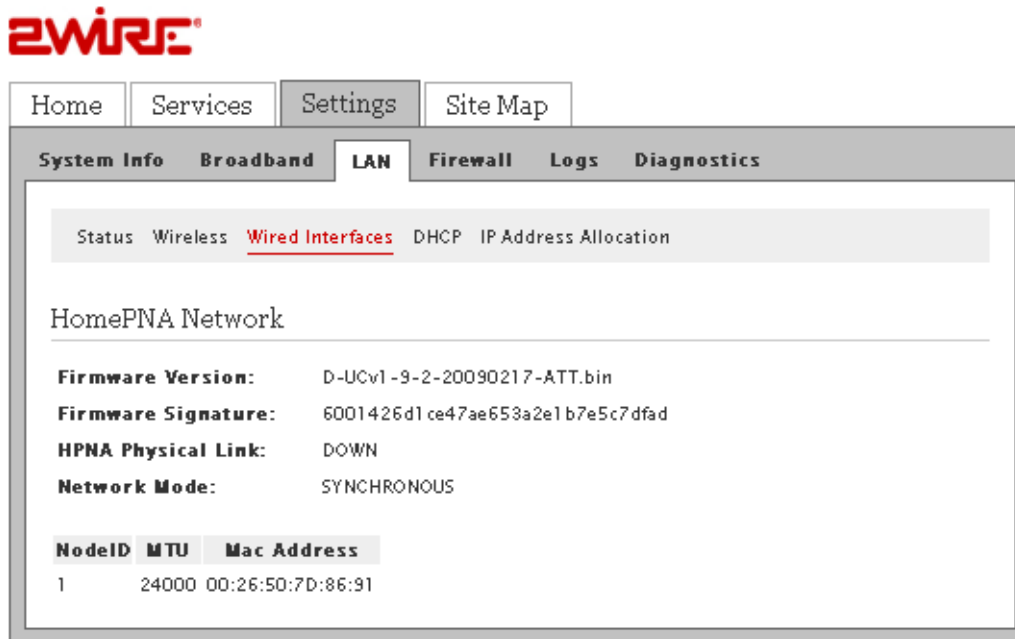
**NOTE TO REVIEWER:** Unable to determine the purpose of this field. Need inputs for this field.

---

6. Enter the duration in seconds in the **Collection Interval** text box. This is the number of seconds during which the counters for data are collected.
7. Click **Save**. This saves the HPNA configuration changes.

## Viewing HomePNA Status

To view HomePNA status page, navigate to **Settings > LAN > Wired Interfaces**. Click **HomePNA Status** listed at the bottom of the wired interfaces page. The following page appears:



Refer to the following table to understand the HomePNA Network parameters listed on the status page:

Parameter	Description
<b>Firmware Version</b>	Firmware version number.
<b>Firmware Signature</b>	Firmware signature number.
<b>HPNA Physical Link</b>	Displays whether the HPNA interface is enabled or disabled.
<b>Network Mode</b>	Network mode of the HPNA interface.
<b>Node ID</b>	Node ID of HPNA interface.
<b>MTU</b>	Maximum Transmission Unit is the maximum size allowed on data packets, that are communicated on HPNA network.
<b>MAC Address</b>	MAC address of the gateway.

## Configuring DHCP

### Objective

To configure Dynamic Host Configuration Protocol (DHCP) for setting up your private network. In this task, we are listing the steps to configure the DHCP server.

DHCP allows dynamic allocation of network addresses. Your gateway can be both a DHCP client and a DHCP server. When communicating with the local network devices, such as computers and printers, your gateway functions as a DHCP server. However, while communicating with your ISP, the gateway functions as a DHCP client.

By default, the gateway uses the 192.168.1.0/255.255.0.0 IP address range. You can select from two additional IP address ranges, or configure the network settings manually. When you select either of them, the LAN clients are assigned IP addresses within the specified range.

---

**Note** You should manually configure these settings **ONLY** if you thoroughly understand IP internetworking. An incorrect configuration can cause unpredictable results.

---

## Steps

1. Navigate to **Settings > LAN > DHCP**. The **DHCP Configuration** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status
Wireless
Wired Interfaces
DHCP
IP Address Allocation

**Warning** Modifying the settings on this page can impact the ability of devices to access your private network.

### DHCP Configuration

**DHCP Server Enabled**  Unchecking will stop the DHCP server from assigning IP addresses to LAN DHCP clients.

**DHCP Network Range** If you change the IP address range, you must renew the DHCP lease for all devices on the network.

192.168.1.0 / 255.255.255.0 (default)  
 172.16.0.0 / 255.255.0.0  
 10.0.0.0 / 255.255.0.0  
 Configure manually

Router Address:   
 Subnet Mask:   
 First DHCP Address:   
 Last DHCP Address:

**DHCP Lease Time:**  hours (24 hours default)

### Select Default Address Allocation Pool for the DHCP Server

Warning: This selection modifies the default LAN network used by the DHCP server for address assignments to new devices. The default setting is Private Network. Change it only to Public Network when you want every new device getting a public address assigned. The recommendation is Private Network. You can change the setting for each individual on the 'IP Address Allocation' page.

**New Device DHCP Pool:** Private Network

2. Enable or disable the DHCP server by selecting or clearing the **DHCP Server Enabled** check box.
3. Select a relevant radio button from **DHCP Network Range**, to use the default range of IP addresses or configure the DHCP server manually. If you are using the default range of IP address, continue to step 5. However, if you want a limited range of IP addresses, then go to step 4.

---

**Note** 3801HGV supports four subnets simultaneously on the LAN. The **192.168.1.0 / 255.255.255.0 (default)** is used as a private subnet by the end user. The **172.16.0.0 / 255.255.0.0** is used as the secondary subnet or public routed subnet by the end user. The remaining options, **10.0.0.0 / 255.255.0.0** and **Configure manually** are held in reserve to be configured and used by the service provider.

---

4. Select the **Configure manually** radio button for setting up a range IP addresses to be assigned to LAN clients. To populate the text fields under this section, refer to the following information:
  - a. Enter the IP address of your gateway (default is 192.168.1.254) used for all communication on your local devices in the **Router Address** text box.
  - b. Enter the subnet mask (default is 255.255.255.0) used for all communication on your local devices in the **Subnet Mask** text box.
  - c. Enter the first IP address in the DHCP address pool that you will be distributing over the private network in the **First DHCP Address** text box.
  - d. Enter the last IP address in the DHCP address pool that you will be distributing over the private network in the **Last DHCP Address** text box.
5. Enter a numerical value in the **DHCP Lease Time** text box. This value represents the number of hours you can use the assigned IP address before the DHCP lease expires.
6. Select **Private Network** from the **New Device DHCP Pool** drop-down list for assigning IP addresses to LAN clients from the private IP address pool. Select **Public Network** to assign IP addresses to LAN clients from public IP address pool. Public network selection is available only when bridge mode is enabled.

---

**Note** Change to the Public IP addressing only when used in conjunction with DMZplus or secondary subnet functionality that allows you to have public IP addresses routed through the device.

---

7. Click **Save**. This saves the DHCP configuration changes.

## Allocating IP Addresses

### Objective

To allocate specific IP addresses to devices that are running in the DHCP mode, and map devices to particular static or private IP addresses.

For Internet public hosting of application or servers associated with static addresses, you can map a device to a specific static IP address or to the next unassigned address from the public pool.

## Steps

1. Navigate to **Settings > LAN > IP Address Allocation**. The **Public-Private NAT Mappings and Device IP Allocation** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status
Wireless
Wired Interfaces
DHCP
IP Address Allocation

### Public-Private NAT Mappings and Device IP Allocation

This section allows you to configure the system to allocate specific IP addresses to devices that are running in DHCP mode, and map devices to particular static or public IP addresses, also known as NAT mappings.

Alternately, you may also statically assign public IP addresses on the devices themselves. Statically addressed device addresses will override settings made on this page.

For each device on the private network, you may override the default DHCP server address, and manually specify a desired IP Address for the DHCP server to issue to the device, or specify an alternate pool to issue from.

Additionally, for Internet public hosting of applications or servers associated with static or public IP addresses, you can map a device to a specific public fixed IP address or to the next unassigned address from the public pool. The default public IP device mapping is to the Router WAN IP address.

**Device : Mkirloskar**

Current Address :	192.168.1.64
Device Status :	Connected DHCP
Firewall:	<input type="button" value="Enabled"/> ▾
Address Assignment :	<input type="button" value="Private from pool:192.168.1.0"/> ▾
WAN IP Mapping :	<input type="button" value="Router WAN IP address (default)"/> ▾

2. Navigate to the relevant device for changing the configuration to override the default DHCP settings.
3. Enable or disable the firewall by selecting the relevant option from the **Firewall** drop-down list.
4. Select the specific address type from the **Address Assignment** drop-down list. You can select from the private IP address pool, or assign a static IP to the device.

---

**NOTE TO REVIEWER:** Unsure of the purpose for this field.

---

5. Leave the **WAN IP Mapping** drop-down list as is. This menu reads **Router WAN IP Address** as the default selection.

---

---

**NOTE TO REVIEWER:** Unsure whether this field remains as is. Any configuration change might bring up more options in the drop-down list. Need inputs for the same.

---

---

6. Click **Save**. This saves the allocated IP address to a specific device or devices.
7. Restart the gateway to view the updated configuration on this page.

### See Also

[Configuring Broadband Settings](#) on page 34

[Using Diagnostics Features](#) on page 93

[Troubleshooting 3801HGV Gateway](#) on page 109

## CHAPTER 10

# Configuring Firewall Settings

This chapter provides information about the tasks you can perform in the **Firewall** tab. Following are the links under the **Firewall** tab, and associated tasks:

- **Status**
  - [Viewing Firewall Status](#) on page 72
- **Applications, Pinholes and DMZ**
  - [Configuring Firewall Settings](#) on page 73
- **Advanced Configuration**
  - [Disabling Attack Detection](#) on page 80
  - [Controlling Inbound and Outbound Traffic](#) on page 82
  - [Configuring Firewall Security Enhancements](#) on page 83
  - [Configuring Application Layer Gateway](#) on page 83

## Viewing Firewall Status

To view the Firewall status page, navigate to **Settings > Firewall > Status**. The **Status** page appears.



Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

[Status](#) Applications, Pinholes and DMZ Advanced Configuration

### Firewall Status

**Firewall Active**

The firewall actively blocks access of unwanted activity from the Internet.

**Current Applications, Pinholes and DMZ Settings: Custom**

Device	Allowed Applications	Application Type	Protocol	Port Number(s)	Public IP
Mkirloskar	Age of Empires	DirectX Game (DirectPlay) host	TCP	47624	172.16.8.16
			UDP	47624	172.16.8.16
	Test	PPTP virtual private network server	TCP	72-80	172.16.8.16



Refer to the following table to understand the parameters listed on the **Firewall Status** page:

Parameter	Description
<b>Firewall Status</b>	View whether firewall is enabled or disabled in this section.
<b>Current Applications, Pinholes and DMZ Settings</b>	View if any applications are hosted in this section.
<b>Device</b>	Displays the name of the configured devices.
<b>Allowed Applications</b>	Displays the name of the application that bypasses the firewall settings.
<b>Application Type</b>	Displays the type of application.
<b>Protocol</b>	Displays the protocol in use.
<b>Port Number(s)</b>	Displays the port number assigned to the application.
<b>Public IP</b>	Displays the IP assigned to the device.

## Configuring Firewall Settings

### Objective

To configure firewall settings in a way that special applications running on computers inside your home network are granted Internet access.

To grant internet access to special applications, you need to open firewall pinholes and associate the intended application(s) with a computer connected to your gateway. If you cannot find a listing for your application, you can define an application with the protocol and port information. Also, you can delete the application profile you have saved. By default, firewall provides maximum protection and blocks unsolicited inbound traffic.

### Steps

1. Navigate to **Settings > Firewall > Applications, Pinholes and DMZ**. The **Allow device application traffic to pass through firewall** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status [Applications, Pinholes and DMZ](#) Advanced Configuration

### Allow device application traffic to pass through firewall

By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application with the protocol and port information.

To allow Internet traffic or users through the Firewall to your LAN devices, applications and servers:

**1) Select a computer**

Choose the computer that will host applications through the firewall

You have chosen **John**

**2) Edit firewall settings for this computer:**

Maximum protection - Disallow unsolicited inbound traffic:

Allow individual application(s) - Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

Filter Applications by:	Application List:	Hosted Applications:
<ul style="list-style-type: none"> <li><input type="radio"/> All applications</li> <li><input checked="" type="radio"/> <a href="#">Games</a></li> <li><input type="radio"/> <a href="#">Audio/video</a></li> <li><input type="radio"/> <a href="#">Messaging and Internet Phone</a></li> <li><input type="radio"/> <a href="#">Servers</a></li> <li><input type="radio"/> <a href="#">Other</a></li> <li><input type="radio"/> <a href="#">User-defined</a></li> </ul>	<div style="border: 1px solid gray; padding: 5px; min-height: 100px;">           Age of Kings            Age of Wonders            Aliens vs Predator            Anarchy Online            Asheron's Call            Baldur's Gate            BattleCom            Battlefield Communicator            Black and White            Dark Reign         </div> <div style="text-align: center; margin: 5px 0;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>	<div style="border: 1px solid gray; padding: 5px; min-height: 100px;">           Age of Empires            Test         </div>
	<a href="#">Add a new user-defined application</a>	<a href="#">Edit or delete user-defined application</a>

Allow all applications (DMZplus mode) - Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

Note: Once DMZplus mode is selected and you click save, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.

2. Select the computer where you want to host the application(s) in the **Select a computer** section. When you host an application for a computer on your network, it implies that you are scaling down the firewall security levels for that application to be accessible on the specified computer.
3. Select the **Allow individual application(s)** radio button.

---

**Note** If the computer you want to select is not listed, you can still select it as long as it is on the same network, and you know its IP address. Enter the IP address of that computer, and then click **Choose**.

---

4. Filter the application list by selecting the category from the **Filter Applications by** bulleted list. Your selection is displayed in the **Application List** list box.

---

**Note** To select multiple applications, hold down the [Shift] or [Ctrl] keys while making your selections. Using the [Shift] key lets you make your selections in a contiguous order while the [Ctrl] key selects the groups in a random order.

---

5. Click **Add**. The application appears in the **Hosted Applications** list box.

---

**Note** To remove a hosted application, select it in the **Hosted Applications** list box, and click **Remove**.

---

## Creating an Application Profile

To create an application profile that bypasses the firewall settings:

1. Navigate to **Settings > Firewall > Applications, Pinholes and DMZ**. The **Allow device application traffic to pass through firewall** page appears.
2. Click **Add a new user-defined application** in the **Edit firewall settings for this computer** section. This lets you create an application profile that is not included in the application list. An application profile configures the gateway firewall to let the application-specific data pass through. The **Firewall Application Profile Definition** page appears.



Home Services **Settings** Site Map

System Info Broadband LAN **Firewall** Logs Diagnostics

Status [Applications, Pinholes and DMZ](#) Advanced Configuration

### Firewall Application Profile Definition

If the desired application requires multiple ports of both TCP and UDP ports, you will need to add multiple definitions. Current definitions for this profile are shown in the Definition List below.

**Application Profile Name:**

**Create Application Definition**

Protocol: TCP  UDP

Port (or Range): From:  To:

Protocol Timeout:  TCP default 86400 seconds, UDP default 600 seconds

Map to Host Port:  Default/blank = same port as above

Application Type:  ▼

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu above, it is recommended that you select it.

**Definition List**

Protocol	Port (or Range)	Host Port	Timeout (sec)
----------	-----------------	-----------	---------------

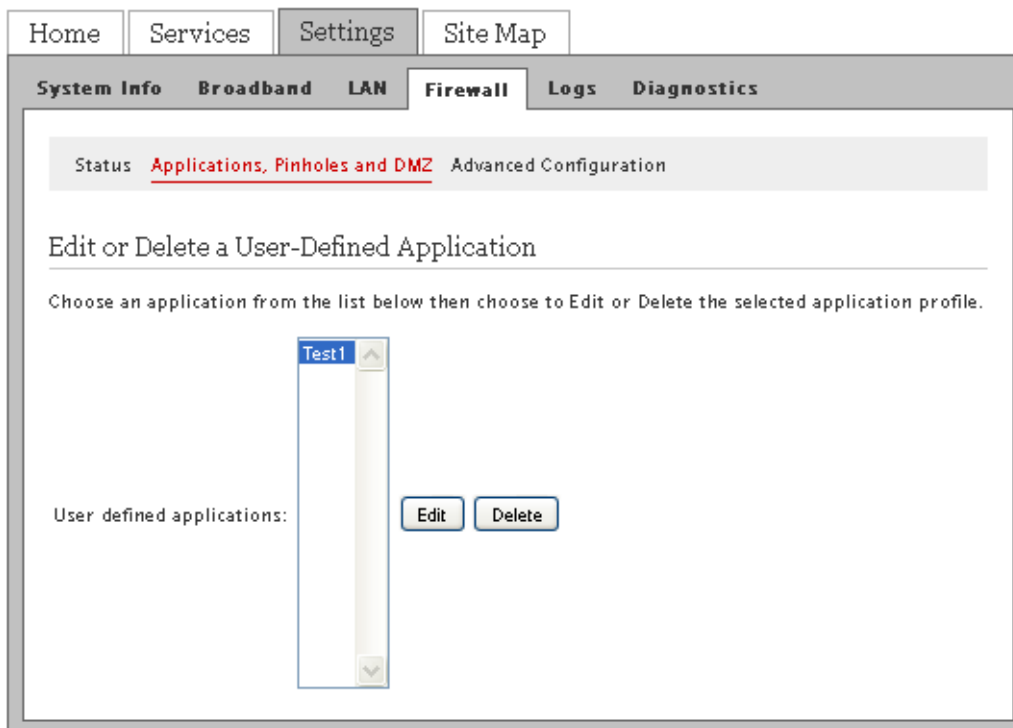
3. Enter a name for the application profile in the **Application Profile Name** text box.
4. Click the **TCP** or **UDP** radio button to select the protocol for the application profile. If the application you are adding requires both, you need to create a separate definition for each.
5. Enter the port or port range used by the application in the **Port (or Range)** text boxes. If only one port is required, enter the port number in the **From** text box. For example, some application require only one port to be opened (such as TCP port 500); others require that all TCP ports from 600 to 1000 be opened.
6. Enter the duration in seconds in **Protocol Timeout** text box. This is the amount of time the connection in the specified range remains open when there is no data transfer. In most cases, the default value is appropriate. If you leave the text box blank, the system uses the default values (86400 seconds for the TCP protocol; 600 seconds for the UDP protocol).
7. Enter a value in the **Map to Host Port** text box. This value must map to the port range you established to the local computer. For example, if you set the value to 4000 and the port range being opened is 100 to 108, the forwarded data to the first value in the range will be

sent to 4000. Subsequent ports will be mapped accordingly; 101 will be sent to 4001, 102 will be sent to 4002, and so on.

8. Select the application type from the **Application Type** drop-down list.
9. Click **Add to List**. This creates a new application profile. Also, the configured information appears in the **Definition List** section of the same page.

You can also view the newly created application listed in the **Applications List** drop-down list on the **Applications, Pinholes and DMZ** page.

10. Click **Back** to return to the **Applications, Pinholes and DMZ** page.
11. To edit a user defined applicaitons, click **Edit or delete user-defined application** in the **Edit firewall settings for this computer** section. This lets you edit an existing profile or assign additional TCP or UDP ports to an existing profile. The **Edit or Delete a User-Defined Application** page appears.




---

**Note** You can add the definition of the profile only when it has not been added to the **Hosted Application** list box. If the profile is added in the list of hosted applications and you want to modify it, then you need to first remove it from the **Hosted Applications** list box.

---

12. Select the application you want to modify from the **User defined applications** list box.
13. Click **Edit**. The **Firewall Application Profile Definition** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status Applications, Pinholes and DMZ Advanced Configuration

### Firewall Application Profile Definition

If the desired application requires multiple ports of both TCP and UDP ports, you will need to add multiple definitions. Current definitions for this profile are shown in the Definition List below.

**Application Profile Name:** Test1

**Create Application Definition**

Protocol: TCP  UDP

Port (or Range): From:  To:

Protocol Timeout:  TCP default 86400 seconds, UDP default 600 seconds

Map to Host Port:  Default/blank = same port as above

Application Type:  ▼

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu above, it is recommended that you select it.

**Definition List**

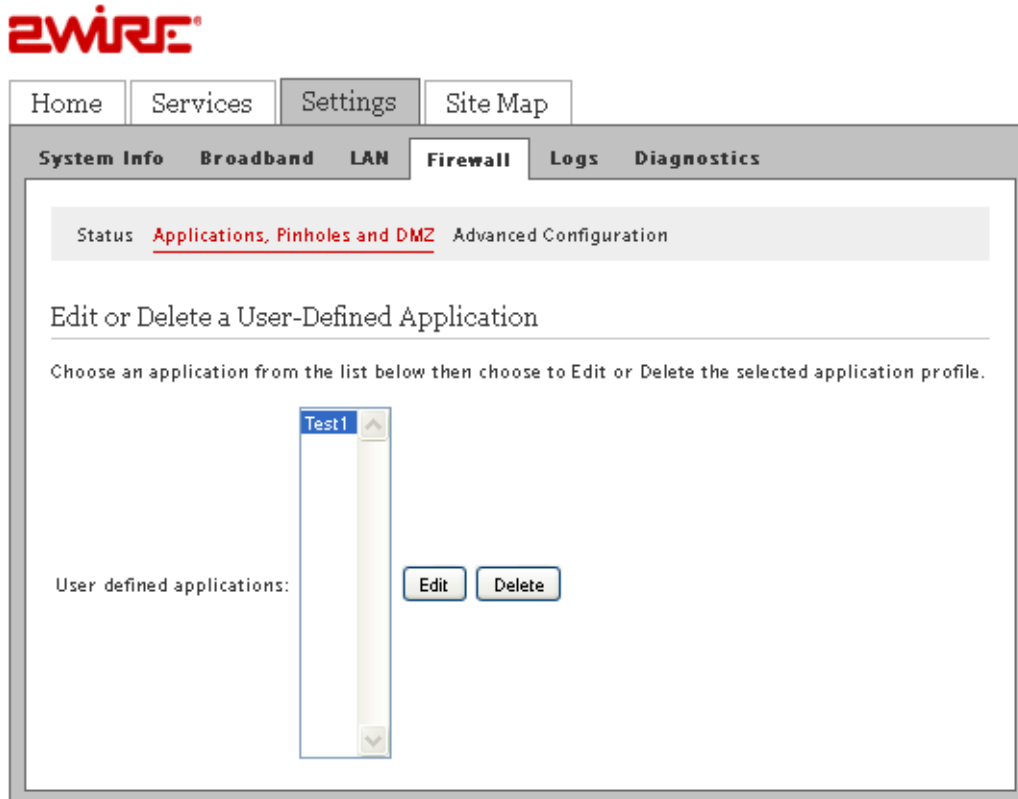
Protocol	Port (or Range)	Host Port	Timeout (sec)	
TCP	72-80	72	86400	<input type="button" value="Remove"/>

14. Modify the information as per your requirement.
15. Click **Add to List**. The configuration changes appear in the **Definition List** section of the same page.
16. Repeat step 8 to 15 for each port or range of ports required for the application profile.

## Deleting User-defined Applications

To delete a user defined application:

1. Click **Edit or delete user-defined application** in the **Edit firewall settings for this computer** section. This lets you delete an existing profile. The **Edit or Delete a User-Defined Application** page appears.



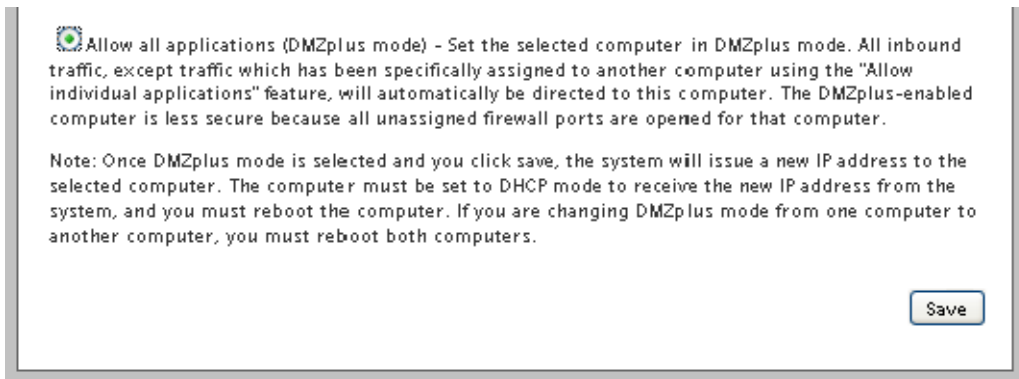
2. Select the application you want to delete from the **User defined applications** list box.
3. Click **Delete**. The configuration successful prompt confirms the deletion. You cannot view the deleted application in the **User defined applications** list box.

## Allowing all Applications

To allow all applications through firewall:

1. On the **Allow device application traffic to pass through firewall** page, select **Allow all applications (DMZplus mode)** radio button. This will enable DMZplus mode. DMZplus is used for hosting applications when hosted applications do not function properly. When in DMZplus mode, the designated computer appears as if it is directly connected to the Internet, has all unassigned TCP and UDP ports opened and pointed to it,

and can receive unsolicited network traffic from the Internet. The DMZplus mode configuration page appears:



2. Click **Save**.
3. Confirm that the computer you selected is configured for DHCP. If it is not, configure it for DHCP.
4. Restart the computer. When the computer restarts, it receives a special IP address from the system and all unassigned TCP and UDP ports are forwarded to it.



**Use the DMZplus mode with caution. A computer in the DMZplus mode is less secure because all available ports are open and all incoming Internet traffic is directed to this computer.**

## Disabling Attack Detection

### Objective

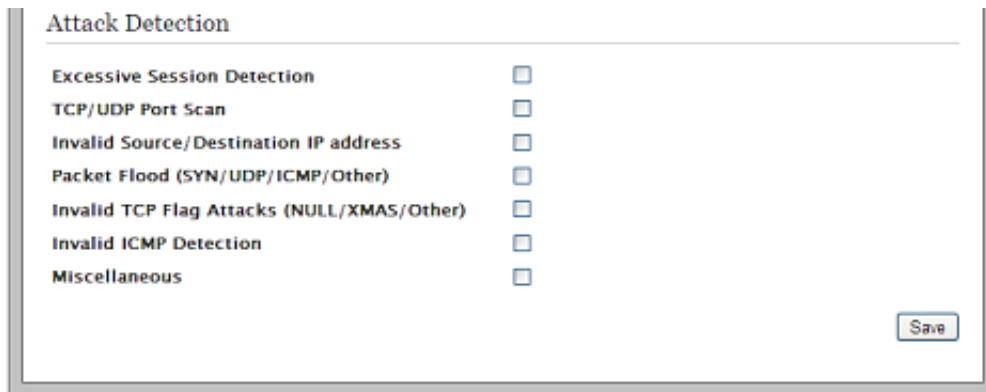
To disable a specific port in the attack detection section.

By default, attack detection is enabled on these ports by the firewall. However, some applications and devices may require the use of specific data ports listed here. The gateway allows users to open the necessary ports through the firewall.



## Steps

1. Navigate to **Settings > Firewall > Advanced Configuration**. The **Advanced Configuration** page to configure **Attack Detection** appears.



Attack Detection	
Excessive Session Detection	<input type="checkbox"/>
TCP/UDP Port Scan	<input type="checkbox"/>
Invalid Source/Destination IP address	<input type="checkbox"/>
Packet Flood (SYN/UDP/ICMP/Other)	<input type="checkbox"/>
Invalid TCP Flag Attacks (NULL/XMAS/Other)	<input type="checkbox"/>
Invalid ICMP Detection	<input type="checkbox"/>
Miscellaneous	<input type="checkbox"/>

Save

2. Clear the **Excessive Session Detection** check box.  
When disabled, the firewall does not detect applications on the local network that are creating excessive sessions to the Internet. This activity is due to a virus infected computer and on detection, the gateway displays a HURL warning page.
3. Clear the **TCP/UDP Port Scan** check box.  
When disabled, the firewall does not detect UDP and TCP port scans, and communicates the port scan packets to the computer.  
A port scan is a series of messages sent by an external entity attempting to break into a computer to learn which computer network services associated with UDP and TCP ports are provided by the computer.
4. Clear the **Invalid Source/Destination IP address** check box.  
When disabled, the firewall does not verify IP addresses for: Broadcast or multicast IP addresses, TCP destination IP address is not unicast, IP source and destination address are the same, Invalid IP source received from private/home network.
5. Clear the **Packet Flood (SYN/UDP/ICMP/Other)** check box.  
When disabled, the firewall does not check for SYN, UDP, ICMP, and other types of packet floods on the local and Internet facing interfaces.
6. Clear the **Invalid TCP Flag Attacks (NULL/XMAS/Other)** check box.  
When disabled, the firewall does not scan inbound and outbound packets for invalid TCP Flag settings, and communicates the packet that could result in NULL/XMAS/Other type of attacks.
7. Clear the **Invalid ICMP Detection** check box.  
When disabled, the firewall does not check for invalid ICMP/code types, and communicates the associated packets to the computer.
8. Clear the **Miscellaneous** check box.  
When disabled, the firewall does not scan any other type of inbound and outbound packets, other than the ones listed in the **Attack Detection** section.
9. Click **Save**. The ports listed in the **Attack Detection** section are disabled.

## Controlling Inbound and Outbound Traffic

### Objective

To control inbound and outbound protocol control services, so that the firewall blocks or passes the traffic from/to the network to/from the Internet.

### Steps

1. Navigate to **Settings > Firewall > Advanced Configuration**. The **Advanced configuration** page to configure the outbound and inbound protocols appears:

The screenshot displays the 'Outbound Protocol Control' and 'Inbound Protocol Control' sections of the firewall configuration interface. The 'Outbound Protocol Control' section includes a note: 'Checking the box ALLOWS the associated traffic type through the firewall.' Below this, a list of protocols is shown with checkboxes: HTTP, HTTPS, FTP, Telnet, SMTP, DNS, NetBIOS, POP3, IMAP, NNTP, IRC, H323, and All Other Protocols. The checkboxes for HTTP, HTTPS, FTP, Telnet, SMTP, DNS, POP3, IMAP, NNTP, IRC, H323, and All Other Protocols are checked, while NetBIOS is unchecked. The 'Inbound Protocol Control' section includes checkboxes for Remote Management (checked) and NetBIOS (unchecked).

Protocol	Checked
HTTP	Yes
HTTPS	Yes
FTP	Yes
Telnet	Yes
SMTP	Yes
DNS	Yes
NetBIOS	No
POP3	Yes
IMAP	Yes
NNTP	Yes
IRC	Yes
H323	Yes
All Other Protocols	Yes

Protocol	Checked
Remote Management	Yes
NetBIOS	No

2. Select or clear any check box in the **Outbound Protocol Control** section. If you select any of the check boxes in the **Outbound Protocol Control** section, the firewall allows the traffic from the network to pass through the firewall to the Internet.
3. Select or clear any check box in the **Inbound Protocol Control** section. If you select any of the check boxes in the **Inbound Protocol Control** section, the firewall allows the corresponding protocol to pass from the Internet to the network.
4. Click **Save**. This saves the configuration changes done to the inbound and outbound protocol control.

---

**Note** Allowing inbound traffic does not mean that the firewall automatically allows this type of traffic to pass through the firewall to the network. Even if a particular protocol/application type is allowed, the firewall still checks and blocks all unsolicited traffic from the Internet unless the firewall is configured to pass the traffic by hosting an application profile.

---

## Configuring Firewall Security Enhancements

### Objective

To configure firewall security enhancements. This allows you to configure the firewall rules to allow traffic on the UDP and TCP ports.

### Steps

1. Navigate to **Settings > Firewall > Advanced Configuration**. The **Advanced configuration** page to configure the security enhancements appears.

Enhanced Security

Stealth Mode	<input type="checkbox"/>
Block Ping	<input type="checkbox"/>
Strict UDP Session Control	<input type="checkbox"/>
UDP Session Timeout	<input type="text" value="600"/> seconds (600-43200 seconds, default = 600 seconds)
TCP Session Timeout	<input type="text" value="86400"/> seconds (300-86400 seconds, default = 86400 seconds)

2. Enable or disable stealth mode by selecting or clearing the **Stealth Mode** check box. When you enable stealth mode, the gateway firewall does not return any information in response to network queries; that is, it will appear to the intruder that your network does not exist. This discourages intruders from accessing your network, because it appears as though there is no active network to access.
3. Enable or disable the execution of external ping request by selecting or clearing the **Block Ping** check box. When you disable **Block Ping**, intruders can use ping to launch an attack against your network, because ping can determine the IP address of the network (for example, 105.246.172.72) from the domain name (for example, www.mynetwork.com). If you enable **Block Ping**, your network will block all ping requests.
4. Enable or disable the restricted transmission of packets by selecting or clearing the **Strict UDP Session Control** check box. When you enable restricted UDP session, security is enhanced and the gateway does not accept packets sent from an unknown source over an existing connection.
5. Enter the duration in seconds in the **UDP Session Timeout** text box. The gateway terminates the UDP connection request after that duration.
6. Enter the duration in seconds in the **TCP Session Timeout** text box. The gateway terminates the TCP connection request after that duration.
7. Click **Save**. This saves the configuration changes done to firewall security enhancements.

## Configuring Application Layer Gateway

### Objective

To configure Application Layer Gateway (ALG) on the firewall of the gateway.

If you enable SIP ALG, client applications can use dynamic TCP/ UDP ports to communicate with the known ports used by the server applications, even though a firewall configuration allows only a limited number of known ports.

If you disable ALG, the ports get blocked and you have to explicitly open up a large number of ports in the firewall rendering the network vulnerable to attacks on those ports.

## Steps

1. Navigate to **Settings > Firewall > Advanced Configuration**. The **Advanced configuration** page to configure the SIP ALG settings appears.



2. Enable or disable the **SIP ALG** on the gateway firewall by selecting or clearing the check box.
3. Click **Save**. This saves the configuration changes.

## See Also

[Configuring LAN Devices](#) on page 50

[Configuring Broadband Settings](#) on page 34

[Using Diagnostics Features](#) on page 93

[Troubleshooting 3801HGV Gateway](#) on page 109

## CHAPTER 11

# Viewing Logs

The **Logs** tab displays all types of logs which you can use to diagnose a problem, if any.

This section gives information about the following tabs:

- Event Log
- System Log
- Upgrade Log
- Firewall Log

## Viewing Event Log

### Objective:

To view event logs.

You can perform the following tasks on this page:

- View all event logs
- Assign a filter to view specific event logs
- Clear logs from the display list

## Viewing All Event Logs

### Steps:

To view all event logs, navigate to **Settings>Logs>Event Logs**. The following page appears.



Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Event Log System Log Upgrade Log Firewall Log

Event Log

Clear Log

Display Filter

Type	Date/Time	Event Description
INF	2009-11-29T22:48:29-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T22:51:02-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T22:53:35-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T22:56:08-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T22:58:41-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:01:15-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:03:48-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:06:21-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:08:54-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:11:27-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:14:01-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:16:34-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:19:07-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
INF	2009-11-29T23:21:40-08:00	fw,fwmon src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated

You can see all the event logs on this page.

**Note** Make sure that the option **all** is selected in the **Display Filter** list.

The following table displays information about the logs that you can view on the **Event Logs** page.

Name	Description
Type	The type of event. Given below is a list of event types: <ul style="list-style-type: none"> <li>• ALM: Alarms</li> <li>• DBG: Debug</li> <li>• EMR: Emergency</li> <li>• ERR: Error</li> <li>• FLT: Faults</li> <li>• INF: Information</li> <li>• NTC: Notice</li> <li>• WRN: Warning</li> </ul>
Date/Time	The date and time when the event occurs, with the latest date on the top.
Event Description	Source and destination IP addresses with their ports, and a brief description of the event.

## Filtering Logs

### Steps

To filter logs:

1. On the **Event Logs** page, select an option in the **Display Filter** drop-down list box.
2. Click **Submit** to view logs pertaining to the option that you selected.

You can clear logs on the **Event Log** page and minimize the clutter from previous events when you try to diagnose a problem.

## Clearing Event Logs

To clear all logs from a list, click the **Clear Log** button.

---

**Note** To clear a particular log type, select an option in the **Display Filter** list and then click **Clear Log**.

---

## Viewing System Log

### Objective:

To view system logs.

You can perform the following steps on this page:

- Filtering and viewing the following types of system logs
  - **DBG:** Debug
  - **INF:** Information
  - **NTC:** Notice
  - **WRN:** Warning
  - **ERR:** Error
  - **FTL:** Faults
  - **ALR:** Alarm
  - **EMR:** Emergency
- Insert mark to distinguish between old logs and new ones while diagnosing a problem
- Clear logs to minimize the clutter from previous events when you try to diagnose a problem.

## Filtering and Viewing System Logs

### Steps:

To filter and view system logs:

1. Navigate to **Settings>Logs>System Log**. The following page appears.

**zWIRE**

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Event Log System Log Upgrade Log Firewall Log

### System Log

Clear Log

Display Filter

Insert Mark in Log

Type	Date/Time	Event Description
INF	P0000-00-00T00:03:02	htpdp: xci_cmd_voicedev_get_vdstat
INF	P0000-00-00T00:03:09	htpdp: Previous log entry repeated 1 times
INF	P0000-00-00T00:04:48	vrsip: The network is not up yet.
INF	P0000-00-00T00:04:48	intpot: Failover state on port 0 changing from 3 to 0
INF	P0000-00-00T00:10:34	htpdp: xci_cmd_voicedev_get_vdstat
WRN	P0000-00-00T00:21:51	ulib: init_force: linking pm_ippool not bbipnet
INF	P0000-00-00T00:21:51	ulib: broadband type changed NONE %sgb; PPPoE on bband0
INF	P0000-00-00T00:21:51	ulib: DSL set to Auto on ds10
INF	P0000-00-00T00:21:51	ulib: PPP username and password changed on ppp0 to test
INF	P0000-00-00T00:22:24	voiced: Port 0: bband lost for 31 sec
INF	P0000-00-00T00:22:24	voiced: Port 1: bband lost for 31 sec
INF	P0000-00-00T00:23:00	ulib: DSL set to RJ11 on ds10
INF	P0000-00-00T00:23:00	ulib: PPP password changed on ppp0
INF	P0000-00-00T00:23:22	lmd: ds10: up G.993.2 interleaved Rate:37372/6275 Max:66263/4294967

2. Select a log type in the **Display Filter** drop-down list box.
3. Click **Submit** to view all logs of the type you selected.

**Note** You can further filter logs by selecting an option from the drop-down list box beside the **Submit** button, and click.



The following table displays information about the logs that you can view on the **System Log** page:

Name	Description
<b>Type</b>	The type of event for example, ALM, DBG, and so on.
<b>Date/Time</b>	The date and time when the event occurs, with the latest date on the top.
<b>Event Description</b>	A brief description of the event..

## Inserting Mark

### Steps

To insert a mark in the log and to view it:

1. Click the **Insert Mark** button on the **System Log** page.
2. Scroll down to the end of the page to view your mark. The figure below displays an inserted mark in the system log.

```

INF 2009-11-30T01:13:26-08:00      named: dropped malicious resp from 202.54.29.5
INF 2009-11-30T02:05:12-08:00      named: Previous log entry repeated 34 times
INF 2009-11-30T02:06:30-08:00      httpd: [REDACTED]
INF 2009-11-30T02:06:42-08:00      httpd: Previous log entry repeated 1 times
Next

```

## Clearing Logs

### Steps

To clear logs:

1. Select a type of logs in the **Display Filter** drop-down list box. You can further filter the logs by selecting an option in the next drop-down list box.
2. Click **Clear Log**.

## Viewing Upgrade Log

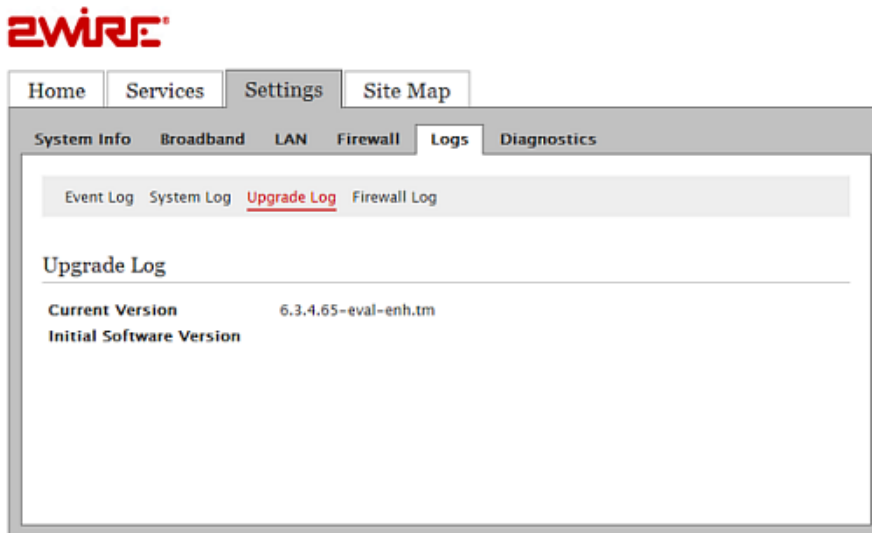
### Objective:

To view upgrade log.

You can view the software upgrade information about your system on this page.

**Steps:**

To view the upgrade information, navigate to **Settings>Logs>Upgrade Log**. The following page appears.



You can view the initial software version and the current software version of the system on this page.

## Viewing Firewall Log

**Objective:**

To view the firewall log.

You can perform the following tasks on this page:

- View firewall log
- Clear log

## Viewing Log

### Steps:

To view the firewall log:

1. Navigate to **Settings>Logs>Firewall Log**. The following page appears.

**ZWIRE**

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Event Log System Log Upgrade Log **Firewall Log**

**Firewall Log**

Clear Log Clear Log

Date and Time	Severity	Details
2009-11-30T00:30:36-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:33:09-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:35:43-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:38:16-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:40:49-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:43:22-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:45:55-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:48:29-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:51:02-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:53:35-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:56:08-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T00:58:41-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated
2009-11-30T01:01:15-08:00	info	src=172.16.102.1 dst=172.16.8.16 ipprot=1 icmp_type=3 icmp_code=1 ICMP Dest Unreachable, session terminated

The following table displays information about the logs that you can view on the **Firewall Log** page:

Name	Description
Type	The type of event. Given below is a list of event types: <ul style="list-style-type: none"> <li>• ALM: Alarms</li> <li>• DBG: Debug</li> <li>• EMR: Emergency</li> <li>• ERR: Error</li> <li>• FLT: Faults</li> <li>• INF: Information</li> <li>• NTC: Notice</li> <li>• WRN: Warning</li> </ul>
Date/Time	The date and time when the event occurs, with the latest date on the top.
Event Description	Source and destination IP addresses with their ports, and a brief description of the event.

## Clearing Log

You can clear logs on the **Firewall Log** page and minimize the clutter from previous events when you try to diagnose a problem.

To clear the firewall log, click the **Clear Log** button.

## CHAPTER 12

# Using Diagnostics Features

This chapter provides information about the tasks you can perform in the **Diagnostic** tab. Following are the links under the **Diagnostics** tab, and associated tasks:

- **Link Test**
  - [Testing Broadband Link](#) on page 93
- **Link Tree**
  - [Viewing Link Tree](#) on page 95
- **DSL**
  - [Viewing DSL Diagnostic Information](#) on page 96
- **IP Utilities**
  - [Testing IP Utilities](#) on page 97
- **NAT**
  - [Viewing NAT Information](#) on page 103
- **Syslog**
  - [Enabling Syslog](#) on page 105
- **Resets**
  - [Resetting the Gateway](#) on page 106

## Testing Broadband Link

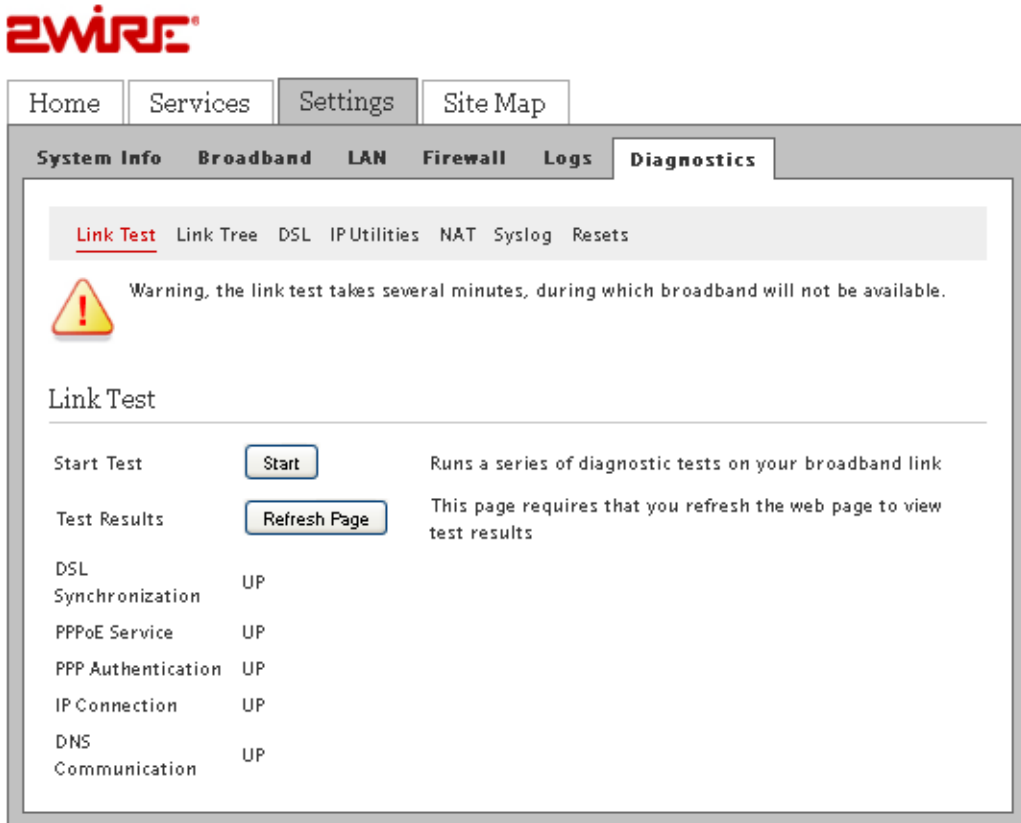
### Objective

To test your broadband connection.

You can run a series of diagnostic tests on your broadband connection on this page.

## Steps

1. Navigate to **Settings > Diagnostics > Link Test**. The **Link Test** page appears.




**2WIRE**

Home Services **Settings** Site Map

System Info Broadband LAN Firewall Logs **Diagnostics**

[Link Test](#) Link Tree DSL IPUtilities NAT Syslog Resets

 Warning, the link test takes several minutes, during which broadband will not be available.

### Link Test

Start Test  Runs a series of diagnostic tests on your broadband link

Test Results  This page requires that you refresh the web page to view test results

DSL Synchronization	UP
PPPoE Service	UP
PPP Authentication	UP
IP Connection	UP
DNS Communication	UP

2. Click **Start** to start running diagnostic tests on your broadband connection.
3. Click **Refresh Page** to view the results of your test.

---

**Note** Running diagnostic tests on your broadband connection may take a few minutes, and broadband will not be available during this time.

---

## Viewing Link Tree

To view Link Tree, navigate to **Settings > Diagnostics > Link Tree**. The **Link Tree** page appears.

**Z-WIRE**

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Link Test Link Tree DSL IP Utilities NAT Syslog Resets

### Link Tree

```

\-->root0 is UP
  |-->global0 is UP
    |-->device0 is UP
    |-->rnat0 is UP
    |-->route0 is UP
    |-->fw0 is UP
    |-->sysio0 is UP
    |-->phone0 is DOWN
    |-->phone1 is DOWN
    |-->led0 is UP
    \-->cms0 is UP
  |-->home0 is UP
    \-->bridge0 is UP
      |-->hostap0 is UP
      \-->ipnet1 is UP
        |-->bridgemon0 is UP
        \-->ippool0 is UP
  \-->bband0 is UP
    |-->dsl0 is UP
      \-->bridge1 is UP
        \-->eapol0 is UP
          \-->autoeth0 is UP
            \-->pppoe0 is UP
              \-->ppp0 is UP
                \-->ipnet0 is UP
                  \-->dnstest0 is UP
  \-->bridge2 is UP
  
```

You can click any link to view its details at the bottom of the page. This is shown in the figure below:

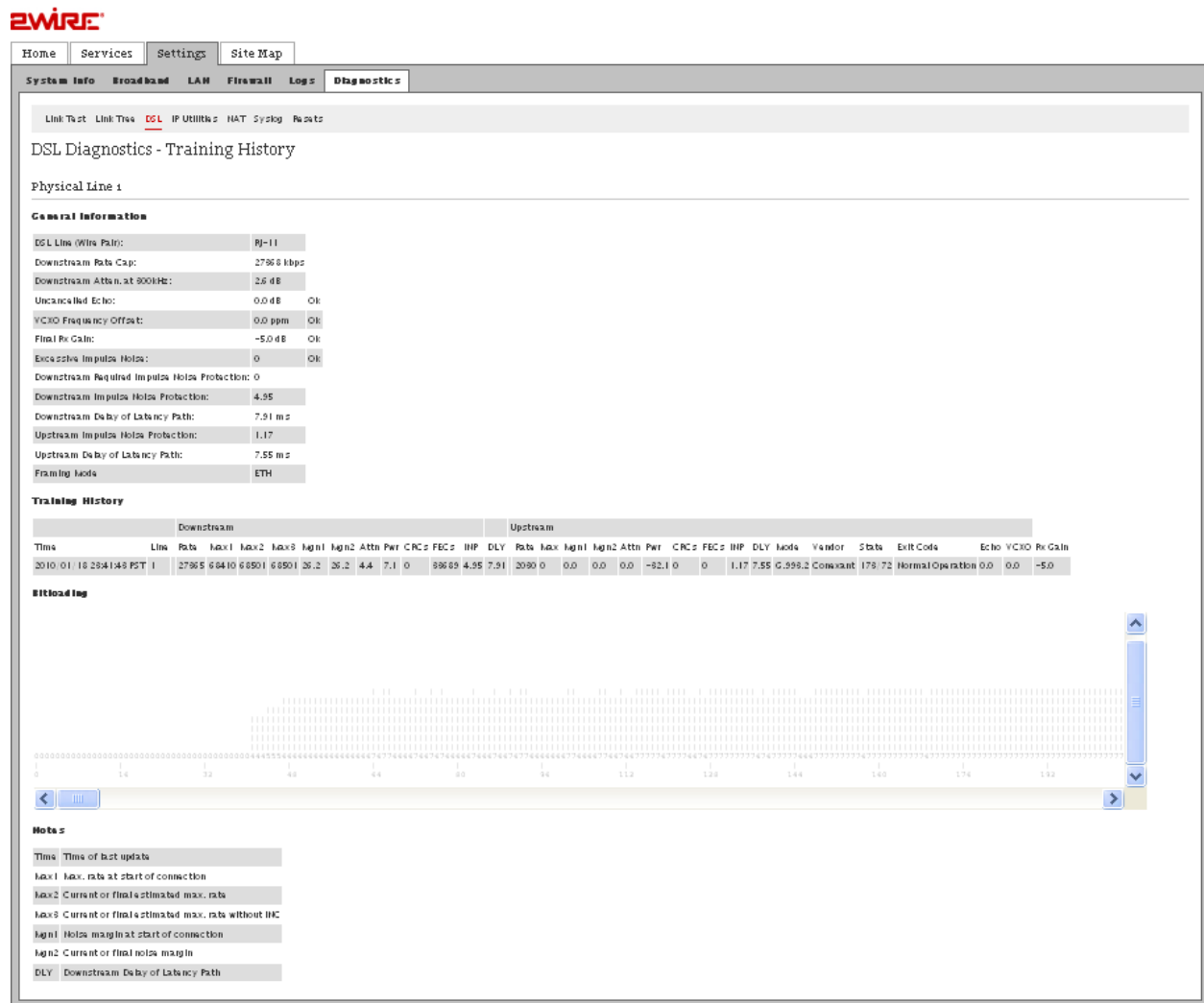
```
pm_root
Dependency State: UP
Link State: UP
Link Detail: NONE
Timeout: 0
File Descriptor flags: 00000000
Reported error string:
File Descriptor State: Count: 0 Active: 0 Events: 0

Module State Change History:
  To State: DOWN at: 00:00:10.52
```

## Viewing DSL Diagnostic Information

The **DSL** page displays diagnostic information about DSL which you can use in case of any problems. To view the DSL diagnostic information, navigate to **Settings > Diagnostics > DSL**. The **DSL** page appears.





You can view the following information on this page:

Parameter	Description
<b>General Information</b>	Technical information about the DSL.
<b>Training History</b>	Information about DSL training history.
<b>Bitloading</b>	Graphic representation of DSL bitloading.
<b>Note</b>	Explanation of terms used in DSL training history.

## Testing IP Utilities

### Objective

To test the following IP utilities:

- **Ping:** A computer network tool used to test whether a particular host is reachable across an IP network; it is also used to self test the network interface card of the computer, or as a latency test
- **Traceroute:** A computer network tool used to determine the route taken by packets across an IP network
- **DNSquery:** A generic query resolution interface

## Testing Ping

To test ping:

1. Navigate to **Settings > Diagnostics > IP Utilities**, and select **ping** in the **Test Type** drop-down list. The following page appears.

**Z-WIRE**

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Link Test Link Tree DSL IP Utilities NAT Syslog Resets

IP Utilities & Tests

Test Type ping

Host address 192.168.1.64

Enable Name Resolution

Test Depth 30 Times or Hops

Packet Size 64 Bytes (Maximum 576)

Test Results Start Stop

2. Type the host address in the **Host Address** text box.
3. Select the **Enable Name Resolution** check box if you want to find the IP address corresponding to the host address.
4. Click **Start** to start testing. You can view the results in the space provided. The following figure displays the test results.

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Link Test Link Tree DSL IP Utilities NAT Syslog Resets

### IP Utilities & Tests

Test Type: ping

Host address: 192.168.1.64

Enable Name Resolution:

Test Depth: 30 Times or Hops

Packet Size: 64 Bytes (Maximum 576)

Test Results: Start Stop

```
Pinging [192.168.1.64] 30 times with: 64 bytes of data
ping successful: icmp_seq=0 time=4 ms
ping successful: icmp_seq=1 time=2 ms
ping successful: icmp_seq=2 time=0 ms
ping successful: icmp_seq=3 time=1 ms
ping successful: icmp_seq=4 time=5 ms
ping successful: icmp_seq=5 time=3 ms
ping successful: icmp_seq=6 time=9 ms
ping successful: icmp_seq=7 time=0 ms
ping successful: icmp_seq=8 time=5 ms
ping successful: icmp_seq=9 time=12 ms
ping successful: icmp_seq=10 time=1 ms
ping successful: icmp_seq=11 time=3 ms
ping successful: icmp_seq=12 time=4 ms
ping successful: icmp_seq=13 time=4 ms
```

5. Click **Stop** to stop testing.

---

**Note** To clear logs, select all logs in the provided space, and press **Delete** on your keyboard.

---

## Testing Traceroute

To test traceroute:

1. Navigate to **Settings > Diagnostics > IP Utilities**, and **traceroute** in the **Test Type** drop-down list. The following page appears.



The screenshot shows the Z-Wire web interface. At the top, there is a navigation bar with tabs for Home, Services, Settings, and Site Map. Below this is a secondary navigation bar with tabs for System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The Diagnostics tab is active, and within it, the IP Utilities sub-tab is selected. The main content area is titled "IP Utilities & Tests" and contains the following configuration options:

- Test Type:** A dropdown menu set to "traceroute".
- Host address:** A text input field containing "localhost".
- Enable Name Resolution:** A checked checkbox.
- Test Depth:** A text input field containing "30", with the label "Times or Hops" to its right.
- Packet Size:** A text input field containing "64", with the label "Bytes (Maximum 576)" to its right.
- Test Results:** Two buttons labeled "Start" and "Stop".

Below the configuration options is a large, empty rectangular box intended for displaying the test results.

2. Type the host address in the **Host Address** text box.
3. Select the **Enable Name Resolution** check box if you want to find the IP address corresponding to the host address.
4. Click **Start** to start testing. You can view the results in the space provided. The following figure displays the test results.

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Link Test Link Tree DSL IP Utilities NAT Syslog Resets

### IP Utilities & Tests

Test Type:

Host address:

Enable Name Resolution:

Test Depth:  Times or Hops

Packet Size:  Bytes (Maximum 576)

Test Results:

```
traceroute 127.0.0.1 with 64 packetsize
1: localhost (127.0.0.1) 0 ms
```

5. Click **Stop** to stop testing.

---

**Note** To clear logs, select all logs in the provided space, and press **Delete** on your keyboard.

---

## Testing Dnsquery

To test dnsquery:

1. Navigate to **Settings > Diagnostics > IP Utilities**, and **dnsquery** in the **Test Type** drop-down list. The following page appears.

**Z-WIRE**

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Link Test Link Tree DSL IP Utilities NAT Syslog Resets

IP Utilities & Tests

Test Type: dnsquery

Host address: localhost

Enable Name Resolution:

Test Depth: 30 Times or Hops

Packet Size: 64 Bytes (Maximum 575)

Test Results: Start Stop

2. Type the host address in the **Host Address** text box.
3. Select the **Enable Name Resolution** check box if you want to find the IP address corresponding to the host address.
4. Click **Start** to start testing. You can view the results in the space provided. The following figure displays the test results.

5. Click **Stop** to stop testing.

---

**Note** To clear logs, select all logs in the provided space, and press **Delete** on your keyboard.

---

## Viewing NAT Information

Network Address Translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for remapping a given address space into another.

Most NAT devices allow the network administrator to configure table entries for permanent use. This feature is referred to as port forwarding, and allows traffic originating in the “outside” network to reach designated hosts in the masqueraded network.

To view NAT information navigate to **Settings > Diagnostics > NAT**. The **NAT** page appears.



Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Link Test
Link Tree
DSL
IP Utilities
NAT
Syslog
Resets

## Pinholes

---

```
external pin-holes (189 available):
pinh[0]: id 1, proto 6, sess tout 86400, pinh tout 0, arg 0 natpt|user, alg MSGAME
  1: 192.168.1.64:47624, n: 172.16.8.16:47624
pinh[1]: id 2, proto 17, sess tout 600, pinh tout 0, arg 0 natpt|user, alg MSGAME
  1: 192.168.1.64:47624, n: 172.16.8.16:47624
pinh[2]: id 3, proto 6, sess tout 86400, pinh tout 0, arg 0 natpt|user, alg PPTP
  1: 192.168.1.64:72-80, n: 172.16.8.16:72-80
```

## Current NAT Sessions

---

```
current secs since boot: 68284
session table 1019/1024 available, 0/512 used in inbound sessions:
sess[235]: bkt 141, flags: 0x00000190, proto: 17, cnt: 2
  1: 172.16.8.16:50918, f: 202.54.29.5:53, n: 172.16.8.16:50918
  last used 67873, max_idle: 600
sess[239]: bkt 205, flags: 0x00000190, proto: 17, cnt: 2
  1: 172.16.8.16:49569, f: 202.54.10.2:53, n: 172.16.8.16:49569
  last used 68070, max_idle: 600
sess[241]: bkt 206, flags: 0x00000190, proto: 17, cnt: 1
  1: 172.16.8.16:49570, f: 202.54.29.5:53, n: 172.16.8.16:49570
  last used 68072, max_idle: 600
sess[238]: bkt 224, flags: 0x00000190, proto: 17, cnt: 2
  1: 172.16.8.16:49548, f: 202.54.29.5:53, n: 172.16.8.16:49548
  last used 68073, max_idle: 600
sess[236]: bkt 241, flags: 0x00000190, proto: 17, cnt: 2
  1: 172.16.8.16:49565, f: 202.54.29.5:53, n: 172.16.8.16:49565
  last used 68064, max_idle: 600
```

## TCP Redirection

---

### Source IP based

Interface Name:

Enabled:  Disabled

Mode:  Blacklist

Networks:

### Destination IP based

Interface Name:

Enabled:  Disabled

Mode:  Blacklist

Networks:



You can view the following information on this page:

Name	Description
<b>Pinholes</b>	A firewall pinhole is a port that is opened through a firewall to allow a particular application/Web site to gain controlled access to the protected network. This area displays the pinholes that you have used.
<b>Current NAT Sessions</b>	Displays information about all current NAT sessions.
<b>TCP Redirection</b>	Displays interface information about the source and destination based IPs.

## Enabling Syslog

### Objective:

To enable the syslog feature.

The syslog feature allows you to send system logs to a remote server. To view logs sent to the remote server, make sure that you install and configure the syslog server when you configure the gateway.

### Steps:

1. Navigate to **Settings>Diagnostics>Syslog**. The following page appears.

The screenshot shows the Z-Wire gateway web interface. At the top, there is a navigation menu with 'Home', 'Services', 'Settings', and 'Site Map'. Below this, there are several tabs: 'System Info', 'Broadband', 'LAN', 'Firewall', 'Logs', and 'Diagnostics'. The 'Diagnostics' tab is selected, and within it, the 'Syslog' sub-tab is active. The Syslog configuration page contains the following fields:

- Enable Syslog:** A checked checkbox.
- Server Location:** A text box containing '192.168.1.65'.
- Server Port:** A text box containing '514' with 'Default: 514' next to it.
- Enable Throttling:** An unchecked checkbox.
- Limit Logging to:** A text box containing '0' followed by 'logs per second'.

A 'Save' button is located at the bottom right of the configuration area.

2. Select the **Enable Syslog** check box.
3. Enter the IP address of the server in the **Server Location** text box.
4. Select **Enable Throttling** if you want to limit the number of logs sent to the server per second. Selecting this feature increases server performance.

5. Enter an integer greater than 0 in the **Limit Logging to** text box.
6. Click **Save**.

## Resetting the Gateway

### Objective

To reset the gateway.

You may need to reset the HomePortal 3801HGV gateway if one or all the LEDs is/are solid red. This indicates that there is some failure within the system. It is recommended that you discuss your problems with customer service before attempting to reset your device.

You can work with the following areas on this page:

- **System & Link Resets**  
You can reset the following in this area:
  - Device List
  - IP/PPP
  - Broadband
  - System
- **Configuration Resets**  
You can reset the following in this area:
  - Wireless Configuration
  - Firewall Configuration
- **Reset to Factory Default State**  
You can reset the gateway to factory default in this area

---

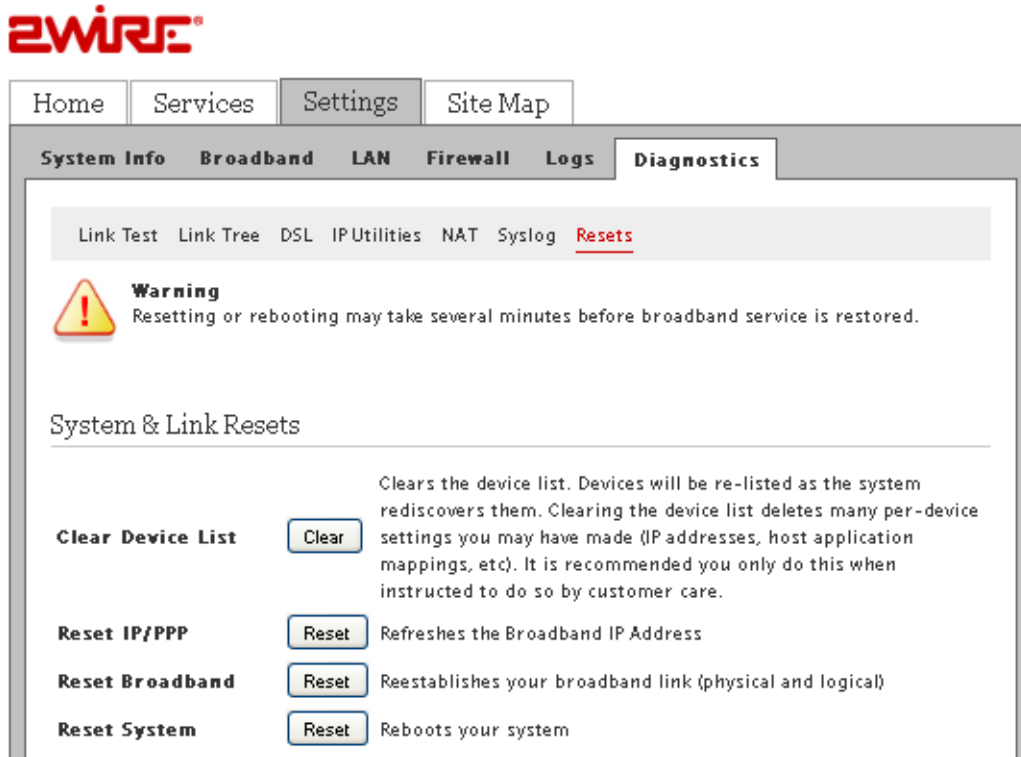
**Note** Resetting the system or rebooting it may take several minutes before broadband is restored.

---

## Resetting System and Links

To reset the system and links:

1. Navigate to **Settings > Diagnostics > Resets**. The **Resets** page appears. The following figure displays the **System and Link Resets** section in the **Resets** page.



2. In the **System & Link Resets** section:
  - a. Click **Clear** if you want to clear the device list. Devices will be re-listed as the system rediscovers them.

---

**Note** Clearing the device list deletes many per-device settings you may have made (IP addresses, host application mappings, and so on). It is recommended that you do this only when instructed by a customer support executive.

---

- b. Click **Reset** for **Reset IP/PPP** if you want to refresh the broadband IP address.
- c. Click **Reset** for **Reset Broadband** if you want to re-establish your broadband connection.
- d. Click **Reset** for **Reset System** if you want to reboot your system.

## Resetting Configuration

To reset the configuration:

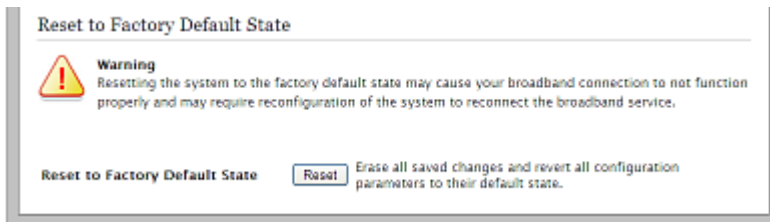
1. Navigate to **Settings > Diagnostics > Resets**. The **Resets** page appears. The following figure displays the **Configuration Resets** section in the **Resets** page.



2. In the **Configuration Resets** section:
  - a. Click **Reset** for **Wireless Configuration Reset** if you want to reset the wireless AP settings to factory default.
  - b. Click **Reset** for **Firewall Configuration Reset** if you want to reset the firewall settings to factory default.

## Resetting Device to Factory Default

In the **Reset to Factory Default State** section, click **Reset** for **Reset to Factory Default State** if you want to reset the firewall settings to factory default.



---

**Note** Resetting device to factory default will erase all saved changes and revert all configuration parameters to their default status.

---

### See Also

- [Configuring LAN Devices](#) on page 50
- [Configuring Firewall Settings](#) on page 72
- [Configuring Broadband Settings](#) on page 34
- [Troubleshooting 3801HGV Gateway](#) on page 109

## CHAPTER 13

# Troubleshooting 3801HGV Gateway

This chapter provides information about troubleshooting the HomePortal 3801HVG gateway hardware and firmware issues. It lists the issues, possible cause(s), and solution(s) in a tabular format. The issues mentioned in this chapter are based on likely user scenarios.

## Connection Issues

The following table provides information to troubleshoot connection issues:

Issue	Possible Cause(s)	What to Do
No POWER light	Power supply is faulty	<ul style="list-style-type: none"><li>• Verify that the AC power cable is securely connected to the gateway</li><li>• Ensure that the AC power cable is not plugged in to a switched outlet that is powered off</li><li>• Power up the gateway with a known good power outlet</li><li>• Replace the location of the gateway if it does not power up with a known good power outlet</li><li>• If the issue persists, the AC power cable needs replacement</li></ul>
POWER LED blinks just after starting the device and then turns solid green	Power on self test (POST)	Normal behavior.
POWER LED is solid red	System POST Failure	<ul style="list-style-type: none"><li>• Press the Reset button on the gateway for 10 seconds</li><li>• Replace the gateway if it does not power up into a normal state</li></ul>
BROADBAND LED blinking	VDSL connection not established	Verify if VDSL service is activated on the phone cable connected to the gateway. To do so, contact the ISP.
	Loose Ethernet or DSL cable	Check the Ethernet cable connection on the gateway and the phone jack, and make sure that it is securely seated in both ports.
SERVICE LED blinking	Internet service is not activated	Contact your ISP to activate Internet service.
BROADBAND LED blinks green for an extended period of time, then turns solid red	Failed broadband link synchronization between the gateway and the DSLAM with which it is directly connected	<ul style="list-style-type: none"><li>• Check the Ethernet cable connection on the computer and gateway, and make sure that it is securely seated in both ports</li><li>• Verify if VDSL service is activated on the phone cable connected to the gateway. To do so, contact the ISP</li></ul>
SERVICE LED is solid red	Internet service authentication failure and/or failure to receive address assignment	<ul style="list-style-type: none"><li>• Contact your ISP to check if the Internet connection is activated</li><li>• Check if the PPPoE or DHCP server is assigning an IP address to your gateway</li></ul>
No ETHERNET light	Inadequate connectivity	Check the Ethernet cable connection on the computer and gateway, and make sure that it is securely seated in both the ports.
	Ethernet interface is disabled	Select the <b>Ethernet Networking</b> check box from <b>Settings &gt; LAN &gt; Wired Interfaces</b> .

Issue	Possible Cause(s)	What to Do
No WIRELESS light	LAN clients are not connected to the gateway through the wireless interface	Ensure that at least one LAN client is connected to the wireless connection of the gateway.
	Wireless Interface is disabled	Select the <b>Enable Wireless Interface</b> check box from <b>Settings &gt; LAN &gt; Wireless</b> .
Internet is not accessible but user interface of the gateway is accessible	Inadequate connectivity	Check the physical connectivity of the RJ11 cable to the phone line port of the gateway device. Try using a different cable.
	Incorrect broadband settings	<ul style="list-style-type: none"> <li>Check the connectivity status of Internet and DSL Link on the user interface by navigating to <b>Settings &gt; Broadband &gt; Status</b></li> <li>Restart the gateway to refresh the broadband connection</li> </ul>
	Incorrect LAN computer settings	Ensure that the correct settings are configured on the LAN computer.
No HOME PNA light	Inadequate connectivity	Check the COAX cable connection on the CABLE port of the gateway and the COAX adapter and make sure that it is securely seated in both ports.
	Home PNA networking is disabled	Select the <b>HomePNA Networking</b> check box from <b>Settings &gt; LAN &gt; Wired Interfaces</b> .

## VoIP Issues

The following table provides information to troubleshoot VoIP issues:

Issue	Possible Cause(s)	What to Do
No VOICE 1 and VOICE 2 lights	Inadequate connectivity	Check the RJ-14 cable connection from the gateway to the phone port(s) and make sure that it is securely seated in both ports.
No VoIP service	VoIP services are not subscribed	<ul style="list-style-type: none"> <li>Check your line status. Navigate to <b>Services &gt; Voice &gt; Status</b></li> <li>Call for VoIP service</li> </ul>
No dial tone	Service is down	Check your line status. Navigate to <b>Services &gt; Voice &gt; Status</b> .
		Verify if the phone is in the Active mode: <ul style="list-style-type: none"> <li>If yes, click <b>Ring Now</b> to test the ring tone</li> <li>If the phone does not ring, check that the RJ-11 is securely connected to the phone port</li> <li>If the issue persists, call the service provider</li> </ul>

## Home PNA Issues

The following table provides information to troubleshoot Home PNA issues:

Issue	Possible Cause(s)	What to Do
No HOME PNA service	HOME PNA service is not activated	Check with your ISP for activating IPTV services.

## System Information Issues

The following table provides information to troubleshoot system information issues:

Issue	Possible Cause(s)	What to Do
Unable to set time and date manually	Override Automatic Time Configuration check box is not selected	Select the <b>Override Automatic Time Configuration</b> check box to apply the manually configured time and date settings. Ensure that you configure the time in hh:mm:ss format and date in yyyy/mm/dd format before selecting the check box.
Device does not detect and log broadband connection issues	Broadband status notification not enabled	Navigate to <b>Settings &gt; System Info &gt; Event Notifications</b> . Select the <b>Broadband Status Notification</b> check box.
Device does not detect tailed router	Router-behind-router detection not enabled	Navigate to <b>Settings &gt; System Info &gt; Event Notifications</b> . Select the <b>Router-Behind-Router Detection</b> check box.

## Broadband Issues

The following table provides information to troubleshoot broadband issues:

Issue	Possible Cause(s)	What to Do
Unable to connect to the Internet	Incorrect interface type	Navigate to <b>Settings &gt; Broadband &gt; Link Configuration</b> . Select the correct interface type from the <b>Choose Interface type</b> drop-down list box.
	Incorrect line type	Navigate to <b>Settings &gt; Broadband &gt; Link Configuration</b> . Select the correct line type from the <b>DSL Line Selection</b> drop-down list box.
	Incorrect connection type	Navigate to <b>Settings &gt; Broadband &gt; Link Configuration</b> . Select the correct connection type from the <b>Connection Type</b> drop-down list box.
	Incorrect PPP authentication settings	Navigate to <b>Settings &gt; Broadband &gt; Link Configuration</b> . Enter the correct <b>Username</b> and <b>Password</b> in the text boxes.
	Routing is disabled. This results in the device not getting the IP address automatically from the ISP	Navigate to <b>Settings &gt; Broadband &gt; Link Configuration</b> . Select the <b>Routing</b> check box.
Unable to get public IP address on LAN computers	Gateway in route mode	Disable the route mode. This disables Routing and NAT on the gateway.

---



---

**NOTE TO REVIEWER:** Suggest Routing and Multicast related issues to be added to this section.

---



---

## LAN Issues

The following table provides information to troubleshoot LAN issues:

Issue	Possible Cause(s)	What to Do
Unable to connect to the gateway through the local Ethernet port	Loose Ethernet cable connection	<ul style="list-style-type: none"> <li>Check the Ethernet cable connection on the computer and gateway, and make sure that it is securely seated in both ports</li> <li>Check the <b>ETHERNET</b> indicator on the gateway; it should blink green</li> </ul>
	Incorrect Ethernet mode selected	Navigate to <b>Settings &gt; LAN &gt; Wired Interfaces</b> . Select the appropriate mode from the <b>Port Mode</b> drop-down list box. <b>Auto-detect</b> is the recommended mode for configuring <b>Local Ethernet</b> connection.
LAN clients are not getting IP addresses to connect to the gateway	DHCP server is disabled	Navigate to <b>Settings &gt; LAN &gt; DHCP</b> . Select the <b>DHCP Server Enabled</b> check box for enabling the gateway to assign IP addresses to the LAN clients automatically.
IP address conflict between LAN computers on the network	Duplication of IP address on the network	If the LAN computer has static IP configured, ensure that DHCP IP addressing on the gateway is not assigning an identical IP address. Change the DHCP server IP addressing range and try assigning a different static IP address to the LAN computers.  If the issue persists, then configure DHCP on the LAN computer to obtain the IP address automatically.
No HomePNA service	HOME PNA services are not activated	Check with your ISP for activating IPTV services.
	Home PNA networking is disabled	Select the <b>HomePNA Networking</b> check box from <b>Settings &gt; LAN &gt; Wired Interfaces</b> .
Wireless client is not locating the gateway	SSID Broadcast is disabled	Navigate to <b>Settings &gt; LAN &gt; Wireless</b> . Select the <b>SSID Broadcast</b> check box in the Network section.
Wireless client is not getting an IP address	Wireless networking is disabled	Navigate to <b>Settings &gt; LAN &gt; Wireless</b> . Select the <b>Enable Wireless Interface</b> checkbox.
	Incorrect authentication type is used	Ensure that you select the relevant authentication type for configuring your wireless client.
	Wireless modes on client and access point are not compatible	Ensure that the wireless mode on the wireless client is compatible to the wireless mode on the gateway.
Wireless signal strength is weak	Wireless client is not in the wireless range	Ensure that your wireless client is within the wireless range of the gateway.
	Incorrect power settings	Change the <b>Power Setting</b> value to increase the signal strength.
	Wireless channel interference	Change the <b>Wireless Channel</b> value. Alternatively, you can also change the Wireless Channel Mode to auto.
Setting custom encryption key on the user interface gives an error	Custom encryption key is not conforming with the security mode, key length, key type, or value type	Configure the custom encryption key in a way that it conforms to the security mode, key length, key type, or value type.
LAN clients are unable to access specific applications or Web sites	Firewall is preventing the LAN clients from accessing specific applications or Web sites	Navigate to <b>Settings &gt; LAN &gt; IP Address Allocation</b> . Browse to the LAN client where access is restricted. Select <b>Disabled</b> from the <b>Firewall</b> drop-down list box.



## Firewall Issues

The following table provides information to troubleshoot firewall issues:

Issue	Possible Cause(s)	What to Do
HTTP service not available	HTTP traffic is disabled	Navigate to <b>Settings &gt; Firewall &gt; Advanced Configuration</b> . Select the <b>HTTP</b> checkbox from the Outbound Protocol Control section to enable the HTTP traffic to pass through the firewall.
Unable to connect to the VPN tunnel	Unsupported port	Check if the VPN service supports PPPoE, L2TP, PPTP, and IPSec ports. If not, then you must open the supported port. To open the supported port, perform port forwarding, that is, add a new user-defined application.

## Diagnostic Issues

The following table provides information to troubleshoot diagnostic issues:

Issue	Possible Cause(s)	What to Do
Ping/Traceroute/DNS query does not respond	Incorrect host address is entered	Ensure that you populate the correct destination IP in the Host Address text box.
Remote logging error	Syslogging is disabled	Enable Syslog and enter the appropriate server location to populate the logs at the remote node.
	Syslog server is not installed/enabled on the remote node	Ensure that you install a third party software to populate the syslogs on the remote node.

## APPENDIX A

# Glossary

Term	Description
Access Point	A device that transports data between a wireless network and a wired network. With the help of the system, a wireless base station is an example of an access point that acts between a wireless node and with other wired PCs and peripherals.
Default Gateway	A device that is placed between network segments (or "subnets") to ensure that traffic is properly routed between different subnets. To communicate with a device on another network, users need to know the default gateway's IP address.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that allows servers to assign IP addresses dynamically to PCs and workstations. The PC or workstation "borrows" the IP address for a period of time, then the IP address returns to the DHCP server for reassignment.
DMZ (Demilitarized Zone)	A computer or small subnetwork that sits between a trusted internal network (such as a LAN), and an untrusted external network (such as the Internet). Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and DNS servers.
DNS (Domain Name System)	The DNS is the way that Internet domain names (such as www.2wire.com) are located and translated into IP addresses.
DSLAM (Digital Subscriber Line Access Multiplexer)	A device found in telephone company central offices that takes a number of DSL subscriber lines and concentrates them onto a single ATM line.
Ethernet	A type of local area network that operates over twisted wire and cable at speeds of up to 10 Mbps.
ICMP (Internet Control Message Protocol)	ICMP supports packets containing error, control, and informational messages. For example, the PING command uses ICMP to test an Internet connection. Although ICMP is generally harmless, there are some message types that should be dropped. Redirect (5), Alternate Host Address (6), and Router Advertisement (9) can be used to redirect traffic from your site. Echo (8), Timestamp (13), and Address Mask Request (17) can be used to obtain information on whether the host is up, the local time, and the address mask used on your network, respectively. ICMP messages are also sometimes used as part of DOS attacks (such as flood ping or ping of death).
Invalid TCP flags.	Combination of TCP flags (such as SYN/FIN) that signal a malicious attempt to get past the firewall.
IP (Internet Protocol).	The standard signaling method used for all communication over the Internet.
IP Address.	A numeric identifier for your computer. Just as the post office delivers mail to your home address, servers know to deliver data to your computer based on your IP address. IP addresses can be dynamic, meaning that your computer "borrows" the IP address for the necessary timeframe, or they can be fixed, meaning that the number is permanently assigned to your computer.
LAN (Local Area Network).	A network connecting a number of computers to each other or to a central server so that the computers can share programs and files.
MAC (Media Access Control) Address	A hardware address that has been embedded into the network interface card (NIC) by its vendor to uniquely identify each node, or point of connection, of a network.
Map to Host Port	When set (not left blank or set to 0), this value provides the mapping offset to the local computer. For example, if this value is set to 4000 and the range being opened is 100 to 108, the forwarded data to the first value in the range will be sent to 4000. Subsequent ports will be mapped accordingly; 101 will be sent to 4001, 102 will be sent to 4002, and so on.
MTU (maximum transmission unit)	The largest size packet or frame, specified in octets (eight-bit bytes), that can be sent from a computer to the network. The Internet's TCP uses the MTU to determine the maximum size of each packet in any transmission. If the MTU is too large, the packet may need to be retransmitted if it encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled. Most computer operating systems provide a default MTU value that is suitable for most users. In general, Internet users should follow the advice of their Internet service provider (ISP) about whether to change the default value and what to change it to.

Term	Description												
NAT (Network Address Translation)	Enables a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. This feature is used by the system so an end user can have an internal computer network in their home, with all its computers using internal IP addresses, using only one routable IP address, which accesses the outside (Internet).												
PAT (Port Address Translation)	Allows hosts on a LAN to communicate with the rest of a network (such as the Internet) without revealing their own private IP address. All outbound packets have their IP address translated to the router's external IP address. Replies come back to the router, which then translates them back into the private IP address of the original host for final delivery.												
PPP (Point-to-Point Protocol)	A protocol that allows a computer to access the Internet using a dial-up phone line and a high-speed modem. This can be accomplished over Ethernet (PPPoE), or over Asynchronous Transfer Mode (ATM; PPPoA).												
PPPoA (Point-to-Point Protocol over ATM)	A specification for connecting multiple computer users on an Ethernet LAN to a remote site through common customer premises equipment (such as a modem). PPPoA combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the ATM (Asynchronous Transfer Mode) protocol, which supports multiple users in a LAN.												
PPPoE (Point-to-Point Protocol over Ethernet)	A specification for connecting multiple computer users on an Ethernet LAN to a remote site through common customer premises equipment (such as a modem). PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a LAN.												
Protocol Timeout	The amount of time (in seconds) during which a connection in the specified range remains open when there is no data transfer. After a connection has been established on a given port, the sender and receiver usually determine when the session is finished and the connection is closed. However, if the connection is left open and data transfer stops, the system must eventually close the connection and reclaim the resources in order to protect your network. In some cases, the system might close the application during normal operation (for example, if there is a long pause between data transfer). If this is the case, lengthening the timeout may help.												
PVC (permanent virtual circuit)	A virtual circuit that is permanently available. Used to establish connections between hosts that communicate frequently.												
Router	The central switching device in a packet-switched computer network that directs and controls the flow of data through the network.												
Subnet Mask	<p>The IP addressing system allows subnetworks or "interchanges" to be created, and devices numbers or "extensions" to be established within these subnetworks. These numbers are created using a mathematical device called a subnet mask. A subnet mask, like the IP address, is a set of four numbers in dotted decimal notation. Subnet masks typically take three forms:</p> <ul style="list-style-type: none"> <li>• 255.0.0.0</li> <li>• 255.255.0.0</li> <li>• 255.255.255.0</li> </ul> <p>The number 255 "masks" out the corresponding number of the IP address, resulting in IP address numbers that are valid for the network. For example, an IP address of 123.45.67.89 and a subnet mask of 255.255.255.0 results in a sub network number of 123.45.67.0 and a device number of 89.</p> <p>The subnet mask used for the network typically corresponds to the class of IP address assigned, as shown in the following table:</p> <table border="1" data-bbox="683 1543 1333 1829"> <thead> <tr> <th data-bbox="688 1549 857 1629">IP Address Class</th> <th data-bbox="857 1549 1062 1629">Dotted-Decimal Notation</th> <th data-bbox="1062 1549 1328 1629">Ranges Corresponding Subnet Mask</th> </tr> </thead> <tbody> <tr> <td data-bbox="688 1629 857 1690">Class A</td> <td data-bbox="857 1629 1062 1690">1.xxx.xxx.xxx to 126.xxx.xxx.xxx</td> <td data-bbox="1062 1629 1328 1690">255.0.0.0</td> </tr> <tr> <td data-bbox="688 1690 857 1751">Class B</td> <td data-bbox="857 1690 1062 1751">128.0.xxx.xxx to 191.255.xxx.xxx</td> <td data-bbox="1062 1690 1328 1751">255.255.0.0</td> </tr> <tr> <td data-bbox="688 1751 857 1822">Class C</td> <td data-bbox="857 1751 1062 1822">192.0.0.xxx to 223.255.255.xx x</td> <td data-bbox="1062 1751 1328 1822">255.255.255.0</td> </tr> </tbody> </table>	IP Address Class	Dotted-Decimal Notation	Ranges Corresponding Subnet Mask	Class A	1.xxx.xxx.xxx to 126.xxx.xxx.xxx	255.0.0.0	Class B	128.0.xxx.xxx to 191.255.xxx.xxx	255.255.0.0	Class C	192.0.0.xxx to 223.255.255.xx x	255.255.255.0
IP Address Class	Dotted-Decimal Notation	Ranges Corresponding Subnet Mask											
Class A	1.xxx.xxx.xxx to 126.xxx.xxx.xxx	255.0.0.0											
Class B	128.0.xxx.xxx to 191.255.xxx.xxx	255.255.0.0											
Class C	192.0.0.xxx to 223.255.255.xx x	255.255.255.0											

Term	Description																												
SYN Flood	A method that the user of a hostile client program can use to conduct a denial-of-service (DOS) attack on a computer server. The hostile client repeatedly sends SYN (synchronization) packets to every port on the server, using fake IP addresses.																												
TCP/IP (Transmission Control Protocol/Internet Protocol)	A method of packet-switched data transmission used on the Internet. The protocol specifies the manner in which a signal is divided into parts, as well as the manner in which "address" information is added to each packet to ensure that it reaches its destination and can be reassembled into the original message.																												
UDP (User Datagram Protocol)	A TCP/IP protocol describing how data packets reach application programs within a destination computer.																												
VPI (Virtual Path Identifier)	Identifier contained in the ATM cell header to designate the virtual path on the physical ATM link.																												
VCI (Virtual Channel Identifier)	Identifier contained in the ATM cell header to designate the virtual channel on the physical ATM link.																												
Wireless	Transmission of data over radio waves rather than wiring.																												
Wireless Channel	<p>The 2Wire gateway supports up to 13 wireless channels (based on country restrictions).</p> <p>For example, the United States and Canada support channels 1 to 11; Europe and Australia support channels 1 to 13.</p> <p>In an 802.11b or 802.11g wireless network, data is transmitted at 2.5GHz. Wireless nodes communicate with each other using radio frequency signals in the band between 2.4GHz and 2.5GHz. Neighboring channels are 5 MHz apart; however, due to the spread spectrum effect of the signals, a node sending signals using a particular channel will use frequency spectrum 12.5MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channels 1 and 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation (such as channels 1 and 6, or channels 6 and 11) will provide a noticeable performance increase over networks with minimal channel separation.</p> <p>The radio frequency channels used in 802.11b/g networks are shown in the following table:</p> <table border="1" data-bbox="685 1115 1193 1640"> <thead> <tr> <th data-bbox="685 1115 878 1157">Channel</th> <th data-bbox="878 1115 1193 1157">Frequency</th> </tr> </thead> <tbody> <tr> <td data-bbox="685 1157 878 1192">Channel 1</td> <td data-bbox="878 1157 1193 1192">2399.5 MHz-2424.5 MHz</td> </tr> <tr> <td data-bbox="685 1192 878 1228">Channel 2</td> <td data-bbox="878 1192 1193 1228">2404.5 MHz-2429.5 MHz</td> </tr> <tr> <td data-bbox="685 1228 878 1264">Channel 3</td> <td data-bbox="878 1228 1193 1264">2409.5 MHz - 2434.5 MHz</td> </tr> <tr> <td data-bbox="685 1264 878 1299">Channel 4</td> <td data-bbox="878 1264 1193 1299">2414.5 MHz - 2439.5 MHz</td> </tr> <tr> <td data-bbox="685 1299 878 1335">Channel 5</td> <td data-bbox="878 1299 1193 1335">2419.5 MHz - 2444.5 MHz</td> </tr> <tr> <td data-bbox="685 1335 878 1371">Channel 6</td> <td data-bbox="878 1335 1193 1371">2424.5 MHz - 2449.5 MHz</td> </tr> <tr> <td data-bbox="685 1371 878 1407">Channel 7</td> <td data-bbox="878 1371 1193 1407">2429.5 MHz - 2454.5 MHz</td> </tr> <tr> <td data-bbox="685 1407 878 1442">Channel 8</td> <td data-bbox="878 1407 1193 1442">2434.5 MHz - 2459.5 MHz</td> </tr> <tr> <td data-bbox="685 1442 878 1478">Channel 9</td> <td data-bbox="878 1442 1193 1478">2439.5 MHz - 2464.5 MHz</td> </tr> <tr> <td data-bbox="685 1478 878 1514">Channel 10</td> <td data-bbox="878 1478 1193 1514">2444.5 MHz - 2469.5 MHz</td> </tr> <tr> <td data-bbox="685 1514 878 1549">Channel 11</td> <td data-bbox="878 1514 1193 1549">2449.5 MHz - 2474.5 MHz</td> </tr> <tr> <td data-bbox="685 1549 878 1585">Channel 12</td> <td data-bbox="878 1549 1193 1585">2454.5 MHz - 2479.5 MHz</td> </tr> <tr> <td data-bbox="685 1585 878 1621">Channel 13</td> <td data-bbox="878 1585 1193 1621">2459.5 MHz - 2484.5 MHz</td> </tr> </tbody> </table> <p>The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and expand to channel 6 (and 11 when necessary), as these three channels do not overlap.</p>	Channel	Frequency	Channel 1	2399.5 MHz-2424.5 MHz	Channel 2	2404.5 MHz-2429.5 MHz	Channel 3	2409.5 MHz - 2434.5 MHz	Channel 4	2414.5 MHz - 2439.5 MHz	Channel 5	2419.5 MHz - 2444.5 MHz	Channel 6	2424.5 MHz - 2449.5 MHz	Channel 7	2429.5 MHz - 2454.5 MHz	Channel 8	2434.5 MHz - 2459.5 MHz	Channel 9	2439.5 MHz - 2464.5 MHz	Channel 10	2444.5 MHz - 2469.5 MHz	Channel 11	2449.5 MHz - 2474.5 MHz	Channel 12	2454.5 MHz - 2479.5 MHz	Channel 13	2459.5 MHz - 2484.5 MHz
Channel	Frequency																												
Channel 1	2399.5 MHz-2424.5 MHz																												
Channel 2	2404.5 MHz-2429.5 MHz																												
Channel 3	2409.5 MHz - 2434.5 MHz																												
Channel 4	2414.5 MHz - 2439.5 MHz																												
Channel 5	2419.5 MHz - 2444.5 MHz																												
Channel 6	2424.5 MHz - 2449.5 MHz																												
Channel 7	2429.5 MHz - 2454.5 MHz																												
Channel 8	2434.5 MHz - 2459.5 MHz																												
Channel 9	2439.5 MHz - 2464.5 MHz																												
Channel 10	2444.5 MHz - 2469.5 MHz																												
Channel 11	2449.5 MHz - 2474.5 MHz																												
Channel 12	2454.5 MHz - 2479.5 MHz																												
Channel 13	2459.5 MHz - 2484.5 MHz																												

## APPENDIX B

# Regulatory Information

## Electrical

### AC Adapter

The AC adapter is designed to ensure your personal safety and to be compatible with this equipment. Please follow these guidelines:

- Do not use the adapter in a high moisture environment. Never touch the adapter when your hands or feet are wet
- Allow adequate ventilation around the adapter. Avoid locations with restricted airflow
- Connect the adapter to a proper power source. The voltage and grounding requirements are found on the product case and/or packaging
- Do not use the adapter if the cord becomes damaged
- Do not attempt to service the adapter. There are no serviceable parts inside. Replace the unit if it is damaged or exposed to excess moisture

### Telecommunication Cord



To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

### Internal Telephone ports (VoIP)

Telecommunication equipment connected to this port (e.g., via “Voice 1 & 2” port) should be UL Listed and the connections shall be made in accordance with Article 800 of the NEC.

### Location – Electrical Considerations



Due to risk of electrical shock or damage, do not use this product near water, including a bathtub, wash bowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool. Also, avoid using this product during electrical storms. Avoid locations near electrical appliances or other devices that cause excessive voltage fluctuations or emit electrical noise (for example, air conditioners, neon signs, high-frequency or magnetic security devices, or electric motors).

## Equipment

### Repairs

Do not, under any circumstances, attempt any service, adjustments, or repairs on this equipment. Instead, contact your local 2Wire distributor or service provider for assistance. Failure to comply may void the product warranty.

### Location – Environmental Considerations

Do not plug the AC/DC power adapter into an outdoor outlet or operate the residential gateway outdoors. It is not waterproof or dustproof, and is for indoor use only. Any damage to the unit from exposure to rain or dust may void your warranty.

Do not use the residential gateway where there is high heat, dust, humidity, moisture, or caustic chemicals or oils. Keep the gateway away from direct sunlight and anything that radiates heat, such as a stove or a motor.

## Declaration of Conformity

### FCC / Industry Canada Compliance

This device has been tested and certified as compliant with the regulations and guidelines set forth in the Federal Communication commission - FCC part 15, FCC part 68 and Industry Canada - ICES003 and RSS-210 Radio and telecommunication regulatory requirements / Le présent matériel est conforme aux spécifications techniques applicables d'Industrie Canada. Cet appareil numérique de la classe [\*] est conforme à la norme NMB-003 du Canada.

Manufacturer: 2Wire, Inc.

Model(s): RG3801HGV-00

### Part 15 of FCC Rules

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

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help



Changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate this equipment.

### TIA 968 (Part 68 of FCC Rules) / IC CS-03

This equipment complies with the Telecommunication Industry Association TIA-968 (FCC part 68) and Industry Canada CS-03 Telecommunication requirements. On the product is a label that contains, among other information, the IC and FCC registration number and ringer equivalence number (REN) for this equipment. If requested, this information may be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in the device not ringing in response to an incoming call. In most, but not all areas, the sum of the RENs should not exceed five (5.0) / L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

To be certain of the number of devices that may be connected to the line, as determined by the total RENs, contact the telephone company to determine the maximum RENs for the calling area.

This product cannot be used on telephone-company-provided coin service. Connection to Party Line Service is subject to state tariffs.

An FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications to maintain uninterrupted service. If trouble is experienced with this equipment, please contact 2Wire, or your local 2Wire distributor or service center in the U.S.A. for repair and/or warrant information. If the trouble is causing harm to the telephone network, the telephone company may request you to remove this equipment from the network until the problem is resolved. No repairs can be done by a customer on this equipment. It is recommended that the customer install an AC surge arrester in the AC outlet to which this device is connected. This is to avoid damage to the equipment caused by local lightning strikes and other electrical surges.

### MPE/SAR/RF Exposure Information

This device was verified for RF exposure and found to comply with Council Recommendation 1999/519/EC and FCC OET-65 RF exposure requirements. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.



While this device is in operation, a separation distance of at least 20 cm (8 inches) must be maintained between the radiating antenna inside the EUT and the bodies of all persons

exposed to the transmitter in order to meet the FCC RF exposure guidelines. Making changes to the antenna or the device is not permitted. Doing so may result in the installed system exceeding RF exposure requirements. This device must not be co-located or operated in conjunction with any other antenna or radio transmitter. Installers and end users must follow the installation instructions provided in this guide.