

# iNID User Guide

Release 1.0

#### Notice to Users

©2008 2Wire, Inc. All rights reserved. This manual in whole or in part, may not be reproduced, translated, or reduced to any machinereadable 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 and the 2Wire logo are registered trademarks of 2Wire, Inc. in the United States and other jurisdictions throughout the world. All other names may be trademarks of their respective owners.

5100-000613-000 Rev B

## Contents

Introd	lucing	the	iNID	Sv	stem
				~,	

i38HG						1
iPSII	• •	•	• •	• •	• •	<u>,</u> T
i3802V	• •	•	•••	• •	• •	. 5 5
Sanica Providar Accass	• •	•	• •	• •	• •	. 5 5
Subscriber Access	• •	•	• •	• •	• •	. 5 5
	• •	•	• •	• •	• •	. J
Installing Your i38HG						
Determining Wireless Access Points Location						10
Avoiding Interference						10
Avoiding Obstructions					. :	10
Connecting the Data Cable						11
Connecting the Power Cable		_				12
Connecting Your Computer to the i38HG			• •	• •		12
Connecting via Ethernet Ports	• •	•	•••	•••	•	12
Connecting via Wireless	• •	•	•••	• •	•	13
Configuring non-2Wire Wireless Adapters	• •	•	•••	•••	•	13
	• •	•	• •	• •	•	10
Setting up System Information						
Meeting Web Browser Requirements						15
Navigating the User Interface					. :	16
Setting up Your Password					. :	18
Configuring Local Date and Time		•				21
Configuring Wireless Notwork						
Selecting the Wireless Access Daint						<b>റ</b> /
Selecting the Wireless Access Point	• •	•	•••	•••	•	24 25
	• •	•	• •	• •	• •	20
	• •	•	• •	• •	• •	20
Using the Encryption Key	• •	•	•••	•••	• •	20
Allowing Devices with MAC Address Filtering	• •	•	•••	•••	• •	28
	• •	•	•••	• •	• •	28
	• •	•	• •	• •	• •	30
Blocking Devices with MAC Address Filtering	• •	•	• •	• •	•	31
Blocking all Devices	• •	•	•••	•••	• •	32
Blocking Individual Devices	• •	•	• •	• •	•	34
Customize Private Wireless Settings	• •	•	• •	• •	• •	36
Configuring Wi-Fi Protected Setup	• •	•	•••	•••	• •	37
Configuring Firewall						
Hosting an Application						40
Removing Unsted Applications	• •	•	• •	• •	•	12
Defining a New Application Profile	• •	•	• •	• •	•	72 // 2
Adding Multiple Definitions to a Profile	• •	•	• •	• •	• •	43 47
	• •	•	• •	• •	• 1	+1 50
Allowing all Applications (DMZplus)	• •	•	•••	• •	•	50
Anowing an Applications (Divizpius)	• •	•	• •	• •	• •	5∠ ⊑≉
	• •	•	•••	•••	• •	94 55
	• •	•	• •	•••	•	35

#### Working with the Power Supply Unit

Replacing the Battery	60
Enabling the Alert	63
Disabling the Alert	65

## **Configuring VoIP Services**

#### **Configuring LAN Devices**

Configuring your LAN Publicly Routed Subnet	70
Configuring DHCP	72
Allocating IP Addresses	75

## **Finding Solutions**

Viewing Statistics	34
Viewing the Wireless AP Statistics	36
Viewing the HPNA Coax Statistics	36
Viewing the HPNA Phone Line Statistics	37
Viewing Individual DSL and Aggregate Bandwidth	38
Viewing the VoIP Service Status	39
Viewing Logs	<b>)</b> 1
Viewing Events Logs	<i>)</i> 1
Viewing System Logs	<i>)</i> 3
Viewing Firewall Logs	96
Viewing Upgrade Logs	98

## **Regulatory Information**

## Introducing the iNID System

The Intelligent Network Device (iNID) system comprises three components: i38HG (inside unit), iPSU (power supply unit), and i3802V (outside unit). These components are dependent on each other and do not have standalone functions. Using these components together provide triple-play service (voice, data, and video) to your home.

## i38HG

The i38HG is the unit that goes inside your home and can be installed by you or your service provider. Working together with the i3802V, the i38HG is a home networking hub that provides an 802.11b/g Wi-Fi access point and Ethernet switch functions for connecting personal computers and other in-home networked devices to the service provider's network. The i38HG has four Ethernet ports for directly connecting computers or devices.

The i38HG includes an integrated wireless access point that allows you to roam wirelessly throughout the home or office. 2Wire high-powered wireless technology virtually eliminates wireless "coldspots" in the home. The i38HG high-power 400mW transmitter ensures that you benefit from increased wireless bandwidth throughout the coverage area. In addition, the i38HG employs a special triple antenna design. The third antenna is used only for transmitting packets, thus mitigating the power loss associated with switching the antenna use back and forth between transmit and receive. This results in greater access point sensitivity, as antenna placement can be better optimized with a dedicated set of receive-only antennas.

To expand the wireless coverage in a home or add additional Ethernet ports in different locations in the home, you can connect up to eight i38HG devices to different in-home phone outlets. Each i38HG is automatically configured to operate on the same wireless network, and can be centrally configured and managed at *http://gateway.2wire.net*.



**Note:** Contact your service provider for information to implement multiple i38HG devices.

Figure 1 shows the i38HG indicators and Table 1 describes their functions.



Figure 1: i38HG Indicators

## Table 1: i38HG Indicators Description

Indicators	Description
POWER	The <b>POWER</b> indicator turns red when the power is first applied, and changes to green within two minutes of power application.
	Constant green indicates that power is on.
	Red indicates that a Power-On Self-Test (POST) failure (unbootable) or another malfunction (for example, alarm) has occurred.
ETHERNET	<ul> <li>Solid green indicates that a device (such as a computer) is connected to an ETHERNET port.</li> </ul>
	• Flickering green indicates that inbound activity from devices is associated with the Ethernet port. The flickering of the light is synchronized to the actual data traffic.
WIRELESS	<ul> <li>Solid green indicates that there is wireless activity associated to a specific access point.</li> </ul>
	<ul> <li>Flickering green indicates that there is inbound activity. The flickering of the light is synchronized to the actual data traffic.</li> </ul>
LINE 1 and LINE 2	<ul> <li>Solid green indicates that the associated VoIP line has been registered with a SIP proxy server.</li> </ul>
	<ul> <li>Flashing green indicates that a telephone is off-hook on the associated VoIP line.</li> </ul>
NID	Solid green indicates that the link between the i38HG and i3802V is healthy.

2

#### Table 1: i38HG Indicators Description (Continued)

Indicators	Description
BROADBAND	This indicator shows the i3802V VDSL status.
	<ul> <li>Constant green indicates successful broadband connection and no interruption in Internet access.</li> </ul>
	<ul> <li>Flashing green indicates that the i3802 is attempting to establish a broadband connection.</li> </ul>
	<ul> <li>Flashing green and red indicate that the broadband connection has failed to establish for three consecutive minutes.</li> </ul>
	<ul> <li>Red indicates that there is no DSL signal.</li> </ul>
SERVICE	<ul> <li>Constant green indicates that the i3802V has a WAN IP address from DHCP and the broadband connection is up.</li> </ul>
	Flashing green indicates that the i3802V is attempting to be authenticated.
	<ul> <li>Red indicates that the i38HG has failed to receive an IP address assignment from the network.</li> </ul>

#### iPSU



**Caution:** To reduce the risk of fire, use 26 AWG or larger telecommunication line wire for the power supply connection.

The Power Supply Unit (iPSU) supplies power to the i3802V and is installed by your service provider. The iPSU optimum operating temperature is between  $-5^{\circ}$  C to  $+50^{\circ}$  C, ambient (23.0° F to 122° F). Unlike the i3802V, the iPSU must be installed in a sheltered area — either inside the garage or home. If the iPSU is equipped with a backup battery, during a temporary AC power outage, the power source is switched to the battery without interruption of the voice-over-IP service. When the AC power is restored, the power source is switched back to the AC power supply. The switchover between the AC power supply and the battery is automatic and instantaneous.

The iPSU itself requires no regular maintenance; however, the battery inside the iPSU requires periodic replacement. Refer to the Working with the Power Supply Unit section for instructions to replace the backup battery. Figure 2 shows the location of the two indicators and two buttons on the power supply unit; Table 2 lists and describes their functions.



Figure 2: iPSU Indicators and Buttons Location



**Note:** The battery provides power for voice over IP services during a power outage. You are responsible to monitor and replace the battery when needed. Your service provide does not monitor the battery and is not responsible for its replacement.

#### Table 2: Power Supply Unit Indicators and Buttons

Indicators and Buttons	Description
Reset — Button	A <b>Reset</b> button is located on the upper left side panel, identifiable by a surrounding red circle. When pressed for up to 9 seconds, the <b>Reset</b> button reboots the outside unit. If the button is pressed for 10 or more seconds, it resets the outside unit to the factory default settings.
	<b>Note:</b> Do not press the <b>Reset</b> button unless you are instructed to do so. Doing so may reset the outside unit to the factory default settings – that means you will lose your personal settings.
POWER	Solid green indicates that the power supply is running on AC power.
	<ul> <li>Off indicates that the power supply is not receiving power from either AC or the battery.</li> </ul>
	<ul> <li>Flashing red indicates that the power is provided by the backup battery or that the outside unit is not yet communicating with the iPSU.</li> </ul>
SILENCE ALARM —	The SILENCE ALARM button is located between POWER and BATTERY indicators.
Button	<ul> <li>If AC power is interrupted for any reasons, a continuous tone indicates that the power supply is running on the backup battery. Pressing the SILENCE ALARM button within 15 seconds immediately silences the audio alert. (The tone stops automatically after 15 seconds.)</li> </ul>
	• When the battery needs replacing, a chirp sounds intermittently unless you press the button to silence it for 12 hours. The chirp resumes after 12 hours if the battery is not replaced.
BATTERY	Solid green indicates that the battery is installed and functioning properly.
	Off indicates that no battery is installed.
	Flashing red indicates that the battery needs to be replaced.
	<b>Note:</b> The <b>BATTERY</b> indicator works properly only when the i38HG is connected to and communicates with the i3802V.

## i3802V

The i3802V is the gateway that acts as the network interface device. It is installed by your service provider on the outside of your home. The i3802V includes a broadband interface and high-speed coaxial and phone line network capabilities to deliver data service to the home. The i3802V has two accessible areas: one for service provider personnel and the other for subscribers.

#### **Service Provider Access**

The service provider access area is locked and can be opened only by the service provider personnel. The i3802V has two cable entries providing wiring from the service provider and to inside your home. The left entry provides cable connection from the service provider to the i3802V. The right entry provides wiring that feeds the inside of your home and power connection for the power supply unit.

#### **Subscriber Access**

As the name implies, the subscriber area is accessible by you. This panel displays indicators that show the i3802V operational status. Some indicators on the i3802V have the same functions as those on the i38HG, where you can view the status inside your home. Figure 3 shows the indicators location and Table 3 describes their status. The subscriber area is fastened with a screw that you can unfasten with any flat-blade screwdriver. To prevent any unauthorized access, you can also lock it with any common household locking devices (such as padlocks or a combination lock).



**Figure 3: iNID Indicators Location** 

Table 3: i3802V	<b>Outside Unit</b>	Indicators	Status
-----------------	---------------------	------------	--------

Indicators	Description
POWER	The <b>POWER</b> indicator turns red when the power is first applied, and changes to green within two minutes of power application.
	<ul> <li>Constant green indicates that power is on and initialization has been completed successfully.</li> </ul>
	<ul> <li>Flashing green indicates that the iNID is booting.</li> </ul>
	• Red indicates that a Power-On Self-Test (POST) failure (unbootable) or another malfunction (for example, alarm) has occurred during self initialization.
VDSL 1 and VDSL 2	These two indicators flash after 60 seconds of power application for 1 to 2 minutes and cycle three times.
	Solid green indicates that the broadband connection is trained.
	<ul> <li>Flashing green indicates that the broadband connection is being attempted (DSL attempting to synchronize).</li> </ul>
	• Alternating flashing green and steady red indicate that the broadband connection fails to establish for more than three consecutive minutes. This pattern continues until the broadband connection is successfully established.
	Flashing red indicates that there is no DSL signal on the line.
	<b>Note:</b> The <b>BROADBAND</b> indicator on the i38HG mirrors one or both of the VDSL indicators, whichever is in the "best" state.
DATA	Solid green indicates that an IU (i38HG) is connected via HPNA.
	<ul> <li>Flashing green indicates that the iNID is attempting IEEE 802.1b/g authentication or attempting to obtain DHCP information.</li> </ul>
	Red indicates that the iNID failed to be IP connected (no DHCP response, and so forth).
	Note: This indicator is the mirrored SERVICE indicator on the i38HG.
COAX	Solid green indicates that a device is connected (such as a Set Top Box).
	• Flickering green indicates that there is inbound activity associated with the COAX port. The flickering of the light is synchronized to the actual data traffic.
	<ul> <li>Red indicates that a device failed to be authenticated or successfully connected.</li> </ul>
LINE 1 and LINE 2	Solid green indicates that the associated VoIP line has been registered with the network and ready for use.
	<ul> <li>Flashing green indicates that a telephone is in use on the associated VoIP line.</li> </ul>
	<b>Note:</b> These two indicators are mirrored <b>LINE 1</b> and <b>LINE 2</b> indicators on the i38HG.

#### Table 3: i3802V Outside Unit Indicators Status (Continued)

Indicators	Description
ETHERNET	<ul> <li>Solid green indicates that a device (such as a computer) is connected to the ETHERNET port.</li> </ul>
	<ul> <li>Flickering green indicates there is inbound activity from devices connected to the Ethernet port. The flickering of the light is synchronized to the actual data traffic.</li> </ul>
BATTERY	Solid green indicates that the AC power is connected and healthy.
	Flashing red indicates that the backup battery is used for power.



**Note:** Call your service provider if any i3802V indicators signify failures. Do not attempt to repair the i3802V as the unit must be serviced by your provider.

iNID User Guide

## Installing Your i38HG

Before installing the i38HG, review the package content and ensure that you have available the items shown in Figure 4.



Figure 4: i38HG Package Content



**Note:** The i38HG and the stand are packaged separately in the container. You should place the i38HG on the stand.

This section provides instructions to connect the following cables and information on these topics:

- Determine a wireless location on page 10
- Connect the data cable on page 11
- Connect the power cable on page 12
- Connect your computer to the i38HG on page 12
- Configure non-2Wire wireless adapter on page 12

## **Determining Wireless Access Points Location**

You can install additional i38HG to improve wireless coverage. The wireless signals are affected by many items in common households. Reliability and performance are the major considerations when planning your wireless network location.

#### **Avoiding Interference**

Wireless signals are subject to interference from other electronic devices including (but not limited to) microwave ovens, cordless telephones, and garage door openers. Proper installation will minimize interference. Place your i38HG at least 5 feet from cordless phones, microwaves, or other electronic devices to avoid potential interference, and more than 6 inches away from television to avoid audio hissing or static.



**Note:** Whenever possible, use the stand provided with the i38HG and install it in the vertical position. If that is not possible, be sure that it is installed in a manner that nothing can be stacked on the top of it. The i38HG generates substantial amounts of heat and could possibly damage something that is stacked on it.

#### **Avoiding Obstructions**

The wireless signal degrades with distance and obstructions (such as ceilings, walls, and furniture). Consider the layout of your home or business when deciding where to place your i38HG.

- Consider where you will use your wireless devices when placing your i38HG. In a single-story building, place the i38HG as high and as close to each wireless computer as possible. To minimize interference, do not place the i38HG behind large objects or other obstructions.
- Place the i38HG in an open area where wireless range will not be directly affected by surroundings. Wireless signal strength will be much stronger in an open area as opposed to an area with obstructions.
- Keep the number of walls and ceilings between your i38HG and other devices on your network to a minimum because the i38HG wireless signal can usually go through one or two walls before it loses connectivity.
- Keep the i38HG away from any large metal objects. Because metal objects can reflect or obstruct signals, wireless signal quality and speed may be adversely impacted.
- Place the i38HG near a window if you want to access the network outside of your home or business.

## **Connecting the Data Cable**

The data cable carries data from the i3802V to the i38HG.



#### Figure 5: Power and Data Cables Connection

- **1.** Connect one end of the data cable (green) to the line 1 outlet (Figure 5).
- 2. Connect the other end of the data cable to the DATA port (green) of your i38HG.
- **3.** Observe **NID**, **BROADBAND**, and **SERVICE** indicators, they light green when the communication is established between the i38HG and i3802V (within 1 minute).



**Note:** Refer to the Finding Solutions section if the indicator does not stay green.

## **Connecting the Power Cable**

- 1. Connect one end of the power supply cable to the **POWER** port of your i38HG (Figure 4).
- 2. Connect the other end of power supply cable to a 3-prong AC electrical outlet.



**Note:** For safety reasons, do not modify electrical outlets that do not have a 3-prong plug with a 3-prong adapter.

3. Observe the **POWER** indicator; it flashes red once, followed by flashing green, then remains solid green.



**Note:** Refer to the Finding Solutions section if the indicator does not stay green.

## **Connecting Your Computer to the i38HG**

There are two ways to connect your computer to the i38HG: via Ethernet or wireless. With either connection, the first computer you connect to the network is used to configure the i38HG for proper operation.

#### **Connecting via Ethernet Ports**

You can directly connect up to four computers to the i38HG using the Ethernet connection. Connect one end of the Ethernet cable (yellow) to any available ETHERNET port (yellow) on the i38HG and the other end to the computer's Ethernet port (Figure 6).

You are now ready to start your system (refer to the Setting up System Information section).

**Note:** Your i38HG is shipped with an 6-foot Ethernet cable. Use a CAT5 cable



**Figure 6: Ethernet Connection** 

#### **Connecting via Wireless**

Your i38HG has an integrated wireless access point (AP) that enables you to connect your wireless-enabled computers to your home network. By default, the i38HG is shipped with WPA-PSK enabled and a preconfigured network name. Refer to the Configuring Wireless Network section to configure your wireless network.

You can connect up to eight i38HGs (that is, APs) in your home. When multiple APs are detected, they are automatically synchronized across all managed access points to create a single wireless network for easier device connectivity. The default service set identifier (SSID) and wireless key is based on the last three digits of the serial number on the first access point that was connected. If you have multiple APs installed, refer to the label on your first installed AP only. All subsequent access points are automatically synchronized with the default SSID or with any custom SSID you define subsequent to initial installation.

Most laptop computers 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. The 2Wire wireless adapter provides a 2Wire Setup Wizard that automatically configures it to communicate with the i38HG during setup. If you are using a non-2Wire wireless adapter, you must manually configure it to communicate with the i38HG. Refer to the Configuring non-2Wire Wireless Adapters section to install a wireless network adapter.

## **Configuring non-2Wire Wireless Adapters**

If you are using a non-2Wire wireless adapter, you must manually configure it to communicate with the i38HG. This section provides instructions to configure your adapter with WPA. You can use WEP if your wireless adapter does not support WPA; however, this decreases the level of security provided for wireless traffic.

- **1.** Install and configure your wireless adapter according to the manufacturer's instructions.
- **2.** Use the network adapter configuration software or Windows network connection wizard to set the network name (SSID) and encryption key (WPA).
- **3.** Enter **2WIRE** (in capital letters) as the network name, followed by the last three digits of the i38HG serial number (for example, 2WIRE110), located on the bottom of your i38HG (Figure 7).



**Note:** If you have multiple APs, use the last three digits of the first i38HG connected to the network.



Figure 7: Wireless Network Name and Encryption Key Location

**4.** Enter the encryption key that is located inside the brackets beneath the bar code on the bottom of your i38HG, (for example, 4119627022).



**Note:** For Mac OS X users, you may need to enter the "\$" character at the beginning of the encryption key (for example, \$4119627022).

## Setting up System Information

After the i38HG is properly connected and the first time you access the i3802V user interface, it is a good idea to set up the basic system information, such as password, date and time, and so forth. This section provides instructions to change the following information:

- Password on page 18
- Date and time page 21

## **Meeting Web Browser Requirements**

- Microsoft Internet Explorer 6.0 or higher
- Firefox 1.5 or higher
- Safari 2.0

## **Navigating the User Interface**

Figure 8 shows the page when you enter *http://gateway.2Wire.net* as the URL into a compatible browser on a computer connected to the i38HG or i3802V (refer to Meeting Web Browser Requirements on page 15). This page contains 5 panes. The following section describes each pane that is indicated by the numbered red arrow.



Figure 8: i3802V User Interface

- **1.** The *tab* pane of the user interface contains the following four tabs that are arranged horizontally. Clicking any of these tabs displays a page that enables you to access associated information.
  - 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 (Figure 8).
  - Services: The Services tab provides links to view your voice line status.
  - Settings: The Settings tab provides the most comprehensive system information. Clicking this tab
    opens a page that provides sub-tabs to access other pages to configure your i38HG and view
    system status.
  - Site Map: The Site Map tab provides a textual view of the user interface. Clicking any links on this
    page takes you directly to the page of interest.
- **2.** The *Summary* pane displays the status of each service. Except the fourth icon, i3802V, you can click other icons to directly access more information.
- 3. This pane displays the backup battery status. You can click <u>Battery Info</u> to directly access the page.



**Notes:** The backup battery status is displayed only if your iPSU is equipped with one.

It is recommended to have a backup battery if you subscribe to voice-over-IP services and is required to maintain voice-over-IP service during a power outage.

- **4.** The *Home Network Devices* pane displays all devices that are connected to the i38HG. You can click the links to view the detailed information of the connected devices.
- **5.** The *Top Networking Features* pane provides shortcuts to directly access the most commonly used pages.

## **Setting up Your Password**

The default system password is automatically set five minutes after the iPSU is connected. You can find the default system password on the iPSU front cover.

Setting a system password protects your i3802V settings from being modified or changed by someone who has not been given permission to do so. After setting a system password, you will be required to enter it whenever you attempt to access a configuration page (for example, when you try to change the broadband connection settings).

To set up a password:

**1.** Enter *http://gateway.2Wire.net* as the URL; the *Home* page opens.

Iome	Servio	es Set	tings	Site Map			
Summa	ary						
	Broadt	oand 2Kbps Kbps	Wire Netwo Name Doris	less <sub>ork</sub>	Firewall Status Enabled	4	<b>i3802V</b> Serial Number: 450712000169
	ig - Liii	ergency D	attery De	аскир			
Battery P Home 1	ower Leve Networ	l Critical <u>Batt</u> k Devices	tery Info	екир			
Battery P Home 1	ower Leve Networ 168.1.64	l Critical <u>Batt</u> k Devices	Device Det	tails			
Battery P Home 1 & 192. & DLo	ower Leve Networ 168.1.64	I Critical <u>Batt</u> k Devices Access Files	Device Det	tails			
Battery P Home 2 8 192 8 DLo 8 Dori	ower Leve Networ 168.1.64 k sL	l Critical <u>Batt</u> k Devices <u>Access Files</u> <u>Access Files</u>	Device Det	tails tails			
Battery P Home 2 I 192. I 192. DLo I Dori Top Ne	ower Leve Networ 168.1.64 k sL	I Critical <u>Batt</u> k Devices <u>Access Files</u> ng Feature	Device Det Device Det Device Det	tails tails tails			
Battery P Home J S 192. DLo Dori Top Ne Wireless	ower Leve Networ! 168.1.64 k sL	I Critical <u>Batt</u> k Devices <u>Access Files</u> ag Feature	Device Det Device Det Device Det Device Det Device Det Device Det Device Det Device Det Device Det Device Det	tails tails tails	tings		
Battery P Home 1 S 192. DLo Dori Top Ne <u>Wireless</u> Refresh v	ower Leve Networ 168.1.64 k sL tworkin	I Critical <u>Batt</u> k Devices <u>Access Files</u> A <u>ccess Files</u> ng Feature	Device Det Device Det Device Det Device Det Device Det Device Det Device Det Device Det Device Det	tails tails tails lify security or set	tings aand connection		
Battery P Home 1 Solution 192. Solution 192.	Networ Networ 168.1.64 k sL tworkin <u>rour Broad</u>	I Critical <u>Batt</u> k Devices <u>Access Files</u> A <u>ccess Files</u> ng Feature <u>band Connec</u> n	Device Det Device Det Device Det Device Det Device Det Device Det Device Det Control Device Det Device Device Det Device Device Devi	tails tails tails lify security or set nnnect your broadl oot	tings and connection		
Battery P Home 1 S 192. Doo Doo Top Ne Refresh Refresh Restart y	Networ! Networ! 168.1.64 k sL vtworkin vour Broad our System etworking	I Critical <u>Batt</u> k Devices <u>Access Files</u> A <u>ccess Files</u> ng Feature <u>band Connec</u> n	Device Det Device Det Device Det Device Det SS - mod tion - reco - rebo - find	tails tails tails lify security or set innect your broadl yot a computer, shar	tings and connection		

2. Click <u>Settings</u> or <u>System Password</u> from the *Top Networking Features* pane; the Settings page opens displaying the system information and more sub-tabs.

Home Services Settings Site Map   System Info Broadband LAN Firewall Logs Diagnostics  Status Password Date & Time Event Notifications Battery Backup  System Information   Manufacturer: 2Wire, Inc.   Model: 13802V   Serial Number: 450712000169   Hardware Version: 2700-100661-002   Software Version: 6.1.3.21-enh.tm   Key Code: 52HP-2374-2262-22AT-F2BQ   First Use Date: Not Set   Current Date & Time: Not Set   Time Since Last Boot: 0 day 1.08:08   DSL Modem 2.66.7 SW:68.14_4.10.1   System Password: Custom   Wireless Access Point   Manufacturer: 2Wire, Inc.   Manufacture: 2Wi	&T U-verse		2WiRE'
System Info Broadband LAN Firewall Logs Diagnostics     Status Password Date & Time Event Notifications Battery Backup    System Information   Manufacturer: 2Wire, Inc.   Model: 13802V   Serial Number: 450712000169   Hardware Version: 2700-100661-002   Software Version: 6.1.3.21-enh.tm   Key Code: 52HP-2374-2262-22AT-F2BQ   First Use Date: Not Set   Time Since Last Bool: 0 day 1:08.08   DSL Modem 2.66.7 SW:68.14_4.10.1   System Password: Custom    Wireless Access Point   Manufacturer: 2Wire, Inc.   Manufacturer: 2Wire, Inc.   Model: 138HG   Serial Number: 390713000392   Hardware Version: 2.700-000679-003   Software Version: 6.1.3.14-eval-wiffitm   Enabled: Yes	Iome Services	Settings Site Map	
Status       Password       Date & Time       Event Notifications         Baseword       System Information         Manufacturer:       2Wire, Inc.         Model:       13802V         Serial Number:       450712000169         Hardware Version:       2700-100661-002         Software Version:       6.1.3.21-enh.tm         Key Code:       52HP-2374-2262-22AT-F2BQ         First Use Date:       Not Set         Current Date & Time:       Not Set         DSL Modem       2.66.7 SW:68.14_4.10.1         System Password:       Custom         Wireless Access Point       Manufacturer:         Manufacturer:       2Wire, Inc.         Model:       138HG         Serial Number:       390713000392         Hardware Version:       2.13.14-eval-wifi.tm         Enabled:       Yes	System Info Broad	lband LAN Firewall Logs Diagr	nostics
System InformationManufacturer:2Wire, Inc.Model:13802VSerial Number:450712000169Hardware Version:2700-100661-002Software Version:6.1.3.21-enh.tmKey Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access PointManufacturer:2Wire, Inc.Model:138HGSerial Number:390713000392Hardware Version:2700-000679-003Software Version:6.1.3.14-eval-wifi.tmEnabled:Yes	Status Password	Date & Time Event Notifications Battery Back	kup 🧹
System Information Manufacturer: 2Wire, Inc. Model: 13802V Serial Number: 450712000169 Hardware Version: 2700-100661-002 Software Version: 6.1.3.21-enh.tm Key Code: 52HP-2374-2262-22AT-F2BQ First Use Date: Not Set Current Date & Time: Not Set Time Since Last Boot: 0 day 1:08:08 DSL Modem 2.66.7 SW:68.14_4.10.1 System Password: Custom Wireless Access Point Wireless Access Point Manufacturer: 2Wire, Inc. Model: 138HG Serial Number: 390713000392 Hardware Version: 2700-000679-003 Software Version: 5.1.3.14-eval-wifi.tm Enabled: Yes			
Manufacturer:2Wire, Inc.Model:13802VSerial Number:450712000169Hardware Version:2700-100661-002Software Version:6.1.3.21-enh.tmKey Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetCurrent Date & Time:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access PointWire, Inc.Manufacturer:2Wire, Inc.Manufacturer:390713000392Hardware Version:2700-000679-003Software Version:6.1.3.14-eval-wifi.tmEnabled:Yes	System Informat	ion	
Model:13802VSerial Number:450712000169Hardware Version:2700-100661-002Software Version:6.1.3.21-enh.tmKey Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetCurrent Date & Time:Not SetCurrent Date & Time:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access Point	Manufacturer:	2Wire, Inc.	
Serial Number:450712000169Hardware Version:2700-100661-002Software Version:6.1.3.21-enh.tmKey Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetCurrent Date & Time:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access Point2Wire, Inc.Manufacturer:2Wire, Inc.Manufacturer:390713000392Hardware Version:2700-000679-003Software Version:5.1.3.14-eval-wifi.tmEnabled:Yes	Model:	i3802V	
Hardware Version:2700-100661-002Software Version:6.1.3.21-enh.tmKey Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetCurrent Date & Time:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access Point	Serial Number:	450712000169	
Software Version:6.1.3.21-enh.tmKey Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetCurrent Date & Time:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access PointCustomManufacturer:2Wire, Inc.Madel:138HGSerial Number:390713000392Hardware Version:2700-000679-003Software Version:6.1.3.14-eval-wifi.tmEnabled:Yes	Hardware Version:	2700-100661-002	
Key Code:52HP-2374-2262-22AT-F2BQFirst Use Date:Not SetCurrent Date & Time:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2.66.7 SW:68.14_4.10.1System Password:CustomWireless Access PointCustomManufacturer:2Wire, Inc.Model:138HGSerial Number:390713000392Hardware Version:2700-000679-003Software Version:6.1.3.14-eval-wifi.tmEnabled:Yes	Software Version:	6.1.3.21-enh.tm	
First Use Date:Not SetCurrent Date & Time:Not SetTime Since Last Boot:0 day 1:08:08DSL Modem2:66.7 SW:68.14_4.10.1System Password:CustomWireless Access PointCustomManufacturer:2Wire, Inc.Model:138HGSerial Number:390713000392Hardware Version:2700-000679-003Software Version:6.1.3.14-eval-wifi.tmEnabled:Yes	Key Code:	52HP-2374-2262-22AT-F2BQ	
Current Date & Time: Not Set Time Since Last Boot: 0 day 1:08:08 DSL Modem 2:66.7 SW:68.14_4.10.1 System Password: Custom Wireless Access Point Manufacturer: 2Wire, Inc. Model: 138HG Serial Number: 390713000392 Hardware Version: 2700-000679-003 Software Version: 6.1.3.14-eval-wifi.tm Enabled: Yes	First Use Date:	Not Set	
Time Since Last Boot:       0 day 1:08:08         DSL Modem       2:66.7 SW:68.14_4.10.1         System Password:       Custom         Wireless Access Point       Custom         Manufacturer:       2Wire, Inc.         Model:       138HG         Serial Number:       390713000392         Hardware Version:       2700-000679-003         Software Version:       6.1.3.14-eval-wifi.tm         Enabled:       Yes	Current Date & Tim	e: Not Set	
DSL Modem 2.66.7 SW:68.14_4.10.1 System Password: Custom Wireless Access Point Manufacturer: 2Wire, Inc. Model: 138HG Serial Number: 390713000392 Hardware Version: 2700-000679-003 Software Version: 6.1.3.14-eval-wifi.tm Enabled: Yes	Time Since Last Bo	ot: 0 day 1:08:08	
System Password: Custom Wireless Access Point Manufacturer: 2Wire, Inc. Model: 138HG Serial Number: 390713000392 Hardware Version: 2700-000679-003 Software Version: 6.1.3.14-eval-wifi.tm Enabled: Yes	DSL Modem	2.66.7 SW:68.14_4.10.1	
Wireless Access Point         Manufacturer:       2Wire, Inc.         Model:       138HG         Serial Number:       390713000392         Hardware Version:       2700-000679-003         Software Version:       6.1.3.14-eval-wifi.tm         Enabled:       Yes	System Password:	Custom	
Model:         138HG           Serial Number:         390713000392           Hardware Version:         2700-000679-003           Software Version:         6.1.3.14-eval-wifi.tm           Enabled:         Yes	Wireless Access	Point	
Serial Number:         390713000392           Hardware Version:         2700-000679-003           Software Version:         6.1.3.14-eval-wifi.tm           Enabled:         Yes	Model	138HG	
Hardware Version:     2700-000679-003       Software Version:     6.1.3.14-eval-wifi.tm       Enabled:     Yes	Serial Number:	390713000392	
Software Version:     6.1.3.14-eval-wifi.tm       Enabled:     Yes	Hardware Version:	2700-000679-003	
Enabled: Yes	Software Version:	6.1.3.14-eval-wifi.tm	
	Enabled:	Yes	
	System Software	Components	



**Note:** The above page is for reference only and is not fully displayed here.

3. Click <u>Password</u>; the Administration Password page opens.

ome S	ervices	Setting	s Site	Мар	
ystem Info	Broadba	ind LAN	Firewall	Logs	Diagnostics
Status Pa	ssword Da	te & Time	Event Notific	ations Ba	ttery Backup
Administr	ation Pas	ssword			
Enter Curre	nt Passwoi	rd:			
Select Pass	word:	O Use	Default Syste	em passwo	rd (printed on the front cover of the power supp
		<ul> <li>Creation</li> </ul>	ate or Edit a C	Custom Pas	sword:
		Ente	er New Passw	ord:	
		Con	firm New Pas	sword:	
		Ente	er a Password	Hint:	
		Not also a w forg	e: When you o set up a pas ord, phrase, o jet it.	choose to p sword hint or question	assword protect the system settings, you shoul in case you forget your password. This hint can that will help you remember your password if yo
		-			
			k		
					a waw
				2WIRI	2
				en ter	
		/	4		
	ŕ		/		
		POWER SUPPLY AND	BATTERY BACKUP	CAUTION! PRICE TO WIRING CHAN	IES UNPLUG FROM WILL AND DISCONNECT BACKUP BATTERY.
	$\bullet \rightarrow$	Advanced Config http://192.168.1.254     System Password: X0	00000000000 III	ATTENTION! This device may include a scover failure. This device replace a worn out battery scor for battery replacement	Sachup Natilary to provide voice service in the event of a commercial will ware the user when the hattary reveals to be replaced. Failure to may last to a loss of vices service during power outages. See inside details.
			Serial Nur	nber 🔵 De	fault Password

- **4.** Select the password option:
  - When Use Default System password is selected, no further action is required, go to Step 7.
  - When Create or Edit a Custom Password is selected, continue with the next step.



**Note:** The default system password is printed on the iPSU front cover.

5. Enter the new password in the Enter New Password field.



**Note:** The password is case-sensitive and can contain a maximum of 31 alpha-numeric characters with no spaces.

**6.** Confirm the new password in the appropriate field.



**Note:** Although it is optional, it is strongly recommended that you enter a password hint to remind you if you forget your password.

-wire

7. Click Save; your password is displayed on the System Information page.

#### AT&T U-verse

Home	Services	Settings Site Map	
System In	fo Broadba	nd LAN Firewall Log	gs Diagnostics
<u>Status</u>	Password Dat	e & Time Event Notifications	Battery Backup
Manufac	turor.	2Wire Inc	
Model:	curer.	i3802V	
Serial Nu	umber:	450712000169	
Hardwar	e Version:	2700-100661-002	
Software	Version:	6.1.3.21-enh.tm	
Key Code	e:	52HP-2374-2262-22AT-F2B	2
First Use	e Date:	April 8, 2008	
Current	Date & Time:	Tuesday, April 8, 2008	
		3:12:15 PM	
		Pacific Daylight Time	
Time Sin	ice Last Boot:	0 day 0:22:07	
DSL Mod	lem	2.66.7 SW:68.14_4.10.1	
System F	Password:	Custom	<
Wireless	s Access Poi	nt	

## **Configuring Local Date and Time**

You do not need to adjust the local date and time as they are set nightly by the service provider.

iNID User Guide

## **Configuring Wireless Network**

When the i38HG is properly installed, the wireless network is functional. Your i38HG is preconfigured with settings that optimize wireless performance. It is recommended that you leave the default settings in place.

If you are knowledgeable with the wireless technology and want to modify the settings, this section provides instructions to perform the following advanced configurations:

- Select the wireless access point on page 24
- Set up your wireless network name on page 25
- Secure your wireless network on page 26
- Customize personal wireless settings on page 36
- Configuring Wi-Fi Protection Setup on page 37

## **Selecting the Wireless Access Point**

You can have up to eight access points (APs) in your home and each access point is automatically synchronized. When multiple APs are detected, they are automatically displayed on the *Wireless Access Point List and Unique Settings* page. Settings are synchronized across the managed APs to create a single wireless network for easier device connectivity.

To select the access point:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click on the Home page; the Wireless Access Point List and Unique Settings page opens.

T&T U-verse		ewire:
Home Services	Settings Site Map	
System Info Broadband	LAN Firewall Logs Diagnostic	s
Status <mark>Wireless</mark> Wired	Interfaces DHCP IP Address Allocation Stati	stics
Warning Modifyin network.	g the settings on this page can impact the ability	y of devices to access your wireless
Wireless Access	Point List and Unique Setting	[S
The system supports multip synchronized to assist in im been detected by the system are unique to each access pu to create a single wireless n	le 2Wire provided Wireless Access Point devices t proving your wireless coverage. If a compatible 2 1, it will automatically be shown in the list below sint. Other settings (e.g. Network and Security) ar etwork for easier connectivity.	to be connected and automatically 2Wire provided access point has with the associated settings that re shared across these access points
Wireless Access Point	Enabled V AP S/N 390713000392	If you have multip
Channel:	Auto 👻	APs, the list
Power:	400 mW 💌	appears here.
Rescan		
Wireless Networ	k Shared Settings	
Network		
Network Name (SSID):	Doris	Set up your wirele
SSID Broadcast:	☑ Default: Enabled	network SSID.
Security		
Wireless Security:	Default: Enabled	Secure your
Authentication Type:	WPA-PSK and WPA2-PSK 💌	wireless network
Wireless Key	O Use default encryption key printed on the S	ystem Label:

Figure 9: Wireless Access Point List and Unique Settings Page

3. Click the **Enable** checkbox next to the access point you want to enable.



**Note:** If you have only one access point, that access point is enabled by default.

4. Select the channel (radio frequency band) the access point uses for your wireless network.



**Note:** It is best to select *Auto* because a channel is automatically selected to minimize interference.

- **5.** Select the power level for your wireless connection from the **Power** drop-down list. The default is 400 mW.
- 6. Click Save.

#### **Setting up the Wireless Network Name**

If you are in a densely populated area, or if you regularly connect to more than one wireless network (such as one at work and one at home), it is good practice to give your wireless network a unique name, which makes it easy to identify when you select the wireless network to which to connect. The default is 2WIREXXX, where XXX represents the last three digits of the serial number on the first access point that was connected (for example, 2WIRE954).

- 1. Open a Web browser and enter http://gateway.2Wire.net to access the 2Wire i3802V user interface.
- 2. Click ron the Home page; the Wireless Access Point List and Unique Settings page opens (Figure 9).
- 3. Enter a name assigned to your wireless network in the Network Name (SSID) field.

This name appears next to n on the Home page.

**4.** Enable or disable the broadcast of the SSID over the wireless network by selecting or deselecting the checkbox.

Enabled is the default setting, which means that your SSID is visible to anyone who is scanning for a network to which to connect.

Deselect the Enable checkbox to help secure your wireless network by not announcing its presence.



**Note:** If you add a PC or device later, the wireless client will be unable to scan and connect to your wireless network when the SSID broadcast is disabled. You will need to manually add a wireless profile in the client device to connect to the wireless network instead of selecting the SSID name from a typical scan list.

5. Click Save.

## **Securing your Wireless Network**

There are two methods to secure your wireless network, using the encryption key or by blocking the Media Access Control (MAC) address.



**Caution:** Wireless Security is enabled by default. Do not disable the security authentication and security features; they protect your private data transmission over the wireless link. Doing so may compromise the security of your PCs or other devices and lead to theft of service or loss of bandwidth.

#### **Using the Encryption Key**

It is good practice to customize an encryption key for wireless communication. When it is defined, each wireless client needs to have that encryption key to connect to your wireless network.

- 1. Open a Web browser and enter http://gateway.2Wire.net to access the 2Wire i3802V user interface.
- 2. Click row on the Home page; the Wireless Access Point List and Unique Settings page opens (Figure 9).
- **3.** Scroll down to the Security pane.



- 4. Select an authentication setting from the Authentication Type drop-down list:
  - WEP-Open. 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 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.
  - WEP-Shared. Similar to the WEP-Open setting, do not select this setting unless there is compatibility issue with an older wireless client. Unlike the WEP-Open setting, the WEP-Shared setting prevents open access by any wireless client; therefore, it is more secure than the WEP-Open setting. Set an encryption key on your AP and enter the same key into your other wireless clients.
  - WPA-PSK. This setting provides good security and works with most wireless clients but perhaps not some older clients. This setting requires that an encryption key to be set on the AP and that the wireless client be configured to use Wi-Fi Protected Access – Pre-Shared Key (WPA-PSK) with the same encryption key.
  - WPA-PSK and WPA2-PSK. This is the default setting. More secure than WPA-PSK, 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.
  - WPA2-PSK. 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.



**Note:** Check the capabilities of the wireless clients that will be accessing this network and find the most secure protocol that is supported by all.

5. Select Use custom encryption key and enter a security key in the field.

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

## **Allowing Devices with MAC Address Filtering**

The MAC address is a factory-programmed address assigned to each hardware device. By default, the i38HG uses its built-in hardware address. Using the MAC address filtering feature enables you to allow wireless connection to all devices or an individual device.

#### **Allowing all Devices**

When the MAC filtering is disabled, all discovered devices are allowed. Be default, the MAC filtering is disabled (that is, allowing all devices). This section provides instructions to allow all devices. To allow individual devices, refer to Allowing Individual Devices.



**Note:** This method is less secure than using the encryption key.

To disable MAC address filtering to allow all devices:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- **2.** Click not the Home page; the Wireless Access Point List and Unique Settings page opens.
- **3.** Scroll down to the MAC Filtering pane.

MAC Filtering

MAC Filtering Edit Blocked/Allowed Device List

4. Click Edit Blocked/Allowed Device List; the Wireless MAC Filtering page opens.

<b>Γ&amp;T U</b> -	verse				<b>2</b> Mi2
Iome	Services	Settings	Site Map		
System I	nfo Broadbar	Id LAN	Firewall Logs	Diagnostics	
Statu	Wireless Wire	d Interfaces D	OHCP IP Address A	ocation Statistics	
Wirele	ss MAC Filter	ring			
Enable	MAC Filtering	J			
Enable					
	- -				
Select	Devices to be	Allowed o	r BIOCKED		
Select th you do n	e devices (by liste ot see a particular	d name or MAC device in the l	Address) that you ist, then click the "I	ant to block or allow onto your escan For Devices" button or ma	wireless network. If nually add a device
using its	MAC address.				,
Note: Ne if MAC fi	wly discovered de Itering is enabled.	vices, or manu	ally added devices v	ill automatically appear in the bl	ocked devices list
Allowed	Devices:		Blocked Devi	es	
	<< >> Re	scan For Devices	5		
	Delete	]			
Add No	w MAC Addr	ess to List N	Manually		
Enter M	AC address		Add To List	]	
					Save
_					



Note: Make sure that the Enable checkbox is not selected.

- 5. Enter the MAC address automatically or manually.
  - To enter the address automatically, click **Rescan For Devices**; the MAC addresses of the allowed devices populated in the *Allowed Devices* pane as shown below.

Allowed Devices:		Blocked Devices
00:16:6f.0e:87:9c 00:18:8b:a3:1d:32 00:e0:4c:03:30:29	<< >> Rescan For Devices Delete	

- To enter the address manually, enter the MAC address in its field using this format, for example, 00:1B:5B:90:F4:80, then click Add to List. The address you entered appears in the Allowed Devices pane.
- 6. Click Save.

#### **Allowing Individual Devices**

This section provides instructions to allow individual devices. To allow all devices, refer to Allowing all Devices.

To allow individual devices:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click on the Home page; the Wireless Access Point List and Unique Settings page opens.
- **3.** Scroll down to the MAC Filtering pane.

MAC Filtering	
MAC Filtering	Edit Blocked/Allowed Device List

4. Click Edit Blocked/Allowed Device List; the Wireless MAC Filtering page opens.

	e					
lome Ser	vices Se	ettings	Site Map			
system Info	Broadband	LAN Fir	rewall Logs	Diagnos	tics	
Status Wire	less Wired Int	erfaces DHC	CP IP Address	Allocation S	atistics	
Wireless M	AC Filtering	5				
Enable MAC	Filtering					
Enable 🔽						
enable E						
Select Devic	es to be Al	lowed or E	Blocked			
Select the devic	es (by listed na	me or MAC Ad	dress) that you	want to bloc	c or allow onto yo	ur wireless network.
you do not see a using its MAC a	a particular dev ddress.	ice in the list,	then click the	Rescan For D	evices" button or i	manually add a devic
Note: Newly dis	covered device	s, or manually	added devices	will automati	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering	covered device is enabled.	s, or manually	added devices	will automati	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. s:	s, or manually	v added devices Blocked	will automati Devices	cally appear in the	e blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. s:	s, or manually	added devices Blocked	will automati Devices	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. .s:	s, or manually	v added devices Blocked 00:16:6( 00:18:8) 00:18:73	will automati Devices :0e:87:9c o:a3:1d:32 :e2:cc:a5	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. s: <<	s, or manually	v added devices Blocked 00:16:61 00:18:81 00:18:73	will automati Devices :0e:87:9c o:a3:1d:32 :e2:cc:a5	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. 	s, or manually scan For Device	v added devices Blocked 00:16:6 00:18:8 00:18:73	will automati Devices :0e:87:9c o:a3:1d:32 :e2:cc:a5	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. s: >> Res Delete	s, or manually scan For Device	v added devices Blocked 00:16:6 00:18:8 00:18:73	will automati Devices 0e:87:9c 5:a3:1d:32 :e2:cc:a5	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. s: >> Res Delete	s, or manually scan For Device	2 added devices Blocked 00:16:66 00:18:81 00:18:73	will automati Devices :0e:87:9c o:a3:1d:32 :e2:cc:a5	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device	covered device is enabled. s: S: Res Delete AC Address	s, or manually ican For Device	v added devices Blocked 00:16:61 00:18:81 00:18:73 00:18:73 00:18:73	will automati Devices :0e:87:9c :a3:1d:32 :e2:cc:a5	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device Add New M/ Enter MAC add	covered device is enabled. s: >> Res Delete AC Address	s, or manually ican For Device ] to List Ma	v added devices Blocked 00:16:6i 00:18:8i 00:18:7i 00:18:7i 00:18:7i 00:18:7i 00:18:7i	will automati	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device Add New M/ Enter MAC add	covered device is enabled. s: >> Res Delete AC Address	s, or manually scan For Device ] to List Ma	v added devices Blocked 00:16:6 00:18:8 00:18:7 00:18:7 00:18 Add To List	will automati	cally appear in the	blocked devices list
Note: Newly dis if MAC filtering Allowed Device Add New M/ Enter MAC add	covered device is enabled. s: S: Res Delete AC Address	s, or manually scan For Device	v added devices Blocked 00:16:6 00:18:8 00:18:7 00:18:7 00:18 Add To List	will automati	cally appear in the	blocked devices list



**Note:** Make sure that the **Enable** checkbox is selected; otherwise, the device will not be allowed.

5. Select the device you want to allow from the *Blocked 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.

6. Click <<; the list(s) you selected appears in the *Blocked Devices* pane, as shown below.



7. Click Save.

## **Blocking Devices with MAC Address Filtering**

The MAC address is a factory-programmed address assigned to each hardware device. By default, the i38HG uses its built-in hardware address. When enabled, the wireless connection is blocked to the MAC address listed in the *Allowed Devices* pane. Using the MAC address filtering feature enables you to block wireless connection to all devices or an individual device.

#### **Blocking all Devices**

This section provides instructions to block all device. To block individual devices, refer to Blocking Individual Devices.

To enable MAC filtering to block all devices:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click on the Home page; the Wireless Access Point List and Unique Settings page opens.
- **3.** Scroll down to the *MAC Filtering* pane.

MAC Filtering	
MAC Filtering	Edit Blocked/Allowed Device List

4. Click Edit Blocked/Allowed Device List; the Wireless MAC Filtering page opens.

	0.00			
lome	Services	Settings	Site Map	
system In	ifo Broadba	und LAN	Firewall Logs	Diagnostics
Status	Wireless Wir	ed Interfaces [	OHCP IP Address	Allocation Statistics
Wireles	s MAC Filte	ering		
Enable	MAC Filterir	ig		
Enable [				
c	_			
Select I	Jevices to D	e Allowed o	BIOCKEU	
Select the	devices (by list	ed name or MAC	Address) that you	want to block or allow onto your wireless network.
using its l	MAC address.	ar device in the	ist, then thek the	Rescan for Devices button of manually add a devic
Note: New	vlv discovered o	evices, or manu	ally added devices	will automatically appear in the blocked devices list
if MAC filt	tering is enable	d.		<i>2</i>
Allowed I	Devices:		Blocked	Devices
00:18:8b	:a3:1d:32			
00:16:6f: 00:e0:4c:	:03:30:29			
	2	Bescan For De	vices	
			inces	
	6	Delete		
Add Ne	w MAC Add	ress to List I	Manually	
Add Ne	w MAC Add	ress to List I	Manually	
Add Ne	w MAC Add	ress to List I	Manually Add To List	
Add Ne	w MAC Add	ress to List I	Manually Add To List	Save

32
- 5. Select the **Enable** checkbox to block all devices.
- 6. Click **Save**; a dialog box opens confirming that the configuration is changed. The MAC addresses on the *Allowed Devices* pane now appear on the *Blocked Devices* pane. For example



**Note:** Make sure to click **Save** to keep the transaction persistent; otherwise, the transaction is only a one-time event.

ome Services	Settings Si	te Map				
stem Info Broadba	nd LAN Firew	all Logs	Diagno	stics		
Status Wireless Wir	ed Interfaces DHCP	IP Address A	llocation	Statistics		
Vireless MAC Filte	ering					
nable MAC Filterin	q					
Fachla 🖂	-					
inable 🔽						
elect Devices to b	e Allowed or Blo	cked				
elect the devices (by list	ed name or MAC Addre	ess) that you	want to blo	ck or allow	onto your	wireless network
ou do not see a particula	ve dovico in the list, the	on click the "	Rescan For	Dentine all lense		10 11 1 1 ×
sing its MAC address	a device in the list, the	en click the		Devices bu	tton or ma	inually add a devi
sing its MAC address.	a device in the list, the	en click the 1		Devices bu	tton or ma	inually add a devi
sing its MAC address. Jote: Newly discovered d	evices, or manually ad	ded devices v	vill automa	tically appea	ar in the bl	locked devices lis
ing its MAC address.	evices, or manually ad	ded devices v	will automa	tically appea	ar in the bl	inually add a devi
lote: Newly discovered d ? MAC filtering is enabled Allowed Devices: 00:18:8b:a3:1d:32	evices, or manually ad	ded devices v Blocked	will automa Devices 0e:87:9c	tically appea	ar in the bl	locked devices lis
Allowed Devices: 00:16:96:00 address. 00:16:90:00 address. 00:18:80:a3:1d:32 00:16:6700:87:90 00:04:07:30:29	evices, or manually ad	ded devices v Blocked 00:16:6f: 00:18:8b 00:18:73:	vill automa Devices 0e:87:9c :a3:1d:32 e2:cc:a5	tically appea	ar in the bl	Inually and a devi
Allowed Devices: 00:46 MAC filtering is enabled Allowed Devices: 00:18:8b:a3:1d:32 00:16:6f:0e:87:9e 00:e0:4c:03:30:29	evices, or manually ad	ded devices v Blocked 00:16:6f 00:18:8b 00:18:73:	will automa Devices 0e:87:9c :a3:1d:32 e2:cc:a5	tically appea	ar in the bl	inually add a devi
Interface a particular sing its MAC address. Note: Newly discovered d FMAC filtering is enabled Allowed Devices: 00:16:670:e8:79:e 00:e0:4c:03:30:29	evices, or manually ad Rescan For Devices	Blocked   00:16:6f; 00:18:8b 00:18:73:	vill automa Devices 0e:87:9c :a3:1d:32 e2:cc:a5	tically appea	ar in the bl	nualiy add a devi
Interse a particular sing its MAC address. Note: Newly discovered d MAC filtering is enabled Allowed Devices: 00:16:670-8679-6 00:60:4c:03:30:29	evices, or manually ad d. Rescan For Devices	ded devices v Blocked 00:16:6f: 00:18:8b 00:18:f3:	will automa Devices 0e:87:9c :a3:1d:32 e2:cc:a5	tically appea	ar in the bl	nualiy add a devi
oli do incide a parten sing its MAC address. Iote: Newly discovered d MAC filtering is enabled Allowed Devices: 00:18:8b:a3:1d:32 00:16:6f:0e:87:9c 00:e0:4c:03:30:29	evices, or manually ad Rescan For Devices	ded devices v Blocked 00:16:6f. 00:18:8b 00:18:73:	vill automa Devices 0e:87:9c a3:1d:32 a2:cc:a5	ically appea	ar in the bl	nualiy ado a devi
Add New MAC Add	evices, or manually ad Rescan For Devices ress to List Manual	ded devices v           Blocked           00:16:6f.           00:18:73	vill automa Devices 0e:87:9c :a3:1d:32 e2:cc:a5	ically appea	ar in the bl	nualiy ado a devi
Idea in the see a particula sing its MAC address. Idea: Newly discovered d MAC filtering is enabled Allowed Devices: 00:18:8b:a3:1d:32 00:16:6f:0e:87:9c 00:e0:4c:03:30:29	Rescan For Devices	Blocked 00:16:6f 00:18:8b 00:18:73	vill automa Devices De:87:9c :a3:1d:32 e2:cc:a5	ically appea	ar in the bl	nualiy ado a devi
Allowed Devices: 00.60 Jacobies A particular Allowed Devices: 00.18.6f.0e.87.9c 00.60.4c.03.30.29	Rescan For Devices	ded devices v Blocked 00:16:6f 00:18:8b 00:18:73	vill automa Devices 0e:87.9c :a3:1d:32 e2:cc:a5	ically appea	ar in the bl	nualiy ado a devi

7. Optionally, select the devices from the *Blocked Devices* pane, click **Delete** to remove them from the pane.

#### **Blocking Individual Devices**

This section provides instructions to block individual devices. To block all devices, refer to Blocking all Devices.

To block individual devices:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click on the Home page; the Wireless Access Point List and Unique Settings page opens.
- **3.** Scroll down to the MAC Filtering pane.

MAC Filtering	
MAC Filtering	Edit Blocked/Allowed Device List

4. Click Edit Blocked/Allowed Device List; the Wireless MAC Filtering page opens.

<b>F&amp;T</b> U-verse			2 wir
Home Services	Settings	Site Map	
System Info Broadba	and LAN	Firewall Logs	Diagnostics
Status <mark>Wireless</mark> Wir	red Interfaces D	HCP IP Address	Allocation Statistics
Wireless MAC Filte	ering		
Enable MAC Filterin	ıg		
Fachle 🗖			
Enable			
Select Devices to b	e Allowed o	r Blocked	
using its MAC address. Note: Newly discovered o if MAC filtering is enable	levices, or manua d.	ally added devices	will automatically appear in the blocked devices list
Allowed Devices:		Blocked	Devices
00:18:8b:a3:1d:32 00:16:6f:0e:87:9c 00:e0:4c:03:30:29	< Rescan For Der Delete	vices	
Add New MAC Add	ress to List N	<b>A</b> anually	
			_
Enter MAC address		Add To List	
			Save

34

- 5. Select the Enable checkbox to block all devices.
- 6. Click **Save**; a dialog box opens confirming that the configuration is changed. The MAC addresses on the *Allowed Devices* pane now appear on the *Blocked Devices* pane.



**Note:** Make sure to click **Save** to keep the transaction persistent; otherwise, the transaction is only a one-time event.

7. 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.

8. Click >>; the list(s) you selected appears in the *Blocked Devices* pane, as shown below.



9. Click Save.

## **Customize Private Wireless Settings**

The *Advanced* Settings pane allows you to customize wireless settings. It is recommended that you leave the default settings in place; however, if you are experiencing connection or performance difficulties, altering these settings may improve performance.

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click not the Home page; the Wireless Access Point List and Unique Settings page opens (Figure 9).
- **3.** Scroll down to the *Advanced* Settings pane.

Advanced Settings			
Wireless Mode:	802.11b/g 💙	Default: 802.11b/g	
DTIM Period:	1	Default: 1	
Maximum Connection Rate:	54 Mbps 💌	Default: 54 Mbps	
Enhanced Mode (pbcc):	<b>V</b>	Default: Enabled	
		S	ave

- 1. Select a wireless mode from its drop-down list.
- 2. Enter a value in the range from 1 to 3 seconds in the DTIM Period field. (The default is 1.)

This Delivery Traffic Indication Message (DTIM) value determines the interval at which the access point sends its broadcast traffic.

**3.** Select the maximum rate at which your wireless connection works. For 802.11b/g-based models, select 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.



**Note:** In rare occasions, you may need to lower the speed if you encounter reliability and inter-operability issues with other nodes in the network.

4. Select the Enhanced Mode checkbox if you want the 802.11b devices to increase the speed to 22 Mbps.



**Note:** The Packet Binary Convolutional Code (PBCC) Enhanced mode works only with 802.11b devices.

5. Click Save.

# **Configuring Wi-Fi Protected Setup**

The i38HG supports Wi-Fi Protected Setup (WPS), which is a standard for easy and secure establishment of a wireless home network. Using WPS simplifies the process of connecting any home device to the wireless network. As an AP, the i38HG issues and revokes credentials to a network. The i38HG provides a push button on the front panel (Figure 10) to enable the synchronization between the AP and the client (analogous to the pairing of the garage door opener and remote control).



**Note:** For the WPS to work, the wireless client device must support the WPS function. The installation and configuration vary among the device manufacturers, refer to your client documentation for instructions.



Figure 10: WPS Location

iNID User Guide

# **Configuring Firewall**

The i3802V includes default firewall settings that block unwanted access from the Internet; it is recommended that you leave the default settings in place. If necessary, you can allow Internet traffic or users through the firewall to your LAN devices, applications, and servers. This section provides instructions to:

- Host an application on your network to allow users access on page 40
- Remove an application on your network to block users access on page 40
- Define an application profile on page 43
- Add multiple definitions to a profile on page 47
- Delete a user-defined application profile on page 50
- Allow all applications (DMZplus) on page 52
- Stop DMZplus on page 54
- Customize firewall settings on page 55



**Caution:** You should be knowledgeable with the firewall configuration to modify these settings; otherwise, you are exposing your computer to outside attacks.

## **Hosting an Application**

To allow access from the Internet to applications running on computers inside your home network, you need to open firewall pinholes and associate the intended application(s) with a computer connected with your i3802V. If you cannot find a listing for your application, you can define an application with the protocol and port information (refer to Defining a New Application Profile on page 43.)

To host an application:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 💋 on the Home page; the Firewall Status page opens.

T&T U-verse	2Wire:
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 Settings: Default	

**3.** Select <u>Applications. Pinholes and DMZ</u>; a page similar to the following opens showing the computers that are connected to the i38HG/i3802V and the application list.

me Services Sett	ings Site M	ар	
n Info Broadband L	AN Firewall	Logs Diagnostics	
us Applications, Pinholes	and DMZ Advance	d Configuration	
w device application	traffic to pass t	hrough firewall	
lefault, the firewall blocks all ( lications running on computer wall pinholes is also known as ired application with the comp r-defined application with the	unwanted access fro rs inside your secure s opening firewall po outer below. If you ca protocol and port ir	m the Internet. You can allow home network by enabling rts or firewall port forwardin annot find a listing for your a iformation.	v access from the Internet to firewall pinholes. Opening g. To do this, associate the application, you can create a
allow Internet traffic or users t	hrough the Firewall	to your LAN devices, applica	tions and servers
elect a computer			
pose the computer that will ho	st applications throu	igh the firewall	
ou have chosen DLok hoose DorisL Enter IP address Choo	DSe		
Edit firewall settings fo	or this compute	r:	
Maximum protection - Disallo	w unsolicited inbour	nd traffic:	
Maximum protection – Disallo	w unsolicited inbour - Choose the applic	nd traffic: ation(s) that will be enabled	to pass through the firewall to
Maximum protection – Disallor Allow individual application(s) computer. Click ADD to add i	w unsolicited inbour – Choose the applic it to the Hosted App Appli	nd traffic: ation(s) that will be enabled lications list.	to pass through the firewall to
Maximum protection – Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications by: • All applications	w unsolicited inbour - Choose the applic it to the Hosted App Appli	nd traffic: ation(s) that will be enabled lications list. cation List:	to pass through the firewall to Hosted Applications:
Maximum protection – Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications by: • All applications • <u>Games</u> • <u>Audio/video</u> • <u>Messaging and Internet</u> <u>Phone</u>	w unsolicited inbour - Choose the applic it to the Hosted App Appli Age of Empires Age of Kings Age of Wonder Aliens vs Pred Anarchy Onlin Absource Cell	nd traffic: ation(s) that will be enabled lications list. cation List: s s ator a Add	to pass through the firewall to Hosted Applications:
Maximum protection – Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications by: • All applications • Games • Audio/video • Messaging and Internet Phone • Servers	w unsolicited inbour - Choose the applic it to the Hosted Appl Age of Empires Age of Kings Age of Kings Age of Wonder Aliens vs Pred Anarchy Online Asheron's Call Baldur's Gate BattleCom	nd traffic: ation(s) that will be enabled lications list. cation List:	to pass through the firewall to Hosted Applications
Maximum protection – Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications Games All applications Games Audio/video Messaging and Internet Phone Servers Other User-defined	w unsolicited inbour - Choose the applic it to the Hosted App Age of Empires Age of Kings Age of Wonder Aliens vs Pred Anarchy Onlin Asheron's Call Baldur's Gate BattleCom BattleFold Com Battlefold Com	nd traffic: ation(s) that will be enabled lications list. cation List: s s ator ator e municator te	to pass through the firewall to Hosted Applications:
Maximum protection - Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications Games Audio/video Messaging and Internet Phone Servers Other User-defined	w unsolicited inbour - Choose the applic it to the Hosted App Appli Age of Empires Age of Kings Age of Wonder Aliens vs Pred Anarchy Online Baldur's Gate Battlefeid Com Black and Whit Add a new use application	nd traffic: ation(s) that will be enabled lications list. cation List: s stor e municator te r-defined	to pass through the firewall to Hosted Applications:
Maximum protection - Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications • Games • Audio/video • Messaging and Internet Phone • Servers • Other • User-defined OAllow all applications (DMZpli xcept traffic which has been spi pplications" feature, will autom	w unsolicited inbour - Choose the applic It to the Hosted App Appli Age of Empires Age of Kings Age of Wonder Aliens vs Pred. Anarchy Onlin Asheron's Call Baldur's Gate BattleCom Battlefold Com Battlefold Com	nd traffic: ation(s) that will be enabled lications list. cation List: s s ator p municator te r-defined elected computer in DMZplu o another computer using th o this computer. The DMZplu	to pass through the firewall to Hosted Applications: we we s mode. All inbound traffic, "Allow individual us-enabled computer is less
Maximum protection - Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications Games Audio/video Messaging and Internet Phone Servers Other User-defined Allow all applications (DMZpli xcept traffic which has been spi pplications" feature, will autom; ecure because all unassigned fi	<ul> <li>unsolicited inbour</li> <li>Choose the applicit</li> <li>to the Hosted App</li> <li>Appli</li> <li>Age of Empires</li> <li>Age of Kings</li> <li>Age of Kings</li> <li>Age of Wonder</li> <li>Ailens vs Predi</li> <li>Anarchy Online</li> <li>Asheron's Call</li> <li>BatlueCom</li> <li>Battlefeid Com</li> <li>Battlefeid Com</li> <li>Black and Whit</li> <li>Add a new use</li> <li>application</li> <li>us mode) - Set the s</li> <li>ecifically assigned t</li> <li>attacally be directed t</li> <li>rewall ports are open</li> </ul>	nd traffic: ation(s) that will be enabled lications list. cation List: s s ator s ator r-defined elected computer in DMZplu o another computer. The DMZplu ted for that computer. The DMZplu	to pass through the firewall to Hosted Applications: we we s mode. All inbound traffic, "Allow individual us-enabled computer is less
Maximum protection - Disallo Allow individual application(s) s computer. Click ADD to add i Filter Applications Games Audio/video Messaging and Internet Phone Servers Other User-defined Allow all applications (DMZpli kcept traffic which has been sp ppplications" feature, will automacure because all unassigned fil tote: Once DMZplus mode is sel elected computer. The compute ind you must reboot the comput	w unsolicited inbour - Choose the applic t to the Hosted App Age of Empires Age of Kings Age of Wonder Age of Kings Age of Wonder Age of Wonder Baldur's Gate Baldur's Gate BattleCom Battlefold Com Black and Whir Add a new use application us mode) - Set the s ecifically assigned tt atically be directed t rewall ports are oper lected and you click rr must be set to DH+ ter. If you are changi computers.	nd traffic: ation(s) that will be enabled lications list. cation List: s s ator a municator te r-defined elected computer in DMZplu o another computer using th o this computer. The DMZpli ted for that computer. save, the system will issue a CP mode to receive the new M	to pass through the firewall to Hosted Applications: we s mode. All inbound traffic, "Allow individual us-enabled computer is less new IP address to the P address from the system, computer to another

**4.** Select the computer that you want to host the application(s).



**Note:** If the computer you want to select is unlisted because it is powered off and the "hide inactive devices" option is enabled; you still can select it as long as it is on the same network and you know its IP address. Replace "Enter IP address" with the intended IP address, then click **Choose**.

#### 5. Select Allow individual application(s).

- **6.** Filter the application list by selecting the category; your selection is displayed in the *Application List* panel.
- 7. Select from the *Application List* panel the application(s) you want to host.



**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.

- 8. Click Add; the application(s) you selected appears in the Hosted Applications panel.
- 9. Click Save; a message appears informing you the status.

#### **Removing Hosted Applications**

- 1. Open a Web browser and enter http://gateway.2Wire.net to access the 2Wire i3802V user interface.
- 2. Click *on the Home page; the Firewall Status page opens, displaying the current hosted application settings.*

#### AT&T U-verse

A À	Ē	-
	L C	

ome	Services Set	tings Site Map			
ystem	Info Broadband	LAN Firewall Logs	Diagnosti	cs	
Stati	s Applications, Pinhole	s and DMZ Advanced Configu	ation		
	_				
Firew	all Status				
Firewa	all Active	ss of unwanted activity from the	Internet.		
Firewa The fire Curre	III Active wall actively blocks acces nt Settings: Custon Allowed Applications	ss of unwanted activity from the n Application Type	Internet.	Port Number(s)	Public IP
Firewa The fire Curre Device DLok	all Active wall actively blocks acce int Settings: Custon Allowed Applications Age of Empires	ss of unwanted activity from the Application Type DirectX Game (DirectPlay) hosi	Protocol TCP	<b>Port Number(s)</b> 47624	Public IP 76.193.113.77
Firewa The fire Curre Device DLok	all Active wall actively blocks acce nt Settings: Custon Allowed Applications Age of Empires	ss of unwanted activity from the Application Type DirectX Game (DirectPlay) host	Protocol TCP UDP	<b>Port Number(s)</b> 47624 47624	Public IP 76.193.113.77 76.193.113.77
Firewa The fire Curren Device DLok	all Active wall actively blocks acce: nt Settings: Custon Allowed Application: Age of Empires Age of Kings	Application Type DirectX Game (DirectPlay) hosi	Protocol TCP UDP TCP	Port Number(s) 47624 47624 47624	<b>Public IP</b> 76.193.113.77 76.193.113.77 76.193.113.77
Firewa The fire Curren Device DLok	all Active wall actively blocks acce nt Settings: Custon Allowed Applications Age of Empires Age of Kings	Application Type DirectX Game (DirectPlay) host	Protocol TCP UDP TCP UDP	Port Number(s) 47624 47624 47624 47624 47624	Public IP 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77
Firewa The fire Curren Device DLok	all Active wall actively blocks acce nt Settings: Custon Allowed Applications Age of Empires Age of Kings Age of Wonders	Application Type DirectX Game (DirectPlay) hosi DirectX Game (DirectPlay) hosi DirectX Game (DirectPlay) hosi	Protocol TCP UDP TCP UDP TCP	Port Number(s) 47624 47624 47624 47624 47624 47624	Public IP 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77

42

- 3. Select Applications. Pinholes and DMZ; a page opens showing hosted applications.
- 4. Select the hosting computer if you do not see the pinhole you want to remove in the list.
- **5.** Scroll to the *Edit firewall settings for this computer* pane.



6. Select the application(s) you want to remove from the Hosted Applications panel, click Remove.



**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.

**7.** Click **Save**; a message appears informing you the status. The application(s) you selected is removed from the *Hosted Applications* panel and returned to the *Application List* panel.

# **Defining a New Application Profile**

An application profile configures your system's firewall to pass through application-specific data. You can define an application profile that is not included in the *Application List*. This feature is typically used if the application for which you would like to pass through data to a given computer is new or has been recently updated to a new version.

To add a new application profile:

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 💋 on the Home page; the Firewall Status page opens.
- **3.** Select <u>Applications</u>. <u>Pinholes and DMZ</u>; a page opens showing the computers that are connected to your i38HG/i3802V and the application list.

Filter Applications by:	Application List:	Hosted Applications:	
<ul> <li>All applications</li> </ul>			
<u>Games</u>	Age of Empires		
Audio/video	Age of Kings		
Messaging and Internet	Aliens vs Predator		
Phone	Anarchy Online	Add	
Servers	Baldur's Gate	Remove	
• Other	BattleCom		
• Other	Battlefield Communicator Black and White		
• <u>oser-dermed</u>		2	
	Add a new year defined		
	application		
Allow all applications (DMZplus cept traffic which has been speci plications" feature, will automati cure because all unassigned firev	mode) – Set the selected computer fically assigned to another compute cally be directed to this computer. T vall ports are opened for that compu	n DMZplus mode. All inbound traffic, r using the "Allow individual he DMZplus-enabled computer is less ter.	
te: Once DMZplus mode is selec ected computer. The computer n d you must reboot the computer. mputer, you must reboot both co	ted and you click save, the system v nust be set to DHCP mode to receive If you are changing DMZplus mode mputers.	vill issue a new IP address to the the new IP address from the system, from one computer to another	
te: Once DMZplus mode is selec ected computer. The computer n d you must reboot the computer. mputer, you must reboot both co	ted and you click save, the system v nust be set to DHCP mode to receive If you are changing DMZplus mode imputers.	ill issue a new IP address to the the new IP address from the system, from one computer to another	
te: Once DMZplus mode is selec ected computer. The computer n d you must reboot the computer. mputer, you must reboot both co	ted and you click save, the system v nust be set to DHCP mode to receive If you are changing DMZplus mode imputers.	ill issue a new IP address to the the new IP address from the system, from one computer to another Save	

4. Scroll down and click Add a new user-defined application; the Firewall Application Profile Definition page opens.

Home Services Set	tings Site Map
System Info Broadband	LAN Firewall Logs Diagnostics
Status Applications, Pinhole	s and DMZ Advanced Configuration
Firewall Application Pro	file Definition
If the desired application require definitions. Current definitions f	s multiple ports of both TCP and UDP ports, you will need to add multiple or this profile are shown in the Definition List below.
Application Profile Name:	
Create Application Definition	n
Protocol:	TCP 💿 UDP 🔘
Port (or Range):	From: To:
Protocol Timeout:	TCP default 8400 seconds, UDP default 600 seconds
Map to Host Post:	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.
	Add to List
Definition List	
Protocol Port (or Range) Hos	t Port Timeout (sec)

#### 44

5. Enter the application profile name in the Application Profile Name field.



**Notes:** For easy identification, use the name of the application (for example, Redwing Game Server).

Clicking **Back** returns to the Allow device application traffic to pass through firewall page.

- **6.** Create a definition for your application that is to be allowed through the firewall.
  - In the **Protocol** field, select the **TCP** or **UDP** radio button. If the application you are adding requires both, you need to create a separate definition for each.
  - In the Port (or Range) field, enter the port or port range the application uses. For example, some applications requires only one port to be opened (such as TCP port 500); others require that all TCP ports from 600 to 1000 be opened.



**Note:** If only one port is required, enter the port number in the **From** field.

- In the Protocol Timeout (seconds) field, optionally enter a value for the amount of time that can pass before the application "times out." When leaving the field blank, the system uses the default values (8400 seconds for the TCP protocol; 600 seconds for the UDP protocol).
- In the Map to Host Port field, enter a value that maps the port range you established in the Port field 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 forth.
- From the Application Type drop-down list, select the application type. If you do not know the application type, select nothing.



**Note:** You can find the above information in the documentation provided by the company that produces the application.

7. Click Add to List; a message appears informing you of the status and the information appears in the *Definition List* pane. For example,

<b>F&amp;T</b> U-verse	
ome Services Setting	S Site Map
ystem Info Broadband LAN	Firewall Logs Diagnostics
Status Applications, Pinholes and	DMZ Advanced Configuration
Configuration Success	ful
irewall Application Profile	Definition
the desired application requires mult efinitions. Current definitions for this	iple ports of both TCP and UDP ports, you will need to add multiple ports are shown in the Definition List below.
Application Profile Name:	VOX
reate Application Definition	
Protocol:	TCP 💿 UDP 🔘
Port (or Range):	From: To:
Protocol Timeout:	TCP default 8400 seconds, UDP default 600 seconds
Map to Host Post:	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.
	Add to List
Definition List	
Protocol Port (or Range) Host Por	t Timeout (sec)
UDP 500 500	600 Remove
	Back

## **Adding Multiple Definitions to a Profile**

Some application requires both TCP and UDP ports. In this case, you need to define additional ports to an existing profile. You can add the definition of the profile only when it has not been added to the hosted application list. If the profile is added to the hosted application list and you want to modify it, you need to first remove it from the *Hosted Applications* panel.

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 🕖 on the Home page; the Firewall Status page opens.

ome	Services S	Settings Site Map			
tem	Info Broadband	LAN Firewall Logs	Diagnos	stics	
State	Applications, Pinho	oles and DMZ Advanced Configu	ration		
rewa ie fire urre	all Active wall actively blocks ac nt Settings: Custo	om	e Internet		
rewa e fire urre evice	all Active wall actively blocks ac nt Settings: Custo Allowed Application	om Application Type DirectX Game (DirectPlay) bos	Protoco	ol Port Numbe	er(s) Public IP
rewa ie fire urre evice Lok	all Active wall actively blocks ac nt Settings: Custo Adlowed Application Age of Empires	ccess of unwanted activity from th om DirectX Game (DirectPlay) hos	Protoco t TCP UDP	ol Port Numbe 47624 47624	er(s) Public IP 76.193.113.77 76.193.113.77
rewa e fire urre evice Lok	all Active wall actively blocks ac nt Settings: Custo Allowed Applicatio Age of Empires Age of Kings	ccess of unwanted activity from th om DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos	Protoco t TCP UDP t TCP	ol Port Numbe 47624 47624 47624	er(s) Public IP 76.193.113.77 76.193.113.77 76.193.113.77
rewa le fire urre evice DLok	all Active wall actively blocks ac nt Settings: Custo Allowed Applicatio Age of Empires Age of Kings	oms Application Type DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos	Protoco t TCP UDP t TCP UDP	ol Port Numbe 47624 47624 47624 47624 47624	er(s) Public IP 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77
irewa ne fire urre Device DLok	all Active wall actively blocks ac nt Settings: Custo Allowed Applicatio Age of Empires Age of Kings Age of Wonders	ons Application Type DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos	Protoco t TCP UDP t TCP UDP t TCP	<b>OI Port Numbe</b> 47624 47624 47624 47624 47624	er(s) Public IP 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77

3. Select <u>Applications</u>. <u>Pinholes and DMZ</u>; a page opens showing hosted applications.

**4.** Scroll to the *Edit firewall settings for this computer* pane.

2) Edit firewall settings f	or this computer:	
OMaximum protection - Disall	ow unsolicited inbound traffic:	
Allow individual application(s this computer. Click ADD to add	<ul> <li>- Choose the application(s) that it to the Hosted Applications list</li> </ul>	will be enabled to pass through the firewall to
Filter Applications by:	Application List:	Hosted Applications:
<ul> <li>All applications</li> </ul>		
<ul> <li><u>Games</u></li> <li><u>Audio/video</u></li> <li><u>Messaging and Internet</u> <u>Phone</u></li> <li><u>Servers</u></li> <li><u>Other</u></li> <li><u>User-defined</u></li> </ul>	Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Black and White Dark Reign Dark Reign 2 Delta Force	Age of Empires Age of Kings Age of Wonders Remove
	Add a new user-defined application	Edit or delete user-defined application

**Note:** If you have not created any profiles, the link will not appear.

5. Click <u>Edit or delete user-defined application</u>; a page similar to the following opens.

omo Comicoo	Sottings	Site Man	
ome Services	Settings	Site Map	
ystem Info Broadba	nd LAN	Firewall Logs	Diagnostics
Status Applications, F	Pinholes and DM	IZ Advanced Confi	iguration
Edit or Delete a Use	er-Defined A	Application	
Choose an application fro	m the list below	then choose to Edi	t or Delete the selected application profile.
	VOX		
User defined applications	s: Edi	t Delete	

48



**Note:** The application you created will not appear here if it has been added to the Hosted Applications. Return to the previous page, select the application intended for modification, click **Remove** to return the application to the available application list.

wai ne

6. Select the application you want to modify, click **Edit**; the selected profile page opens.

<b>&amp;T U-vers</b>	e				C	יאחלוד
Iome Se	rvices	Settings	Site M	lap		
System Info	Broadba	nd LAN	Firewall	Logs	Diagnostics	
Status <mark>App</mark>	lications,	Pinholes and D	MZ Advance	ed Config	guration	
Firewall Ap	plicatio	n Profile D	efinition			
If the desired a definitions. Cur	pplication rent defini	requires multi itions for this	ple ports of b profile are sho	oth TCP a own in th	and UDP ports, you will need to add e Definition List below.	multiple
Application I	Profile Na	ime:	VOX			
Create Appli	cation De	finition				
Protocol			TCP  OUDP  O	)		
Port (or F	Range):		From:	To		
Protocol	Timeout:			TCP defa	ult 8400 seconds, UDP default 600	seconds
Map to H	lost Post:			Default/	blank = same port as above	
Applicati	on Type:		-		~	
			Note: In some specialized fi application ye it is recomme	e rare ins rewall ch ou are ad ended tha	tances, certain application types re anges in addition to simple port for ding appears in the application type tt you select it.	quire rwarding. If the e menu above,
						Add to List
Definition L	ist					
Protocol Port	(or Rang	e) Host Port	Timeout (se	c)		
UDP 500		500	600	Rem	ove	
						Back



Note: You are prompted to enter your password if one is set up.

- 7. Modify any information, as necessary.
- **8.** Click **Add to List**; a message appears informing you of the status and the information appears in the *Definition List* pane.

# **Deleting Profiles**

You can delete only the profiles you created. Before deleting a user-defined profile, make sure to remove it from the *Hosted Applications* pane.

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 🦉 on the Home page; the Firewall Status page opens.

ome	Services Se	ettings Site Map			
stem	Info Broadband	LAN Firewall Logs I	Diagnosti	cs	
Stati	us Applications, Pinho	les and DMZ Advanced Configur	ation		
irewa ne fire urre	all Active wall actively blocks acc nt Settings: Custo	ess of unwanted activity from the	Internet.		
irewa ne fire urre Jevica	all Active wall actively blocks acc nt Settings: Custo e Allowed Application	ess of unwanted activity from the m ns Application Type	Internet. Protocol	Port Number(s)	Public IP
irewa ne fire urre Jevica	all Active wall actively blocks acc nt Settings: Custo e Allowed Application Age of Empires	ess of unwanted activity from the m ns Application Type DirectX Game (DirectPlay) host	Internet. Protocol TCP	Port Number(s) 47624	<b>Public IP</b> 76.193.113.77
irewa ne fire urre Vevice )Lok	all Active wall actively blocks acc nt Settings: Custo e Allowed Application Age of Empires	ess of unwanted activity from the m Application Type DirectX Game (DirectPlay) host	Internet. Protocol TCP UDP	<b>Port Number(5)</b> 47624 47624	<b>Public IP</b> 76.193.113.77 76.193.113.77
irewa ne fire urre Device DLok	all Active wall actively blocks acc nt Settings: Custo e Allowed Application Age of Empires Age of Kings	ess of unwanted activity from the m Application Type DirectX Game (DirectPlay) host DirectX Game (DirectPlay) host	Internet. Protocol TCP UDP TCP	Port Number(s) 47624 47624 47624 47624	<b>Public IP</b> 76.193.113.77 76.193.113.77 76.193.113.77
irewa ne fire urre Device DLok	all Active wall actively blocks acc nt Settings: Custo e Allowed Application Age of Empires Age of Kings	ess of unwanted activity from the m Application Type DirectX Game (DirectPlay) host DirectX Game (DirectPlay) host	Internet. Protocol TCP UDP TCP UDP	Port Number(s) 47624 47624 47624 47624 47624	<b>Public IP</b> 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77
irewa he fire urre Device	all Active wall actively blocks acc nt Settings: Custo e Allowed Application Age of Empires Age of Kings Age of Wonders	ess of unwanted activity from the m Application Type DirectX Game (DirectPlay) host DirectX Game (DirectPlay) host DirectX Game (DirectPlay) host	Internet. Protocol TCP UDP TCP UDP TCP	Port Number(s) 47624 47624 47624 47624 47624 47624	<b>Public IP</b> 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77

3. Select <u>Applications</u>, <u>Pinholes and DMZ</u>; a page opens showing hosted applications.

**4.** Scroll to the *Edit firewall settings for this computer* pane.

2) Edit firewall settings f	for this computer:	
OMaximum protection - Disall	ow unsolicited inbound traffic:	
Allow individual application(s this computer. Click ADD to add     Aldebergererererererererererererererererere	s) – Choose the application(s) that I it to the Hosted Applications list.	will be enabled to pass through the firewall to
Filter Applications by:	Application List:	Hosted Applications:
All applications		
• <u>Games</u>	Aliens vs Predator	Age of Empires
<u>Audio/video</u>	Asheron's Call	Age of Wonders
Messaging and Internet	Baldur's Gate BattleCom	Add
<u>Phone</u>	Battlefield Communicator	Remove
<u>Servers</u>	Black and White Dark Reign	
Other	Dark Reign 2	
<ul> <li><u>User-defined</u></li> </ul>	Delta Force 💌	
		The state of the second state of the state
	<u>Add a new user-defined</u> application	<u>Edit or delete user-defined</u> <u>application</u>

**Note:** If you have not created any profiles, the link will not appear.

5. Click <u>Edit or delete user-defined application</u>; a page similar to the following opens.

ome Services	Settings	Site Map	
ystem Info Broadbar	nd LAN F	Firewall Logs	Diagnostics
Status Applications, F	Pinholes and DM	Z Advanced Con	figuration
dit on Doloto o Uac	n Dafinad A	pplication	
	er Denned A	pheation	
noose an application from	m the list below	then choose to Ec	lit or Delete the selected application profile.
	VOX		
	VOX		
	VOX		
User defined applications	VOX Edit	Delete	
User defined applications	VOX Edit	Delete	



**Note:** The application you created will not appear here if it has been added to the Hosted Applications. Return to the previous page, select the application intended for modification, click **Remove** to return the application to the available application list.

6. Select the application you want to delete, click Delete.



**Note:** Be sure to select the intended application. Once you click **Delete**, the application is deleted.

# Allowing all Applications (DMZplus)

DMZplus is a special firewall mode that is used for hosting applications. When in the 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.
- Can receive unsolicited network traffic from the Internet.



**Caution:** 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.

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 🦉 on the Home page; the Firewall Status page opens.
- 3. Select <u>Applications</u>. <u>Pinholes and DMZ</u>; a page opens showing hosted applications.

ome Sei	rvices	Settings	Site 1	Map				
stem Info	Broadband	I LAN	Firewall	Logs	Diagnost	ics		
Status App	lications, Pir	holes and D	MZ Advand	ced Confi	guration			
llow devic	e applicat	tion traffi	c to pass	throug	h firewall;			
By default, the f applications rur firewall pinhole desired applica user-defined ag	firewall block nning on con s is also kno tion with the oplication wit	cs all unwant nputers insic wn as openi computer b th the protoc	ed access fr le your secu ng firewall p elow. If you col and port	om the Ir re home r orts or fin cannot fin informati	nternet. You c network by en rewall port fo nd a listing fo on.	an allow acces abling firewall rwarding. To d r your applica	s from the In pinholes. Op o this, associ tion, you can	ternet to ening ate the create a
To allow Interne	et traffic or u	sers through	the Firewal	l to your	LAN devices,	applications a	nd servers	
1) Select a (	computer							
Choose the con	nputer that w	/ill host appl	ications thro	ough the f	firewall			
<ul> <li>You have choose Dori</li> <li>Choose Dori</li> <li>Enter IP addi</li> </ul>	osen DLok <u>sL</u> ress	Choose						
O Allow individ	dual applicat							
his computer.	Click ADD to	add it to th	ose the appl e Hosted Ap	ication(s) plications	that will be e s list.	nabled to pass	through the	firewall to
Filter A	Click ADD to	add it to th <b>b by</b> :	ose the appl e Hosted Ap <b>App</b>	ication(s) plications <b>lication</b>	that will be e s list. List:	nabled to pass	through the	firewall to
this computer. Filter A All app Games Audio/ Messag Phone Servers Other User-d	Click ADD to pplications video ing and Inter efined	rnet	Age of Empir Age of Empir Age of Kings Age of Wond Aliens vs Pre Anarchy Onli Asheron's Ca Baldur's Gate Baldur's Gate Baldur	ication(s) plication lication es ers dator ne II : : : : : : : : : : : : : : : : : :	that will be e s list. List:	Add Remove	s through the	firewall to
this computer. Filter A All app Games Audio/ Messag Phone Servers Other User-d	video ing and Inter efined	add it to th s by:	sse the appl Hosted Ap Age of Empiring Age of Empiring Age of Kings Age of Wond Aliens vs Pre Anarchy Onli Asheron's Gate Baldute Battlefield Co Black and W wdd a new us pplication	ication(s) plications lication es ers dator ne ll ser mmunicat hite	that will be e s list. List:	Add Remove	s through the	firewall to
this computer. Filter A All app Games Audio/ Messag Phone Servers Other User-d Allow all ap except traffic applications" f secure becaus Note: Once DN selected comp computer, you	video oppications pplications lications video efined opplications (C which has be eature, will a eature, will a eatur	ion(s) - Choice of add it to the solution of t	sse the appl e Hosted Ap Age of Empir Age of Kings Age of Wond Alliens vs Pre Anarchy Onli Asheron's Cate Balduer's Gate Battlefed Com Battlefed Com Battlefed Com Battlefed Com Battlefed A a new us pplication de) – Set the ly assigned be directed poorts are op and you clici be set to Di ou are changiters.	ication(s) plications lication es ers dator ne II mmunicat hite selected to anothe to this cr ened for t k save, th HCP mode ging DMZ	that will be e s list. List:	Add Add Remove	All inbound v individual bled compute address to the ster to anothe	firewall to ications: traffic, r is less ne ystem,

4. Select the computer that you want to allow all applications.



**Note:** If the computer you want to select is unlisted because it is powered off and the "hide inactive devices" option is enabled; you still can select it as long as it is on the same network and you know its IP address. Replace "Enter IP address" with the intended IP address, then click **Choose**.

5. Select the Allow all applications (DMZplus mode) button.

- 6. Click Save.
- **7.** Confirm that the computer you selected in Step 1 is configured for DHCP. If it is not, configure it for DHCP.
- **8.** 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.

#### **Stopping DMZplus**

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 🖉 on the Home page; the Firewall Status page opens.
- 3. Select Applications. Pinholes and DMZ; a page opens showing hosted applications.

T&T U-ve	rse			2Wire:	
Home S	Services	Settings	Site Map		
System Info	Broadba	and LAN F	irewall Logs	Diagnostics	
Status A	Applications,	Pinholes and DM	Z Advanced Con	figuration	
Allow dev	vice applic	eation traffic	to pass throu	ıgh firewall	
By default, th applications firewall pinh desired appli user-defined	he firewall blo running on c oles is also k ication with t d application	ocks all unwanted computers inside mown as opening the computer belo with the protocol	l access from the your secure home firewall ports or ow. If you cannot and port informa	Internet. You can allow access from the Internet to e network by enabling firewall pinholes. Opening firewall port forwarding. To do this, associate the find a listing for your application, you can create a tion.	
To allow Inte	ernet traffic o	r users through t	he Firewall to you	r LAN devices, applications and servers	
1) Select	a comput	er			
Choose the o	computer tha	t will host applica	ations through th	e firewall	
<ul> <li>You have</li> <li><u>Choose D</u></li> <li>Enter IP a</li> </ul>	chosen DLok <u>DorisL</u> address	Choose			
2) Edit fir	ewall sett	ings for this	computer:		
Maximum	n protection -	- Disallow unsoli	cited inbound traf	fic:	
O Allow ind this compute	lividual applic er. Click ADD	cation(s) – Choos ) to add it to the I	e the application( Hosted Applicatio	s) that will be enabled to pass through the firewall to ns list.	



Note: The above presentation shows half of the screen only.

4. Select the computer that you want to stop the DMZplus mode.



**Note:** If the computer you want to select is unlisted because it is powered off and the "hide inactive devices" option is enabled; you still can select it as long as it is on the same network and you know its IP address. Replace "Enter IP address" with the intended IP address, then click **Choose**.

- 5. Select the Maximum protection button from the *Edit firewall settings for this computer* pane.
- 6. Click Save.
- 7. Access the computer that you selected in Step 1.
- 8. Restart the computer.

## **Customizing Firewall Configuration**

The i3802V comes with a set of default firewall settings that you can change to adapt to your environment. You can change the timeout sessions and protocol that you want to go through the firewall.

....

- **1.** Open a Web browser and enter *http://gateway.2Wire.net* to access the 2Wire i3802V user interface.
- 2. Click 💋 on the Home page; the Firewall Status page opens.

ome	Services	Settings Site Map			
stem	Info Broadband	I LAN Firewall Logs	Diagnosti	cs	
Statu	Applications, Pin	holes and DMZ Advanced Configu	ration		
irew	all Status				
-					
irewa	all Active				
irewa	all Active	access of unwanted activity from the	Internet.		
Firewa The fire Curre	all Active wall actively blocks a nt Settings: Cus	access of unwanted activity from the	Internet.		
Firewa The fire Curre Device	all Active wall actively blocks a nt Settings: Cus Allowed Applicat	access of unwanted activity from the tom ions Application Type	Protocol	Port Number(s)	Public IP
Tirewa The fire Curre Device DLok	all Active wall actively blocks on nt Settings: Cus Allowed Applicat Age of Empires	access of unwanted activity from the tom ions Application Type DirectX Game (DirectPlay) hos	Protocol TCP	<b>Port Number(s)</b> 47624	Public IP 76.193.113.77
Tirewa The fire Curre Device DLok	all Active wall actively blocks on nt Settings: Cus Allowed Applicat Age of Empires	access of unwanted activity from the tom ions Application Type DirectX Game (DirectPlay) hos	Protocol TCP UDP	<b>Port Number(s)</b> 47624 47624	Public IP 76.193.113.77 76.193.113.77
irewa he fire Curre Device DLok	all Active wall actively blocks of nt Settings: Cus Allowed Applicat Age of Empires Age of Kings	access of unwanted activity from the tom ions Application Type DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos	Protocol TCP UDP TCP	<b>Port Number(s)</b> 47624 47624 47624 47624	Public IP 76.193.113.77 76.193.113.77 76.193.113.77
Firewa The fire Curre Durre Device DLok	all Active wall actively blocks of nt Settings: Cus Allowed Applicat Age of Empires Age of Kings	access of unwanted activity from the tom ions Application Type DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos	Protocol TCP UDP TCP UDP	Port Number(s) 47624 47624 47624 47624 47624	Public IP 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77
Firewa The fire Curre Device DLok	all Active wall actively blocks of nt Settings: Cus Allowed Applicat Age of Empires Age of Kings Age of Wonders	access of unwanted activity from the tom ions Application Type DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos DirectX Game (DirectPlay) hos	Protocol TCP UDP TCP UDP TCP	Port Number(s) 47624 47624 47624 47624 47624 47624	Public IP 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77 76.193.113.77

**3.** Click <u>Advanced Configuration</u>; the following page opens displaying the default settings.

System Info Broadband LAN Firewall Logs Diagnostics     Status Applications, Pinholes and DMZ Advanced Configuration     Enhanced Security     Status Applications, Pinholes and DMZ Advanced Configuration     Enhanced Security     Status Applications, Pinholes and DMZ Advanced Configuration    Enhanced Security   Status Applications, Pinholes and DMZ Advanced Configuration    Enhanced Security   Status Mappe Image: Control image:			Лар	Site N	Settings	Services	Iome
Status Applications, Pinholes and DM2 Advanced Configuration   Enhanced Security Stealth Mode Image: Configuration   Stealth Mode Image: Configuration Image: Configuration   Block Ping Image: Configuration Image: Configuration   Strict UDP Session Control Image: Configuration Image: Configuration   UDP Session Timeout Image: Configuration Image: Configuration   UDP Session Timeout Image: Configuration Image: Configuration   Outbound Protocol Control Image: Configuration Image: Configuration   Checking the box ALLOWS the associated traffic type through the firewall. Image: Configuration   HTTP Image: Configuration Image: Configuration   FTP Image: Configuration Image: Configuration   POP3 Image: Configuration Image: Configuration   NNTP Image: Configuration Image: Configuration   NNTP Image: Configuration Image: Configuration   NATEBIOS Image: Configuration Image: Configuration   NetBIOS Image: Configuration Image: Configuration   Nutre Image: Configuration Image: Configuration   Nutre Image: Configuration Image: Configuration   Marce Image: Configuration Image: Configuration   Nutre <th></th> <th>Diagnostics</th> <th>Logs</th> <th>Firewall</th> <th>id LAN</th> <th>Broadbar</th> <th>system Ir</th>		Diagnostics	Logs	Firewall	id LAN	Broadbar	system Ir
Enhanced Security  stealth Mode  Getailth Mode  strict UDP Session Control  UDP Session Timeout  600 seconds (60-43200 seconds, default = 600 seconds)  TCP Session Timeout  600 seconds (300-86400 seconds, default = 86400 seconds)  TCP Session Timeout  6400 seconds (300-86400 seconds, default = 86400 seconds)  TCP Session Timeout  Cutbound Protocol Control  TTP  740  740  740  740  740  740  740  74		figuration	ed Conf	1Z Advand	inholes and D	Applications, P	Status
stealth Mode Image: strain of the stra						d Security	Enhand
Block Ping       ✓         Strict UDP Session Control       □         UDP Session Timeout       600 seconds (60-43200 seconds, default = 600 seconds)         TCP Session Timeout       86400 seconds (300-86400 seconds, default = 86400 seconds)         Outbound Protocol Control       C         Outbound Protocol Control       C         Checking the box ALLOWS the associated traffic type through the firewall.         HTTP       ✓         FTP       ✓         SMTP       ✓         POP3       ✓         IMAP       ✓         NNTP       ✓         IRC       ✓         INAP       ✓         INAP <td< td=""><td></td><td></td><td></td><td></td><td>~</td><td>ode</td><td>Stealth</td></td<>					~	ode	Stealth
Strict UDP Session Control       □         UDP Session Timeout       600 seconds (60-43200 seconds, default = 600 seconds)         TCP Session Timeout       86400 seconds (300-86400 seconds, default = 86400 seconds)         Outbound Protocol Control					<b>V</b>	3	Block P
UDP Session Timeout       600       seconds (60-43200 seconds, default = 600 seconds)         TCP Session Timeout       86400       seconds (300-86400 seconds, default = 66400 seconds)         Outbound Protocol Control					itrol	Session Col	Strict U
TCP Session Timeout 66400   seconds (300-86400 seconds, default = 86400 seconds)   Outbound Protocol Control   Checking the box ALLOWS the associated traffic type through the firewall.   HTTP Image: Colspan="2">Image: Colspan="2" Image:	= 600 seconds)	43200 seconds , default = 600 sec	nds (60-	secor	600	on Timeout	UDP Ses
Outbound Protocol Control         Checking the box ALLOWS the associated traffic type through the firewall.         HTTP       Ø         HTTPS       Ø         FTP       Ø         Telnet       Ø         DNS       Ø         NNTP       Ø         IMAP       Ø         NNTP       Ø         IRC       Ø         All Other Protocols       Ø         Inbound Protocol Control       Ø         NetBIOS       Ø         All Other Protocols       Ø         Hatack Detection           Catacity Session Det tool           Excessive Session Det tool           TC/UUP Port Scan       Ø	= 86400 seconds)	-86400 seconds, default = 86400 s	nds (300	00 secor	864	on Timeout	TCP Ses
Checking the box ALLOWS the associated traffic type through the firewall. HTTP HTTPS FTP					Control	d Protocol	Outbou
HTTP       ✓         HTTPS       ✓         FTP       ✓         Telnet       ✓         SMTP       ✓         DNS       ✓         POP3       ✓         IMAP       ✓         NNTP       ✓         IRC       ✓         All Other Protocols       ✓         NetBIOS       ✓         All Other Protocols       ✓         Kattack Detection       ✓         C       ✓         Attack Detection       □		h the firewall.	e throug	traffic type	the associate	e box ALLOWS	Checking
HTTPS Image: state sta					<b>V</b>		нттр
FTP Image: set of the se					<b>V</b>		HTTPS
Telnet Image: set of the					<b>V</b>		FTP
SMTP   SMTP SMTP					<b>V</b>		Telnet
DNS Image: set of the se					<b>V</b>		SMTP
NetBIOS Constraints of the second sec					<b>v</b>		DNS
POP3  POP3 POP3 POP3 POP3 POP3 POP3 POP3							NetBIOS
IMAP   INTP   IRC   IRC   IRC   IB23   IDound Protocols   Inbound Protocol Control     NetBIOS     Excessive Session Detection   TCP/UDP Port Scan					<b>V</b>		POP3
NNTP   IRC  IRC  IRC  IRC  IRC  IRC  IRC  IR					<b>V</b>		IMAP
IRC  H323 H323 H323 H323 H323 H323 H323 H32					<b>v</b>		NNTP
H323   All Other Protocols   Inbound Protocol Control  NetBIOS  Attack Detection  Excessive Session Detection  CP/UDP Port Scan					<b>V</b>		IRC
All Other Protocols  Inbound Protocol Control  NetBIOS  Attack Detection  Excessive Session Detection  CP/UDP Port Scan					<b>V</b>		H323
Inbound Protocol Control  NetBIOS  Attack Detection  Excessive Session Detection  TCP/UDP Port Scan					<b>~</b>	Protocols	All Oth
NetBIOS  Attack Detection Excessive Session Detection TCP/UDP Port Scan					ontrol	Protocol C	Inboun
Attack Detection  Excessive Session Detection  TCP/UDP Port Scan							NetBIOS
Excessive Session Detection						etection	Attack
TCP/UDP Port Scan					ection	Session Det	Excession
			<b>V</b>			Port Scan	TCP/UD
Invalid Source/Destination IP address			<b>V</b>	ss	tion IP addr	urce/Destina	Invalid 9
Packet Flood (SYN/UDP/ICMP/Other)				)	P/ICMP/Othe	od (SYN/UDI	Packet F
Invalid TCP Flag Attacks (NULL/XMAS/Other)			<b>V</b>	AS/Other)	s (NULL/XM	P Flag Attacl	Invalid
Invalid ICMP Detection			<b>V</b>			MP Detection	Invalid
Miscellaneous V			<b>~</b>			eous	Miscella

56

- **4.** Customize your Internet security.
  - Stealth Mode: When the Stealth Mode is selected, your computer is "invisible" to port-scanning
    programs. Consequently, no reply is received in response in their quest to gain unauthorized
    access to computers and servers. If your computer is always connected to Internet, it is good
    practice to select the Stealth Mode to prevent potential hacking to your computer.
  - Block Ping: When enabled, Block Ping blocks all ping requests. Ping is a basic Internet program that, when used without malicious intent, allows a user to verify that a particular IP address exists and can accept requests. Hackers can use ping to launch an attack against your network, because ping can determine the network's IP address from the domain name.
  - Strict UDP Session Control: Enabling this feature provides increased security by preventing the i3802V from accepting packets sent from an unknown source over an existing connection. The ability to send traffic based on destination only is required by some applications. Enabling this feature may not allow some on-line applications to work properly.
  - UDP Session Timeout: Typically, the User Datagram Protocol (UDP) is used to exchange small data from one computer to another. Transmission Control Protocol (TCP) is used for larger data exchanges; therefore, the timeout setting for UDP is lower than that of TCP.
  - TCP Session Timeout: Transmission Control Protocol (TCP) is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message(s) to be exchanged by the application programs at each end have been exchanged. The maximum timeout is 24 hours.
- **5.** Select the protocol(s) from the *Outbound Control* pane that you allow the traffic from the network to pass through the firewall to the Internet.



**Note:** NetBIOS is primarily used for Local Area Network (LAN) communication. Typically, this protocol is not used on the Ethernet at large. For security reasons, it is blocked from the Internet to your local area network by default.

6. Select items from the Attack Detection pane to prevent unauthorized access to your computers.



**Note:** These are stateless firewall checks and apply to DMZPlus or routed mode.

- Excessive Session Detection: When enabled, the firewall detects applications on the local network that are creating excessive sessions out to the Internet. This activity is likely due to a virus or "worm" infected computer (for example, Blaster Worm).
- TCP/UDP Port Scan: A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a well-known port number (such as UDP and TCP), the computer provides. When enabled, the firewall detects UDP and TCP port scans, and drops the packet.
- Invalid Source/Destination IP address. When enabled, the firewall checks and verifies the following IP addresses:
  - IP source address (broadcast or multicast)
  - TCP destination IP address (not unicast)

- If the IP source and destination address are the same
- Invalid IP source received from private/home network

**Note:** The packets are dropped when IP addresses cannot be verified.

- Packet Flood (SYN/UDP/ICMP/Other). When enabled, the firewall checks for SYN, UDP, ICMP, and other types of packet floods on the local and Internet-facing interfaces and stops the flood.
- Invalid TCP Flag Attacks (NULL/XMAS/Other). When enabled, the firewall scans inbound and outbound packets for invalid TCP flag settings, and drops the packet to prevent SYN/FIN, NULL, and XMAS attacks.
- Invalid ICMP Detection. The firewall checks for invalid ICMP/code types, and drops the packets.
- Miscellaneous. The firewall checks for the following, and drops the packets or terminates the associated session:
  - Unknown IP protocol (drop packet)
  - Port 0 attack detected (drop packet)
  - TCP SYN packet (drop packet)
  - Not a start session packet (drop packet)
  - ICMP destination unreachable (terminate session)
- 7. Click Save; a message appears informing you of the operational status.

# Working with the Power Supply Unit

The iPSU needs no scheduled maintenance other than regular battery inspection and replacement. If the power supply unit is equipped with a backup battery, it continues to provide voice-over-IP services in case of emergency during a power outage. During a temporary AC power outage, the power source is switched to the battery without interruption of the voice-over-IP service. When the AC power is restored, the power source is switched back to the power supply unit. The switchover between the power supply unit and the battery is automatic and instantaneous.



**Note:** Reserve the battery charge during a power outage. Do not access the Internet when the power is running on the battery. Doing so will discharge the battery at a much faster rate and shorten the voice-over-IP service time.

This section provides instructions to:

- Replace the battery on page 60
- Enable the audio alert on page 63
- Disable the audio alert on page 65



**Note:** You are solely responsible for periodically replacing this battery to provide uninterruptable voice-over-IP services during a power outage. Your service provide does not monitor the battery and is not responsible for its replacement.

# **Replacing the Battery**

The battery is rated for a service life of up to five years, which varies depending on operational and environmental conditions. The battery life expectancy depends on the operating environment as temperature extremes shorten the battery life. The optimum operating temperature is between  $-5^{\circ}$  C to  $+50^{\circ}$  C, ambient (23.0° F to 122° F).

The battery is specifically designed to use with the iNID system. Contact your service provider for battery replacement information.

To replace the battery:

**1.** Use a Phillips screwdriver to unfasten two screws (one on each side) securing the power supply battery cover, and put them in a safe place (Figure 11).



Figure 11: Power Supply Unit Cover Removal

- 2. Bring the battery cable and battery cable connector to visibility (located on top of the backup battery).
- **3.** Press down on the tension springs and pull to disconnect the battery cable connector from the battery cable (Figure 12).



#### Figure 12: Battery Connector

- 4. Release the safety strap securing the battery.
- **5.** Remove the old battery from the housing and put it safely aside.



Note: Be careful when you remove the battery; it is heavy.

6. Insert the new battery gently into the housing.



**Note:** Be sure to place the battery inside the raised bottom edge of the case.

- 7. Connect the battery cable connector to the battery cable.
- **8.** Observe the **BATTERY** indicator on the iPSU, it should light green when the i38HG and i3802V are communicating properly.



**Note:** A faulty battery is indicated if the **BATTERY** indicator does not light green within 5 minutes assuming the iPSU is plugged into AC power.

**9.** Secure the battery with the safety strap.



- **10.** Place the housing cover over the unit and press gently on it until it snaps into place.
- **11.** Fasten the cover with the two screws you removed earlier.



**Note:** If you have disabled the alert earlier, make sure to enable the alert (page 63).

### **Enabling the Alert**

To enable the alert:

**1.** Enter *http://gateway.2Wire.net* as the URL; the *Home* page opens.

2WIRE AT&T U-verse Home Services Settings Site Map Summary Broadband Wireless Firewall i3802V 3 4 🕹 27232Kbps Network Status Serial 1 2000Kbps Name Enabled Number: 450712000169 Doris Warning - Emergency Battery Backup Battery Power Level Critical Battery Info Home Network Devices Device Details 8 192.168.1.64 💐 DLok Access Files Device Details 💐 DorisL Access Files Device Details Top Networking Features Wireless - modify security or settings <u>Refresh your Broadband Connection</u> - 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

2. Click Battery Info; the Emergency Battery Backup page opens.



- 3. Click **Enable** to enable the battery audible alert.
- 4. Click Save.

### **Disabling the Alert**

By default, the audible alert is enabled to warn you when the battery is exhausted. It is recommended that you do not disable the audible alert unless you intend to replace the battery within a short time. A chirping tone sounds to alert you that when the battery is exhausted and needs replacing. The duration of the chirping sound is 0.2 seconds and happens once every 5 seconds. You can turn off the chirping sound to disable the alert for 12 hours or permanently.



Caution: Disable the audio alert with caution!

If you disabled the alert and did not replace the backup battery on a timely manner, you will have no voice-over-IP services in case of emergency during an AC power outage.

To disable the alert:

**1.** Enter *http://gateway.2Wire.net* as the URL; the *Home* page opens.



2. Click Battery Info; the *Emergency Battery Backup* page opens.

System Info       Broadband       LAN       Firewall       Logs       Diagnostics         Status       Password       Date & Time       Event Notifications       Battery Backup         Emergency       Battery Backup       Image: Comparison of the system is designed to provide emergency backup services using a built-in battery pack. This page provistatus and health information about the battery.         Battery Status       Charging         Disable Alert for 12 hours       Emetry Audible Alert	Home c	Services	Settings	Site Map	
Status Password Date & Time Event Notifications Battery Backup         Emergency Battery Backup         Image: Comparison of the system is designed to provide emergency backup services using a built-in battery pack. This page provide status and health information about the battery.         Battery Status       Charging         Disable Alert for 12 hours         Battery Audible Alert       Enable	System Info	Broadban	d LAN I	Firewall Logs	Diagnostics
Emergency Battery Backup          WARNING - BATTERY POWER LEVEL CRITICAL         The system is designed to provide emergency backup services using a built-in battery pack. This page provistatus and health information about the battery.         Battery Status       Charging         Disable Alert for 12 hours         Battery Audible Alert       Enable	Status P	assword Date	e & Time Even	t Notifications	attery Backup
The system is designed to provide emergency backup services using a built-in battery pack. This page provi status and health information about the battery. Battery Status Charging Disable Alert for 12 hours Battery Audible Alert I Enable		RNING - BAT	TERY POWER	LEVEL CRITICAL	
Battery Status Charging Disable Alert for 12 hours Battery Audible Alert I Enable	The system i status and he	s designed to ealth informati	provide emerge on about the b	ency backup servic attery.	es using a built-in battery pack. This page provid
Battery Audible Alert 🕑 Enable	Battery Statu	us Chargin	g		
	Disable				

- 3. Click **Disable Alert for 12 hours** to turn off the low-battery notification or deselect the **Enable** checkbox to disable the alert permanently.
- 4. Click Save.

# **Configuring VoIP Services**

There is no user-configuration needed for VoIP service. All server and line configuration are performed by your service provider. Refer to Table 5 in the Finding Solutions section if you encounter VoIP services related issues.

iNID User Guide
# **Configuring LAN Devices**

Typically, your Internet service provider automatically assigns and configures a dynamic IP address when your system connects to the Internet. Businesses or power users may use a static address enabling them to run advanced services such as Internet servers and video conferences. The availability of static IP addresses is usually an additional service offered by service providers. In addition, changes from the default behavior of the gateway for private IP addressing may also be used by some users.

Configure these settings ONLY if you are very familiar with computer networking technologies. This section provides instructions to set up your private network that includes:

- Configuring additional network on page 70
- Configuring DHCP on page 72
- Allocating IP addresses on page 75

# **Configuring your LAN Publicly Routed Subnet**

You can create a local network that has broadband network-accessible IP addresses by creating a route from the Internet to the specified public network. This feature is typically used in conjunction with broadband service that provides a range of available IP addresses. Once enabled, the public IP addresses can be assigned to local computers.



**Note:** Set up your LAN publicly routed subnet first if you want to use the public address with your DHCP configuration.

- 1. Open a Web browser and enter http://gateway.2Wire.net in the address line, the Home page opens.
- 2. Click (1), the Broadband Status page opens.

&T U-verse		SWISE.
Iome Services Setting	gs Site Map	
ystem Info Broadband LAN	I Firewall Logs Diagnostic	cs.
Status Link Configuration Mult	icast	
Internet: • Connected DSL Link: • Connected Internet Details		
Broadband Link Type:	Built in modem – VDSL	
Connection Type:	Direct IP (DHCP or Static)	
Current Internet Connection:		
IP Address:	76.193.113.77	
Subnet Mask:	255.255.255.0	
Default Gateway:	76.193.113.1	
Primary DNS:	68.94.156.1	
Secondary DNS:	68.94.157.1	
Host Name:		
Domain:		
MAC Address:	00:1d:5a:5f:db:60	
MTU:	1500	

**3.** Click <u>Link Configuration</u>; the following page opens.

ome Services	Settings	Site Map			
ystem Info Broadba	nd LAN Fir	ewall Logs	Diagnostics		
Status Link Configura	tion Multicast				
Warning Modify to access your b and services run	ing the settings or roadband connecti ning on your privat	n this page can i on. Modification te network.	npact the ability may also affect	of devices on broadband-e	your private netwo nabled applications
Broadband IP Netw	rork				
Broadband IP Netw Upstream MTU: 12	ork 00				
Broadband IP Netv Upstream MTU: 1 Supplementary Net Add Additional Netwo	ork 00 work rk □Enable				
Broadband IP Netw Upstream MTU: 15 Supplementary Net Add Additional Netwo Router Address:	ork 00 work rk Enable				
Broadband IP Netw Upstream MTU: 1 Supplementary Net Add Additional Netwo Router Address: Subnet Mask	oork 00 work tk Enable				

- 1. Change the Upstream Maximum Transmission Unit (MTU), if necessary.
- 2. Select **Enable** to add a secondary network to the broadband WAN interface.
- 3. Enter information in the following fields:
  - Router Address: Enter the router address (this is the router address from the secondary subnet provided by the service provider).
  - **Subnet Mask**: Enter the subnet mask (this is the router mask from the secondary subnet provided by the service provider).
- 4. Select the **Auto Firewall Open** checkbox if you want to automatically disable the firewall for all devices using addresses from this subnet. (By default, the firewall protection is enabled.)



**Note:** You can individually enable the firewall on a per device basis (refer to Allocating IP Addresses on page 75) or on a per application basis using the Firewall option (refer to Allowing all Applications (DMZplus) on page 52).

5. Click Save.

# **Configuring DHCP**

Dynamic Host Configuration Protocol (DHCP) allows for dynamic allocation of network addresses and configuration to newly attached hosts. The i3802V can be both DHCP client and DHCP server. The i3802V acts as a client when it communicates to your service provider over the Internet using the IP address. For this communication, you cannot modify the related DHCP settings. The i3802V is a DHCP server to your local network devices such as the i38HG and computers connecting to it.

To configure the default DHCP information used as a local server:

1. Open a Web browser and enter *http://gateway.2Wire.net* in the address line; the *Home* page opens (Figure 13).

<b>™</b>	verse					
lome	Services	Settings	Site Map			
Summ	ary Broadband ↓ 27232Kbp ↑ 2000Kbps ng - Emerger	s Wir Netw Nam Dori	eless vork e s Backup	Firewall Status Enabled	Ņ	<b>i3802V</b> Serial Number: 450712000169
Battery I Home	Power Level Critic	cal <u>Battery Info</u> vices				
Battery I Home	Power Level Critic Network Dev 2.168.1.64	cal <u>Battery Info</u> vices <u>Device D</u>	<u>etails</u>			
Battery I Home I 192 I DLc I Dor	Power Level Critic Network Dev 2.168.1.64 ok <u>Acces</u> risL <u>Acces</u>	xices vices <u>Device D</u> <u>SS Files</u> <u>Device D</u> <u>Device D</u> <u>Dev</u>	etails etails etails			
Battery I Home I 192 DLC DO Top N Wireless	Power Level Critic Network Dev 2.168.1.64 ok Access risL Access etworking Fe	al <u>Battery Info</u> vices <u>Device D</u> ss Files <u>Device D</u> ss Files <u>Device D</u> eatures - mo	etails etails etails bdify security or se	ettings		
Battery I Home S 192 DLC Dor Top N Wireless Refresh	Power Level Critic Network Dev 1.168.1.64 ok Acces isL Acces etworking Fe your Broadband (	cal <u>Battery Info</u> vices <u>Device D</u> ss Files <u>Device D</u> ss Files <u>Device D</u> eatures - mo <u>Connection</u> - rec	etails etails etails odify security or so	ettings dband connection		
Battery I Home I 192 DLC Dor Top No Wireless Refresh Restart	Power Level Critic Network Dev 2.168.1.64 ok Access etworking Fe s your Broadband for your System	cal <u>Battery Info</u> vices <u>Device D</u> ss Files <u>Device D</u> ss Files <u>Device D</u> eatures <u>- mo</u> <u>- rec</u> - rec	etails etails etails odify security or se connect your broad poot	ettings dband connection		
Battery I Home I 192 Dor Top No Wireless Refresh Home N	Power Level Critic Network Dev 2.168.1.64 ok Access etworking Fe s your Broadband I your System letworking	cal Battery Info vices Device D SS Files Device D SS FILES D	etails etails etails odify security or se connect your broad poot d a computer, sha	ettings dband connection re a file		

Figure 13: Home Page

2. Click <u>Settings</u>; the System Information page opens (Figure 14).

&T U-verse		2WRE
lome Services	Settings Site Map	
ystem Info Broadbar	nd LAN Firewall Logs	Diagnostics
Status Password Dat	e & Time Event Notifications Ba	attery Backup
System Information		
Manufacturer:	2Wire, Inc.	
Model:	i3802V	
Serial Number:	450712000169	
Hardware Version:	2700-100661-002	
Software Version:	6.1.3.21-enh.tm	
Key Code:	52HP-2374-2262-22AT-F2BQ	
First Use Date:	Not Set	
Current Date & Time:	Not Set	
Time Since Last Boot:	0 day 1:08:08	
DSL Modem	2.66.7 SW:68.14_4.10.1	
System Password:	Custom	
Wireless Access Poi	nt	
Manufacturer:	2Wire, Inc.	
Model:	138HG	
Serial Number:	390713000392	
Hardware Version:	2700-000679-003	
Software Version:	6.1.3.14-eval-wifi.tm	
Enabled:	Yes	
System Software Co	mponents	

Figure 14: System Information Page

**3.** Click <u>LAN</u>; a page similar to the following opens, displaying the private network information and LAN devices connected to your network.

&T U-verse			ewire:
Iome Services	Settings S	ite Map	
system Info Broadband	LAN Firev	vall Logs Diagnostics	
Status Wireless Wired I	nterfaces DHCP	IP Address Allocation Statistics	
Private Network Router/Gateway Address	. 192.168.	1.254	
Subnet Mask:	255.255.	255.0	
Private Network DHCP In	fo:		
Range:	192.168.	1.64 - 192.168.1.253	
Allocated	4		
Remaining	186		
Timeout	1440 min	utes	
Interfaces			
Interface Status Act	ive Devices Inac	tive Devices	
+ Ethernet Enabled	1	0	
A HomePNA1 Enabled	0		
- Homer Linubicu	0	0	

4. Click <u>DHCP</u>; the DHCP Configuration page opens.

me Services	Settings Site Map	
stem Info Broadban	d LAN Firewall Log	s Diagnostics
Status Wireless Wired	I Interfaces DHCP IP Address	Allocation Statistics
Warning Modifyin network.	ng the settings on this page car	impact the ability of devices to access your private
OHCP Configuration	1	
DHCP Network Range	If you change the IP address devices on the network.	range, you must renew the DHCP lease for all
	I92.168.1.0 / 255.255.2	55.0 (default)
	0172.16.0.0 / 255.255.0.0	
	○10.0.0.0 / 255.255.0.0	
	○ Configure manually	
	Router Address:	
	Subnet Mask:	
	First DHCP Address:	
	Last DHCP Address	
	cast offer states.	
DHCP Lease Time:	24 hours (24 hours def	ault)
elect Default Addre	ess Allocation Pool for t	ne DHCP Server
Manajara This aslast	differente defende (AN)	
warning: This selection mo lew devices. The default s device getting a public ado for each individual on the '	etting is Private Network. Chan Iress assigned. The recommend IP Address Allocation' page.	used by the DHCP Server for address assignments to ge it only to Public Network when you want every new ation is Private Network. You can change the setting
New Device DHCP Pool		Private Network 🗸

#### Figure 15: DHCP Configuration

- 5. Select Configure manually if you want to set up a range for the DHCP address IP pool.
- 6. Enter information in the following fields:
  - Router Address: This is the IP address of your i3802V used for all communication on your local devices.
  - Subnet Mask: This is the subnet mask used for all communication on your local devices (the default is 255.255.255.0).
  - First DHCP Address: The first IP address in the DHCP address pool that you will be distributing over the private network.
  - Last DHCP Address: The last IP address in the DHCP address pool that you will be distributing over the private network.
- **7.** Enter a numerical value in the **DHCP Lease Time** field. This value represents the number of hours you can use the assigned IP address before the DHCP lease expires.
- 8. Select a public IP address pool that is assigned via DHCP on the local area network.



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

9. Click Save.

# **Allocating IP Addresses**

You can allocate specific IP addresses to devices that are running in the DHCP mode, and map devices to particular static (public) or private IP addresses. For Internet public hosting of application or servers associated with static 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.



**Note:** Alternatively, you may also statically configure public or private IP addresses on the device themselves. Statically addressed device addresses override settings made on this page.

1. Open a Web browser and enter http://gateway.2Wire.net in the address line, the Home page opens (Figure 13).

at U-	/erse					<b>2</b> WJ	SE.
ome	Services	Settings	Site Map				-
Summa	ary						
	Broadband	🔊 Wir	eless 🔽	Firewall		i3802V	
	<ul> <li>27232Kbp</li> <li>2000Kbps</li> </ul>	s Netv Nam Dori	vork le s	Status Enabled	4	Serial Number: 45071200016	59
Warnir Battery P	ng - Emerger 'ower Level Critic	ncy Battery H al <u>Battery Info</u>	Backup				
Warnin <sup>Battery P</sup> Home I	ng - Emerger Iower Level Critic Network Dev	ncy Battery H al <u>Battery Info</u> vices	Backup				
Warnin Battery P Home I S 192.	ng - Emerger Yower Level Critic Network Dev .168.1.64	ncy Battery F al <u>Battery Info</u> vices <u>Device D</u>	Backup etails				_
Warnin Battery P Home J S 192. S DLoi S Dori	ng - Emerger wwer Level Critic Network Dev .168.1.64 k Acces isL Acces	ancy Battery F al <u>Battery Info</u> vices <u>Device D</u> s Files <u>Device D</u> s Files <u>Device D</u>	Backup Intails Intails				-
Warnin Battery P Home I © 192. © DLoi © Dori Cop Ne	ng - Emerger ower Level Critic Network Dev .168.1.64 k Acces isL Acces etworking Fe	ncy Battery F al <u>Battery Info</u> vices <u>Device D</u> s Files <u>Device D</u> s Files <u>Device D</u> vatures	Backup etails etails				
Warnin Battery P Home J 192. S Dori S Dori Cop Ne <u>Wireless</u>	ng - Emerger ower Level Critic Network Dev .168.1.64 k Acces isL Acces etworking Fe	ncy Battery F al <u>Battery Info</u> vices <u>Device D</u> s Files Device D s Files Device D a trues - mo	Backup etails etails etails odify security or so	ettings			
Warnin Battery P Home J S 192. S DLoi S Dori Cop Ne <u>Wireless</u>	ng - Emerger lower Level Critic Network Dev .168.1.64 k Acces isL Acces etworking Fe	ncy Battery F al <u>Battery Info</u> vices <u>Device D</u> s Files Device D s Files Device D a trues - mo connection - rec	Backup	ettings dband connection			
Warnin Battery P Home J Dori Op Ne Vireless Refresh y Restart y	ng - Emerger lower Level Critic Network Dev .168.1.64 k Acces isL Acces etworking Fe your Broadband ( your System	ncy Battery F al Battery Info vices s Files Device D s Files Device D a trues connection = rec - rec	Backup	ettings dband connection			
Warnin Battery P Home J S 192. S DLoi S Dori Cop Ne <u>Wireless</u> <u>Refresh y</u> <u>Restart y</u>	ng - Emerger ower Level Critic Network Dev .168.1.64 k Acces isL Acces etworking Fe your Boadband ( your System etworking	ncy Battery F al Battery Info vices s Files Device D s Files Device D s Files Device D a trues - mo connection - rec - rel - fin	Backup	ettings dband connection ure a file			

Figure 16: Home Page

2. Click <u>Settings</u>; the System Information page opens (Figure 14).

Broadband     LAN     Firewall     Logs     Diagnostics       Status     Password     Date & Time     Event Notifications     Battery Backup       system Information	ome Services	Settings Site Map	
Status       Password       Date & Time       Event Notifications       Battery Backup         System Information	ystem Info Broadb	and LAN Firewall Logs Diagnostics	
Average response back a nine brenchonneauon's backup backup	Status Password D	ate & Time Event Notifications Rattery Rackup	
Anufacturer:2Wire, Inc.Manufacturer:2Wire, Inc.Model:13802VSerial Number:450712000169Hardware Version:2700-100661-002Software Version:6.1.3.21-enh.tmSey Code:52HP-2374-2262-22AT-F28QFirst Use Date:Not SetSurrent Date & Time:Not SetSind Seiter Last Boot:0 day 1:08:08Sat Modem:2.66.7 SW:68.14_4.10.1		are a time Event notifications battery backup	
Wanufacturer:         2Wire, Inc.           Manufacturer:         13802V           Wodel:         13802V           Serial Number:         450712000169           Hardware Version:         2700-100661-002           Software Version:         6.1.3.21-enh.tm           Key Code:         52HP-2374-2262-22AT-F2BQ           First Use Date:         Not Set           Surrent Date & Time:         Not Set           State Last Boot:         0 day 1:08:08           Sat Modem         2.66.7 SW:68.14_4.10.1			
Manufacturer:         2Wire, Inc.           Model:         13802V           Serial Number:         450712000169           Jardware Version:         2700-100661-002           Software Version:         6.1.3.21-enh.tm           Key Code:         52HP-2374-2262-22AT-F28Q           First Use Date:         Not Set           Surrent Date & Time:         Not Set           Since Last Boot:         0 day 1:08:08           Stat Modem         2.66.7 SW:68.14_4.10.1	System Informatio	n	
Model:         i3802V           Serial Number:         450712000169           Jardware Version:         2700-100661-002           Software Version:         61.3.21-enh.tm           Gey Code:         52HP-2374-2262-22AT-F28Q           First Use Date:         Not Set           Surrent Date & Time:         Not Set           Fine Since Last Boot:         0 day 1:08:08           St Modem         2.66.7 SW:68.14_4.10.1	Manufacturer:	2Wire, Inc.	
Serial Number:         450712000169           Hardware Version:         2700-100661-002           Software Version:         6.1.3.21-enh.tm           Key Code:         52HP-2374-2262-22AT-F2BQ           Tist Use Date:         Not Set           Current Date & Time:         Not Set           Time Since Last Boot:         0 day 1:08:08           SL Modem         2.66.7 SW:68.14_4.10.1	Model:	i3802V	
Hardware Version:     2700-100661-002       Software Version:     6.1.3.21-enh.tm       Key Code:     52HP-2374-2262-22AT-F2BQ       First Use Date:     Not Set       Current Date & Time:     Not Set       Time Since Last Boot:     0 day 1:08:08       2SL Modem     2.66.7 SW:68.14_4.10.1	Serial Number:	450712000169	
Software Version:         6.1.3.21-enh.tm           Key Code:         52HP-2374-2262-22AT-F2BQ           First Use Date:         Not Set           Current Date & Time:         Not Set           Fime Since Last Boot:         0 day 1:08:08           DSL Modem         2.66.7 SW:68.14_4.10.1	Hardware Version:	2700-100661-002	
Key Code:         52HP-2374-2262-22AT-F2BQ           First Use Date:         Not Set           Current Date & Time:         Not Set           Fime Since Last Boot:         0 day 1:08:08           DSL Modem         2.66.7 SW:68.14_4.10.1	Software Version:	6.1.3.21-enh.tm	
First Use Date:     Not Set       Current Date & Time:     Not Set       Fime Since Last Boot:     0 day 1:08:08       DSL Modem     2.66.7 SW:68.14_4.10.1	Key Code:	52HP-2374-2262-22AT-F2BQ	
Current Date & Time:         Not Set           Fime Since Last Boot:         0 day 1:08:08           OSL Modem         2.66.7 SW:68.14_4.10.1	First Use Date:	Not Set	
Time Since Last Boot:         0 day 1:08:08           OsL Modem         2.66.7 SW:68.14_4.10.1	Current Date & Time:	Not Set	
<b>DSL Modem</b> 2.66.7 SW:68.14_4.10.1	Time Since Last Boot	0 day 1:08:08	
	DSL Modem	2.66.7 SW:68.14_4.10.1	
System Password: Custom	System Password:	Custom	
	Wireless Access Po	pint	
Vireless Access Point	Manufacturer:	2Wire, Inc.	
Vireless Access Point Vanufacturer: 2Wire, Inc.	Model:	138HG	
Vireless Access Point Manufacturer: 2Wire, Inc. Model: 138HG	Serial Number:	390713000392	
Vireless Access Point Manufacturer: 2Wire, Inc. Model: 138HG serial Number: 390713000392	Hardware Version:	2700-000679-003	
Vireless Access Point Vanufacturer: 2Wire, Inc. Vodel: 138HG Vodel: 390713000392 Vodel: 2700-000679-003	Coffuero Marcioni	6.1.3.14-eval-wifi.tm	
Vireless Access Point Vanufacturer: 2Wire, Inc. Vodel: 138HG Serial Number: 390713000392 Version: 2700-000679-003 Software Version: 6.1.3.14-eval-wifi.tm	software version.		

Figure 17: System Information Page

**3.** Click <u>LAN</u>; a page similar to the following opens, displaying the private network information and LAN devices connected to your network.

T&T U-verse			ewire:
Home Services	Settings	Site Map	
System Info Broadband	LAN F	irewall Logs Diagnostics	
Status Wireless Wired I	Interfaces DH	ICP IP Address Allocation Statistic	s
Private Network Router/Gateway Address	:: 192.1	68.1.254	
Subnet Mask:	255.2	55.255.0	
Private Network DHCP In	ifo:		
Range:	192.1	68.1.64 - 192.168.1.253	
Allocated	4		
Remaining	186		
Timeout	1440	minutes	
Interfaces			
Interface Status Act	tive Devices	nactive Devices	
+ Ethernet Enabled	1	0	
ᅌ HomePNA1 Enabled	0	0	

**4.** Click <u>IP Address Allocation</u>; a page similar to the following opens, displaying the devices in your network.

ome Service	es Settings	Site Map	
ystem Info Broa	idband LAN	Firewall Logs	Diagnostics
Status Wireless	Wired Interfaces	DHCP IP Address	Allocation Statistics
Public-Private I	NAT Mappings	and Device II	? Allocation
This section allows y DHCP mode, and ma	ou to configure the o devices to particul	system to allocate ar static or public	specific IP addresses to devices that are running in IP addresses, also known as NAT mappings.
Alternately, you may device addresses will	also statically assig override settings m	n public IP address ade on this page.	es on the devices themselves. Statically addressed
For each device on th a desired IP Address Additionally, for Inte	e private network, y for the DHCP server met public hosting	ou may override th to issue to the dev of applications or s	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. ervers associated with static or public IP addresses,
For each device on the a desired IP Address Additionally, for Inter you can map a device yool. The default pub Device : DLok	e private network, y for the DHCP server rnet public hosting e to a specific public lic IP device mappir	You may override th to issue to the dev of applications or s fixed IP address o ng is to the Router	e default DHCP server address, and manually specify vice, or specify an alternate pool to issue from. ervers associated with static or public IP addresses, r to the next unassigned address from the public WAN IP address.
For each device on th a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address :	le private network, y for the DHCP server rnet public hosting to a specific public lic IP device mappir 192.168.1.67	You may override th to issue to the dev of applications or s fixed IP address o ng is to the Router	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. ervers associated with static or public IP addresses, r to the next unassigned address from the public WAN IP address.
For each device on th a desired IP Address Additionally, for Inte you can map a device pool. The default put <b>Device : DLok</b> Current Address : Device Status :	ie private network, y for the DHCP server rnet public hosting to a specific public olic IP device mappin 192.168.1.67 Connected DHCF	You may override th to issue to the dev of applications or s fixed IP address o ng is to the Router	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. ervers associated with static or public IP addresses, r to the next unassigned address from the public WAN IP address.
For each device on th a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall:	ie private network, y for the DHCP server rnet public hosting to a specific public olic IP device mappin 192.168.1.67 Connected DHCF Enabled v	You may override th to issue to the dev of applications or s fixed IP address o ng is to the Router	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. ervers associated with static or public IP addresses, r to the next unassigned address from the public WAN IP address.
For each device on th a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall: Address Assignmen	ie private network, y for the DHCP server rnet public hosting to a specific public lic IP device mappin 192.168.1.67 Connected DHCF Enabled v t : Private from pool	You may override the to issue to the dev of applications or s fixed IP address o ng is to the Router 192.168.1.0	e default DHCP server address, and manually specify vice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, r to the next unassigned address from the public WAN IP address.
For each device on the a desired IP Address Additionally, for Inte you can map a device pool. The default pub <b>Device : DLok</b> Current Address : Device Status : Firewall: Address Assignmen WAN IP Mapping :	I private network, y for the DHCP server rnet public hosting to a specific public lic IP device mappir 192.168.1.67 Connected DHCf Enabled V t : Private from pool: Router WAN IP a	rou may override th to issue to the dev of applications or s f fixed IP address o ng is to the Router 192.168.1.0	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, r to the next unassigned address from the public WAN IP address.
For each device on th a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall: Address Assignmen WAN IP Mapping : Device : DorisL	ie private network, y for the DHCP server rnet public hosting to a specific public lic IP device mappin 192.168.1.67 Connected DHCf Enabled v t : Private from pool Router WAN IP a	rou may override th to issue to the dev of applications or s fixed IP address o ng is to the Router 192.168.1.0	e default DHCP server address, and manually specify vice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, or to the next unassigned address from the public WAN IP address.
For each device on the a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall: Address Assignmen WAN IP Mapping : Device : DorisL Current Address :	In private network, y for the DHCP server rnet public hosting i to a specific public lic IP device mappin 192.168.1.67 Connected DHCF Enabled I Private from pool: Router WAN IP a 192.168.1.66	rou may override th to issue to the dev of applications or s fixed IP address o ng is to the Router 192.168.1.0	e default DHCP server address, and manually specify vice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, or to the next unassigned address from the public WAN IP address.
For each device on the a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall: Address Assignmen WAN IP Mapping : Device : DorisL Current Address : Device Status :	In private network, y for the DHCP server rnet public hosting i to a specific public lic IP device mappin 192.168.1.67 Connected DHCF Enabled I Private from pool: Router WAN IP a 192.168.1.66 Connected DHCF	rou may override th to issue to the dev of applications or s fixed IP address o ng is to the Router 192.168.1.0	e default DHCP server address, and manually specify vice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, or to the next unassigned address from the public WAN IP address.
For each device on the a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall: Address Assignmen WAN IP Mapping : Device : DorisL Current Address : Device Status : Firewall:	ie private network, y for the DHCP server rnet public hosting i to a specific public lic IP device mappir 192.168.1.67 Connected DHCF Enabled I Private from pool: Router WAN IP a 192.168.1.66 Connected DHCF Enabled Enabled	rou may override th to issue to the dev of applications or s fixed IP address o ng is to the Router 192.168.1.0	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, or to the next unassigned address from the public WAN IP address.
For each device on the a desired IP Address Additionally, for Inte you can map a device pool. The default put Device : DLok Current Address : Device Status : Firewall: Address Assignmen WAN IP Mapping : Device : DorisL Current Address : Device Status : Firewall: Address Assignmen	ie private network, y for the DHCP server rnet public hosting to a specific public lic IP device mappir 192.168.1.67 Connected DHCF Enabled 192.168.1.66 Connected DHCF Enabled 192.168.1.66 Connected DHCF Enabled T: Private from pool:	rou may override th to issue to the dev of applications or s fixed IP address o ng is to the Router 192.168.1.0 v 192.168.1.0 v	e default DHCP server address, and manually specify rice, or specify an alternate pool to issue from. servers associated with static or public IP addresses, or to the next unassigned address from the public WAN IP address.

- 5. Go to the intended device and select the following to override the default DHCP settings:
  - Select the address or address pool from which you want to select an IP address from the WAN IP Mapping drop-down list.
  - Select the specific address or address type to assign from the Address Assignment drop-down list.
- 6. Click Save.

iNID User Guide

# **Finding Solutions**

The i3802V comes with diagnostics tools, such as link test, DSL, IP PING, trace route, DNS query, and so forth. This section provides helpful information to solve common issues. It also provides instructions to view various statistics and logs.

- Connection on page 80
- VoIP on page 82
- iPSU on page 83
- System information on page 83
- Statistics on page 84
- Logs on page 91

## **Table 4: Connection Issues**

Symptoms	Problems	W	nat to Do
The <b>POWER</b> indicator on the i38HG does not light.	Faulty power supply	1.	Verify that the AC power cable is securely connected to the i38HG (Connecting the Power Cable on page 12).
		2.	Ensure that the AC power cable is not plugged in to a switched outlet that is turned off.
		3.	Power up the i38HG with a known good power outlet.
		4.	Call your service provider if the i38HG does not power up with a known good power outlet.
The <b>POWER</b> indicator on the i38HG remains solid red.	System Post Failure	1.	Press the <b>Reset</b> button on the i38HG for 10 seconds.
		2.	Call your service provider if the i38HG does not power up into a normal state.
No connection to the Internet via the Ethernet connection.	No communication between the iNID and i38HG	1.	Check the data cable is properly connected (Connecting the Data Cable on page 11).
		2.	Check the NID, BROADBAND, and SERVICE indicators on the i38HG, they should light green.
		3.	Call your service provider if problem persists.
	Loose Ethernet cable connection	1.	Check the Ethernet cable connection on your computer and i38HG, and make sure that it is securely seated in both ports (Connecting Your Computer to the i38HG on page 12).
		2.	Check the <b>ETHERNET</b> indicator on the i38HG, it should light green.
		3.	Verify that you can connect to the Internet via wireless connection.
		4.	Call your service provider if problem persists.

# Table 4: Connection Issues (Continued)

Symptoms	Problems	w	nat to Do
No connection to the Internet via the wireless connection.	No communication between the iNID and i38HG	1.	Check the data cable is properly connected (Connecting the Data Cable on page 11).
		2.	Check the NID, BROADBAND, and SERVICE indicators on the i38HG, they should light green.
		3.	Check the <b>WIRELESS</b> indicator on the i38HG, it should light green.
		4.	Call your service provider if problem persists.
	Mis-match network name and/ or encryption key	1.	Verify the network name (Setting up the Wireless Network Name on page 25).
		2.	Verify the encryption key (Securing your Wireless Network on page 26).
		3.	View the wireless AP status (Viewing the Wireless AP Statistics on page 86).
		4.	Check the <b>SERVICE</b> indicator on the i38HG, it should light green.
		5.	Call your service provider if problem persists.
Weak wireless signals. Hissing or static sounds.	Radio interference	1.	Change the wireless settings (Customize Private Wireless Settings on page 36).
		2.	Change the access point location (Determining Wireless Access Points Location on page 10).
		3.	Click on the Home page and click <b>Rescan</b> to scan for a new channel.

# Table 4: Connection Issues (Continued)

Symptoms	Problems	What to Do
The <b>BROADBAND</b> indicator blinks green for an extended period of time, then turns solid red.	Broadband connection Failure	Call your service provider if the broadband connection failed to connect after 10 minutes.
The <b>SERVICE</b> indicator lights red.	Broadband service authentication failure	Call your service provider if the broadband connection failed to connect after 10 minutes.

## Table 5: VoIP Services Issues

Symptoms	Problems	What to Do		
No VoIP service	VoIP services are not subscribed.	1.	Check your line status (Viewing VoIP Service Status on page 89).	
		2.	Call your service provider for VoIP service.	
No dial tone.	Service is down.	1.	Check your line status (Viewing VoIP Service Status on page 89).	
		2.	Verify if the phone is in the Active mode.	
			<ul> <li>If yes, click <b>Ring Now</b> to test the ring tone.</li> </ul>	
			<ul> <li>If the phone does not ring, check and make sure that the RJ-11 is securely connected to the phone port.</li> </ul>	
			<ul> <li>If no, call your service provider.</li> </ul>	

# Table 6: The Power Supply Unit Common Issues

Symptoms	Problems	What to Do		
The iPSU emits chirping sound.	The backup battery life is exhausted.	1.	Check to see if the <b>BATTERY</b> indicator on the IPSU is flashing red.	
		2.	Replace the battery (Replacing the Battery on page 60).	
The <b>POWER</b> indicator is flashing red.	Normal behavior.	1.	Flashing red indicates that the power is provided by the backup battery. The <b>POWER</b> button returns to green when the AC power is switched back.	
		2.	If the home is not experiencing a power outage, check to make sure that the iPSU is plugged into a working outlet.	
		3.	No action is required.	

# Table 7: System Information Issues

Symptoms	Problems	What to Do		
Cannot change the i38HG	Incorrect password.	1.	Go to the Home page.	
settings		2.	Click <u>System Password</u> at the bottom of the <i>Home</i> page; the <i>Login</i> page opens.	
		3.	Click <u>I forgot the password</u> ; the <i>Login</i> page opens displaying your password hint.	
		4.	Enter your password and click <b>Submit</b> .	
		5.	Click I still can't remember the password if you still do not remember the password, the Reset System Password page opens.	
		6.	Enter information in all fields.	
		7.	Click Submit.	

# **Viewing Statistics**

This section provides instructions to view the following statistics:

- Wireless access points on page 86
- HPNA coax on page 86
- HPNA phone line on page 87
- DSL bandwidth on page 88
- VoIP on page 89

To access the statistics page:

**1.** Enter *http://gateway.2wire.net*. The user interface *Home* page opens, displaying the aggregate upstream and downstream bandwidths (Figure 18).

Iome	Services	Settings	Site Map			
		0	I			
Summ	arv					
					-	
	Broadband	, SWire	eless 📝	Firewall		iNID i3802V
	27232KDP	Netwo	vork 🤍	Status		13002
	2024Kbps	Nam	e	Enabled		Serial
						31071200000
Warni	ng - Emerger	ncy Battery E	Backup			
Warni	ng - Emergei	ncy Battery E	Backup			
Warni Battery	ng - Emerger Power Level Critic	ncy Battery E	Backup			
Warni Battery	ng - Emerger Power Level Critic	ncy Battery E al <u>Battery Info</u>	Backup			
Warni <sup>Battery</sup>	ng - Emerger Power Level Critic Network Dev	ncy Battery E al <u>Battery Info</u> vices	Backup			
Warni Battery Home	ng - Emerger Power Level Critic Network Dev ok <u>Acces</u>	ncy Battery E al <u>Battery Info</u> rices <u>5 Files</u> <u>Device D</u>	etails			
Warni Battery Home & DLC & 192	ng - Emerger Power Level Critic Network Dev ok <u>Acces</u> 2.168.1.64	al <u>Battery Info</u> rices <u>s Files</u> <u>Device D</u> <u>Device D</u>	etails etails			
Warni Battery Home S DLc S 192 S Dor	ng - Emerger Power Level Critic Network Dev 2.168.1.64 isL Acces	acy Battery E al <u>Battery Info</u> vices <u>s Files</u> <u>Device D</u> <u>Device D</u> s Files <u>Device D</u>	etails etails etails			
Warni Battery Home S DLa S 192 S Dor	ng - Emerger Power Level Critic Network Dev ok <u>Acces</u> 2.168.1.64 risL <u>Acces</u>	acy Battery E al Battery Info vices <u>s Files</u> Device D <u>Device D</u> <u>s Files</u> Device D	etails etails etails			
Warni Battery Home S DLc S 192 S Dor	ng - Emerger Power Level Critic Network Dev ok <u>Acces</u> 1.168.1.64 isL <u>Acces</u>	acy Battery E al Battery Info vices s Files Device D Device D s Files Device D	etails etails			
Warni Battery Home S DLa S 192 S Dor Top N	ng - Emerger Power Level Critic Network Dev ok <u>Acces</u> 1.168.1.64 risL <u>Acces</u> etworking Fe	acy Battery E al <u>Battery Info</u> vices s Files <u>Device D</u> <u>Device D</u> s Files <u>Device D</u> atures	etails etails etails			
Warni Battery Home S DLc S 192 S Dor Top N Wireless	ng - Emerger Power Level Critic Network Dev ok Acces 2.168.1.64 rist Acces etworking Fe	acy Battery E al Battery Info vices s Files Device D Device D s Files Device D atures - mo	etails etails etails etails	tings		
Warni Battery I Home S DLc S 192 S Dor Top N Wireless Refresh	ng - Emerger Power Level Critic Network Dev National Acces C.168.1.64 C.168.1	acy Battery E al Battery Info vices s Files Device D Device D s Files Device D atures - mo connection - rec	etails etails etails etails odify security or set	tings band connection		
Warni Battery I Home S DLc S 192 S Dor Top N <u>Wireless</u> <u>Refresh</u> <u>Restart</u>	ng - Emerger Power Level Critic Network Dev ok Acces 1.168.1.64 isL Acces etworking Fe i your Broadband G your System	acy Battery E al <u>Battery Info</u> vices <u>s Files</u> <u>Device D</u> <u>Device D</u> s Files <u>Device D</u> attures <u>- mo</u> <u>- ret</u>	etails etails etails etails odify security or se connect your broad poot	tings band connection		
Warni Battery I Home S DLc S Do Do Top N <u>Wireless</u> <u>Refresh</u> <u>Restart</u> <u>Home N</u>	ng - Emerger Power Level Critic Network Dev ok Acces 1.168.1.64 isL Acces etworking Fe s your Broadband G your System letworking	acy Battery E al <u>Battery Info</u> vices <u>s Files</u> <u>Device D</u> <u>Device D</u> s Files <u>Device D</u> atures <u>- mo</u> <u>- rec</u> - ret - fin	etails etails etails etails etails edify security or se connect your broad poot d a computer, shar	tings band connection e a file		

Figure 18: The Home Page

2. Click <u>Home Networking</u>; the LAN Status page opens.

&T U-verse		ewire:
ome Services S	ettings Site Map	
ystem Info Broadband	LAN Firewall Logs Diagnostics	5
Status Wireless Wired In	terfaces DHCP IP Address Allocation Statis	tics
Private Network Router/Gateway Address:	192.168.1.254	
Subnet Mask:	255.255.255.0	
Private Network DHCP Inf	o:	
Range:	192.168.1.64 - 192.168.1.253	
Allocated	4	
Remaining	186	
Timeout	1440 minutes	
Interfaces		
Interface Status Acti	ve Devices Inactive Devices	
+ Ethernet Enabled	1 0	
₩ Ethernet Enabled	1 0 0 0	

3. Click <u>Statistics</u>; the page opens displaying the wireless access point information (Figure 19).

T&T U-verse					<b>5</b> MIJ
Home Services	Settings	Site Map			
System Info Broadban	d LAN	Firewall Logs	Diagnosti	cs.	
Status Wireless Wire	d Interfaces E	HCP IP Address All	ocation Stat	istics	
Access Point S/N: 39 Packets transmitted:	9 <b>071300039</b> 5489	2			
Packets received:	4598 2142612				
Bytes received:	111032377				
Error packets transmitted:	119				
Error packets received:	5				
Discards transmitted:	72				
Discards received:	5				

Figure 19: The LAN Statistics Page

#### **Viewing the Wireless AP Statistics**

If you have multiple access points, each one is listed separately. The detailed wireless AP statistics shows the aggregate of all interfaces (that is, HPNA and Ethernet) connected to the AP. This pane shows the total received and transmitted packets and bytes as well as the total errors and discarded packets.



**Note:** The information under the *Private Network* panel is automatically generated.

#### **Viewing the HPNA Coax Statistics**

The HPNA coax statistics shows the IPTV status.

1. Scroll down on the LAN Statistics page until you reach the HomePNA Network (Coax) pane (Figure 20).

HomePNA Network (Coax)

Firmwar	e Vers	ion:	1.7.4 Mar	11 2007										
Firmwar	e Sign	ature:	0f85d7aa1	ad5206773	e4668	8335129	9674							
HPNA P	hysica	l Link:	UP											
Network	Mode:	:	SYNCHRO	ONOUS										
NodelD	MTU	Mac Ad	dress											
1	17000	00:1D:5A:5	5F:E6:89											
3	8192	00:11:E6:0	0:19:71											
2	8192	00:11:E6:0	0:0C:69											
0	9216	00:15:9A:E	39:FC:6C											
4	8192	00:11:E6:0	0:11:96											
Detaile	d Stati	istics (Co	oax)											
HPNA E	thernet	frames ser	nt:		5406	643								
HPNA E	thernet	frames rec	eived:		1957	73								
HPNA E	thernet	bytes sent	:		7259	993882								
HPNA E	thernet	bytes rece	ived:		6199	9685								
HPNA br	badcast	t Ethernet b	iytes sent: frames rece	ived	4021	1								
	ultionet	t Ethornot fr	ramos cont:	veu.	5007	104								
	ultionst	Ethornot fr	rames sent.	(od)	490	34								
HPINA III	uncast		rames recei	ved:	489									
Invalid Le	angin H		net frames :	sent:	0									
	angin H		net frames i	PC amana	0									
	hornet	transmit fr	erved with C	AC enois.	0									
	hemet	transmit ma	arries droppe	au. J.	0									
	nemet	receive trai	mes aroppe	a:	0									
	introl re	equests ser	aiuad:		0/5									
	introl re	equests rec	erved.		0									
	introl re	epiles sent:			0									
HPNA co	introl re	ephes receiv	/ed:		675									
Interfac	е		Local (Coax	:)	F	Remote			Remote		Remote		Remote	
Station	ID		1		4	4			3		2		0	
Mac Ad	dress		00:1D:5A:5	F:E6:89	(	00:11:E6	6:00:1	1:96	00:11:E6:00	:19:71	00:11:E6:0	0:0C:69	00:15:94	:B9:FC
Master			√											
Interval	Start		10:53	11:08	1	10:53	1	1:08	10:53	11:08	10:53	11:08	10:53	11:08
Interval	End		11:08	11:20	1	11:08	1	1:20	11:08	11:20	11:08	11:20	11:08	11:20

Figure 20: The HPNA Coax Statistics Pane

- 2. View the HPNA Physical Link status.
  - Up indicates that the operation is normal.
  - Down indicates that the IPTV is not connected.
- 3. Verify that there are no CRC errors or dropped frames.
- 4. Scroll down to view the detailed information of each interface.

#### **Viewing the HPNA Phone Line Statistics**

The HPNA phone line statistics shows the status of your phone lines and Internet speed throughout your home.

 Scroll down on the LAN Statistics page until you reach the HomePNA Network (Phoneline) pane (Figure 21).

#### HomePNA Network (Phoneline)

Firmware Version:	1.7.4 Mar 11 2007
Firmware Signature:	0f85d7aa1ad5206773e4668335129674
HPNA Physical Link:	UP
Network Mode:	SYNCHRONOUS

#### NodeID MTU Mac Address

1 17000 00:18:58:93:F4:79

Detailed Statistics (Phoneline)

HPNA Ethernet frames sent:	1432
HPNA Ethernet frames received:	1576
HPNA Ethernet bytes sent:	241951
HPNA Ethernet bytes received:	163169
HPNA broadcast Ethernet frames sent:	67
HPNA broadcast Ethernet frames received:	74
HPNA multicast Ethernet frames sent:	5
HPNA multicast Ethernet frames received:	7
Invalid Length HPNA Ethernet frames sent:	0
Invalid Length HPNA Ethernet frames received:	0
HPNA Ethernet frames received with CRC errors:	0
HPNA Ethernet transmit frames dropped:	0
HPNA Ethernet receive frames dropped:	0
HPNA control requests sent:	386
HPNA control requests received:	84
HPNA control replies sent:	84
HPNA control replies received:	386

#### Figure 21: The HPNA Phoneline Statistics Pane

- 2. Scroll down to the HomePNA Network (Phoneline) pane and view the HPNA Physical Link status.
  - Up indicates that the operation is normal.
  - Down indicates that the HPNA phone line is not connected to the i38HG.
- **3.** Verify that there are no CRC errors or dropped frames.

## **Viewing Individual DSL and Aggregate Bandwidth**

- **1.** Enter *http://gateway.2wire.net* on the address line; the user interface *Home* page opens (Figure 18).
- 2. Click the Broadband icon ( ) on the Home page; the Broadband Status page opens.
- **3.** Scroll down the page to view the physical line 1 and physical line 2 detailed information.

DSL Details		
Modem Type:	Built in modem – VDS	iL
Physical Line 1		
DSL Line (Wire Pair):	RJ-11	
Current DSL Connection:		
	Down	Up
Rate:	13616 kbs	920 kbs
Max Rate:	64000 kbs	Not Available
Noise Margin:	37.5 dB	Not Available
Attenuation:	4.0 dB	Not Available
Output Power:	14.3 dBm	-31.0 dBm
Protocol:	G.993.2	
Channel:	Interleaved	
DSLAM Vendor Information	Country: {255} Vendo	r: {CXSY} Specific: {16898
Rate Cap:	64000 kbs	
Attenuation @ 300kHz:	4.0 dB	
Final Receive Gain:	-7.0 dB	Ok
Physical Line 2		
DSL Line (Wire Pair):	RJ-11	
Current DSL Connection:		
	Down	Up
Rate:	13616 kbs	1080 kbs
Max Rate:	64000 kbs	Not Available
Noise Margin:	37.0 dB	Not Available
Attenuation:	4.0 dB	Not Available
Output Power:	14.3 dBm	-31.0 dBm
Protocol:	G.993.2	
Channel:	Interleaved	
DSLAM Vendor Information	Country: {255} Vendo	r: {CXSY} Specific: {16898
Rate Cap:	64000 kbs	
Attenuation @ 300kHz:	4.0 dB	
Final Receive Gain:	-5.0 dB	Ok
Aggregated Information		
DSL Line (Wire Pair):		
Current DSL Connection:		
	Down	Up
Rate:	27232 kbs	2000 kbs
Max Rate:	27232 kbs	Not Available
Protocol	C 993 2	
DSI AM Vandar Information	Country (255) Vander	r (CYSV) Spacific: (16000)
Bate Cap:	27222 kbs	i. (evait sherine: (10988)
Rate Cap.	27232 KUS	



**Note:** The number of physical lines displays is dependent on the number of lines in use.

## **Viewing the VoIP Service Status**

- **1.** Enter *http://gateway.2wire.net* on the address line. The user interface *Home* page opens, displaying the aggregate upstream and downstream bandwidths (Figure 18).
- 2. Click <u>Services</u>; the following page opens.

AT&T U-verse		2)	WIRE'
Home Services	Settings Site Map		
Status Voice			
Click on the tab of th	ne service you are interes	ted in viewing.	

3. Click <u>Voice</u>; the Status page opens.

T&T U-verse				<b>5</b> ਆਂਤ		
Home	Services	Settings	Site Map			
Status	oice					
Status	Line Stats					
Status						
Line Statu	ls:					
Name Stat	us					
Name Stat sip1 Acti	ve					



**Note:** The voice-over-IP service is disabled if you have not subscribed to the service.

**4.** Click <u>Line</u>; the *Lines* page opens, displaying the line status as well as the phone and port numbers associated with each line.

<b>F&amp;T</b> U-verse				2 wir	
Home	Services	Settings	Site Map		
Status	Voice				
State Lines	us <mark>Line</mark> Stats				
Line 1					
Active	Yes				
Phone	Number 4088569	9343			
Port Nu	mber 0				
Locate	Ring I	Now			
Line 2					
Active	Yes				
Phone	Number 4088569	9302			
Port Nu	imber 1				

# **Viewing Logs**

Logs provide an audit trail of activities that are helpful for troubleshooting and diagnostics purposes.

# **Viewing Events Logs**

- **1.** Enter *http://gateway.2wire.net* on the address line; the user interface *Home* page opens, displaying the aggregate upstream and downstream bandwidths (Figure 18).
- 2. Click <u>Settings</u>; the System Information page opens.

<b>&amp;T</b> U-verse		2Wire:
Iome Services	Settings Site Map	
System Info Proadba	nd LAN Eirowall Logs Diagnostics	
System mo Broauba	iu LAIN FITEWall LOGS Diagliostics	
Status Password Da	te & Time Event Notifications Battery Backup	
System Information	1	
bybeenn mitormacior		
Manufacturer:	2Wire, Inc.	
Model:	i3802V	
Serial Number:	450712000169	
Hardware Version:	2700-100661-002	
Software Version:	6.1.3.21-enh.tm	
Key Code:	52HP-2374-2262-22AT-F2BQ	
First Use Date:	Not Set	
Current Date & Time:	Not Set	
Time Since Last Boot:	0 day 1:08:08	
DSL Modem	2.66.7 SW:68.14_4.10.1	
System Password:	Custom	
Wireless Access Poi	nt	
Manufacturer:	2Wire, Inc.	
Model:	138HG	
Serial Number:	390713000392	
Hardware Version:	2700-000679-003	
Software Version:	6.1.3.14-eval-wifi.tm	
Enabled:	Yes	
Crustom Coftware Co		
System Sonware Co	inponents	

**3.** Click <u>Logs</u>; the *Event Log* page opens.

T&T	U-verse		2	WISE.
Home	e Services S	Settings	Site Map	
Systei	m Info Broadband	LAN F	irewall Logs Diagnostics	
Ev	ent Log System Log	Upgrade Log	Firewall Log	
Evei	nt Log			
Clea	Clear	Log		
Clea				
Disp	all all	✓ Submit		
Туре	e Date/Time		Event Description	
INF	2008-04- 08T15:03:56-07:00	fw,fwmon	src=60.172.222.9 dst=76.193.113.77 ipprot=6 sport=60 dport=135 event id: 261	000
INF	2008-04- 08T15:37:27-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:39:32-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:41:37-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:43:42-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:45:47-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:47:52-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:49:57-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:52:02-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:54:07-07:00	igmp	bridge0: querier ver 3 sending general query	



**Note:** The log starts from the oldest to the latest date; that is, the latest log appears at the bottom of the page.

- 4. Click **Clear Log** if you want to minimize the clutter from previous events when you are trying to diagnose a problem.
- 5. Filter the log category from the **Display Filter** drop-down list.
- 6. Click Submit; the page refreshes and displays the logs of your selection.
- 7. View the log.
  - *Type*: The type of the event: *INF* for information, *ERR* for errors, *WRN* for warning, and so forth.
  - Date/Time: The date and time when the event occurs listing from the latest date on the top.
  - Event Description: Includes the source and destination IP addresses as well as their ports, and a brief description of the event.

# **Viewing System Logs**

- **1.** Enter *http://gateway.2wire.net* on the address line; the user interface *Home* page opens, displaying the aggregate upstream and downstream bandwidths (Figure 18).
- 2. Click <u>Settings</u>; the System Information page opens.

<b>f&amp;T</b> U-verse		2Mire:
Home Services	Settings Site Map	]
System Info Broadba	nd LAN Firewall Log	s Diagnostics
Status Passward Da	te 9 Time - Event Natifications	Patters Parkur
Status Password Da		
System Information	1	
byotom mormation	•	
Manufacturer:	2Wire, Inc.	
Model:	i3802V	
Serial Number:	450712000169	
Hardware Version:	2700-100661-002	
Software Version:	6.1.3.21-enh.tm	
Key Code:	52HP-2374-2262-22AT-F2BQ	
First Use Date:	Not Set	
Current Date & Time:	Not Set	
Time Since Last Boot:	0 day 1:08:08	
DSL Modem	2.66.7 SW:68.14_4.10.1	
System Password:	Custom	
T4T 1 4 TO 1		
Wireless Access Poi	nt	
Manufacturer:	2Wire, Inc.	
Model:	138HG	
Serial Number:	390713000392	
Hardware Version:	2700-000679-003	
Software Version:	6.1.3.14-eval-wifi.tm	
Enabled:	Yes	
System Software Co	mponents	
System Software O	mponents	

**3.** Click <u>Logs</u>; the *Event Log* page opens.

T&T	U-verse		2 wire	0
Home	e Services	Settings	Site Map	_
Syster	m Info Broadband	LAN F	irewall Logs Diagnostics	
Ev	ent Log System Log	Upgrade Log	Firewall Log	
Ever	nt Log			
Clea	Clear	Log		
	all	V Submit	1	
Disp	blay Filter		- -	
Туре	e Date/Time		Event Description	
INF	2008-04- 08T15:03:56-07:00	fw,fwmon	src=60.172.222.9 dst=76.193.113.77 ipprot=6 sport=6000 dport=135 event id: 261	
INF	2008-04- 08T15:37:27-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:39:32-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:41:37-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:43:42-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:45:47-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:47:52-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:49:57-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:52:02-07:00	igmp	bridge0: querier ver 3 sending general query	
INF	2008-04- 08T15:54:07-07:00	igmp	bridge0: querier ver 3 sending general query	

4. Click System Log; the System Log page opens.

T&T I	Jverse	2WiR
Home	Services	Settings Site Map
Systen	ı Info Broadban	d LAN Firewall Logs Diagnostics
Eve	nt Log System Log	Upgrade Log Firewall Log
Syste	em Log	
Clea	Log	Clear Log
Selec	t Device	Gateway 💌
Disp	ay Filter	DBG or higher V (All) V Submit
Inser	t Mark in Log	Insert Mark
Туре	Date/Time	Event Description
INF	2008-04- 08T15:03:39-07:00	cwmd: retried session started, server: 'https://cwmp.c01.sbcglobal.net/cwmp/services/CWMP', event code(s): '0 BOOTSTRAP'
WRN	2008-04- 08T15:03:40-07:00	cwmd: authentication has already been tried once and we still don't get in
WRN	2008-04- 08T15:03:40-07:00	cwmd: session failed
INF	2008-04- 08T15:03:40-07:00	cwmd: session will be retried in 213645(ms)
INF	2008-04- 08T15:07:15-07:00	cwmd: retried session started, server: 'https://cwmp.c01.sbcglobal.net/cwmp/services/CWMP', event code(s): '0 BOOTSTRAP'
WRN	2008-04- 08T15:07:16-07:00	cwmd: authentication has already been tried once and we still don't get in
MON	2008-04-	cwmd: session failed
WKIN	08115:07:16-07:00	



**Note:** The log starts from the oldest to the latest date; that is, the latest log appears at the bottom of the page.

- 5. Click **Clear Log** if you want to minimize the clutter from previous events when you are trying to diagnose a problem.
- 6. Select from the Select Device drop-down list the hardware device you want to view.
- 7. Filter the log category from the **Display Filter** drop-down list; the list is updated to your specification.
  - ALM for alarms
  - DBG for debug
  - EMR for emergency
  - ERR for errors
  - FLT for faults
  - NTC for notice
  - *INF* for information
  - WRN for warning
- 8. Click Submit; the page refreshes and displays the logs of your selection.
- 9. Click Insert Mark if you want to insert a delimitation point in the logs.



**Note:** The latest log appears at the bottom of the page; scroll down the page to view your insertion mark.

**10.** View the log.

- Type: The type of events: ERR for errors, INF for information, WRN for warning, and so forth.
- Date/Time: The date and time when the event occurs listing from the latest date on the top.
- Event Description: Includes a brief description of the event.

# **Viewing Firewall Logs**

- **1.** Enter *http://gateway.2wire.net* on the address line; the user interface *Home* page opens, displaying the aggregate upstream and downstream bandwidths (Figure 18).
- 2. Click <u>Settings</u>; the System Information page opens.

&T U-verse		2Wire
ome Services	Settings Site Map	
ystem Info Broadba	and LAN Firewall Logs	5 Diagnostics
Status Password Da	to & Time Event Notifications	atten/ Packup
Status Tassword Da	te a fille Event Notifications E	
System Information	a	
Manufacturer:	2Wire, Inc.	
Model:	i3802V	
Serial Number:	450712000169	
Hardware Version:	2700-100661-002	
Software Version:	6.1.3.21-enh.tm	
Key Code:	52HP-2374-2262-22AT-F2BQ	
First Use Date:	Not Set	
Current Date & Time:	Not Set	
Time Since Last Boot:	0 day 1:08:08	
DSL Modem	2.66.7 SW:68.14_4.10.1	
System Password:	Custom	
Wireless Access Po	int	
Manufacturer:	2Wire, Inc.	
	12840	
Model:	130110	
Model: Serial Number:	390713000392	
Model: Serial Number: Hardware Version:	390713000392 2700-000679-003	
Model: Serial Number: Hardware Version: Software Version:	390713000392 2700-000679-003 6.1.3.14-eval-wifi.tm	

**3.** Click <u>Logs</u>; the *Event Log* page opens.

Г&Т	U-verse		2Wire
Home	e Services	Settings	Site Map
Syster	m Info Broadband	LAN F	Firewall Logs Diagnostics
Ev	ent Log System Log	Upgrade Log	Firewall Log
Ever	nt Log		
Clea	Ir Log	Log	
Disp	all all	v Submit	
Туре	e Date/Time		Event Description
INF	2008-04- 08T15:03:56-07:00	fw,fwmon	src=60.172.222.9 dst=76.193.113.77 ipprot=6 sport=6000 dport=135 event id: 261
INF	2008-04- 08T15:37:27-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:39:32-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:41:37-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:43:42-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:45:47-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:47:52-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:49:57-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:52:02-07:00	igmp	bridge0: querier ver 3 sending general query
INF	2008-04- 08T15:54:07-07:00	igmp	bridge0: querier ver 3 sending general query

4. Click Firewall Log; the Firewall Log page opens.

# AT&T U-verse

•	
A A I	
νu	

Home	Services	Settings	Site Map			
System I	nfo Broadba	nd LAN	Firewall Logs	Diagnostics		
Event	Log System Log	g Upgrade Log	Firewall Log			•
Firewa	ll Log				_	
Clear Lo	g Clear Log					
Da	te and Time	Severity		Details		
2008-0 07:00	4-08T15:03:56-	info sro evi	:=60.172.222.9 dst ent id: 261	t=76.193.113.77 ipprot=6 sport=6000 dport=135		

- 5. Click **Clear Log** if you want to minimize the clutter from previous events when you are trying to diagnose a problem.
- 6. View the log.
  - Date and Time: The date and time when the event occurs listing from the latest date on the top.
  - Severity: ERR for errors, INF for information, WRN for warning, and so forth.
  - Details: Includes the source and destination IP addresses as well as their ports, and a brief description of the event.

#### **Viewing Upgrade Logs**

**1.** Enter *http://gateway.2wire.net* on the address line; the user interface *Home* page opens, displaying the aggregate upstream and downstream bandwidths (Figure 18).

•

2. Click <u>Settings</u>; the System Information page opens.

&T U-verse		20035	
ome Services	Settings Site Map		-
ystem Info Broadbar	nd LAN Firewall Log	s Diagnostics	
Status Password Date	e & Time Event Notifications	Battery Backup	
System Information			
Manufacturer:	2Wire, Inc.		
Model:	i3802V		
Serial Number:	450712000169		
Hardware Version:	2700-100661-002		
Software Version:	6.1.3.21-enh.tm		
Key Code:	52HP-2374-2262-22AT-F2BQ		
First Use Date:	Not Set		
Current Date & Time:	Not Set		
Time Since Last Boot:	0 day 1:08:08		
DSL Modem	2.66.7 SW:68.14_4.10.1		
System Password:	Custom		
Wireless Access Poin	nt		
Manufacturer:	2wire, Inc.		
Model:	200712000202		
Hardware Version	2700-000679-003		
Software Version	6 1 3 14-eval-wifi tm		
Enabled:	Yes		
System Software Co	mponents		

**3.** Click <u>Logs</u>; the *Event Log* page opens.

<b>Γ&amp;T U</b> -	verse			EWIRE'			
Home	Services	Settings	Site Map				
System I	nfo Broadbar	nd LAN F	irewall Logs	Diagnostics			
Event	Log System Log	Upgrade Log	Firewall Log				
E I.	T						
Event	Log						
Clear Log							
	_						
Display	y Filter all	Submit					
Туре	Date/Time		E	ent Description			
INF 08	008-04- 8T15:03:56-07:00	fw,fwmon	src=60.172.222.9 d dport=135 event id:	st=76.193.113.77 ipprot=6 spor 261	t=6000		
INF 08	008-04- 8T15:37:27-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:39:32-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:41:37-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:43:42-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:45:47-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:47:52-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 20	008-04- 8T15:49:57-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:52:02-07:00	igmp	bridge0: querier ver	3 sending general query			
INF 08	008-04- 8T15:54:07-07:00	igmp	bridge0: querier ver	3 sending general query			

**4.** Click <u>Upgrade Log</u>, the *Upgrade Log* page opens, displaying the software versions information.

SWISE.

# AT&T U-verse

Home Services Settings Site Map	_
System Info Broadband LAN Firewall Logs Diagnostics	
Event Log System Log Upgrade Log Firewall Log	
Upgrade Log	
Current Version 6.1.3.21-enh.tm	
Initial Software Version 6.1.3.21-enh.tm	

iNID User Guide

# **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**



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

#### **Location - Electrical Considerations**



**Warning:** The electrical cord of this product must be plugged into a properly grounded outlet or adapter. Failure to comply could result in an electric shock hazard. If you do not know whether your outlet or adapter is properly grounded, you should consult a licensed electrician.



**Caution:** Due to the risk of electrical shock or terminal damage, do not use the terminal 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 power pack into an outdoor outlet or operate the terminal outdoors. It is not waterproof or dust proof, 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 terminal 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 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 and FCC part 68

Manufacturer: 2Wire, Inc.

Model: i38HG

## **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.



**Caution:** 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)

This equipment complies with the Telecommunication Industry Association TIA-968 (FCC part 68) Telecommunication requirements. On the product is a label that contains, among other information, the 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)

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

This equipment uses the following TIA1096 compliance jacks: RJ11C.

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 arrestor 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.

#### **RF Exposure Information**

This device was verified for RF exposure and found to comply with Council Recommendation 1999/519/EC and FCC 0ET-65 RF exposure requirements.

#### **Wi-Fi Only**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. For additional compliance information, please reference FCC ID: PGR2Wi38HG.

#### **MPE/SAR Labeling**

**Warning:** 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 Equipment Under Test (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.

iNID User Guide