



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 machine-readable form without prior written approval.

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

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

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

2Wire 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

Introducing the iNID System

i38HG	1
iPSU	3
i3802V	5
Service Provider Access	5
Subscriber Access	5

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

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 Network

Selecting the Wireless Access Point	24
Setting up the Wireless Network Name	25
Securing your Wireless Network	26
Using the Encryption Key	26
Allowing Devices with MAC Address Filtering	28
Allowing all Devices	28
Allowing Individual Devices	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 Hosted Applications	42
Defining a New Application Profile	43
Adding Multiple Definitions to a Profile	47
Deleting Profiles	50
Allowing all Applications (DMZplus)	52
Stopping DMZplus	54
Customizing Firewall Configuration	55

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 84
 Viewing the Wireless AP Statistics 86
 Viewing the HPNA Coax Statistics 86
 Viewing the HPNA Phone Line Statistics 87
 Viewing Individual DSL and Aggregate Bandwidth 88
 Viewing the VoIP Service Status 89
Viewing Logs 91
 Viewing Events Logs 91
 Viewing System Logs 93
 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.

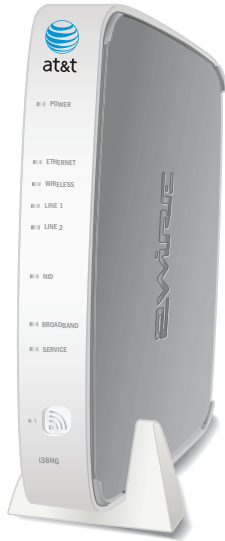


Figure 1: i38HG Indicators

Table 1: i38HG Indicators Description

Indicators	Description
POWER	<p>The POWER indicator turns red when the power is first applied, and changes to green within two minutes of power application.</p> <ul style="list-style-type: none"> • 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 style="list-style-type: none"> • Solid green indicates that a device (such as a computer) is connected to an ETHERNET port. • 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 style="list-style-type: none"> • Solid green indicates that there is wireless activity associated to a specific access point. • Flickering green indicates that there is inbound activity. The flickering of the light is synchronized to the actual data traffic.
LINE 1 and LINE 2	<ul style="list-style-type: none"> • Solid green indicates that the associated VoIP line has been registered with a SIP proxy server. • Flashing green indicates that a telephone is off-hook on the associated VoIP line.
NID	<p>Solid green indicates that the link between the i38HG and i3802V is healthy.</p>



Table 1: i38HG Indicators Description (Continued)

Indicators	Description
BROADBAND	<p>This indicator shows the i3802V VDSL status.</p> <ul style="list-style-type: none"> – Constant green indicates successful broadband connection and no interruption in Internet access. – Flashing green indicates that the i3802 is attempting to establish a broadband connection. – Flashing green and red indicate that the broadband connection has failed to establish for three consecutive minutes. – Red indicates that there is no DSL signal.
SERVICE	<ul style="list-style-type: none"> • Constant green indicates that the i3802V has a WAN IP address from DHCP and the broadband connection is up. • Flashing green indicates that the i3802V is attempting to be authenticated. • Red indicates that the i38HG has failed to receive an IP address assignment from the network.

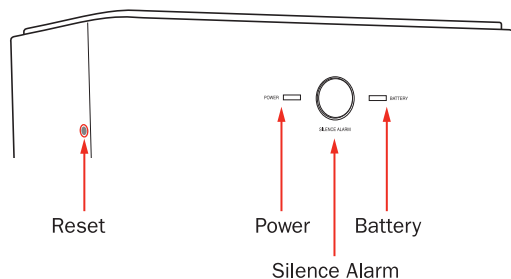
iPSU



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°C to $+50^{\circ}\text{C}$, 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 provider 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	<p>A Reset button is located on the upper left side panel, identifiable by a surrounding red circle. When pressed for up to 9 seconds, the Reset 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.</p> <p>Note: Do not press the Reset 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.</p>
POWER	<ul style="list-style-type: none"> • Solid green indicates that the power supply is running on AC power. • Off indicates that the power supply is not receiving power from either AC or the battery. • Flashing red indicates that the power is provided by the backup battery or that the outside unit is not yet communicating with the iPSU.
SILENCE ALARM — Button	<p>The SILENCE ALARM button is located between POWER and BATTERY indicators.</p> <ul style="list-style-type: none"> • 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.) • 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	<ul style="list-style-type: none"> • 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. <p>Note: The BATTERY indicator works properly only when the i38HG is connected to and communicates with the i3802V.</p>

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).

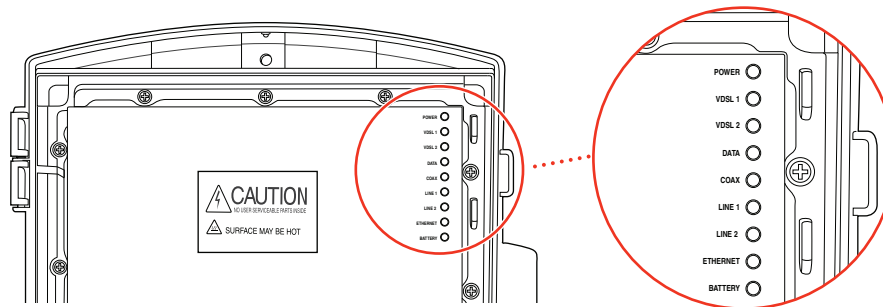


Figure 3: iNID Indicators Location

Table 3: i3802V Outside Unit Indicators Status

Indicators	Description
POWER	<p>The POWER indicator turns red when the power is first applied, and changes to green within two minutes of power application.</p> <ul style="list-style-type: none"> • Constant green indicates that power is on and initialization has been completed successfully. • Flashing green indicates that the iNID is booting. • 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	<p>These two indicators flash after 60 seconds of power application for 1 to 2 minutes and cycle three times.</p> <ul style="list-style-type: none"> • Solid green indicates that the broadband connection is trained. • Flashing green indicates that the broadband connection is being attempted (DSL attempting to synchronize). • 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. <p>Note: The BROADBAND indicator on the i38HG mirrors one or both of the VDSL indicators, whichever is in the “best” state.</p>
DATA	<ul style="list-style-type: none"> • Solid green indicates that an IU (i38HG) is connected via HPNA. • Flashing green indicates that the iNID is attempting IEEE 802.1b/g authentication or attempting to obtain DHCP information. • Red indicates that the iNID failed to be IP connected (no DHCP response, and so forth). <p>Note: This indicator is the mirrored SERVICE indicator on the i38HG.</p>
COAX	<ul style="list-style-type: none"> • 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. • Red indicates that a device failed to be authenticated or successfully connected.
LINE 1 and LINE 2	<ul style="list-style-type: none"> • Solid green indicates that the associated VoIP line has been registered with the network and ready for use. • Flashing green indicates that a telephone is in use on the associated VoIP line. <p>Note: These two indicators are mirrored LINE 1 and LINE 2 indicators on the i38HG.</p>



Table 3: i3802V Outside Unit Indicators Status (Continued)

Indicators	Description
ETHERNET	<ul style="list-style-type: none"> • Solid green indicates that a device (such as a computer) is connected to the ETHERNET port. • 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.
BATTERY	<ul style="list-style-type: none"> • 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.



Installing Your i38HG

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

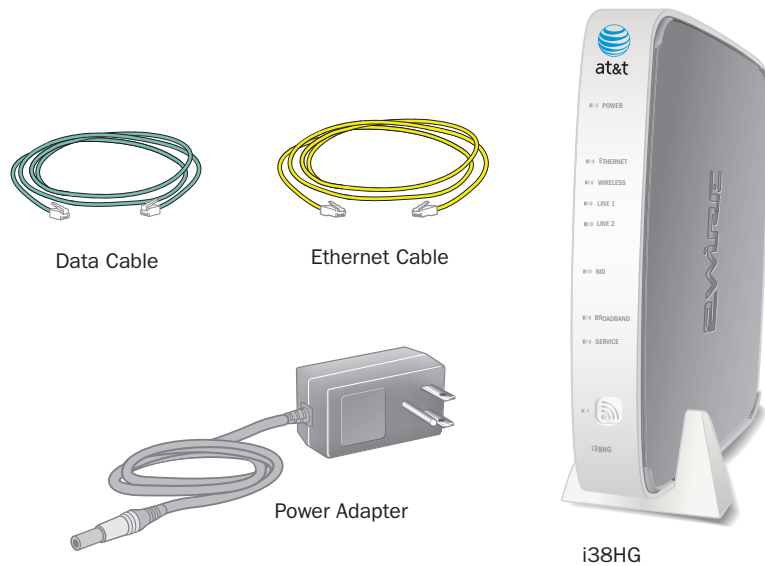


Figure 4: i38HG Package Content



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.

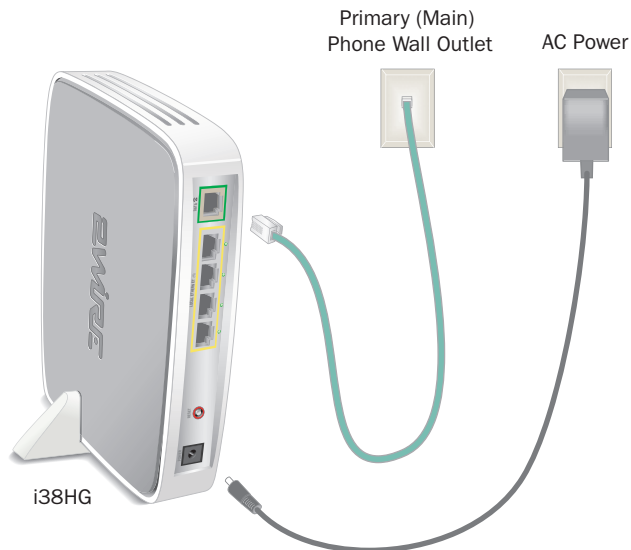


Figure 5: Power and Data Cables Connection

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 a 6-foot Ethernet cable. Use a CAT5 cable if you need additional or longer Ethernet cable.

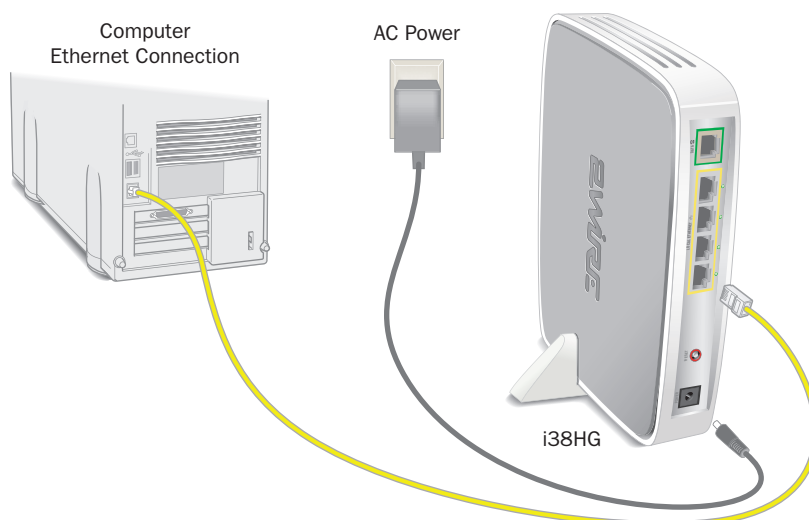


Figure 6: Ethernet Connection

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.

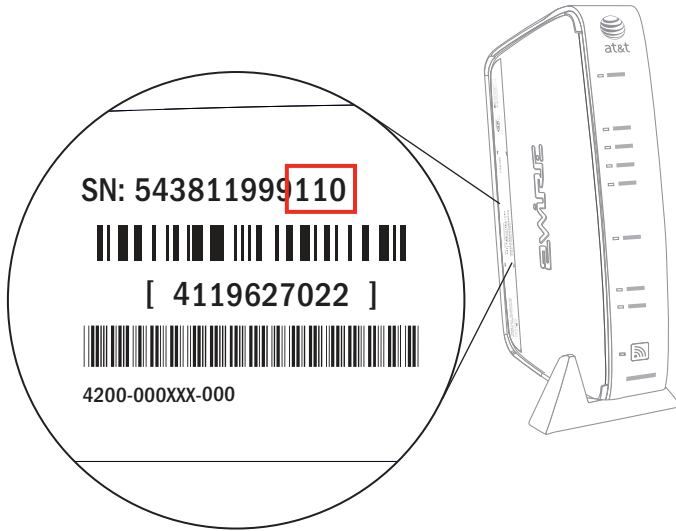


Figure 7: Wireless Network Name and Encryption Key Location

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.

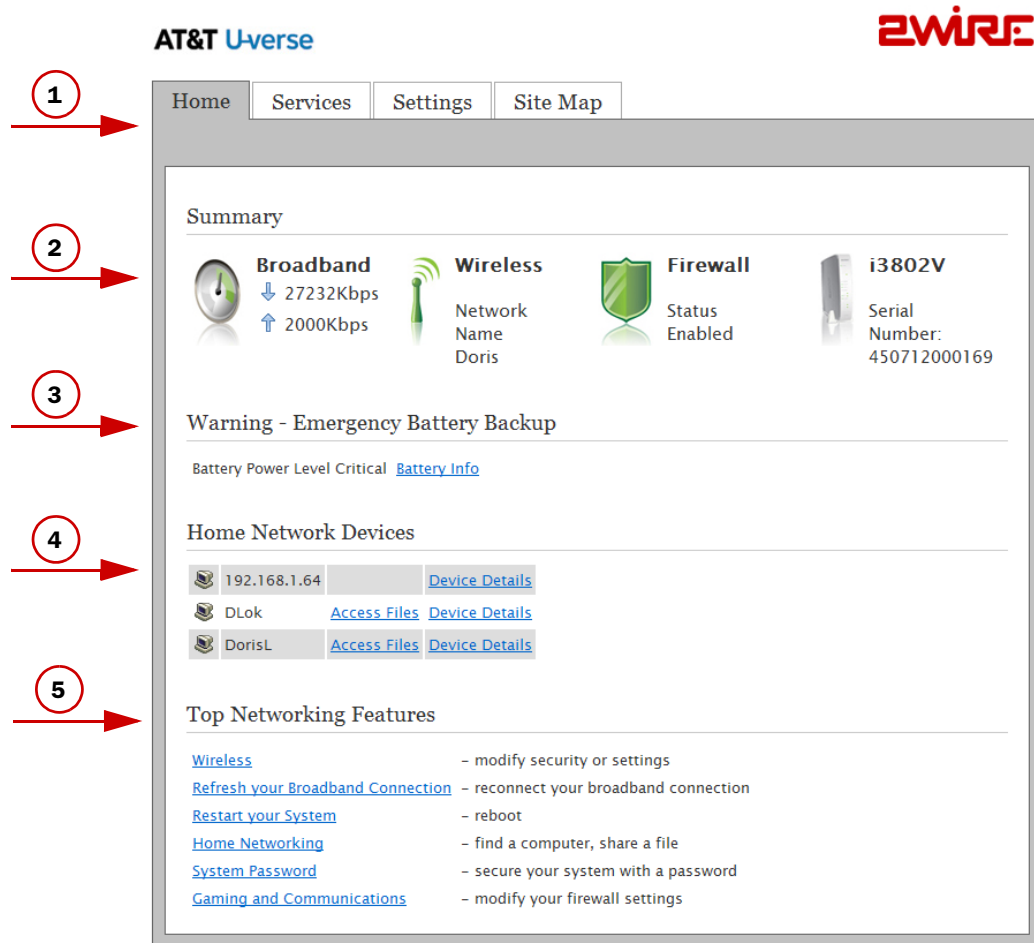


Figure 8: i3802V User Interface

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 [Battery Info](#) 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.

The screenshot displays the AT&T U-verse 2Wire i3802V Home page. At the top, there are navigation tabs for Home, Services, Settings, and Site Map. The main content area is titled 'Summary' and features four status cards: Broadband (showing download and upload speeds), Wireless (showing network name 'Doris'), Firewall (showing status 'Enabled'), and i3802V (showing serial number '450712000169'). Below the summary is a 'Warning - Emergency Battery Backup' section with a 'Battery Info' link. The 'Home Network Devices' section lists three devices: '192.168.1.64', 'DLok', and 'DorisL', each with 'Access Files' and 'Device Details' links. The 'Top Networking Features' section lists several actions: 'Wireless' (modify security or settings), 'Refresh your Broadband Connection' (reconnect broadband), 'Restart your System' (reboot), 'Home Networking' (find computer, share file), 'System Password' (secure system with password), and 'Gaming and Communications' (modify firewall settings).

2. Click [Settings](#) or [System Password](#) from the *Top Networking Features* pane; the *Settings* page opens displaying the system information and more sub-tabs.

AT&T U-verse 2WIRE®

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:	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 Point

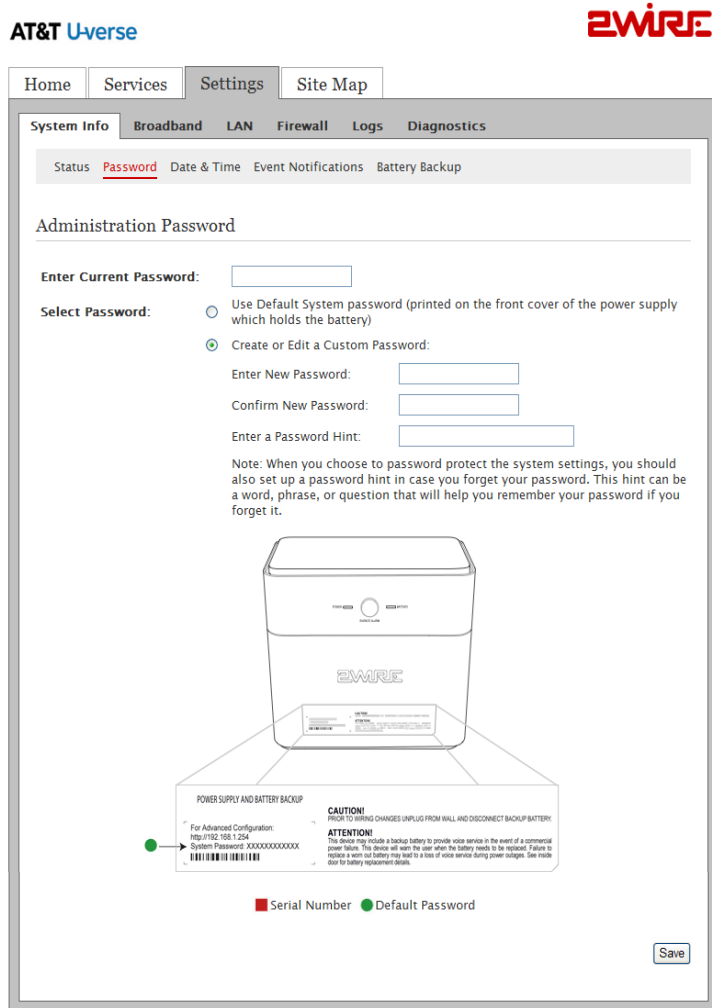
Manufacturer:	2Wire, Inc.
Model:	I38HG
Serial Number:	390713000392
Hardware Version:	2700-000679-003
Software Version:	6.1.3.14-eval-wifi.tm
Enabled:	Yes

System Software Components



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

3. Click [Password](#); the *Administration Password* page opens.



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.

- 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.

- 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.

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

AT&T U-verse 2WIRE®

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:	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:	April 8, 2008
Current Date & Time:	Tuesday, April 8, 2008
	3:12:15 PM
	Pacific Daylight Time
Time Since Last Boot:	0 day 0:22:07
DSL Modem	2.66.7 SW:68.14_4.10.1
System Password:	Custom

←

Wireless Access Point

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.



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:

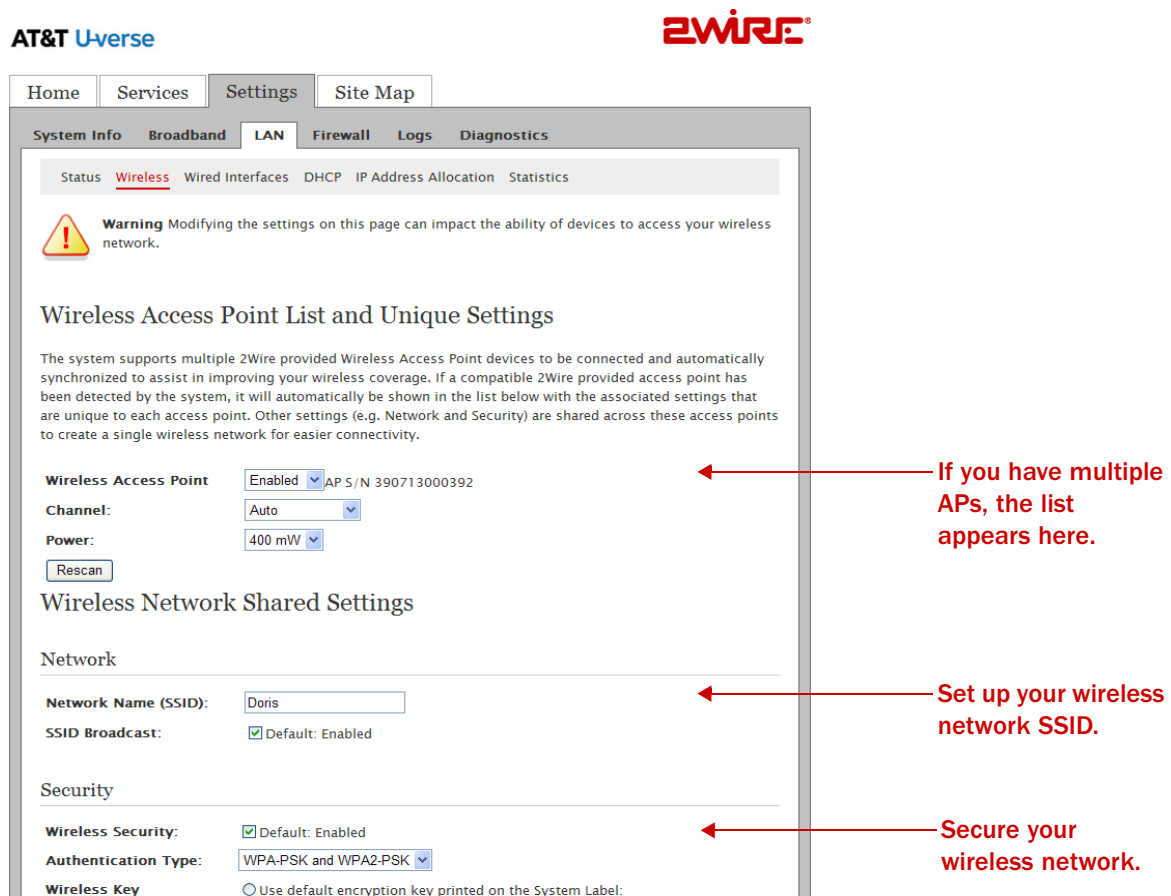
- Select the wireless access point on [page 24](#)
- Set up your wireless network name on [page 25](#)
- Secure your wireless network on [page 26](#)
- Customize personal wireless settings on [page 36](#)
- Configuring Wi-Fi Protection Setup on [page 37](#)

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.



The screenshot shows the AT&T U-verse 2Wire user interface. The main navigation bar includes Home, Services, Settings, and Site Map. The sub-navigation bar includes System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The current page is titled "Wireless Access Point List and Unique Settings" and contains a warning message, a description of the system's wireless capabilities, and configuration options for the wireless access point, network, and security. Red arrows point to specific fields with explanatory text:

- Wireless Access Point:** Enabled (dropdown), AP S/N 390713000392 (text field). *If you have multiple APs, the list appears here.*
- Channel:** Auto (dropdown).
- Power:** 400 mW (dropdown).
- Rescan:** Button.
- Wireless Network Shared Settings:**
 - Network:**
 - Network Name (SSID):** Doris (text field). *Set up your wireless network SSID.*
 - SSID Broadcast:** Default: Enabled
 - Security:**
 - Wireless Security:** Default: Enabled
 - Authentication Type:** WPA-PSK and WPA2-PSK (dropdown). *Secure your wireless network.*
 - Wireless Key:** Use default encryption key printed on the System 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  on 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  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  on the *Home* page; the *Wireless Access Point List and Unique Settings* page opens (Figure 9).
3. Scroll down to the *Security* pane.



← Enter your encryption key.

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. By 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  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.

AT&T U-verse 2WIRE®

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

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

Wireless MAC Filtering

Enable MAC Filtering

Enable

Select Devices to be Allowed or Blocked

Select the devices (by listed name or MAC Address) that you want to block or allow onto your wireless network. If you do not see a particular device in the list, then click the "Rescan For Devices" button or manually add a device using its MAC address.

Note: Newly discovered devices, or manually added devices will automatically appear in the blocked devices list if MAC filtering is enabled.

Allowed Devices: Blocked Devices

<< >>
Rescan For Devices
Delete

Add New MAC Address to List Manually

Enter MAC address



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.



AT&T U-verse **2WIRE®**

Home Services **Settings** Site Map

System Info Broadband **LAN** Firewall Logs Diagnostics

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

Wireless MAC Filtering

Enable MAC Filtering

Enable

Select Devices to be Allowed or Blocked

Select the devices (by listed name or MAC Address) that you want to block or allow onto your wireless network. If you do not see a particular device in the list, then click the "Rescan For Devices" button or manually add a device using its MAC address.

Note: Newly discovered devices, or manually added devices will automatically appear in the blocked devices list if MAC filtering is enabled.

Allowed Devices: Blocked Devices

00:16:6f:0e:87:9c
00:18:8b:a3:1d:32
00:18:f3:e2:cc:a5

Add New MAC Address to List Manually

Enter MAC address



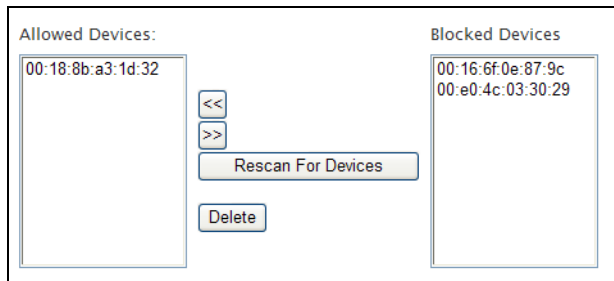
Note: Make sure that the **Enable** checkbox is selected; otherwise, the device will not be allowed.

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](#).

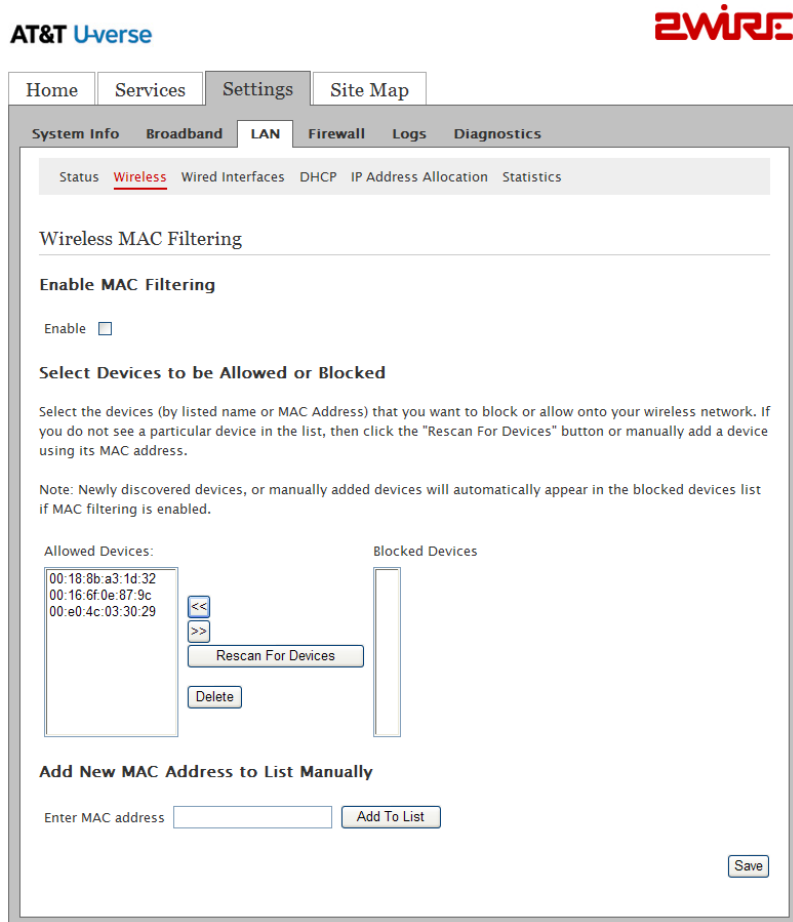
To enable MAC filtering to block all devices:

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.



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.

AT&T U-verse 2WIRE®

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

Status Wireless Wired Interfaces DHCP IP Address Allocation Statistics

Wireless MAC Filtering

Enable MAC Filtering

Enable

Select Devices to be Allowed or Blocked

Select the devices (by listed name or MAC Address) that you want to block or allow onto your wireless network. If you do not see a particular device in the list, then click the "Rescan For Devices" button or manually add a device using its MAC address.

Note: Newly discovered devices, or manually added devices will automatically appear in the blocked devices list if MAC filtering is enabled.

Allowed Devices:		Blocked Devices:
00:18:8b:a3:1d:32	<<	00:16:6f:0e:87:9c
00:16:6f:0e:87:9c	>>	00:18:8b:a3:1d:32
00:e0:4c:03:30:29	Rescan For Devices	00:18:f3:e2:cc:a5
	Delete	

Add New MAC Address to List Manually


Enter MAC address

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](#).

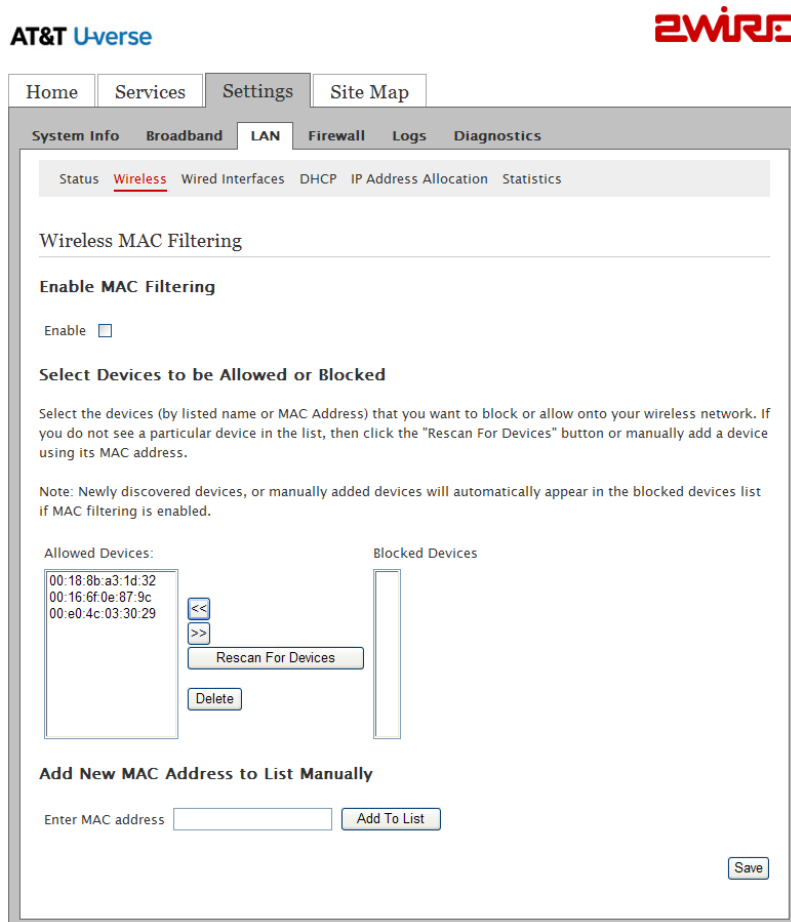
To block individual devices:

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.



The screenshot shows the AT&T U-verse 2Wire user interface. The top navigation bar includes Home, Services, Settings, and Site Map. Below this, there are tabs for System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The 'Wireless' sub-tab is active, showing options for Status, Wired Interfaces, DHCP, IP Address Allocation, and Statistics. The main content area is titled 'Wireless MAC Filtering' and includes an 'Enable MAC Filtering' section with an unchecked 'Enable' checkbox. Below this is a section for 'Select Devices to be Allowed or Blocked' with instructions and a 'Rescan For Devices' button. There are two lists: 'Allowed Devices' containing three MAC addresses (00:18:8b:a3:1d:32, 00:16:6f:0e:87:9c, 00:e0:4c:03:30:29) and an empty 'Blocked Devices' list. A 'Delete' button is located between the lists. At the bottom, there is a section for 'Add New MAC Address to List Manually' with an input field and an 'Add To List' button. A 'Save' button is located in the bottom right corner.

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.



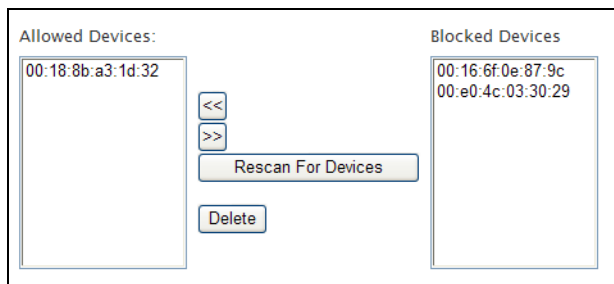
Note: Make sure to click **Save** to keep the transaction persistent; otherwise, the transaction is only a one-time event.

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  on 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): Default: Enabled

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



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](#)




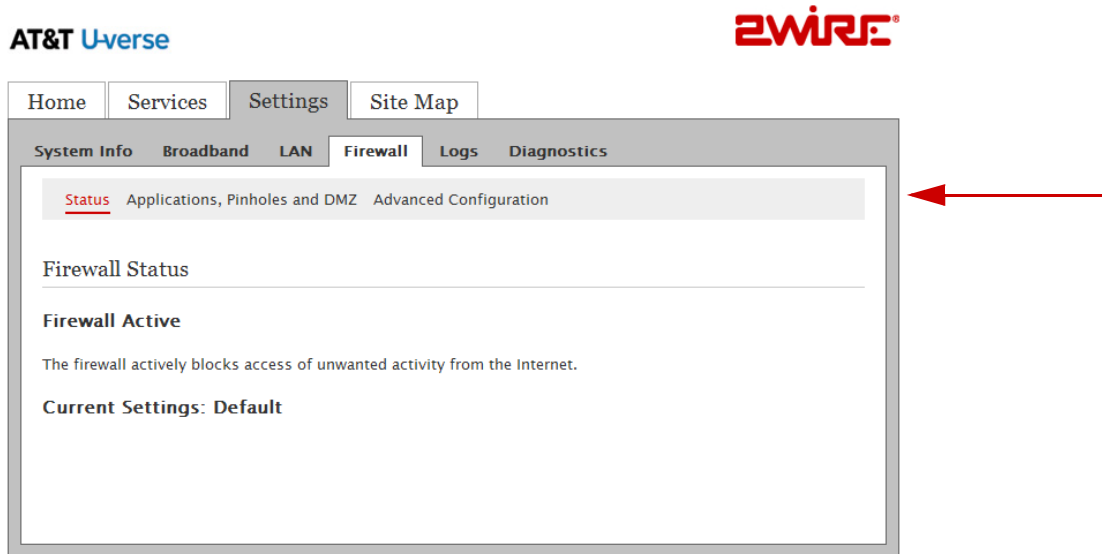
Caution: You should be knowledgeable with the firewall configuration to modify these settings; otherwise, you are exposing your computer to outside attacks.

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.



3. Select [Applications, Pinholes and DMZ](#); a page similar to the following opens showing the computers that are connected to the i38HG/i3802V and the application list.

The screenshot shows the AT&T U-verse web interface for configuring the firewall. The top navigation bar includes 'Home', 'Services', 'Settings', and 'Site Map'. Below this, a secondary navigation bar has 'System Info', 'Broadband', 'LAN', 'Firewall', 'Logs', and 'Diagnostics'. The 'Firewall' tab is active, and the sub-tab 'Applications, Pinholes and DMZ' is selected, leading to an 'Advanced Configuration' page.

The page title is 'Allow device application traffic to pass through firewall'. It explains that the firewall blocks unwanted access and that pinholes can be opened for specific applications. It instructs the user to select a computer and edit its firewall settings.

1) Select a computer
 Choose the computer that will host applications through the firewall.
 You have chosen DLok.
 Links: [Choose DorisL](#),

2) Edit firewall settings for this computer:

- Maximum protection - Disallow unsolicited inbound traffic:
- Allow individual application(s) - Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.
- Allow all applications (DMZplus mode) - Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

A red arrow points to the 'Allow individual application(s)' radio button.

Filter Applications by:

- All applications
- Games
- Audio/video
- Messaging and Internet Phone
- Servers
- Other
- User-defined

Application List:

- Age of Empires
- Age of Kings
- Age of Wonders
- Aliens vs Predator
- Anarchy Online
- Asheron's Call
- Baldur's Gate
- BattleCom
- Battlefield Communicator
- Black and White

Hosted Applications:

[Add a new user-defined application](#)

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.

The screenshot shows the AT&T U-verse user interface. At the top, there are navigation tabs: Home, Services, Settings, and Site Map. Below these are sub-tabs: System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The 'Firewall' sub-tab is selected, and the 'Status' link is highlighted. The main content area shows 'Firewall Status' with a 'Firewall Active' indicator and a message: 'The firewall actively blocks access of unwanted activity from the Internet.' Below this, it says 'Current Settings: Custom' and displays a table of hosted applications.

Device	Allowed Applications	Application Type	Protocol	Port Number(s)	Public IP
DLok	Age of Empires	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77
	Age of Kings	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77
	Age of Wonders	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77

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.

2) Edit firewall settings for this computer:

Maximum protection – Disallow unsolicited inbound traffic:

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

Filter Applications by:	Application List:	Hosted Applications:
<ul style="list-style-type: none"> All applications Games Audio/video Messaging and Internet Phone Servers Other User-defined 	<ul style="list-style-type: none"> Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Black and White Dark Reign Dark Reign 2 Delta Force 	<ul style="list-style-type: none"> Age of Empires Age of Kings Age of Wonders

[Add a new user-defined application](#)

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

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

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.

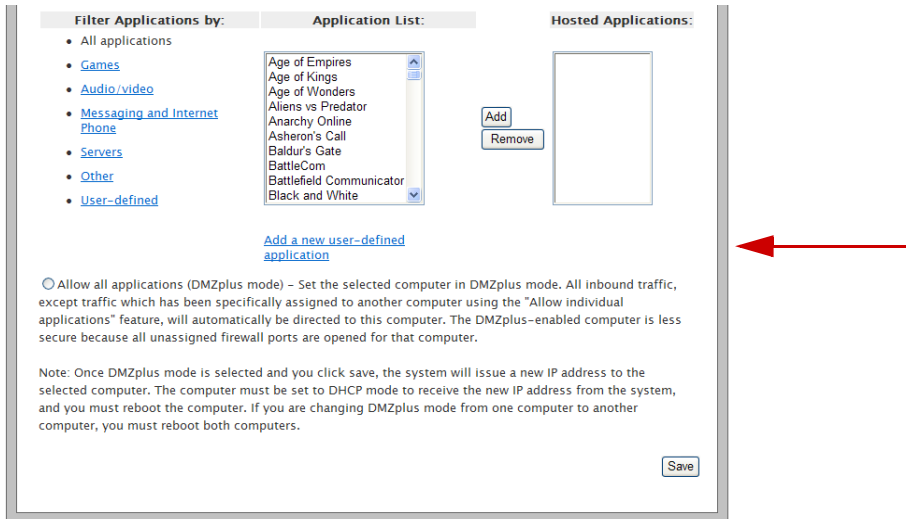
7. Click **Save**; a message appears informing you the status. The application(s) you selected is removed from the *Hosted Applications* panel and returned to the *Application List* panel.

Defining a New Application Profile

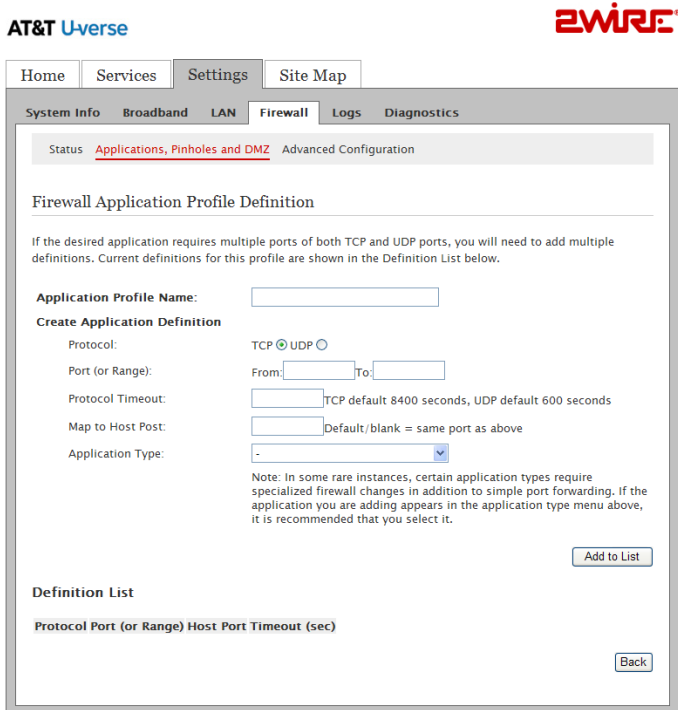
An application profile configures your system's firewall to pass through application-specific data. You can define an application profile that is not included in the *Application List*. This feature is typically used if the application for which you would like to pass through data to a given computer 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 [Applications, Pinholes and DMZ](#); a page opens showing the computers that are connected to your i38HG/i3802V and the application list.



4. Scroll down and click [Add a new user-defined application](#); the *Firewall Application Profile Definition* page opens.



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,


The screenshot shows the AT&T U-verse 2Wire router's web interface. The navigation menu includes Home, Services, Settings, and Site Map. The main menu has System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The Firewall section is active, showing a status message: "Configuration Successful". Below this is the "Firewall Application Profile Definition" section for a profile named "VOX". It includes fields for Protocol (TCP/UDP), Port (or Range) (From/To), Protocol Timeout, Map to Host Post, and Application Type. A note explains that certain application types require specialized firewall changes. An "Add to List" button is present. Below the "Definition List" section, a table shows the current definitions:

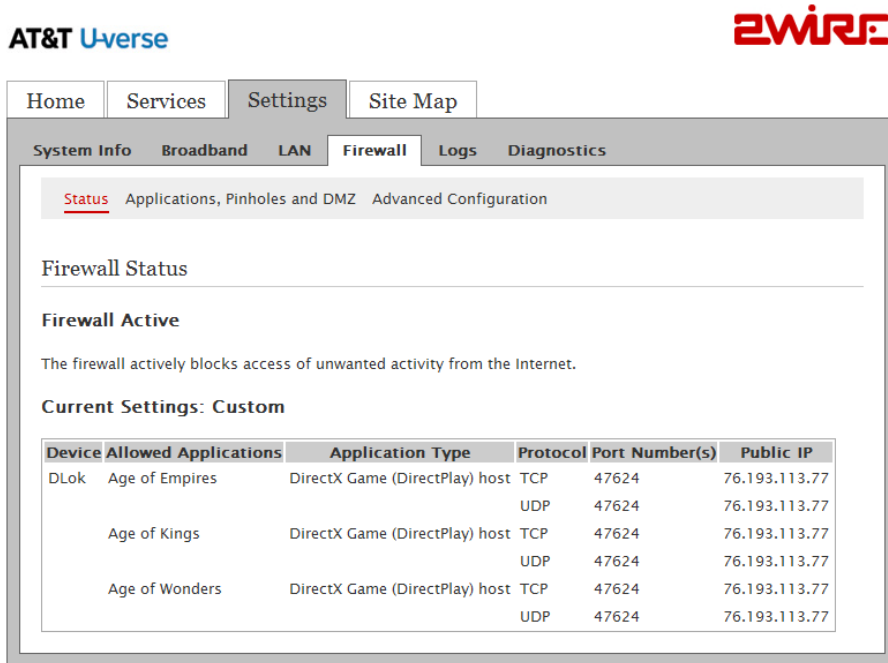
Protocol	Port (or Range)	Host Port	Timeout (sec)	
UDP	500	500	600	Remove

At the bottom right of the interface, there is a "Back" button. A red arrow points to the right side of the interface, near the "Back" button.

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.



The screenshot shows the 2Wire i3802V user interface. At the top, there are logos for AT&T U-verse and 2Wire. Below the logos is a navigation menu with tabs for Home, Services, Settings, and Site Map. Under the Settings tab, there are sub-tabs for System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The Firewall tab is selected, and the page title is 'Status Applications, Pinholes and DMZ Advanced Configuration'. The main content area shows 'Firewall Status' with a sub-section 'Firewall Active' indicating that the firewall is active and blocking unwanted activity. Below this, it shows 'Current Settings: Custom' and a table of allowed applications.

Device	Allowed Applications	Application Type	Protocol	Port Number(s)	Public IP
DLok	Age of Empires	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77
	Age of Kings	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77
	Age of Wonders	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77

3. Select [Applications, Pinholes and DMZ](#); a page opens showing hosted applications.

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


2) Edit firewall settings for this computer:

Maximum protection - Disallow unsolicited inbound traffic:

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

Filter Applications by:	Application List:	Hosted Applications:
<ul style="list-style-type: none">All applicationsGamesAudio/videoMessaging and Internet PhoneServersOtherUser-defined	<ul style="list-style-type: none">Aliens vs PredatorAnarchy OnlineAsheron's CallBaldur's GateBattleComBattlefield CommunicatorBlack and WhiteDark ReignDark Reign 2Delta Force	<ul style="list-style-type: none">Age of EmpiresAge of KingsAge of Wonders

[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 [Edit or delete user-defined application](#); a page similar to the following opens.

AT&T Uverse **ZWIRE®**

Home Services **Settings** Site Map

System Info Broadband LAN **Firewall** Logs Diagnostics

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

Edit or Delete a User-Defined Application

Choose an application from the list below then choose to Edit or Delete the selected application profile.

User defined applications:



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 modify, click **Edit**; the selected profile page opens.

AT&T U-verse
ZWIRE

Home
Services
Settings
Site Map

System Info
Broadband
LAN
Firewall
Logs
Diagnostics

Status Applications, Pinholes and DMZ Advanced Configuration

Firewall Application Profile Definition

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

Application Profile Name: VOX

Create 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.

Definition List

Protocol	Port (or Range)	Host Port	Timeout (sec)	
UDP	500	500	600	<input type="button" value="Remove"/>




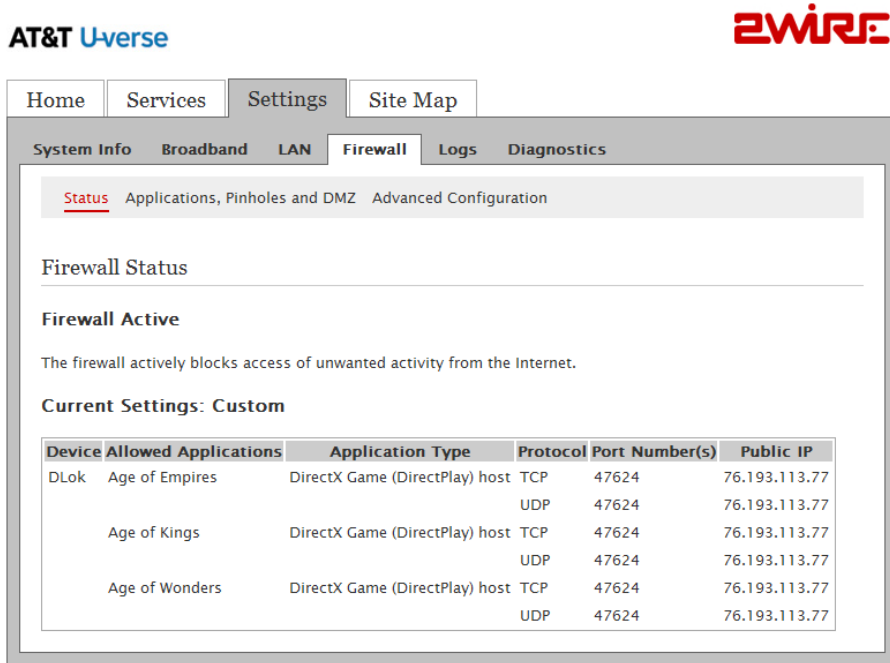
Note: You are prompted to enter your password if one is set up.

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.



3. Select [Applications, Pinholes and DMZ](#); a page opens showing hosted applications.

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

2) Edit firewall settings for this computer:

Maximum protection - Disallow unsolicited inbound traffic:

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

Filter Applications by:	Application List:	Hosted Applications:
<ul style="list-style-type: none"> All applications Games Audio/video Messaging and Internet Phone Servers Other User-defined 	<div style="border: 1px solid gray; padding: 5px;"> Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Black and White Dark Reign Dark Reign 2 Delta Force </div>	<div style="border: 1px solid gray; padding: 5px;"> Age of Empires Age of Kings Age of Wonders </div>
	<input type="button" value="Add"/> <input type="button" value="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 [Edit or delete user-defined application](#); a page similar to the following opens.

AT&T Uverse
ZWIRE

Home Services **Settings** Site Map

System Info Broadband LAN **Firewall** Logs Diagnostics

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

Edit or Delete a User-Defined Application

Choose an application from the list below then choose to Edit or Delete the selected application profile.

VOX

User defined applications:



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 [Applications, Pinholes and DMZ](#); a page opens showing hosted applications.

Home Services Settings Site Map

System Info Broadband LAN Firewall Logs Diagnostics

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

Allow device application traffic to pass through firewall

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

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

1) Select a computer

Choose the computer that will host applications through the firewall

You have chosen DLok
[Choose DorisL](#)
 Enter IP address

2) Edit firewall settings for this computer:

Maximum protection - Disallow unsolicited inbound traffic:
 Allow individual application(s) - Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.

Filter Applications by:	Application List:	Hosted Applications:
<ul style="list-style-type: none"> All applications Games Audio/video Messaging and Internet Phone Servers Other User-defined 	<ul style="list-style-type: none"> Age of Empires Age of Kings Age of Wonders Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Black and White 	<div style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Remove"/> </div>

[Add a new user-defined application](#)

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

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

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




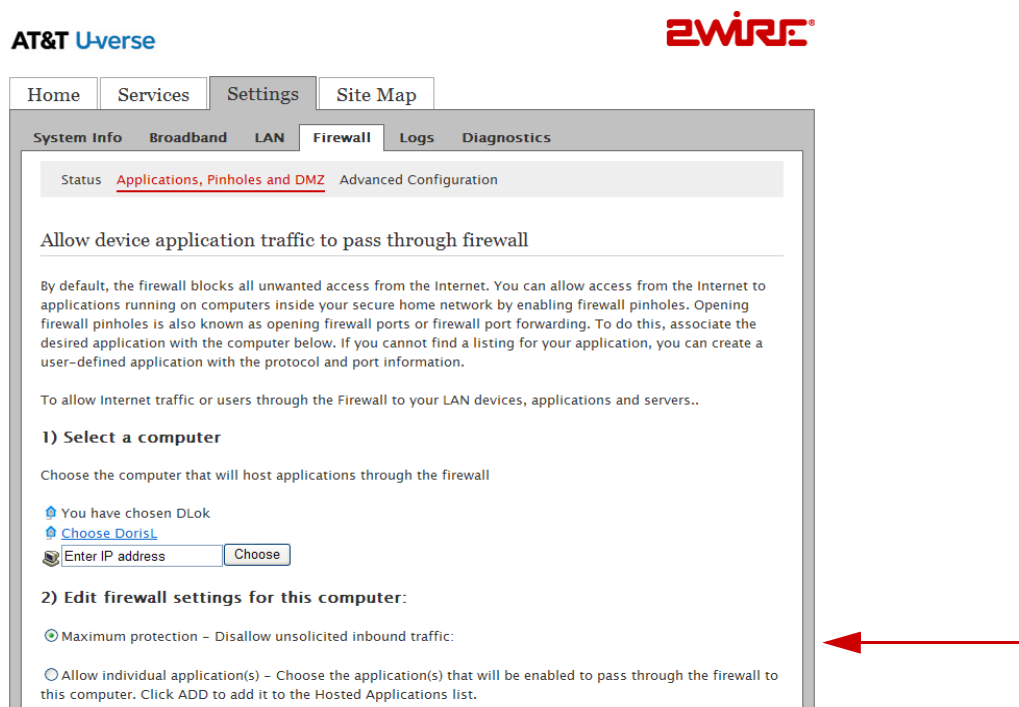
Note: If the computer you want to select is unlisted because it is powered off and the "hide inactive devices" option is enabled; you still can select it as long as it is on the same network and you know its IP address. Replace "Enter IP address" with the intended IP address, then click **Choose**.

- 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.



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.

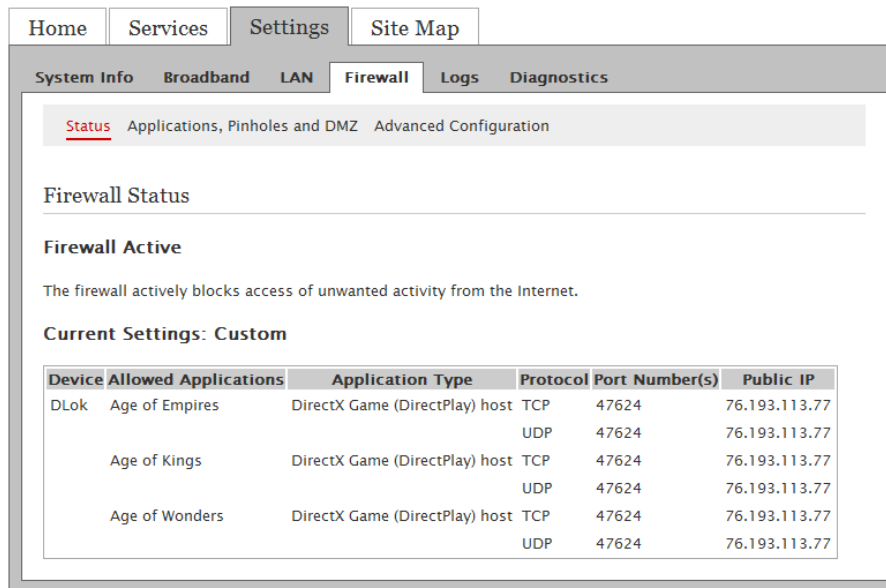
Customizing Firewall Configuration

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.

AT&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: Custom

Device	Allowed Applications	Application Type	Protocol	Port Number(s)	Public IP
DLok	Age of Empires	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77
	Age of Kings	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77
	Age of Wonders	DirectX Game (DirectPlay) host	TCP	47624	76.193.113.77
			UDP	47624	76.193.113.77

3. Click [Advanced Configuration](#); the following page opens displaying the default settings.

The screenshot shows the AT&T U-verse 2Wire web interface. At the top, there are navigation tabs: Home, Services, Settings, and Site Map. Below these are sub-tabs: System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The 'Firewall' sub-tab is selected, and the 'Advanced Configuration' link is highlighted in red. The main content area is titled 'Enhanced Security' and contains several settings:

- Stealth Mode:**
- Block Ping:**
- Strict UDP Session Control:**
- UDP Session Timeout:** seconds (60-43200 seconds, default = 600 seconds)
- TCP Session Timeout:** seconds (300-86400 seconds, default = 86400 seconds)

Below this is the 'Outbound Protocol Control' section, with a note: 'Checking the box ALLOWS the associated traffic type through the firewall.'

- HTTP:**
- HTTPS:**
- FTP:**
- Telnet:**
- SMTP:**
- DNS:**
- NetBIOS:**
- POP3:**
- IMAP:**
- NNTP:**
- IRC:**
- H323:**
- All Other Protocols:**

The 'Inbound Protocol Control' section has one setting:

- NetBIOS:**

The 'Attack Detection' section has several settings:

- Excessive Session Detection:**
- TCP/UDP Port Scan:**
- Invalid Source/Destination IP address:**
- Packet Flood (SYN/UDP/ICMP/Other):**
- Invalid TCP Flag Attacks (NULL/XMAS/Other):**
- Invalid ICMP Detection:**
- Miscellaneous:**

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

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°C to $+50^{\circ}\text{C}$, 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).

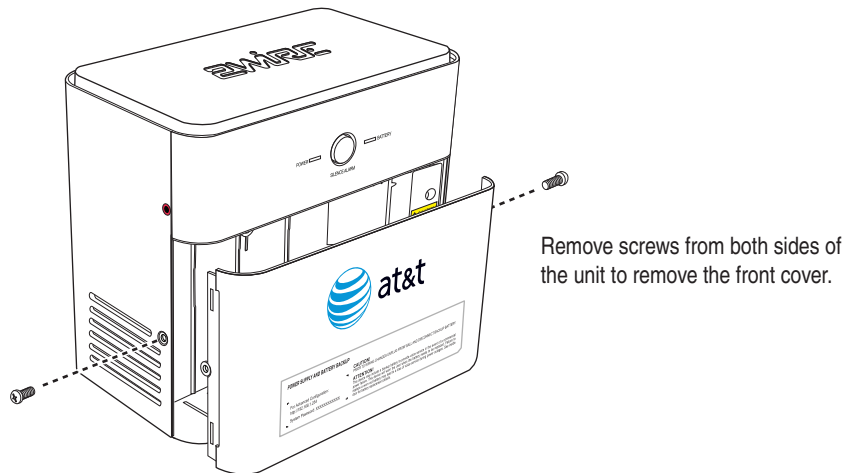


Figure 11: Power Supply Unit Cover Removal

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).

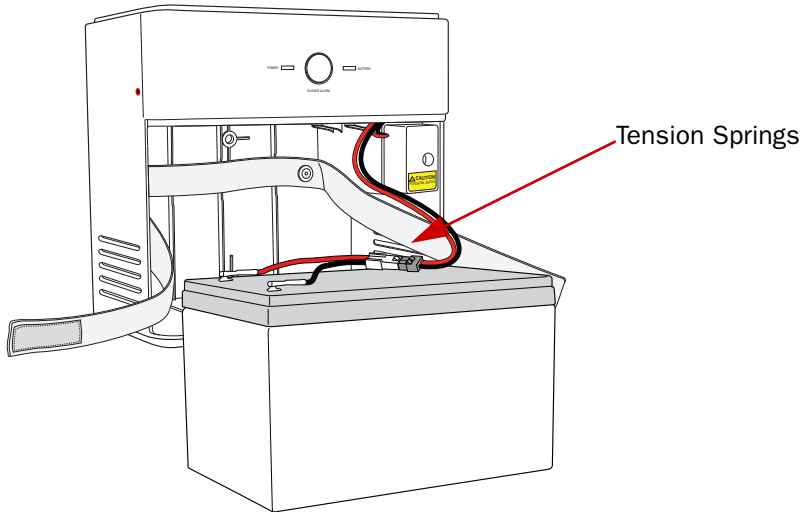


Figure 12: Battery Connector

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.



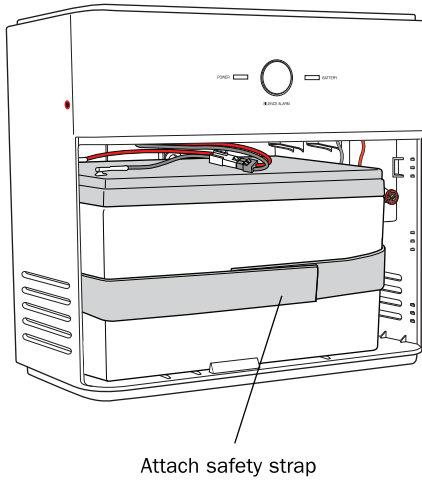
Note: Be sure to place the battery inside the raised bottom edge of the case.

-
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.

- Secure the battery with the safety strap.



- Place the housing cover over the unit and press gently on it until it snaps into place.
- 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).

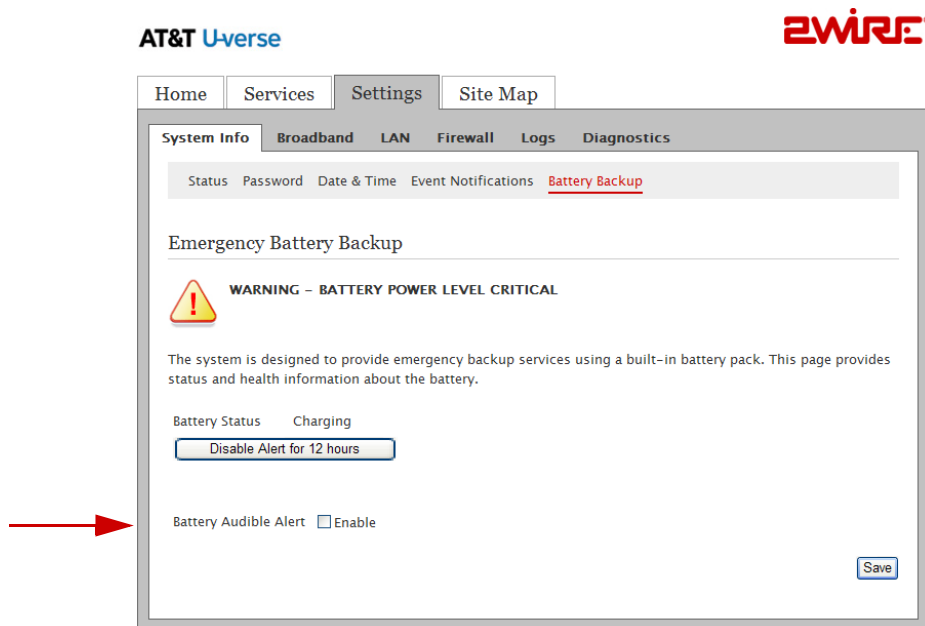
Enabling the Alert

To enable the alert:

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

The screenshot displays the AT&T U-verse 2Wire gateway interface. At the top, there are navigation tabs for Home, Services, Settings, and Site Map. The main content area is titled 'Summary' and includes four status cards: Broadband (showing download and upload speeds), Wireless (showing network name 'Doris'), Firewall (showing status 'Enabled'), and i3802V (showing serial number '450712000169'). Below the summary is a 'Warning - Emergency Battery Backup' section, which is highlighted by a red arrow. This section shows 'Battery Power Level Critical' and a link to 'Battery Info'. Further down, there are sections for 'Home Network Devices' (listing IP addresses and device names like DLok and DorisL) and 'Top Networking Features' (listing links for Wireless, Refresh your Broadband Connection, Restart your System, Home Networking, System Password, and Gaming and Communications).

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.

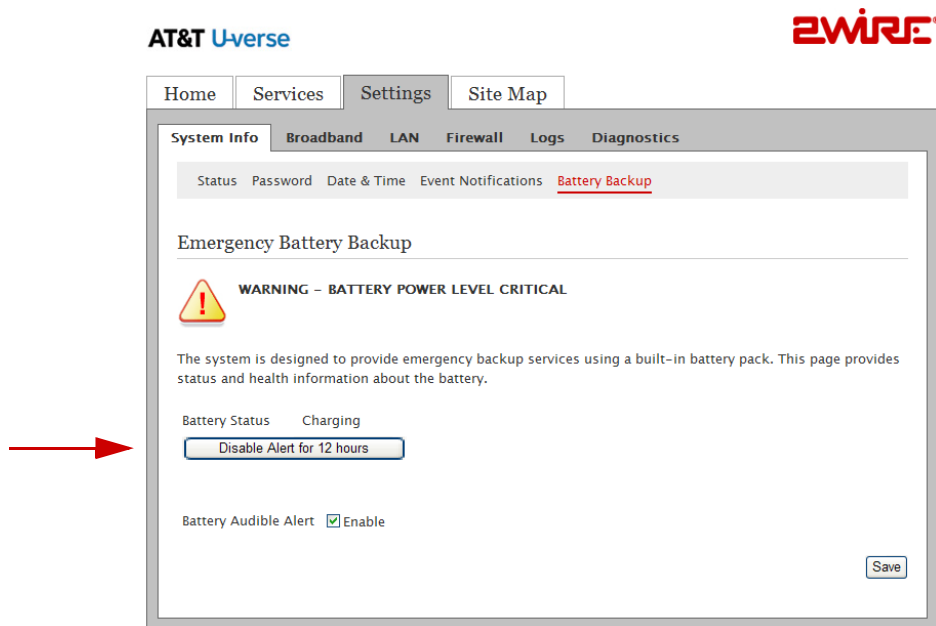
To disable the alert:

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

The screenshot shows the AT&T U-verse 2Wire gateway interface. At the top, there are navigation tabs for Home, Services, Settings, and Site Map. The main content area is divided into several sections:

- Summary:** Displays four status cards:
 - Broadband:** Shows download speed of 27232Kbps and upload speed of 2000Kbps.
 - Wireless:** Shows Network Name as Doris.
 - Firewall:** Shows Status as Enabled.
 - i3802V:** Shows Serial Number as 450712000169.
- Warning - Emergency Battery Backup:** A red arrow points to this section, which displays "Battery Power Level Critical" and a link to "Battery Info".
- Home Network Devices:** Lists three devices:
 - 192.168.1.64 with a "Device Details" link.
 - DLok with "Access Files" and "Device Details" links.
 - DorisL with "Access Files" and "Device Details" links.
- Top Networking Features:** Lists several actions:
 - [Wireless](#) - modify security or settings
 - [Refresh your Broadband Connection](#) - reconnect your broadband connection
 - [Restart your System](#) - reboot
 - [Home Networking](#) - find a computer, share a file
 - [System Password](#) - secure your system with a password
 - [Gaming and Communications](#) - modify your firewall settings

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



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.



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

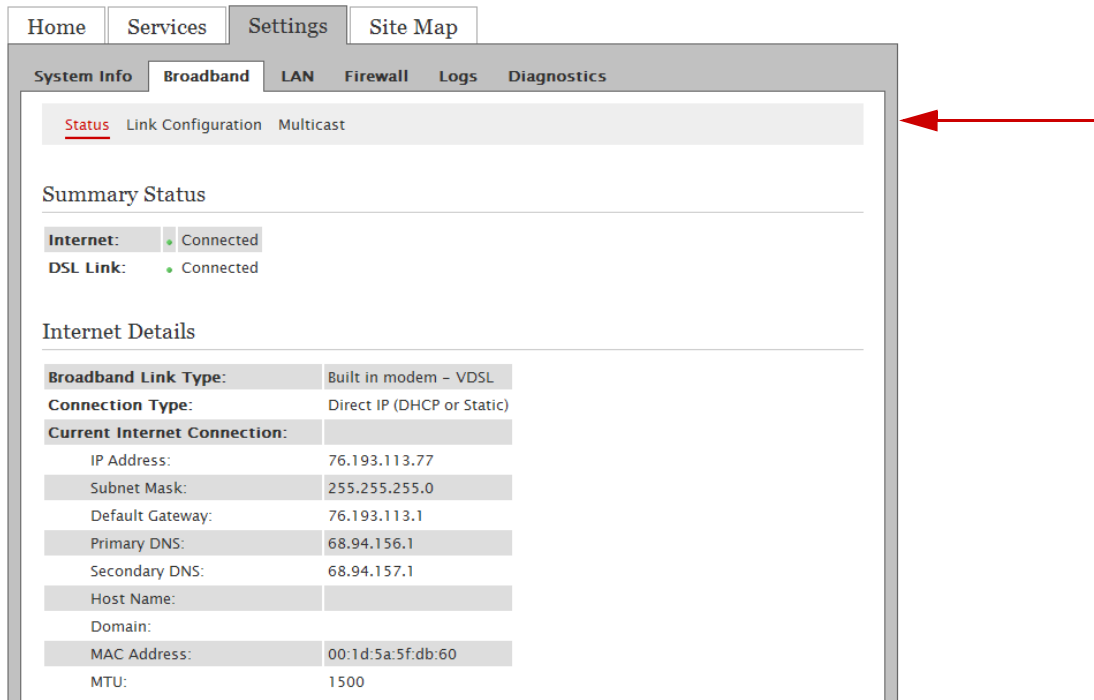
You can create a local network that has broadband network-accessible IP addresses by creating a route from the Internet to the specified public network. This feature is typically used in conjunction with broadband service that provides a range of available IP addresses. Once enabled, the public IP addresses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

AT&T U-verse



The screenshot shows the 2Wire web interface. At the top, there are navigation tabs: Home, Services, Settings, and Site Map. Below these, there are sub-tabs: System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The 'LAN' sub-tab is selected, and within it, the 'Status' sub-tab is highlighted with a red arrow. The main content area displays the following information:

Summary Status

- 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 [Link Configuration](#); the following page opens.

The screenshot shows the AT&T U-verse Z-WIRE router configuration interface. At the top, there are navigation tabs: Home, Services, Settings, and Site Map. Below these are sub-tabs: System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The 'Link Configuration' sub-tab is selected, showing a status bar with 'Link Configuration' and 'Multicast'. A warning icon and text state: 'Warning: Modifying the settings on this page can impact the ability of devices on your private network to access your broadband connection. Modifications may also affect broadband-enabled applications and services running on your private network.' The 'Broadband IP Network' section has an 'Upstream MTU' field set to 1500. The 'Supplementary Network' section includes an 'Add Additional Network' checkbox (unchecked), 'Router Address' and 'Subnet Mask' input fields, and an 'Auto Firewall Open' checkbox (unchecked). A 'Save' button is located at the bottom right.

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).

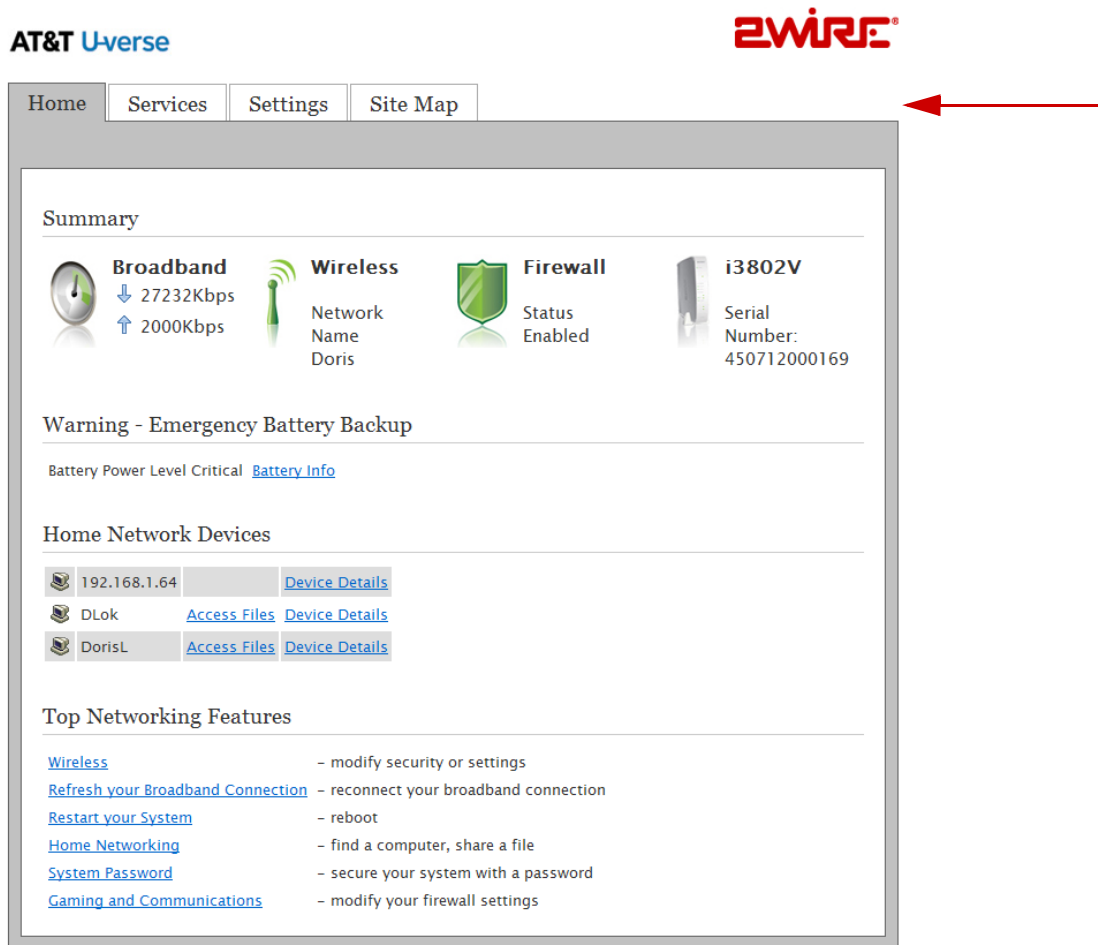


Figure 13: Home Page

- Click [Settings](#); the *System Information* page opens (Figure 14).

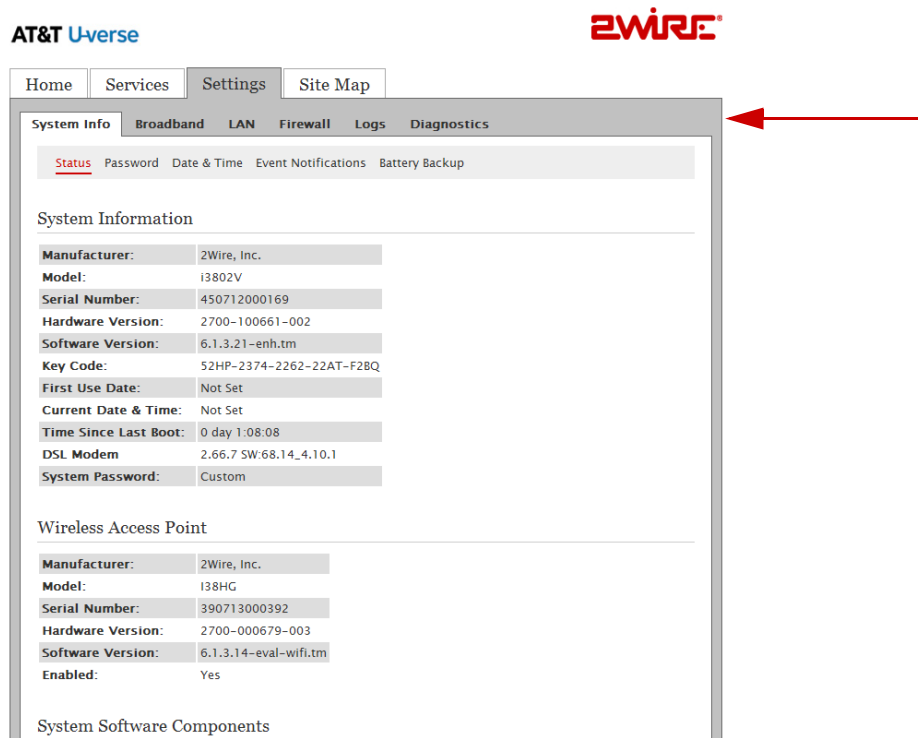
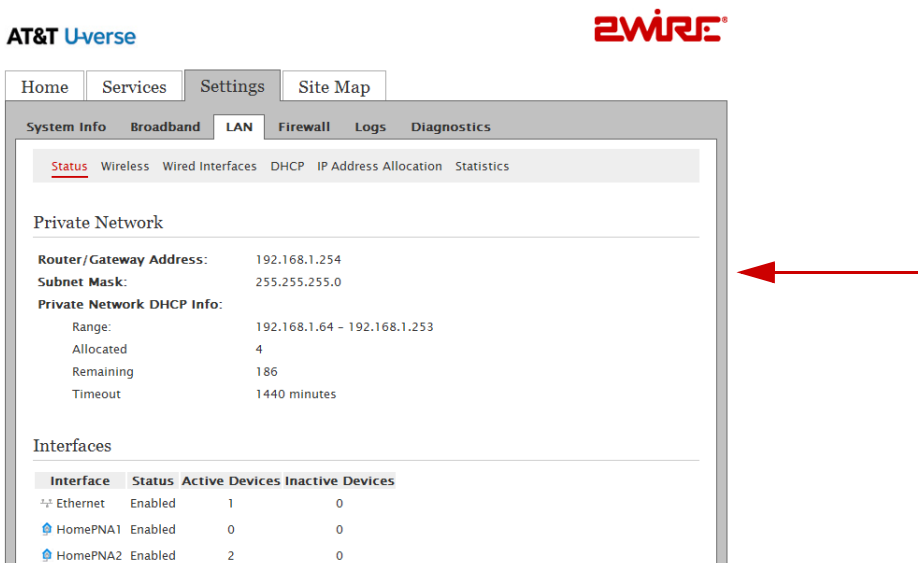


Figure 14: System Information Page

- Click [LAN](#); a page similar to the following opens, displaying the private network information and LAN devices connected to your network.



- Click **DHCP**; the *DHCP Configuration* page opens.

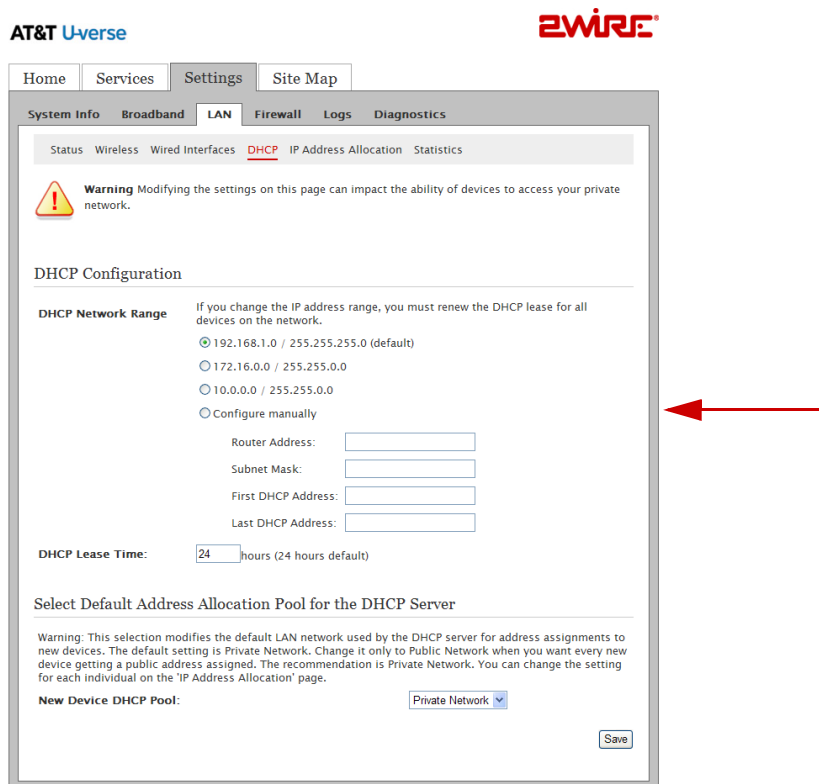


Figure 15: DHCP Configuration

- Select **Configure manually** if you want to set up a range for the DHCP address IP pool.
- 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.
- 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.
- 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.

- 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&T U-verse **2Wire**

Home Services Settings Site Map

Summary

Broadband
 ↓ 27232Kbps
 ↑ 2000Kbps

Wireless
 Network Name
 Doris

Firewall
 Status
 Enabled

i3802V
 Serial Number:
 450712000169

Warning - Emergency Battery Backup

Battery Power Level Critical [Battery Info](#)

Home Network Devices

192.168.1.64	Device Details
DLok	Access Files Device Details
DorisL	Access Files Device Details

Top Networking Features

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

Figure 16: Home Page

- Click [Settings](#); the *System Information* page opens (Figure 14).

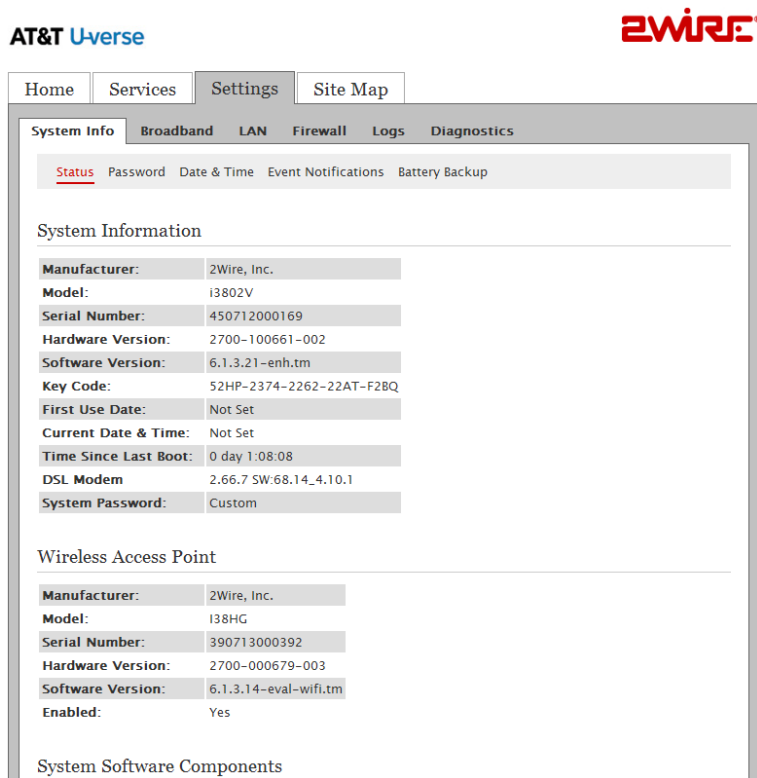


Figure 17: System Information Page

- Click [LAN](#); a page similar to the following opens, displaying the private network information and LAN devices connected to your network.



- Click [IP Address Allocation](#); a page similar to the following opens, displaying the devices in your network.

The screenshot shows the AT&T U-verse 2Wire router configuration interface. The top navigation bar includes Home, Services, Settings, and Site Map. Below this, there are tabs for System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The LAN tab is active, and the sub-tab is IP Address Allocation. The page title is "Public-Private NAT Mappings and Device IP Allocation".

The page contains the following text:

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

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

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

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

There are two device configuration sections:

Device : DLok

- Current Address : 192.168.1.67
- Device Status : Connected DHCP
- Firewall: Enabled
- Address Assignment : Private from pool:192.168.1.0
- WAN IP Mapping : Router WAN IP address (default)

Device : DorisL

- Current Address : 192.168.1.66
- Device Status : Connected DHCP
- Firewall: Enabled
- Address Assignment : Private from pool:192.168.1.0
- WAN IP Mapping : Router WAN IP address (default)

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

- 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.
- Click **Save**.



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	What to Do...
The POWER indicator on the i38HG does not light.	Faulty power supply	<ol style="list-style-type: none"> 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 POWER indicator on the i38HG remains solid red.	System Post Failure	<ol style="list-style-type: none"> 1. Press the Reset 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 ETHERNET 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	What to Do...
No connection to the Internet via the wireless connection.	No communication between the iNID and i38HG	<ol style="list-style-type: none"> 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 WIRELESS indicator on the i38HG, it should light green. 4. Call your service provider if problem persists.
	Mis-match network name and/or encryption key	<ol style="list-style-type: none"> 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 SERVICE 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	<ol style="list-style-type: none"> 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 <i>Home</i> page and click Rescan to scan for a new channel.

Table 4: Connection Issues (Continued)

Symptoms	Problems	What to Do...
The BROADBAND 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 SERVICE 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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Check your line status (Viewing VoIP Service Status on page 89). 2. Verify if the phone is in the Active mode. <ul style="list-style-type: none"> – If yes, click Ring Now to test the ring tone. – If the phone does not ring, check and make sure that the RJ-11 is securely connected to the phone port. – If no, call your service provider.



Table 6: The Power Supply Unit Common Issues

Symptoms	Problems	What to Do...
The iPSU emits chirping sound.	The backup battery life is exhausted.	<ol style="list-style-type: none"> 1. Check to see if the BATTERY indicator on the IPSU is flashing red. 2. Replace the battery (Replacing the Battery on page 60).
The POWER indicator is flashing red.	Normal behavior.	<ol style="list-style-type: none"> 1. Flashing red indicates that the power is provided by the backup battery. The POWER 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 settings	Incorrect password.	<ol style="list-style-type: none"> 1. Go to the <i>Home</i> page. 2. Click System Password at the bottom of the <i>Home</i> page; the <i>Login</i> page opens. 3. Click I forgot the password; the <i>Login</i> page opens displaying your password hint. 4. Enter your password and click Submit. 5. Click I still can't remember the password if you still do not remember the password, the <i>Reset System Password</i> 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:

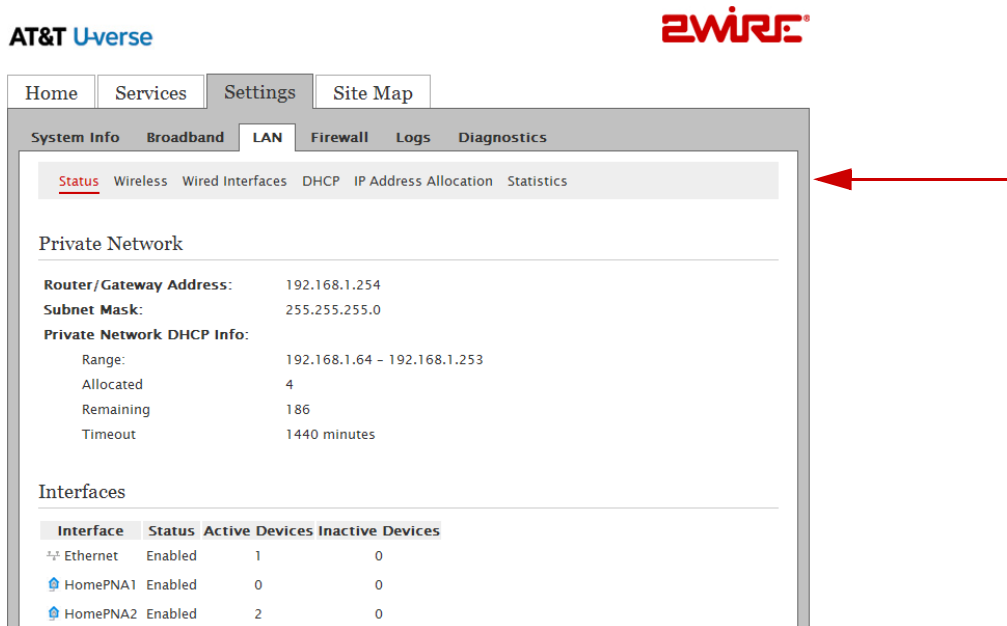
1. Enter `http://gateway.2wire.net`. The user interface Home page opens, displaying the aggregate upstream and downstream bandwidths ([Figure 18](#)).

AT&T U-verse

The screenshot shows the AT&T U-verse Home page with a navigation bar at the top containing 'Home', 'Services', 'Settings', and 'Site Map'. The main content area is titled 'Summary' and features several status cards: 'Broadband' showing download (27232Kbps) and upload (2024Kbps) speeds; 'Wireless' with a 'Network Name' field; 'Firewall' with 'Status Enabled'; and 'iNID i3802V' with a 'Serial Number: 310712000005'. Below this is a 'Warning - Emergency Battery Backup' section with a 'Battery Power Level Critical' and a link to 'Battery Info'. The 'Home Network Devices' section lists three devices: 'DLok', '192.168.1.64', and 'DorisL', each with links for 'Access Files' and 'Device Details'. The 'Top Networking Features' section lists several actions: 'Wireless' (modify security or settings), 'Refresh your Broadband Connection' (reconnect broadband), 'Restart your System' (reboot), 'Home Networking' (find computer, share file), 'System Password' (secure system), and 'Gaming and Communications' (modify firewall settings). A red arrow points to the 'Home Networking' link.

Figure 18: The Home Page

2. Click [Home Networking](#); the LAN Status page opens.



3. Click [Statistics](#); the page opens displaying the wireless access point information (Figure 19).

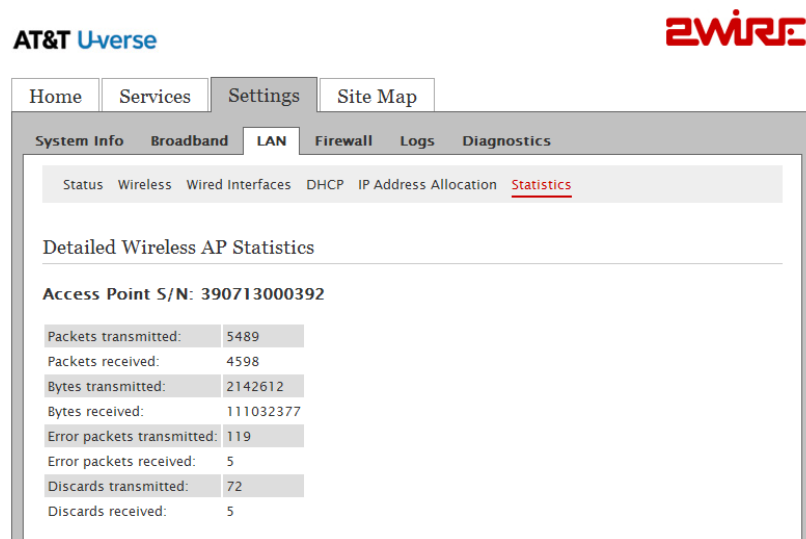


Figure 19: The LAN Statistics Page

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)

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

NodeID	MTU	Mac Address
1	17000	00:1D:5A:5F:E6:89
3	8192	00:11:E6:00:19:71
2	8192	00:11:E6:00:0C:69
0	9216	00:15:9A:B9:FC:8C
4	8192	00:11:E6:00:11:96

Detailed Statistics (Coax)

HPNA Ethernet frames sent:	540643
HPNA Ethernet frames received:	19573
HPNA Ethernet bytes sent:	725993882
HPNA Ethernet bytes received:	6199685
HPNA broadcast Ethernet bytes sent:	4021
HPNA broadcast Ethernet frames received:	18
HPNA multicast Ethernet frames sent:	523734
HPNA multicast Ethernet frames received:	489
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:	675
HPNA control requests received:	0
HPNA control replies sent:	0
HPNA control replies received:	675

Interface	Local (Coax)		Remote		Remote		Remote		Remote	
Station ID	1		4		3		2		0	
Mac Address	00:1D:5A:5F:E6:89		00:11:E6:00:11:96		00:11:E6:00:19:71		00:11:E6:00:0C:69		00:15:9A:B9:FC:8C	
Master	√									
Interval Start	10:53	11:08	10:53	11:08	10:53	11:08	10:53	11:08	10:53	11:08
Interval End	11:08	11:20	11:08	11:20	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.


1. 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	00:1B: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

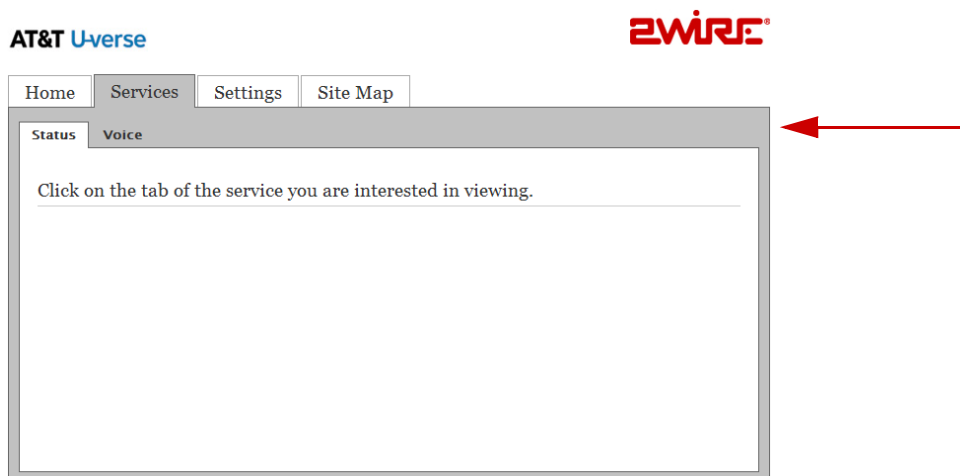
Modem Type:	Built in modem - VDSL	
Physical Line 1		
DSL Line (Wire Pair):	RJ-11	
Current DSL Connection:		
	Down	Up
Rate:	13616 kbs	920 kbs
Max Rate:	64000 kbs	Not Available
Noise Margin:	37.5 dB	Not Available
Attenuation:	4.0 dB	Not Available
Output Power:	14.3 dBm	-31.0 dBm
Protocol:	G.993.2	
Channel:	Interleaved	
DSLAM Vendor Information	Country: {255} Vendor: {CXSX} 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} Vendor: {CXSX} 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:	G.993.2	
DSLAM Vendor Information	Country: {255} Vendor: {CXSX} Specific: {16898 }	
Rate Cap:	27232 kbs	



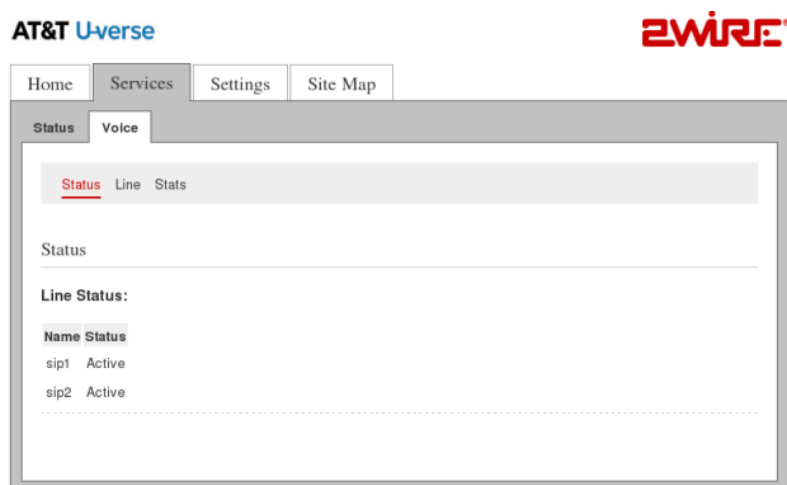
Note: The number of physical lines displays is dependent on the number of lines in use.

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 [Services](#); the following page opens.

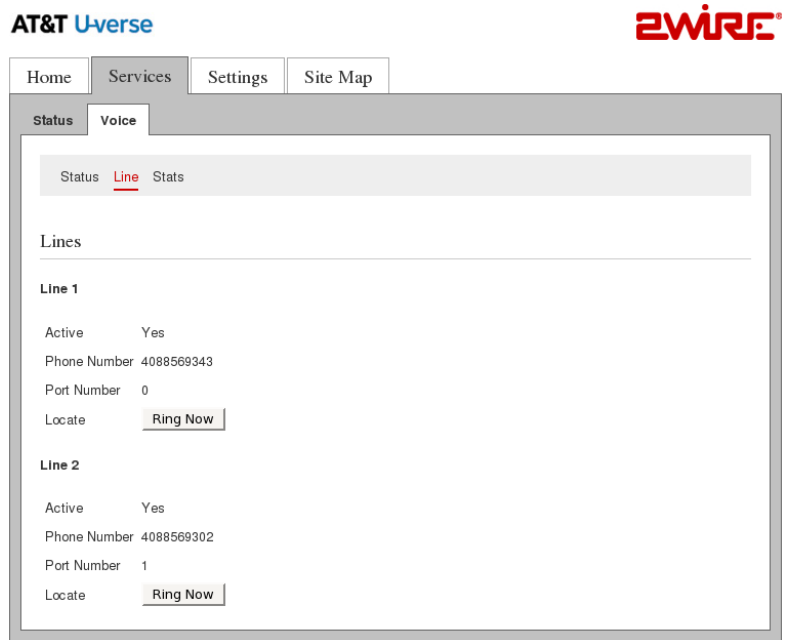


3. Click [Voice](#); the *Status* page opens.



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

4. Click [Line](#); the *Lines* page opens, displaying the line status as well as the phone and port numbers associated with each line.

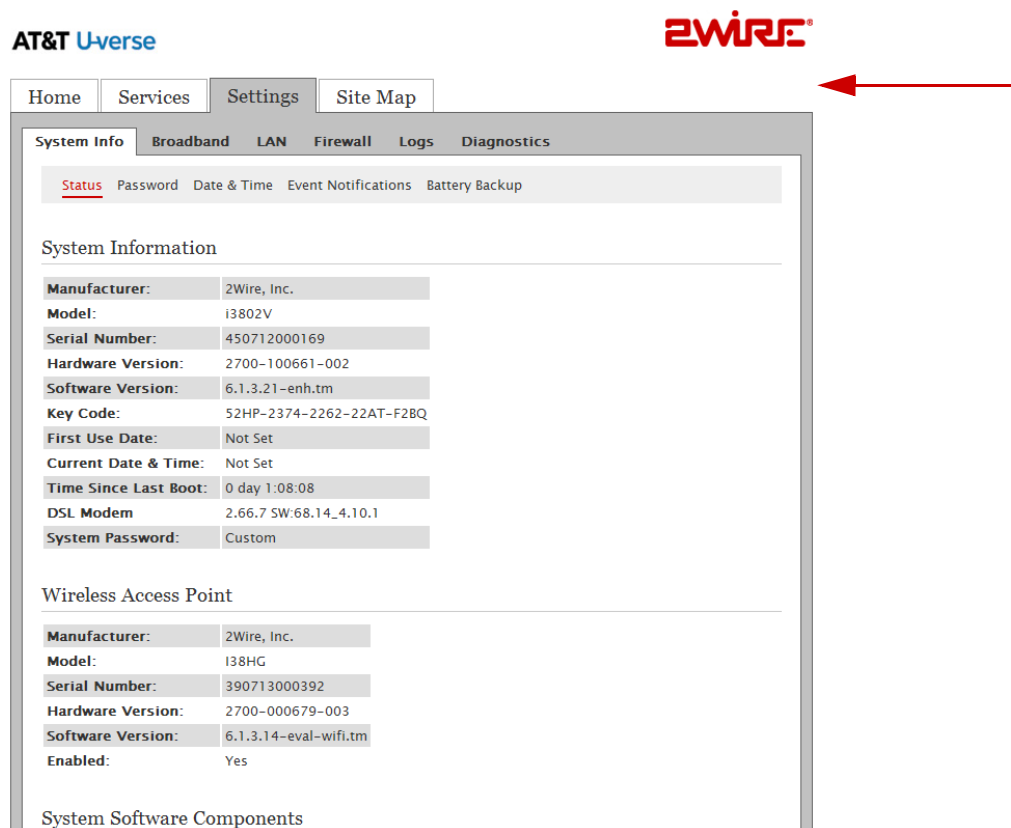


Viewing Logs

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 [Settings](#); the *System Information* page opens.



AT&T U-verse **2WIRE**

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:	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 Point

Manufacturer:	2Wire, Inc.
Model:	I38HG
Serial Number:	390713000392
Hardware Version:	2700-000679-003
Software Version:	6.1.3.14-eval-wifi.tm
Enabled:	Yes

System Software Components

- Click [Logs](#); the *Event Log* page opens.

AT&T U-verse **eWIRE**

Home Services Settings Site Map

System Info Broadband LAN Firewall **Logs** Diagnostics

Event Log System Log Upgrade Log Firewall Log

Event Log

Clear Log

Display Filter

Type	Date/Time	Event Description	
INF	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

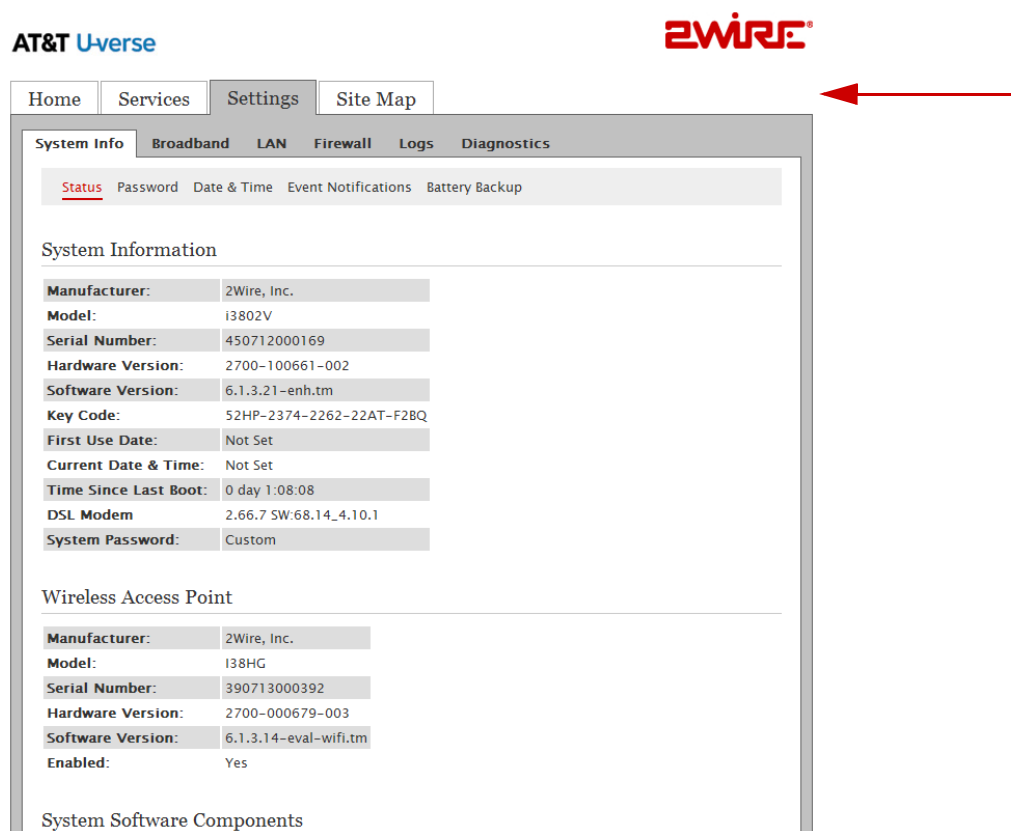


Note: The log starts from the oldest to the latest date; that is, the latest log appears at the bottom of the page.

- Click **Clear Log** if you want to minimize the clutter from previous events when you are trying to diagnose a problem.
- Filter the log category from the **Display Filter** drop-down list.
- Click **Submit**; the page refreshes and displays the logs of your selection.
- 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 [Settings](#); the *System Information* page opens.



AT&T U-verse **2WIRE®**

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:	i3802V
Serial Number:	450712000169
Hardware Version:	2700-100661-002
Software Version:	6.1.3.21-enh.tm
Key Code:	52HP-2374-2262-22AT-F28Q
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.
Model:	I38HG
Serial Number:	390713000392
Hardware Version:	2700-000679-003
Software Version:	6.1.3.14-eval-wifi.tm
Enabled:	Yes

System Software Components

3. Click [Logs](#); the *Event Log* page opens.

AT&T U-verse **2WIRE®**

Home Services Settings Site Map

System Info Broadband LAN Firewall **Logs** Diagnostics

Event Log System Log Upgrade Log Firewall Log

Event Log

Clear Log

Display Filter

Type	Date/Time	Event Description	
INF	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.

AT&T U-verse **2WIRE®**

Home Services Settings Site Map

System Info Broadband LAN Firewall **Logs** Diagnostics

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

System Log

Clear Log

Select Device

Display Filter

Insert Mark in Log

Type	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	
WRN	2008-04-08T15:07:16-07:00	cwmd: session failed...	
INF	2008-04-08T15:07:16-07:00	cwmd: session will be retried in 198090(ms)	



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.

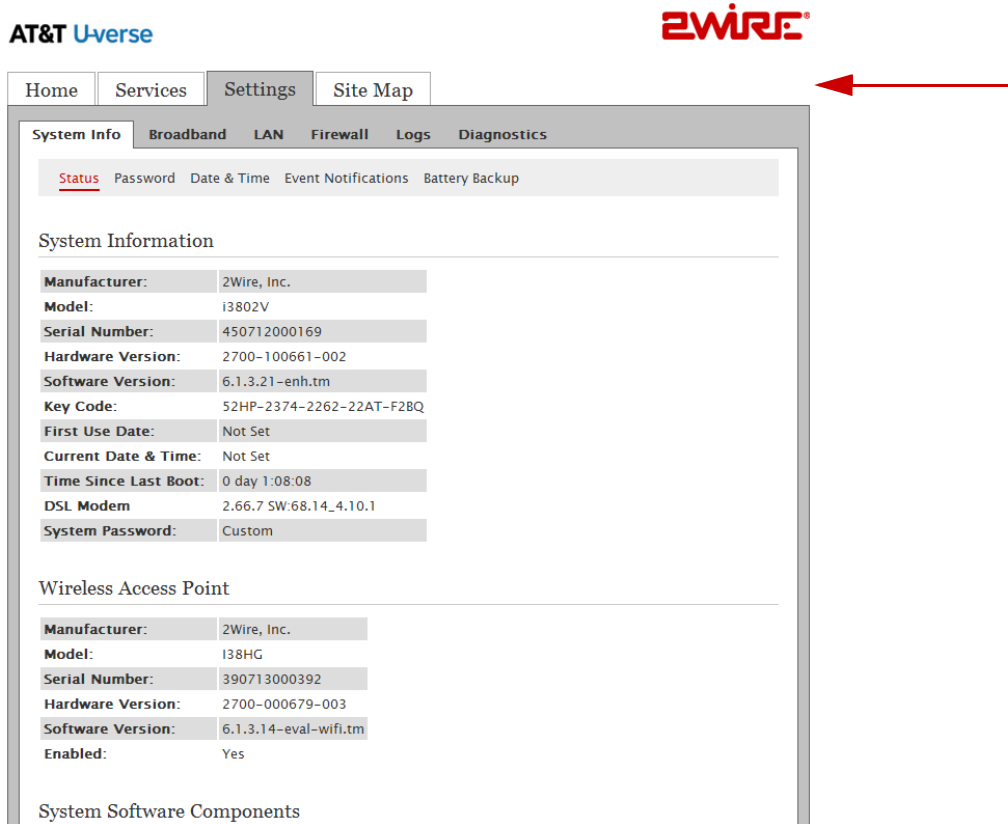


Note: The latest log appears at the bottom of the page; scroll down the page to view your insertion mark.

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 [Settings](#); the *System Information* page opens.



3. Click [Logs](#); the *Event Log* page opens.

AT&T U-verse eWIRE®

Home Services Settings Site Map

System Info Broadband LAN Firewall **Logs** Diagnostics

Event Log System Log Upgrade Log Firewall Log

Event Log

Clear Log

Display Filter

Type	Date/Time		Event Description
INF	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 eWIRE®

Home Services Settings Site Map

System Info Broadband LAN Firewall **Logs** Diagnostics

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

Firewall Log

Clear Log

Date and Time	Severity	Details
2008-04-08T15:03:56-07:00	info	src=60.172.222.9 dst=76.193.113.77 ipprot=6 sport=6000 dport=135 event id: 261

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 [Settings](#); the *System Information* page opens.

The screenshot shows the AT&T U-verse 2Wire user interface. At the top, there are navigation tabs: Home, Services, Settings, and Site Map. A red arrow points to the Settings tab. Below the tabs, there are sub-tabs: System Info, Broadband, LAN, Firewall, Logs, and Diagnostics. The main content area displays system information for both the main device and the wireless access point.

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 Point	
Manufacturer:	2Wire, Inc.
Model:	I38HG
Serial Number:	390713000392
Hardware Version:	2700-000679-003
Software Version:	6.1.3.14-eval-wifi.tm
Enabled:	Yes

System Software Components

3. Click [Logs](#); the *Event Log* page opens.

AT&T U-verse ZWIRE®

Home Services Settings Site Map

System Info Broadband LAN Firewall **Logs** Diagnostics

[Event Log](#) System Log Upgrade Log Firewall Log

Event Log

Clear Log

Display Filter

Type	Date/Time		Event Description
INF	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 [Upgrade Log](#), the *Upgrade Log* page opens, displaying the software versions information.

AT&T U-verse ZWIRE®

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



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 OET-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.

