HomePortal® Intelligent Gateway Configuration Guide

Firmware Version: 9.3.1.17

Notice to Users

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.

932010

5100-000899-000

Contents

About This Guide

The *HomePortal® Intelligent Gateway 9.3.1.17 Configuration Guide* is designed to serve as a reference to configure the gateway that uses the 9.3.1.17 firmware. This guide contains the following chapters:

Audience

This guide is intended for use by:

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

Supported Hardware Platforms

The following gateway hardware platforms are compatible with 9.3.1.17 firmware:

- 5011NV
- 5012NV

Document Layout

Each chapter in this document has information (topics/subtopics) for configuring or viewing the links under different tabs on the user interface of your gateway.

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

- *Objective*
- *Steps*
- *See Also*

These sections help you to easily find your topics of interest and guide you through them in a simple and logical manner.

The *See Also* section has cross-referenced links to other topics within this document, which may assist you in enhancing your experience with the gateway.

Style Conventions

The following style conventions are used in this guide:

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

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

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

Typographical Conventions

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

Related Documents

In addition to this guide, the HomePortal Intelligent Gateway Software documentation library includes:

Agile Part Number	Description
5100-000900-000	HomePortal® 5011NV/5012NV Intelligent Gateway Installation Guide
5100-000923-000	HomePortal® Intelligent Gateway 9.3.1.17 CLI Reference Guide
5100-000874-000	HomePortal® 5012NV Intelligent Gateway Datasheet

Support

Technical support is available from the 2Wire Web site: http://support.2wire.com.

CHAPTER 1

Introducing the HomePortal Intelligent Gateway Software

Welcome to the 2Wire family. The HomePortal Intelligent Gateway Software delivers a powerful user experience with its easy-to-use features. It enables you to connect to the Internet and perform a host of functions which makes your home network safe, convenient, and an enjoyable experience!

The HomePortal Intelligent Gateway Software enables high-speed Internet access and offers a host of other features such as:

- **Home Networking**
  Share files, printers, and a broadband connection with every computer and other network-ready devices in the home or small office through the advanced LAN technology.
- **Superior Wireless Performance**
  High-powered 802.11n wireless technology from 2Wire virtually eliminates wireless “cold spots” at home. HomePortal intelligent gateway provides up to seven times the true power of traditional access points, and increases wireless bandwidth by using powerful 400 mW transmitters.
- **Parental Controls (Internet Access Controls and Content Screening)**
  Parental controls offer easy-to-use tools to limit access to specific Web sites, monitor browsing history and usage, and enforce time restrictions on common applications. Parental control settings are straightforward and easily managed by users.
- **Advanced Firewall Monitoring**
  This feature monitors inbound and outbound network traffic for suspicious activities, which helps eliminate security issues before they have a chance to proliferate. The firewall actively detects and defends against common Internet threats (such as distributed denial of service attacks) using stateful packet inspection. It is also subscriber-friendly, enabling simple configuration setup for common in-home applications such as online gaming.
- **Network Address Translation (NAT)**
  NAT technology modifies network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another.
- **IPTV**
  HomePortal intelligent gateway is optimized for the delivery of IPTV throughout the home. Hardware accelerated QoS minimizes potential issues such as pixelation and image freezes, delivering a better IPTV experience.
- **DNS Resolution**
  Configure your gateway to resolve the domain name to IP address.
- **Quality of Service (QoS)**
  QoS features such as policies, priority queuing, shaping, and management allow you to effectively manage available Internet bandwidth.
- **Logs**
  The gateway maintains internal logs of Broadband status and WAN-side connection flows, letting you or the ISP’s technician effectively diagnose issues.
- **Ping Client**
  The gateway allows you to ping LAN and WAN side IP addresses within your network. This lets you know whether a network device is responding or not.
- **Intuitive Web Interface**
  Configure your gateway settings from the gateway's user-friendly Web interface.
- **Parental Controls (Internet Access Controls and Content Screening)**
  Limits access to specific Web sites, monitor browsing history and usage, and enforce time restrictions on common applications.
- **Remote Firmware Upgrade**
  Enable remote firmware upgrades on the user interface of the gateway for using the latest firmware.

See Also

Accessing the User Interface on page 3

Configuring the Internet Connection on page 5

CHAPTER 2

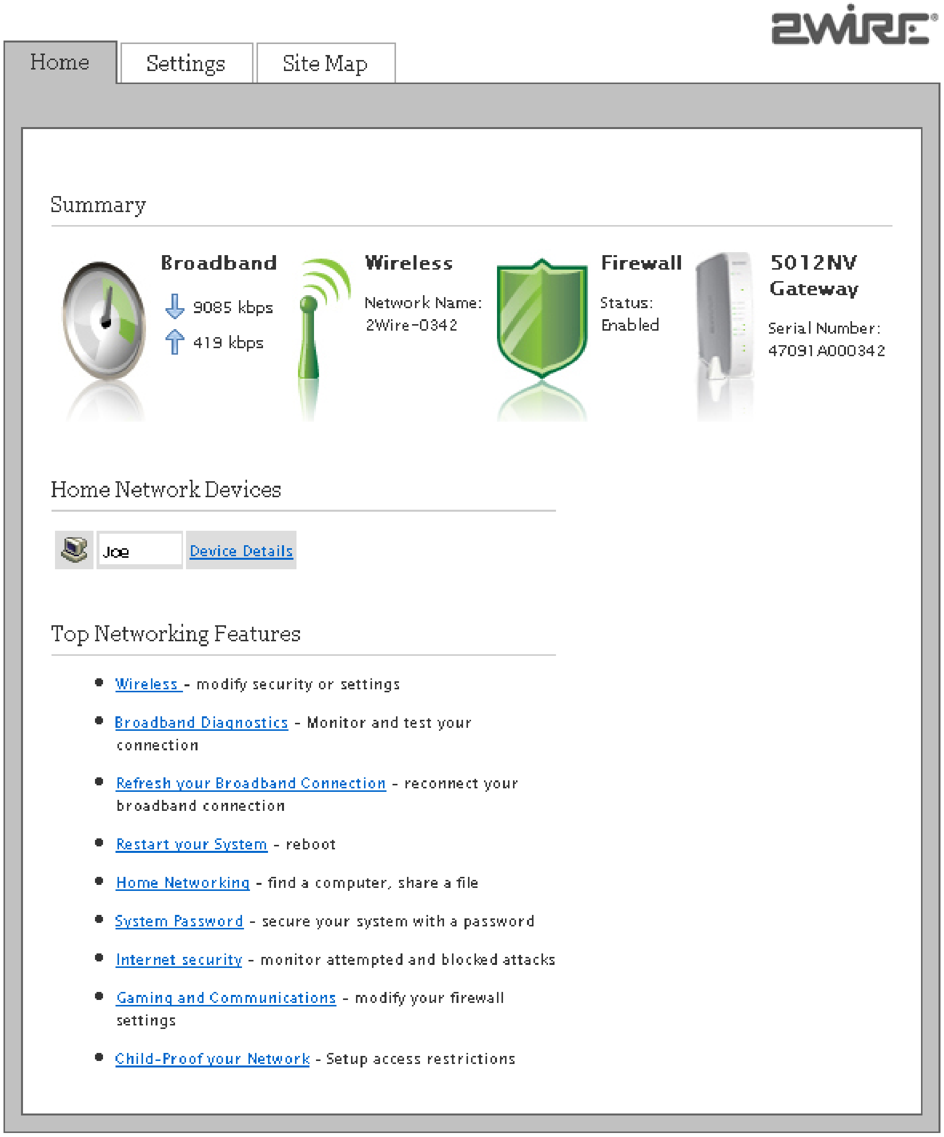
Accessing the User Interface

This chapter provides an overview about the accessible links on the user interface.

To launch the user interface, access any of the following URLs on the computer connected to the gateway:

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

This opens the **Home** page.



Summary

Broadband
9085 kbps
419 kbps

Wireless
Network Name:
2Wire-0342

Firewall
Status:
Enabled

5012NV Gateway
Serial Number:
47091A000342

Home Network Devices

Joe Device Details

Top Networking Features

- Wireless - modify security or settings
- Broadband Diagnostics - Monitor and test your connection
- 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
- Internet security - monitor attempted and blocked attacks
- Gaming and Communications - modify your firewall settings
- Child-Proof your Network - Setup access restrictions

Figure 1: Home page

The **Home** page has gateway link tabs and three panels as listed below:

- System Link Tabs
  - Home
  - Settings
  - Site Map
- Summary
- Home Network Devices
- Top Networking Features

System Link Tabs

Home

The **Home** tab provides the most relevant information about your Broadband service at a glance. You can also access links on this page that let you perform the related activities on the user interface of the gateway.

Settings

The **Settings** tab provides links to view and configure gateway information. Also, you can configure Broadband services, LAN settings, Firewall settings, VoIP settings, and perform Diagnostics on your gateway.

Site Map

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

Summary

The **Summary** panel displays the **Broadband** icon, network name (SSID) of the gateway next to the **Wireless** icon, security status next to the **Firewall** icon, and serial number next to the **5012NV Gateway** icon. Click an icon to access the relevant page directly.

Home Network Devices

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

Top Networking Features

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

See Also

Introducing the HomePortal Intelligent Gateway Software on page 1

Configuring the Internet Connection on page 5

CHAPTER 3

Configuring the Internet Connection

This chapter provides information to configure the Internet connection from the user interface.

Objective

To configure and connect to the Internet through the gateway.

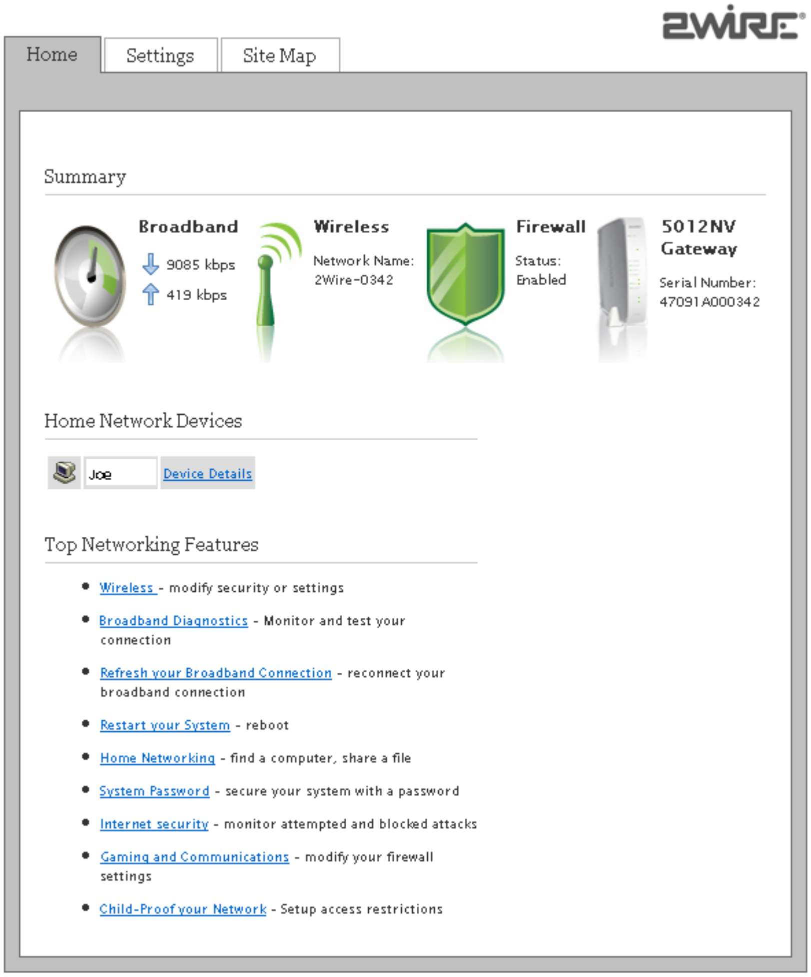
Your Internet connection settings are automatically provisioned by your ISP. If the information is not populated, then you have to manually configure your Internet connection settings.

If you are connecting through Direct IP, then you are not required to enter PPP authentication information. However, if you are connecting through PPPoE or PPPoA, ensure that you have the following ATM information and authentication settings from your ISP:

- Circuit identifier (VPI/VCI)
- Encapsulation method
- PPP username
- PPP password

Steps

1. Access the **Home** page of the gateway by entering the URL http://gateway.2Wire.net into a compatible browser.



Summary

Broadband
9085 kbps
419 kbps

Wireless
Network Name:
2Wire-0342

Firewall
Status:
Enabled

5012NV Gateway
Serial Number:
47091A000342

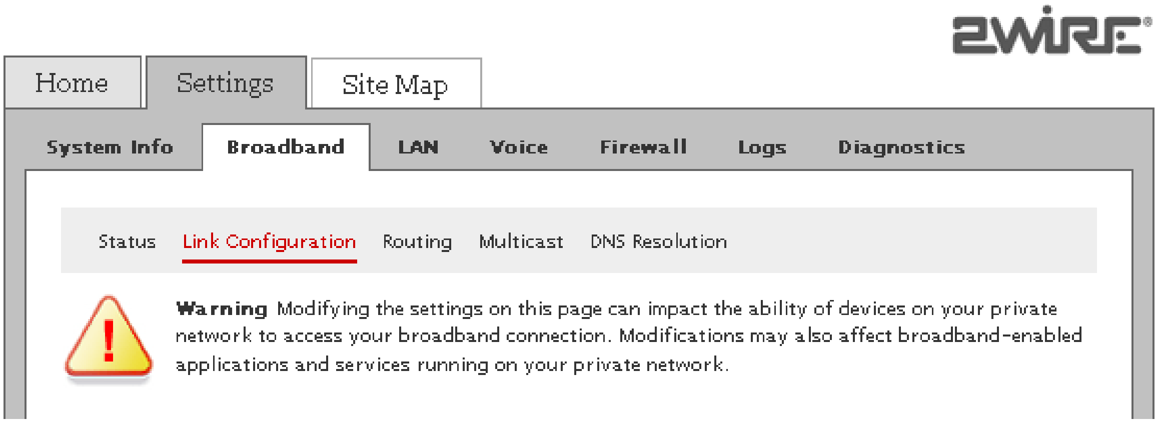
Home Network Devices

Joe Device Details

Top Networking Features

- Wireless - modify security or settings
- Broadband Diagnostics - Monitor and test your connection
- 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
- Internet security - monitor attempted and blocked attacks
- Gaming and Communications - modify your firewall settings
- Child-Proof your Network - Setup access restrictions

2. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.



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.

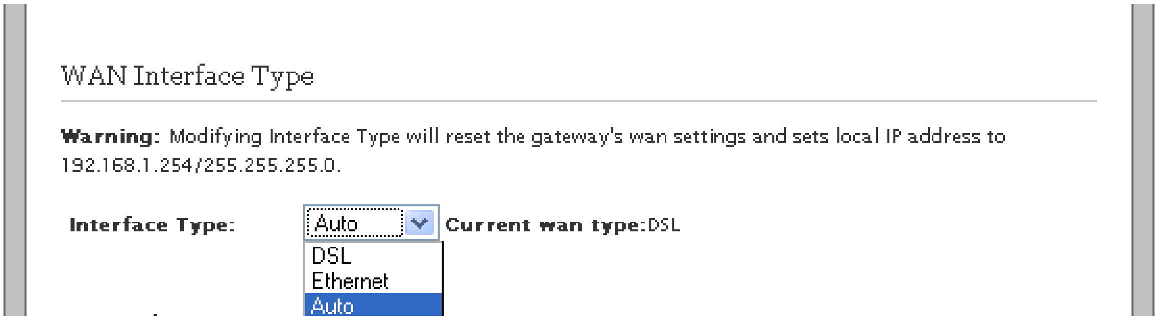
3. Perform the following tasks to activate the Internet service on your gateway:
   - Selecting Broadband Interface Type on page 6
   - Modifying Connection Type on page 6
   - Modifying DSL and ATM Settings on page 7
   - Entering PPP Authentication Parameters on page 8
   - Modifying Broadband IP Network Settings on page 9
   - Configuring Routing Mode on page 10

Selecting Broadband Interface Type

The **WAN Interface Type** panel allows you to select the type of Broadband interface for connecting to the Internet.

To select the Broadband interface type:

1. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.
2. Navigate to the **WAN Interface Type** panel.



WAN Interface Type

Warning: Modifying Interface Type will reset the gateway's wan settings and sets local IP address to 192.168.1.254/255.255.255.0.

Interface Type: Auto **Current wan type:**DSL

3. Select the **Interface Type** option:
   - If your Broadband connectivity is through the DSL port of the gateway, then select DSL from the drop-down list box.
   - If your Broadband connectivity is through the Ethernet port of the gateway, then select Ethernet from the drop-down list box.

   It is recommended to select **Auto** as it enables the gateway to automatically detect the type of connection used to connect to the Broadband service.

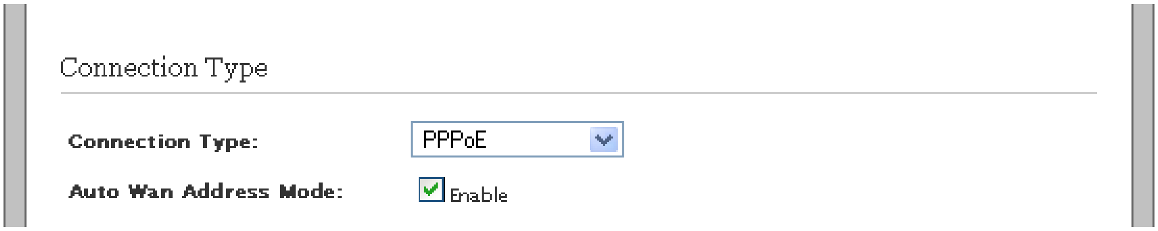
Modifying Connection Type

The **Connection Type** panel allows you to select the type of Broadband connection type for connecting to the Internet.

Note **PPPoE** is not displayed in the **Interface Type** drop-down list box, if you select **Ethernet** as the WAN interface type.

To select the Broadband connection type:

1. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.
2. Navigate to the **Connection Type** panel.



Connection Type

Connection Type: PPPoE

Auto Wan Address Mode: ☑ Enable

3. Select the type of connection from **Connection Type** drop-down list box.

   The types of connections available are **PPPoE**, **PPPoA**, **Direct IP (DHCP)**, or **Direct IP (Static)**.

   - If you select **PPPoE** or **PPPoA**, entering PPP user credentials is necessary to authenticate yourself as the subscriber on the server of the ISP.
   - If you select **Direct IP (DHCP)** or **Direct IP (Static)**, you are not required to enter your user name and password.

4. Select the **Enable** check box next to the **Auto Wan Address Mode** field.

   This lets the gateway to failover from **PPPoE** or **PPPoA** to other connection types, such as **Direct IP (DHCP)** or **Direct IP (Static)**.

Note If you select **Direct IP (DHCP)** or **Direct IP (Static)**, then skip to Modifying Broadband IP Network Settings on page 9. Also, ensure that the routing mode is enabled by referring to Configuring Routing Mode on page 10.

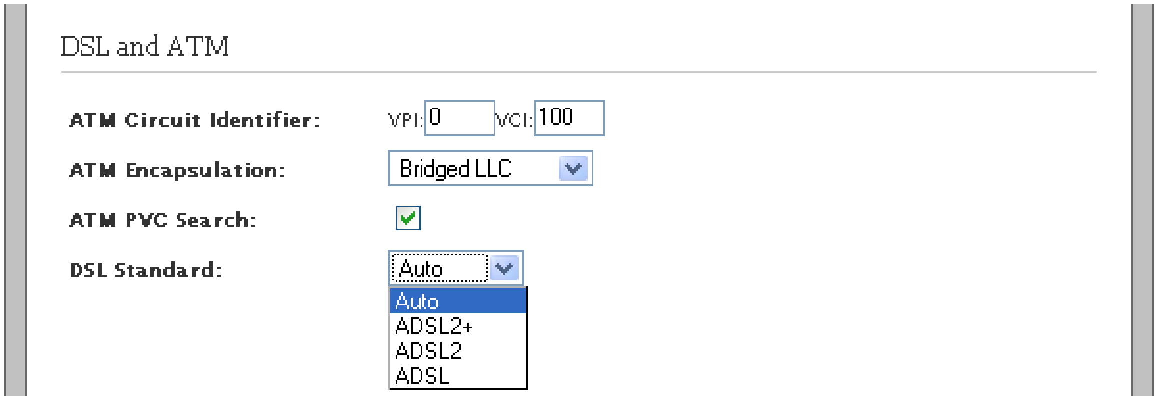
Modifying DSL and ATM Settings

The **DSL and ATM** panel allows you to change the type of DSL line and manually configure the ATM settings. The information required to configure this setting is provided by your ISP.

Note The **DSL and ATM** panel is not available if you select **Ethernet** as the WAN interface type.

To configure DSL and ATM settings:

1. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.
2. Navigate to the **DSL and ATM** panel.



DSL and ATM

ATM Circuit Identifier: VPI: 0 VCI: 100

ATM Encapsulation: Bridged LLC

ATM PVC Search: ☑

DSL Standard: Auto

3. Leave the **VPI** and **VCI** values next to the **ATM Circuit Identifier** field as is, if these text boxes are pre-populated.

   If these text boxes are empty, then enter the **VPI** and **VCI** values for connecting to the ISP server.

4. Select the encapsulation method from the **ATM Encapsulation** drop-down list box.
   - Select **Bridged LLC** or **Bridged VC-Mux** for PPPoE type of connection.
   - Select **Routed LLC** or **Routed VC-Mux** for PPPoA type of connection.

5. Select the **ATM PVC Search** check box to enable the PVC search.

   PVC search enables the gateway to automatically detect and populate VPI and VCI values supported by your ISP.

6. Select the type of DSL connection from the **DSL Standard** drop-down list box.

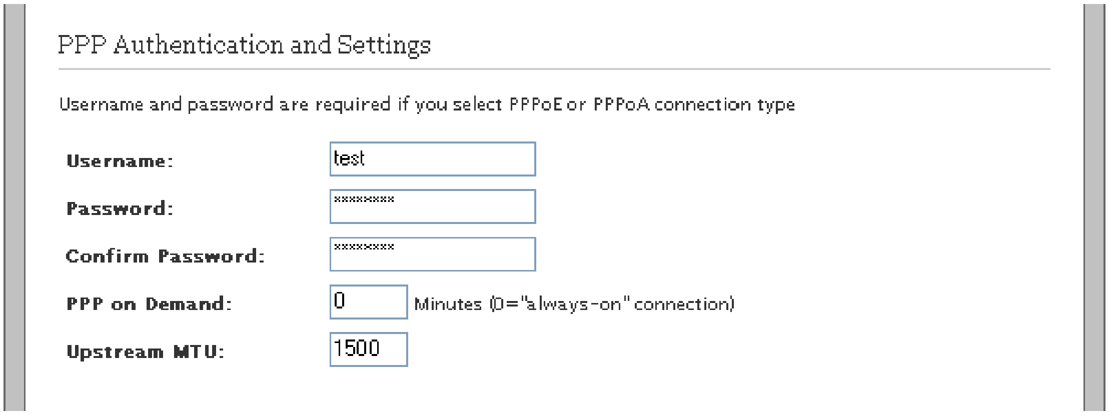
   The types of standards available are **ADSL**, **ADSL2**, or **ADSL2+**. Selecting **Auto** enables the gateway to automatically select the type of DSL standard for seamless connectivity.

Entering PPP Authentication Parameters

The **PPP Authentication and Settings** panel lets you enter the PPP authentication parameters which the gateway uses to connect to the ISP. The PPPoE or PPPoA connection type requires PPP authentication parameters to be entered manually.

To enter PPP authentication parameters:

1. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.
2. Navigate to the **PPP Authentication and Settings** panel.



PPP Authentication and Settings

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

Username: test

Password: *********

Confirm Password: ********

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

Upstream MTU: 1500

3. Enter the PPPoE **Username** and **Password** in the **PPP Authentication and Settings** panel.

   This information is provided by the ISP.

4. Leave the **PPP on Demand** text box as is, unless your ISP has indicated otherwise.

   If the value is set to 0 minutes, the PPP session will be persistent (always-on). If the value is between 1 to 10080 minutes, the PPP session will timeout if the gateway does not detect outbound traffic destined for the Internet in the specified time. However, when the gateway detects outbound traffic, the session is re-established.

5. Leave the **Upstream MTU** value as is.

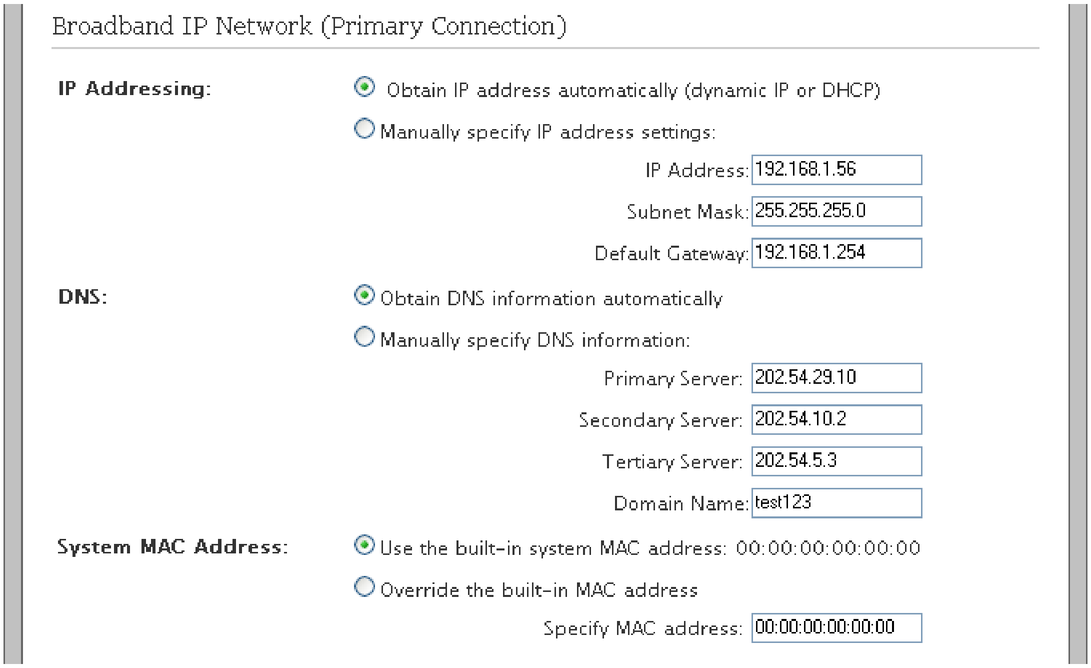
   This is the maximum size allowed for data packets that are communicated on the network of your ISP.

Modifying Broadband IP Network Settings

The **Broadband IP Network (Primary Connection)** panel lets you manually change the Broadband IP and DNS addresses provided by your ISP, if you do not want to use the assigned parameters. Also, you can override the existing MAC address by specifying it manually.

To modify Broadband IP Network settings:

1. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.
2. Navigate to the **Broadband IP Network (Primary Connection)** panel.



Broadband IP Network (Primary Connection)

IP Addressing: ● Obtain IP address automatically (dynamic IP or DHCP)

○ Manually specify IP address settings:

IP Address: 192.168.1.56

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

DNS: ● Obtain DNS information automatically

○ Manually specify DNS information:

Primary Server: 202.54.29.10

Secondary Server: 202.54.10.2

Tertiary Server: 202.54.5.3

Domain Name: test123

System MAC Address: ● Use the built-in system MAC address: 00:00:00:00:00:00

○ Override the built-in MAC address

Specify MAC address: 00:00:00:00:00:00

3. Select the **IP Addressing** option:
   - If you select **Obtain IP address automatically (dynamic IP or DHCP)** radio button, the associated parameters are configured dynamically.
   - If you select **Manually specify IP address settings** radio button, you have to enter the static **IP Address**, **Subnet Mask**, and **Default Gateway** values in corresponding text boxes. Contact your ISP to get this information.
4. Select the **DNS** addressing option:
   - If you select **Obtain DNS information automatically** radio button, the associated parameters are configured dynamically.
   - If you select **Manually specify DNS information** radio button, you have to enter the **Primary Server** address, **Secondary Server** address, **Tertiary Server** address, and **Domain Name** values in corresponding text boxes. The tertiary server is the alternative DNS server to primary and secondary DNS server. Contact your ISP to get this information.

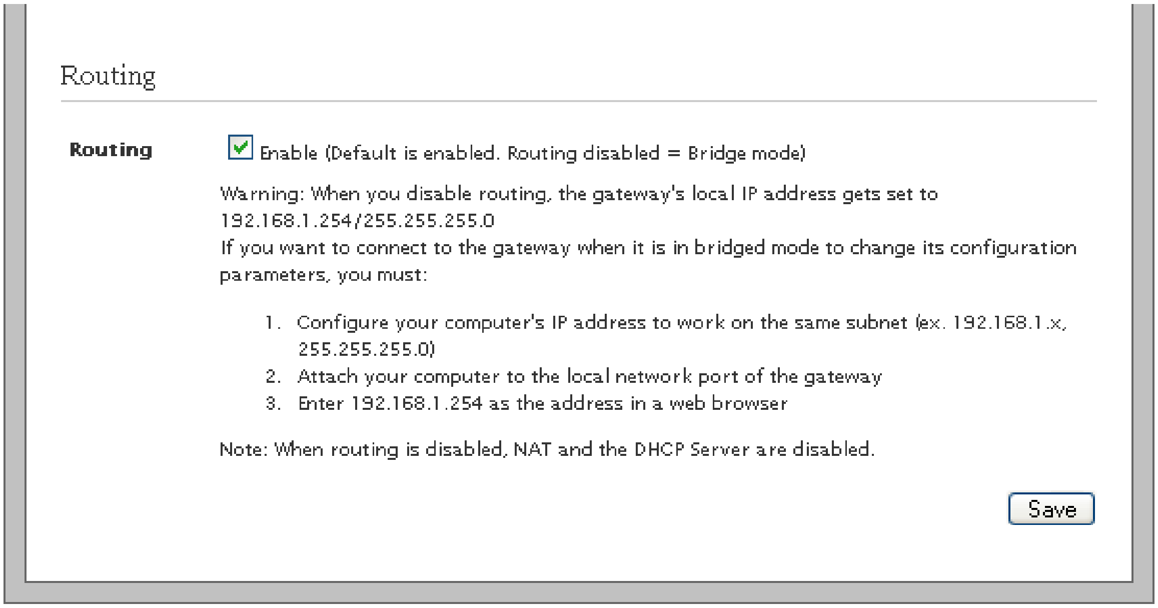
5. Select the **System MAC Address** option:
   - If you select **Use the built-in system MAC address: 00:1e:c7:a1:9c:50** radio button, your gateway connects to the Internet using the built-in MAC address.
   - If you select **Override the built-in MAC address** radio button, you have to specify the MAC address manually. You may have to override the existing MAC address if your cable modem connects to network devices based on their MAC address.

Configuring Routing Mode

The **Routing** panel lets you enable the routing mode. The gateway is pre-configured in the routing mode. Routing is disabled to configure your gateway in bridge mode.

To ensure that the gateway is in routed mode:

1. On the **Settings** tab, click **Broadband**, and then click **Link Configuration**.
2. Navigate to the **Routing** panel.



Routing

Routing ☑ Enable (Default is enabled. Routing disabled = Bridge mode)

Warning: When you disable routing, the gateway's local IP address gets set to 192.168.1.254/255.255.255.0
If you want to connect to the gateway when it is in bridged mode to change its configuration parameters, you must:

1. Configure your computer's IP address to work on the same subnet (ex. 192.168.1.x, 255.255.255.0)
2. Attach your computer to the local network port of the gateway
3. Enter 192.168.1.254 as the address in a web browser

Note: When routing is disabled, NAT and the DHCP Server are disabled.

3. Ensure that the **Enable** check box next to the **Routing** field is selected.

Note Routing is disabled to configure your gateway in bridge mode. When routing is disabled, the NAT and the DHCP servers are also disabled. Also, ensure that the WAN protocol is compatible to bridging mode.

4. Click **Save**.

   The Internet LED on the gateway becomes solid green and you can access the Internet. Open a Web browser to verify successful connection to the Internet.

See Also

Managing Broadband Settings on page 18

CHAPTER 4

Managing System Information

This chapter provides information about the tasks you can perform within the **System Info** tab. The links under the **System Info** tab and their associated tasks are as follows:

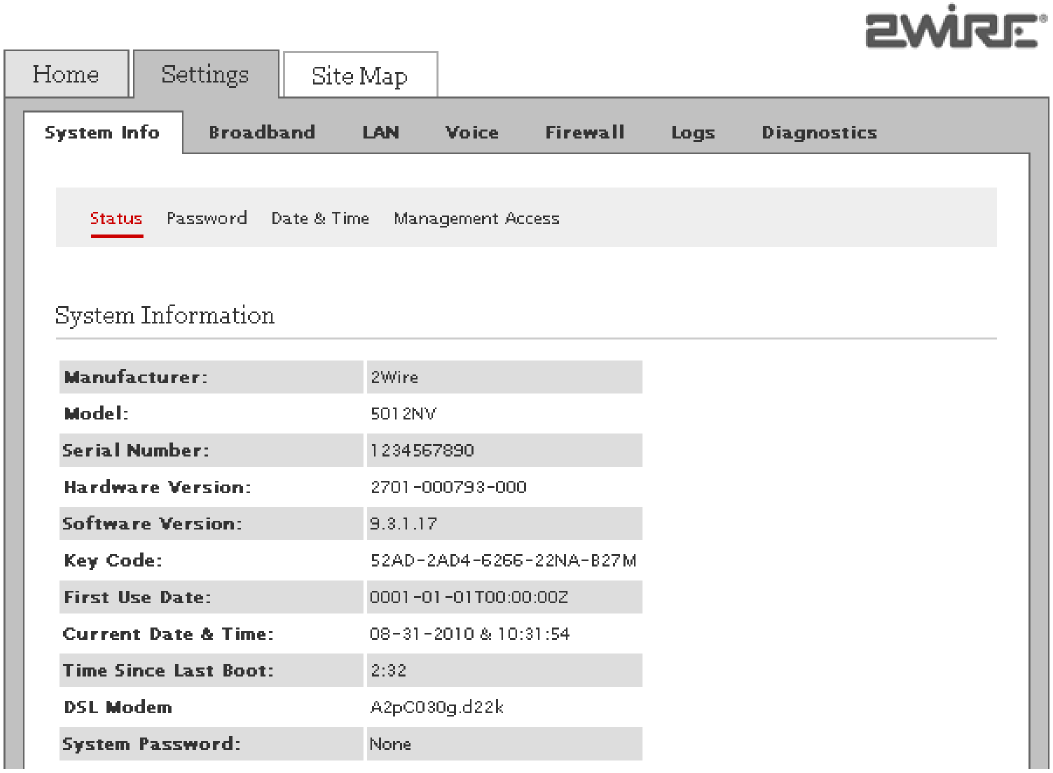
- Status
  - Viewing System Information on page 11
- Password
  - Creating System Password on page 12
  - Configuring System Password on page 13
- Date & Time
  - Configuring Date and Time on page 14
- Management Access
  - Enabling Remote Firmware Upgrade on page 16

Viewing System Information

View your gateway information at a glance. Find details pertaining to your gateway including the manufacturer name, model and serial number, and hardware and software versions.

On the **Settings** tab, click **System Info**, and then click **Status**.

Refer to the following image and table for information about the parameters listed in the **System Information** panel:



System Information

Manufacturer:	2Wire
Model:	5012NV
Serial Number:	1234567890
Hardware Version:	2701-000793-000
Software Version:	9.3.1.17
Key Code:	52AD-2AD4-6266-22NA-B27M
First Use Date:	0001-01-01T00:00:00Z
Current Date & Time:	08-31-2010 & 10:31:54
Time Since Last Boot:	2:32
DSL Modem	A2pC030g.d22k
System Password:	None

Parameter	Description
Manufacturer	Name of the gateway manufacturer.
Model	Model number of the gateway.
Serial Number	Serial number of the gateway.
Hardware Version	Hardware version number of the gateway.
Software Version	Software version number installed on the gateway.
Key Code	Key code of the gateway.
First Use Date	Date when the gateway was powered on for the first time out of factory.
Current Date and Time	Your current date and time.
Time Since Last Boot	Time elapsed since you last booted the gateway.
DSL Modem	Hardware version of the DSL modem. This field is only visible if the Broadband connectivity is through the DSL port of the gateway.
System Password	Displays **Default** if you use the default system password for your gateway. Displays **Custom** if you have created your own password for your gateway. Displays **None** if you have not enabled password protection for your gateway.

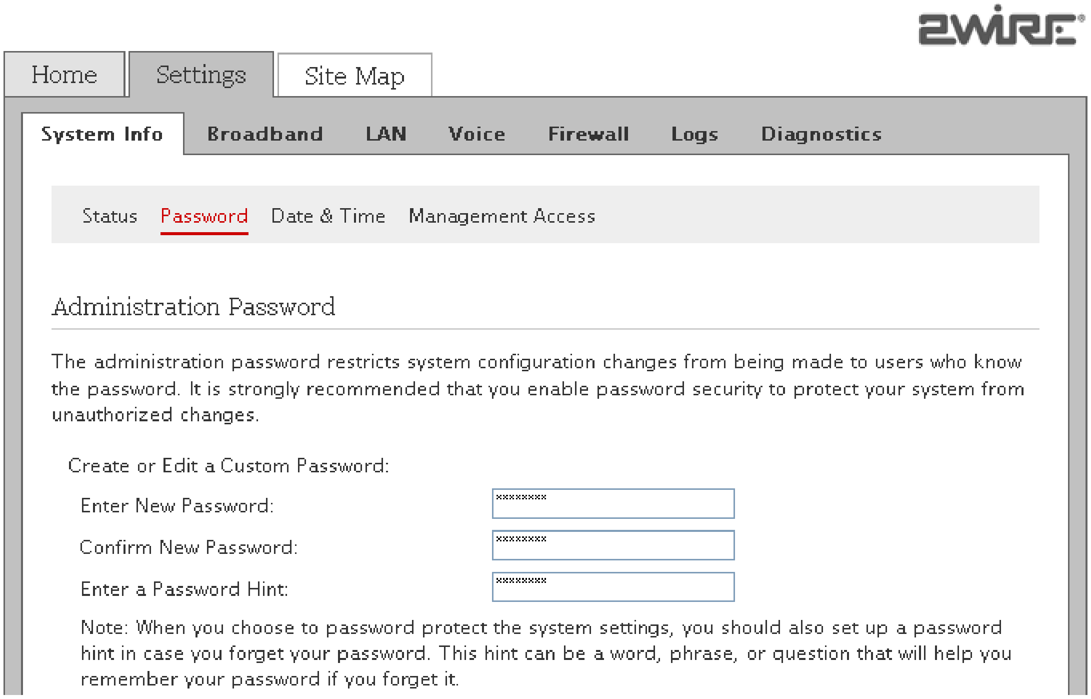
Creating System Password

Objective

To create a password for your gateway in order to protect it against unauthorized access.

Steps

1. On the **Settings** tab, click **System Info**, and then click **Password**.



Administration Password

The administration password restricts system configuration changes from being made to users who know the password. It is strongly recommended that you enable password security to protect your system from unauthorized changes.

Create or Edit a Custom Password:

Enter New Password: *********

Confirm New Password: *********

Enter a Password Hint: *********

Note: When you choose to password protect the system settings, you should also set up a password hint in case you forget your password. This hint can be a word, phrase, or question that will help you remember your password if you forget it.

2. Enter a password in the **Enter New Password** text box.

The password is case-sensitive, and can contain alpha-numeric characters with no spaces.

3. Enter the same password in the **Confirm New Password** text box.
4. Enter a hint in the **Enter a Password Hint** text box.

   A password hint can be a word, a phrase, or a question that can help you in case you forget your password.

Note It is strongly recommended that you enter a hint to act as a reminder.

5. Click **Save**.

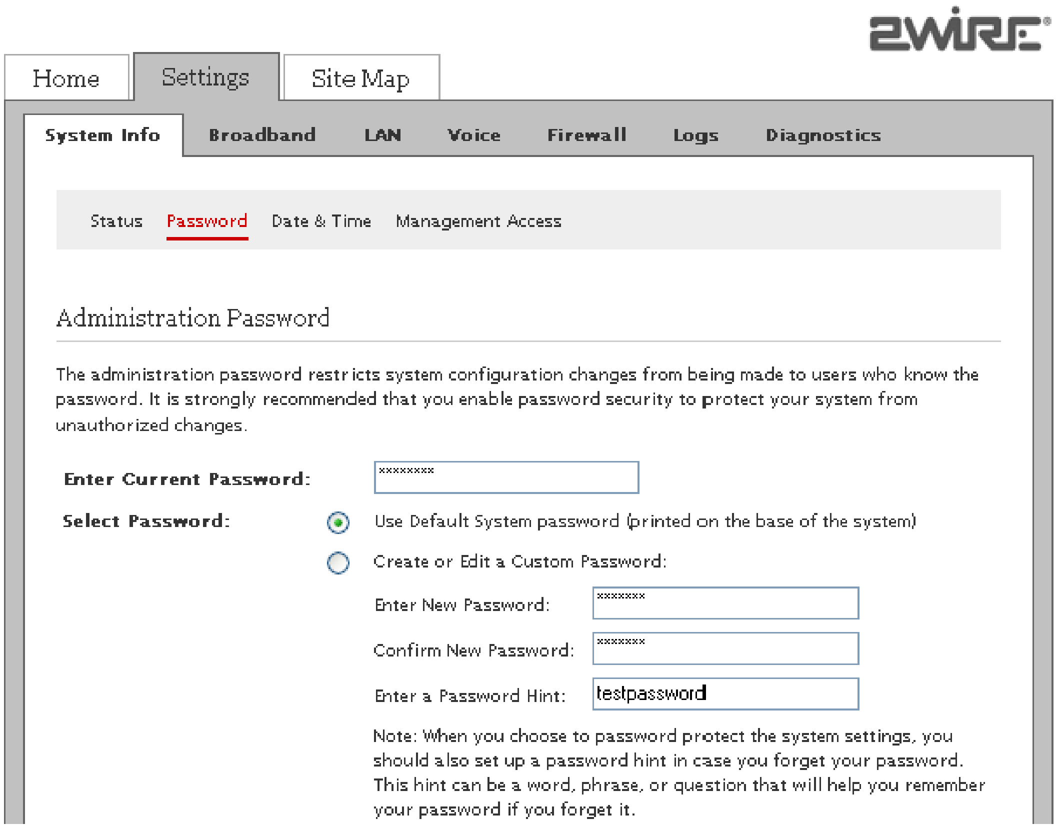
Configuring System Password

Objective

To modify the user defined password or use default password.

Steps

1. On the **Settings** tab, click **System Info**, and then click **Password**.



Administration Password

The administration password restr icts system configuration changes from being made to users who know the password. It is strongly recommended that you enable password security to protect your system from unauthor ized changes.

Enter Current Password: xxxxxxxx

Select Password:

● Use Default System password (printed on the base of the system)

○ Create or Edit a Custom Password:

Enter New Password: xxxxxxx

Confirm New Password: xxxxxxx

Enter a Password Hint: testpassword

Note: When you choose to password protect the system settings, you should also set up a password hint in case you forget your password. This hint can be a word, phrase, or question that will help you remember your password if you forget it.

2. Enter the default password in the **Enter Current Password** text box.

   The default password is printed on the base of the gateway.

3. Select the password option:
   - If you select **Use Default System password (printed on the base of the system)** radio button, skip to step 7 for using the default password. The lower section of the **Password** page displays the location and identification of the default password. Once you have saved the configuration changes, no further action is required.
   - If you select **Create or Edit a Custom Password** radio button, continue to step 4 for modifying the user defined password.
4. Enter a password in the **Enter New Password** text box.

   The password is case-sensitive, and can contain up to 31 alpha-numeric characters with no spaces.
5. Enter the same password in the **Confirm New Password** text box.
6. Enter a hint in the **Enter a Password Hint** text box.

   A password hint can be a word, a phrase, or a question that can help you in case you forget your password.

Note It is strongly recommended that you enter a hint to act as a reminder.

7. Click **Save**.

Configuring Date and Time

Objective

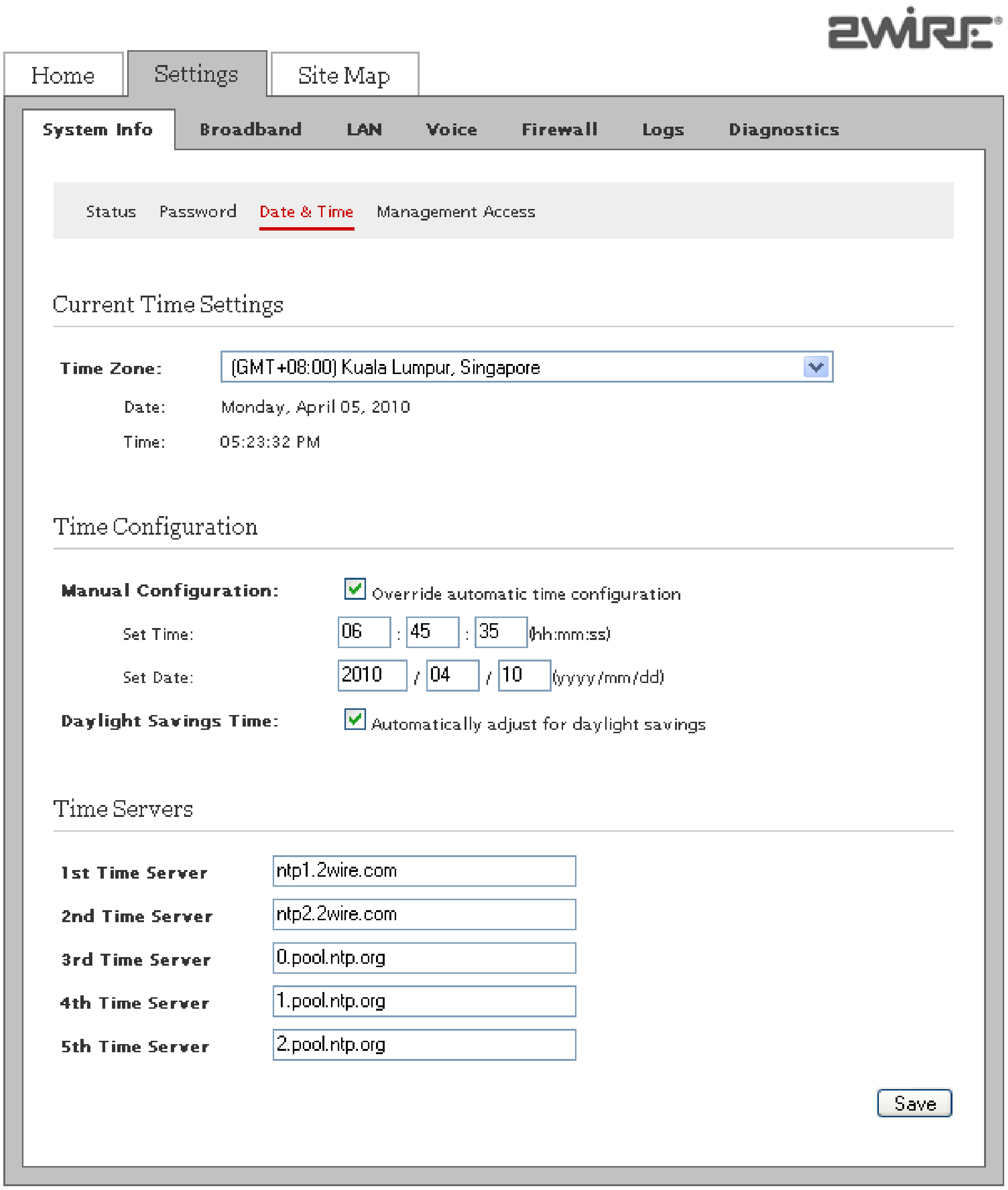
To configure the date and time on your gateway. You can either set up the date and time automatically or configure it manually.

The gateway sets the time automatically using time servers on the Internet. It retrieves date and time information in Greenwich Mean Time (GMT). Your local time is set using the Time Zone setting you configured when you set up your gateway.

Note It is recommended that you use the automatically configured time zone settings.

Steps

1. On the **Settings** tab, click **System Info**, and then click **Date & Time**.



Current Time Settings

Time Zone: (GMT+08:00) Kuala Lumpur, Singapore

Date: Monday, April 05, 2010

Time: 05:23:32 PM

Time Configuration

Manual Configuration: ☑ Override automatic time configuration

Set Time: 06 : 45 : 35 (hh:mm:ss)

Set Date: 2010 / 04 / 10 (yyyy/mm/dd)

Daylight Savings Time: ☑ Automatically adjust for daylight savings

Time Servers

1st Time Server	ntp1.2wire.com
2nd Time Server	ntp2.2wire.com
3rd Time Server	0.pool.ntp.org
4th Time Server	1.pool.ntp.org
5th Time Server	2.pool.ntp.org

2. Perform any of the following tasks:
   - Setting Date and Time Automatically on page 15
   - Manually Configuring Date and Time on page 16

Setting Date and Time Automatically

To set date and time automatically:

1. On the **Settings** tab, click **System Info**, and then click **Date & Time**.
2. Navigate to the **Current Time Settings** panel.
3. Select the desired **Time Zone** from the drop-down list box.
4. Leave the **Time Servers** values in the **Internet Time Servers (NTP)** panel as is, unless you want to change the location of the servers.

   The gateway automatically updates the time and date based on the inputs from these servers.
5. Click **Save**.

Note Select the **Daylight Savings Time** check box in the **Time Configuration** panel if daylight savings time is observed in your country/state.

Manually Configuring Date and Time

To manually configure the date and time:

1. On the **Settings** tab, click **System Info**, and then click **Date & Time**.
2. Navigate to **t**he **Time Configuration** panel.
3. Select the **Override automatic time configuration** check box.

   This task lets you override the automatically configured date and time settings on your gateway.
4. Enter the current time in the text boxes next to the **Set Time** field in the hh:mm:ss format.
5. Enter today's date in the text boxes next to the **Set Date** field in the yyyy/mm/dd format.
6. Select the **Automatically adjust for daylight savings** check box.
7. Click **Save**.

Note When you configure the date and time manually, remember to select the **Override automatic time configuration** check box.

Enabling Remote Firmware Upgrade

Objective

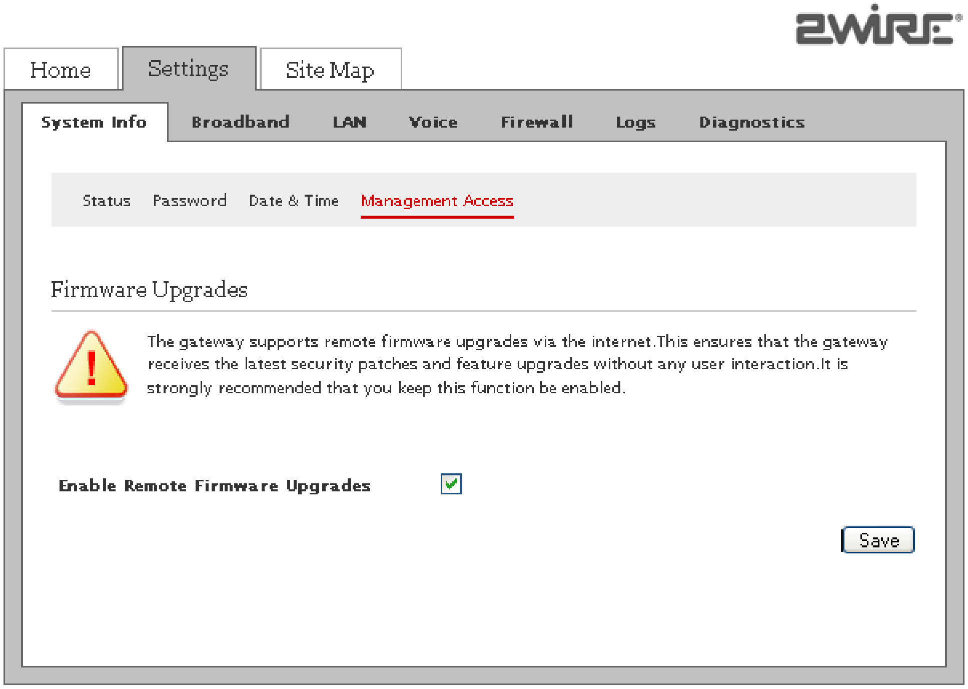
To enable remote firmware upgrade.

If you enabled this feature, the firmware on your gateway upgrades remotely without any user intervention, thus ensuring that the gateway has the latest security patches and feature upgrades for optimized performance.

Steps

1. On the **Settings** tab, click **System Info**, and then click **Management Access**.

   This open the **Firmware Upgrades** page.



Firmware Upgrades

The gateway supports remote firmware upgrades via the internet.This ensures that the gateway receives the latest security patches and feature upgrades without any user interaction.It is strongly recommended that you keep this function be enabled.

Enable Remote Firmware Upgrades ☑

2. Select the **Enable Remote Firmware Upgrades** check box.
3. Click **Save**.

See Also

Using Diagnostics Features on page 72

System Information Issues on page 84

CHAPTER 5

Managing Broadband Settings

This chapter provides information about the tasks you can perform within the **Broadband** tab. The links under the **Broadband** tab and their associated tasks are as follows:

- Status
  - Viewing Broadband Status on page 18
- Link Configuration
  - Configuring the Internet Connection on page 5
- Routing
  - Adding Static Routes on page 23
- Multicast
  - Configuring IP Multicast Settings on page 24
  - Viewing Multicast Settings on page 25
- DNS Resolution
  - Resolving Domain Name on page 26

Viewing Broadband Status

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

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

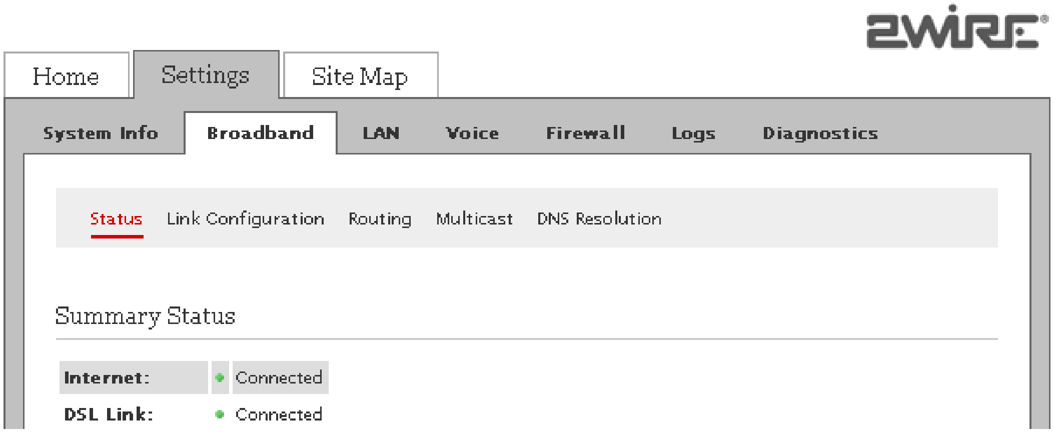
On the **Settings** tab, click **Broadband**, and then click **Status**. The following panels are displayed:

- Summary Status
- Internet Details
- DSL Details
- Traffic Statistics
- DSL Link Errors

Note The **DSL Link** field in the **Summary Status** panel, **ATM Traffic** section in the **Traffic Statistics** panel, **DSL Details** panel, and **DSL Link Errors** panel are not visible if you select **Ethernet** as the WAN interface type on the **Link Configuration** page.

Summary Status

Refer to the following image and table for information about the parameters listed in the **Summary Status** panel:



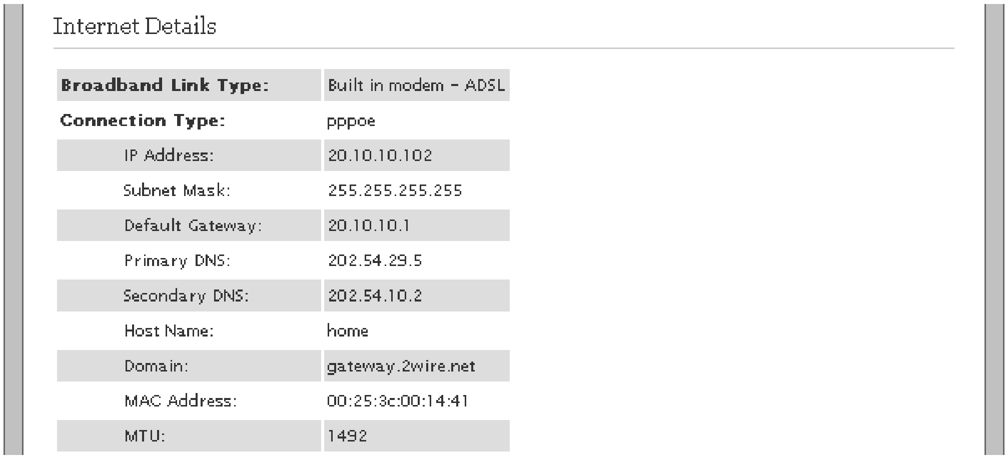
Summary Status

Internet:	● Connected
DSL Link:	● Connected

Parameter	Description
Internet	Displays the status of the Internet Connection. This displays **Connected** when the ISP acitvates your Internet connection.
DSL Link	Displays the status of the DSL connection. This displays **Connected** when the DSL port of the gateway is connected to the telephone jack. Ensure that your ISP activates the ADSL connection.

Internet Details

Refer to the following image and table for information about the parameters listed in the **Internet Details** panel:



Internet Details

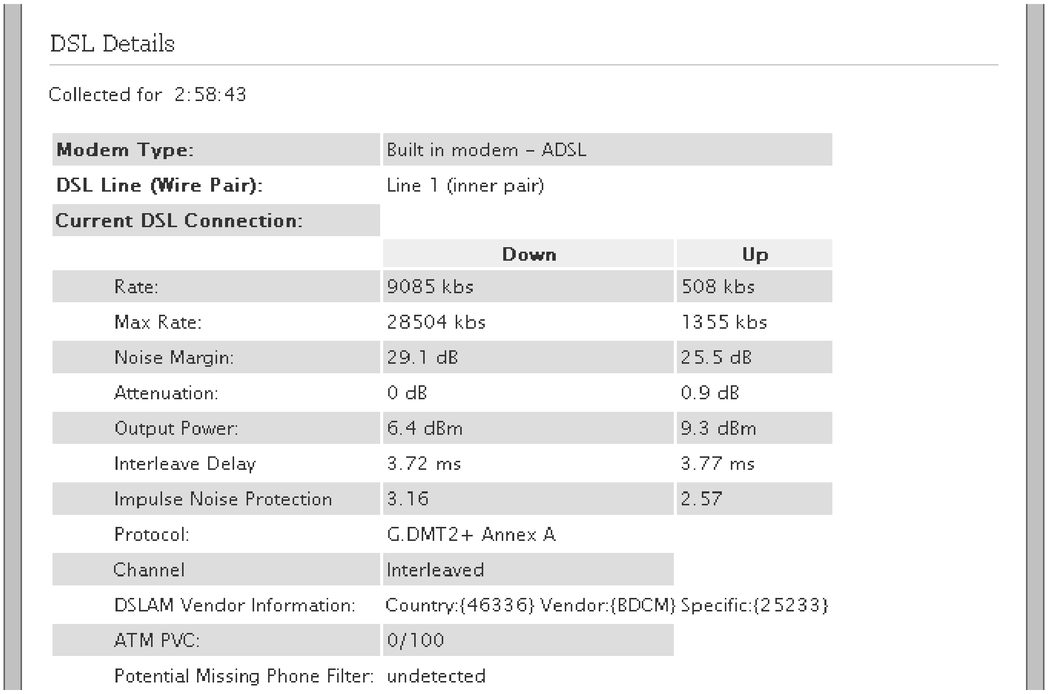
Broadband Link Type:	Built in modem - ADSL
Connection Type:	pppoe
IP Address:	20.10.10.102
Subnet Mask:	255.255.255.255
Default Gateway:	20.10.10.1
Primary DNS:	202.54.29.5
Secondary DNS:	202.54.10.2
Host Name:	home
Domain:	gateway.2wire.net
MAC Address:	00:25:3c:00:14:41
MTU:	1492

Parameter		Description
Broadband Link Type		Indicates the type of Broadband connection.
Connection Type		Identifies the method by which the gateway connects to the ISP. The available methods to connect to the ISP are PPPoE, PPPoA, Direct IP (DHCP), or Direct IP (Static).
Current Internet Connection		
	IP Address	Indicates the IP address assigned by the ISP to the gateway for connecting to the Internet.

Parameter		Description
	Subnet Mask	Indicates the subnet mask assigned by the ISP to the gateway.
	Default Gateway	Indicates the default gateway address that assigns an IP address to your gateway for accessing the Internet.
	Primary DNS	Indicates the IP address of the primary DNS server that the gateway uses for Domain Name resolution. DNS allows Internet users to specify a name (domain name) to reach a Web page (for example, www.domainname.com) instead of its Internet address (for example, 111.222.111.222). When you enter the name of a Web location (URL), the DNS looks up the name and resolves it to the Internet address of the Web page.
	Secondary DNS	Displays the backup if the Primary DNS fails to respond.
	Host Name	Displays the host name configured on the gateway.
	Domain	Displays the domain that associates your gateway with your ISP on the Broadband link.
	MAC Address	Displays the MAC address of the gateway.
	MTU	Indicates the maximum size of packets that are communicated on your ISP network.

DSL Details

Refer to the following image and table for information about the parameters listed in the **DSL Details** panel:



DSL Details

Collected for 2:58:43

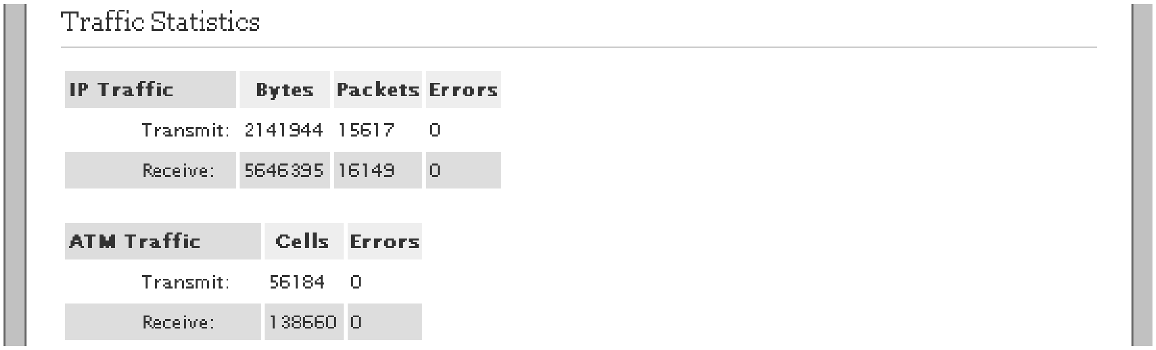
Modem Type:	Built in modem – ADSL	
DSL Line (Wire Pair):	Line 1 (inner pair)	
Current DSL Connection:		
	Down	**Up**
Rate:	9085 kbs	508 kbs
Max Rate:	28504 kbs	1355 kbs
Noise Margin:	29.1 dB	25.5 dB
Attenuation:	0 dB	0.9 dB
Output Power:	6.4 dBm	9.3 dBm
Interleave Delay	3.72 ms	3.77 ms
Impulse Noise Protection	3.16	2.57
Protocol:	G.DMT2+ Annex A	
Channel	Interleaved	
DSLAM Vendor Information:	Country:{46336} Vendor:{BDCM} Specific:{25233}	
ATM PVC:	0/100	
Potential Missing Phone Filter:	undetected	

Parameter	Description
Modem Type	Displays the type of modem: • **Built-in ADSL modem** -or- • **External Broadband modem through the Internet**
DSL Line (Wire Pair)	Displays **Line 1 (inner pair)**, **Line 2 (outer pair)**, or **searching for DSL signal**. During installation, the gateway auto-detects whether the DSL signal is on Line 1 or Line 2.

Parameter		Description
Current DSL Connection		
	Rate	Displays the upload and download speeds in kilobits per second.
	Max Rate	Displays the maximum trained rates for upstream and downstream data in kilobits per second.
	Noise Margin	Displays the current downstream and upstream noise margin in dB.
	Attenuation	Displays the current downstream and upstream DSL attenuation in dB.
	Output Power	Displays the current downstream and upstream DSL transmit and receive power in dB.
	Interleave Delay	Displays the downstream and upstream interleave delay duration in milliseconds (ms).
	Impulse Noise Protection	Displays the measurement of how much impulse noise can be mitigated. It is dependent on the current line configuration.
	Protocol	Displays the protocol used to communicate between your gateway and your ISP.
	Channel	Displays the setting that is determined by your ISP's DSLAM equipment. Values are **Fast** or **Interleaved**.
	DSLAM Vendor Information	Lists information about the DSLAM, including country, DSLAM vendor, and specifics.
	ATM PVC	Displays the VPI/VCI value currently in use by your ISP.
	Potential Missing Phone Filter	Detects if the DSL port of the gateway is connected to the phone socket through a DSL phoneline filter.

Traffic Statistics

Refer to the following image and table for information about the parameters listed in the **Traffic Statistics** panel:



Traffic Statistics

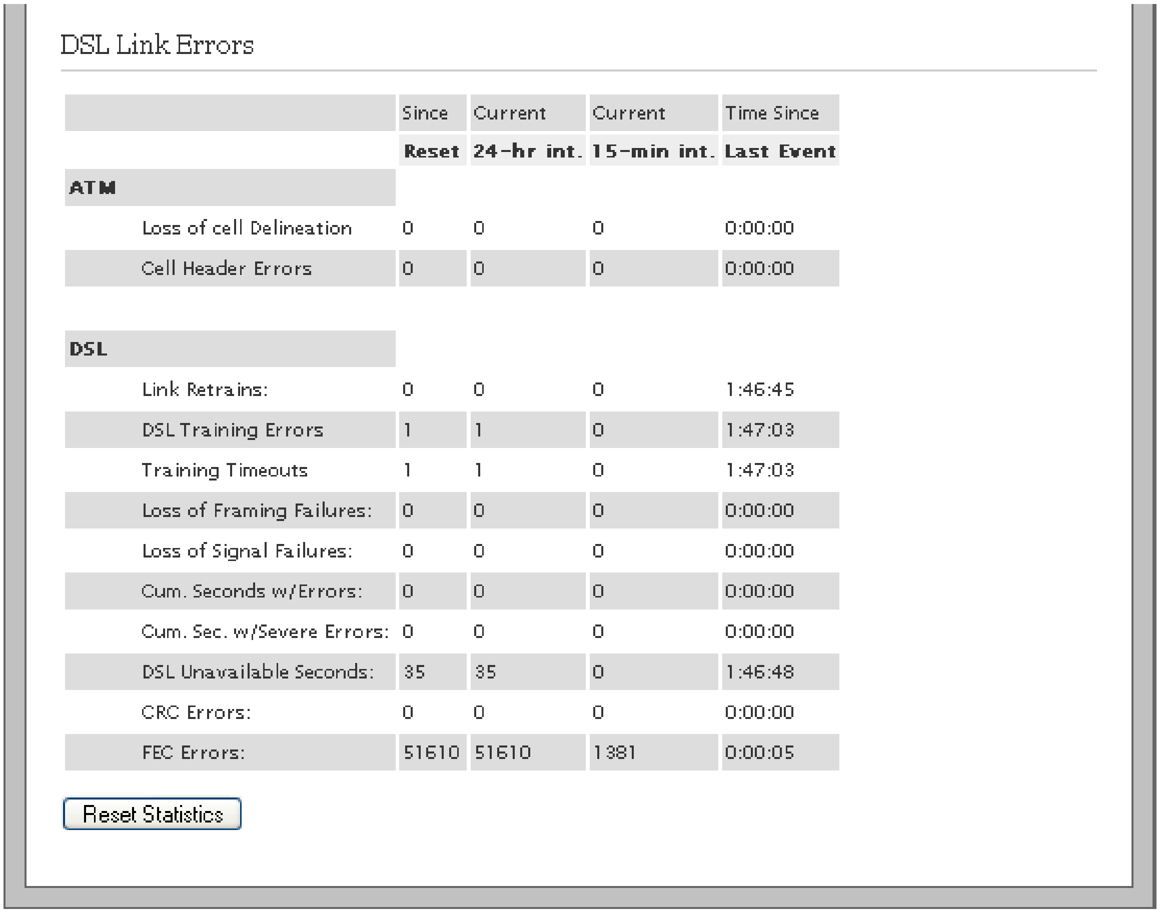
IP Traffic	Bytes	Packets	Errors
Transmit:	2141944	15617	0
Receive:	5646395	16149	0

ATM Traffic	Cells	Errors
Transmit:	56184	0
Receive:	138660	0

Parameter	Description
IP Traffic	
Transmit	Displays the cumulative number of bytes, IP packets, and errors transmitted.
Receive	Displays the cumulative number of bytes, IP packets, and errors received.
ATM Traffic	
Transmit	Displays the cumulative number of ATM cells and errors transmitted.
Receive	Displays the cumulative number of ATM cells and errors received.

DSL Link Errors

Refer to the following image and table for information about the parameters listed in the **DSL Link Errors** panel:



DSL Link Errors

	Since	Current	Current	Time Since
	Reset	**24-hr int.**	**15-min int.**	**Last Event**
ATM				
Loss of cell Delineation	0	0	0	0:00:00
Cell Header Errors	0	0	0	0:00:00
DSL				
Link Retrains:	0	0	0	1:46:45
DSL Training Errors	1	1	0	1:47:03
Training Timeouts	1	1	0	1:47:03
Loss of Framing Failures:	0	0	0	0:00:00
Loss of Signal Failures:	0	0	0	0:00:00
Cum. Seconds w/Errors:	0	0	0	0:00:00
Cum. Sec. w/Severe Errors:	0	0	0	0:00:00
DSL Unavailable Seconds:	35	35	0	1:46:48
CRC Errors:	0	0	0	0:00:00
FEC Errors:	51610	51610	1381	0:00:05

Parameter	Description
ATM	
Loss of cell Delineation	Displays the number of loss of cell delineation events since the last reset.
Cell Header Errors	Displays the number of cell header errors since the last reset.
DSL	
Link Retrains	Displays the number of DSL retrains since the gateway was last restarted, and the time elapsed since the last retrain.
DSL Training Errors	Displays the number of failed DSL retrains since the gateway was last restarted, and the elapsed time since the last failed retrain.
Training Timeouts	Displays the number of timeouts waiting for response from ATU-C since the gateway was last restarted, and the elapsed time since the last initialization timeout.
Loss of Framing Failures	Displays the number of DSL loss of framing failures since the gateway was last restarted, and the elapsed time since the last line search initialization.
Loss of Signal Failures	Displays the number of DSL loss of signal failures since the 2Wire gateway was last restarted, and the elapsed time since the last loss of signal failure.
Cum. Seconds w/Errors	Displays the number of cumulative errored seconds since the gateway was last restarted, and the elapsed time since the last error.

Parameter	Description
Cum. Sec. w/Severe Errors	Displays the number of severely errored seconds since the gateway was last restarted, and the elapsed time since the last severely errored second.
DSL Unavailable Seconds	Displays the DSL link unavailable seconds after the ISP connection was established and the statistics were last reset. Also displays the elapsed time since the last establishment.
CRC Errors	Displays the Cyclic Redundancy Check (CRC) errors.
FEC Errors	Displays the Forward Error Correction (FEC) errors.

Note After rectifying the issues that are displayed in different panels of the **Status** page, you must reset this page to determine if the issue is resolved. Click **Reset Statistics** at the bottom of the **Status** page to view the updated statistics.

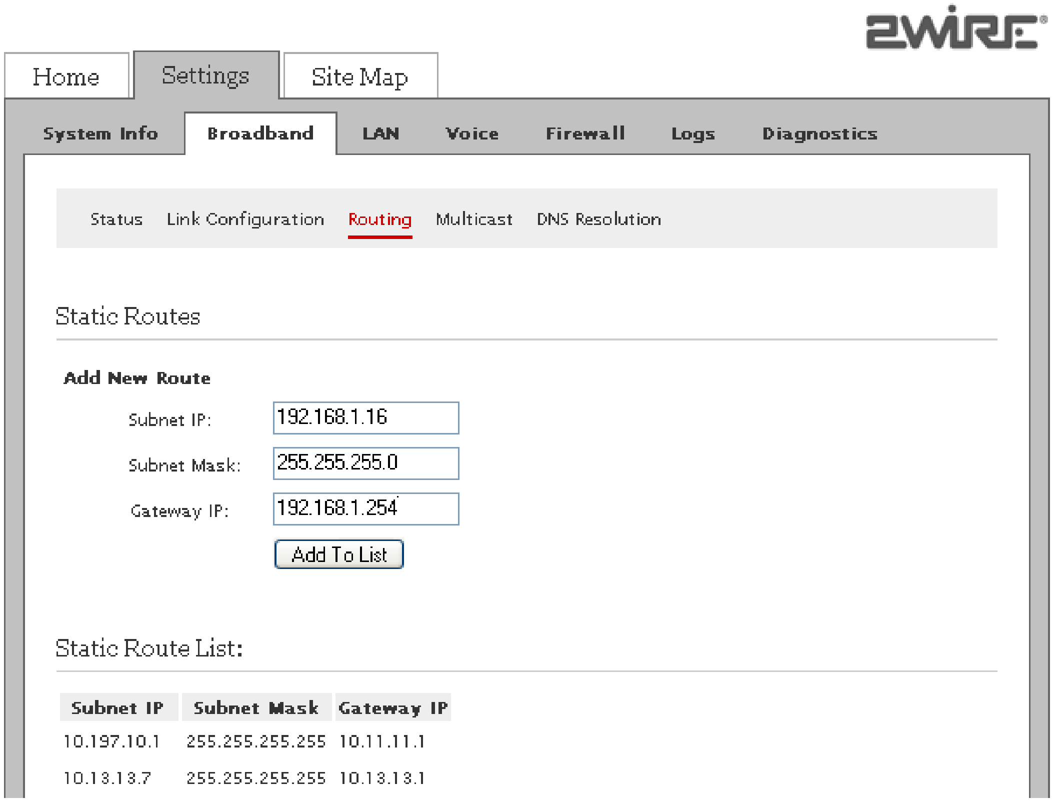
Adding Static Routes

Objective

To manually configure static routes for specifying the data transmission path between the devices that are outside the gateway network.

Steps

1. On the **Settings** tab, click **Broadband**, and then click **Routing**.



Static Routes

Add New Route

Subnet IP: 192.168.1.16

Subnet Mask: 255.255.255.0

Gateway IP: 192.168.1.254

Static Route List:

Subnet IP	Subnet Mask	Gateway IP
10.197.10.1	255.255.255.255	10.11.11.1
10.13.13.7	255.255.255.255	10.13.13.1

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

5. Click **Add To List**.

Note The **Static Route List** panel displays the new **Subnet IP**, **Subnet Mast**, and **Gateway IP**.

Configuring IP Multicast Settings

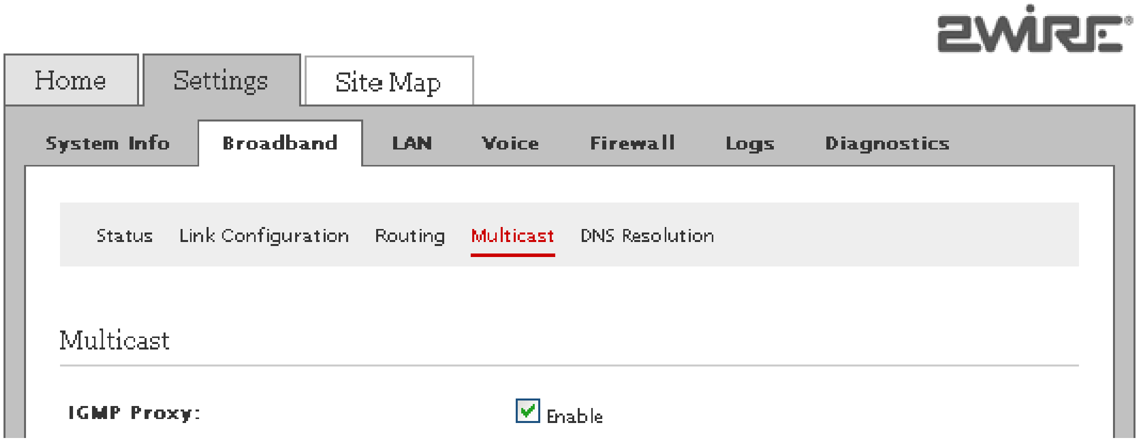
Objective

To configure IGMP or IP Multicast for activating IPTV services through the gateway.

Internet Group Management Protocol (IGMP) is used to manage IP Multicast sessions. IGMP provides a means to automatically allow the flow of multicast traffic, which blocks unwanted traffic in your local network.

Steps

1. On the **Settings** tab, click **Broadband**, and then click **Multicast**.



IGMP Proxy: ☑ Enable

2. Select the **IGMP Proxy** check box to enable the feature.

   If you enable this feature, the Set Top Box (STB) connected to the gateway gains controlled access to multicast services like IPTV using IGMP/MLD Proxying.

   Note To access IPTV services through the gateway, **IGMP Proxy** must be enabled.

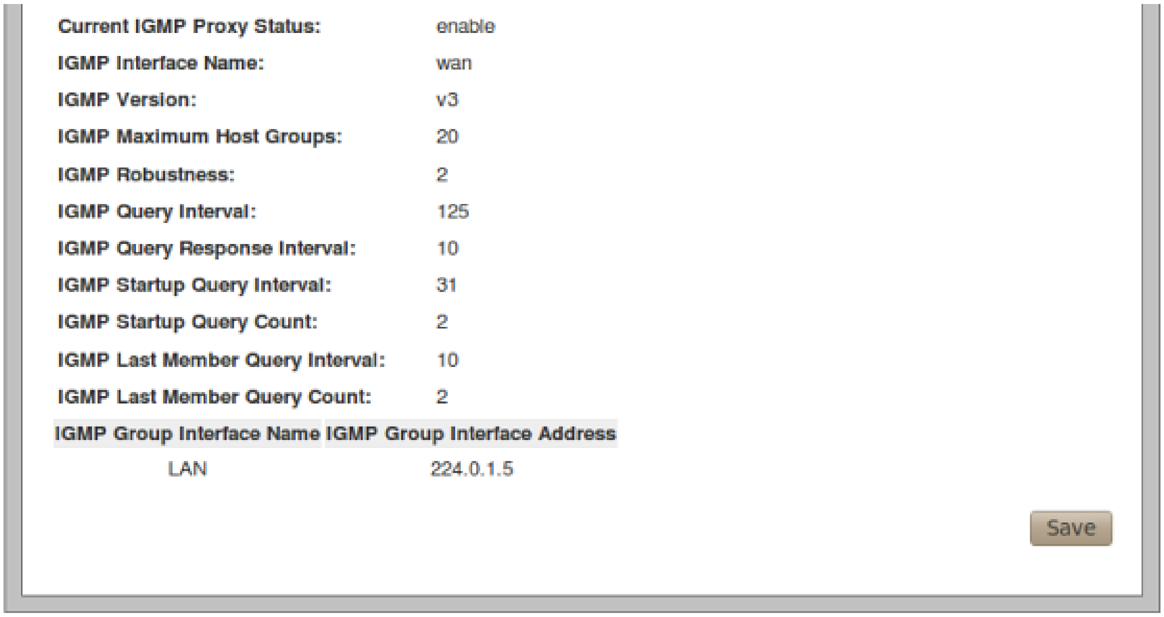
3. Click **Save**.

Viewing Multicast Settings

View the multicast settings to determine the IGMP functionality and status of its associated services.

On the **Settings** tab, click **Broadband**, and then click **Multicast**.

Refer to the following image and table for information about the parameters listed on the **Multicast** page:



Current IGMP Proxy Status: enable
IGMP Interface Name: wan
IGMP Version: v3
IGMP Maximum Host Groups: 20
IGMP Robustness: 2
IGMP Query Interval: 125
IGMP Query Response Interval: 10
IGMP Startup Query Interval: 31
IGMP Startup Query Count: 2
IGMP Last Member Query Interval: 10
IGMP Last Member Query Count: 2

IGMP Group Interface Name	IGMP Group Interface Address
LAN	224.0.1.5

Parameter	Description
Current IGMP Proxy Status	Displays the current status of IGMP Proxy configuration. If the Broadband connection is not functional, the IGMP Proxy status displays disabled even though IGMP Proxy is enabled.
IGMP Interface Name	Displays the name of the interface for which statistics are being reported.
IGMP Version	Displays the IGMP version.
IGMP Maximum Host Groups	Displays the maximum number of multicast groups.
IGMP Robustness	Displays the time interval that the gateway waits for a report in response to a group-specific query.
IGMP Query Interval	Displays the time interval at which the gateway sends membership queries when it is the querier.
IGMP Query Response Interval	Displays the time interval that the gateway waits for a report in response to a general query.
IGMP Startup Query Interval	Displays the amount of time in seconds between successive General Query messages sent by a querier during startup.
IGMP Startup Query Count	Displays the number of general query messages sent at startup.
IGMP Last Member Query Interval	Displays the time interval that the gateway waits for a report in response to a group-specific query.
IGMP Last Member Query Count	Displays the number of Group-Specific Query messages sent before the gateway assumes that there are no members of the host group being queried on this interface.
IGMP Group Interface Name	Displays the name of the interfacerequesting for multicast access.
IGMP Group Interface Address	Displays the multicast IP address your LAN host (STB) sends to join the corresponding streams.

Resolving Domain Name

Objective

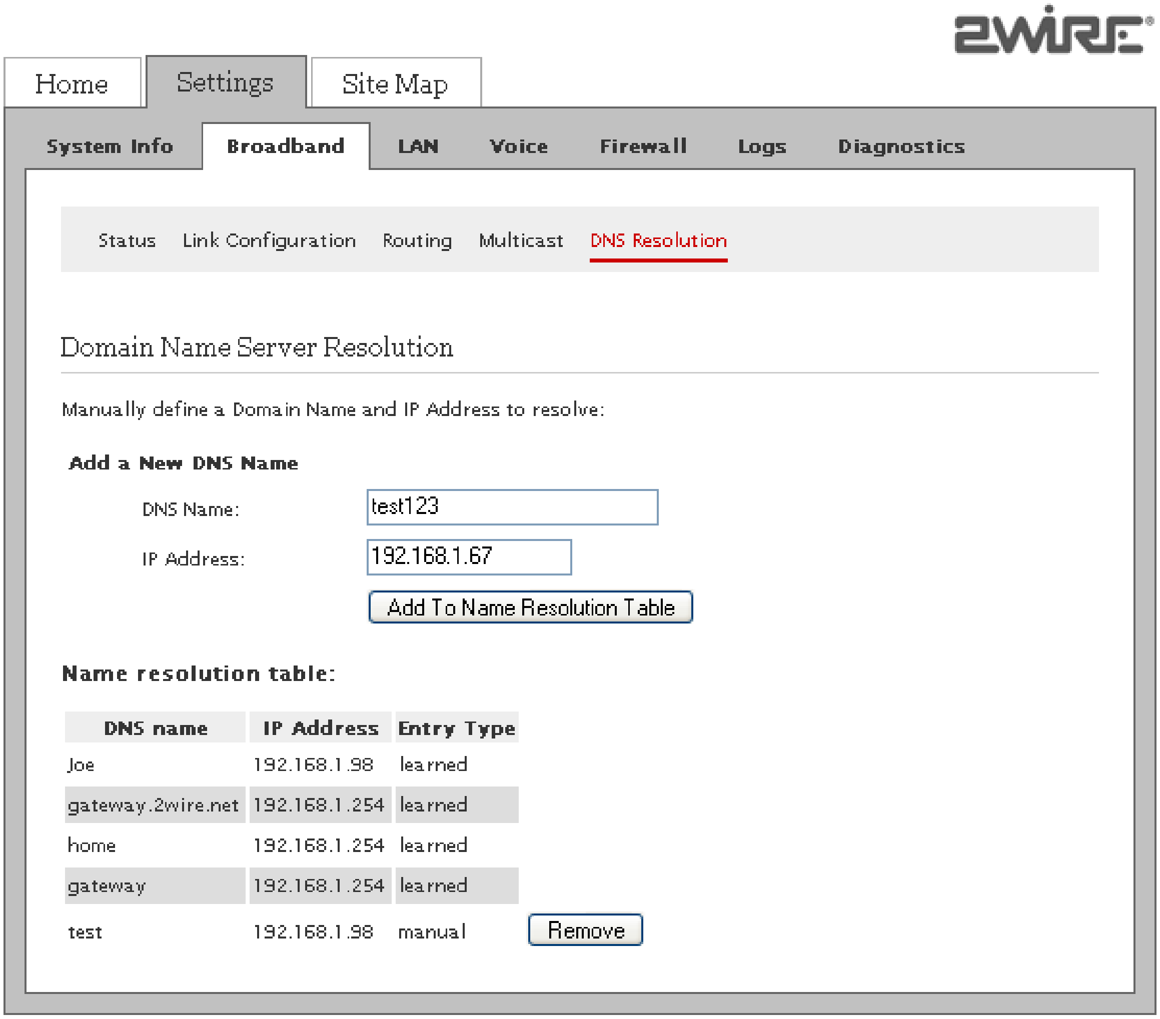
To manually add a domain name for resolving the IP address of the networked devices.

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

Note Verify that the domain name is not in use before specifying the DNS name for a networked device.

Steps

1. On the **Settings** tab, click **Broadband**, and then click **DNS Resolution**.



Domain Name Server Resolution

Manually define a Domain Name and IP Address to resolve:

Add a New DNS Name

DNS Name: test123

IP Address: 192.168.1.67

Name resolution table:

DNS name	IP Address	Entry Type	
Joe	192.168.1.98	learned	
gateway.2wire.net	192.168.1.254	learned	
home	192.168.1.254	learned	
gateway	192.168.1.254	learned	
test	192.168.1.98	manual	Remove

2. Enter a name for the network device in the **DNS Name** text box.
3. Enter the IP address of the network device in the **IP Address** text box.
4. Click **Add To Name Resolution Table**.

   The **Name Resolution Table** panel displays the newly added and existing **DNS name**, **IP address**, and **Entry type** values in the corresponding columns. The **Entry type** column displays whether the DNS name is **learned** (auto-populated) or **manual** (manually added).

Note To delete the manually added user appearing in the **Name resolution table**, locate the relevant details and click **Remove**.

See Also

Managing LAN Devices on page 28

Managing Firewall Settings on page 56

Using Diagnostics Features on page 72

LAN Issues on page 84

CHAPTER 6

Managing LAN Devices

This chapter provides information about the tasks you can perform within the **LAN** tab. The links under the **LAN** tab and their associated tasks are as follows:

Viewing LAN Status

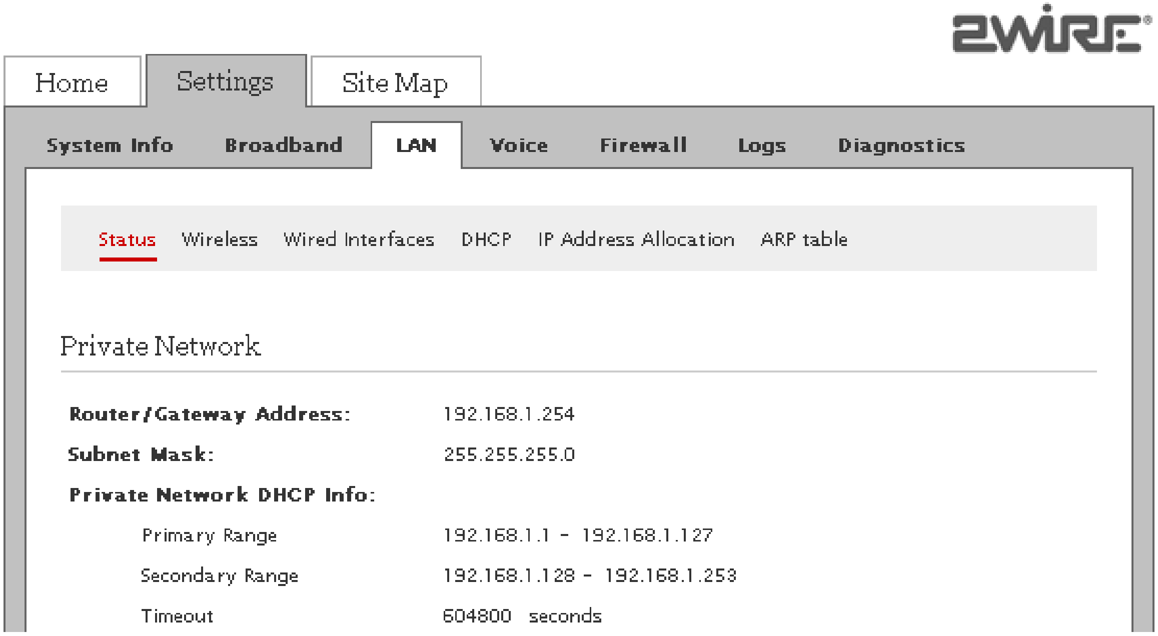
View the LAN client parameters, LAN interface status, wireless parameters, and traffic statistics.

On the **Settings** tab, click **LAN**, and then click **Status**. The following panels are displayed:

- Private Network
- Interfaces
- Wireless
- Devices
- Traffic Statistics

Private Network

Refer to the following image and table for information about the parameters listed in the **Private Network** panel:



Private Network

Router/Gateway Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Private Network DHCP Info:

Primary Range 192.168.1.1 - 192.168.1.127

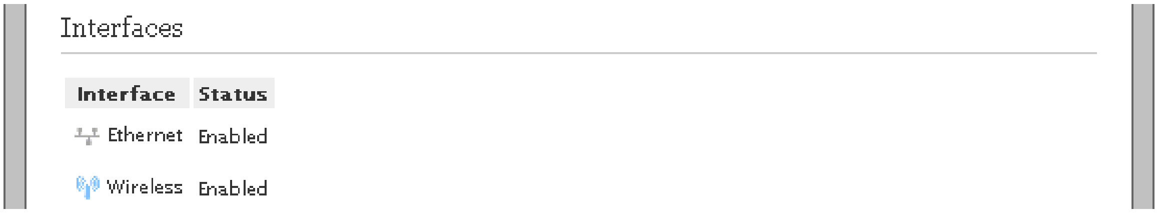
Secondary Range 192.168.1.128 - 192.168.1.253

Timeout 604800 seconds

<table>
<tr><th colspan="2">Parameter</th><th>Description</th></tr>
<tr><td colspan="2"><b>Router/Gateway Address</b></td><td>IP address allocated to the gateway.</td></tr>
<tr><td colspan="2"><b>Subnet Mask</b></td><td>Subnet mask allocated to the gateway.</td></tr>
<tr><td colspan="3"><b>Private Network DHCP Info</b></td></tr>
<tr><td rowspan="3"></td><td><b>Primary Range</b></td><td>Range of IP addresses available on the network to be automatically assigned to the network devices.</td></tr>
<tr><td><b>Secondary Range</b></td><td>Range of IP addresses available on the network to be assigned to the LAN clients on the network after the gateway exhausts primary range of IP address(es).</td></tr>
<tr><td><b>Timeout</b></td><td>Time in seconds to grant the DHCP lease to a LAN client.</td></tr>
</table>

Interfaces

Refer to the following image and table for information about the parameters listed in the **Interfaces** panel:



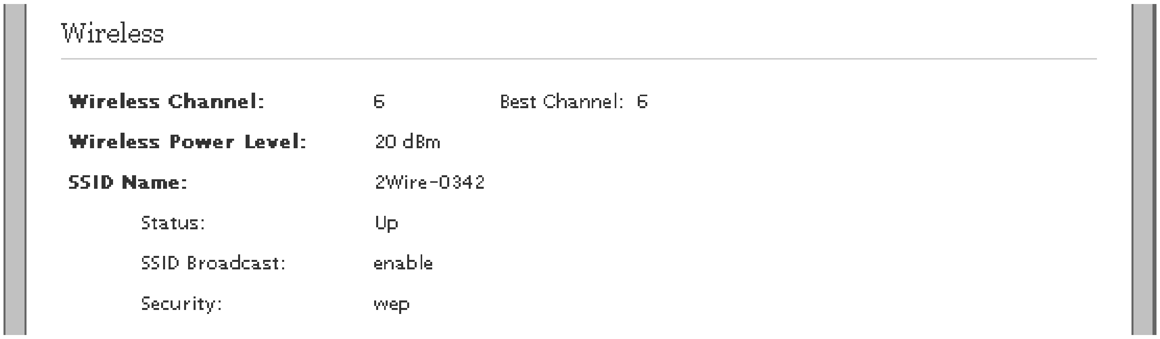
Interfaces

Interface	Status
Ethernet	Enabled
Wireless	Enabled

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

Wireless

Refer to the following image and table for information about the parameters listed in the **Wireless** panel:



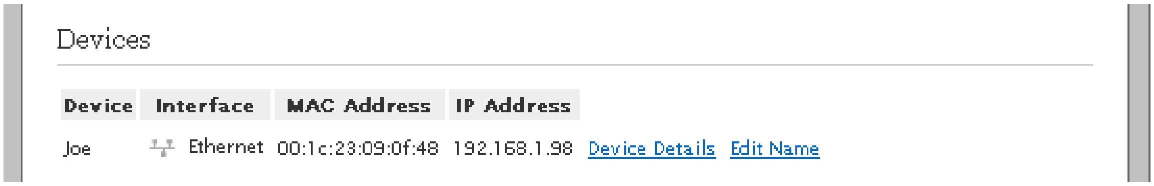
Wireless

Wireless Channel:	6	Best Channel: 6
Wireless Power Level:	20 dBm	
SSID Name:	2Wire-0342	
Status:	Up	
SSID Broadcast:	enable	
Security:	wep	

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

Devices

Refer to the following image and table for information about the parameters listed in the **Devices** panel:



Devices

Device	Interface	MAC Address	IP Address		
Joe	Ethernet	00:1c:23:09:0f:48	192.168.1.98	Device Details	Edit Name

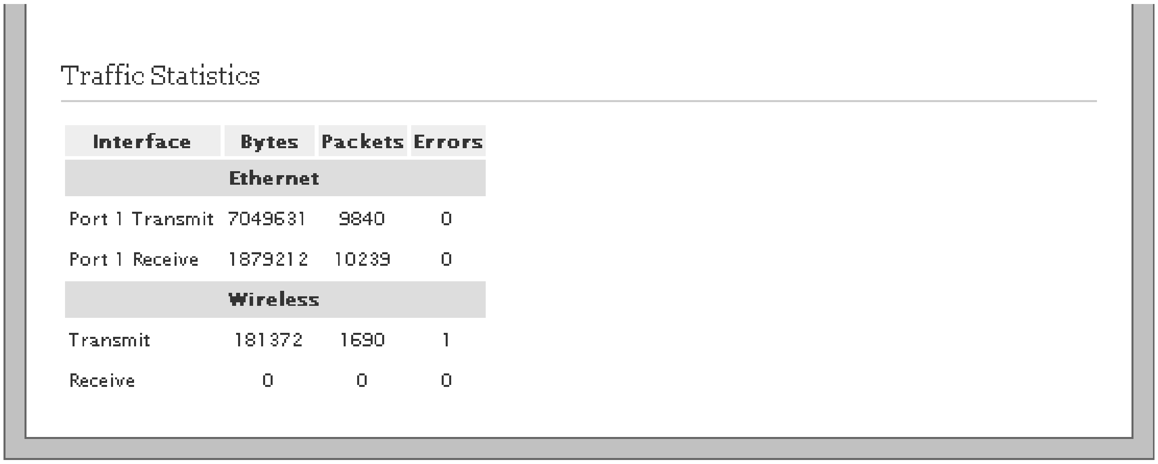
Parameter	Description
Device	Displays the name of the network device.
Interface	Displays the interface type used by the network device.
MAC Address	Displays the MAC address of the network device.
IP Address	Displays the IP address allocated to the network device.

Note Click **Device Details** to view further information about the network device.

Note Click **Edit Name** to modify the name of the network device appearing on the Status page.

Traffic Statistics

Refer to the following image and table for information about the parameters listed in the **Traffic Statistics** panel:



Traffic Statistics

Interface	Bytes	Packets	Errors
Ethernet			
Port 1 Transmit	7049631	9840	0
Port 1 Receive	1879212	10239	0
Wireless			
Transmit	181372	1690	1
Receive	0	0	0

Parameter	Description
Ethernet	Displays the number of bytes, packets, and errors while transmitting and receiving data from the Ethernet interfaces.
Wireless	Displays the number of bytes, packets, and errors while transmitting and receiving data from the wireless interfaces.

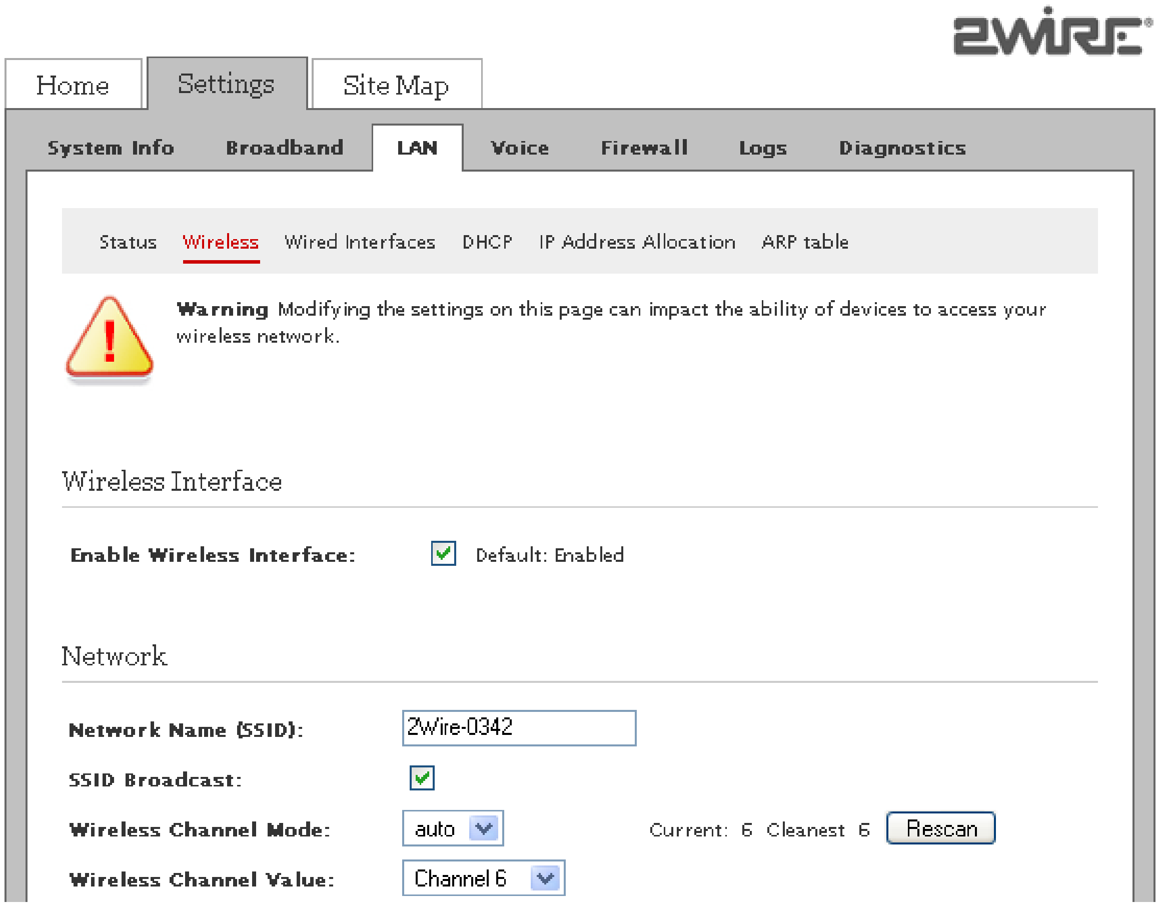
Setting Up Your Wireless Network

Objective

To set up the access to the wireless interface of the gateway. 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 recommended to provide a unique name for your wireless network to easily identify it, and connect to the desired wireless network.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.



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

Wireless Interface

Enable Wireless Interface: ☑ Default: Enabled

Network

Network Name (SSID): 2Wire-0342

SSID Broadcast: ☑

Wireless Channel Mode: auto Current: 6 Cleanest 6

Wireless Channel Value: Channel 6

2. Select the **Enable Wireless Interface** check box to enable the accessibility of the wireless interface.
3. Enter a name assigned to your wireless network in the **Network Name (SSID)** text box.

   The default name is 2WIRE*XXX*, where *XXX* represents the last three digits of your 2Wire gateway serial number (for example, 2WIRE008). This name appears next to the **Wireless** icon on the **Home** page.
4. Selecting the **SSID Broadcast** check box enables the visibility of the gateway to users who scan to connect to a wireless network.

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

5. Select the type of **Wireless Channel Mode** from the drop-down list box.

   The types of modes available are **fixed** or **auto**. Also, you can click **Rescan** to search for a channel with the lowest interference in the entire spectrum.

   - If you select **Fixed** from the drop-down list box, you must select a relevant wireless channel value that is compatible with the wireless clients in the vicinity.
   - If you select **Auto** from the drop-down list box, a channel is automatically selected to minimize interference. It is recommended to select auto, as this ensures seamless connectivity.

6. Select a **Wireless Channel Value** (radio frequency band) from the drop-down list box only if the selection is **Fixed** in the **Wireless Channel Mode** drop-down list box.

Note	Wireless clients or wireless adapter cards auto-detect the channels transmitted by the gateway. If you are having problems with your wireless network, it could be due to radio interference. You can change the wireless channel value to reduce interference.

7. Click **Save**.

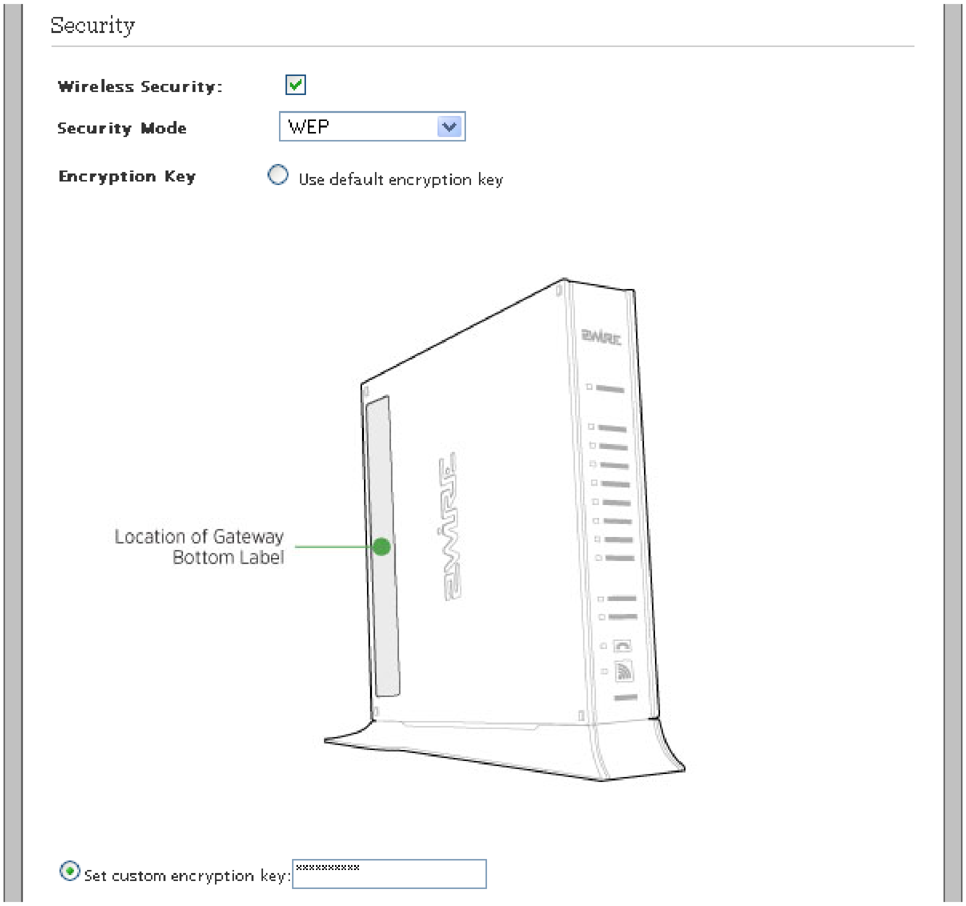
Securing the Wireless Network Using Encryption Key

Objective

To block unauthorized users to access your network. Each wireless client must use the key for connecting to the network. It is recommended that you customize the encryption key for wireless communication.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.
2. Navigate to the **Security** panel.



Security

Wireless Security: ☑

Security Mode: WEP

Encryption Key ○ Use default encryption key

● Set custom encryption key: **********

3. Select the **Wireless Security** check box to enable the wireless security.
4. Select an authentication setting from the **Security Mode** drop-down list box.

   Refer to the following table for information about the types of secure authentication protocol types:

Authentication Type	Description
WEP	The Wireless Encryption Protocol (WEP) is an older security protocol that allows any wireless clients within the radio range to access your network without an encryption key. This setting provides the least level of security. For security reasons, do not select this setting unless there is a compatibility issue with an older wireless client. For added protection, set an encryption key on your access point and enter the same key into your other wireless clients.
WPA-PSK	This setting provides good security and works with most newer wireless clients. This setting requires an encryption key on the access point and the wireless client configured to use Wi-Fi Protected Access – Pre-Shared Key (WPA-PSK) with the same encryption key.
WPA2-PSK	This setting requires that wireless clients use only WPA2-PSK to access your networks. An encryption key must be configured on the access point and entered into the wireless client. WPA2-PSK is currently the most secure Wi-Fi encryption protocol but may not be available on older wireless clients.
WPA-PSK Mixed	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 access point and the same key must be entered on the wireless client.

5. Select the **Encryption Key** option:
   - If you select **Use default encryption key** radio button, you can continue to use the encryption key that came with your gateway.
   - If you select **Set custom encryption key** radio button, you have to create a custom encryption key. You can define a 64-bit or 128-bit hexadecimal/ASCII encryption key. For 64-bit encryption, enter a 10-digit hexadecimal number or 5 ASCII characters. For 128-bit encryption, enter a 26-digit hexadecimal number or 13 ASCII characters. This security key will be used by all clients to access your wireless network.

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

6. Click **Save**.

Configuring Wi-Fi Protected Setup Using PIN Method

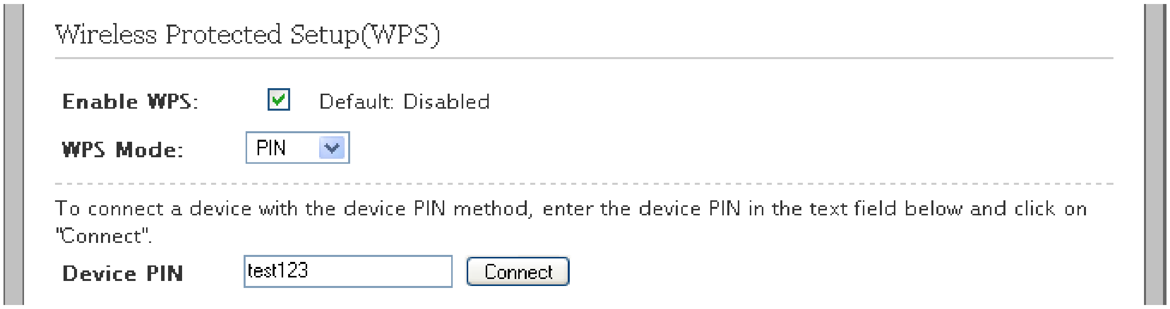
Objective

To configure Wi-Fi Protected Setup (WPS) for simplifying the process of accessing the wireless network of your gateway.

WPS supports PIN-based configuration method. When WPS is enabled, the gateway automatically detects the presence of a WPS-enabled LAN client. PIN-based configuration method requires WPA or WPA2 enabled security.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.
2. Navigate to the **Wi-Fi Protected Setup** panel.



Wireless Protected Setup(WPS)

Enable WPS: ☑ Default: Disabled

WPS Mode: PIN

To connect a device with the device PIN method, enter the device PIN in the text field below and click on "Connect".

Device PIN test123

3. Select the **Enable WPS** check box.

   This enables the configuration of WPS using the **PIN** method.
4. Select **PIN** from the **WPS Mode** drop-down list box.
5. Click **Save**.
6. Enter the PIN generated by the wireless client in the **Device PIN** text box.
7. Click **Connect** to establish the wireless connectivity.

Configuring Wi-Fi Protected Setup Using PUSH Method

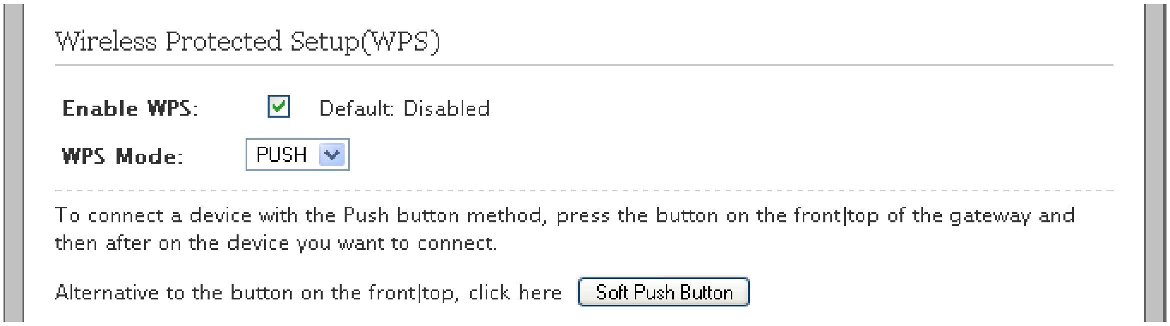
Objective

To configure Wi-Fi Protected Setup (WPS) for simplifying the process of accessing the wireless network of your gateway.

WPS supports push button configuration methods. When WPS is enabled, the gateway automatically detects the presence of a WPS-enabled LAN client. Push button configuration method requires WPA or WPA2 enabled security.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.
2. Navigate to the **Wi-Fi Protected Setup** panel.



Wireless Protected Setup(WPS)

Enable WPS: ☑ Default: Disabled

WPS Mode: PUSH

To connect a device with the Push button method, press the button on the front|top of the gateway and then after on the device you want to connect.

Alternative to the button on the front|top, click here

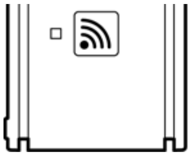
3. Select the **Enable WPS** check box.

   This enables the configuration of WPS using the **Push** method.
4. Select **PUSH** from the **WPS Mode** drop-down list box.
5. Click **Save**.
6. Click **Soft Push Button** followed by using the PUSH method on the LAN client (as advised by the OEM of the wireless client).

   -OR-

   Push the WPS button found at the front panel of the gateway followed by using the PUSH method on the LAN client (as advised by the OEM of the wireless client).

The WPS button found at the front panel of the gateway appears as follows:



The synchronization between the access point and the client is established within 120 seconds.

Enabling Wireless Multimedia

Objective

To enable wireless multimedia (WMM).

The WMM feature helps you to control the multimedia traffic on the shared network connections.

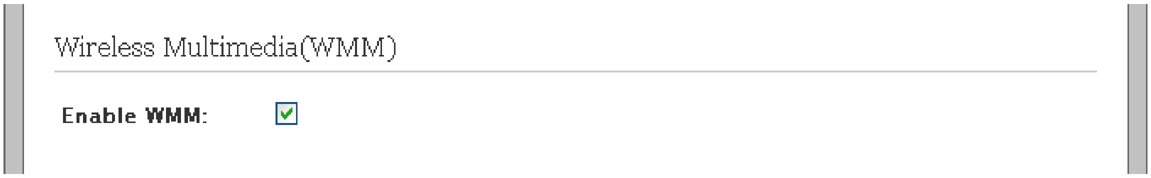
If you enable this feature, the gateway prioritizes the data packets based on the following four categories:

- Voice
- Video
- Best effort
- Background

This minimizes the chance of packet collisions caused by more than one device accessing the wireless medium at the same time. Before transmitting the gate on the network, network devices have to wait for a preconfigured time period to find if any other device is communicating. The random back-off period gives all devices a fair opportunity to transmit.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.
2. Navigate to the **Wireless Multimedia(WMM)** panel.



Wireless Multimedia(WMM)

Enable WMM: ☑

3. Select the **Enable WMM** check box.
4. Click **Save**.

Securing the Wireless Network Using MAC Filtering

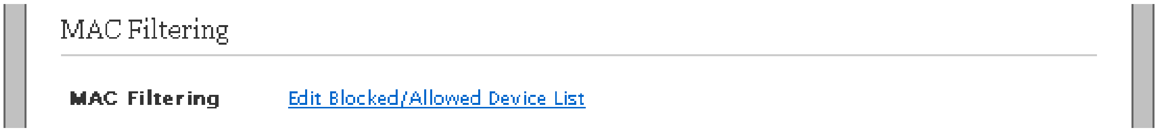
Objective

To block or allow wireless connection to all devices available on the network, or an individual device based on the MAC address of the device.

You allow only “known and trusted” devices to associate with the wireless access point. MAC address filtering is disabled by default. When enabled, the wireless connection is granted only to the MAC addresses that are pre-configured as whitelist.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.
2. Navigate to the **MAC Filtering** panel.

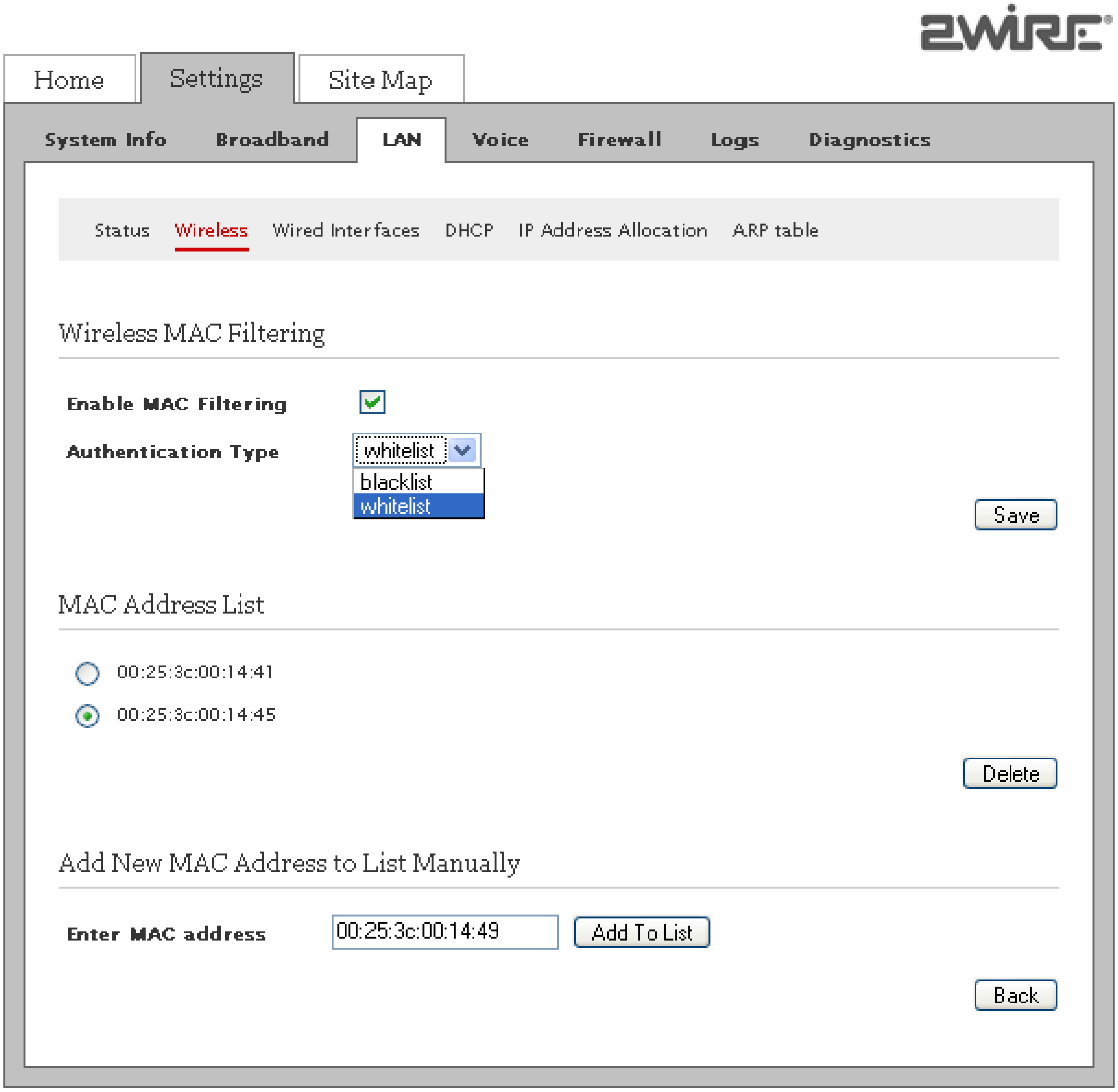


MAC Filtering

MAC Filtering: Edit Blocked/Allowed Device List

3. Click **Edit Blocked/Allowed Device List** link.

   This opens the **Wireless MAC Filtering** page.



Wireless MAC Filtering

Enable MAC Filtering ☑

Authentication Type: whitelist

MAC Address List

○ 00:25:3c:00:14:41

● 00:25:3c:00:14:45

Add New MAC Address to List Manually

Enter MAC address: 00:25:3c:00:14:49

4. Select the **Enable MAC Filtering** check box to enable MAC filtering.

Note	Disabling MAC address filtering allows all the wireless clients to access the gateway.

5. Select the **Authentication Type** option:
   - If you select **whitelist**, only the network devices that have their MAC addresses listed under **MAC Address List** panel are granted wireless access of the gateway.

- If you select **blacklist**, only the network devices that have their MAC addresses listed under **MAC Address List** panel are blocked from accessing the wireless services of the gateway.

6. Click **Save**.
7. Navigate to the **Add New MAC Address to List Manually** panel.
8. Enter the MAC address of the device in **Enter MAC address** text box.
9. Click **Add To List**.

   This populates the MAC address of the device in the **MAC Address List** panel.

Note To delete an entry from the **MAC Address List** panel, select the radio button of the relevant MAC address and click **Delete**.

Customizing Advance Wireless Settings

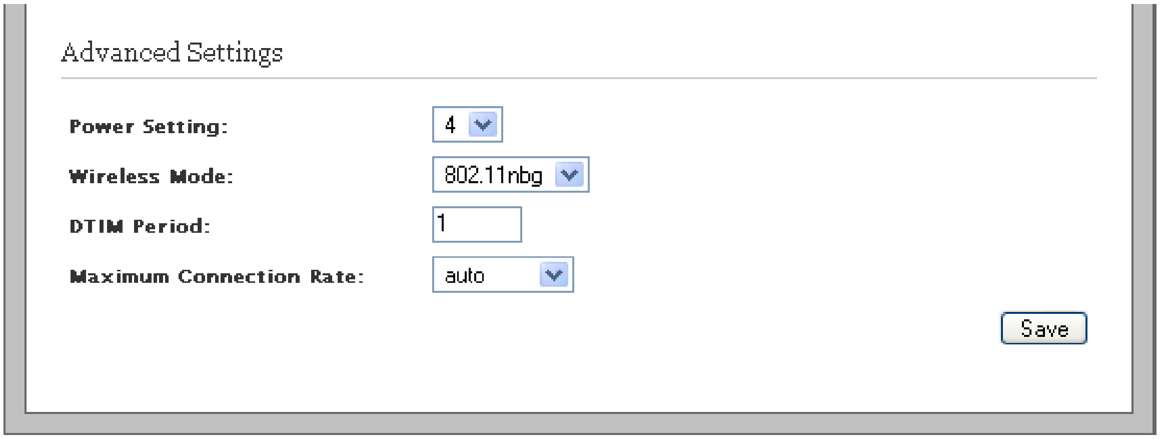
Objective

To customize the advanced wireless settings for optimizing the performance and accessibility of the wireless interface.

Note It is recommended that you retain the default settings. However, if you are experiencing connection or performance difficulties, altering these settings may improve performance.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wireless**.
2. Navigate to the **Advanced Settings** panel.



Advanced Settings

Power Setting: 4

Wireless Mode: 802.11nbg

DTIM Period: 1

Maximum Connection Rate: auto

3. Select the power level for your wireless connection from the **Power Setting** drop-down list box.

   Select an appropriate power level value in the range of **1** to **7**. The configured power level is the actual transmitted radio power at the access point.

   Refer to the following table for the power setting value and their associated radio output power levels:

Power Setting	Radio Output Power (dBm)
1	14
2	15
3	16
4	17

Power Setting	Radio Output Power (dBm)
5	18
6	19
7	20

4. Select the **Wireless Mode** from the drop-down list box.

   This allows you to force the gateway to use **802.11b**, **802.11g**, **802.11bg**, **802.11ng**, or **802.11nbg** modes of operation.

   Note Check the wireless mode supported by the wireless adapter before configuring this option.

5. Enter the **DTIM Period** in the text box.

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

6. Select the **Maximum Connection Rate** from the drop-down list box.

   This is the maximum rate at which your wireless connection works.

   - Select **1**, **2**, **5.5**, **11**, or **24** Mbps for 802.11b-based models.
   - Select **1**, **2**, **5.5**, **6**, **9**, **11**, **12**, **24**, **36**, **48**, or **54** Mbps for 802.11b/g-based models.

   It is recommended to select **auto** so that the access point determines the maximum rate at which the wireless connection must operate.

7. Click **Save**.

Disabling Ethernet Ports

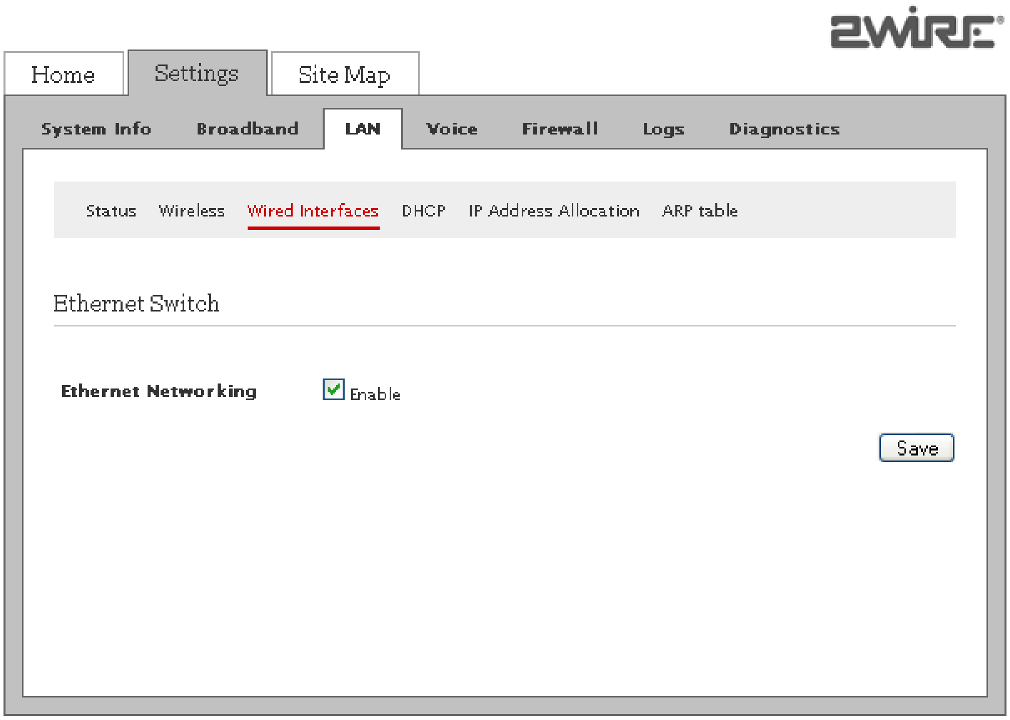
Objective

To disable the local Ethernet ports used to physically connect your gateway to the network devices.

This blocks the physical access to your gateway through the Ethernet ports, thus securing the access to your gateway. However, after disabling the Ethernet ports, you can still continue to access your gateway using the wireless connection.

Steps

1. On the **Settings** tab, click **LAN**, and then click **Wired Interfaces**.



Ethernet Switch

Ethernet Networking ☑ Enable

2. Clear the **Ethernet Networking** check box to disable the Ethernet ports on your gateway.
3. Click **Save**.

Note By default, the Ethernet ports are enabled and are capable of auto-negotiating the bandwidth required by the LAN clients.

Setting Up DHCP to Assign Default Range of IP Address

Objective

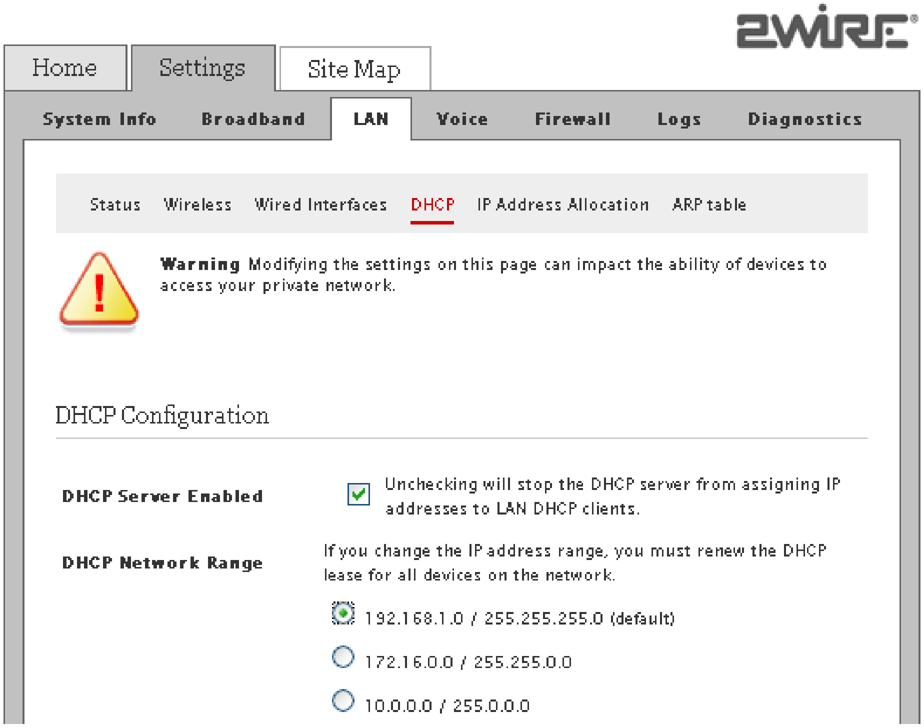
To set up your private network by assigning default range of IP address.

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

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

Steps

1. On the **Settings** tab, click **LAN**, and then click **DHCP**.



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

DHCP Configuration

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

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

● 192.168.1.0 / 255.255.255.0 (default)

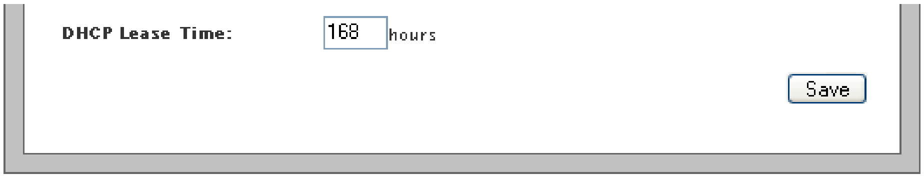
○ 172.16.0.0 / 255.255.0.0

○ 10.0.0.0 / 255.0.0.0

2. Select the **DHCP Server Enabled** check box to enable the DHCP server.
3. Select any of the **192.168.1.0 / 255.255.255.0 (default)**, **172.16.0.0 / 255.255.0.0** or **10.0.0.0 / 255.255.0.0** radio buttons.

   This lets your gateway dynamically assign the default range of IP address(es) to the LAN client(s)

   Note The software supports private, public routed, and public proxied subnets simultaneously on the LAN.



DHCP Lease Time: 168 hours

4. Enter a numerical value in the **DHCP Lease Time** text box.

   This value represents the number of hours you can use the assigned IP address before the DHCP lease expires.
5. Click **Save**.

Setting Up DHCP to Assign Manually Configured Range of IP Address

Objective

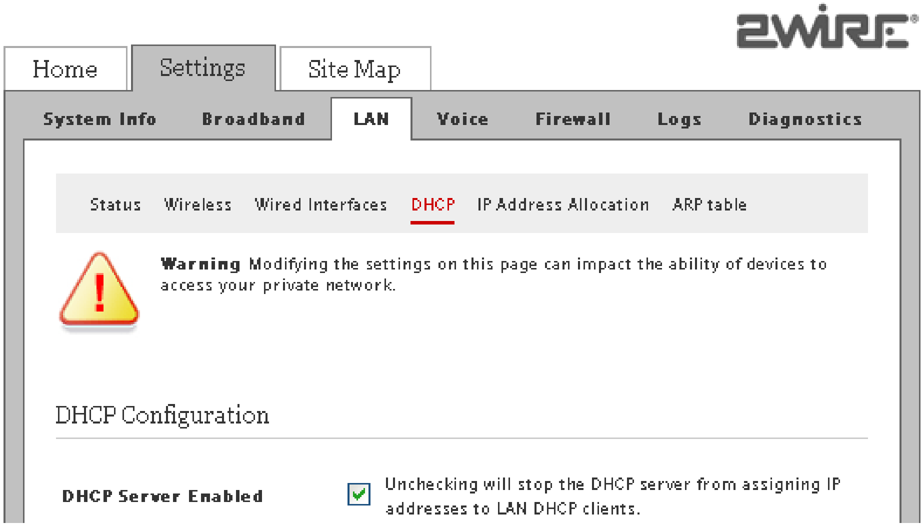
To set up your private network by assigning manually configured range of IP address.

By default, the gateway uses the 192.168.1.0/255.255.0.0 IP address range. When you select manual configuration, the LAN clients are assigned IP addresses within the specified range.

Note Manually configure these settings *only* if you have expertise in IP inter-networking. An incorrect configuration can cause unpredictable results.

Steps

1. On the **Settings** tab, click **LAN**, and then click **DHCP**.

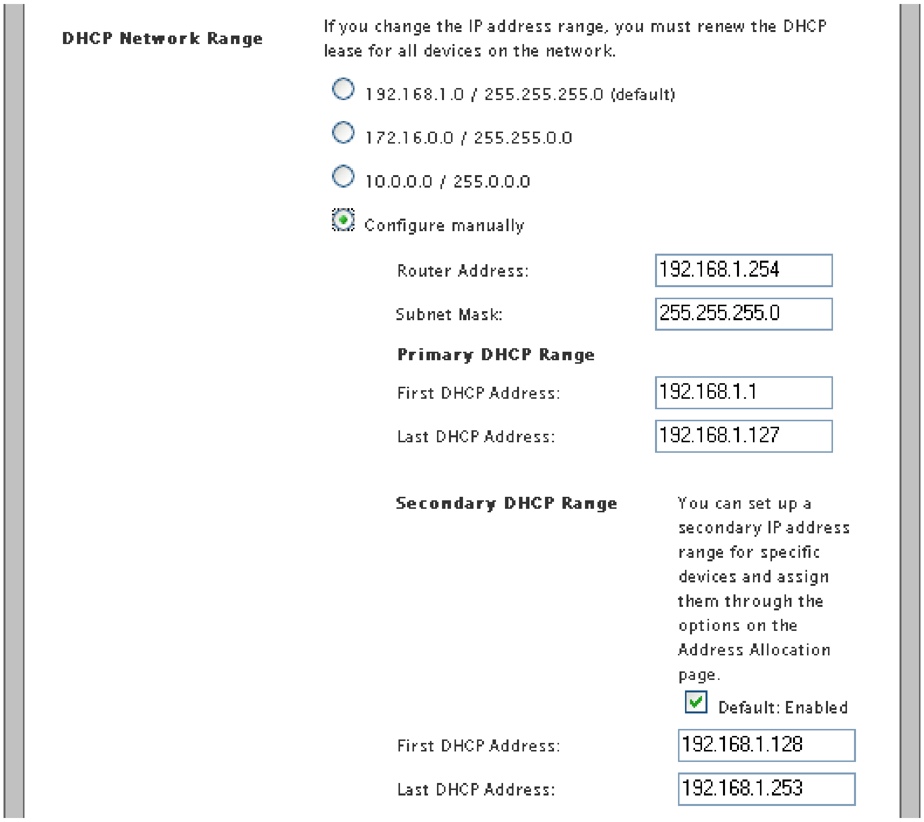


Warning Modifying the settings on this page can impact the ability of devices to access your private network.

DHCP Configuration

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

2. Select the **DHCP Server Enabled** check box to enable the DHCP server.



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

○ 192.168.1.0 / 255.255.255.0 (default)

○ 172.16.0.0 / 255.255.0.0

○ 10.0.0.0 / 255.0.0.0

● Configure manually

Router Address: 192.168.1.254

Subnet Mask: 255.255.255.0

Primary DHCP Range

First DHCP Address: 192.168.1.1

Last DHCP Address: 192.168.1.127

Secondary DHCP Range You can set up a secondary IP address range for specific devices and assign them through the options on the Address Allocation page.

☑ Default: Enabled

First DHCP Address: 192.168.1.128

Last DHCP Address: 192.168.1.253

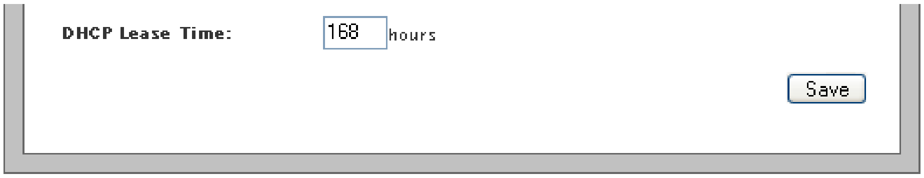
3. Select the **Configure manually** radio button.

   This lets you set up a range IP address(es) to be assigned to the LAN client(s).

4. Enter the default IP address of your gateway used for all communication on your local devices in the **Router Address** text box.
5. Enter the subnet mask used for all communication on your local devices in the **Subnet Mask** text box.
6. Configure the range of IP address in the **Primary DHCP Range** panel for automatically assigning them to the networked devices.

7. Enter the first IP address in the DHCP address pool that you will be distributing over the private network in the **First DHCP Address** text box.
8. Enter the last IP address in the DHCP address pool that you will be distributing over the private network in the **Last DHCP Address** text box.
9. Configure the range of IP address in the **Secondary DHCP Range** panel for manually assigning them to specific devices on the network from the IP Address Allocation page.
10. Enable the secondary DHCP range of manual IP addressing by selecting the **Default** check box.
11. Enter the first IP address in the secondary DHCP address pool that is manually assigned over the private network in the **First DHCP Address** text box.
12. Enter the last IP address in the secondary DHCP address pool that is manually assigned over the private network in the **Last DHCP Address** text box.

Note The software supports private, public routed, and public proxied subnets simultaneously on the LAN.



DHCP Lease Time: 168 hours

13. Enter a numerical value in the **DHCP Lease Time** text box.

    This value represents the number of hours you can use the assigned IP address before the DHCP lease expires.
14. Click **Save**.

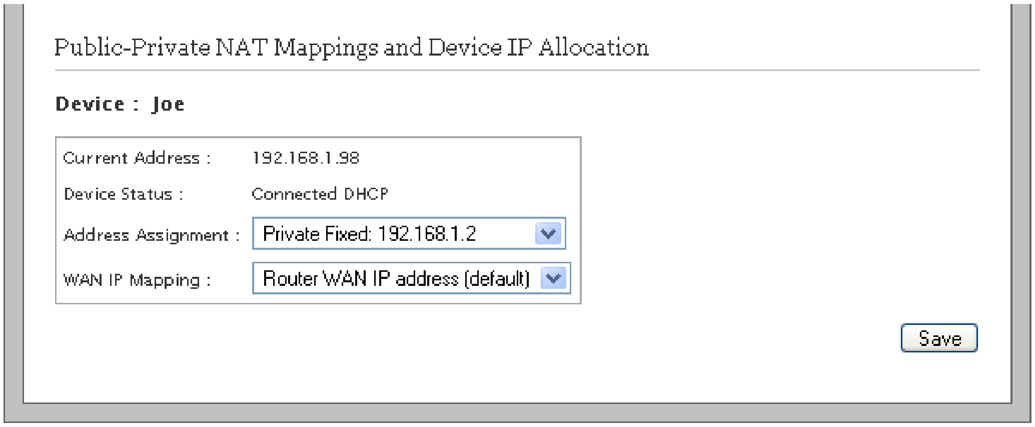
Allocating Static IP Address

Objective

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

Steps

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Public-Private NAT Mappings and Device IP Allocation** panel.



Public-Private NAT Mappings and Device IP Allocation

Device : Joe

Current Address : 192.168.1.98

Device Status : Connected DHCP

Address Assignment : Private Fixed: 192.168.1.2

WAN IP Mapping : Router WAN IP address (default)

3. Locate the relevant device on the network to change the default DHCP settings.

4. View the privately assigned IP address and the address assignment mode next to the **Current Address** and **Device Status** fields.
5. Select the static IP from the **Address Assignment** drop-down list box,

   The static IP is represented as **Private Fixed: *xxx.xxx.xxx.xxx***, where *xxx.xxx.xxx.xxx* indicates the IP address. This selection allocates the static IP address to the relevant device on the network.
6. Leave the **WAN IP Mapping** drop-down list box as is.
7. Click **Save** next to the device where you have modified the settings.
8. Renew the IP address of the corresponding computer.

Configuring Public IP Network

Objective

To configure public IP network or public proxied network. This method lets you specify a subnet mask for provisioning the public IP address on the primary Broadband connection to be statically assigned or dynamically distributed to specific devices on the network.

Steps

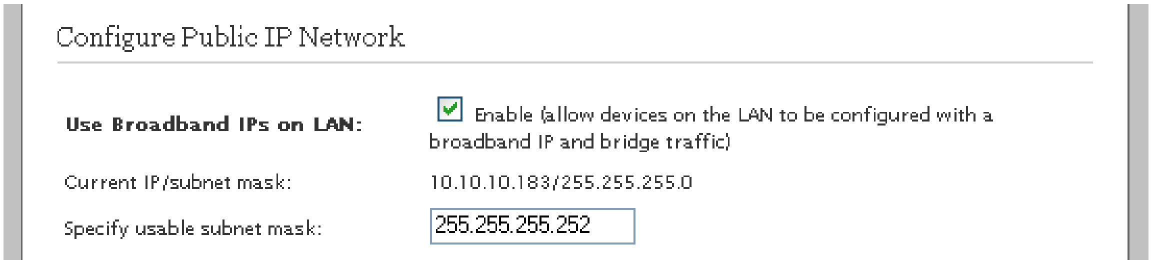
1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Perform the following tasks to configure the public proxied IP network on your gateway:
   - Enabling Public IP Network on page 44
   - Selecting Default Address Allocation Pool on page 45
   - Assigning Public IP Network Address to LAN Client(s) on page 45

Enabling Public IP Network

The **Configure Public IP Network** panel allows you to enable the public proxied IP network and specify usable subnet mask that determines the number of IP addresses available for the public proxied IP network clients.

To enable the public IP network:

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Configure Public IP Network** panel.



Configure Public IP Network

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

Current IP/subnet mask: 10.10.10.183/255.255.255.0

Specify usable subnet mask: 255.255.255.252

3. Select the **Use Broadband IPs on LAN** check box.

   This enables the gateway to assign public IP addresses to the devices on the network.
4. View the **Current IP/subnet mask**.

   This is the IP address and subnet mask that is currently assigned to your gateway by your ISP.
5. Enter the subnet mask provided by your ISP in the **Specify usable subnet mask** text box.

   This lets the gateway estimate the number of devices that can connect to the gateway using the IP addresses from the primary Broadband interface. This must be a superset of the current subnet mask.
6. Click **Save** in the **Select Default Address Allocation Pool for the DHCP Server** panel.

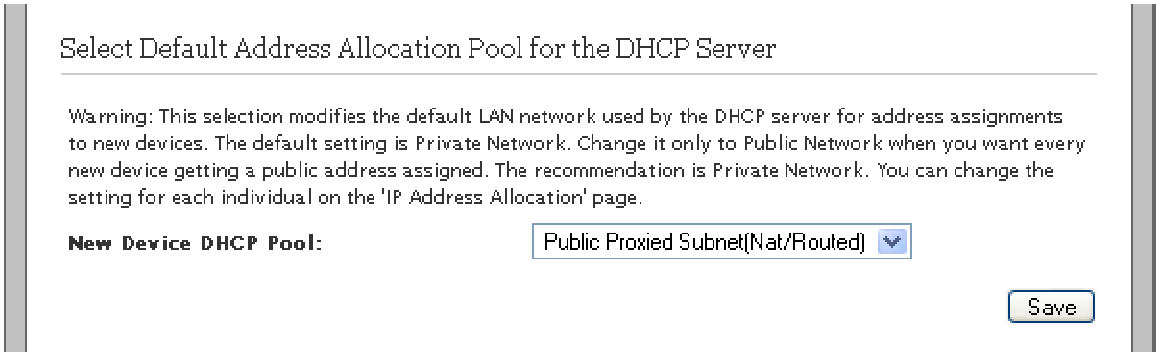
The gateway enables the public proxied network and populates the adequate IP address(es) for allocation.

Selecting Default Address Allocation Pool

The **Select Default Address Allocation Pool for the DHCP Server** panel lets you determine the IP address allocation pool to the next associating LAN client.

To select the default address allocation pool:

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Select Default Address Allocation Pool for the DHCP Server** panel.



Select Default Address Allocation Pool for the DHCP Server

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

New Device DHCP Pool: Public Proxied Subnet(Nat/Routed)

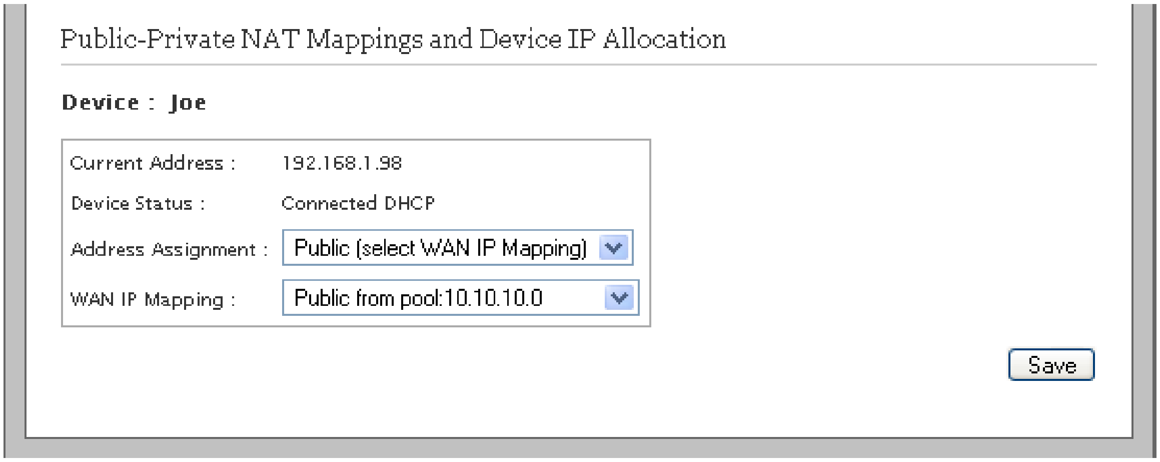
3. Select **Public Proxied Subet(Nat/Routed)** from the **New Device DHCP Pool** drop-down list box, if you want to assign the Broadband IPs to the newly associating LAN clients.
4. Click **Save**.

Assigning Public IP Network Address to LAN Client(s)

The **Public-Private NAT Mappings and Device IP Allocation** panel lets you statically or dynamically assign the existing LAN clients to public proxied IP network.

To assign the public proxied IP address to the LAN clients:

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Public-Private NAT Mappings and Device IP Allocation** panel.



Public-Private NAT Mappings and Device IP Allocation

Device : Joe

Current Address :	192.168.1.98
Device Status :	Connected DHCP
Address Assignment :	Public (select WAN IP Mapping)
WAN IP Mapping :	Public from pool:10.10.10.0

3. Locate the relevant LAN client from the list of devices for overriding the default DHCP IP address assignment.
4. View the currently assigned IP address and the connection mode next to the **Current Address** and **Device Status** fields.

5. Select **Public (select WAN IP Mapping)** from the **Address Assignment** drop-down list box.

   This enables the network device to fetch the IP address from the public pool.

6. Select the public IP from the **WAN IP Mapping** drop-down list box.

   The public IP is represented as **Public from pool:** ***xxx.xxx.xxx.xxx*** or **Public Fixed:** ***xxx.xxx.xxx.xxx*** where *xxx.xxx.xxx.xxx* indicates the IP address. This lets you assign a dynamic IP or a fixed IP from the public pool.

7. Click **Save** next to the device where you have modified the settings.
8. Renew the IP address of the corresponding computer.

Configuring Supplementary Network

Objective

To configure supplementary network or public routed network. This method lets you specify the router address and subnet mask for statically assigning or dynamically distributing IP address(es) to specific devices on the network.

Steps

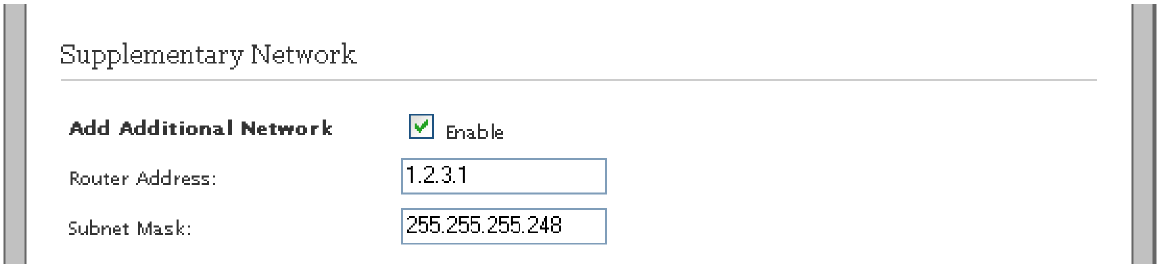
1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Perform the following tasks to configure the public proxied IP network on your gateway:
   - Enabling Supplementary Network on page 46
   - Selecting Default Address Allocation Pool on page 45
   - Assigning Public IP Network Address to LAN Client(s) on page 45

Enabling Supplementary Network

The **Supplementary Network** panel allows you to enable the public routed IP network and specify the router address and subnet mask. These entries determine the number of IP addresses available for the public routed IP network clients.

To enable the supplementary network:

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Supplementary Network** panel.



Supplementary Network

Add Additional Network ☑ Enable

Router Address: 1.2.3.1

Subnet Mask: 255.255.255.248

3. Select the **Add Additional Network** check box.

   This enables the configuration for supplementary network.

4. Enter an IP address in the **Router Address** text box.

   The gateway assigns the subset of this IP address for configuring the devices on the supplementary network. This address must not be in the range of WAN IP address or LAN IP address.

5. Enter the **Subnet Mask** in the text box.

   This lets the gateway estimate the number of available supplementary network IP address(es).

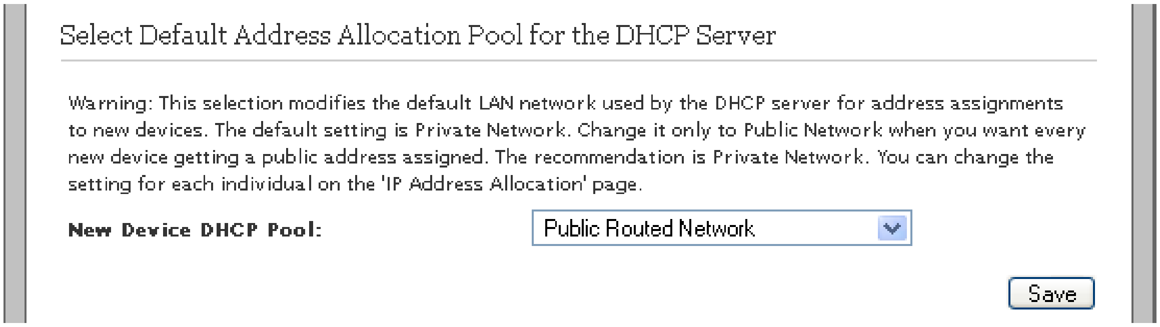
6. Click **Save** in the S**elect Default Address Allocation Pool for the DHCP Server** panel.

Selecting Default Address Allocation Pool

The **Select Default Address Allocation Pool for the DHCP Server** panel lets you determine the IP address allocation pool to the next associating LAN client.

To select the default address allocation pool:

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Select Default Address Allocation Pool for the DHCP Server** panel.



Select Default Address Allocation Pool for the DHCP Server

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

New Device DHCP Pool: Public Routed Network

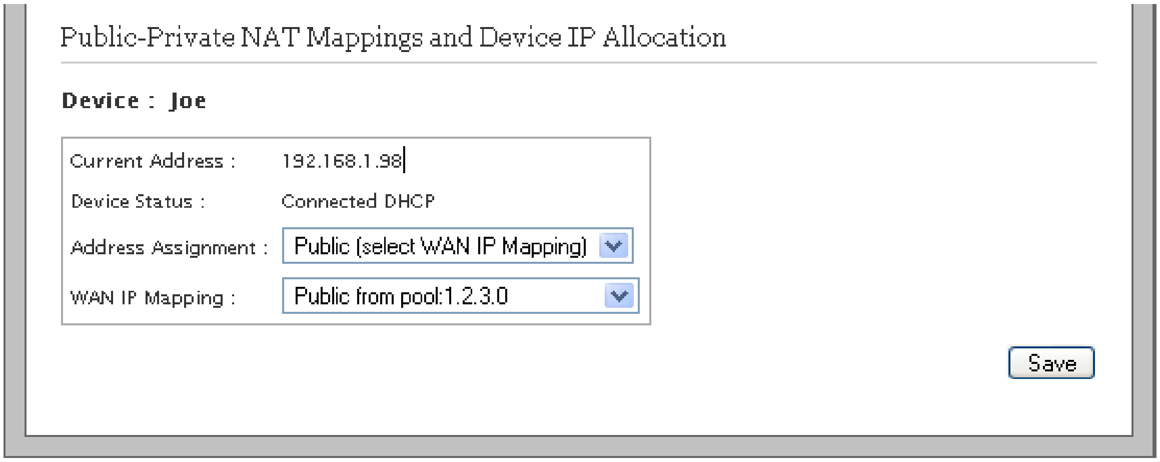
3. Select **Public Routed Network** from the **New Device DHCP Pool** drop-down list box, if you want to assign the supplementary IPs to the newly associating LAN clients.
4. Click **Save**.

Assigning Public IP Network Address to LAN Client(s)

The **Public-Private NAT Mappings and Device IP Allocation** panel lets you statically or dynamically assign the existing LAN clients to public routed IP network.

To assign the public routed IP address to the LAN clients:

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Public-Private NAT Mappings and Device IP Allocation** panel.



Public-Private NAT Mappings and Device IP Allocation

Device : Joe

Current Address : 192.168.1.98

Device Status : Connected DHCP

Address Assignment : Public (select WAN IP Mapping)

WAN IP Mapping : Public from pool:1.2.3.0

3. Locate the relevant device for changing the configuration to override the default DHCP settings.

   The **Public-Private NAT Mappings and Device IP Allocation** panel appears.
4. Locate the relevant LAN client from the list of devices for overriding the default DHCP IP address assignment.
5. View the currently assigned IP address and the connection mode next to the **Current Address** and **Device Status** fields.
6. Select **Public (select WAN IP Mapping)** from the **Address Assignment** drop-down list box.

This enables the relevant network device to fetch the IP address from the public pool.

7. Select the supplementary IP from the **WAN IP Mapping** drop-down list box.

   The supplementary IP is represented as **Public from pool: *xxx.xxx.xxx.xxx*** or **Public Fixed: *xxx.xxx.xxx.xxx*** where *xxx.xxx.xxx.xxx* indicates the IP address. This selection must resemble the IP address entered in the **Router Address** text box. This lets you assign a dynamic IP or a fixed IP from the supplementary public pool.

8. Click **Save** next to the device where you have modified the settings.
9. Renew the IP address of the corresponding computer.

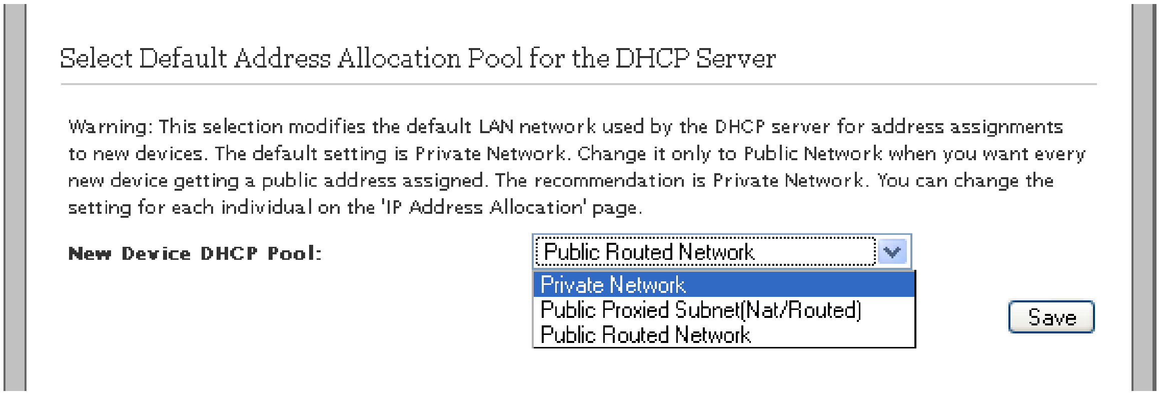
Configuring Default Address Allocation Pool for DHCP Server

Objective

To configure the gateway for allocating private, public proxied, or public routed IP addresses to any newly associating network devices.

Steps

1. On the **Settings** tab, click **LAN**, and then click **IP Address Allocation**.
2. Navigate to the **Select Default Address Allocation Pool for the DHCP Server** panel.



Select Default Address Allocation Pool for the DHCP Server

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

New Device DHCP Pool: Public Routed Network

3. Select the default address allocation pool from the **New Device DHCP Pool** drop-down list box.

   The types of address allocation pools are **Private Network**, **Public Proxied Network**, or **Public Routed Network**.

   - If you select **Private Network** from the drop-down list box, then the gateway assigns IP addresses as configured on **DHCP Configuration** page.
   - If you select **Public Proxied Network** from the drop-down list box, then the gateway assigns Broadband IPs.
   - If you select **Public Routed Network** from the drop-down list box, then the gateway assigns supplementary network IPs.

4. Click **Save**.

Accessing ARP Table Data

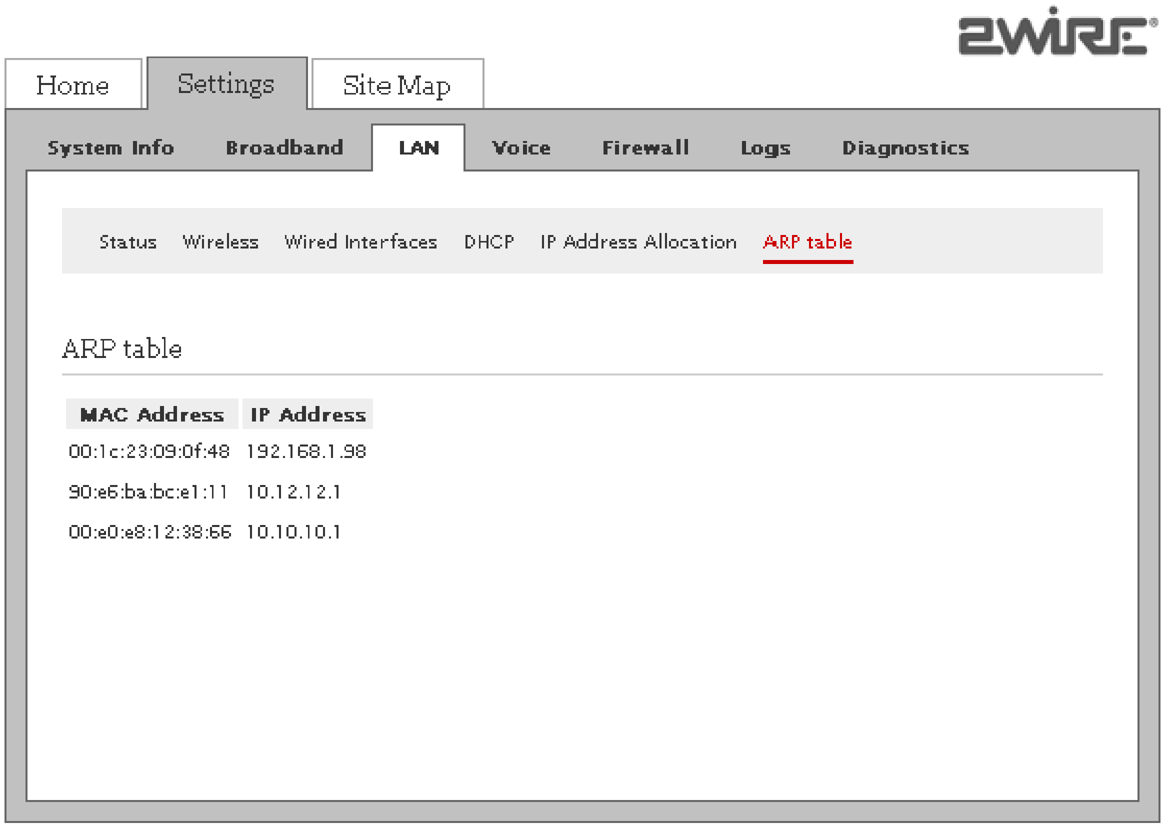
Objective

To determine the IP address of the devices on the network, based on the MAC address of that device.

This page is used to determine the IP address of the networked device, if the MAC address of the networked device is known.

Steps

1. On the **Settings** tab, click **LAN**, and then click **ARP table**.



ARP table

MAC Address	IP Address
00:1c:23:09:0f:48	192.168.1.98
90:e6:ba:bc:e1:11	10.12.12.1
00:e0:e8:12:38:66	10.10.10.1

2. Determine the **MAC Address** listed in the left column and view the associated **IP Address** listed in the right column.

See Also

Managing Broadband Settings on page 18

Using Diagnostics Features on page 72

LAN Issues on page 84

CHAPTER 7

Managing Voice-Based Services

This chapter provides information about the tasks that you can perform within the **Voice** tab. The links under the **Voice** tab and their associated tasks are as follows:

- Status
  - Viewing VoIP Line Status on page 50
- Server
  - Configuring SIP Server on page 51
- Line
  - Configuring Lines on page 52
- Stats
  - Viewing External Line Statistics on page 54

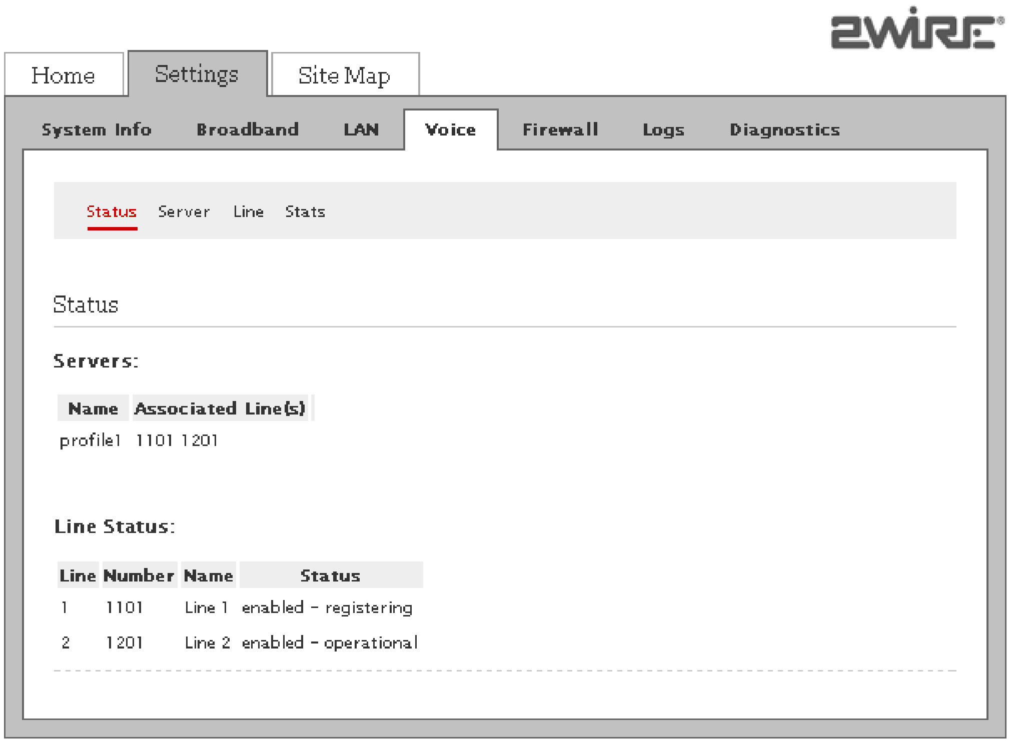
Note You can access the **Voice** tab only if you have subscribed for the VoIP service with your ISP.

Viewing VoIP Line Status

View the server profile and the associated lines with those profiles. Also, view the line status.

On the **Settings** tab, click **Voice**, and then click **Status**.

Refer to the following image and table for information about the parameters listed in the **Status** panel:



Status

Servers:

Name	Associated Line(s)
profile1	1101 1201

Line Status:

Line	Number	Name	Status
1	1101	Line 1	enabled - registering
2	1201	Line 2	enabled - operational

Parameter		Description
Servers		
	Name	Displays the profile name. You can configure two profiles on the gateway, but have only one profile in use.
	Associated Line	Displays the phone lines associated with the profile.
Line Status		
	Line	Displays the serial number for indexing the line status.
	Number	Displays the phone number of the configured line.
	Name	Displays the **Line Name** configured on the Line page.
	Status	Displays the status of the configured line on the gateway. The status can be as follows: • **Enabled-Registering** when lines try to register with the SIP server. • **Enabled-Operation** when lines have successfully registered with the SIP server. • **Disabled** when lined fail to register with the SIP server.

Configuring SIP Server

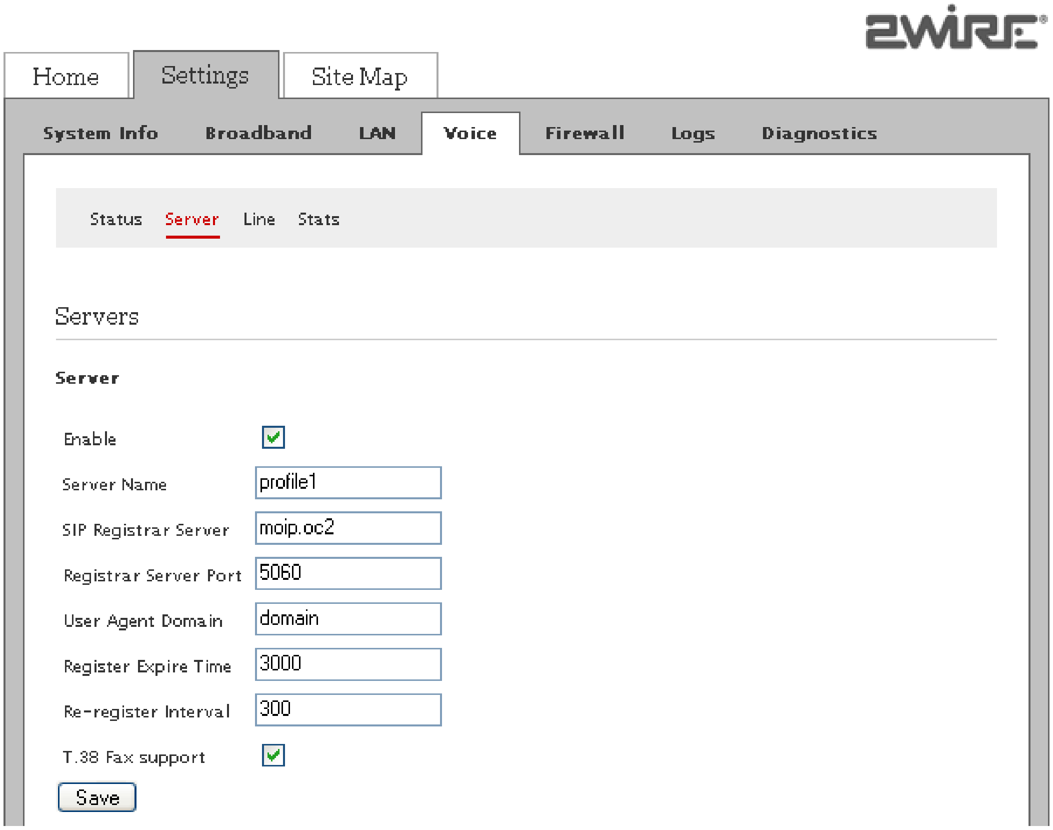
Objective

To configure the authentication parameters for the SIP server to enable the VoIP services on the gateway.

Your ISP gives the required information to configure the SIP server.

Steps

1. On the **Settings** tab, click **Voice**, and then click **Server**.



Servers

Server

Enable	☑
Server Name	profile1
SIP Registrar Server	moip.oc2
Registrar Server Port	5060
User Agent Domain	domain
Register Expire Time	3000
Re-register Interval	300
T.38 Fax support	☑

2. Select the **Enable** check box.
3. Enter a alphanumeric name in the **Server Name** text box.
4. Enter the server address in the **SIP Registrar Server** text box.
5. Enter the server port in the **Registrar Server Port** text box.
6. Enter the domain name in the **User Agent Domain** text box.
7. Enter the expire time in the **Register Expire Time** text box.
8. Enter the re-register interval time in the **Re-register Interval** text box.
9. Select the **T.38 Fax support** check box.

   This enables the gateway to permit faxes to be transported across IP networks using T.38 mode.
10. Click **Save**.

Note If your ISP has multiple SIP servers, you may have to configure additional servers on this page. You can modify or disable the existing server profiles. However, disabling any profile eliminates the associated line as well.

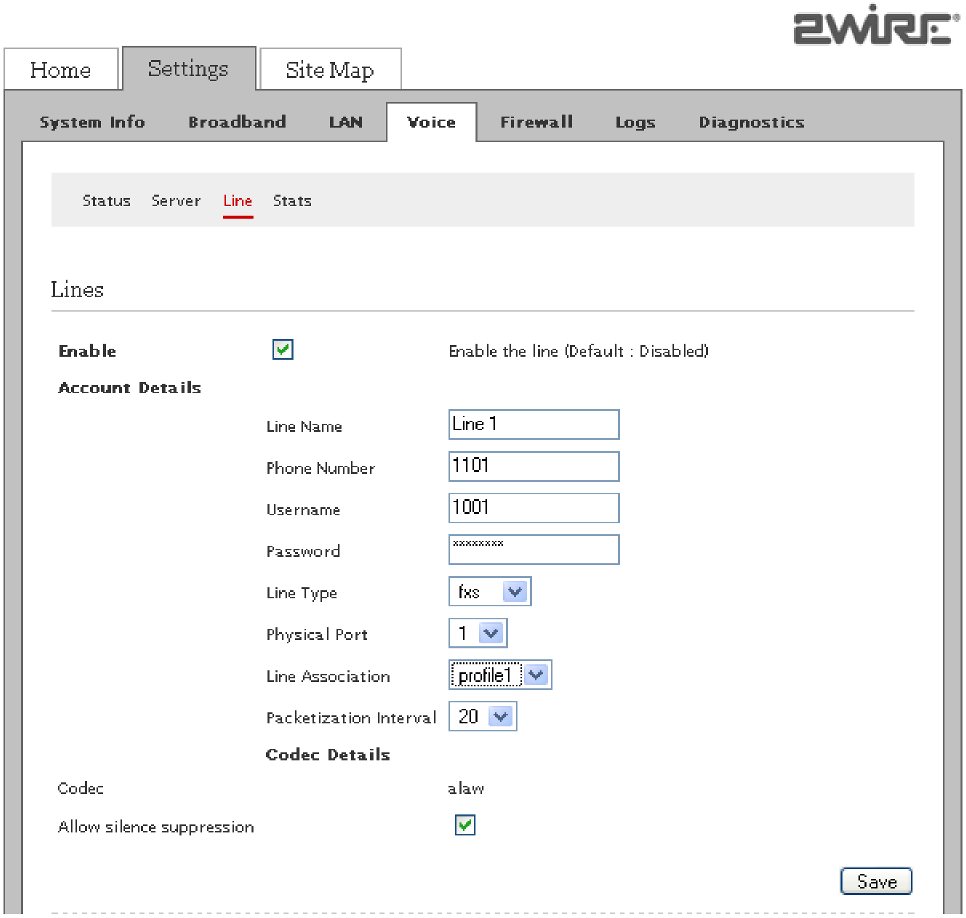
Configuring Lines

Objective

To configure one or two phone lines at a time on the gateway. Also, you can configure your phone number as well as the user name and password for your VoIP account to prevent unauthorized access.

Steps

1. On the **Settings** tab, click **Voice**, and then click **Line**.



Lines

Enable ☑ Enable the line (Default : Disabled)

Account Details

Line Name	Line 1
Phone Number	1101
Username	1001
Password	********
Line Type	fxs
Physical Port	1
Line Association	profile1
Packetization Interval	20

Codec Details

Codec	alaw
Allow silence suppression	☑

2. Select the **Enable** check box.

   This activates the line for use.
3. Edit the **Line Name** text box if you want to change the auto-populated line name.
4. Enter the **Phone Number**, **Username**, and **Password** in corresponding text boxes.

   The information is provided by the ISP.
5. Select the **Line Type** from the drop-down list box.

   The types of lines available are Foreign eXchange Subscriber (**fxs**) or Digital Enhanced Cordless Technology (**dect**)
   - If you select **fxs** from the drop-down list box, physical connectivity to the telephone is mandatory for the service to function.
   - If you select **dect** from the drop-down list box, you need a DECT phone. These phones are different from the usual cordless phones because they let you use the Wi-Fi access point to connect to your gateway and configure VoIP connection.
6. Select the **Physical Port** from the drop-down list box.

   The availble ports are **1** or **2**. This selection is based on the physical end point value or the port number on the splitter. If you are using a splitter and you have configured the details for P1/F1 port in this section, then your selection must be 1 from the drop-down list box.
7. Select the **Line Association** from the drop-down list box.

   The availble associations are **profile 1** or **profile 2**. The association value is pre-defined in the **Server Name** text box on the Server page.
8. Select the **Packetization Interval** from the drop-down list box.

   The available values are **10**, **20**, or **30**. This value determines the number of VoIP packets transmitted per second while advertising the associated data on the network. Lowering the value of Real-time Transport Protocol (RTP) Packet Size / Packetization Interval improves the quality of sound and decreases the degree of latency, but increases the bandwidth usage.
9. Enable silence supression codec by selecting the **Allow silence suppression** check box.

   If you enable silence suppression for VoIP communication, no packets are transmitted during periods of silence. This setting reduces the bandwidth usage during silent periods.
10. Click **Save**.

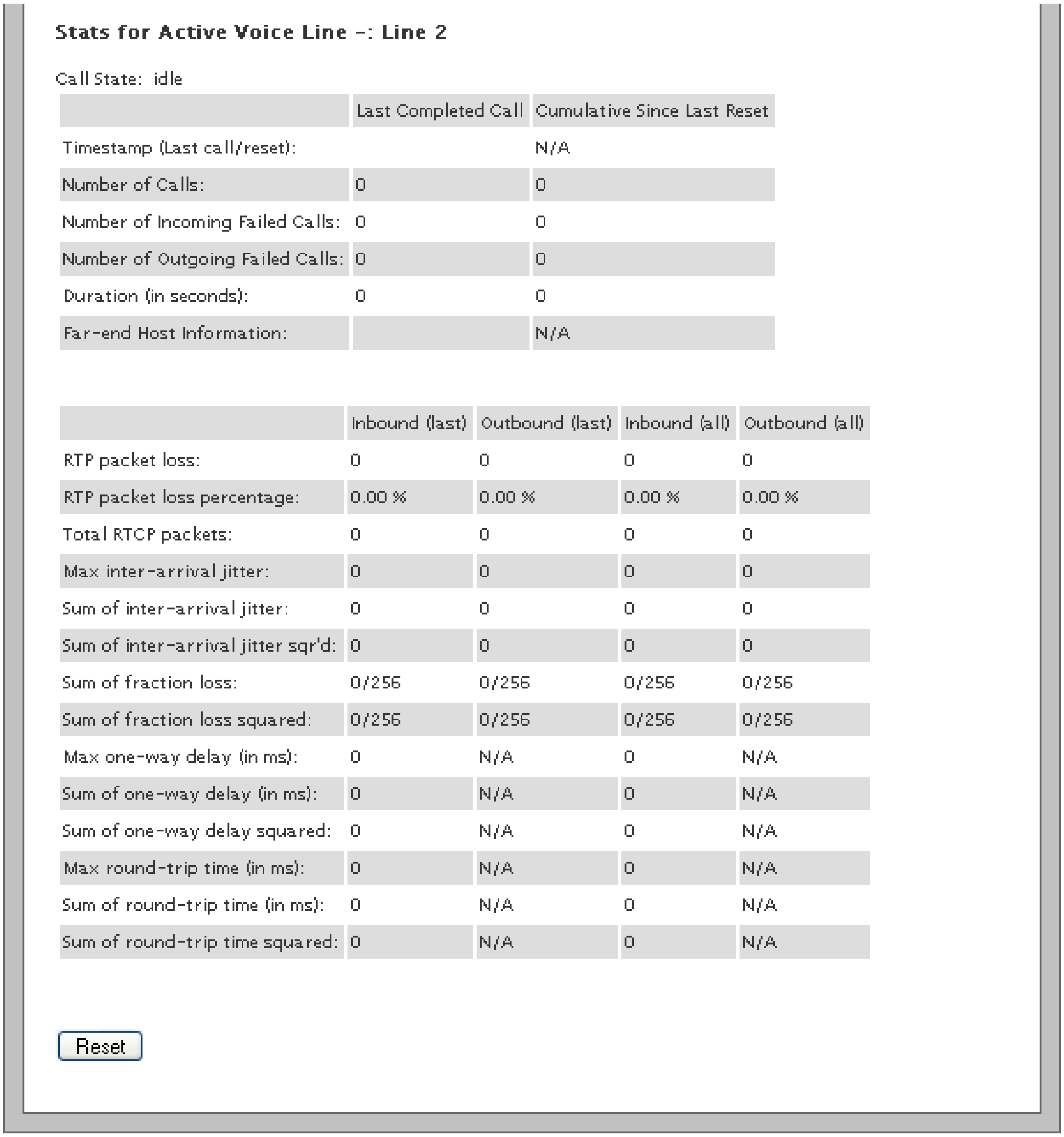
    To use the second line, configure the second line in the **Line 2** panel, and repeat the above steps.

Viewing External Line Statistics

View the VoIP call statistics for the relevant phone line.

On the **Settings** tab, click **Voice**, and then click **Stats**.

Refer to the following image and table for information about the parameters listed in the **Voice - External Line Stats** panel:



Stats for Active Voice Line -: Line 2

Call State: idle

	Last Completed Call	Cumulative Since Last Reset
Timestamp (Last call/reset):		N/A
Number of Calls:	0	0
Number of Incoming Failed Calls:	0	0
Number of Outgoing Failed Calls:	0	0
Duration (in seconds):	0	0
Far-end Host Information:		N/A

	Inbound (last)	Outbound (last)	Inbound (all)	Outbound (all)
RTP packet loss:	0	0	0	0
RTP packet loss percentage:	0.00 %	0.00 %	0.00 %	0.00 %
Total RTCP packets:	0	0	0	0
Max inter-arrival jitter:	0	0	0	0
Sum of inter-arrival jitter:	0	0	0	0
Sum of inter-arrival jitter sqr'd:	0	0	0	0
Sum of fraction loss:	0/256	0/256	0/256	0/256
Sum of fraction loss squared:	0/256	0/256	0/256	0/256
Max one-way delay (in ms):	0	N/A	0	N/A
Sum of one-way delay (in ms):	0	N/A	0	N/A
Sum of one-way delay squared:	0	N/A	0	N/A
Max round-trip time (in ms):	0	N/A	0	N/A
Sum of round-trip time (in ms):	0	N/A	0	N/A
Sum of round-trip time squared:	0	N/A	0	N/A

Parameter	Description
Stats for Active Voice Line -: Line 1	Displays status information about Line 1.
Timestamp (Last call/reset)	Displays the time when the call started.
Number of Calls	Displays the number of calls since last reset.
Number of Incoming Failed Calls	Displays the number of missed calls.

Parameter	Description
Number of Outgoing Failed Calls	Displays the number of incomplete outgoing calls.
Duration (in seconds)	Displays the time duration for which the VoIP connection was in use.
Far-end Host Information	Displays the IP and RTP port number of the host seperated by a colon.
The different types of columns that display the value for each statistic are as follows:	
Inbound (last)	Displays the last captured inbound value in this field for a specific statistic.
Outbound (last)	Displays the last captured outbound value in this field for a specific statistic.
Inbound (all)	Displays the the total inbound value in this field for a specific statistic since the last reset.
Outbound (all)	Displays the the total outbound value in this field for a specific statistic since the last reset.
The different types of statistics for a voice line are as follows:	
RTP packet loss	Displays the number of RTP data packets lost during a call. A RTP data packet consists of the fixed RTP header, a possibly empty list of contributing sources, and the payload data.
RTP packet loss percentage	Displays the percentage of RTP data packets lost while communicating with the SIP server.
Total RTCP packets	Displays the total number of Real-time Control Protocol (RTCP) packets used while communicating with the SIP server. RTCP is based on the periodic transmission of control packets to all participants in the session. An RTCP packet contains Packet Loss, Jitter, Delay, Signal Level, Call Quality Metrics, and Echo Return Loss.
Max inter-arrival jitter	Displays the maximum inter-arrival Jitter at source and destination for the latest operation. A jitter value captures the amount of variability in the arrival times of the datagrams at the receiver.
Sum of inter-arrival jitter	Displays the average inter-arrival Jitter at source and destination for the latest operation.
Sum of inter-arrival jitter squared	Displays the sum of square of inter-arrival jitter values for packets sent from source to destination and destination to source.
Sum of fraction loss	Displays the fraction of packets missed by the codec as the sum of both lost and late packets.
Sum of fraction loss squared	Displays the fraction of packets missed by the codec as the sum of square of both lost and late packets.
Max one-way delay (in ms)	Displays the maximum one-way delay duration in ms from source to destination and destination to source. One-way delay is the excess time taken to get data across the network. 150 mSec is specified in ITU-T G.114 recommendation as the maximum desired one-way latency to achieve high-quality voice.
Sum of one-way delay (in ms)	Displays the sum of one-way delay duration in ms from source to destination and destination to source.
Sum of one-way delay squared	Displays the sum of squarred one-way delay duration in ms from source to destination and destination to source.
Max round-trip time (in ms)	Displays the maximum response time taken by the VoIP signals. The round-trip time is tracked to measure the latency and the performance of the network.
Sum of round-trip time (in ms)	Displays the sum of response time taken by the VoIP signals.
Sum of round-trip time squared	Displays the sum of squarred response time taken by the VoIP signals

Note To reset the statistics, click **Reset** at the bottom of the page.

See Also

VoIP Issues on page 84

CHAPTER 8

Managing Firewall Settings

This chapter provides information about the tasks you can perform within the **Firewall** tab.

Note The gateway includes default firewall settings that block unwanted access from the Internet. It is recommended that you do not modify the default settings. However, you can configure the firewall settings to allow Internet traffic or users through the firewall to your LAN devices, applications, and servers.

The links under the **Firewall** tab and their associated tasks are as follows:

- Status
  - Disabling Firewall Service on page 56
  - Viewing Firewall Status on page 57
- Applications, Pinholes and DMZ
  - Configuring Firewall Settings on page 58
  - Configuring DMZ Mode on page 61
- Advanced Configuration
  - Disabling Attack Detection on page 62
  - Managing Outbound Traffic on page 63
  - Configuring Firewall Security Enhancements on page 64
  - Configuring Application Layer Gateway on page 65
  - Configuring UPnP Security on page 65
  - Blocking Web Site Access on page 66
  - Configuring Time of Day Restriction on page 67
- Access Control
  - Configuring Time of Day Restriction on page 67
- Content Screening
  - Blocking Web Site Access on page 66

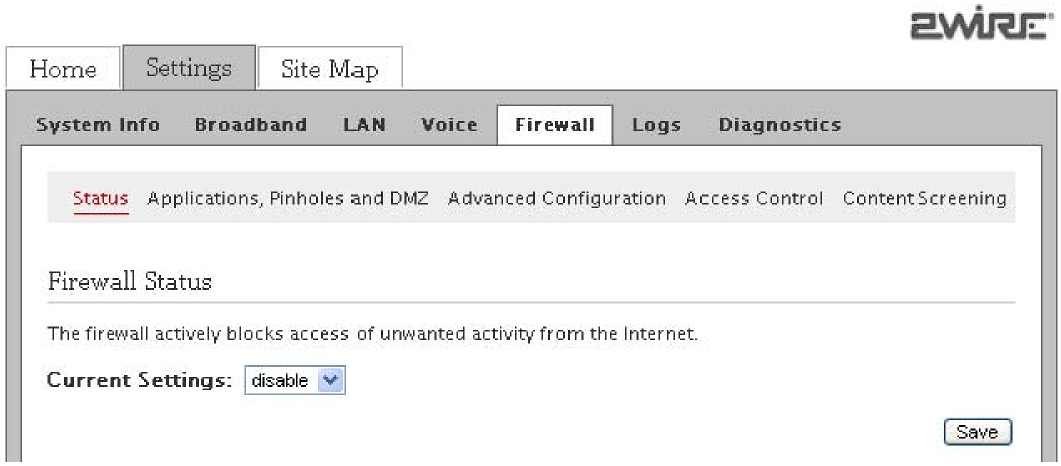
Disabling Firewall Service

Objective

To disable firewall services on the gateway so that all the ports on the nework are opened and unsolicited network traffic can pass through the gateway. By default, firewall services are enabled on the gateway for security reasons.

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Status**.



Firewall Status

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

Current Settings: disable

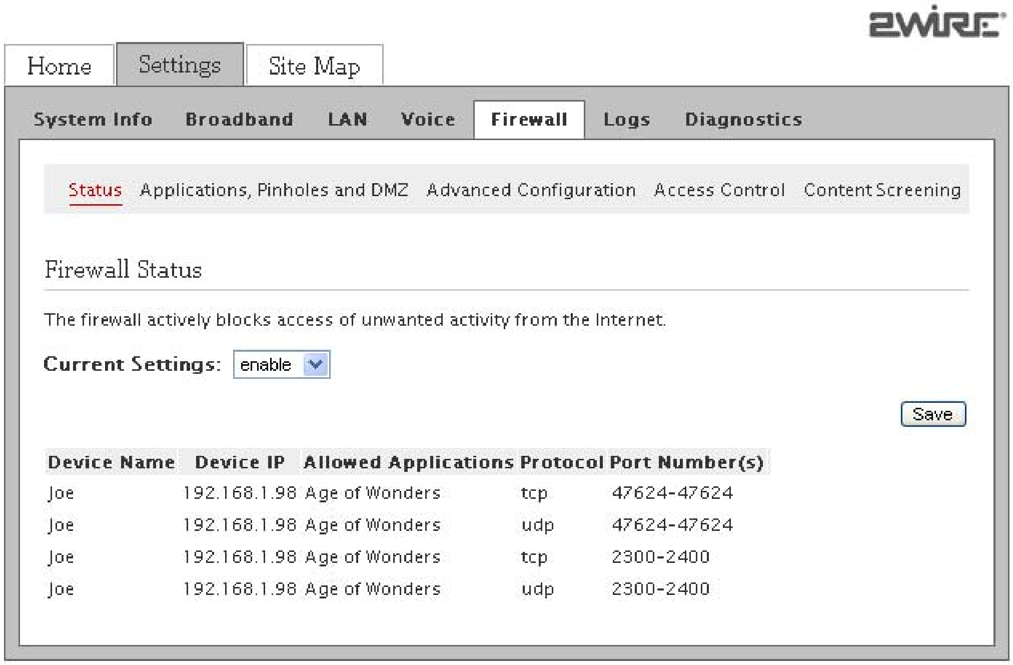
2. Select **disable** from the **Currrent Settings** drop-down list box.
3. Click **Save**.

Viewing Firewall Status

View the status of firewall and if any port forwarding rules are configured.

On the **Settings** tab, click **Firewall**, and then click **Status**.

Refer to the following image and table for information about the parameters listed in the **Firewall Status** panel:



Firewall Status

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

Current Settings: enable

Device Name	Device IP	Allowed Applications	Protocol	Port Number(s)
Joe	192.168.1.98	Age of Wonders	tcp	47624-47624
Joe	192.168.1.98	Age of Wonders	udp	47624-47624
Joe	192.168.1.98	Age of Wonders	tcp	2300-2400
Joe	192.168.1.98	Age of Wonders	udp	2300-2400

Parameter	Description
Device Name	Displays the name of the configured devices.
Device IP	Displays the IP of the configured device.
Allowed Applications	Displays the name of the application that bypasses the firewall settings.
Protocol	Displays the protocol in use.
Port Number(s)	Displays the port number assigned to the application.

Configuring Firewall Settings

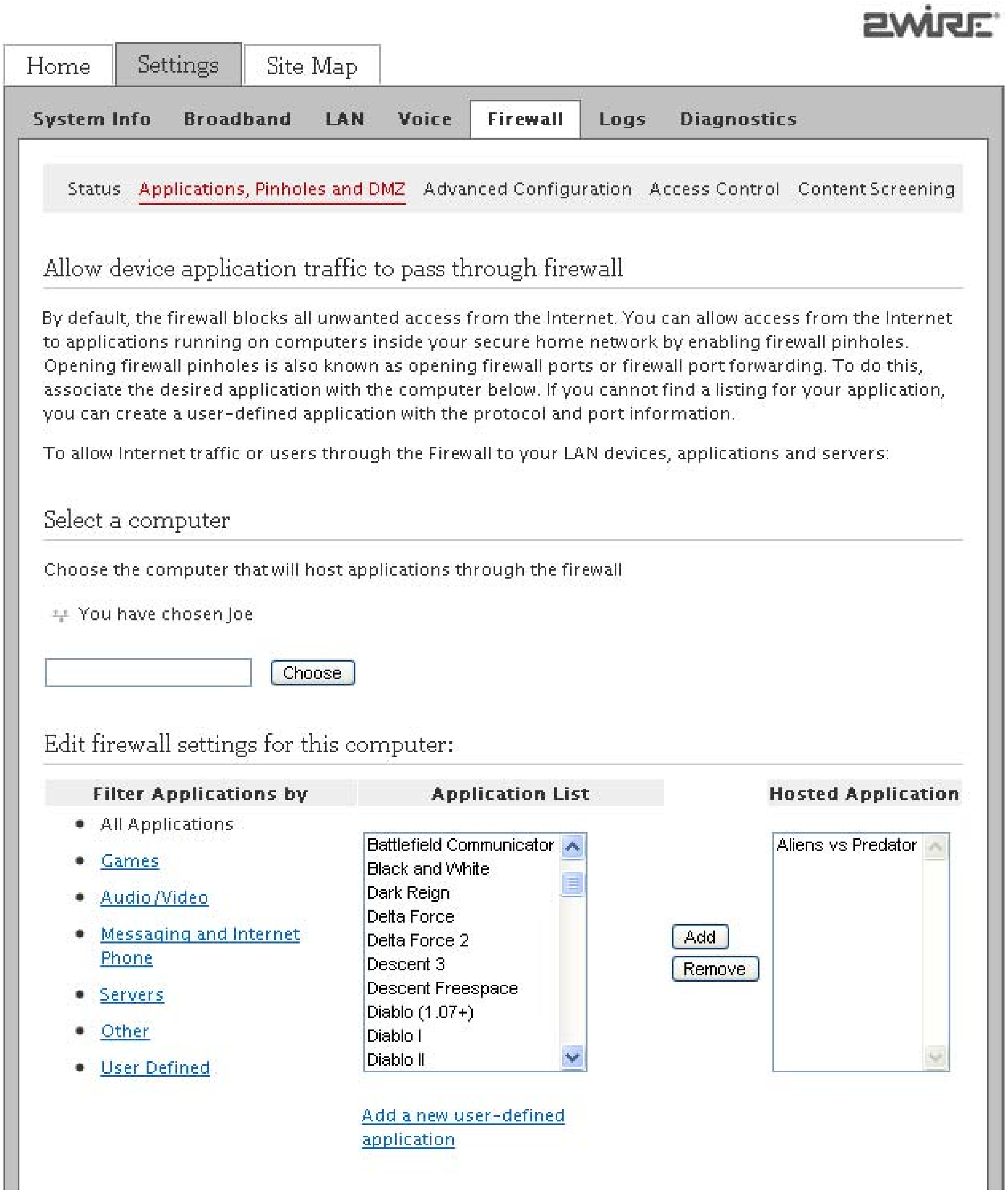
Objective

To modify applications, pinholes, and DMZ setting on the firewall in a way that special applications running on computers inside your home network are granted Internet access.

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

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Applications, Pinholes and DMZ**.



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:

Select a computer

Choose the computer that will host applications through the firewall

You have chosen Joe

Edit firewall settings for this computer:

2. Select the computer through which you want to host the application(s) in the **Select a computer** panel.

   If you host an application for a computer on your network, it implies that you are scaling down the firewall security levels for that application to be accessible on the specified computer.

   Note If the required computer is not available in the list, you can still select it as long as it is on the same network, and you know its IP address. Enter the IP address of the required computer, and click **Choose**.

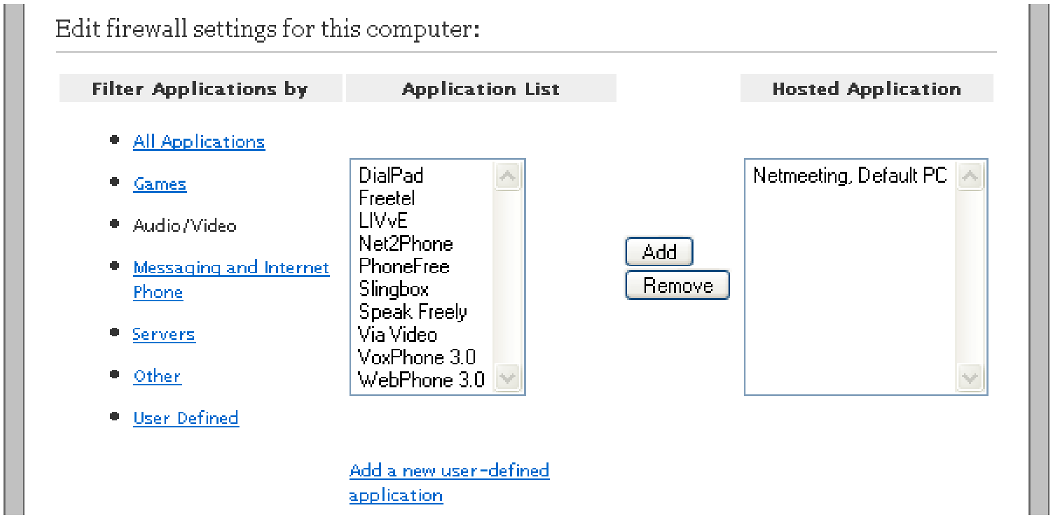
3. You can perform the following tasks:
   - Hosting an Application on page 59
   - Adding User-Defined Applications on page 59

Hosting an Application

The **Edit firewall settings for this computer** panel lets you grant access to the applications running on computers inside your home network from the Internet. You have to open firewall pinholes and associate the intended application(s) with a computer connected to your gateway.

To host an application:

1. On the **Settings** tab, click **Firewall**, and then click **Applications, Pinholes and DMZ**.
2. Navigate to the **Edit firewall settings for this computer** panel.



Edit firewall settings for this computer:

Filter Applications by	Application List	Hosted Application
• All Applications • Games • Audio/Video • Messaging and Internet Phone • Servers • Other • User Defined	DialPad Freetel LIVvE Net2Phone PhoneFree Slingbox Speak Freely Via Video VoxPhone 3.0 WebPhone 3.0	Netmeeting, Default PC

Add a new user-defined application

3. Filter the application list by selecting the category from the **Filter Applications by** bulleted list.

   Your selection appears in the **Application List** list box.
4. Select the applications to be hosted from the **Application List** list box.
5. Click **Add**.

   The selected application appears in the **Hosted Applications** list box.

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

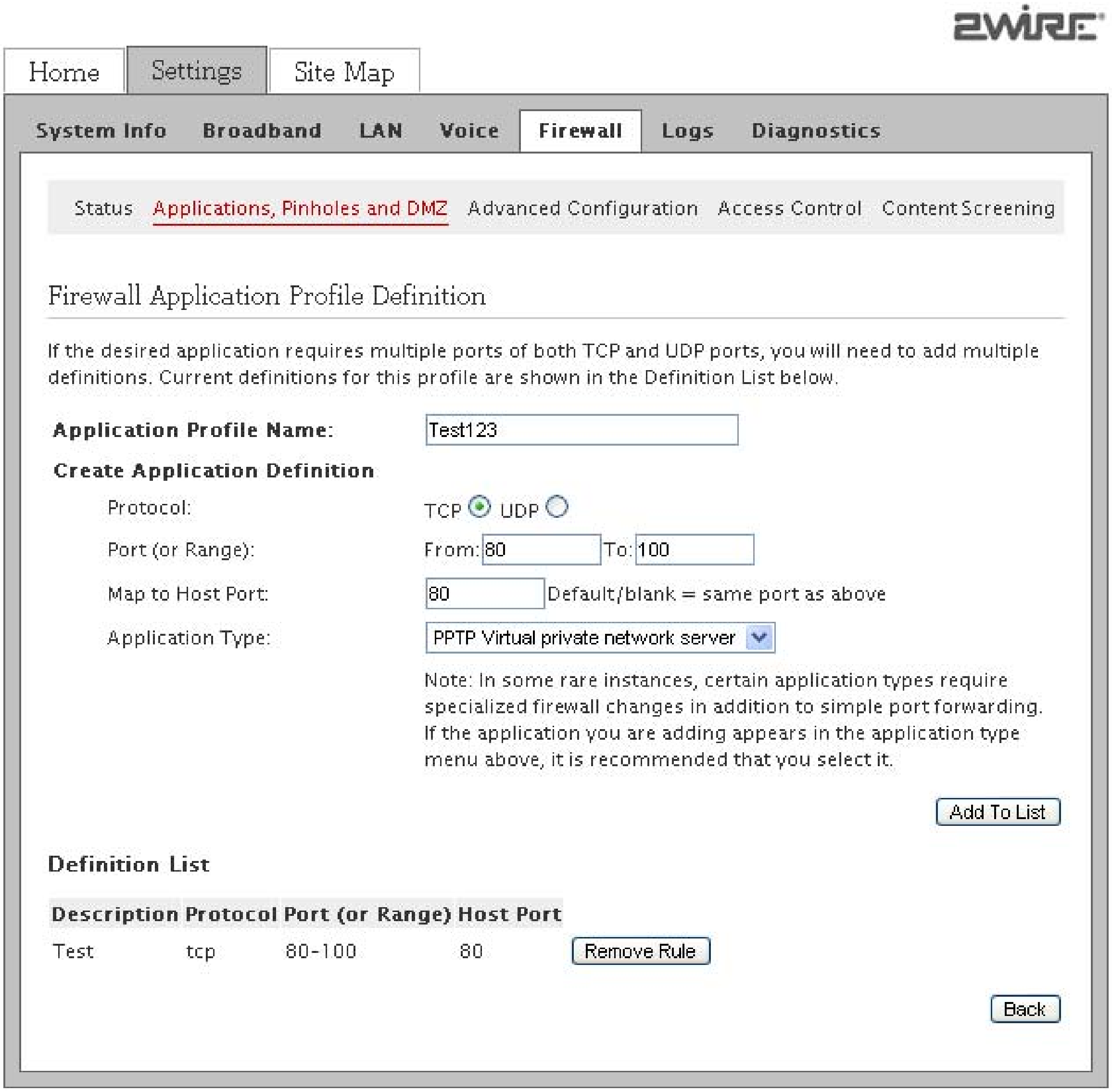
Adding User-Defined Applications

The **Firewall Application Profile Definiton** panel lets you create an application profile that is not included in the application list. An application profile configures the gateway firewall to let the application-specific data pass through.

To add user-defined applications:

1. On the **Settings** tab, click **Firewall**, and then click **Applications, Pinholes and DMZ**.
2. Navigate to the **Edit firewall settings for this computer** panel.
3. Click **Add a new user-defined application** below the **Application List** list box.

   This opens the **Firewall Application Profile Definition** page.



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: Test123

Create Application Definition

Protocol: TCP ● UDP ○

Port (or Range): From: 80 To: 100

Map to Host Port: 80 Default/blank = same port as above

Application Type: PPTP Virtual private network server

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

Description	Protocol	Port (or Range)	Host Port	
Test	tcp	80-100	80	Remove Rule

4. Enter a name for the application profile in the **Application Profile Name** text box.
5. Click the **TCP** or **UDP** radio button to select the required protocol for the application profile.

   If the application you are adding requires both, you have to create a separate definition for each.
6. Enter the port or port range used by the application in the **Port (or Range)** text boxes.

   If only one port is required, enter the port number in the **From** text box. For example, some applications require only one port to be opened (such as TCP port 500); others require that all TCP ports from 600 to 1000 be opened.
7. Enter the time duration in seconds in the **Protocol Timeout** text box.

   This is the amount of time the connection in the specified range remains open when there is no data transfer. In most cases, the default value is appropriate. If you leave the text box blank, the gateway uses the default values.

8. Enter a value in the **Map to Host Port** text box.

   This value must map to the port range you established to the local computer. For example, if you set the value to 4000 and the port range being opened is 100 to 108, the forwarded data to the first value in the range will be sent to 4000. Subsequent ports will be mapped accordingly; 101 will be sent to 4001, 102 will be sent to 4002, and so on.

9. Select the **Application Type** from the drop-down list box.

   The available application types are **FTP(file transfer protocol) Server**, **H.323-based Internet telephony**, **IRC (Internet relay chat) Server**, **PPTP Virtual private network server**, or **SIP-based Internet telephony**.

10. Click **Add to List** to create a new application profile.

    The configured information appears in the **Definition List** panel of the same page.

    The added application is also listed in the **Applications List** drop-down list box on the **Applications, Pinholes and DMZ** page.

Note To delete the user defined application, click **Remove Rule** next to the listed application profile in the **Definition List** panel.

Configuring DMZ Mode

Objective

To configure DMZ mode for a computer.

DMZ mode is a special firewall mode that is used for hosting applications if an application does not function properly using the Allow individual application(s) options. When in DMZ mode, the designated computer:

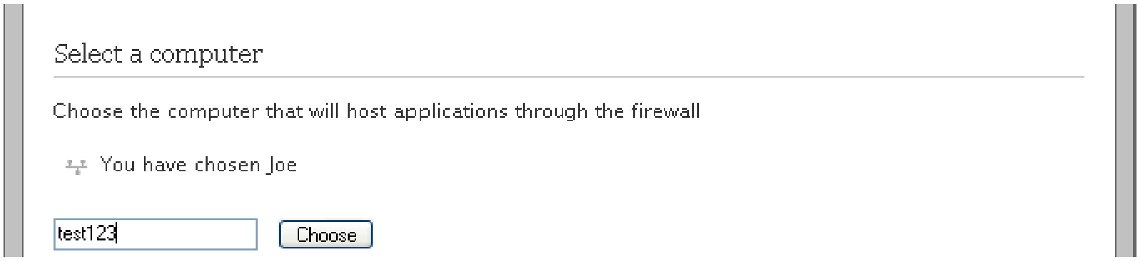
- Shares your gateway's IP address (router address).
- Appears as if it is directly connected to the Internet.
- Has all of the unassigned TCP and UDP ports opened and directing towards it.
- Can receive unsolicited network traffic from the Internet.

Although the computer in DMZ mode appears to the Internet users as if it is directly connected to the Internet, but it is still protected by your gateway's firewall. All traffic is inspected by the firewall's Stateful Packet Inspection (SPI) engine and all known hacker attacks continue to be blocked.

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

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Applications, Pinholes and DMZ**.
2. Navigate to the **Select a computer** panel.



Select a computer

Choose the computer that will host applications through the firewall

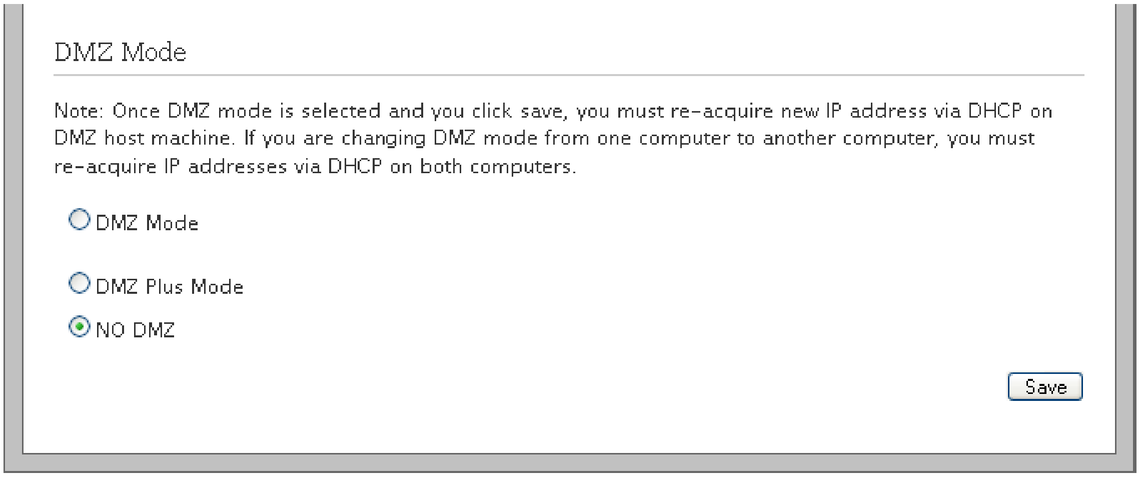
You have chosen Joe

test123

3. Select the required computer where you want to host the application(s) in the **Select a computer** panel.

Note Verify that the computer you selected is configured for DHCP. If the selected computer is not configured for DHCP, configure the DHCP settings and restart the computer. After the computer restarts, it receives an IP address from the gateway and all unassigned TCP and UDP ports are forwarded to it.

4. Navigate to the **DMZ Mode** panel.



DMZ Mode

Note: Once DMZ mode is selected and you click save, you must re-acquire new IP address via DHCP on DMZ host machine. If you are changing DMZ mode from one computer to another computer, you must re-acquire IP addresses via DHCP on both computers.

○ DMZ Mode

○ DMZ Plus Mode

● NO DMZ

5. Select the **DMZ Mode** option:
   - If you select **DMZ Mode** radio button, the network traffic is directly routed to the selected computer. In DMZ mode, the designated computer is connected to the Internet through the gateway, and can receive unsolicited network traffic from the Internet.
   - If you select **DMZ Plus Mode** radio button, the gateway assigns a Broadband/WAN IP to the selected computer. In DMZplus mode, the designated computer is directly connected to the Internet, has all unassigned TCP and UDP ports opened, and can receive unsolicited network traffic from the Internet.
   - If you select **NO DMZ** radio button, configured firewall rules are applicable for the selected computer.
6. Click **Save**.

Disabling Attack Detection

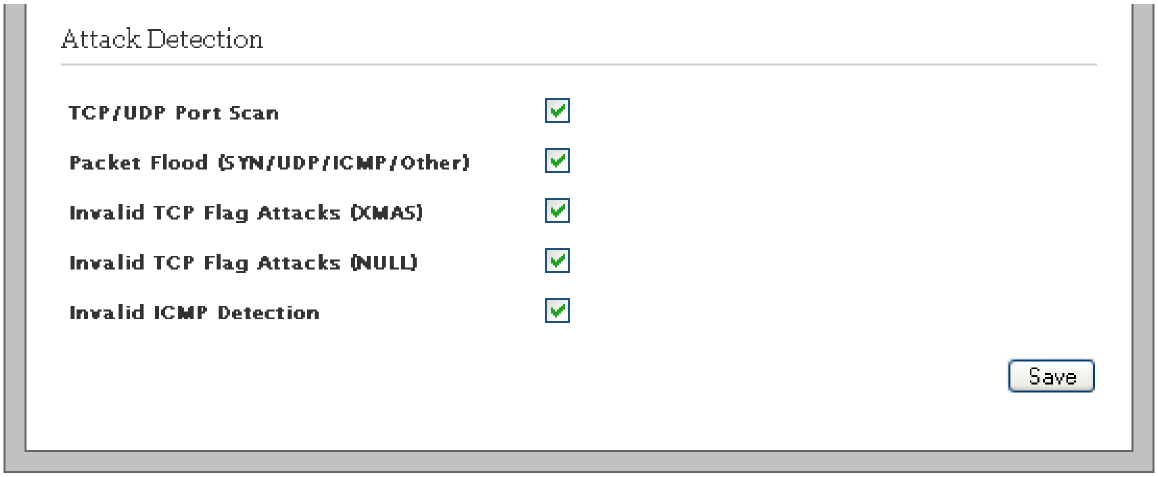
Objective

To disable a specific port in the attack detection panel.

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

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to the **Attack Detection** panel.



Attack Detection

TCP/UDP Port Scan ☑

Packet Flood (SYN/UDP/ICMP/Other) ☑

Invalid TCP Flag Attacks (XMAS) ☑

Invalid TCP Flag Attacks (NULL) ☑

Invalid ICMP Detection ☑

3. Clear the **TCP/UDP Port Scan** check box.

   If you disable this feature, the firewall does not detect UDP and TCP port scans, and communicates the port scan packets to the computer. A port scan is a series of messages sent by an external entity attempting to break into a computer to learn which computer network services associated with UDP and TCP ports are provided by the computer.
4. Clear the **Packet Flood (SYN/UDP/ICMP/Other)** check box.

   If you disable this feature, the firewall does not check for SYN, UDP, ICMP, and other types of packet floods on the local and Internet facing interfaces.
5. Clear the **Invalid TCP Flag Attacks (XMAS)** check box.

   If you disable this feature, the firewall does not scan inbound and outbound packets for invalid TCP Flag settings or TCP XMAS attack and communicates the associated packets to the computer.
6. Clear the **Invalid TCP Flag Attacks (NULL)** check box.

   If you disable this feature, the firewall does not scan inbound and outbound packets for invalid TCP Flag settings or TCP NULL attack and communicates the associated packets to the computer.
7. Clear the **Invalid ICMP Detection** check box.

   If you disable this feature, the firewall does not check for invalid ICMP type/code types and communicates the associated packets to the computer.
8. Click **Save**.

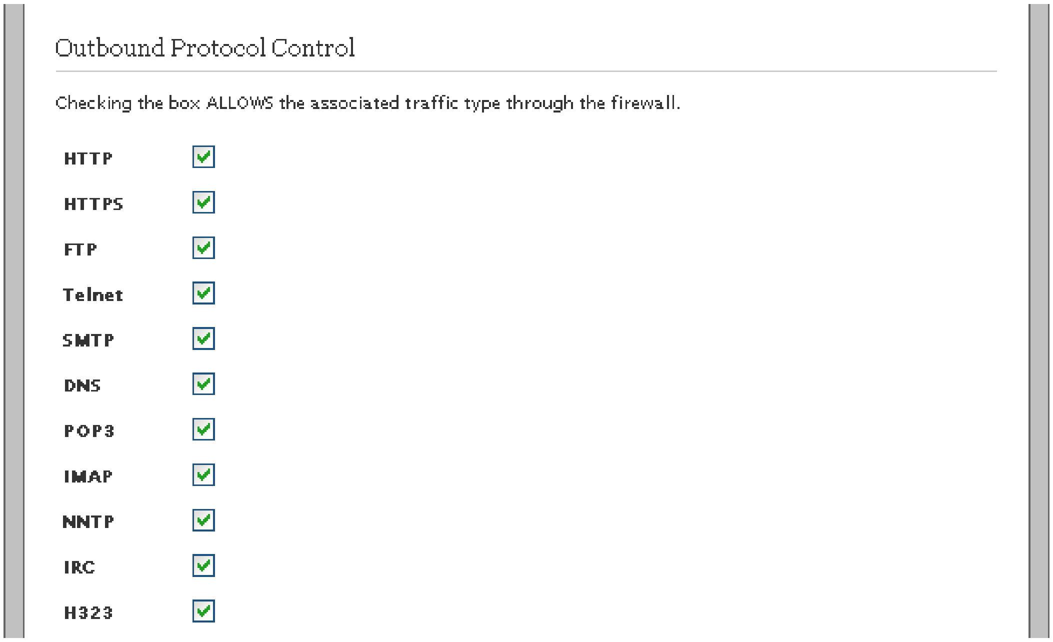
Managing Outbound Traffic

Objective

To configure the firewall for blocking or passing the outbound network traffic from your network.

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to view the **Outbound Protocol Contro**l panel.



Outbound Protocol Control

Checking the box ALLOWS the associated traffic type through the firewall.

HTTP	☑
HTTPS	☑
FTP	☑
Telnet	☑
SMTP	☑
DNS	☑
POP3	☑
IMAP	☑
NNTP	☑
IRC	☑
H323	☑

3. Select the required check box(es) in the **Outbound Protocol Control** panel.

   If you select any of the check box(es) in the **Outbound Protocol Control** panel, the firewall allows the associated traffic to pass through the firewall from the network to the Internet.

4. Click **Save**.

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

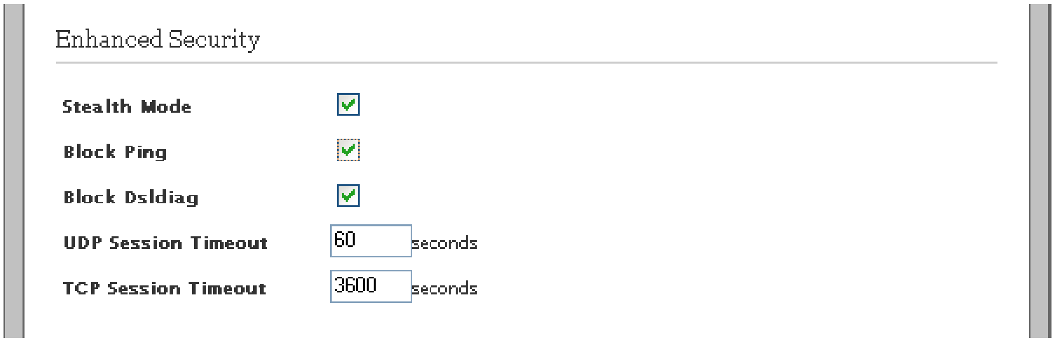
Configuring Firewall Security Enhancements

Objective

To configure the firewall rules for filtering the traffic passing through the gateway.

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to the **Enchanced Security** panel.



Enhanced Security

Stealth Mode	☑
Block Ping	☑
Block Dsldiag	☑
UDP Session Timeout	60 seconds
TCP Session Timeout	3600 seconds

3. Select the **Stealth Mode** check box to enable the stealth mode.

If you enable stealth mode, the gateway firewall does not return any information in response to network queries. This discourages intruders from accessing your network.

4. Select the **Block Ping** check box to disable the execution of external ping requests.
   - If you enable **Block Ping**, your network will block all ping requests.
   - If you disable **Block Ping**, intruders can use ping to launch an attack against your network since ping can determine the IP address of the network (for example, 105.246.172.72) from the domain name (for example, www.mynetworkdevice.com).
5. Select the **Block Dsldiag** check box to disable the execution of external DSL diagnostic requests.

   If you enable **Block Dsldiag**, the dsldiagd daemon running on the device blocks the remote user from connecting to the gateway and checking the DSL statistics, training history, and so on.
6. Enter the time duration in seconds in the **UDP Session Timeout** text box.

   The gateway terminates the UDP connection request after the specified duration.
7. Enter the time duration in seconds in the **TCP Session Timeout** text box.

   The gateway terminates the TCP connection request after the specified duration.
8. Click **Save**.

Configuring Application Layer Gateway

Objective

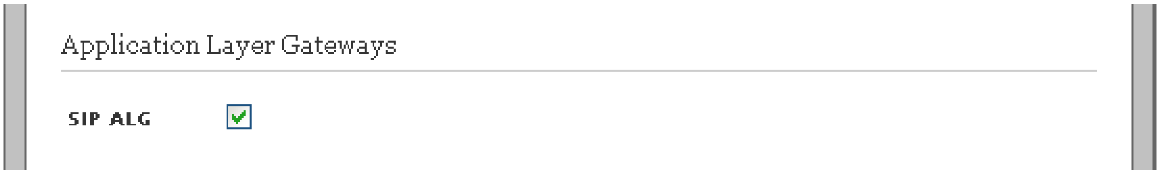
To enable or disable Application Layer Gateway (ALG) on the firewall of the gateway.

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

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

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to the **Application Layer Gateways** panel.



Application Layer Gateways

SIP ALG ☑

3. Enable or disable the **SIP ALG** on the gateway firewall by selecting or clearing the check box.
4. Click **Save**.

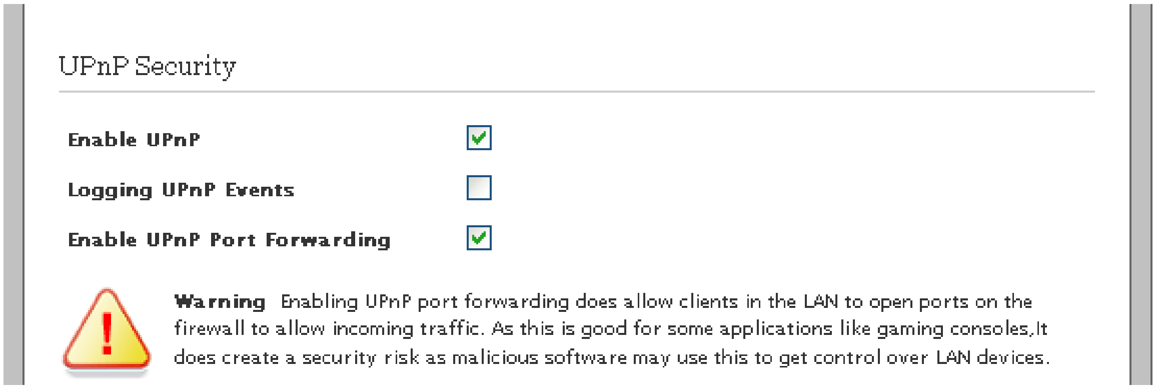
Configuring UPnP Security

Objective

To let the UPnP LAN clients aceess the network and open the ports on the gateway.

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to the **UPnP Security** panel.



UPnP Security

Enable UPnP ☑

Logging UPnP Events □

Enable UPnP Port Forwarding ☑

Warning Enabling UPnP port forwarding does allow clients in the LAN to open ports on the firewall to allow incoming traffic. As this is good for some applications like gaming consoles,It does create a security risk as malicious software may use this to get control over LAN devices.

3. Select **Enable UPnP** check box.

   This enables the UPnP LAN clients to connect to the gateway.

4. Select the **Logging UPnP Events** check box.

   This enables you to view every event related to UPnP on the Logs page.

5. Select the **Enable UPnP Port Forwarding** check box.

   This allows the applications that support UPnP to open and close the ports on the gateway. This saves you from the hassle of manually configuring the port forwarding for individual applications.

6. Click **Save**.

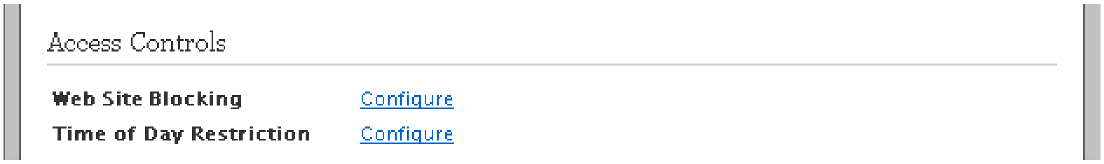
Blocking Web Site Access

Objective

To block access to specific Web Sites (URLs) within the LAN.

Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to the **Access Controls** panel.



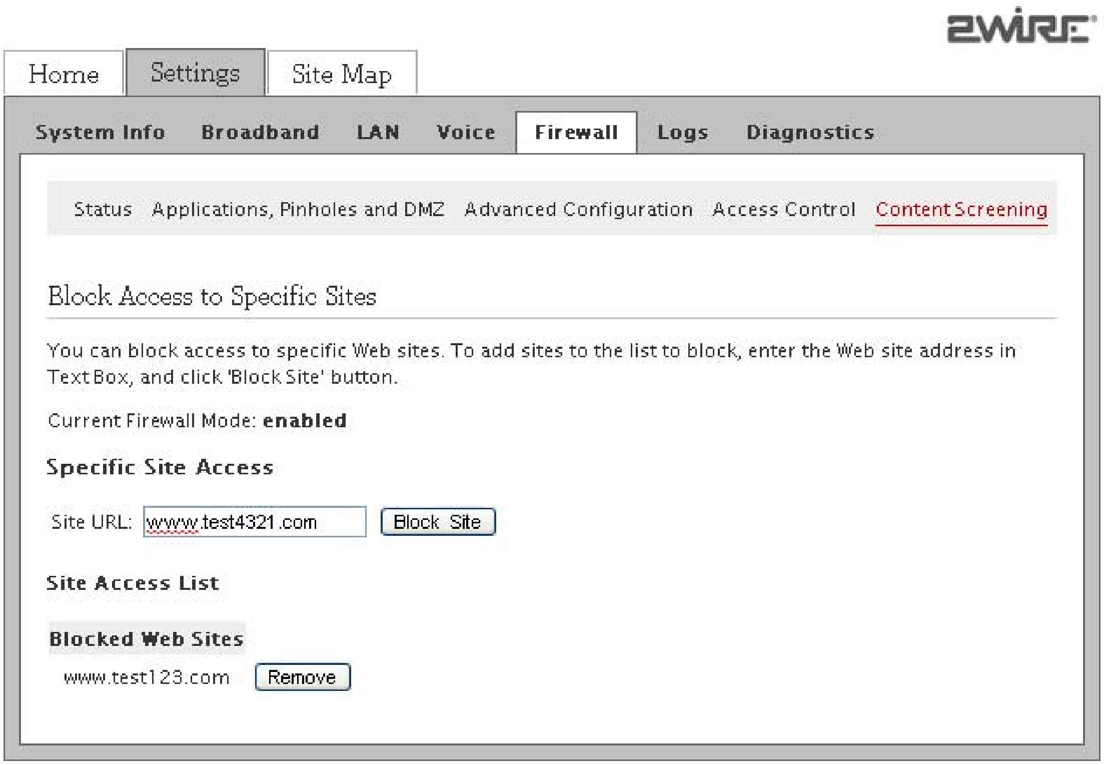
Access Controls

Web Site Blocking Configure

Time of Day Restriction Configure

3. Click **Configure** next to the **Web Site Blocking** field.

   This opens the **Block Access to Specific Sites** page.



Block Access to Specific Sites

You can block access to specific Web sites. To add sites to the list to block, enter the Web site address in Text Box, and click 'Block Site' button.

Current Firewall Mode: **enabled**

Specific Site Access

Site URL: www.test4321.com

Site Access List

Blocked Web Sites

www.test123.com

Note You can also click **Content Screening** to access the **Block Access to Specific Sites** page.

4. Enter the URL of the site to be blocked in the **Site URL** text box (For example, http://www.yahoo.com).
5. Click **Block Site**.

   The blocked Web site appears under the **Blocked Web Sites** panel.

Note If you want to restore access to the blocked sites, browse to the **Blocked Web Sites** panel and click **Remove** next to the site that is blocked.

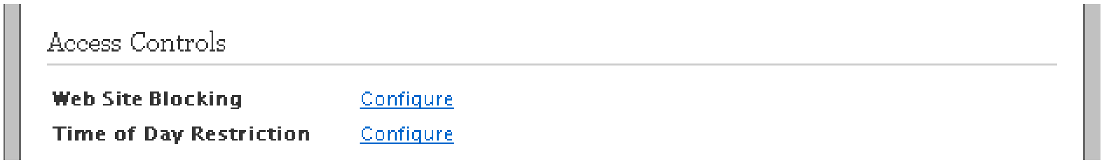
Configuring Time of Day Restriction

Objective

To limit the Internet usage during a specific time period.

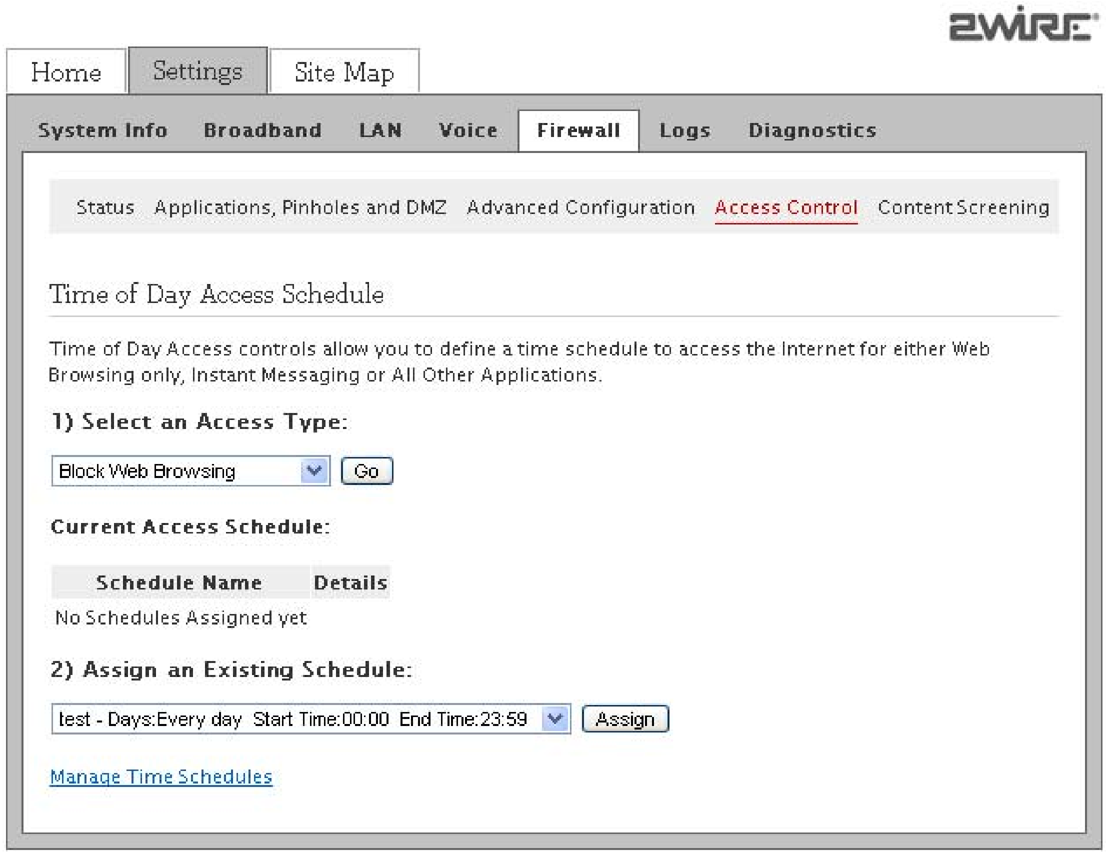
Steps

1. On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**.
2. Navigate to the **Access Controls** panel.



3. Click **Configure** next to the **Time of Day Restriction** field.

   This opens the **Time of Day Access Schedule** page.



Time of Day Access Schedule

Time of Day Access controls allow you to define a time schedule to access the Internet for either Web Browsing only, Instant Messaging or All Other Applications.

1) Select an Access Type: Block Web Browsing

Current Access Schedule:

Schedule Name	Details
No Schedules Assigned yet	

2) Assign an Existing Schedule: test - Days:Every day Start Time:00:00 End Time:23:59

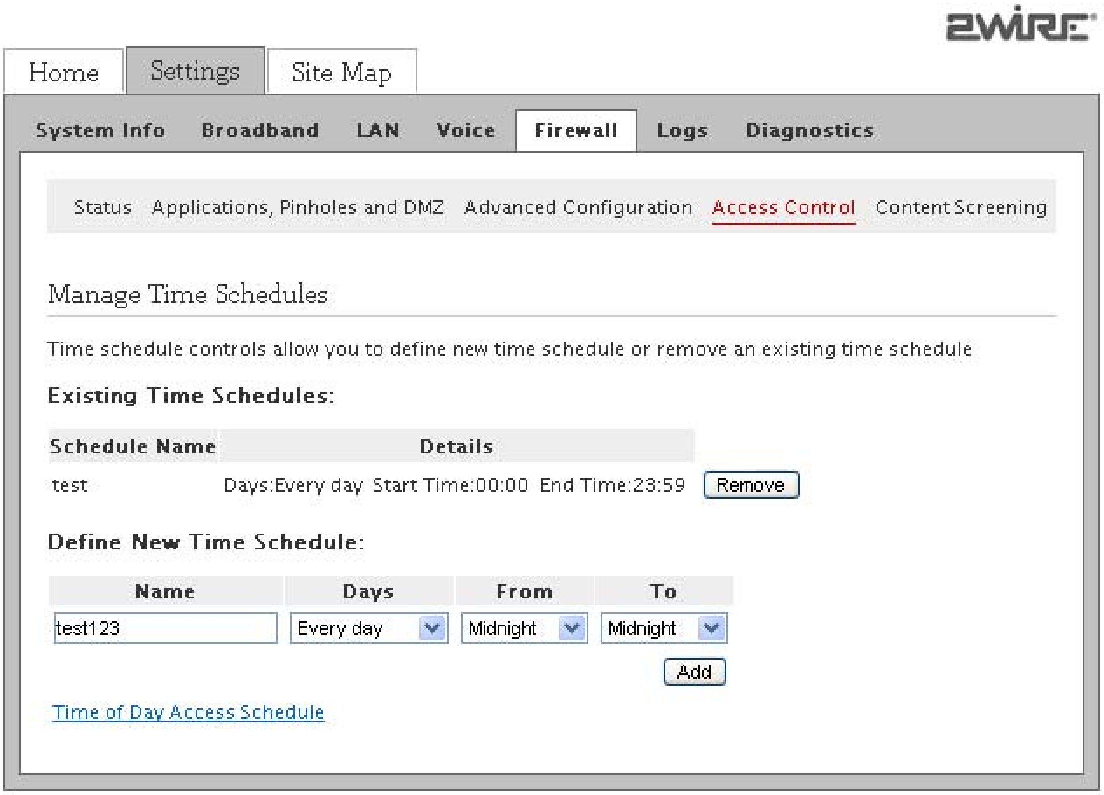
Note You can also click **Access Control** to access the **Time of Day Access Schedule** page.

4. Select the type of access you want to restrict from the **Select an Access Type** drop-down list box.

   The available access types are **Block Web Browsing**, **Block Instant Messaging**, or **Block All Other Applications**.

5. Browse to the bottom of the page and click **Manage Time Schedules** to predefine time schedules for restricting access.

   This opens the **Manage Time Schedules** page.



Manage Time Schedules

Time schedule controls allow you to define new time schedule or remove an existing time schedule

Existing Time Schedules:

Schedule Name	Details
test	Days:Every day Start Time:00:00 End Time:23:59

Define New Time Schedule:

Name	Days	From	To
test123	Every day	Midnight	Midnight

6. Browse to the **Define New Time Schedule** panel and perform the following actions:
   a. Enter an appropriate name in the **Name** text box for the new time schedule.
   b. From the drop-down list boxes, select the days and time period.
   c. Click **Add** to populate the new time schedule in the **Existing Time Schedules** panel.
7. Click **Time of Day Access Schedule** to return to the main page.
8. Browse to the **Assign an Existing Schedule** panel and perform the following actions:
   a. Select a predefined time schedule from the drop-down list box.
   b. Click **Assign**.

See Also

Managing LAN Devices on page 28

Managing Broadband Settings on page 18

Using Diagnostics Features on page 72

Firewall Issues on page 85

CHAPTER 9

Viewing Logs

This chapter provides information to view, filter, and clear the log entries on the **Logs** Tab from the user interface.

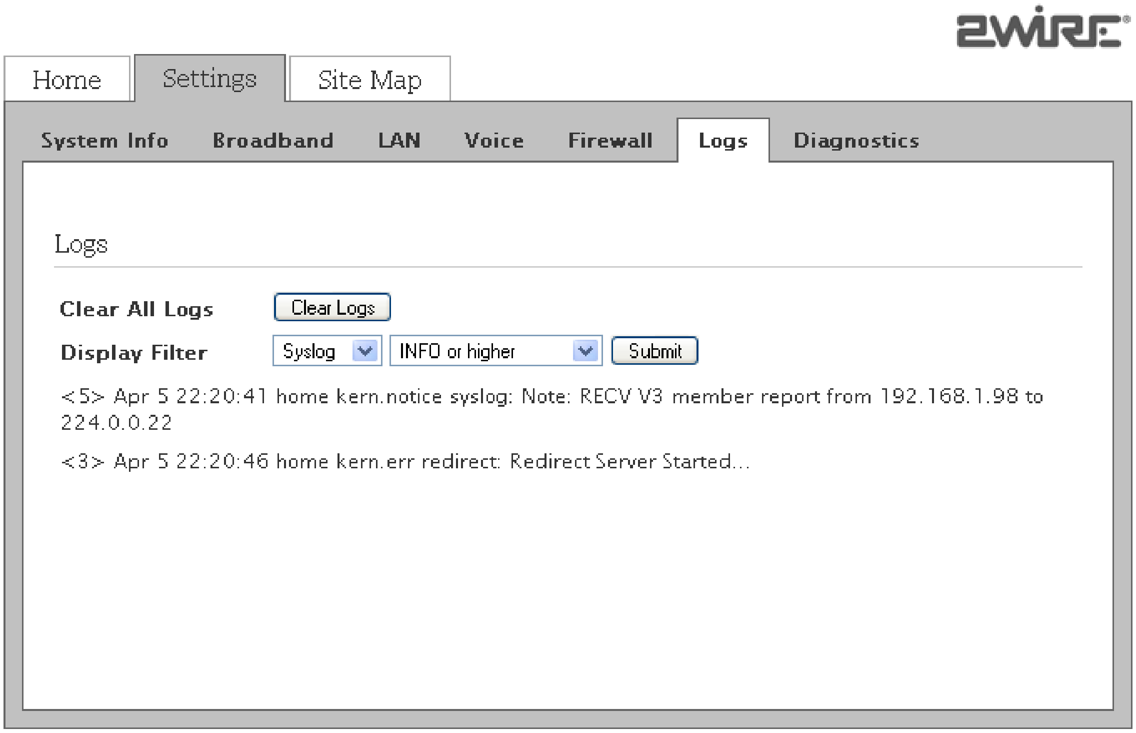
You can perform the following tasks on the **Logs** page:

- Viewing Specific Log Entries on page 70
- Filtering Log Entries on page 71
- Clearing Log Entries on page 71

Viewing Specific Log Entries

View log entries on this page to determine if there are any module specific issues or to ensure satisfactory performace of the device.

On the **Settings** tab, click **Logs**.



Clear All Logs

Display Filter: Syslog, INFO or higher

```
<5> Apr 5 22:20:41 home kern.notice syslog: Note: RECV V3 member report from 192.168.1.98 to
224.0.0.22

<3> Apr 5 22:20:46 home kern.err redirect: Redirect Server Started...
```

You can view log entries pertaining to a specifc module on this page, by selecting the desired module in the **Display Filter** list. The event logs are available in the following format:

```
<3> Mar 10 07:41:16 home kern.err dhcpd_dns[2673]: [truncated]
```

where <3> is the severity level, `<Mar 10 07:41:16>` is the time-stamp, `<kern.err dhcpd_dns[2673]>` is the module name, and `<[truncated]>` is the brief description of the log.

Filtering Log Entries

To filter log entries:

1. On the **Settings** tab, click **Logs**.
2. From the **Logs** page, select an option from the logs facility and the severity level drop-down list boxes next to the **Display Filter**.
3. Click **Submit** to view log entries associated with the selected option.

The following table lists the severity levels and their respective description:.

Severity Types (Lowest to Highest)	Description
Debug	Software debugging messages. Associated integer value is 0.
Info	Informational messages. Informational messages report significant non-error events. Associated integer value is 1.
Notice	Conditions that do not signify errors, but are of interest, or might warrant special handling. Associated integer value is 2.
Warning	Conditions that warrant monitoring. Associated integer value is 3.
Error	Standard error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels. Associated integer value is 4.
Critical	Critical conditions, such as hardware or firmware errors. Associated integer value is 5.
Alert	Conditions that must be corrected immediately, such as firewall not functioning. Associated integer value is 6.
Emergency	System panic or other conditions that cause the gateway to stop functioning. Associated integer value is 7.

The following table lists the log facilities and their respective description:.

Log Facility	Description
Syslog	Shows the current system log, which registers all significant events within the gateway since it was last restarted.
Dhcpc	Shows DHCP client related log messages.
Dhcpd	Shows DHCP daemon/server related log messages.
Firewall	Shows all detailed firewall events, such as Internet Access Control and Firewall Monitoring.
PPP	Shows log entries of transactions between the Internet server and the gateway.
NAT	Shows NAT log entries.
UPnP	Shows logs related to UPnP protocol events.
NPWEB	Shows logs related to the operations performed on the user interface.

Clearing Log Entries

You can clear the log entries on the **Logs** page and minimize the clutter from previous events when you try to diagnose a problem.

To clear the log entries from the list:

1. On the **Settings** tab, click **Logs**.
2. From the **Logs** page, click **Clear Logs**.

CHAPTER 10

Using Diagnostics Features

This chapter provides information about the tasks you can perform within the **Diagnostics** tab. The links under the **Diagnostics** tab and their associated tasks are as follows:

- Link Test
  - Diagnosing Broadband Link on page 72
- DSL
  - Viewing DSL Diagnostic Information on page 74
- IP Utilities
  - Testing IP Utilities on page 78
- NAT
  - Viewing NAT Information on page 79
- Syslog
  - Enabling Syslog on page 80
- Resets
  - Resetting the Gateway on page 81

Diagnosing Broadband Link

Diagnose if the Broadband and Service connections are established.

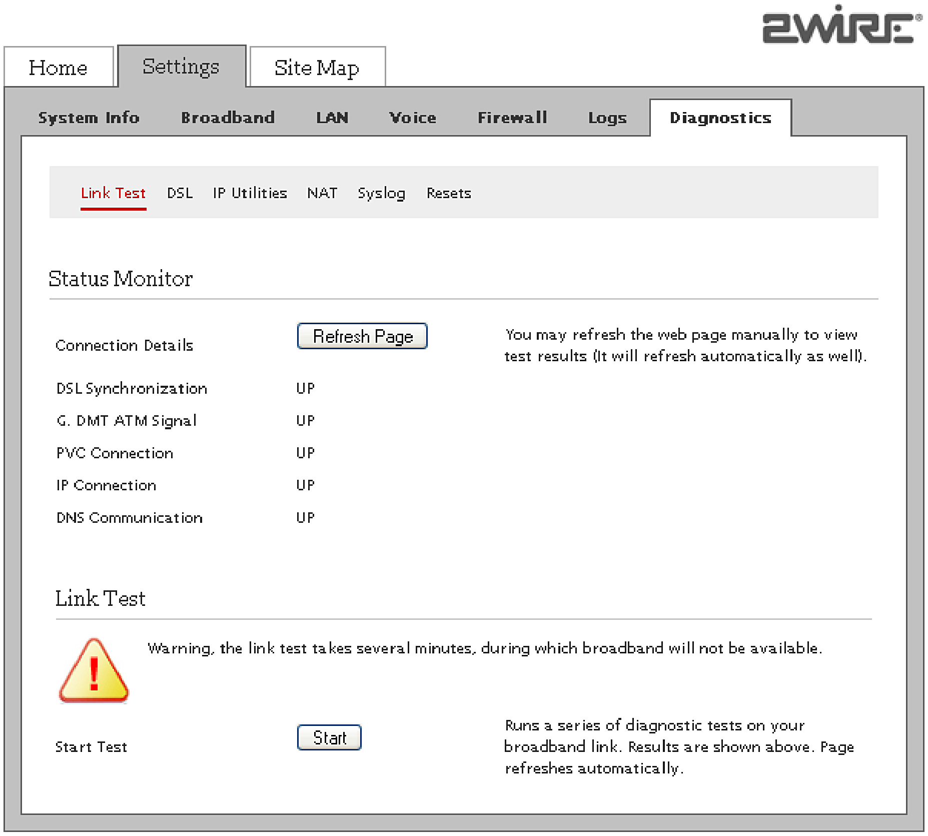
On the **Settings** tab, click **Diagnostics**, and then click **Link Test**. The following panels are displayed:

- Status Monitor
- Link Test

Note The **G. DMT ATM Signal** and **PVC Connection** fields are not visible in the **Status Monitor** panel, if you select **Ethernet** as the WAN interface type on the **Link Configuration** page.

Status Monitor

Refer to the following image and table for information about the parameters listed in the **Status Monitor** panel:



Status Monitor

Connection Details

You may refresh the web page manually to view test results (It will refresh automatically as well).

DSL Synchronization	UP
G. DMT ATM Signal	UP
PVC Connection	UP
IP Connection	UP
DNS Communication	UP

Link Test

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

Start Test

Runs a series of diagnostic tests on your broadband link. Results are shown above. Page refreshes automatically.

Parameter	Description
DSL Synchronization	Displays if the DSL interface is synchronized.
G. DMT ATM Signal	Displays if the gateway is able to connect to the G.DMT DSL mode.
PVC Connection	Displays if the ATM Circuit Identifier (VPI and VCI) value are correctly used. Even if the DSL signal is up and these values are incorrect, the gateway will not be able to establish Internet connection.
IP Connection	Displays if the gateway has received an IP address.
DNS Communication	Displays if the ISP's DNS server is reachable.

Note Click **Refresh Page** next to the **Connection Details** field, to refresh the results appearing in this panel.

Link Test

This panel lets you test the Broadband link.

Navigate to the **Link Test** panel and click **Start** next to the **Start Test** field.

This initiates diagnostic tests on your Broadband connection and the results appear in the **Status Monitor** panel.

Note Running diagnostic tests on your Broadband connection may take a few minutes, and Broadband will not be available during the testing period.

Viewing DSL Diagnostic Information

View diagnostic information of DSL and solve issues pertaining to DSL connection.

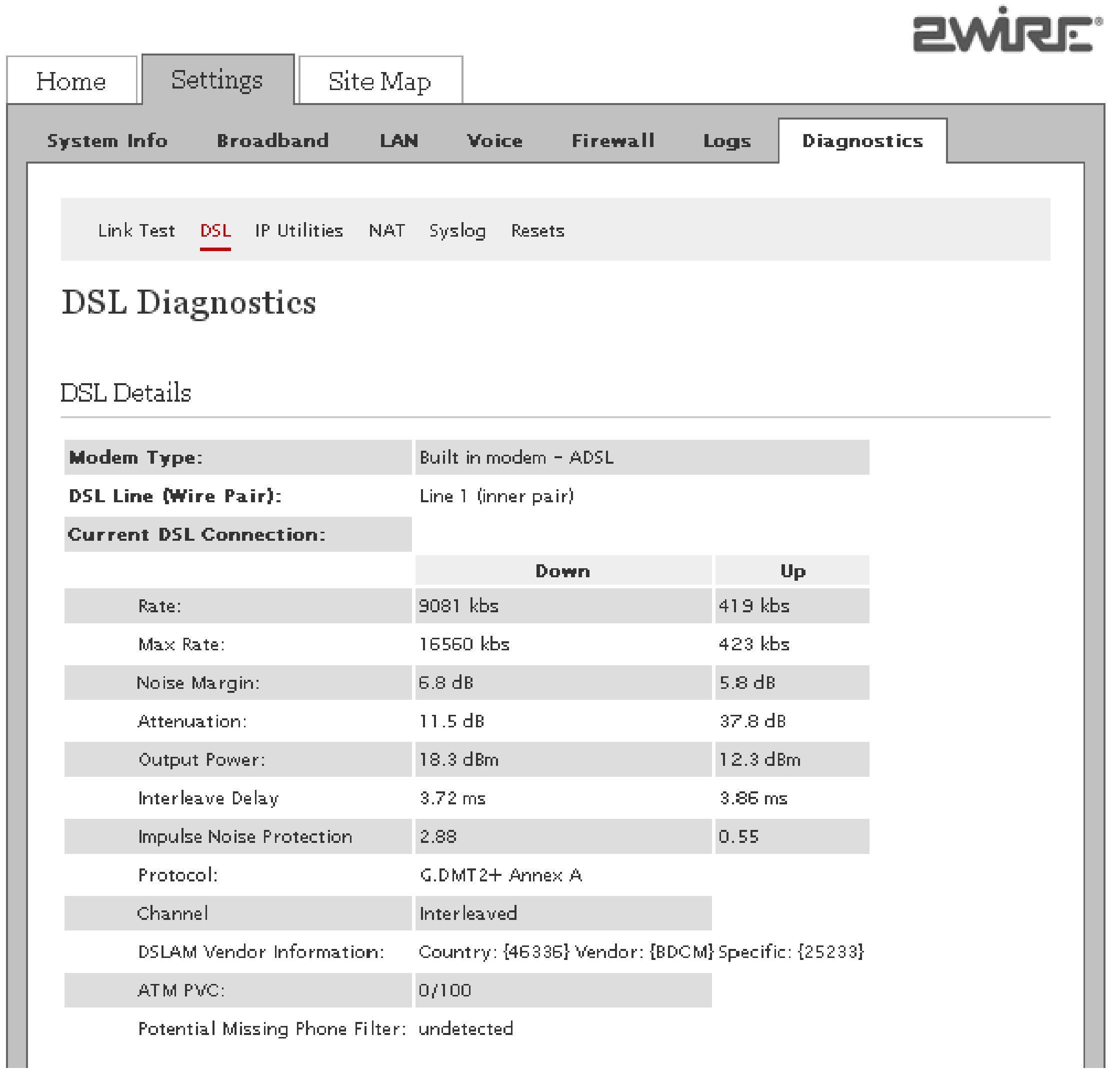
On the **Settings** tab, click **Diagnostics**, and then click **DSL**. The following panels are displayed:

- DSL Details
- DSL Link Errors
- Bitloading

Note The **DSL** page is not visible if you select **Ethernet** as the WAN interface type on the **Link Configuration** page.

DSL Details

Refer to the following image and table for information about the parameters listed in the **DSL Details** panel:



DSL Diagnostics

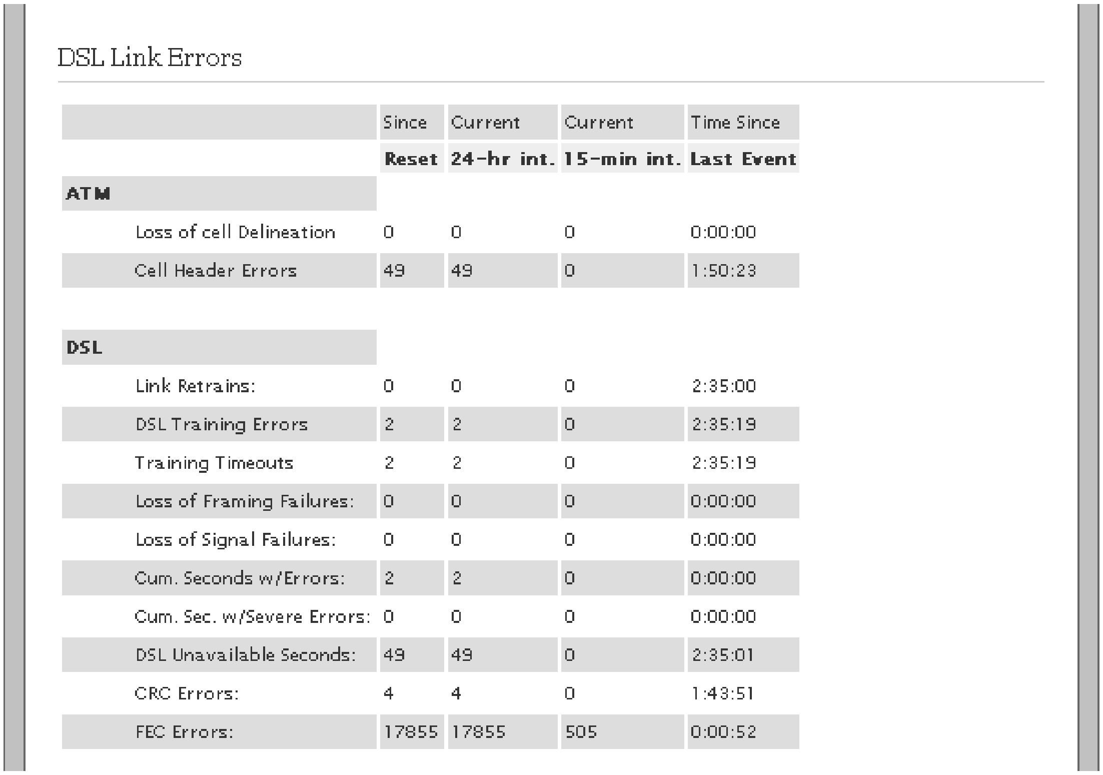
DSL Details

Modem Type:	Built in modem - ADSL	
DSL Line (Wire Pair):	Line 1 (inner pair)	
Current DSL Connection:		
	Down	**Up**
Rate:	9081 kbs	419 kbs
Max Rate:	16560 kbs	423 kbs
Noise Margin:	6.8 dB	5.8 dB
Attenuation:	11.5 dB	37.8 dB
Output Power:	18.3 dBm	12.3 dBm
Interleave Delay	3.72 ms	3.86 ms
Impulse Noise Protection	2.88	0.55
Protocol:	G.DMT2+ Annex A	
Channel	Interleaved	
DSLAM Vendor Information:	Country: {46336} Vendor: {BDCM} Specific: {25233}	
ATM PVC:	0/100	
Potential Missing Phone Filter:	undetected	

Parameter	Description
Modem Type	Displays the type of modem: • **Built-in ADSL modem** -or- • **External Broadband modem through the Internet**
DSL Line (Wire Pair)	Displays **Line 1 (inner pair)**, **Line 2 (outer pair)**, or **searching for DSL signal**. During installation, the gateway auto-detects whether the DSL signal is on Line 1 or Line 2.
Current DSL Connection	
Rate	Displays the upload and download speeds in kilobits per second.
Max Rate	Displays the maximum trained rates for upstream and downstream data in kilobits per second.
Noise Margin	Displays the current downstream and upstream noise margin in dB.
Attenuation	Displays the current downstream and upstream DSL attenuation in dB.
Output Power	Displays the current downstream and upstream DSL transmit and receive power in dB.
Interleave Delay	Displays the downstream and upstream interleave delay duration in milliseconds (ms).
Impulse Noise Protection	Displays the measurement of how much impulse noise can be mitigated. It is dependent on the current line configuration.
Protocol	Displays the protocol used to communicate between your gateway and your ISP.
Channel	Displays the setting that is determined by your ISP's DSLAM equipment. Values are **Fast** or **Interleaved**.
DSLAM Vendor Information	Lists information about the DSLAM, including country, DSLAM vendor, and specifics.
ATM PVC	Displays the VPI/VCI value currently in use by your ISP.
Potential Missing Phone Filter	Detects if the DSL port of the gateway is connected to the phone socket through a DSL phoneline filter.

DSL Link Errors

Refer to the following image and table for information about the parameters listed in the **DSL Link Errors** panel:



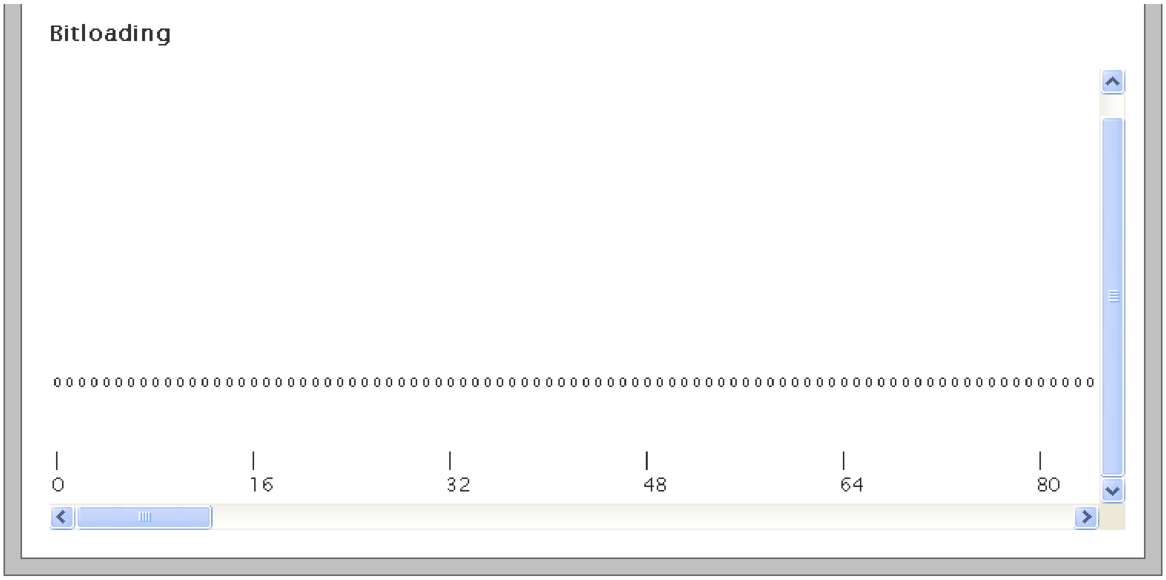
DSL Link Errors

	Since	Current	Current	Time Since
	Reset	**24-hr int.**	**15-min int.**	**Last Event**
ATM				
Loss of cell Delineation	0	0	0	0:00:00
Cell Header Errors	49	49	0	1:50:23
DSL				
Link Retrains:	0	0	0	2:35:00
DSL Training Errors	2	2	0	2:35:19
Training Timeouts	2	2	0	2:35:19
Loss of Framing Failures:	0	0	0	0:00:00
Loss of Signal Failures:	0	0	0	0:00:00
Cum. Seconds w/Errors:	2	2	0	0:00:00
Cum. Sec. w/Severe Errors:	0	0	0	0:00:00
DSL Unavailable Seconds:	49	49	0	2:35:01
CRC Errors:	4	4	0	1:43:51
FEC Errors:	17855	17855	505	0:00:52

Parameter	Description
ATM	
Loss of cell Delineation	Displays the number of loss of cell delineation events since the last reset.
Cell Header Errors	Displays the number of cell header errors since the last reset.
DSL	
Link Retrains	Displays the number of DSL retrains since the gateway was last restarted, and the time elapsed since the last retrain.
DSL Training Errors	Displays the number of failed DSL retrains since the gateway was last restarted, and the elapsed time since the last failed retrain.
Training Timeouts	Displays the number of timeouts waiting for response from ATU-C since the gateway was last restarted, and the elapsed time since the last initialization timeout.
Loss of Framing Failures	Displays the number of DSL loss of framing failures since the gateway was last restarted, and the elapsed time since the last line search initialization.
Loss of Signal Failures	Displays the number of DSL loss of signal failures since the gateway was last restarted, and the elapsed time since the last loss of signal failure.
Cum. Seconds w/Errors	Displays the number of cumulative errored seconds since the gateway was last restarted, and the elapsed time since the last error.
Cum. Sec. w/Severe Errors	Displays the number of severely errored seconds since the gateway was last restarted, and the elapsed time since the last severely errored second.
DSL Unavailable Seconds	Displays the DSL link unavailable seconds after the ISP connection was established and the statistics were last reset. Also displays the elapsed time since the last establishment.
CRC Errors	Displays the cyclic redundancy check errors.
FEC Errors	Displays the forward error correction errors.

Bitloading

The **Bitloading** panel lets you view the graphic representation of DSL bitloading.



Bitloading

```
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

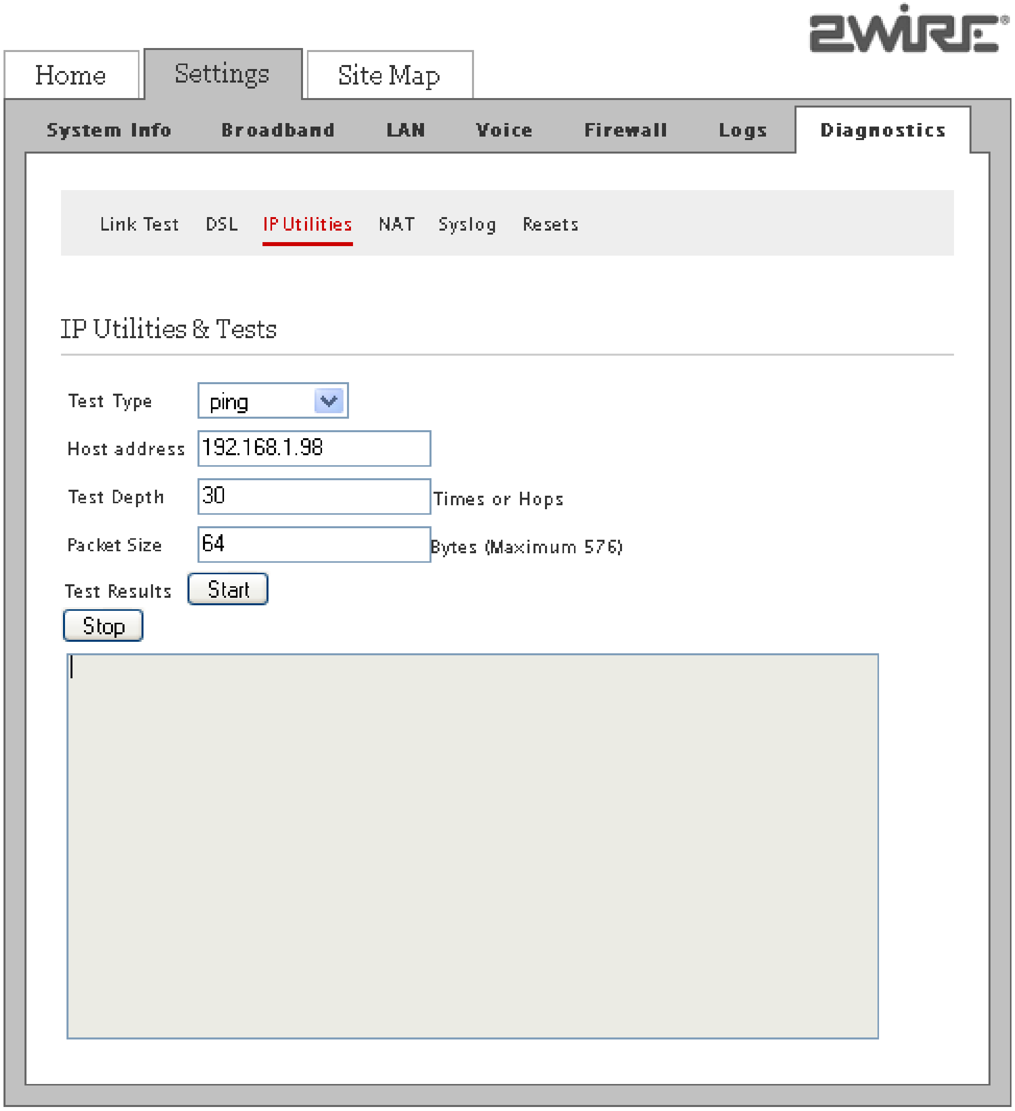
Testing IP Utilities

Objective

To test the gateway IP utilities such as ping, traceroute, and DNS query. This lets you determine if there are any communication issues between the gateway and the host/Internet.

Steps

1. On the **Settings** tab, click **Diagnostics**, and then click **IP Utilities**.



IP Utilities & Tests

Test Type: ping

Host address: 192.168.1.98

Test Depth: 30 Times or Hops

Packet Size: 64 Bytes (Maximum 576)

Test Results

2. Select the **Test Type** option from the drop-down list box:
   - If you select **ping** from the drop-down list box, you can test whether a particular host is reachable across an IP network. Also, you can self-test the network interface card of the computer, or use the tool for latency test.
   - If you select **traceroute** from the drop-down list box, you can determine the route taken by the data packets across an IP network.
   - If you select **dnsquery** from the drop-down list box, you can test if your gateway is resolving the domain name to IP address.

3. Type the IP address of the destination in the **Host Address** text box.
4. Click **Start** or **Stop** testing.

   You can view the results in the area below the **Test Results** text box.

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

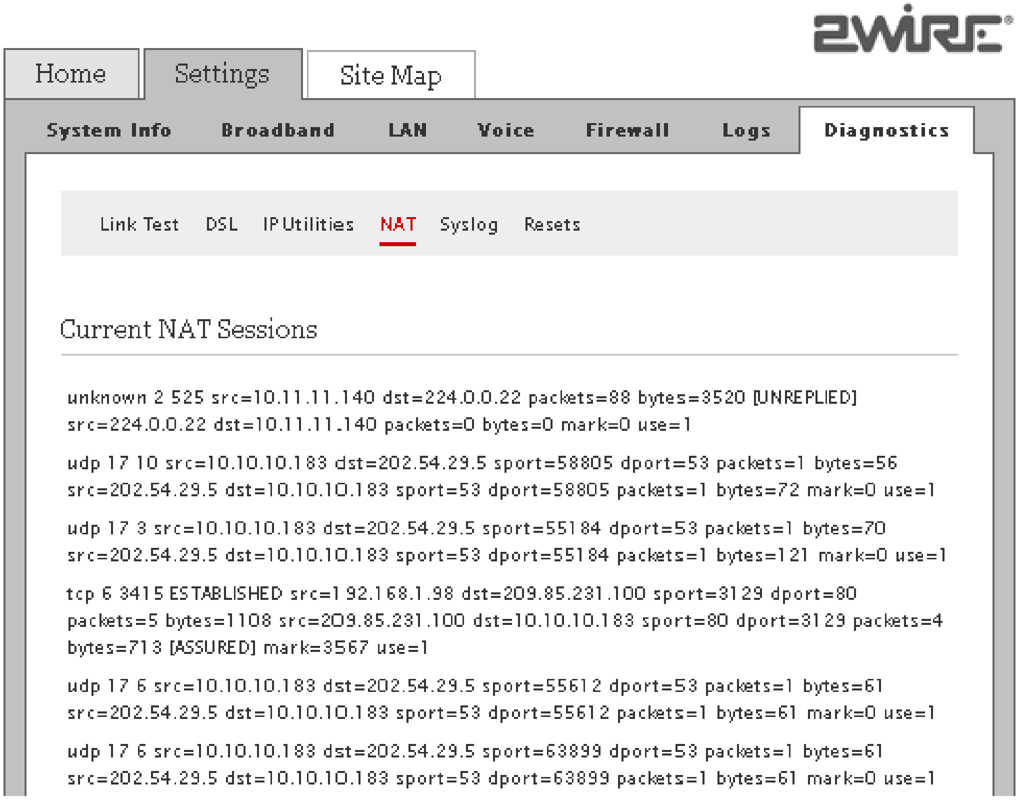
Viewing NAT Information

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

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

On the **Settings** tab, click **Diagnostics**, and then click **NAT**.

The **Current NAT Sessions** panel displays the data pertaining to the sessions initiated from the LAN client. This panel also displays the data sent to the LAN client, if port forwarding is enabled for a LAN computer.



Current NAT Sessions

```
unknown 2 525 src=10.11.11.140 dst=224.0.0.22 packets=88 bytes=3520 [UNREPLIED]
src=224.0.0.22 dst=10.11.11.140 packets=0 bytes=0 mark=0 use=1

udp 17 10 src=10.10.10.183 dst=202.54.29.5 sport=58805 dport=53 packets=1 bytes=56
src=202.54.29.5 dst=10.10.10.183 sport=53 dport=58805 packets=1 bytes=72 mark=0 use=1

udp 17 3 src=10.10.10.183 dst=202.54.29.5 sport=55184 dport=53 packets=1 bytes=70
src=202.54.29.5 dst=10.10.10.183 sport=53 dport=55184 packets=1 bytes=121 mark=0 use=1

tcp 6 3415 ESTABLISHED src=192.168.1.98 dst=209.85.231.100 sport=3129 dport=80
packets=5 bytes=1108 src=209.85.231.100 dst=10.10.10.183 sport=80 dport=3129 packets=4
bytes=713 [ASSURED] mark=3567 use=1

udp 17 6 src=10.10.10.183 dst=202.54.29.5 sport=55612 dport=53 packets=1 bytes=61
src=202.54.29.5 dst=10.10.10.183 sport=53 dport=55612 packets=1 bytes=61 mark=0 use=1

udp 17 6 src=10.10.10.183 dst=202.54.29.5 sport=63899 dport=53 packets=1 bytes=61
src=202.54.29.5 dst=10.10.10.183 sport=53 dport=63899 packets=1 bytes=61 mark=0 use=1
```

Enabling Syslog

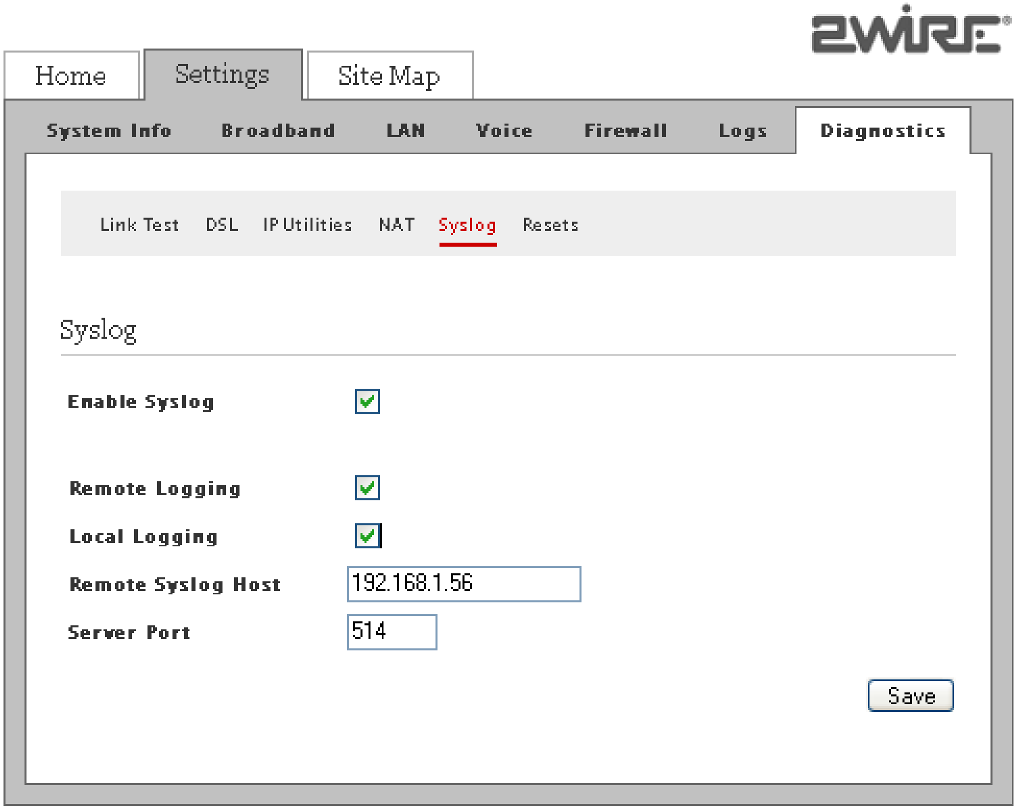
Objective

To enable the syslog feature for sending system logs to a remote server.

Note Syslog service must be installed and configured on the remote server for receiving the system logs.

Steps

1. On the **Settings** tab, click **Diagnostics**, and then click **Syslog**.



Syslog

Enable Syslog ☑

Remote Logging ☑

Local Logging ☑

Remote Syslog Host 192.168.1.56

Server Port 514

2. Select the **Enable Syslog** check box.
3. Select the **Remote Logging** check box to reproduce the logs on a remote computer that is running the syslog server.
4. Select the **Local Logging** check box to reproduce the logs on the local node running the syslog server.
5. Enter the IP address of the computer running the syslog server in the **Remote Syslog Host** text box.
6. Enter the outbound port number where the syslog server is located in the **Server Port** text box.

   Note Ensure that the outbound port number in the node running syslog server matches the value listed in this text box.

7. Click **Save**.

Resetting the Gateway

Objective

To reset the gateway.

You may have to reset the gateway if any or all the LEDs are solid red. This indicates that there is some failure within the gateway.

Note It is recommended that you contact customer service before attempting to reset your gateway.

Steps

1. On the **Settings** tab, click **Diagnostics**, and then click **Resets**.
2. You can perform the following tasks:
   - Resetting System and Links on page 81
   - Resetting Device to Factory Default on page 82

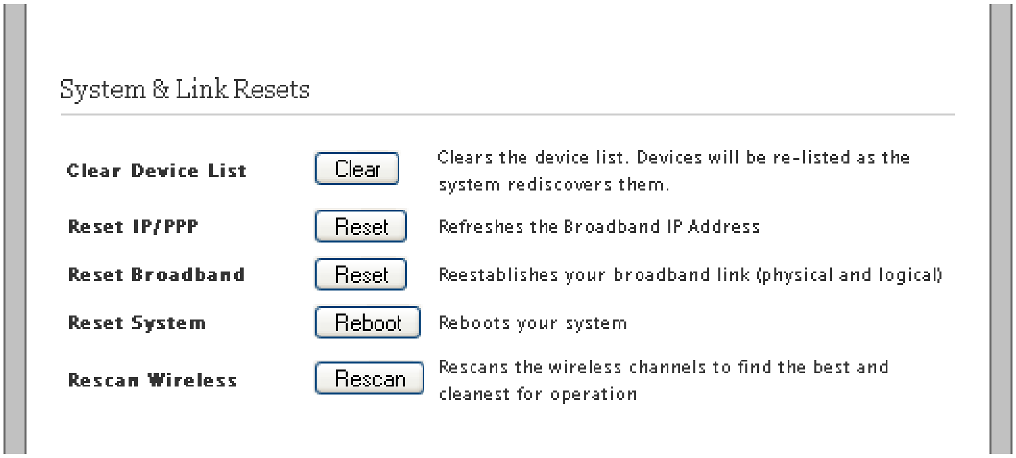
Note When you reset or reboot the gateway, it may take several minutes before the Broadband service is restored.

Resetting System and Links

You can clear the list of networked devices, reset the IP/PPP, reestablish the Broadband link, and restart your gateway in this panel.

To reset the gateway parameters:

1. On the **Settings** tab, click **Diagnostics**, and then click **Resets**.
2. Navigate to the **System and Link Resets** panel.



System & Link Resets

Clear Device List	Clear	Clears the device list. Devices will be re-listed as the system rediscovers them.
Reset IP/PPP	Reset	Refreshes the Broadband IP Address
Reset Broadband	Reset	Reestablishes your broadband link (physical and logical)
Reset System	Reboot	Reboots your system
Rescan Wireless	Rescan	Rescans the wireless channels to find the best and cleanest for operation

3. Click **Clear** next to the **Clear Device List** field if you want to clear the device list on the home page and the status page under LAN.

   Devices will be re-listed as the gateway rediscovers them.

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

4. Click **Reset** next to the **Reset IP/PPP** field if you want to refresh the Broadband IP address.
5. Click **Reset** next to the **Reset Broadband** field if you want to reestablish your Broadband connection.

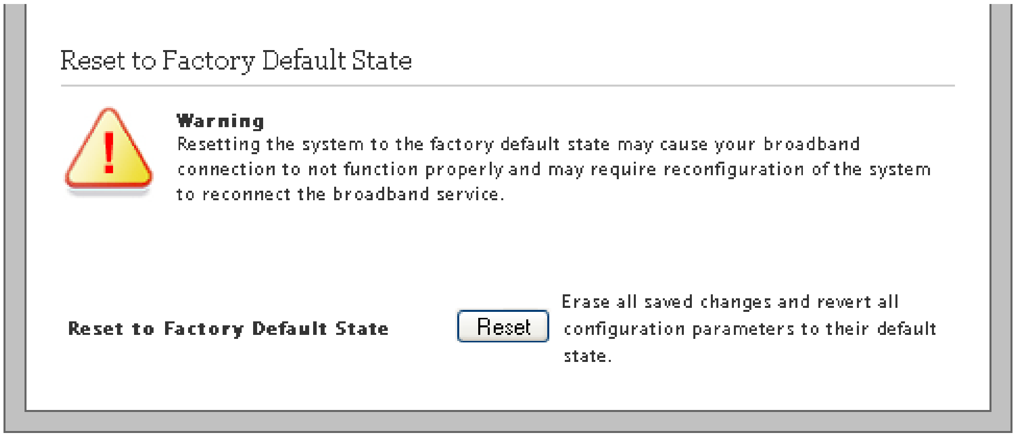
6. Click **Reboot** next to the **Reset System** field if you want to reboot your gateway.
7. Click **Rescan** next to the **Rescan Wireless** field if you want to refresh the list of wireless access points and find the most suitable one for your use.

Resetting Device to Factory Default

The **Reset to Factory Default State** panel lets you reset the gateway to factory default settings.

To reset the gateway to factory default settings:

1. On the **Settings** tab, click **Diagnostics**, and then click **Resets**.
2. Navigate to the **Reset to Factory Default State** panel.



Reset to Factory Default State

Warning
Resetting the system to the factory default state may cause your broadband connection to not function properly and may require reconfiguration of the system to reconnect the broadband service.

Reset to Factory Default State Reset Erase all saved changes and revert all configuration parameters to their default state.

3. Click **Reset** next to the **Reset to Factory Default State** field if you want to reset the configured parameters on the gateway to the factory default settings.

⚠ Resetting the gateway to factory default will erase all saved changes and revert all configuration parameters to their default values.

See Also

Managing LAN Devices on page 28

Managing Firewall Settings on page 56

Managing Broadband Settings on page 18

Diagnostic Issues on page 85

CHAPTER 11

Troubleshooting Configuration Issues

This chapter provides information about troubleshooting software configuration and operational issues. It lists the possible cause(s) and solution(s) for the issues. The issues are based on likely user scenarios.

Broadband Issues

The following table provides information to troubleshoot Broadband issues:

Issue	Possible Cause(s)	What to Do
Unable to connect to the Internet	Incorrect interface type	On the **Settings** tab, click **Broadband**, and then click **Link Configuration**. Select the correct interface type from the **Choose Interface type** drop-down list box.
	Incorrect line type	On the **Settings** tab, click **Broadband**, and then click **Link Configuration**. Select the correct line type from the **DSL Standard** drop-down list box.
	Incorrect connection type	On the **Settings** tab, click **Broadband**, and then click **Link Configuration**. Select the correct connection type from the **Connection Type** drop-down list box.
	Incorrect PPP authentication settings	On the **Settings** tab, click **Broadband**, and then click **Link Configuration**. Enter the correct **Username** and **Password** in the text boxes.
	Routing is disabled (This results in the gateway not getting the IP address automatically from the ISP.)	On the **Settings** tab, click **Broadband**, and then click **Link Configuration**. Select the **Routing** check box.
Unable to get public IP address on LAN computers	Gateway in route mode	Disable the route mode. This disables Routing and NAT on the gateway.

Connection Issues

The following table provides information to troubleshoot connection issues:

Issue	Possible Cause(s)	What to Do
No ETHERNET light	Ethernet interface is disabled	On the **Settings** tab, click **LAN**, and then click **Wired Interface**. Select the **Ethernet Networking** check box.
No WIRELESS light	Wireless Interface is disabled	On the **Settings** tab, click **LAN**, and then click **Wireless**. Select the **Enable Wireless Interface** check box.
	LAN clients are not connected to the gateway through the wireless interface	Ensure that at least one LAN client is connected to the wireless connection of the gateway.
Internet is not accessible but user interface of the gateway is accessible	Incorrect Broadband settings	• On the **Settings** tab, click **Broadband**, and then click **Status.** Check the connectivity status of Internet and DSL Link. • Restart the gateway to refresh the Broadband connection.
	Incorrect LAN computer settings	Ensure that the correct settings are configured on the LAN computer.

VoIP Issues

The following table provides information to troubleshoot VoIP issues:

Issue	Possible Cause(s)	What to Do
No VoIP service	VoIP services are not activated	• On the **Settings** tab, click **Voice**, and then click **Status.** Check your line status. • Contact your ISP regarding VoIP service activation.
No dial tone	Service is down	On the **Settings** tab, click **Voice**, and then click **Status.** Check your line status.

System Information Issues

The following table provides information to troubleshoot system information issues:

Issue	Possible Cause(s)	What to Do
Unable to set time and date manually	**Override Automatic Time Configuration** check box is not selected	Select the **Override automatic time configuration** check box to apply the manually configured time and date settings. Ensure that you configure the time in hh:mm:ss format and date in yyyy/mm/dd format before selecting the check box.

LAN Issues

The following table provides information to troubleshoot LAN issues:

Issue	Possible Cause(s)	What to Do
Unable to connect to the gateway through the local Ethernet port	Ethernet networking is disabled	On the **Settings** tab, click **LAN**, and then click **Wired Interfaces.** Select the **Ethernet Networking** check box.
LAN clients are not getting IP addresses to connect to the gateway	DHCP server is disabled	On the **Settings** tab, click **LAN**, and then click **DHCP**. Select the **DHCP Server Enabled** check box for enabling the gateway to assign IP addresses to the LAN clients automatically.
IP address conflict between LAN computers on the network	Duplication of IP address on the network	If the LAN computer has static IP configured, ensure that DHCP IP addressing on the gateway is not assigning an identical IP address. Change the DHCP server IP addressing range and try assigning a different static IP address to the LAN computers. If the issue persists, then configure DHCP on the LAN computer to obtain the IP address automatically.
Wireless client is not locating the gateway	SSID Broadcast is disabled	On the **Settings** tab, click **LAN**, and then click **Wireless**. Select the **SSID Broadcast** check box in the **Network** panel.
Wireless client is not getting an IP address	Wireless networking is disabled	On the **Settings** tab, click **LAN**, and then click **Wireless**. Select the **Enable Wireless Interface** checkbox.
	Incorrect authentication type is used	Ensure that you select the relevant authentication type for configuring your wireless client.
Wireless signal strength is weak	Incorrect power settings	Change the **Power Setting** value to increase the signal strength.
	Wireless channel interference	Change the **Wireless Channel** value. Alternatively, you can also change the Wireless Channel Mode to “auto”.

Issue	Possible Cause(s)	What to Do
Setting custom encryption key on the user interface gives an error	Custom encryption key is not conforming with the security mode, key length, key type, or value type	Configure the custom encryption key in a way that it conforms to the security mode, key length, key type, or value type.
LAN clients are unable to access specific applications or Web sites	Firewall is preventing the LAN clients from accessing specific applications or Web sites	Refer to Hosting an Application on page 59 for rendering Internet access to specific applications.

Firewall Issues

The following table provides information to troubleshoot firewall issues:

Issue	Possible Cause(s)	What to Do
HTTP service not available	HTTP traffic is disabled	On the **Settings** tab, click **Firewall**, and then click **Advanced Configuration**. Select the **HTTP** checkbox from the **Outbound Protocol Control** panel to enable the HTTP traffic to pass through the firewall.
Unable to connect to the VPN tunnel	Unsupported port	Check if the VPN service supports PPPoE, L2TP, PPTP, and IPSec ports. If not, then you must open the supported port by adding a new user-defined application.

Diagnostic Issues

The following table provides information to troubleshoot diagnostic issues:

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

APPENDIX A

Glossary

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

Term	Description
MTU (Maximum Transmission Unit)	The largest size packet or frame, specified in octets (eight-bit bytes), that can be sent from a computer to the network. The Internet's TCP uses the MTU to determine the maximum size of each packet in any transmission. If the MTU is too large, the packet may have to be retransmitted if it encounters a router that can't handle such a large packet. Too small MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled. Most computer operating systems provide a default MTU value that is suitable for most users. In general, Internet users should follow the advice of their Internet Service Provider (ISP) about whether to change the default value and what to change it to.
NAT (Network Address Translation)	Enables a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. This feature is used by the gateway so an end user can have an internal computer network in their home, with all its computers using internal IP addresses, using only one routable IP address, which accesses the outside (Internet).
PAT (Port Address Translation)	Allows hosts on a LAN to communicate with the rest of a network (such as the Internet) without revealing their own private IP address. All outbound packets have their IP address translated to the router’s external IP address. Replies come back to the router, which then translates them back into the private IP address of the original host for final delivery.
PPP (Point-to-Point Protocol)	A protocol that allows a computer to access the Internet using a dial-up phone line and a high-speed modem. This can be accomplished over Ethernet (PPPoE), or over Asynchronous Transfer Mode (ATM, PPPoA).
PPPoA (Point-to-Point Protocol over ATM)	A specification for connecting multiple computer users on an Ethernet LAN to a remote site through common customer premises equipment (such as a modem). PPPoA combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the ATM (Asynchronous Transfer Mode) protocol, which supports multiple users in a LAN.
PPPoE (Point-to-Point Protocol over Ethernet)	A specification for connecting multiple computer users on an Ethernet LAN to a remote site through common customer premises equipment (such as a modem). PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a LAN.
Protocol Timeout	The amount of time (in seconds) during which a connection in the specified range remains open when there is no data transfer. After a connection has been established on a given port, the sender and receiver usually determine when the session is finished and the connection is closed. However, if the connection is left open and data transfer stops, the gateway must eventually close the connection and reclaim the resources in order to protect your network. In some cases, the gateway might close the application during normal operation (for example, if there is a long pause between data transfer). In such cases, lengthening the timeout may help.
PVC (Permanent Virtual Circuit)	A virtual circuit that is permanently available. Used to establish connections between hosts that communicate frequently.
Router	The central switching device in a packet-switched computer network that directs and controls the flow of data through the network.

<table>
<tr><th>Term</th><th>Description</th></tr>
<tr><td>Subnet Mask</td><td>The IP addressing system allows subnetworks or “interchanges” to be created, and devices numbers or “extensions” to be established within these subnetworks. These numbers are created using a mathematical device called a subnet mask. A subnet mask, like the IP address, is a set of four numbers in dotted decimal notation. Subnet masks typically take three forms:
• 255.0.0.0
• 255.255.0.0
• 255.255.255.0
The number 255 “masks” out the corresponding number of the IP address, resulting in IP address numbers that are valid for the network. For example, an IP address of 123.45.67.89 and a subnet mask of 255.255.255.0 results in a sub network number of 123.45.67.0 and a device number of 89.
The subnet mask used for the network typically corresponds to the class of IP address assigned, as shown in the following table:
<table>
<tr><th>IP Address Class</th><th>Dotted-Decimal Notation</th><th>Ranges Corresponding Subnet Mask</th></tr>
<tr><td>Class A</td><td>1.<i>xxx.xxx.xxx</i> to 126.<i>xxx.xxx.xxx</i></td><td>255.0.0.0</td></tr>
<tr><td>Class B</td><td>128.0.<i>xxx.xxx</i> to 191.255.<i>xxx.xxx</i></td><td>255.255.0.0</td></tr>
<tr><td>Class C</td><td>192.0.0.<i>xxx</i> to 223.255.255.<i>xxx</i></td><td>255.255.255.0</td></tr>
</table>
</td></tr>
<tr><td>SYN Flood</td><td>A method that the user of a hostile client program can use to conduct a denial-of-service (DOS) attack on a computer server. The hostile client repeatedly sends SYN (synchronization) packets to every port on the server, using fake IP addresses.</td></tr>
<tr><td>TCP/IP (Transmission Control Protocol/Internet Protocol)</td><td>A method of packet-switched data transmission used on the Internet. The protocol specifies the manner in which a signal is divided into parts, as well as the manner in which “address” information is added to each packet to ensure that it reaches its destination and can be reassembled into the original message.</td></tr>
<tr><td>UDP (User Datagram Protocol)</td><td>A TCP/IP protocol describing how data packets reach application programs within a destination computer.</td></tr>
<tr><td>VPI (Virtual Path Identifier)</td><td>Identifier contained in the ATM cell header to designate the virtual path on the physical ATM link.</td></tr>
<tr><td>VCI (Virtual Channel Identifier)</td><td>Identifier contained in the ATM cell header to designate the virtual channel on the physical ATM link.</td></tr>
<tr><td>Wireless</td><td>Transmission of data over radio waves rather than wiring.</td></tr>
</table>